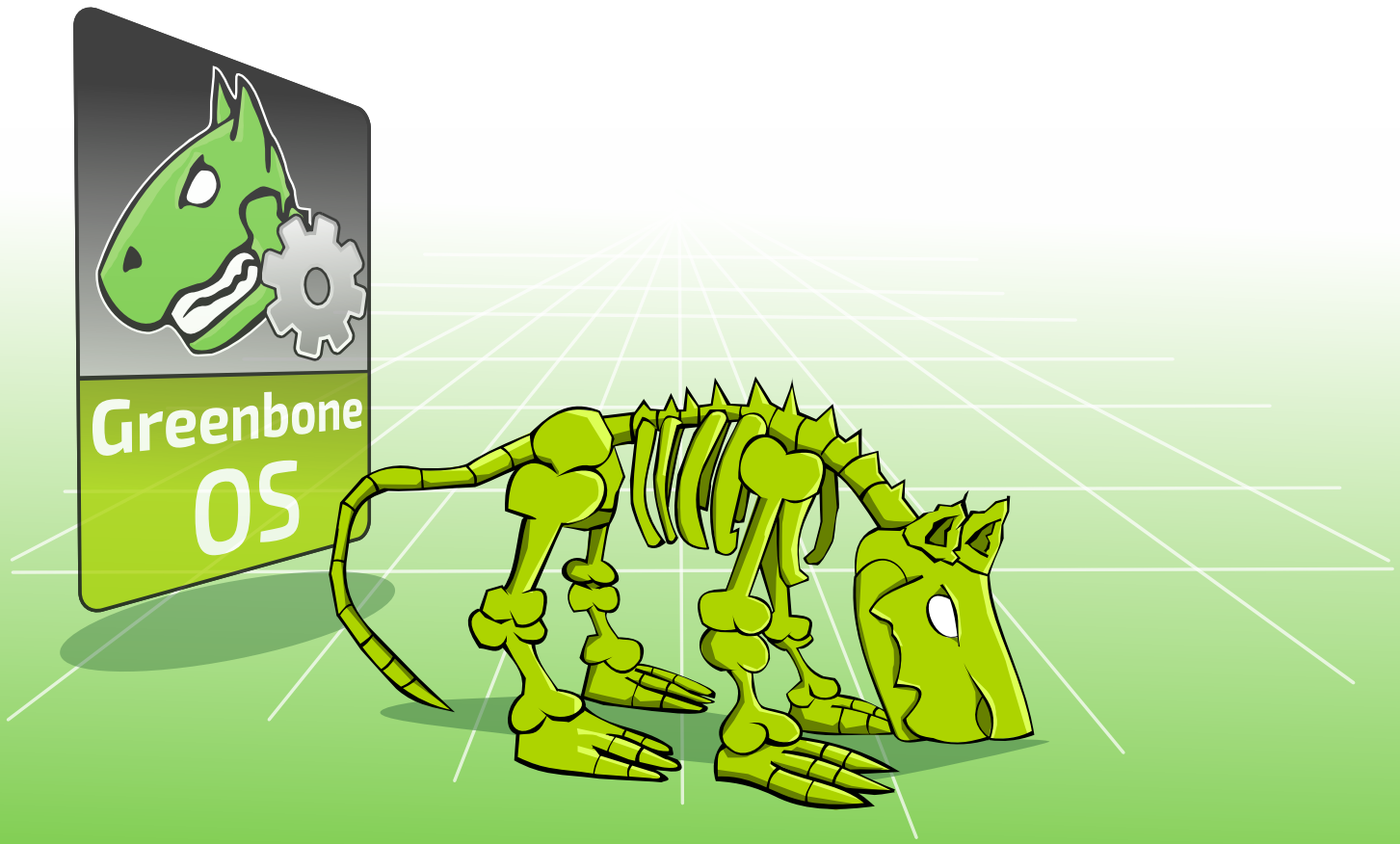
Greenbone

Security Manager

with

Greenbone OS 4



User Manual

Greenbone

Sustainable Resilience

Greenbone

Sustainable Resilience

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück Germany
http://www.greenbone.net

Status: GOS 4, April 4, 2018

This is the manual for the Greenbone Security Manager with Greenbone OS (GOS) version 4. Due to the numerous functional and other differences between GOS 4 and previous versions, this manual should not be used with older versions of GOS.
The Greenbone Security Manager is under constant development. This manual attempts to always document the latest software release. It is, however, possible that latest functionality has not been captured in this manual.
Should you have additional notes or error corrections for this manual please send an email to support (mailto:support@greenbone.net).

Contributers to this manual are:

- Greenbone Networks GmbH
- OpenSource Training Ralf Spenneberg
- Alexander Rau, arX IT Services

Contents

CHAPTER 1

Introduction

Vulnerability management is a core element in modern information technology (IT) compliance. IT compliance is defined as the adherence to legal, corporate and contractual rules and regulations as they relate to IT infrastructures. Within its context IT compliance mainly relates to information security, availability, storage and privacy. Companies and agencies have to comply with many legal obligations in this area.

The control and improvement in IT security is an ongoing process that consists at a minimum of these three steps:

- Discovery of the current state
- Taking actions to improve the current state
- Review of the measures taken

The Greenbone Security Manager (GSM) assists companies and agencies with automated and integrated vulnerability assessment and management. Its task is to discover vulnerabilities and security gaps before a potential attacker would. GSM can achieve this through different perspectives of an attacker:

External The GSM attacks the network externally. This way it can identify badly configured or misconfigured firewalls.

DMZ Here the GSM can identify actual vulnerabilities. These could be exploited by attackers if they get past the firewall.

Internal Many attacks are executed internally by insiders through methods of social engineering or a worm. This is why this perspective is very important for the security of the IT infrastructure.

For DMZ and internal scans it can be differentiated between authenticated and non-authenticated scans. When performing an authenticated scan the GSM uses credentials and can discover vulnerabilities in applications that are not running as a service but have a high risk potential. This includes web browsers, office applications or PDF viewers. For a further discussion on the advantages and disadvantages on authenticated scans see section *Pros and Cons of Authenticated Scans* (page 92).

Due to new vulnerabilities being discovered on a daily basis, regular updates and testing of systems are required. The Greenbone Security Feed ensures that the GSM is provided with the latest testing routines and can discover the latest vulnerabilities reliably. Greenbone analyzes CVE [1] messages and security bulletins of vendors and develops new testing routines daily.

With a scan using the Greenbone Security Manager, staff responsible for IT, receive a list of vulnerabilities that have been identified on the network. Especially if no vulnerability management has been practiced, the list is often extensive. For the selection of remediation measures a prioritization is inevitable. Most important are the measures that protect against critical risks and remediate those respective security holes.

[1] The Common Vulnerability and Exposures (CVE) project is a vendor neutral forum for the identification and publication of new vulnerabilities.

The GSM utilizes the Common Vulnerability Scoring System (CVSS). CVSS is an industry standard for the classification and rating of vulnerabilities. This assists in prioritizing the remediation measures.

To deal with vulnerabilities fundamentally two options exist:

1. Removal of the vulnerability through updating the software, removal of the component or a change in configuration.
2. Implementation of a rule in a firewall or intrusion prevention system (virtual patching).

Virtual patching is the apparent remediation of the vulnerability through a compensating control. The real vulnerability still exists. The attacker can still exploit the vulnerability if the compensating control fails or by utilizing an alternate approach. An actual patch/update of the affected software is always preferred over virtual patching.

The Greenbone Security Manager supports the testing of the implemented remediation measures as well. With its help responsible IT staff can document the current state of IT security, recognize changes and document these changes in reports. To communicate with management the GSM offers abstraction of technical details in simple graphics or in the form of a traffic light that displays the state of security in the colours red, yellow and green. This way the IT security process can be visualized in a simplified way.

Read Before Use

The Greenbone Security Manager (GSM) includes a full-featured Vulnerability Scanner. While the vulnerability scanner is designed to have a minimal invasive impact on your network environment, it still needs to interact and communicate with the target systems which are analyzed during a vulnerability scan.

Remember that it is the fundamental task of this solution to find and identify otherwise undetected vulnerabilities. The scanner must behave to a certain extent like a real attacker would.

While the default and recommended settings reduce the impact of the vulnerability scanner to the environment to a minimum, unwanted side effects may still occur. The scanner settings allow the control and refinement of the scanner's effects. Please be aware of the following general side effects:

- Log and alert messages may show up on the target systems triggered by the probes of the vulnerability scanner.
- Log and alert messages may show up on firewalls and intrusion detection and prevention systems.
- Scans may increase latency on the target and/or the network being scanned, in extreme cases resulting in situations similar to a denial of service (DoS) attack.
- Scans may trigger bugs in fragile or insecure applications resulting in faults or crashes.
- Scans may result in user accounts being locked due to the testing of default username/password combinations.
- Embedded systems and elements of operational technology with weak network stacks are especially subject to possible crashes or even broken devices.

Remember that triggering faults, crashes or locking with default settings means that an attacker can do the very same at unplanned times and to an unplanned extent. Finding out about it earlier than the attacker is the key to resilience.

While these side effects are very rare when using the default and recommended settings, the vulnerability scanner allows the configuration of invasive behavior and thus will increase the probability of the above listed effects.

Before using the GSM to scan the target systems in your environment please be aware of these facts and verify that you are authorized to execute such scans.

GSM Overview

The Greenbone Security Manager is a dedicated appliance for vulnerability scanning and vulnerability management. It is a specifically developed platform optimized for vulnerability management. It is offered in different performance levels.

	GSM 6400	GSM 5300	GSM 650	GSM 600	GSM 400	GSM 100	GSM 25	GSM 25V	GSM One
Use Case	Large Enterprise/ Service Providers	Large Enterprise/ Service Providers	Medium Enterprise/ Branch Location	Medium Enterprise/ Branch Location	Medium Enterprise/ Branch Location	SME/ Small Branch Location	Sensor for Managed Services/ Branch Scans	Virtual Scan Sensor	Special use/ Training/ Audit-via-Laptop
Target IP Addresses	5,000-50,000	3,000-30,000	500-10,000	500-6,000	300-2,000	50-500	20-300	20-300	20-300
Ports									
Management/ Feed	1 out of band management	1 out of band management	1	1	1	1	1	N/A	N/A
Scan GbE-Base-TX	0-24 Ports	0-24 Ports	6 Ports	6 Ports	6 Ports	4 Ports	4 Ports	N/A	N/A
Scan SFP	0-24 Ports	0-24 Ports	2 Ports	2 Ports	2 Ports	-	-	N/A	N/A
Scan 10 GbE XFP	0-6 Ports	0-6 Ports	-	-	-	-	-	N/A	N/A
Virtual Ports	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1	1
Port Roles	1 management, others dynamic	1 management, others dynamic	8 ports dynamic	8 ports dynamic	8 ports dynamic	4 ports dynamic	4 ports dynamic	1 port management/ scan/ update	1 port management/ scan/ update
VLAN Support	256 per Ethernet Port	256 per Ethernet Port	128 per Ethernet Port	128 per Ethernet Port	64 per Ethernet Port	64 per Ethernet Port	64 per Ethernet Port	no	no
Hardware									
Fan speed control	-	-	✓	✓	✓	✓	✓	N/A	N/A
Redundant Fan	✓	✓	✓	✓	✓	-	-	N/A	N/A
Redundant P/S	✓	✓	-	-	-	-	-	N/A	N/A
Redundant HDD	✓	✓	-	-	-	-	-	N/A	N/A
Hot-Swap P/S	✓	✓	-	-	-	-	-	N/A	N/A
Hot-Swap HDD	✓	✓	-	-	-	-	-	N/A	N/A
Hot-Swap Fan	✓	✓	-	-	-	-	-	N/A	N/A
LCD	✓	✓	✓	✓	✓	-	-	N/A	N/A
GSM Networks									
Master Mode (Scan & Management)	up to 50 sensors	up to 30 sensors	up to 12 sensors	up to 12 sensors	up to 2 sensors	-	-	-	-
Slave Sensor Mode (Managed via Master)	✓	✓	✓	✓	✓	✓	✓	✓	-
Airgap Master	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	FTP	-	-	-
Airgab Slave	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	-	-	-
Greenbone OS									
SSH v2 support	✓	✓	✓	✓	✓	✓	✓	✓	✓
NTP	✓	✓	✓	✓	✓	✓	✓	–	–
GMP	✓	✓	✓	✓	✓	✓	✓	✓	✓
HTTPS (GUI)	✓	✓	✓	✓	✓	✓	-	-	✓
SNMP v2	✓	✓	✓	✓	✓	-	-	-	-
Syslog (UDP/ TCP/TLS)	✓	✓	✓	✓	✓	✓	✓	-	-
Alerts (SMTP, HTTP,...)	✓	✓	✓	✓	✓	✓	-	-	-
Report Plugins	✓	✓	✓	✓	✓	✓	-	-	✓
IPv6 support	✓	✓	✓	✓	✓	✓	✓	✓	✓
RAID	✓	✓	-	-	-	-	-	-	-
Certificate Management	✓	✓	✓	✓	✓	✓	-	-	✓
Backup/ Restore	USB, Periodic	USB, Periodic	USB, Periodic	USB, Periodic	USB, Periodic	USB	USB	VM Snapshot via Hypervisor	VM Snapshot via Hypervisor

3.1 Enterprise class (GSM 5300/6400)

The GSM 5300 and GSM 6400 are designed for the operation in large companies and agencies. The GSM 6400 can control sensors in up to 50 security zones and is recommended for up to 50,000 monitored IP addresses. The GSM 5300 can control sensors in up to 30 security zones and is recommended for up to 30,000 monitored IP addresses. The appliances themselves can be controlled as a slave sensor by another master.

Fig. 3.1: The GSM 6400 supports up to 50,000 IP addresses

The appliances in the enterprise class come in a 2U 19" chassis for easy integration into the data center. For easy installation and monitoring they are equipped with a two line, 16 characters per line LCD display. For uninterruptible operation they have redundant, hot swappable power supplies, hard drives and fans.

For management of the appliance, in addition to an out-of-band management Ethernet port, a serial port is available. The serial port is setup as a Cisco compatible console port.

To connect to the monitored systems both appliances can be equipped with three modules. The following modules can be used in any order:

- 8 Port Gigabit Ethernet 10/100/1000 Base-TX (copper)
- 8 Port Gigabit Ethernet SFP (small-form factor-pluggable)
- 2 Port 10-Gigabit Ethernet XFP

Up to 512 VLANs can be configured and managed per port for the GSM 6400 (total of 24576), up to 256 per port for the GSM 5300 (total of 12288).

3.2 Midrange class (GSM 400/600/650)

The GSM 400, GSM 600 and GSM 650 are designed for mid-sized companies and agencies as well as larger branch offices. The GSM 650 can control sensors in up to 12 security zones and is recommended for up to 10,000 monitored IP addresses. The GSM 600 can also control sensors in up to 12 security zones and is recommended for up to 6,000 monitored IP addresses. The GSM 400 can control 2 sensors and is recommended for up to 2,000 monitored IP addresses. The appliances themselves can be controlled as a slave sensor by another master.

Aside from the current GSM 400, GSM 600 and GSM 650 appliances, Greenbone is still fully supporting the older appliances in this class. The GSM 500, GSM 510 and GSM 550 appliances were replaced by more up to date hardware in 2014.

The appliances in the midrange class come in a 1U 19" chassis for easy integration into the data center. For easy installation and monitoring they are equipped with a two line, 16 characters per line LCD display. For uninterruptible operation the appliances come with redundant fans. However, hot-swapping during operation is not possible.

For management of the appliance, in addition to a management Ethernet port, a serial port is available. The serial port is setup as a Cisco compatible console port.

Fig. 3.2: The GSM 650 supports up to 10,000 IP addresses

To connect to the monitored systems both appliances are equipped with eight ports in total, which are pre-configured and set up as follows:

- 6 Port Gigabit Ethernet 10/100/1000 Base-TX (copper)
- 2 Port Gigabit Ethernet SFP (small-form factor-pluggable)

A modular configuration of the ports is not possible. Up to 64 VLANs can be configured and managed per port for the GSM 650 and GSM 600 (total of 512), 16 VLANs per port for GSM 400 (total of 128). One of these ports is also used as management port.

3.3 SME class (GSM 100)

The GSM 100 is designed for smaller companies and agencies as well as branches. The GSM 100 is recommended for the monitoring of up to 100 IP addresses. Controlling sensors in other security zones is not considered. However, the GSM 100 itself can be controlled as a slave-sensor by another master.

The appliance comes as 1U steel chassis. For easy integration into the data center an optional rack kit can be used. The appliance does not come with a display.

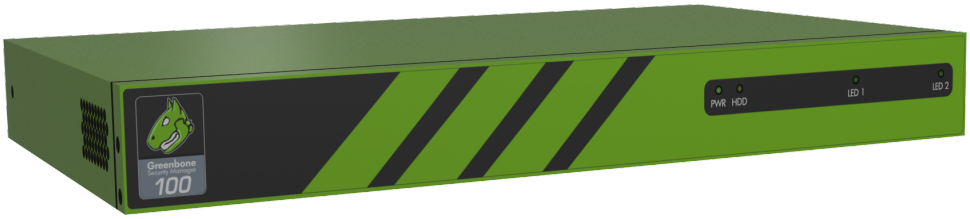


Fig. 3.3: The GSM 100 intended for smaller companies

For management of the appliance, in addition to a management Ethernet port, a serial port is available. The serial port is setup as a Cisco compatible console port.

To connect to the monitored systems the appliance comes with four 10/100/1000 Gigabit Ethernet Ports (RJ45) in total. These ports support up to 8 VLANs. One of these ports is also used as management port.

3.4 Sensors (GSM 25/25V)

The GSM 25 is designed as sensor for smaller companies and agencies as well as branches. The GSM 25 is recommended for up to 300 monitored IP addresses and requires the control of an additional appliance in master mode. The GSM of the midrange an enterprise class (GSM 500 and up) can be utilized as controllers for the GSM 25/25V.

The GSM 25 appliance comes as a 1U steel chassis. For easy integration into the data center an optional rack kit can be used. The appliance does not come with a display.

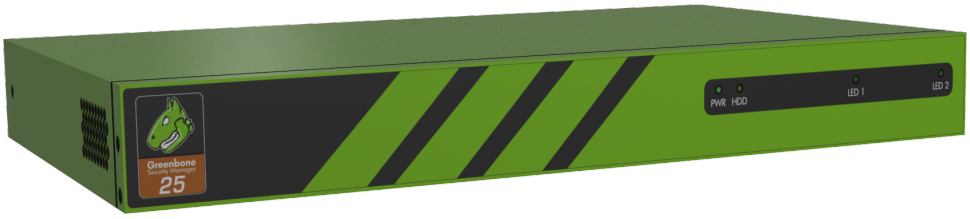


Fig. 3.4: The GSM 25 is a sensor and can only be operated with a GSM

For management of the appliance, in addition to a management Ethernet port, a serial port is available. The serial port is setup as a Cisco compatible console port.

To connect to the monitored systems the appliance comes with four 10/100/1000 Gigabit Ethernet Ports (RJ45) in total. These ports support up to 8 VLANs. One of these ports is also used as management port.

The GSM 25V is a virtual Appliance and provides a simple and cost effective option to monitor virtual infrastructures. In contrast to the GSM 25 the virtual version only comes with one virtual port for management, scanning and updates.

3.5 GSM ONE

The GSM ONE is designed for specific requirements such as audit using a laptop or educational purposes. The GSM ONE is recommended for up to 300 monitored IP addresses and can neither control other sensors nor be controlled as a sensor by a larger appliance.

The GSM ONE only comes with one virtual port that is used for management, scan and updates. This port does not support the use of VLANs.

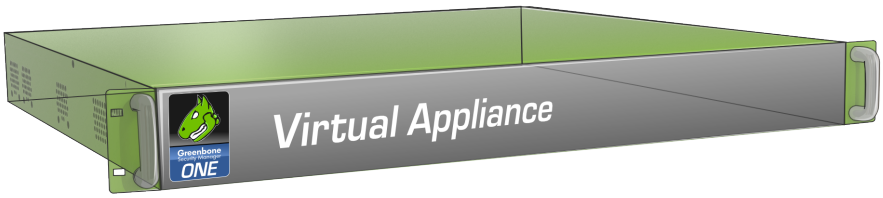


Fig. 3.5: The GSM ONE is a virtual instance.

The GSM ONE has all the functions of the larger systems except for the following:

- Master Mode: the GSM ONE cannot control other appliances as sensors.
- Slave Mode: the GSM ONE cannot be controlled as a slave sensor by other master-mode appliances.
- Alerts: the GSM ONE cannot send any alerts via SMTP, SNMP, syslog or HTTP.
- VLANs: the GSM ONE does not support VLANs on the virtual port.

3.6 GSM CE

The Greenbone Security Manager Community Edition (GSM CE) is a derivative of the GSM ONE for evaluation purposes. The GSM CE may be deployed using VirtualBox on Microsoft Windows, MacOS and Linux systems.

In contrast to the commercial version the GSM CE uses the OpenVAS Community Feed instead of the Greenbone Security Feed. While the commercial versions support seamless updates of the operating systems new versions of the GSM CE are provided as ISO images requiring a new full installation. Further differences between the other GSM models and the GSM CE are explained on https://www.greenbone.net/en/community-edition/.

Both the Community Edition and the GSM ONE are optimized for the usage on a mobile computer. Features required for enterprise vulnerability management like schedules, alerts and remote scan engines are only available on the full featured appliances.

Migrating from GOS 3 to GOS 4

Version 4 of the Greenbone operating system is the most extensive overhaul compared to any prior version. Many internal functions and features were redesigned. This is also true for the graphical web interface and the command line interface for the administration. The following sections briefly explain the steps required during the migration of the appliances and the changes of default behaviour between version 3 and 4 you should be aware of.

With increasing complexity of a GSM setup, the migration can get complex as well. Customers are encouraged to plan and execute the migration in close coordination with the Greenbone Support.

4.1 GSM ONE

This section covers the migration of your data from a GSM ONE using GOS 3.1 to a GSM ONE using GOS 4. An usual update of the system like in the past is not supported. This is attributed to the extensive modifications in the system and the new database management system. The migration is achieved in three steps:

- Backup of the user data on the GSM ONE using GOS 3.1
- Export of the backup file
- Import and restore of the backup on the GSM ONE using GOS 4

Please contact the Greenbone Support and request a virtual image of GSM ONE with GOS 4. Provide your subscription key ID. You will receive a virtual image with GOS 4 and a guide for the migration.

4.2 GSM 25V

The virtual sensors are replaced by new virtual images. Please contact the Greenbone Support Team to receive GOS 4 images of the GSM 25V and provide the subscriptions key IDs for the respective sensors.

Because sensors do not store scan data, the setup and configuration of the sensor will be solely done in GOS 4. No migration steps are required.

4.3 GSM 25 and GSM 100

The small hardware appliances GSM 25 and GSM 100 require a migration of the user data via a USB Stick. GOS 4 eliminates this limitation for future upgrades.

Before starting the migration process please contact Greenbone Support. You will receive a detailed guide for the migration as well as advice tailored to your specific setup.

If you intend to keep the user data of the GSM, it is mandatory to create a userdata backup via USB Stick and store the settings as well, which could be done via copy & paste. In case you have no physical access to the GSM, please contact the Greenbone Support for an alternative procedure involving additional manual steps.

A pre-condition for the migration of a GSM is that it has direct access to the Greenbone Security Feed service. If it doesn't (for example Airgap or separate security zones), please contact Greenbone Support for an alternative procedure involving additional manual steps.

To start the migration, your appliance needs to be at least at GOS version 3.1.42 or newer. Earlier GOS versions do not offer a migration. Note that you should have physical or at least console access to the system(s) in question. It might be necessary to configure some initial settings to reintegrate the GSM into the network.

In GOS 4 you are offered a guided setup. Via the Setup menu the userdata backup is imported with item Data Import.

4.4 GSM 400 up-to 6400

All hardware appliances offer a seamless migration from GOS 3.1 to GOS 4. The user data will be moved to the new version and your system settings will be kept for the most part, although there are exceptions. Especially complex setups like Master-Slave, Airgap or Expert-Net should be carefully planned accordingly.

Before starting the migration process please contact Greenbone Support. You will receive a detailed guide for the migration as well as advice tailored to your specific setup.

As a general guideline, you should begin by creating a user data backup and store it on a USB Stick. While your user data should be moved automatically during the migration, a backup is a safety measure that should always be undertaken.

A pre-condition for the migration of a GSM is that it has direct access to the Greenbone Security Feed service. If it doesn't (for example Airgap or separate security zones), please contact Greenbone Support for an alternative procedure involving additional manual steps.

To start the migration, your appliance needs to be at least at GOS version 3.1.42 or newer. Earlier GOS versions do not offer a migration. Note that you should have physical or at least console access to the system(s) in question. It might be necessary to configure some initial settings to reintegrate the GSM into the network.

In GOS 4 you are offered a guided setup and migration. You have the option to restore the migrated user data from 3.1. This is a one-time offer. If you deny, the data will be deleted from the appliance and the only copy left is the backup on your USB Stick.

4.5 Changes of default behaviour

The following list displays the changes of default behaviour from GOS 3 to GOS 4. Depending on the current features used, these changes may apply to the currently deployed setup. Please check the following list to decide whether changes to the currently deployed setup are required. Greenbone Support may help during this process.

- NVTs: Starting with GOS 4.2 policy violation NVTs now have a score of 10 by default (see section *Compliance and special scans* (page 157)). In the past these NVTs had a score of 0 and overrides were required (see section *Severity* (page 160), *Severity* (page 163), *Severity* (page 164), etc.)
- GMP: The OpenVAS Management Protocol has been replaced with the Greenbone Management Protocol. The major difference is the transport channel used. While OMP uses a SSL-encrypted channel on port 9390/tcp GMP uses ssh. Therefore the older `omp.exe` tool cannot connect to

GOS 4 appliances. The new appliances require the GVM-Tools (see section *Greenbone Management Protocol* (page 205)). The GVM-Tools are compatible with GOS 3.1, so that you can migrate your scripts prior to migrating the GSM.

- GMP: The Greenbone Management Protocol changed the API lightly. New commands are available and some commands have changed their usage. The complete reference guide and the changes are available at http://docs.greenbone.net/API/OMP/omp-7.0.html#changes.
- TLS: If an external CA should be used (see section *Certificate* (page 29)), the certificate requests generated by the GOS menu option now generate 3072 bit keys. Some CAs do not support such long keys yet. In those cases the PKCS12 import still support keys with a key length of 2048 bits.
- Master/Slave: While deployment using GOS 3.1 require two ports for a master/slave setup starting with GOS 4.2 only one port is required. The port 22/tcp is used for controlling the slave and the synchronization of updates and feeds. The former used port 9390/tcp for the remote control of the slaves by the master is not used anymore. In addition, as a security measure, the identity of all linked master/slave appliances is now validated via a key exchange in GOS 4. It will be necessary to perform this key exchange when migrating old GOS 3.1 slaves or sensors. Note that on GOS 4, slaves are regarded a special type of scanners and are configured in the web interface under the respective section.
- Report Format Plugins: In contrast to GOS 3.1, Report Format Plugins in GOS 4 connected to an Alert will not be executed if the RFP was set to disabled.
- Report Format Plugins: All Report Format Plugins (RFPs) which were uploaded manually in GOS 3.1 or which were created by cloning another RFP will be automatically disabled during the migration to GOS 4. Some might not work on GOS 4 anymore. If they are not used anywhere, you should remove them. For some RFPs we meanwhile have advanced versions in the preconfigured set of RFPs and you should switch to those if you want to use them for example in an Alert. Before re-activating a RFP, test it with a report and make sure it is not automatically used with an Alert in the background while you are testing it. If in doubt, you can also ask the Greenbone Support what to do with a certain RFP.
- Expert-Net: If you had Expert networking mode (Expert-Net) enabled in GOS 3.1, the network configuration will be reset after upgrading to GOS 4. Please contact Greenbone Support for further details and be prepared to configure your GSM without remote network access.

CHAPTER 5

I want to ...

This chapter will guide you to different areas of the manual to complete simple single tasks.

I want to ...

- do my first scan. Please see section *Simple Scan* (page 79).
- do an authenticated scan. Please see section *Authenticated Scan using Local Security Checks* (page 91).
- upgrade the GSM. Please see section: *Upgrade Management* (page 47).
- setup central authentication using LDAP. Please see section *Central User Management* (page 75).
- connect verinice to the GSM. Please see section *Verinice* (page 224).
- connect OMD/Check_MK/Nagios to the GSM. Please see section *Nagios* (page 231).
- use notes to manage the results. Please see section *Notes* (page 127).
- manage false positives using overrides. Please see section *Overrides and False Positives* (page 130).
- manage and use report formats. Please see section *Report Plugins* (page 152).

CHAPTER 6

System Administration

The administration of the Greenbone Operating System (GOS) version 4 is fully achieved through a menu based console access. The administrator does not need any commandline or shell access to fulfill the configuration or maintenance tasks. Only for support and troubleshooting purposes shell access is provided. To access the system administration interface you need to login as admin on the console. This chapter is organized based on the system administration menu structure. First the *Setup*, then the *Maintenance* and finally the *Advanced* submenu is covered.

6.1 Introduction

6.1.1 Log in as admin

Once turned on the appliance will boot. The boot process can be monitored via serial console. The boot process of the virtual appliance can be monitored in the hypervisor (VirtualBox or VMWare).

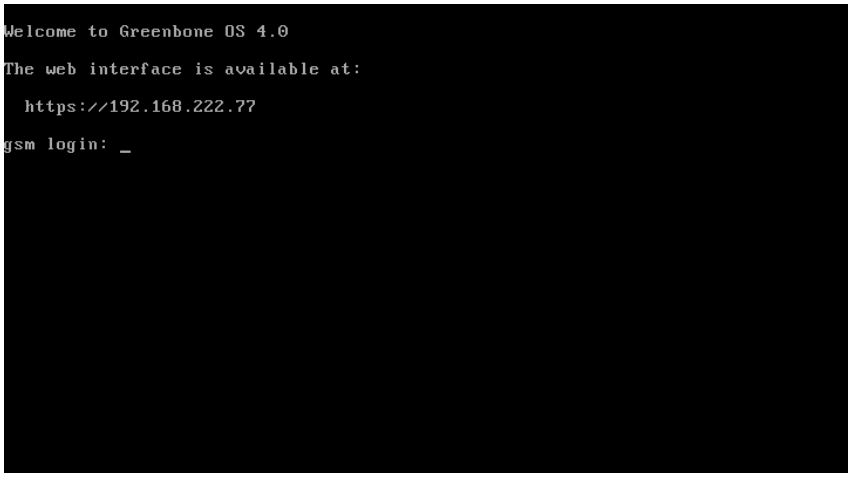


Fig. 6.1: Boot screen of the appliance

After the boot process is completed you can log into the system locally using the console. The default login is user: `admin` with password: `admin`. After the login (if not already configured) the GSM may remind you that the setup has not been completed yet.

Authorization Concept

The GSM offers two different levels of access. There is a user level and a system level. The user level (Web Admin) access is available via the graphical web interface or the Greenbone management

protocol (GMP). The system level (GSM Admin) is only available via console or secure shell protocol (SSH).

User Level Access

The user level access does support the management of users, groups and fine-grained permissions via either the web interface or GMP. Further details may be found in section *User Management* (page 65). While the user level may be access either via the web interface or the Greenbone management protocol (GMP) the GMP access is turned of by default on all devices but sensors. Furthermore in its delivery state no account has been defined on all GSM devices for accessing the user level. Thus no unauthorized access is possible between the commissioning and the configuration of the device.

System Administration Level Access

The system administration interface is only available via the console or SSH. Only one account is supported: `admin`. This account is to be used for all system administration of the GSM. This unprivileged user may not directly modify any system files but can only instruct the system to modify some configurations.

When delivered by Greenbone the user `admin` is assigned the password `admin`. During the first setup this password should be changed. Trivial passwords are declined. This includes the password `admin` as well. All network interfaces are disabled by default and no IP address is assigned. The SSH service is disabled as well. To use SSH for accessing the GSM the network interfaces and the SSH service need to be enabled first. The Greenbone Security Manager Community Edition (GSM CE) and the GSM ONE enables the network interfaces using DHCP immediately after the installation but the SSH service is disabled as well.

If the SSH service is enabled only `admin` may login remotely.

6.1.2 System Administration Access

The CLI can be accessed via serial console or SSH. However, SSH access is possibly deactivated and has to be enabled using the serial console first (see section *SSH* (page 32)).

Access via SSH from UNIX/Linux can be done directly via command line:

```
$ ssh admin@<gsm>
```

Replace *gsm* with the IP address or DNS name of the GSM appliance. To verify the host-key, its checksum can be displayed via serial port prior. To do this change into the submenu *Setup* followed by *Services* and *SSH* and select *Fingerprint*.

Access to the command line via serial port is described in the respective section of the setup guide. Login is preformed with user *admin* (see section *Log in as admin* (page 17)). The factory default password is *admin*. Alternatively SSH can be used to log in (see section *SSH* (page 32)).

6.1.3 Committing Changes

All changes introduced through the system administration menus are not saved and activated immediately. Rather the menu is modified and a new *Save* option is added if you have any pending modifications.

If you exit the menu without saving any pending modification a warning is displayed. You may choose to go back (ESC), save (Yes) or discard (No) the modifications.

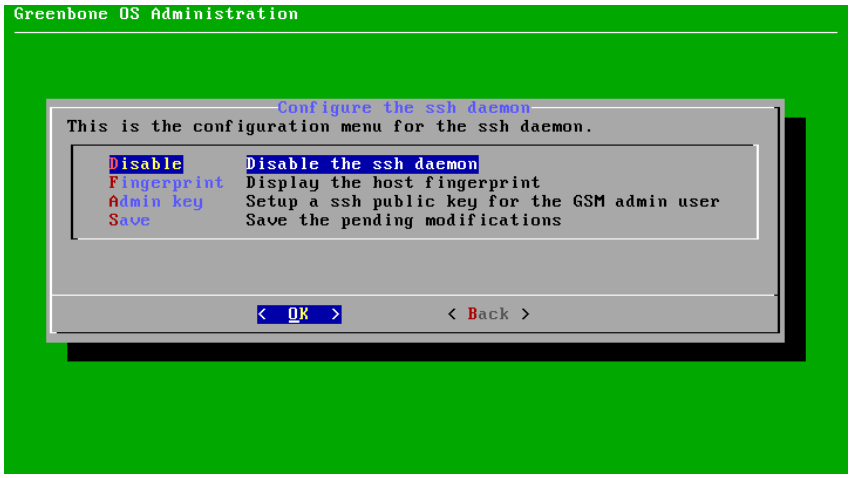


Fig. 6.2: Save pending modifications

Fig. 6.3: Discard pending modifications

6.2 Setup Menu

6.2.1 Users Management

The system administration interface allows the management of users and passwords. In particular, it offers the possibility to change the password of the system administrator and to manage web users. These web users may be administrators (scan administrator respectively), guests and Super Admin.

System Administrator password change

The password of the system administrator may be changed. This is especially important during the first base configuration. The factory setting *admin/admin* is not suitable for a production environment.

The respective function is available in the *Setup* menu. Here you will find the user management in the *User* submenu.

The following users can be configured (see section *Authorization Concept* (page 17)):

1. GSM-Admin: This is the administrator which can log into via command line (i.e. via serial port).
2. Web-Admin: This is the administrator which can log into the web interface.

To change the GSM-Admin password select the option *Password*. You will be asked to enter the current (UNIX) password of the administrator. Afterwards you must enter the new password twice.

This change is effective immediately. A commit of the change is not required. A rollback is not possible either.

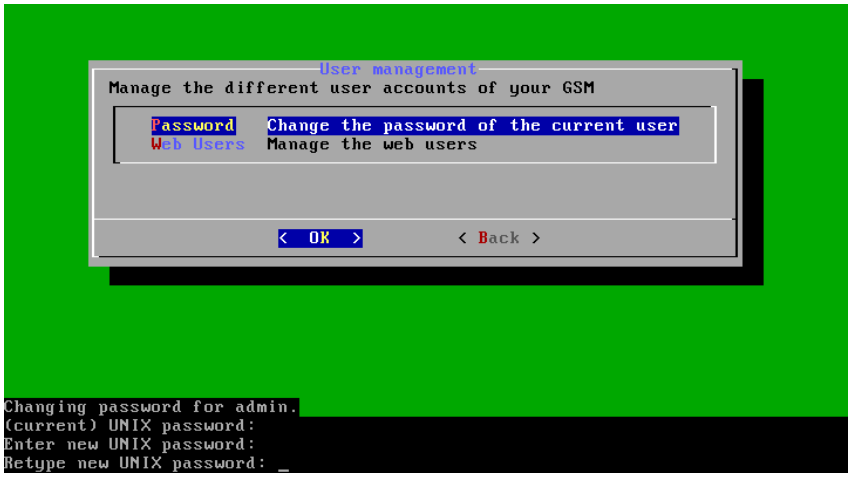


Fig. 6.4: Changing of the GSM administrator password

Note: Trivial passwords are being rejected. This includes the default password *admin*.

Managing Web Users

To be able to use the GSM appliance a web administrator must be set up. This user is being referred to as scan administrator in some documentation and by some applications.

The set-up of the first web admin is only possible through the system administration interface. Within *Setup* menu switch to the *User* option and select *Web Users*. Several new options are displayed.

- List Users - This displays a list of the current web users.

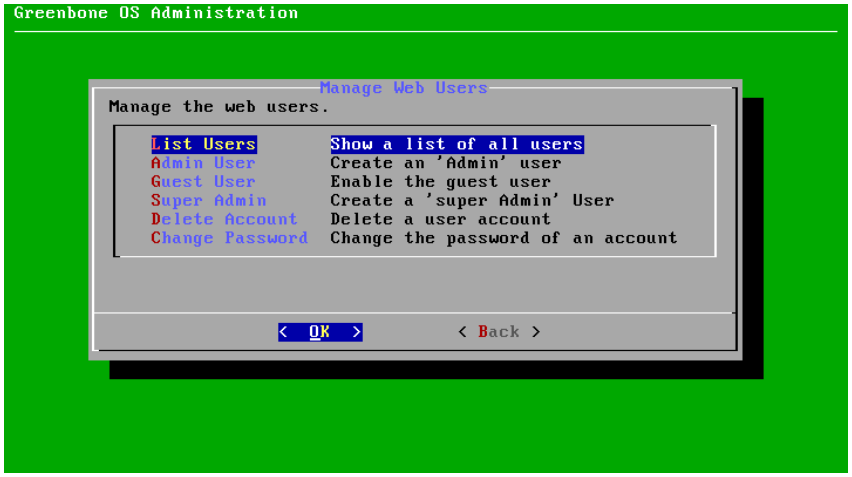


Fig. 6.5: Web users management

- Admin User - This creates a new web administrator. The first web admin has to be defined using the system administration interface. Once logged in the web admin may be used to add further web administrator or normal web users.
- Enable Guest - This enables the guest user. This may not be done using the web interface but only the system administration interface.
- Super Admin - This creates the super admin. Only one super admin may be defined. The super admin may only be defined using the system administration interface.
- Delete Account - This option may be used to delete a web user.
- Change Password - This option may be used to change the password of any web user.

More than one user with administrative rights can be set up. Further configuration of the users using the system administration interface is not possible. It is only possible to display the existing users or delete them if applicable.

To edit the existing users, or add users with less permissions, use the web-interface.

The following screen shot displays the creation of a web administrator:

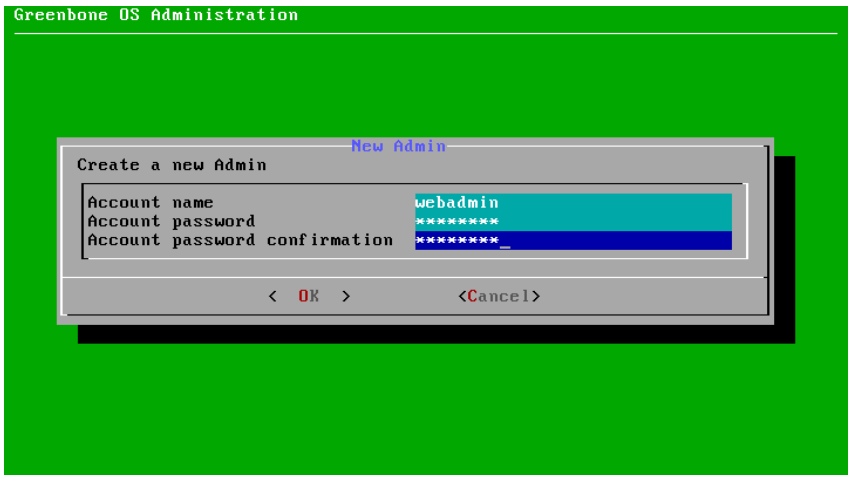


Fig. 6.6: Web admin creation

To create the user use the <Enter> key. To navigate from field to field use the cursor keys.

6.2.2 Network configuration

The network configuration menu offers the following options:

- Configure the Network Interfaces
- Configure the Domain Name Servers
- Global Gateway (IPv4 and IPv6)
- Hostname and Domainname
- Management IP addresses (IPv4 and IPv6)
- Display MAC and IP addresses
- Enable Expert Mode

Any change within the network configuration has to be saved via the Menu and the GSM needs to be rebooted for the change to be fully effective.

Network Interfaces

The GSM may have up to 24 network interfaces. At least one network interface must be configured to access the GSM via the network. Usually the first network adapter `eth0` is used for this purpose. The admin has to configure this network interface and to attach the appliance to the network.

Depending on the actual model the first network interface may be preconfigured:

- GSM ONE: DHCP
- All other models: no IP address set

IPv6 is disabled on all models by default.

To configure the adapter enter the *Setup* menu and navigate to the *Network* submenu. Here choose the option *Configure the Network Interfaces*.

You will be able to configure the network interface `eth0`.

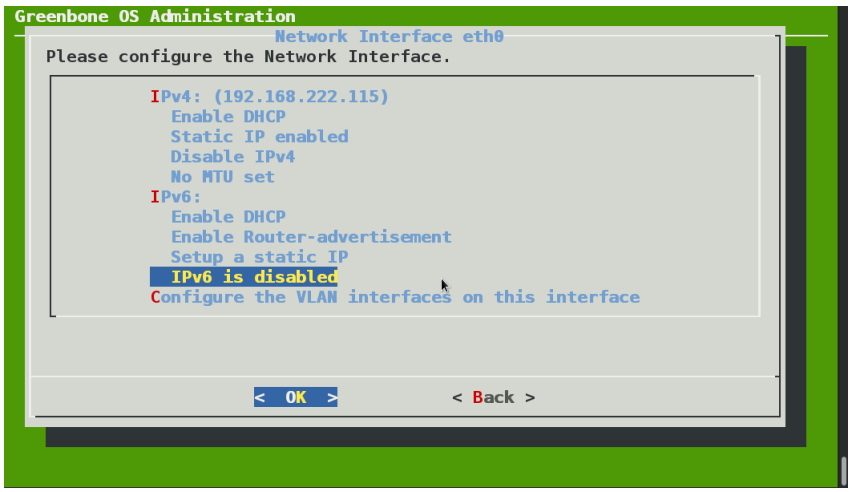


Fig. 6.7: Configuration of eth0

To setup a static IP address choose the appropriate option, remove the text `dhcp` from the configuration line and replace it with the correct IP address including the prefix length.

To configure a network interface to use DHCP choose the option *Enable DHCP*. This option is only available if currently a static IP address is configured.

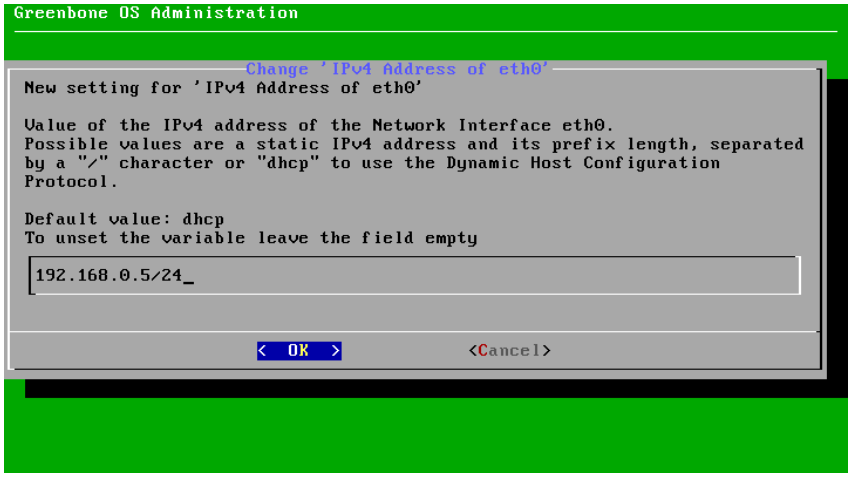


Fig. 6.8: Entering a static IP address

To configure the MTU of the interface use the appropriate option from the menu. To use the default values leave the field in the dialogue empty.

When configuring IPv6 addresses the admin has the choice of:

- Stateful DHCPv6
- Router Advertisement
- Static IP

Depending on the mechanism used the gateway and the dns server need to be configured manually.

This menu supports the configuration of VLANs as well. To configure a VLAN subinterface choose the option *Configure the VLAN interfaces on this interface* and enter the VLAN number.

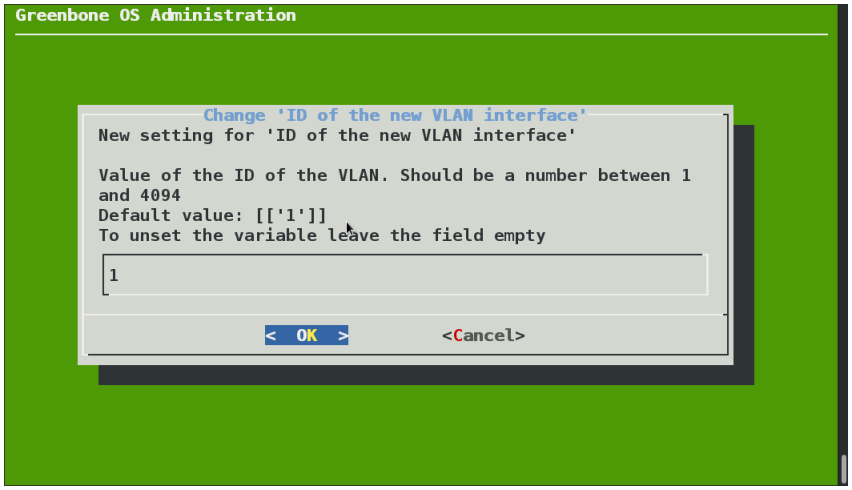


Fig. 6.9: Creating a new VLAN subinterface

The next screen will display a success message. After acknowledgement of this message the interface may be configured using IPv4 and/or IPv6 using the usual dialogue.

Additional VLAN subinterfaces may be added.

Always ensure that any changes are saved before exiting the menu. If pending modifications are detected you will be warned appropriately.

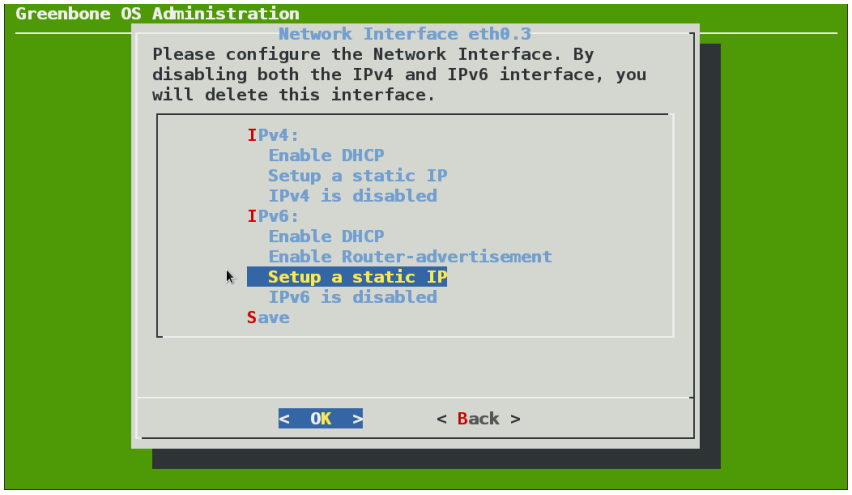


Fig. 6.10: Configuring the VLAN subinterface eth0.3

DNS server

In order to receive the feed and updates the GSM requires a reachable and functioning DNS server for name resolution. If the GSM uses a proxy to download the feed and updates this setting is not required.

If DHCP is used for the configuration of the network interfaces, the DNS servers provided by the DHCP protocol will be used.

The GSM appliance supports up to three DNS servers. At least one DNS server is required. Additional servers will only be used at an outage of the first server. To configure the DNS servers enter the *Setup* menu and choose the submenu *Network*. Here choose *Configure the Domain Name Servers*.

You will be able to configure three different DNS servers. These servers can be configured using either an IPv4 or an IPv6 address.

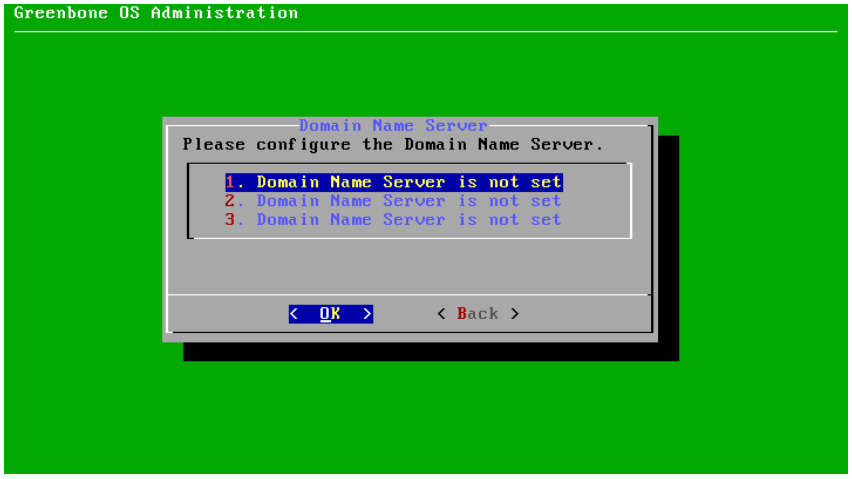


Fig. 6.11: Setup DNS servers

Any change has to be committed by choosing *Save* in the menu.

If the DNS servers can be reached and are functional is shown by the Selfcheck (see section *Selfcheck* (page 45))

Global Gateway

The global gateway may be automatically obtained using DHCP or router advertisements. If the GSM is configured to use static IP addresses the global gateway has to be configured manually. Separate options are available for IPv4 and IPv6.

The global gateway is often called the default gateway as well. To configure the global gateway use the option *Global Gateway* for IPv4 and *Global Gateway (IPv6)* for IPv6 within the *Network* submenu.

When using DHCP to assign IP addresses the global gateway will also be set via DHCP unless the global gateway has been set explicitly.

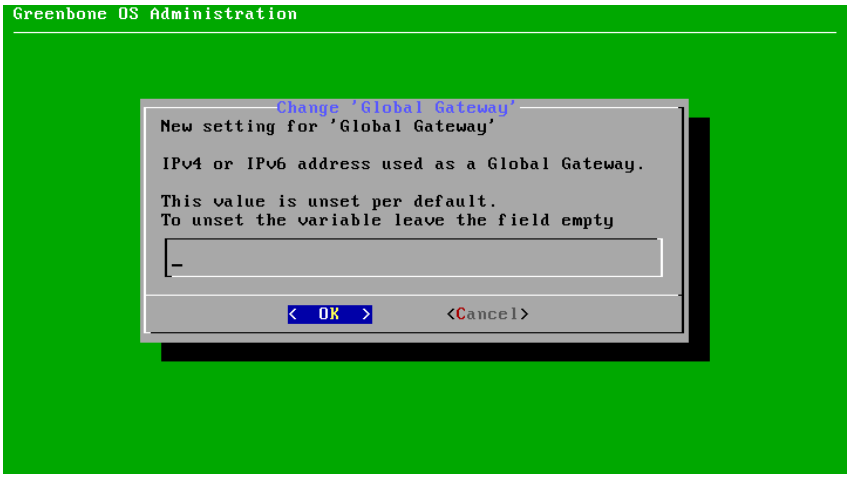


Fig. 6.12: Configuring the global gateway

Hostname/Domainname

While the GSM does not require a special hostname the hostname is an important item when creating certificates and sending emails. The options *Hostname* and *domainname* may be used to modify the fully qualified domainname of the appliance. While the hostname is used to configure the short hostname the domainname option is used for the domain suffix. The factory default values are:

- Hostname: gsm
- Domainname: gbuser.net

Management IP Addresses

These options allow the configuration of the management interfaces for IPv4 and IPv6 access. If these options are not configured the administrative interfaces will be available on all network interfaces. To restrict the access enter either the IP address or the name of the network interface (e.g. eth0) in the dialogue. All administrative access (SSH, HTTPS, GMP) will be restricted to the appropriate interface and will not be available on the other interfaces any more.

Display MAC/IP addresses

These menu options provide a simple overview on the use MAC addresses and the currently configured IP addresses of the appliance. These options do not support the configuration of the MAC addresses.

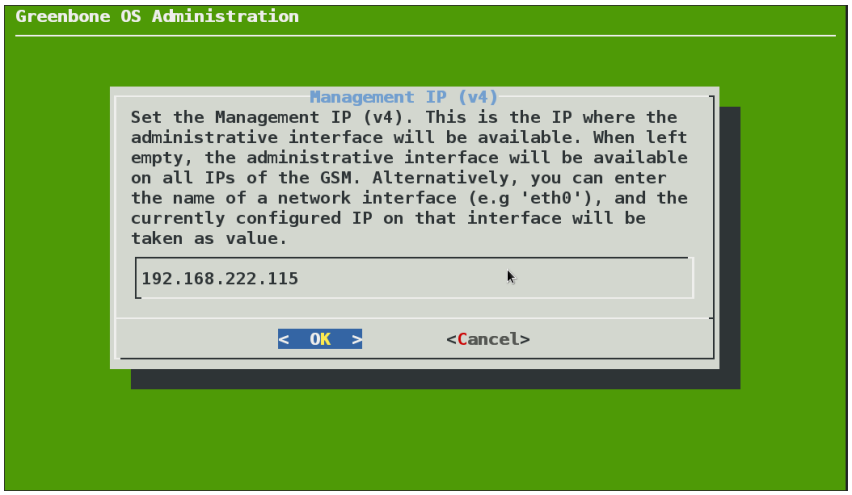


Fig. 6.13: Restricting management access

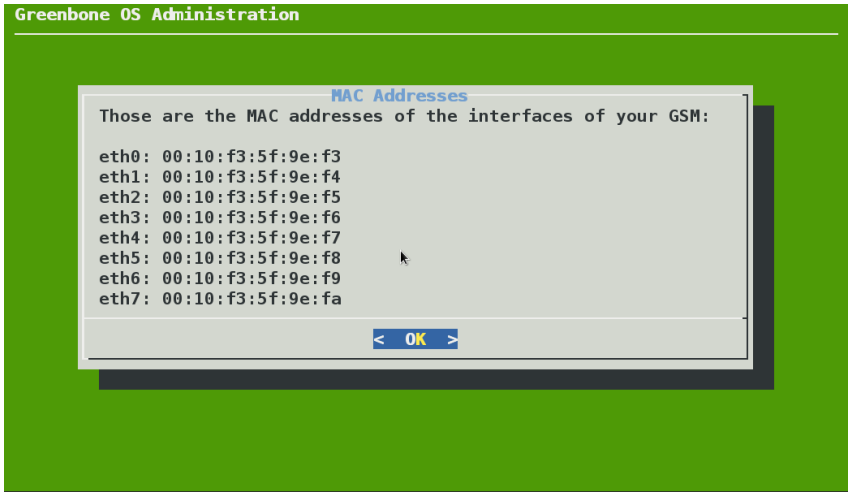


Fig. 6.14: Display the MAC addresses

Expert Mode

While most network configuration tasks can be handled via the menus, very complex setups using different static routes require further configuration. While the configuration of VLANs is now supported multiple static routes are currently not possible using the menus.

For the respective changes in the configuration an expert mode is provided. Please only use this mode, if your setup actually requires it.

The expert mode requires the configuration of these settings in separate files for each network card underneath the directory /etc/network/interfaces.d in the filesystem.

The creation, editing and activation of these settings is covered in this section.

To use the expert mode it must be activated first. Enter the *Setup* menu. Navigate to *Network* and choose *Expert*.

A new menu will be displayed.

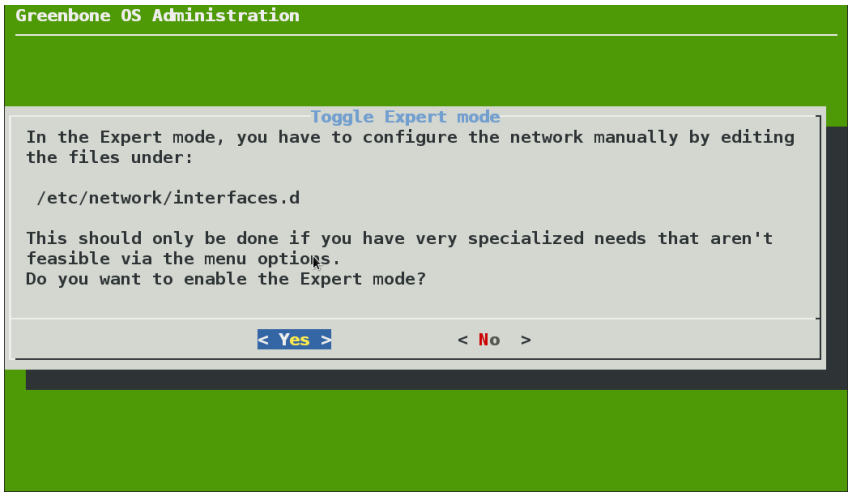


Fig. 6.15: Enable Expert Mode

To revert back to normal mode at the later date use the menu option *Expert*. The network service will be immediately restarted. All manually made changes in Expert Mode are reverted back and are lost! Some settings like hostname are currently not supported in Expert Mode. Currently best practice is to setup all required settings in normal mode and then change to Expert Mode.

When enabling the Expert Mode the admin starts with the current configuration of the network cards. Once the mode is enabled a new menu option *Edit* is displayed instead of the interfaces submenu. This options drops the admin user in a shell in the `/etc/network/interfaces.d` directory.

The syntax of the files adhere to the Debian standard. To call an additional command when enabling the network card the keyword `up` may be used. To achieve the same task while disabling the card the keyword `down` is used.

Additional IP addresses

The menus only support the configuration of one IP address per network card. To add additional addresses to the same card the expert mode may be used. To add an additional address use the command **`ip`** with the `addr` argument

```
iface eth0 inet static
  address 192.168.222.115/24
  up ip addr add 192.168.222.200/24 dev eth0
```

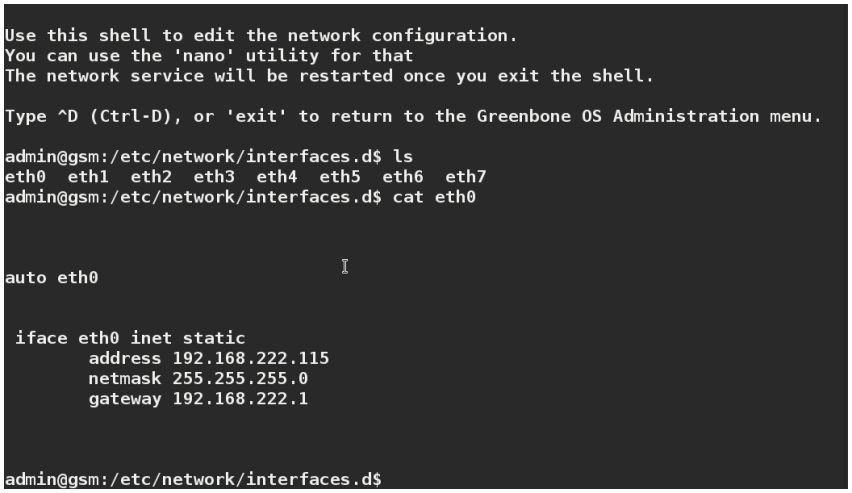


Fig. 6.16: Depending on the model several configuration files are available

Static Routing

Most networks only have one gateway. This gateway often is referred to as default gateway. Sometimes historically grown networks use different routers for different destinations. If these routers do not communicate data through dynamic routing protocols client systems often require static routes for those destinations. The expert configuration allows for configuration of unlimited static routes.

To set a route use the **ip** command with the `route` argument

```
iface eth0 inet static
  ...
  up ip route add default via 192.168.81.1
  up ip -f inet6 route add default via 2607:f0d0:2001::1
```

6.2.3 Services

To access the GSM appliance remotely basically two options are available

HTTPS This is the usual option for the creation, execution and analysis of the vulnerability scans. This option is activated by default and cannot be deactivated. Configuration is only possible for the timeout of the automatic logout when the HTTPS session is inactive.

SSH This option allows the possibility to access the command line, CLI and GOS-Admin-Menu of the GSM appliance. This access is deactivated by default and must be activated first. This can be done via serial console for example.

GMP (Greenbone Management Protocol) The Greenbone Management Protocol (GMP) allows for the communication with other Greenbone products (i.e. an additional GSM). This protocol is based on the OpenVAS Management Protocol. It can also be used for the communication of in-house software with the appliance (see section Greenbone Management Protocol (page 205)).

SNMP SNMP Read access of the GSM is possible via SNMPv3 (see section *SNMP* (page 36))

HTTPS

Timeout

The timeout value of the web interface can be set via *Setup/Services/HTTPS/Timeout*.

The value of the timeout can be between 1 and 1440 minutes (1 day). The default is 15 minutes.

Ciphers

The HTTPS ciphers may be configured. The current setting allows only secure ciphers using at least 128 Bit key length explicitly disallowing AES-128-CBC, Camellia-128-CBC and the cipher suites used by SSLv3 and TLSv1.0.

The string used to define the ciphers is validated by GNUTLS and has to conform to the corresponding syntax.

Certificate

This menu option supports the generation of self-signed HTTPS certificates or the import of certificates signed by external certificate authorities.

The menu offers the following choices:

- Download: Download the current HTTPS certificate for import in your browser
- CSR: Generate a Certificate Signing Request for the HTTPS certificate
- Generate : Auto-generate a new self-signed HTTPS certificate
- PKCS12: Import a PKCS#12 file as new HTTPS certificate
- Certificate: Import a certificate signed by an external certificate authority

These different options are explained in the following sections.

The GSM appliance basically can use two types of certificates:

- Self-signed certificates
- Certificates issued by an external certificate authority

The use of self-signed certificates is the easiest way. It poses, however, the lowest security and more work for the user:

- The trust of a self-signed certificate can only be checked manually by the user through manual import of the certificate and examination of the finger print of the certificate.
- Self-signed certificates cannot be revoked. Once they are accepted by the user in the browser they are stored permanently in the browser. If an attacker gains access to the corresponding private key a man-in-the –middle attack on the connection protected by the certificate can be launched.

The use of a certificate issued by a certificate authority has several advantages:

- All clients trusting the authority can verify the certificate directly and establish a security connection. No warning is displayed in the browser.
- The certificate can be revoked easily by the certificate authority. If the clients have the ability to check the certificate status they can decline a certificate that may still be within its validity period but has been revoked. As mechanisms the Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) can be used.
- Especially when multiple systems within an organization serve SSL protected information the use of an organizational CA simplifies the management drastically. All clients simply have to trust the organizational CA to accept all of the certificates issued by the CA.

All modern operating systems support the creation and management of their own certificate authority. Under Microsoft Windows Server the Active Directory Certificate Services support the administrator in the creation of a root CA[2]. For Linux systems various options are available. One option is described in the IPSec-Howto[3].

[2] https://technet.microsoft.com/en-us/library/cc731183.aspx
[3] http://www.ipsec-howto.org/x600.html

When creating and exchanging certificates it needs to be considered that the admin verifies how the systems are accessed later before creating the certificate. The IP address or the DNS name respectively, is stored when creating the certificate. Additionally after creating the certificate a reboot is required so that all services can use the new certificate. This needs to be taken into consideration when changing certificates.

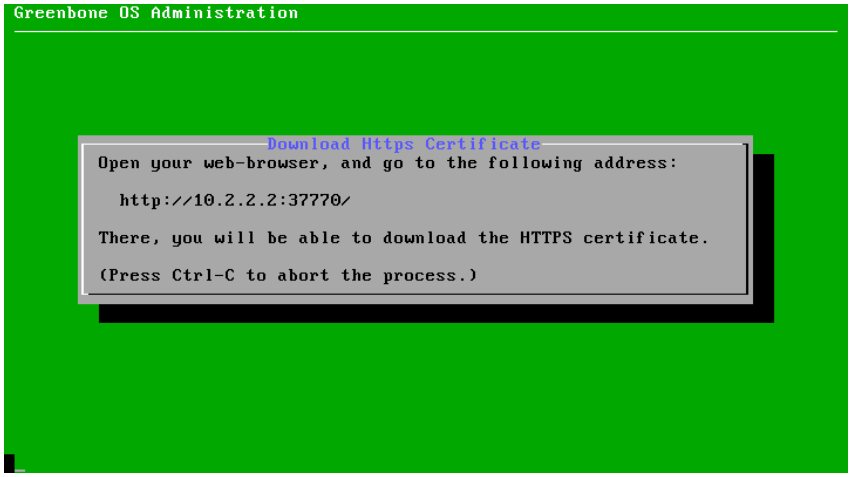


Fig. 6.17: Downloading the certificate

Self-signed certificates To support a quick setup the GSM supports self-signed certificates. However, by factory default of many variants such a certificate is not pre-installed and must be created by the administrator. The GSM ONE, however, already comes with a pre-installed certificate.

Self-signed certificates can be easily created using the Option *Generate* (see section *Generate* (page 31)). After creating the certificate a reboot is required so all services can use the new certificate.

Certificate by an external certificate authority To import a certificate by an external certificate authority two options are available:

- Generate a CSR on the GSM , sign it using an external CA and import the certificate
- Generate the CSR and the certificate externally and import both using a PCKS#12 file

The next step depends on whether you require a certificate signing request (CSR) which will be subsequently signed by a certificate authority or whether you already have a key and signed certificate you would like to use for this GSM.

If you need to create a new CSR use the menu option *CSR* (see section *CSR* (page 31)). Then sign the request and use the menu option *Certificate* to import the signed certificate (see section *Certificate* (page 32)).

If you already have a key and a signed certificate you would like to use for this GSM, the menu option *PKCS12* must be used instead to transfer the key and certificate to the GSM. The command expects the key and certificate in PKCS#12 format (see section *PKCS12* (page 31)).

Download Using this option the GSM will start an additional webserver running on an unprivileged port offering just the HTTPS certificate file for download. The URL and the port used are displayed in the console.

After the successful download the fingerprint of the certificate is displayed for verification within the browser.

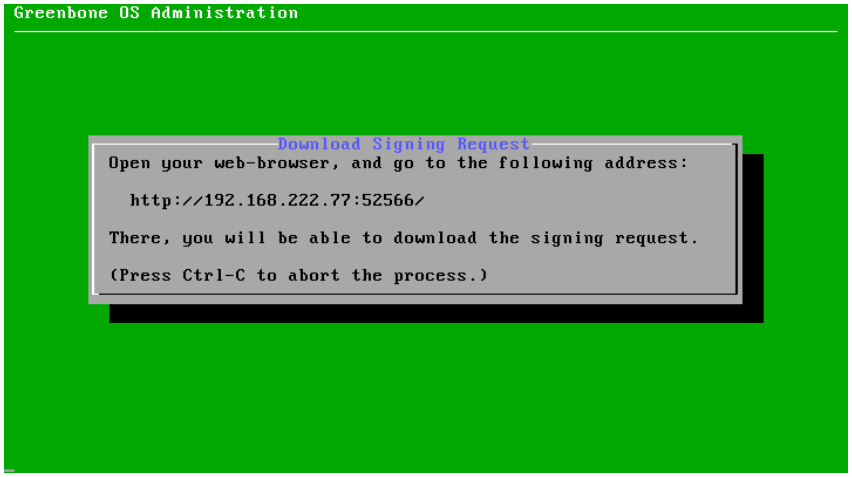


Fig. 6.18: Downloading the certificate signing request

CSR If you choose the option to generate a new certificate signing request you are warned that the creation of a new CSR will overwrite the current key. After confirmation the CSR will be offered for download on an unprivileged port. The URL to use including the port is displayed on the console.

After downloading the certificate signing request (CSR) use an external certificate authority to sign the CSR and proceed to upload the certificate again (see section *Certificate* (page 32)).

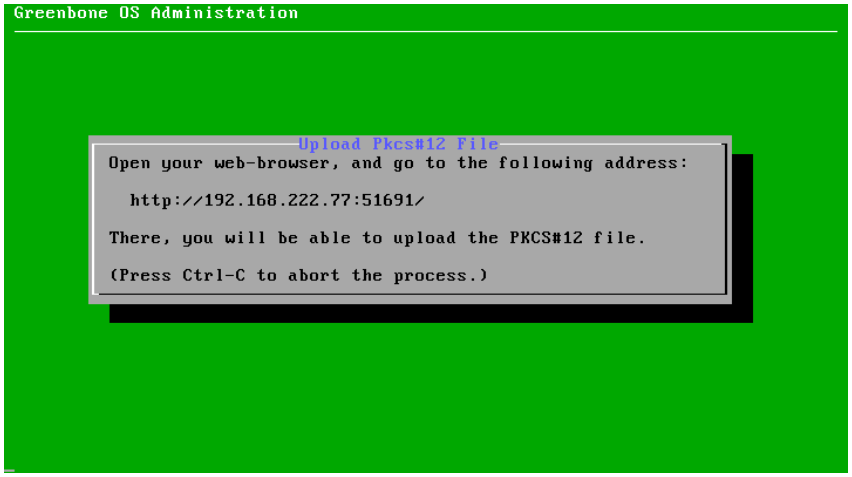


Fig. 6.19: Uploading the PKCS#12 container

Generate By choosing the option *Generate* you create a new self-signed certificate. The old private key and certificate are overwritten. You will be warned during the process that these old credentials will be lost after the process. Once the process is finished a message is displayed proposing the import of the certificate within the browser using the *Download* option (see section *Download* (page 30)).

To enable the new certificate a *Reboot* of the GSM is required (see section *Reboot* (page 48)).

PKCS12 To import both a private key and a signed certificate the option *PKCS12* may be used. The private key and the certificate need to be formatted as PKCS#12 file. The file may be protected using an export password.

To import the PKCS#12 file choose the menu option. The GSM will start an upload server on an unprivileged port. The URL to use including the port will be displayed in the console (see figure *Uploading the PKCS#12 container* (page 31)). Enter the URL in a browser, choose the file containing the PKCS#12 container and upload the file to the GSM.

If an export password was used to protect the PKCS#12 container you will be prompted to enter the password.

The certificate will be activated after a reboot (see section *Reboot* (page 48)).

Certificate Use the option *Certificate* to upload a certificate signed by an external authority. You will be warned that the old certificate will be overwritten in the process. After confirmation the GSM will start an upload server on an unprivileged port. The URL to use including the port will be displayed in the console. Enter the URL in a browser, choose the file containing the certificate in Base64 format and upload the file to the GSM.

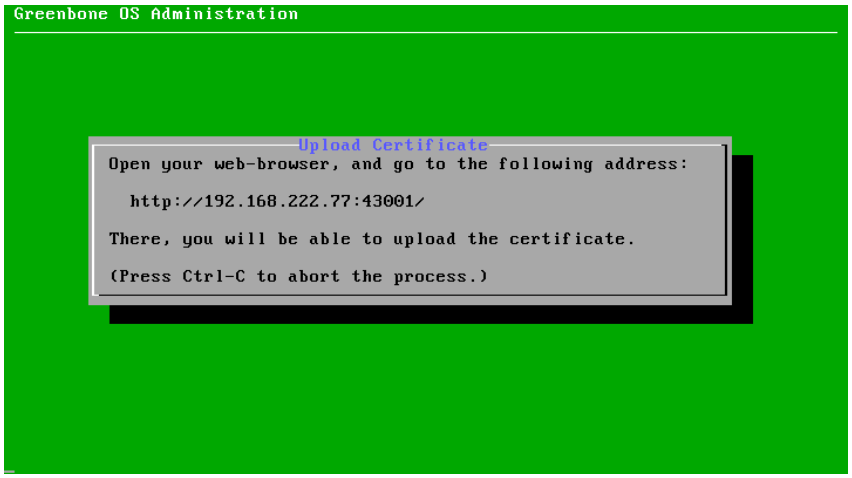


Fig. 6.20: Uploading the signed certificate

Once the certificate is retrieved by the GSM the console will display the fingerprint of the certificate for verification. Check the fingerprint and confirm the certificate.

The certificate will be activated after a reboot (see section *Reboot* (page 48)).

Fingerprints

To check and display the fingerprints of the certificate used by the GSM the menu option *Fingerprints* may be used. This option will just display the following fingerprints of the currently active certificate:

- SHA1
- SHA256
- BB

SSH

SSH access can also be configured in the GOS-Admin-Menu (*Setup/Services/SSH*). This menu offers three different options:

- Enable
- Fingerprint
- Admin key

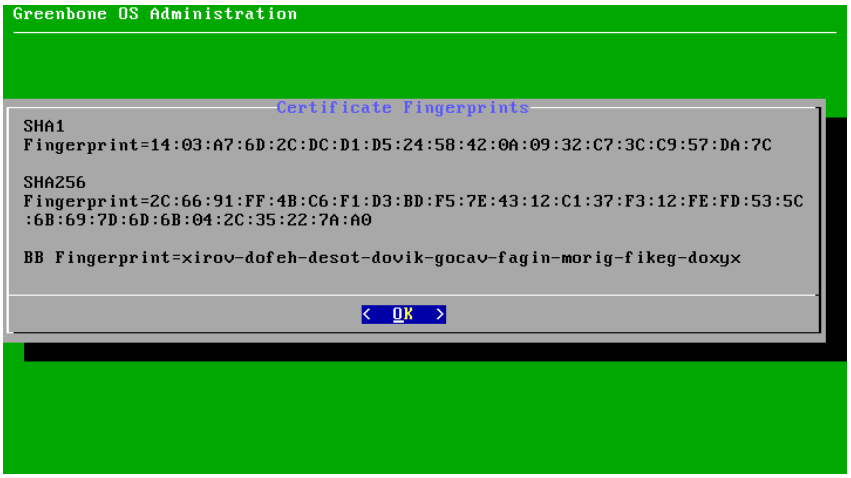


Fig. 6.21: TLS Fingerprints

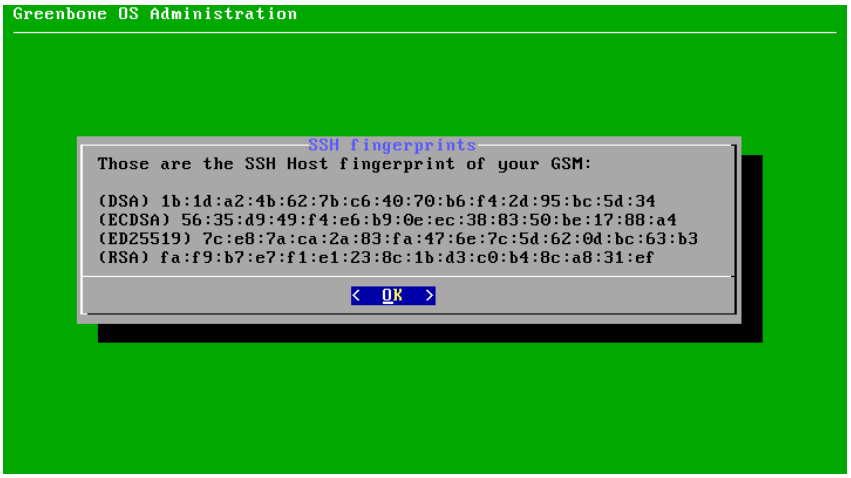


Fig. 6.22: SSH Fingerprints

Enable

This option enables the SSH Server embedded in the GSM appliance. To activate the setting you need to save the configuration setting using the menu. A reboot of the appliance is not required!

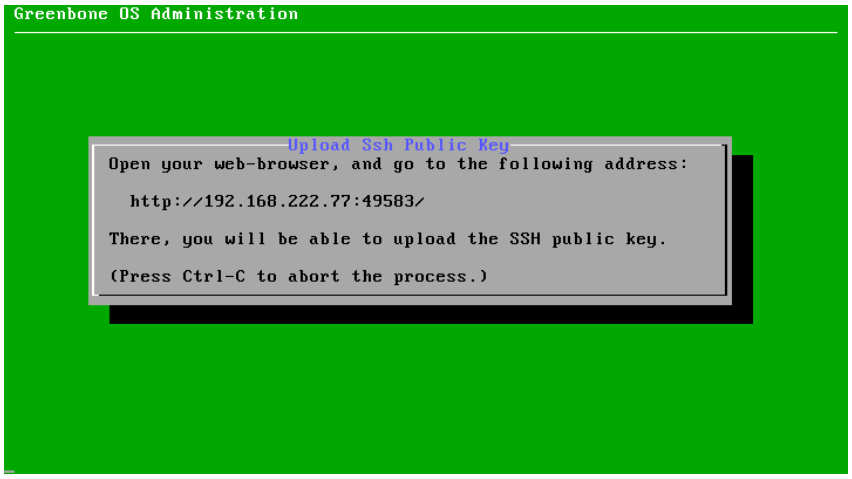


Fig. 6.23: Public key upload

Fingerprint

The GSM provides different host key pairs for its own authentication. The client decides which key pair to use. In the GOS menu on the console you may display the fingerprint of the public keys used by the SSH server of the appliance (see figure *SSH Fingerprints* (page 33)). The MD5 fingerprints of the following keys are displayed:

- DSA
- ECDSA
- ED25519
- RSA

Admin key

GOS 4 offers the upload of public keys for the key-based authentication of the admin user. Once the appropriate option is selected in the menu the GSM will start a web page on an unprivileged port. This page will support the upload of a public key used for the authentication of the admin user via SSH (see figure *Public key upload* (page 34)).

Once the key is uploaded the console will display the following notice:

Of course, the SSH server needs to be enabled to log in to the appliance. These keys may be generated using the command `ssh-keygen` when using OpenSSH on Linux or `puttygen.exe` when using Putty on Windows.

GMP

The Greenbone Management Protocol may be activated via the menu. Navigate to *Setup* followed by *Services*. Here the option *GMP* may be used.

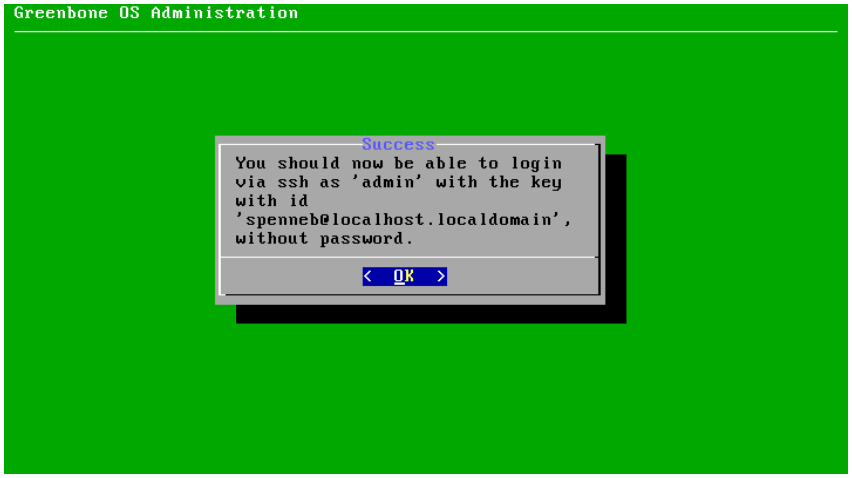


Fig. 6.24: Public key accepted

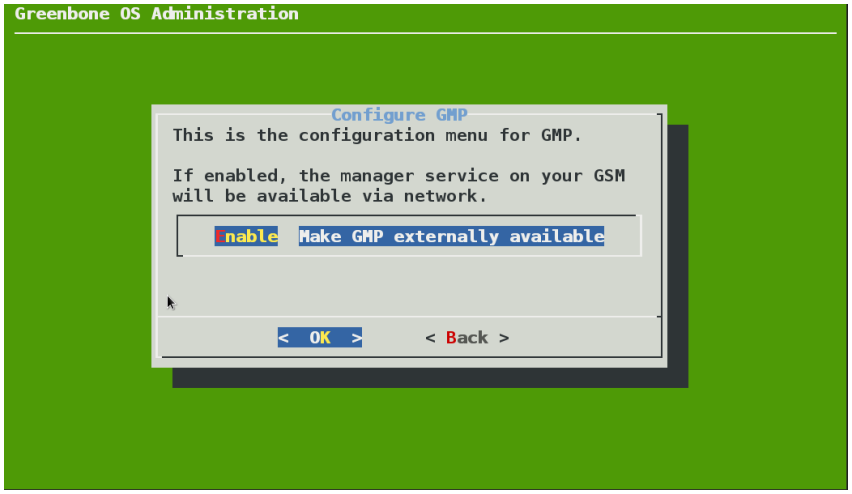


Fig. 6.25: Enabling the Greenbone Management Protocol

SNMP

The GSM appliance supports SNMP. The SNMP support can both be used for sending of traps through alerts as well as the monitoring of vital parameters of the appliance.

The supported parameters are specified in a Management Information Base (MIB) file. The current MIB is available from the Greenbone tech [doc] portal[4].

The GSM appliance supports SNMP version 3 for read access and SNMPv1 for traps.

To configure the SNMPv3 navigate to *Setup* followed by *Services*. Here the option *SNMP* is available.

The menu supports:

- Enabling/disabling of the SNMP service
- Setting location and contact
- Configuration of username, authentication and privacy passphrase for SNMPv3

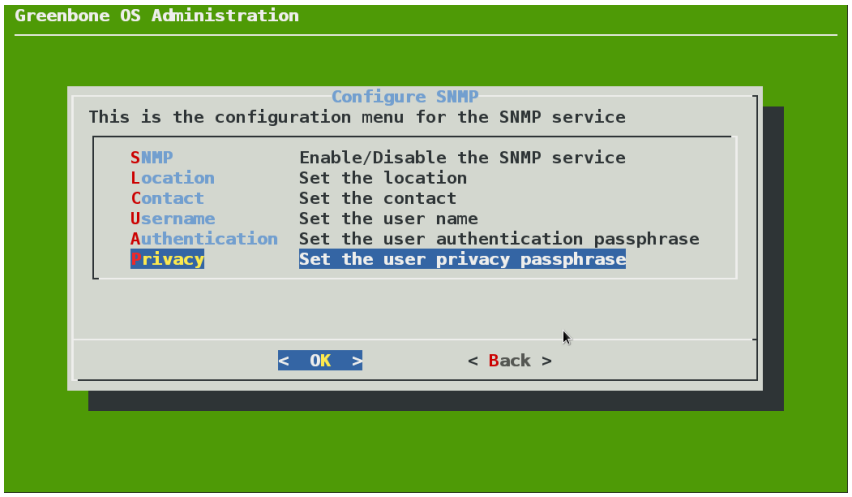


Fig. 6.26: SNMPv3 configuration

When configuring the authentication and privacy passphrase please be aware of the fact that the GSM uses SHA-1 and AES128 respectively.

Afterwards test read access of the SNMP service under Linux/Unix with `snmpwalk`:

```
$ snmpwalk -v 3 -l authPriv -u user -a sha -A password -x aes -X key 192.168.222.115
iso .3.6.1.2.1.1.1.0 = STRING: "Greenbone Security Manager"
iso .3.6.1.2.1.1.5.0 = STRING: "gsm"
...
```

The following information may be gathered:

- Uptime
- Network interfaces
- Memory
- Harddisk
- Load
- CPU

[4] http://docs.greenbone.net/API/SNMP/snmp-gos-4.1.en.html

6.2.4 Data import

If you are currently using a GSM running an older version of the GOS a direct upgrade is not possible. Rather than just installing an upgrade package like in the past, a complete reinstall of the GSM is required. This path is required because the underlying database system has been completely exchanged and depending on the model you are using the filesystem of the GSM is now encrypted as well.

To upgrade the GSM you now need to backup your data on the old GSM. After installing the new firmware you may import the backup using this option.

If you choose this option you are first warned that the import will overwrite all existing configuration on the GSM.

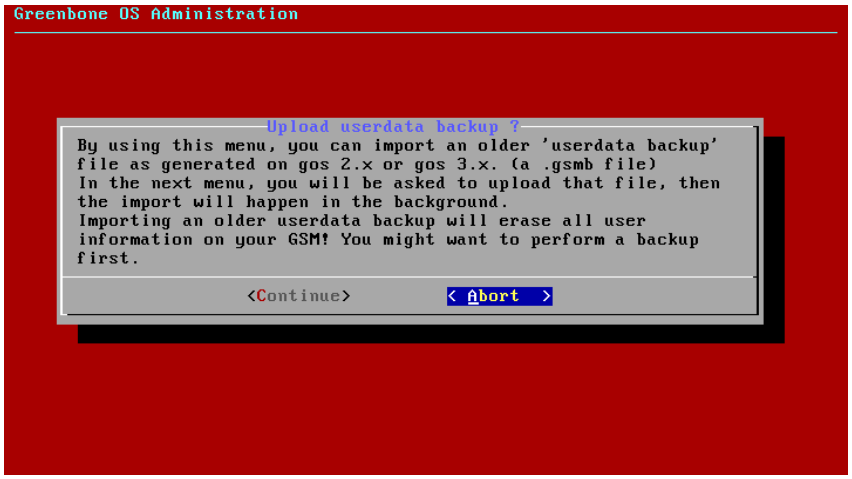


Fig. 6.27: Data import warning message

Once you have confirmed the warning the GSM will start a webservice to upload the backup file.

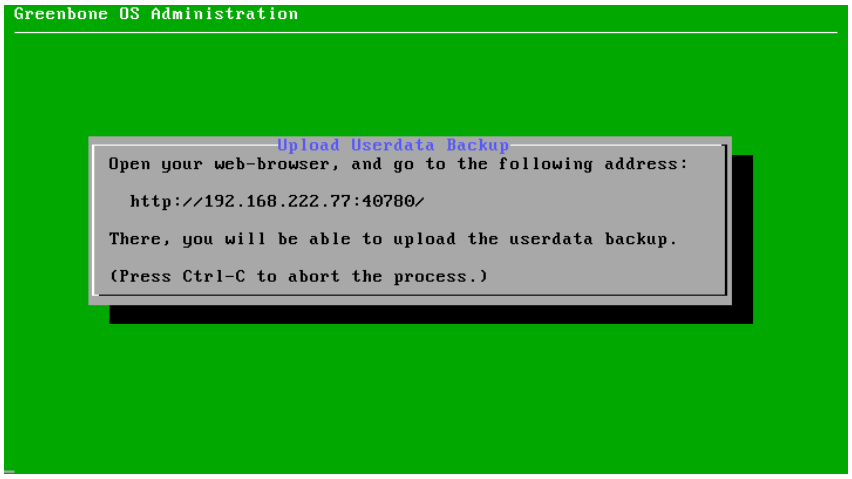


Fig. 6.28: Data import upload message

The import of the backup will take several minutes. During this period the GSM will not allow any web access. A detailed upgrade manual depicting the upgrade to GOS 4 from older versions for your model is available. Please contact the Greenbone Support.

6.2.5 Backup

The Greenbone Security Manager supports automatic backups. These backups may be stored locally or remote. The backups will be performed daily. Backups will be stored using the following schema:

- Last 7 daily backups
- Last 5 weekly backups
- Last 12 monthly backups

Backups older than one year will be automatically deleted. In factory state the backups are disabled.

To enable the backups navigate to *Setup* followed by *Backup*.

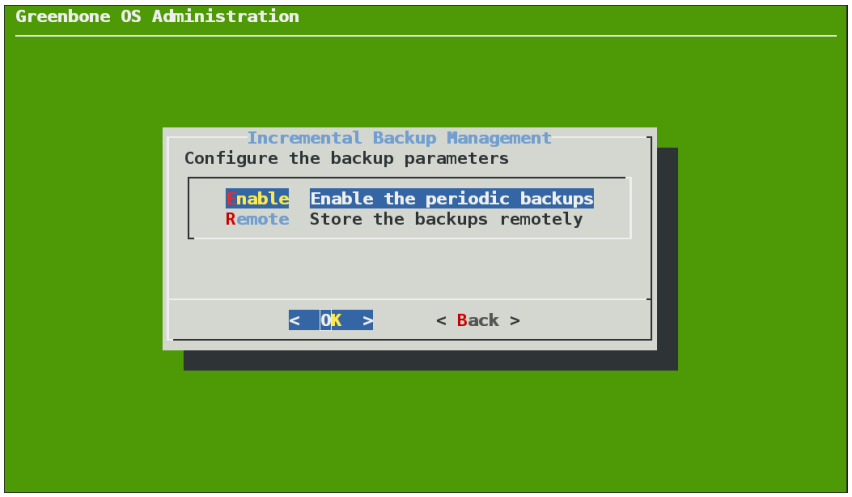


Fig. 6.29: Configuring Backups

By default the backups are stored locally. To store the backups on a remote server the server has to be setup appropriately. The GSM uses the SFTP protocol supported by the secure shell to transfer the backups. The remote server is therefore provided using a URL like the following:

```
username@hostname[:port]/directory
```

The optional port may be omitted if the server uses port 22.

The GSM will verify the identity of the remote server before logging in. To identify the remote server the GSM will use the public key of the remote host. To upload this public key use the menu option and a web browser.

The GSM uses a SSH private key to logon on the remote server. To enable this logon process the public key of the GSM must be enabled in the `authorized_keys` file on the remote server. To GSM generates such a private/public key pair. To download the public key use the menu option and download the key using a web browser.

If several GSM appliances upload their backups to the same remote server the files must be distinguishable. The admin has to set a unique backup identifier in these cases on each GSM appliance. If this value is not set the hostname will be used. If the hostname was modified from the default and is unique the backup files will be distinguishable as well.

Since the setup of the remote backup including the keys might be error-prone a test routine is available. This option will test the successful login to the remote system.

6.2.6 Feed

The *Feed* menu underneath *Setup* support the configuration and setup of the Greenbone feed. The Greenbone feed provides updates to the network vulnerability tests (NVT), the SCAP data (CVE and

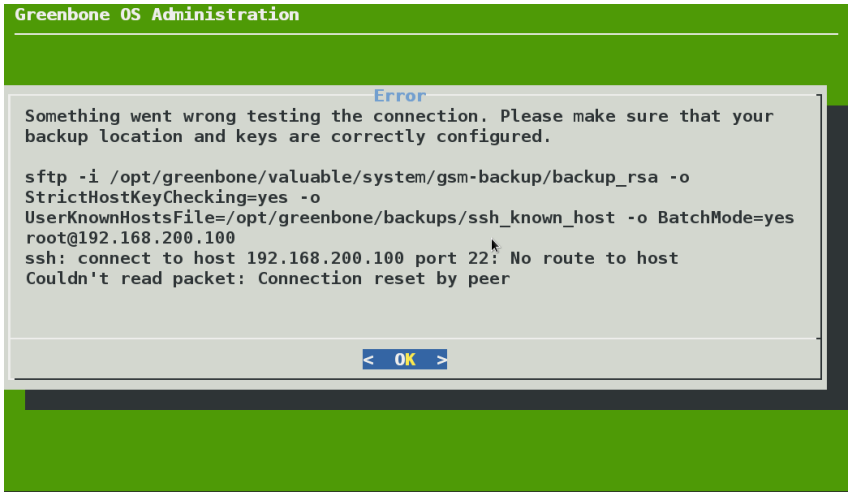


Fig. 6.30: Testing the remote backup

CPE) and the advisories from the CERT-Bund and DFN-CERT. Additionally the feed provides updates to the GOS operating system.

To use the Feed a subscription key is required. This key entitles your GSM to download the commercial feed provided by Greenbone.

If no valid subscription key is stored on the appliance the appliance will use only the public Greenbone community feed and not the commercial grade Greenbone security feed.

To configure the feed several options are available:

- Key Upload and Editor
- Enable/Disable Synchronization
- Sync port
- Sync proxy
- Cleanup

These options are further explained in the following sections. Whenever configuring any of these options you will need to save the configuration.

Key

These menu options are used to store a new Greenbone security feed (GSF) subscription key on the appliance. Either HTTP upload or Copy/Paste may be used. Please use this option carefully because the new key will overwrite any key already stored on the device. You will be warned when selecting this option.

If the warning is confirmed the GSM will start a webserver for uploading. You can then use your Browser to upload the new key.

Synchronization

This options supports the enabling and disabling of the automatic feed synchronization. If your GSM does not have any internet access and you do not want the GSM to try to access the Greenbone services on the Internet this feature may be disabled. If the synchronization has been disabled it may be enabled again using the same menu option.

The time of the feed synchronization may be changed using *Setup/Time* (see section *Time* (page 45)).

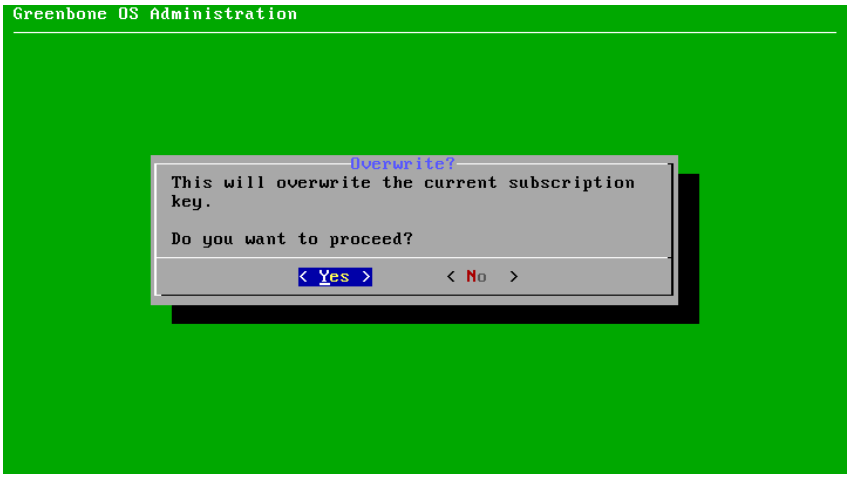


Fig. 6.31: The new key will overwrite any stored key.

Fig. 6.32: Enabling the feed synchronization happens after saving.

Sync port

The Greenbone security feed is provided by Greenbone on two different ports:

- 24/tcp
- 443/tcp

While port 24/tcp is the default port many firewall setups do not allow traffic to pass to this port on the Internet. Therefore this menu option allows the modification of the port to 443/tcp. This port is most often allowed.

Fig. 6.33: The sync may use either 24/tcp or 443/tcp

Note: The port 443/tcp is usually used by https traffic. While the GSM may use this port the actual traffic is not https but ssh. The GSM uses rsync embedded in ssh to retrieve the feed. Firewalls support deep inspection and application awareness may still reject the traffic if these features are enabled.

Sync proxy

If the security policy does not allow for direct Internet access the GSM may deploy a https proxy service. This proxy must not inspect the SSL traffic but must support the CONNECT method. The traffic passing through the proxy is not https but ssh encapsulated in http-proxy.

To set the proxy the menu option *Sync proxy* may be used. Please ensure the following syntax when defining the proxy:

```
http://proxy:port
```

Cleanup

This option removes the GSF subscription key. This option is useful if an appliance is at the end of life and needs to be removed from production. The cleanup ensures that no licenses are left on the device. Without the GSF subscription key the GSM will only retrieve the Community Feed. You will be warned accordingly when choosing this option.

6.2.7 Time Synchronization

To synchronize the appliance with central time servers the GSM appliance supports the NTP-Protocol. Up to four different NTP servers can be configured. The appliance will choose the most suitable server.

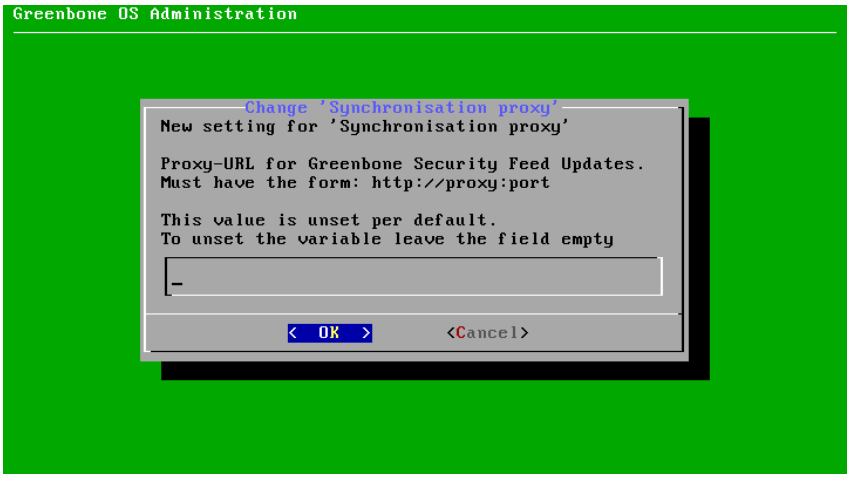


Fig. 6.34: The sync may use a http proxy

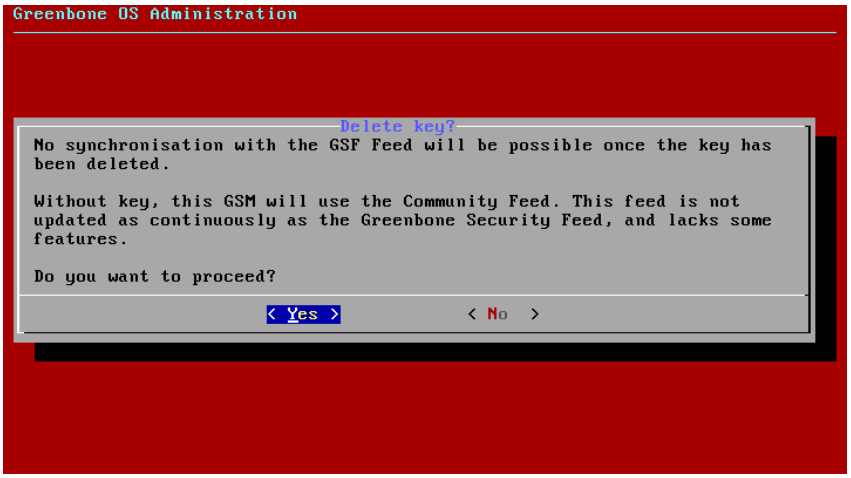


Fig. 6.35: Cleanup will remove the GSF key

During an outage of one server the other server will be used automatically.

Both IP addresses and DNS names are supported.

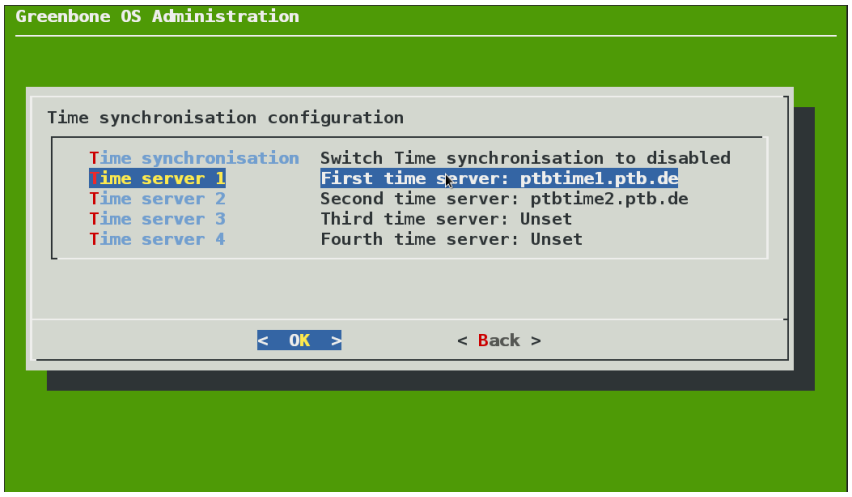


Fig. 6.36: Up to four NTP servers are supported.

6.2.8 Keyboard

This menu displays the current keyboard layout of the appliance and if necessary supports the modification to your required needs and locale.

In *Setup* menu select the option *Keyboard* using the arrow keys and confirm with `Enter`. Select the desired layout in the new dialog.

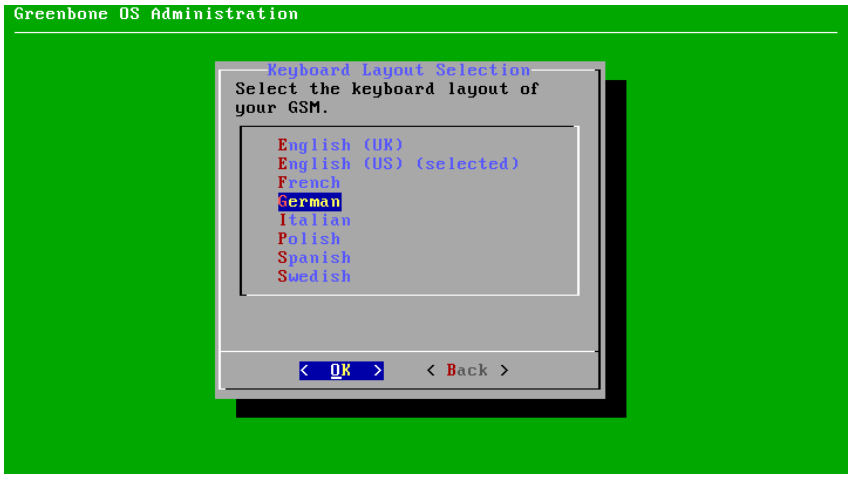


Fig. 6.37: Keyboard layout selection

After confirming the selection you will be prompted if you really want to change the keyboard layout. Confirmed your choice with `Yes` or discard it using `No`. The change will be confirmed with the message `Keyboard layout set to ...`.

6.2.9 Mail Server

If you want to send reports after completion of a scan automatically via email the appliance needs to be configured with a mail server. This server is called a mailhub or smart host. The appliance itself does not come with a mail server.

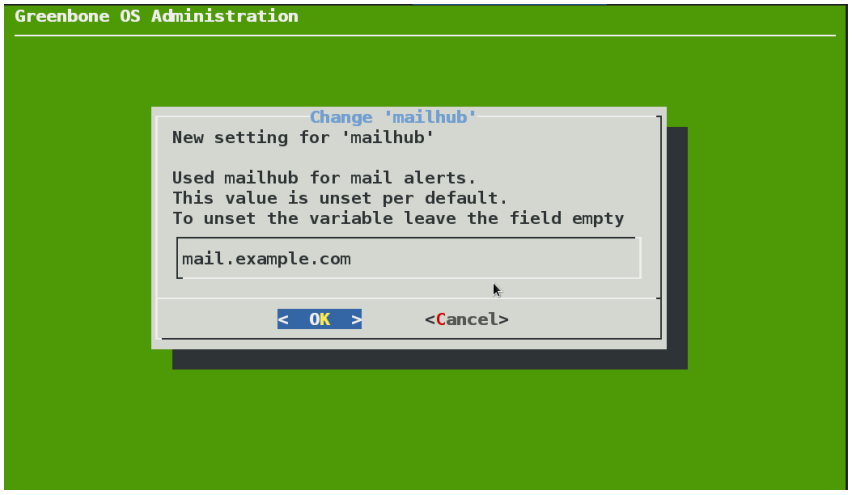


Fig. 6.38: Configuring the smart host

Confirm that the mail server that the mail server accepts emails sent form the appliance. The appliance does not store emails in case of delivery failure. A second delivery attempt at a later time will not be attempted. On the mail server possible spam protection such as grey listing must be deactivated for the appliance. Authentication using a username and password is also not supported by the appliance. The authentication must be done IP based!

To configure the mail server use the *Mail* option within the *Setup* menu.

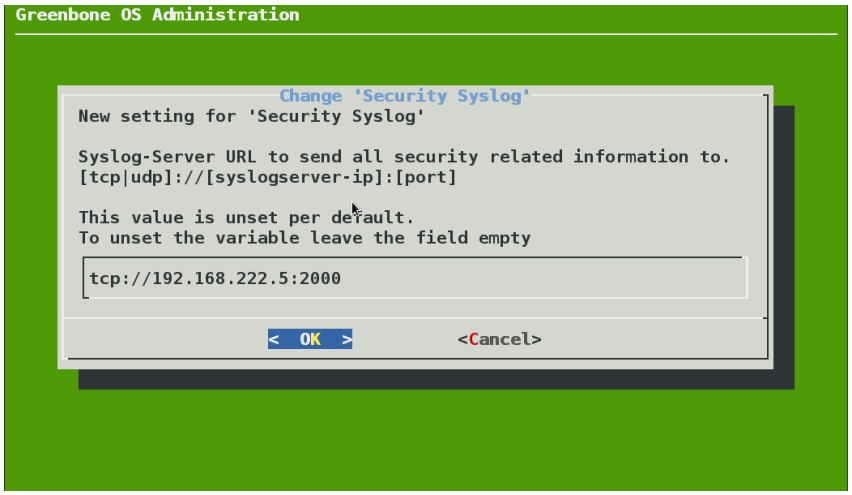


Fig. 6.39: Configuring the remote syslog server

6.2.10 Central Logging Server

The GSM appliance supports the configuration of a central logging server for the collection of the logs. Either only the security relevant logs or all syslog logs may be sent to a remote logging server. The security relevant logs contain

- user authentication
- user authorization

The GSM appliance uses the Syslog protocol. Central collection of the logs allows for central analysis, management and monitoring of logs. Additionally the logs are always also stored locally.

One logging servers can be configured for each kind of log (security or full). Both are used. As transport layer both UDP (default) and TCP can be used. TCP ensures delivery of the logs even when packet loss occurs. If packet loss occurs during a transmission via UDP the log messages will be lost.

To setup the log server use the option *Remote Syslog* within *Setup*. Choose either `Security` or `Full` and enter the remote syslog server.

If no port is specified the default port 514 will be used. If the protocol is not specified UDP will be used.

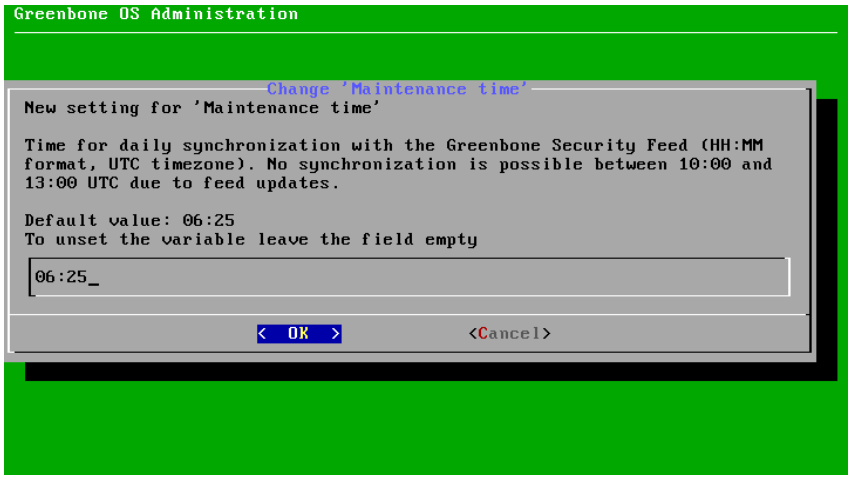


Fig. 6.40: At maintenance time the feed synchronization happens.

6.2.11 Time

This option displays and supports the modification of the maintenance time. During maintenance the daily feed synchronization takes place. You may choose any time during the day but from 10:00 to 13:00 UTC. During this period Greenbone itself updates the feed and disables the synchronization services.

If you are located in a different time zone please convert the time to UTC before entering in the dialogue.

6.3 Maintenance

The *Maintenance* option in the menu covers the main maintenance tasks:

- Selfcheck
- Manual Backup and Restore
- Upgrade Management
- Manual Feed Management
- Power Management like shutdown and reboot

6.3.1 Selfcheck

The selfcheck option checks the setup of the appliance. The selfcheck will display wrong or missing configuration details which might prevent the correct function of the appliance. The following items are checked:

- Network connection

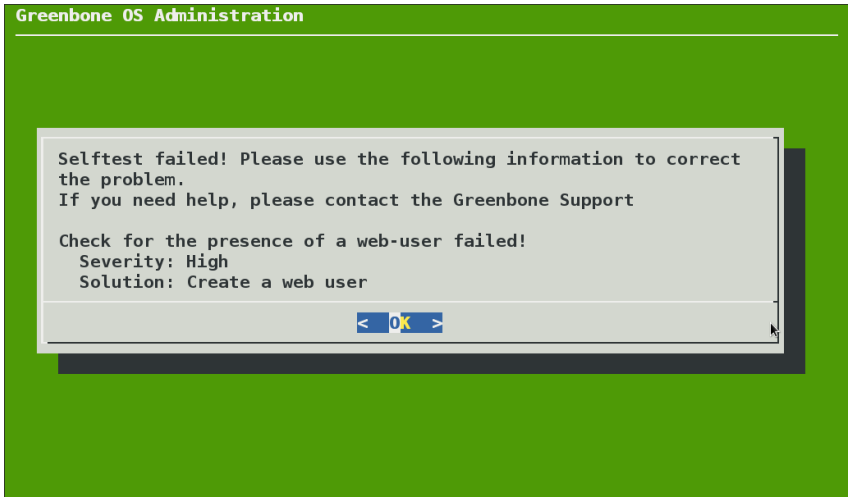


Fig. 6.41: Selfcheck checks the user configuration

- DNS resolution
- Feed reachability
- Available Updates
- User configuration

Any found problems are listed on the result page.

6.3.2 Backup and Restore

While the *Setup* lists a backup option supporting scheduled local and remote backups the option within the *Maintenance* menu supports the manual run of a backup job. Depending on the backup location configured within *Setup* the manually triggered backups are stored remotely or locally. These backups may be transferred to a USB stick for offsite storage.

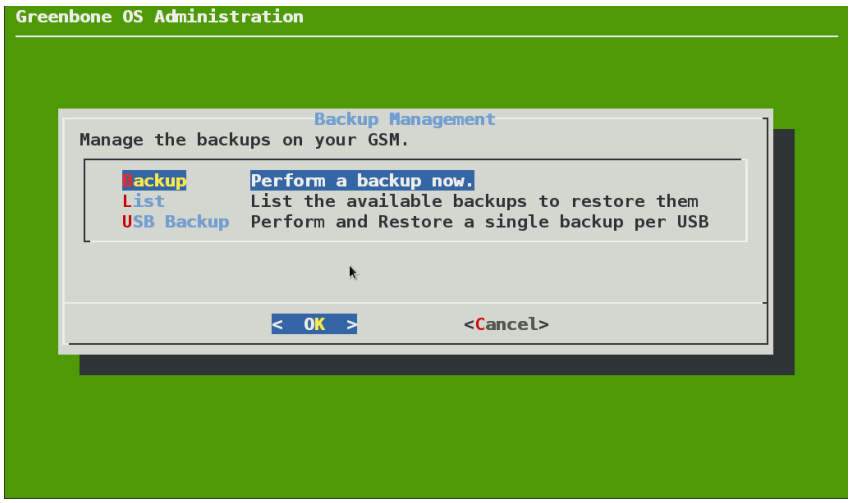


Fig. 6.42: Backups may be manually triggered

Alternatively the backups can be restored using this menu. Use the option *List* to display a list of available backups. Choose the correct backup file and restore it.

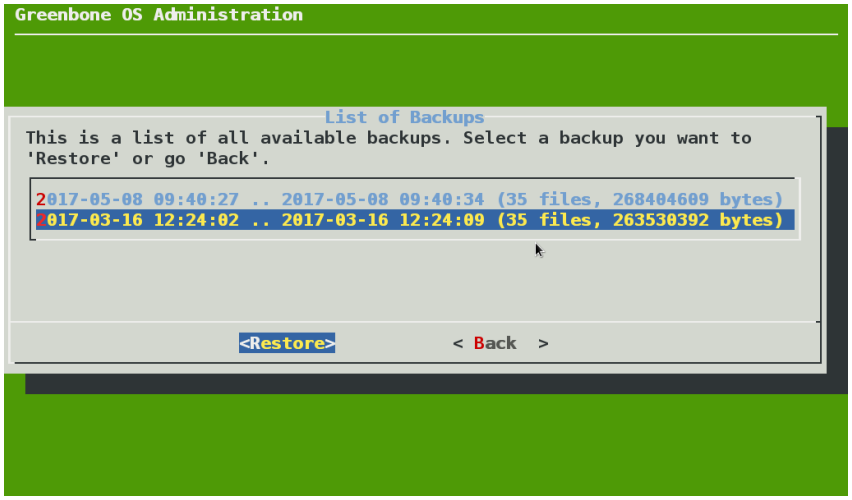


Fig. 6.43: Restoring the appliance

6.3.3 Upgrade Management

During the feed update the appliance will also download new operating system upgrades when available. While this upgrades are automatically downloaded they are not automatically installed. Since these upgrades might interrupt current scan tasks they need to be carefully scheduled. The upgrades may only be installed manually using *Upgrades* within *Maintenance*.

You will be prompted to install the upgrade if an upgrade is available. If additionally to the upgrade a release switch is possible, this will be offered as well.

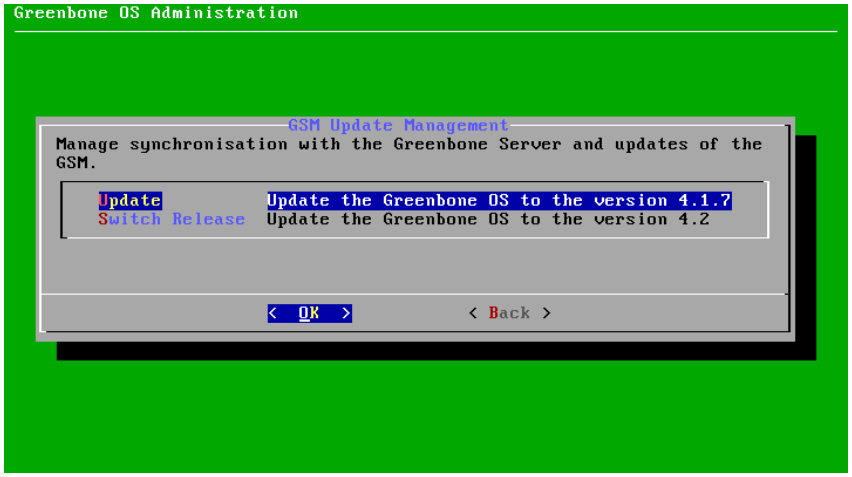


Fig. 6.44: Upgrade and switch release possible

6.3.4 Feed Management

By default the appliance will try to download new feeds and operating system updates daily. The automatic feed synchronization may be disabled. If the feed synchronization needs to be triggered manually this can be achieved using *Maintenance/Feed*.

Fig. 6.45: Manual feed update

6.3.5 Power Management

The Greenbone Security Manager should not be turned off using the power switch. Rather the appliance should be shutdown and rebooted using the menu. This ensures that mandatory cleanup processes are run during the shutdown and reboot.

Shutdown

To shutdown the appliance navigate to *Maintenance* followed by *Power*. Choose `Shut down` in the following menu and confirm your selection. The appliance will shutdown. The shutdown process may take up to several minutes.

This will shut down all running processes and scan tasks.

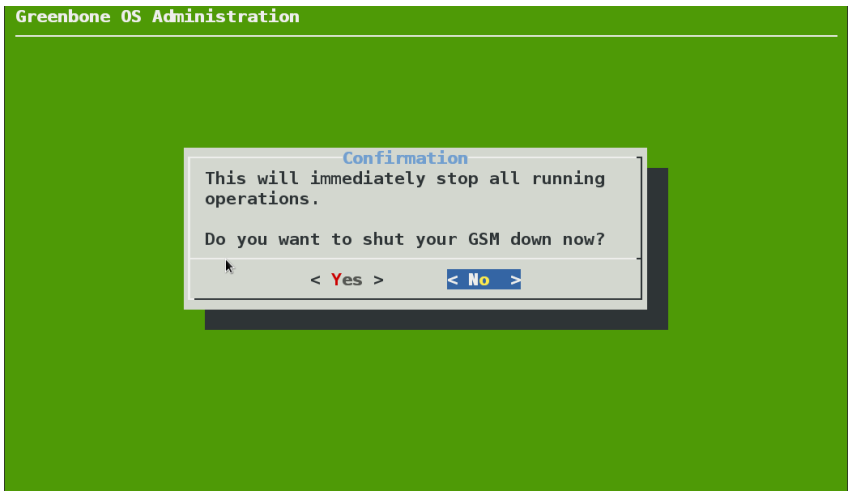


Fig. 6.46: Shutting down the appliance.

Reboot

To reboot the appliance navigate to *Maintenance* followed by *Power*. Choose `Reboot` in the following menu and confirm your selection. The appliance will reboot. The reboot process may take up to several minutes.

This will shut down all running processes and scan tasks.

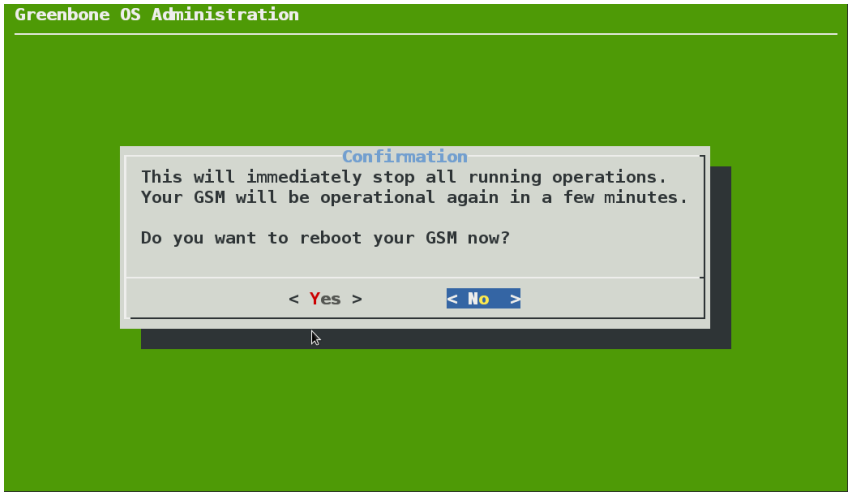


Fig. 6.47: Rebooting down the appliance.

6.4 Advanced

The *Advanced* option in the menu provides access to the support features of the GSM. Currently the *Support* option is the only option in this menu.

6.4.1 Support

The *Support* should only be used in concert with the Greenbone Support. If these options are used without guidance menu offers three different options:

- Superuser
- Support
- Shell

These options will be explained in the following sections.

Superuser

On the GSM command line the menu option *Shell* starts a UNIX command line as unprivileged user *admin*. Any UNIX command can be executed.

The privileged account `root` should only be used in emergencies in consultation with the Greenbone support team. If any modifications are done without consultation you are not entitled to receive assistance by the Greenbone support team anymore.

The `root` login is disabled via SSH. The privileged user `root` may only login via Console. In delivery state the user `root` does not have any password and is directly able to login. Using `su` to switch from the `admin` user to the `root` user is disabled by default. It may be enabled using `superuser` and `superuserpassword` (see section *Superuser* (page 49)).

Enabling the password for `root` should only be done briefly in emergencies. To remind the `admin` user of this setting it is displayed during the login process including the root-password in clear text.

To obtain root rights (superuser) on the GSM appliance the command **`su`** needs to be entered. In the factory default settings this is only possible after first enabling the superuser and providing a password to this user.

The enabling of root access should only be done by exception and by consulting with Greenbone support.

This is done using this menu *Superuser*. This menu has two options:

- Superuser
- Password

Using the first option you may enable or disable the Superuser account. You will be warned that this should only be done by exception.

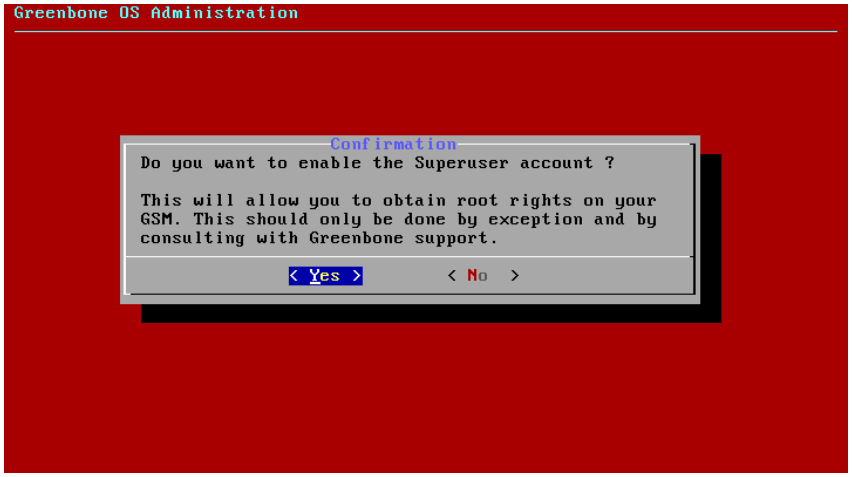


Fig. 6.48: Superuser warning

Once the superuser has been enabled the second option *Password* must be used to provide a password. To ensure the correctness of the password the password must be entered twice.

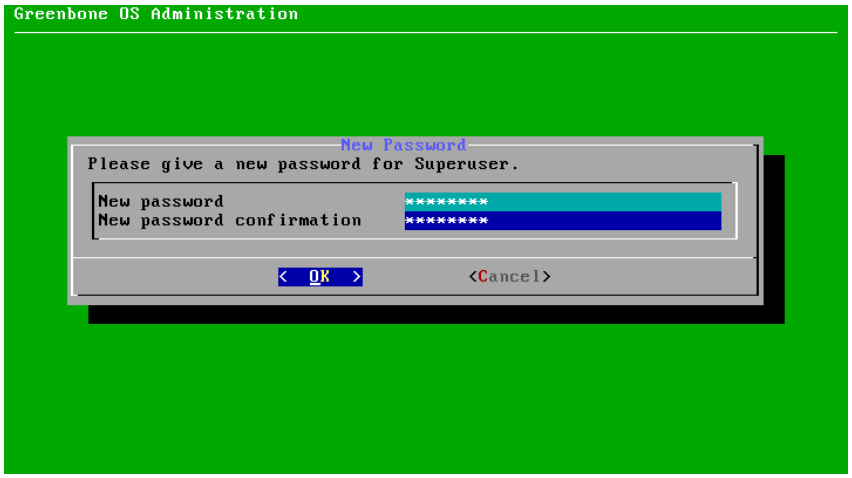


Fig. 6.49: Superuser password

All modifications need to be saved to be activated.

Support

Sometimes the Greenbone support requires additional information to troubleshoot and support customers. The required data is collected by the *Support* option. This option will create an encrypted support package including all configuration data of the GSM appliance. The package may be encrypted

using the GPG public key of the Greenbone support team. The support package is stored on the appliance.

If an encrypted support package is generated it may be downloaded via http using a browser.

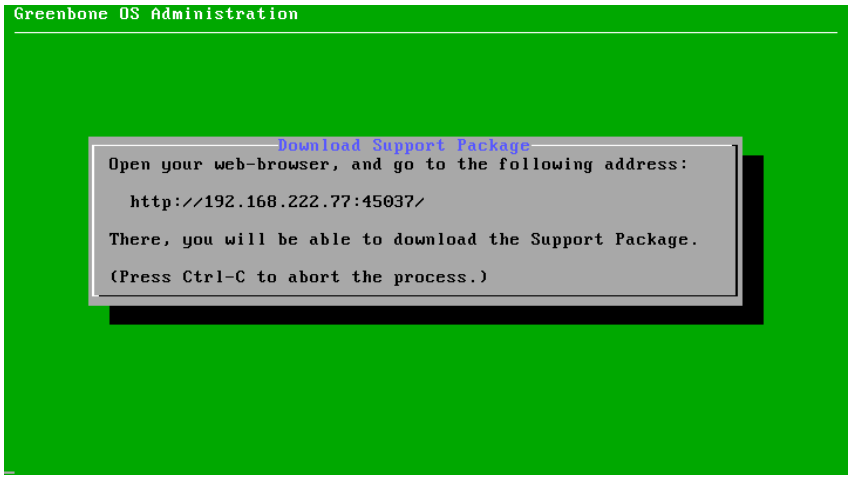


Fig. 6.50: Downloading the encrypted support package

If the support package is not encrypted the download needs to be done using the Secure Copy Protocol. You need to enable the SSH service first (see section *SSH* (page 32)). On Microsoft Windows

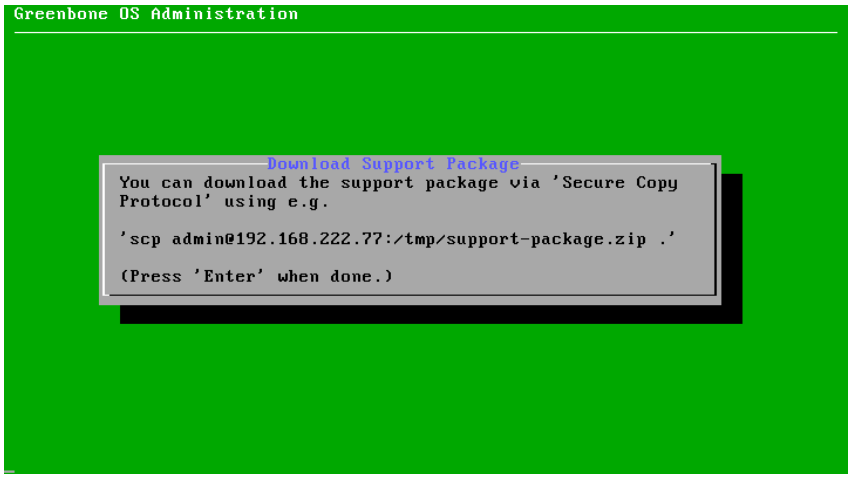


Fig. 6.51: Secure copy the unencrypted support package

systems The support package may be downloaded using either `pscp`, which is a command line tool included in Putty, or WinSCP and smarTTY which are graphical tools implementing secure copy.

Shell

For support reasons in consultation with the Greenbone support shell access is provided using this menu option. The shell access is not required for any administrative work but just for diagnostics and support. If you choose this options an appropriate warning is displayed.

Once the warning is confirmed you are placed in a Linux shell using the unprivileged user `admin`. Root access requires the enabling of the superuser and the provision of a password. You may then switch to root using the command `su`. To leave the shell enter `exit` or `Ctrl-D`.

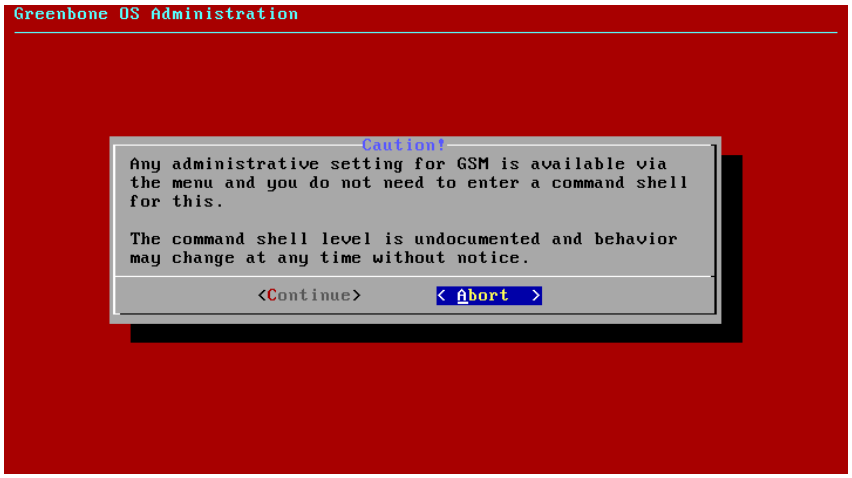


Fig. 6.52: The shell should only be used for diagnostic purposes.

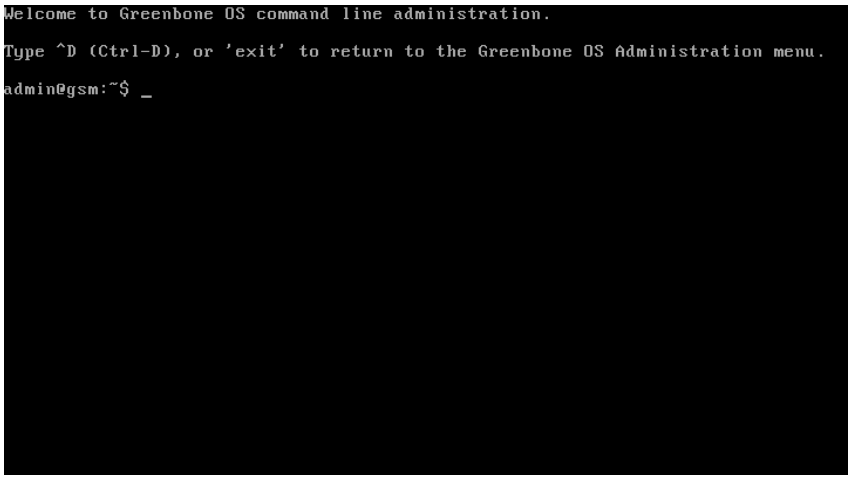


Fig. 6.53: Accessing the local shell

GUI Introduction

7.1 GUI Concepts

This chapter covers recurring concepts when using the web user interface of the Greenbone Security Manager. This includes the dashboard, standard icons, Powerfilters and tags.

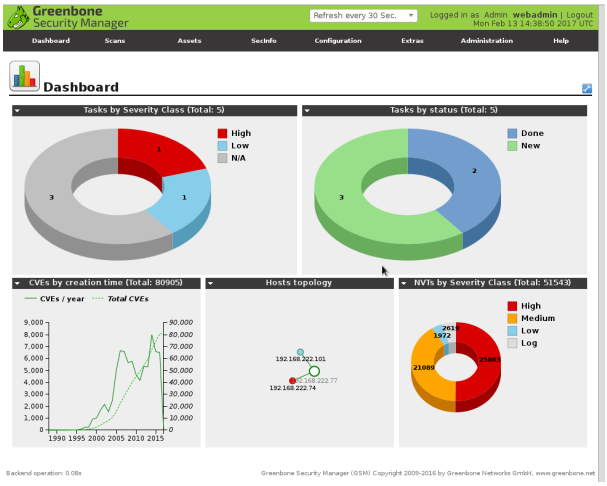
7.1.1 Dashboard

The Greenbone Security Manager has four dashboards:

- Main dashboard
- Scan dashboard
- Assets dashboard
- SecInfo dashboard

The default dashboards may be modified using the wrench icon in the upper right corner. You can add and remove charts and reset the dashboard to its defaults as well.

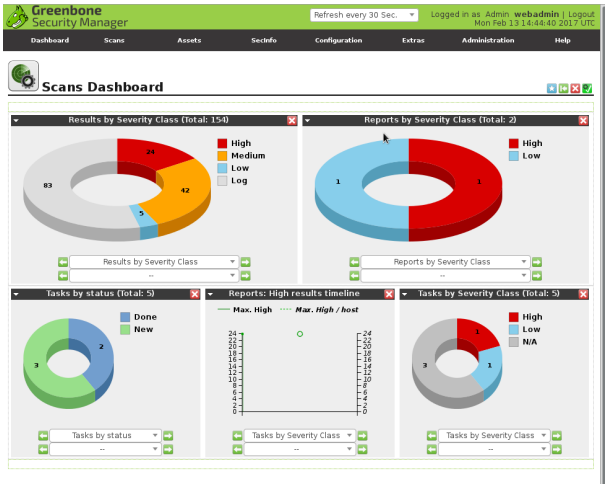
Main Dashboard



The main dashboard displays all tasks both by status and by severity at the top. At the bottom the host topology is shown and the CVEs and NVTs are rated by severity and creation time.

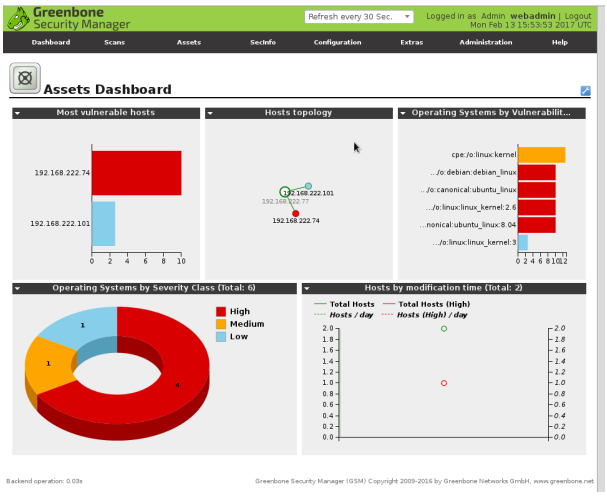
This view provides a quick presentation of the state of your network. All elements may be selected using the mouse and support a drill-down.

Scan dashboard



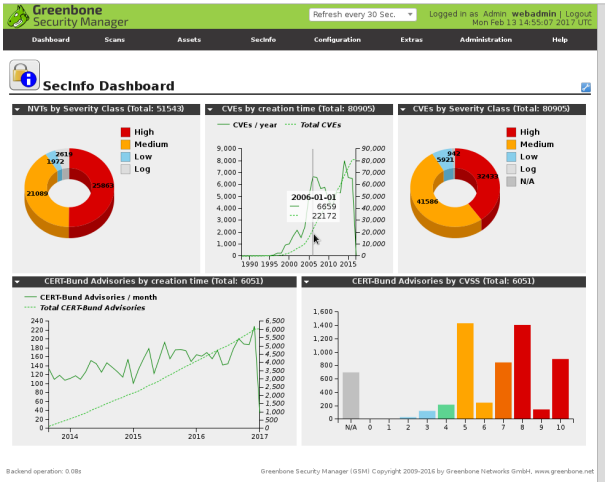
The scan dashboard concentrates on the actual scan tasks. It shows the individual scanned hosts and the full reports by their severity class. Additionally the tasks by status and severity class are shown at the bottom as well. These two graphics are already shown on the main dashboard.

Assets dashboard



The assets dashboard includes the host topology from the main dashboard and additionally displays the most vulnerable hosts, the distribution of the found vulnerabilities compared with the discovered operating systems and the operating systems by severity class.

SecInfo dashboard



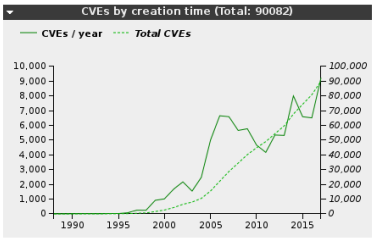
The SecInfo dashboards displays the NVTs, CVEs and CERT Bund advisories by their corresponding severity class. Additionally it displays both CVEs and CERT Bund advisories by their creation time.

Charts

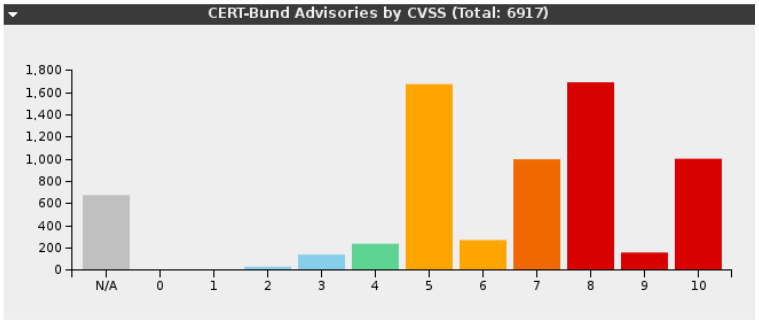
The charts in the dashboards can be customized. This allows to display and format the data in different ways. The created graphs can be downloaded and included into other documents.

There are three different chart types available:

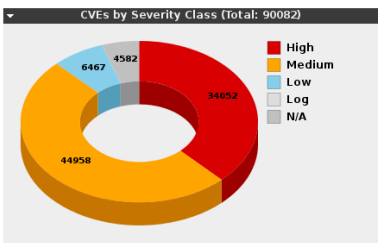
- Line chart



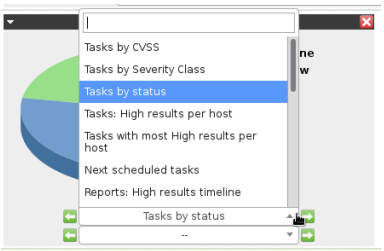
- Bar chart



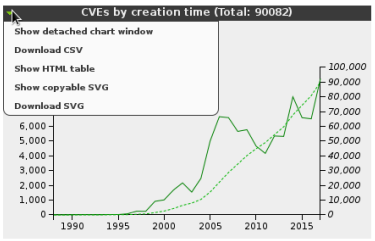
- Donut chart



The contents of the charts can be selected via the drop down menu at the bottom of the chart. This is available as soon as the edit icon in the upper left corner of the dashboard has been selected. This immediately also changes the chart type automatically.



Downloading the pictures or a copy can be selected through the context menu at the top left of the chart.



7.1.2 Icons

The web user interface uses recurring icons for the execution of identical actions. The reference of these icons results from the context of the current view.

- Display context aware help.
- Display a list of current objects.
- Create a new object. It could be a user, a target, a task, permission or a filter.
- Move an object to the trash can.
- Edit an object.
- Copy/Clone a resource.
- Export a resource as GSM object. This object can then be imported on another GSM.
- Refresh the page.
- Expand or collapse additional information, for example, the Powerfilter in the view.
- Delete an object irrevocably.
- Jump to the next object (page) in a view.
- Jump to the last object (page) in a view.
- Other users have permission to access the object as well.

Other icons can only be accessed in a certain context. This applies to the following icons:

- Start of a currently not running task.
- Stop a currently running task. All discovered results will be written to the database.
- Resume a stopped task.
- Enable or disable overrides.

- Indicates if a fix for a vulnerability exists.
- Indicates a vendor patch.
- Indicates a workaround.
- Indicates no solution exists.
- Indicates that a scan configuration is being amended with additional NVTs automatically.
- Indicates that a scan configuration is not activating new NVTs automatically.
- Reset to factory defaults
- Save changes
- Upload/Import external files

7.1.3 Powerfilter

Almost every screen in the web user interface offers the possibility to filter the information displayed. The required entries can be performed in the filter bar at the top of the web user interface.

Fig. 7.1: The Powerfilter offers filtering of the displayed results everywhere.

The filter bar can be expanded by . This opens a new overlay. Multiple context aware parameters are being displayed that are being combined to become the Powerfilter. They can also be entered in the filter bar directly.

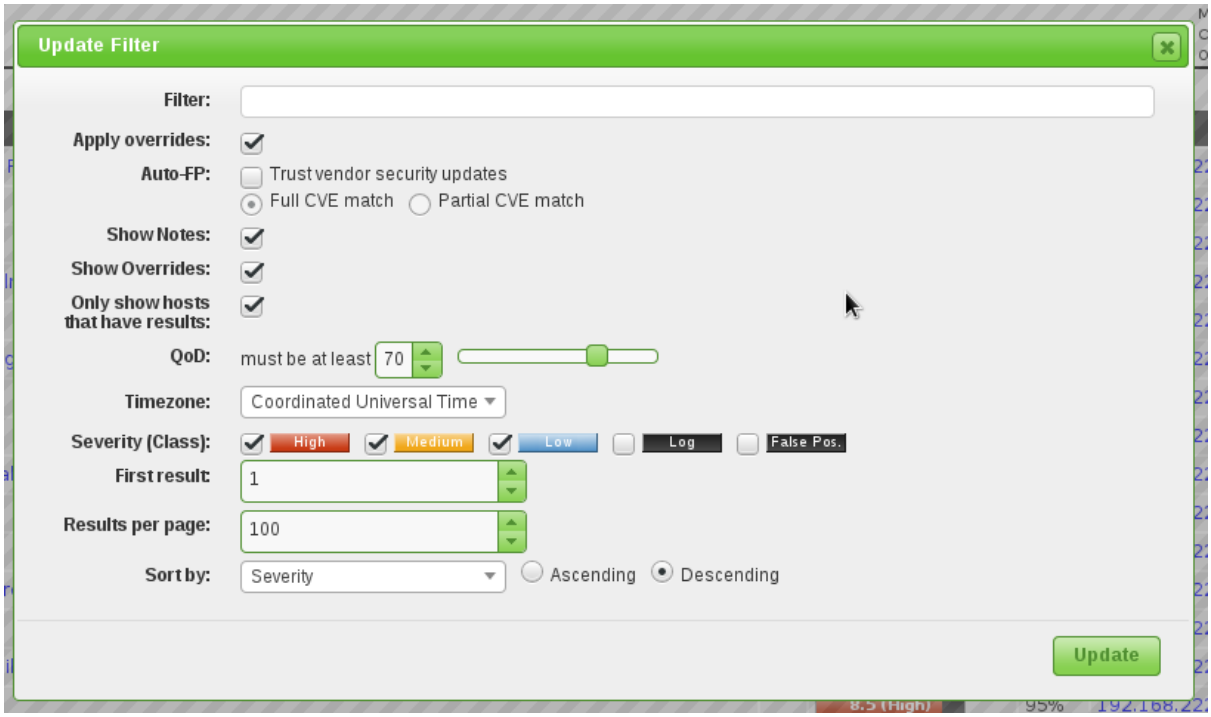


Fig. 7.2: The Powerfilter can be expanded in an overlay.

Thereby the Powerfilter is context aware again. Depending on the context more or less options are available respectively after expanding.

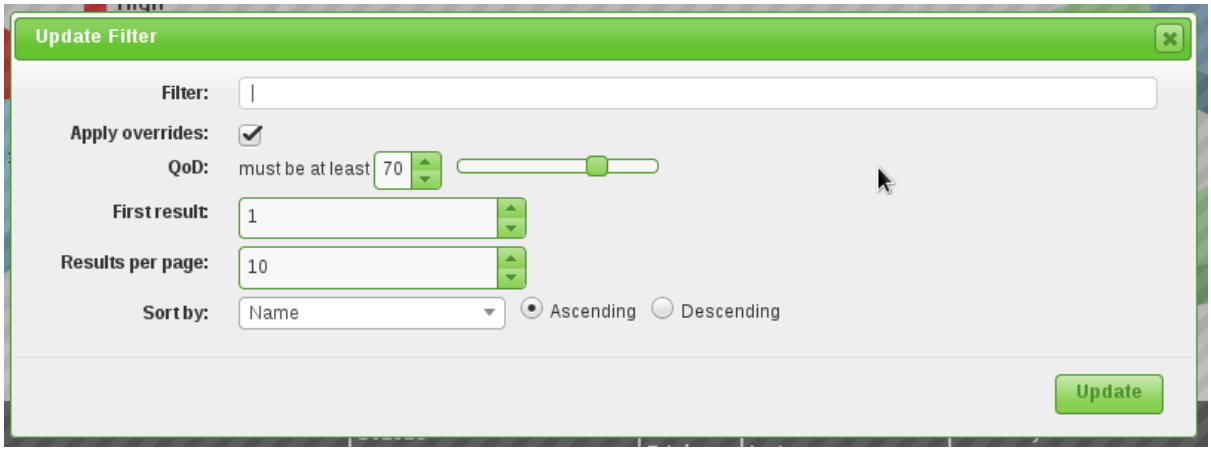


Fig. 7.3: The options of the Powerfilter are context aware.

Note: The Powerfilter is not case sensitive.

A typical Powerfilter search could search for all CVE-2012-* vulnerabilities within the 192.168.222.0/24 network:

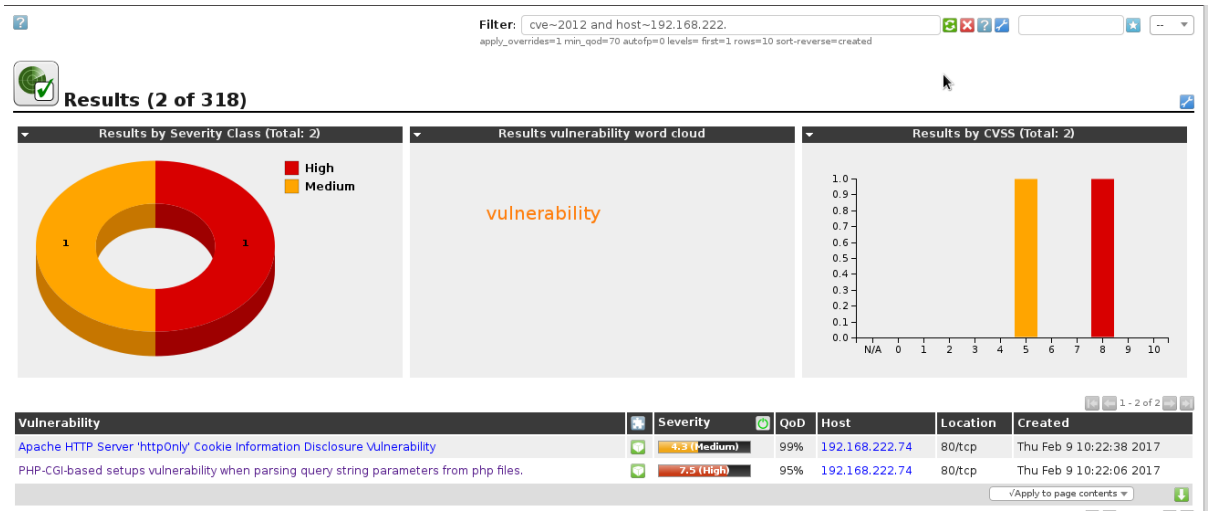


Fig. 7.4: Powerfilters may search for CVEs

Components

The possible components of the Powerfilter depend on its context. In general the specification of the following parameters is always possible:

- ***rows*:** Enter the amount of the results to be displayed. Mostly the value is *rows=10*. Entering a value of `-1` will display all results. Entering a value of `-2` will use the value that was pre-set in *My Settings* under *Rows Per Page*.
- ***first*:** Sets from which position the results should be displayed. If a search returns 50 results but only 10 should be displayed at the same time, *rows=10 first=11* displays the second 10 results.
- ***sort*:** Defines the column that should be used for sorting the results (*sort=name*). The results are being sorted ascending. The name of the column can mostly be deducted from the name

of the column. By clicking the column the name of the column can be verified. Typical column names are:

  - *name*
  - *severity*
  - *host*
  - *location*

  The column names will be changed to small caps and spaces to underscores. Additionally a couple of other fields are available.

  - *uuid*: The uuid of a result
  - *comment*: A possible comment
  - *modified*: Date and time of the last modification
  - *created*: Data and time of the creation

- ***sort-reverse*:** Defines the column that should be used for sorting the results (*sort-reverse=name*). The results will be sorted descending.
- ***tag*:** Selects only the results with a specific Tag (see also *Tags* (page 61)). It can be filtered by a specific tag value (*tag="server:mail"*) or search only for the tag (*tag="server"*). Regular expressions are also allowed.

Note: By filtering using tags custom categories can be created and used in the filters. This allows for versatile and granular filter functionality!

When specifying these components many operators can be used:

- = equals i.e. rows=10
- ~ contains i.e. name~admin
- < less than i.e. created<-1 w older than a week
- > greater than i.e. created>-1 w younger than a week
- :RegEx i.e. name:admin$

There are a couple of special features. If the value is omitted after the equal sign all results will be displayed where this value is not set:

```
comment=
```

shows all results without a comment.

If the column that should be searched is omitted all columns will be searched:

```
=192.168.15.5
```

This searches if at least one column contains the search string.

The data is usually *or* combined. This can be specifically specified with the key word `or`. To achieve an and-combination the keyword *and* needs to be specified. Using *not* will negate the filter.

Date specifications

Date specifications in the Powerfilter can be absolute or relative. An absolute data specification has the following format:

```
2014-05-26T13h50
```

The time can be omitted:

```
2014-05-26
```

The time of 12:00am will be assumed automatically. The date specification can be used in the search filter i.e. *created>2014-05-26*.

Relative time specifications are always calculated in relation to the current time. Positive time specification are interpreted as being in the future. Time specification in the past are defined with a prepended minus (-). For time periods the following letters can be used:

- s second
- m minute
- h hour
- d day
- w week
- m month (30 days)
- y year (365 days)

To view the results of the past 5 days enter *-5d*. A combination *5d1h* is not permitted. This is to be replaced with *121h* respectively.

To limit the time period , i.e. month, for which information should be displayed the following expression can be used:

```
modified>2014-06-01 and modified<2014-07-01
```

Text phrases

In general, additionally text phrases that are being searched for can be specified. Then only results are being displayed in which the text phrases where found. If the text phrases or not limited to a column (*name=text*) all columns will be searched. This means that also columns that are hidden from the current view will be searched as well.

The following examples can be useful:

`overflow` Finds all results that contain the word `overflow`. This applies to both `Overflow` as well as `Bufferoverflow`. Also `192.168.0.1` will find `192.168.0.1` as well as `192.168.0.100`.

`remote exploit` Will find all results containing `remote` or `exploit`. Of course results that contain both words will be displayed as well.

`remote and exploit` Both words must be found in a result in any column. The results do not have to be found in the same column.

`"remote exploit"` The exact string is being searched for and not the individual words.

`regexp 192\.168\.[0-9]+.1` The regex is being searched for.

Fig. 7.5: Often used Powerfilters can be saved and retrieved again.

Saving and Management

Interesting and often used filters can be saved as well. This simplifies their re-use. For example, to display the NVTs that were modified or added to the feed last week, in the GUI select *SecInfo Management* followed by *NVTs*. Then edit the Powerfilter so that it has the following content (see figure *Often used Powerfilters can be saved and retrieved again.* (page 60)):

```
Created>-1w or modified>-1w sort-reverse=created rows=1 first=1
```

Fig. 7.6: The filters can be selected via the drop down box.

This displays all the NVTs that were created or modified last week. This filter can now be given a name. Use the field to the right of the Powerfilter. Enter the name and confirm with . The filter is now being saved and can be selected via the drop down box next to it.

To use a previously saved filter use the drop down box and confirm afterwards by clicking *Switch Filter* (see figure *The filters can be selected via the drop down box.* (page 61)). If Java script is activated the filter is executed immediately after selection from the drop down box.

If a specific filter should always be activated in a specific view it can be done in the user settings (see also chapter *My Settings* (page 62)). In this example (see figure *Often used filters can be set up as default filter in the user settings.* (page 61)) it is the *NVT Filter*.

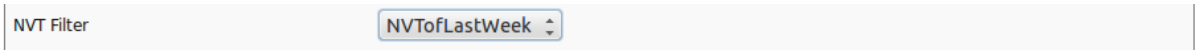


Fig. 7.7: Often used filters can be set up as default filter in the user settings.

All saved filters can be managed in *Configuration/Filters*. Here, filters can be deleted, edited, cloned and exported as GSM object for import into other appliances.

Fig. 7.8: All filters can be easily managed.

These filters can then be used to filter results of events for the alerts as well.

Filters can be shared.

7.1.4 Tags

Tags are discretionary information that can be linked to any resource. Tags are simply created directly with the resources. Then the tags can be used to filter objects respectively with the help of the Powerfilter (see section *Powerfilter* (page 57)). This presents very powerful and granular filter possibilities.

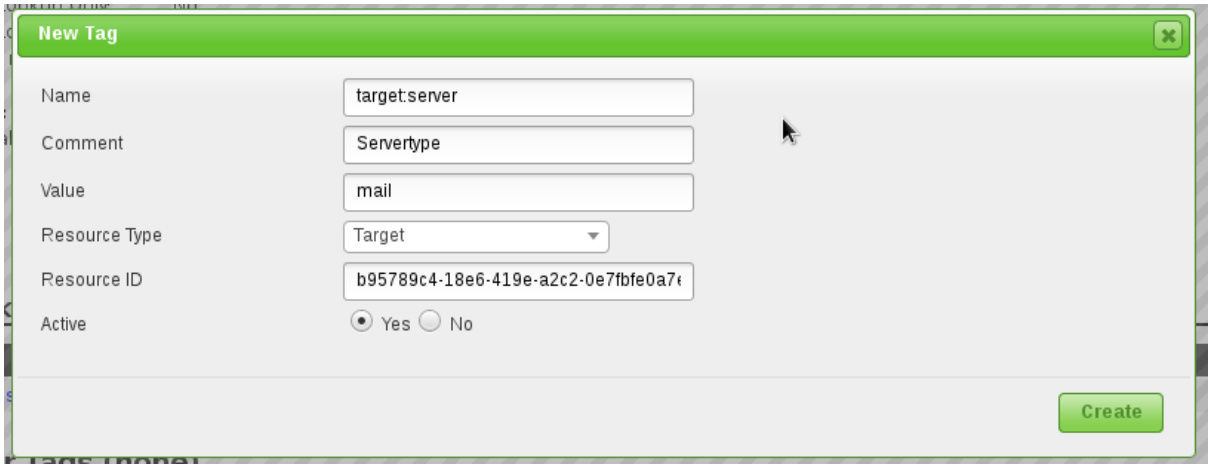


Fig. 7.9: Tags are discretionary strings that can be assigned a value.

Afterwards these tags can be used in filter expressions. With the filter `tag=target:server` the specific tag must be set in order to be included. The assigned value is irrelevant and can be empty. With `tag="target:server=mail"` the exact tag with the respective value must be set.

7.2 My Settings

Every user of the GSM appliance can manage their own settings for the web interface. This setting can be accessed by either selecting *Extras* under the submenu *My Settings* or by clicking on the user name at the top right.

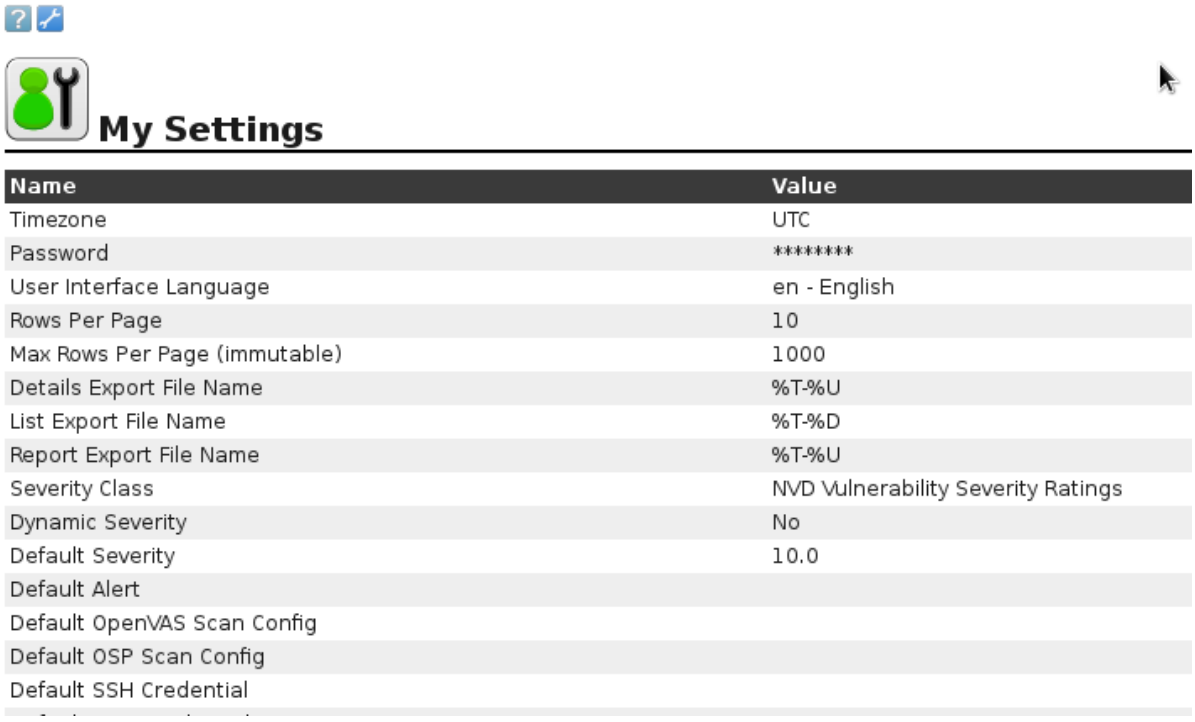


Fig. 7.10: Every user can manage their own settings.

By clicking the icon in the upper left corner the user can modify these settings. Important settings are:

***Timezone*:** Internally the GSM saves all information in the UTC time zone. In order to display the data in the time zone of the user the respective selection is required here.

***Password*:** Here the user can change their password.

***User Interface Language*:** Here the language is defined. The default uses the browser setting. To always get an English or German interface use *english* or *german*.

***Rows Per Page*:** This is the amount of results in a list.

***Wizard Rows*:** This defines how long to display the wizard for. For example, if the value is set to 3 the wizard won't be displayed in the task overview as soon as a minimum of 4 tasks are available.

***Details Export File Name*:** This defines the default name of the file for exported resource details. The format string can contain alphanumeric characters, hyphens, underscores and placeholders that will be replaced as follows:

- %C The creation date in the format YYYYMMDD. This gives the current date if a creation is not available, e.g. when exporting lists of resources
- %c The creation time in the format HHMMSS. Falls back to the current time similar to %C.
- %D The current date in the format YYYYMMDD
- %F The name of the format plugin used (XML for lists and types other than reports).
- %M The modification date in the format YYYYMMDD If the modification date is not available this gives either the creation date or the current date if a creation date is no available as well, e.g. when exporting lists of resources.
- %m The modification time in the format HHMMSS. Falls back to the creation time or current time similar to %M.
- %N The name for the resource or the associated task for reports. Lists and types without a name will use the type (see %T).
- %T The resource type, e.g. “task”, “port_list”. Pluralized for list pages.
- %t The current time in the format HHMMSS
- %U The unique ID of the resource or “list” for lists for multiple resources.
- %u The name for the currently logged in user.
- %% The percent sign (%).

***List Export File Name*:** This defines the default name of the file for exported resource lists (see above).

***Port Export File Name*:** This defines the default name of the file for exported reports (see above).

***Severity Class*:** Here the classification of the vulnerability respective to the score can be defined.

- NVD Vulnerability Severity Ratings
  - 7.0 - 10.0: High
  - 4.0 - 6.9: Medium
  - 0.0 - 3.9: Low
- BSI Vulnerability Traffic Light
  - 7.0 - 10.0: Red
  - 4.0 - 6.9: Yellow
  - 0.0 - 3.9: Green
- OpenVAS classic
  - 5.1 - 10.0: High
  - 2.1 - 5.0: Medium

  - 0.0 - 2.0: Low
- PCI-DSS
  - 4.3 - 10.0: High
  - 0.0 - 4.2: None

***Filter*:** Here specific default filters for each page can be specified that are being activated automatically when the page is loaded.

CHAPTER 8

GUI Administration

8.1 User Management

The Greenbone Security Manager allows for the definition and the management of different users with different roles and permissions. When initializing the GSM the first user, the web/scan administrator respectively, is being created via the GOS-Admin-Menu already. This user allows the login and management of additional users.

The GSM user management supports a role based permission concept when accessing the web interface. Various roles are already set up by default. Additional roles can be created and used by an administrator. The role defines which options of the web interface can be viewed and modified by the user. The role enforcement is not implemented in the web interface but rather in the underlying GMP protocol and hence affecting all GMP clients. Read and write access can be assigned to roles separately.

In addition to the roles the GSM user management supports groups as well. This serves mainly for logical grouping. Groups and roles may be used to assign permissions to several users at once.

Each user may be assigned an IP address range containing the allowed or denied targets. The GSM appliance will then refuse to scan any other IP addresses than the ones specified for the respective user. Similarly the access to specific interfaces of the GSM appliance can be allowed and denied.

This user management is contained within the GSM. External sources for the user management are not supported. However, to support central authentication and to allow password synchronization the Greenbone Security Manager may be integrated with a central LDAP or RADIUS server. But this server will only be used to verify the password during the log in process of the user. All other settings are being performed in the User Management of the GSM appliance.

These functions are being covered in more detail below.

8.1.1 Creating and Managing Users

The dialog for the creation and management of users can be accessed via the *Administration* menu. This menu is only visible to administrators as only they are allowed to create and manage additional users. The dialog to create a new user can be accessed via the white asterisk on blue background  or by selecting the wrench an existing user can be modified.

When creating a new user the following options are available:

- *Login Name*: This is the name the user logs in with. If an LDAP server is used for central password management, the user needs to be created with the identical name (rDN) as used by the LDAP server. This is also true when using a RADIUS server. The name can be a maximum of 80 characters and can contain letters and numbers.
- *Password*: This is the password for the user. The password can be a maximum of 40 characters and can contain any type of character. Please note when using special characters that they are available on all keyboards and operating systems in use.

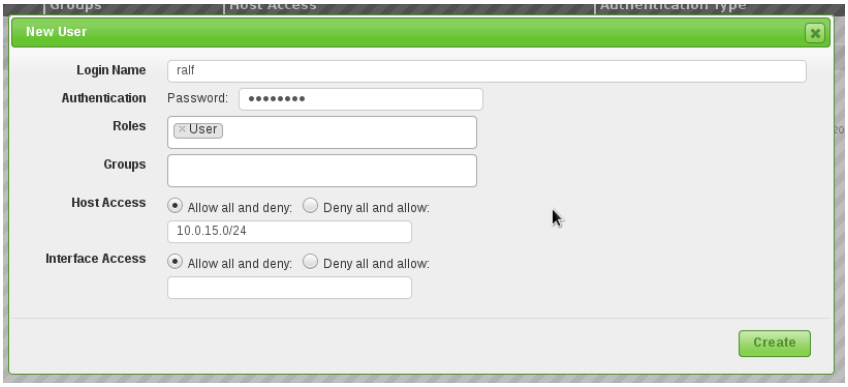


Fig. 8.1: Creating a new user.

- *Roles (optional)*: Each user can have multiple roles. The roles define the permissions of a user when using the OMP protocol. Since the Greenbone Security Assistant utilizes the OMP protocol the roles define directly the features in the web interface. While it is possible to add and configure additional roles, at the beginning, the roles *Admin*, *User*, *Info*, *Observer*, *Guest* and *Monitor* are available. These roles are discussed in more detail in section *User Roles* (page 67).
- *Groups*: Each user can be a member of multiple groups. Permissions management can be performed via groups as well (see section *Permissions* (page 73)).
- *Host Access*: These systems may be analyzed by the user in a scan. Alternatively you can specify which systems should not be considered in a scan. These restrictions also apply to administrators. They can, however, remove these restrictions themselves. This function simply serves as a self-protection for administrators. Normal users (*User*) and roles without access to the user management respectively cannot circumvent this restriction. Basically either a whitelist (deny all and allow) or a blacklist (allow all and deny) are possible. In the first case the scanning of all systems is denied in general and only explicitly listed systems are allowed to be scanned. In the latter case the scanning of all systems is allowed except the listed systems. System names as well as IPv4 and IPv6 addresses can be entered. Furthermore individual IP addresses as well as address ranges and network segments can be specified. The following listing shows some examples:
  - 192.168.15.5 (IPv4 address)
  - 192.168.15.5-192.168.15.27 (IPv4 range long form)
  - 192.168.15.5-27 (IPv4 range short form)
  - 192.168.15.128/25 (CIDR notation)
  - 2001:db8::1 (IPv6 address)
  - 2001:db8::1-2001:db8::15 (IPv6 range long form)
  - 2001:db8::1-15 (IPv6 range short form)
  - 2001:db8::/120 (CIDR notation)

  All options can be mixed and matched and entered as a comma separated list. The netmask in the CIDR notation is restricted to a maximum of 20 for IPv4 and 116 for IPv6. In both cases the result is a maximum of 4096 IP addresses.
- *Interface Access*: If the GSM uses several network adapters to connect to different networks the usage of these adapter may be restricted for the scan by the user. A comma separated list of network adapters can be entered and similar to the Host Access it can be chosen between a whitelist and blacklist methodology.

Tip: In general the whitelist methodology should be used and scans of systems denied except for the chosen systems. This is to ensure that users do not scan systems by accident or unknowingly

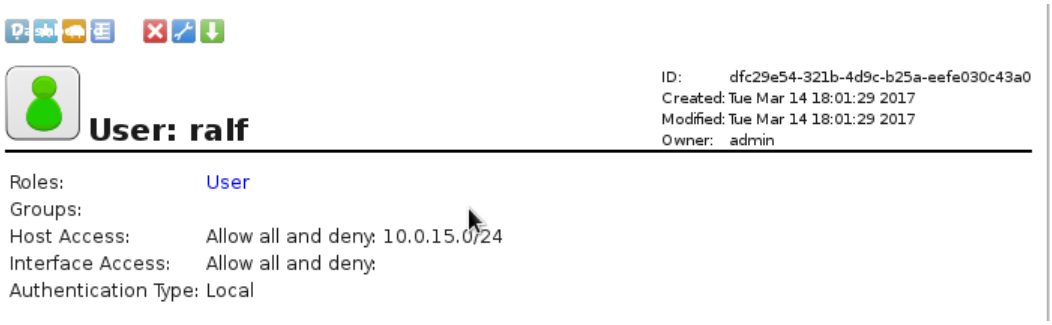


Fig. 8.2: Displaying a user.

that are outside of there are of responsibility, are located somewhere on the Internet or react to a malfunctioning scan.

After creating the user the user's properties are displayed. The display should be verified to ensure that the user does not have too many permissions assigned to him.

8.1.2 Simultaneous Log in

It is possible, of course, that two users are logged into a GSM at the same time. If the same user wants to log in multiple times the login must be performed from a different PC or at least a different browser. Another log in in the same browser invalidates the first login.

8.2 User Roles

The Greenbone Security Assistant supports the creation and configuration of your own user roles. Like in all other instances the modification of the factory provided roles is not possible. However they may be copied (cloned) and subsequently modified. This ensures consistent behaviour when updating the software.

The role management can be accessed via the web interface in the menu *Administration* in the submenu *Roles*. The following three roles are available by default:

- *Admin*: This role by default has all permissions. It is especially allowed to create and manage other users.
- *Guest*: This role corresponds with the Info role. It merely is not allowed to change its settings.
- *Info*: This role (Information Browser) only has read access to the NVTs and SCAP information. All other information is not available.
- *Monitor*: This role has access to performance data of the GSM (see section *Appliance Performance* (page 220)).
- *Observer*: This role has read access to the system. It is not allowed to start or create new scans. It has only read access to the scans for which the respective users have been set up as observers.
- *Super Admin*: This role has access to all objects of all users. It has no relation to the SuperUser in the command line. This role can not be configured in the web interface. The configuration is only possible in the GOS-Admin-Menu (see section *Super Admin* (page 69)),
- *User*: This role by default has all permissions with the exception of user, role and group management. Besides, this role is not allowed to synchronize and manage the feeds. In the web interface there is no access to the menu option *Administration*. All other options, however, are available to this role.

Additional roles can easily be created. The simplest way to create a new role is copying one of the existing roles that reflects your needs the closest and modify it. In rare cases you might want to create a role that only supports limited functionality. In those cases it makes more sense to start with an empty role.

User can have more than one role. Therefore permissions can be grouped with the help of the roles. If more than more than one role is assigned to a user the permissions of the roles will all be added.

Hence a role *Maintenance* can be created for example. This role is being assigned the following permissions:

- *authenticate*
- *get_settings*
- *write_settings*
- *help*
- *describe_cert*
- *describe_feed*
- *describe_scap*
- *sync_cert*
- *sync_feed*
- *sync_scap*

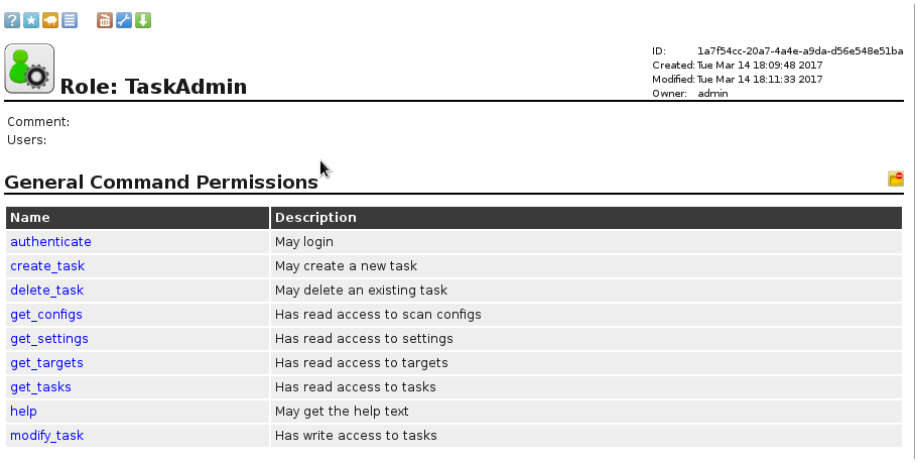


Fig. 8.3: The TaskAdmin role only has restricted access.

Additional roles then can have the name *TargetAdmin*, *ScanConfigAdmin*, *TaskAdmin* and *Scanner* and assigned permissions respectively. Important is the fact that roles require at minimum the permissions *authenticate* and *get_settings*. These are an imperative requirement to log into the web interface. The permission *write_settings* makes sense as well. Then a user can change his own password, time zone and other personal settings.

Users can be assigned different permutations of these roles. This allows specific users to configure target systems, scan configurations or configure and start the actual scan. In the selection of the permissions only the permissions that are not assigned are being displayed. This simplifies adding and the overview of the still available permissions.

If a user logs in with the role *TaskAdmin* later the menu options are restricted respectively.

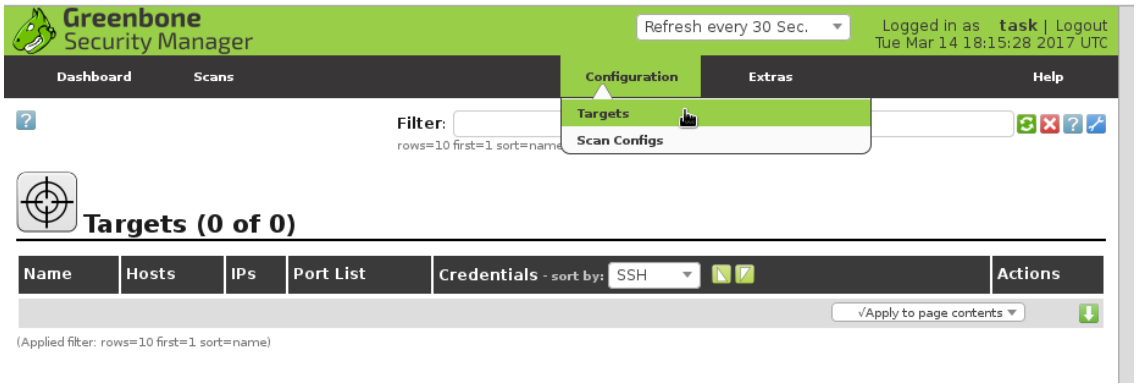


Fig. 8.4: The menu selection for the TaskAdmin role is restricted.

8.2.1 Guest Log in

The GSM can be configured for guest log in. The guest user is only allowed to access the SecInfo-Management (see chapter *SecInfo Management* (page 139)). This offers easy access to current information without password.

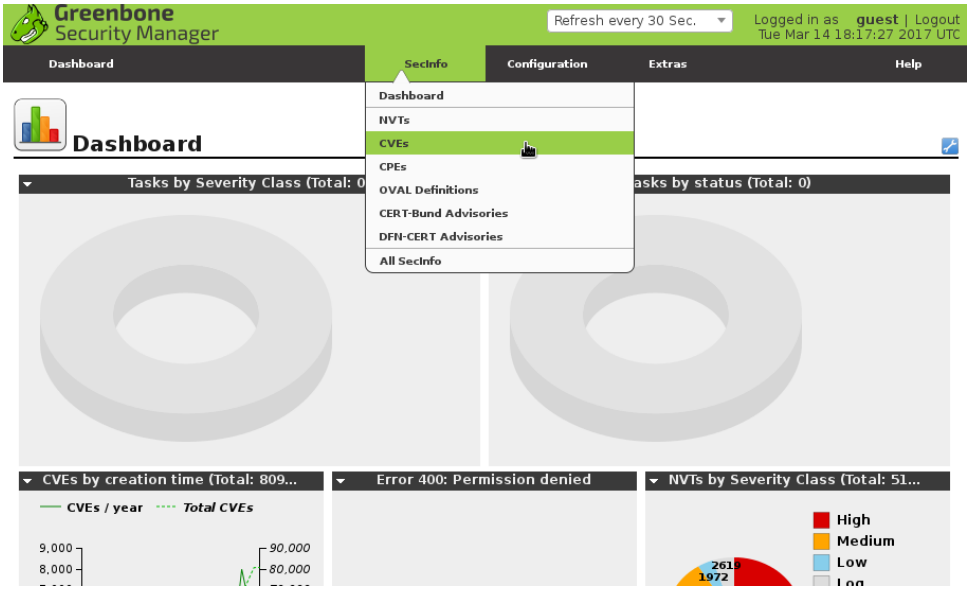


Fig. 8.5: The guest role has access to the SecInfo Dashboard.

To allow this guest access a user can be created and assigned the *Guest* role.

Having knowledge of the password this user now can log in and is presented with the dashboard.

To allow a guest log in without password it must be activated on the command line first. To do so start the GOS-Admin-Menu and select the option *User* followed by *Web Users*. Afterwards activate the *Guest User* in the respective option. Enter the name of the guest user and his password. Save the pending changes. No reboot is required. Now the guest login is available at the web login screen (see figure *Log in as guest user without password.* (page 70))

8.2.2 Super Admin

The Super Admin is the highest level of access. It was introduced with the new permission concept. The regular admin role is equal to a simple user but additionally allows the creation, modification and deletion of users. Furthermore the admin can view, modify and delete any permission on the system

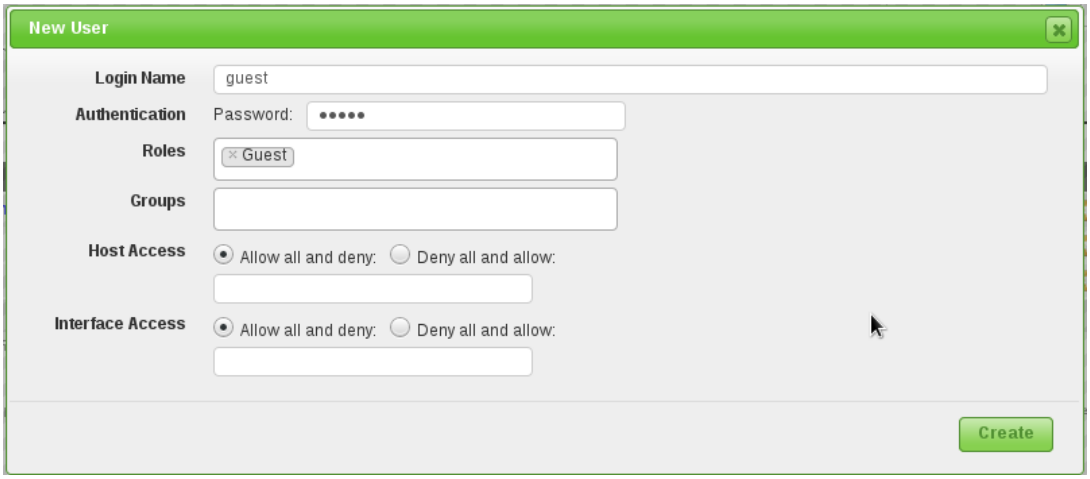


Fig. 8.6: Create a guest user.

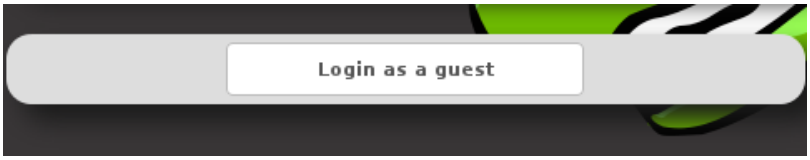


Fig. 8.7: Log in as guest user without password.

but the admin is at the same time subjected to those permissions. If any user creates a private scan configuration but does not share it, the admin may not access the scan configuration. Of course the Admin could create respective permissions itself to the resource created by the user but this is quite cumbersome. For the collaborative work of groups of users additional permissions might be setup (see section *Super Permissions* (page 70)).

Again for diagnostic purposes these are not very helpful and the Super Admin is more suited. The Super Admin is excluded from the permission restrictions. The Super Admin is allowed to view and edit any configuration settings of any user.

But the Super Admin can not be created in the web interface. To create the Super Admin access to the command line is required. This user and password can be created in Gos-Admin-Menu under the menu *User/Web Users* submenu *Super Admin*.

Afterwards the super admin may be edited in the web interface.

The Super Admin can not be modified by the regular admin. Only the Super Admin itself can modify the settings of this user!

Super Permissions

Roles and groups can be assigned with Super-Permissions. Then all objects within a group may be accessed.

Any resource created on the GSM (scan, configuration, target, and so on) is either global or is owned by a specific user. Global resources are identified by the icon . Any resource that is not global can be viewed and used only by its owner initially. Individual permissions are necessary to make the resource available to other users. This is very cumbersome. Therefore the Greenbone OS offers the option to assign *Super Permissions*. A user can get these Super Permissions for:

- User
- Role
- Group

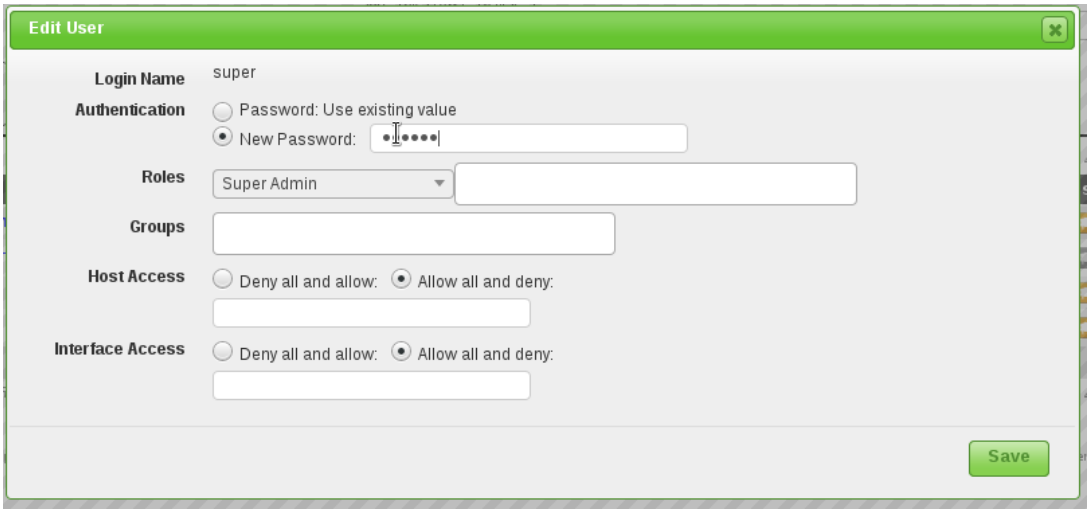


Fig. 8.8: The Super Admin **can not** be created in the web interface!

- Any

These Super Permissions then allow complete access to any resources of the respective user, role, group or effectively all resources. The any access can not be set explicitly. It is a privilege of the Super Admin (see section *Super Admin* (page 69)). This is why the last Super Permission can only be set by creating a Super Admin.

A user can only set Super Permissions for objects created by himself. First the user must determine the Resource ID of the user, the role or the group for which to set the Super Permissions.

Afterwards the values can be entered in the dialog.

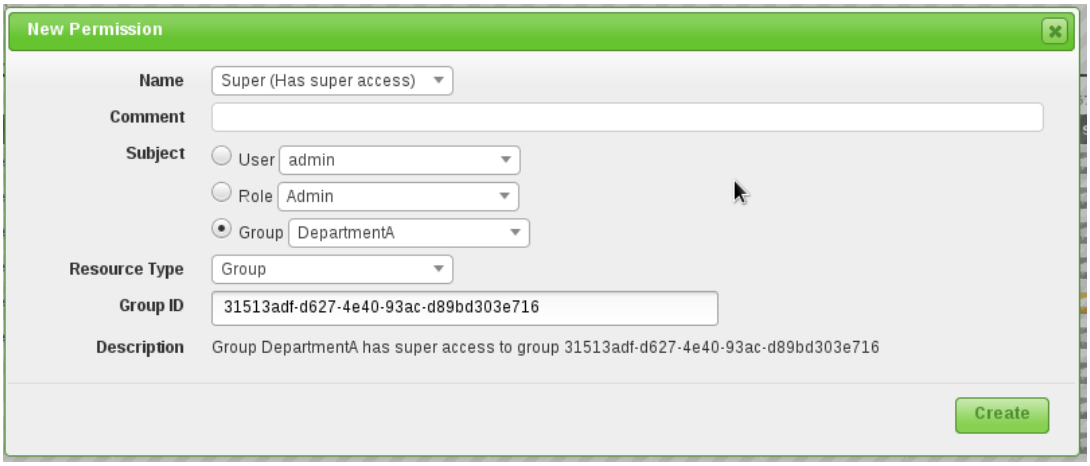


Fig. 8.9: For the Super Permission the Resource ID is required.

In the success message instead of the Resource ID the name is being displayed in clear text.

In this example all members of the group DepartmentA have full access to the object created by the other users within the same group. If a user with the role *observer* is member of the group DepartmentA this user may execute only read permissions on all objects created by the members of the group. The observer role restricts the available permissions.

The Super Permissions simplify the permission management on the GSM. Super Permissions for entire groups can be assigned very easily. This allows all users of a group access to all resources that are being created by other members of the group.

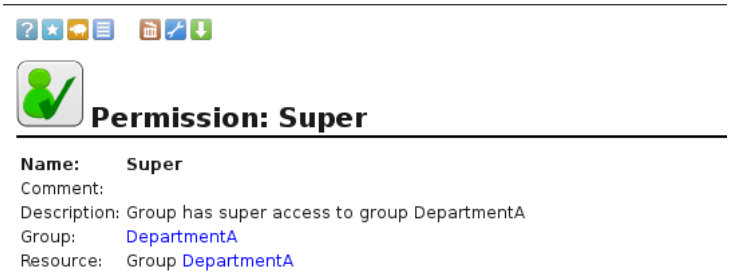


Fig. 8.10: The group DepartmentA has Super Access to the resources of the group DepartmentA.

GetUsers Role for Observers

The GSM allows for management of observers (see section *Permissions* (page 89)). These are users that have read access to specific tasks and their respective reports. These observers by default can only get permissions to tasks and reports by administrators. Regular users can not grant observers access to their own tasks. Therefore they can not share their tasks with other users. The respective dialog to manage permissions in not functional and does not support the selection of users.

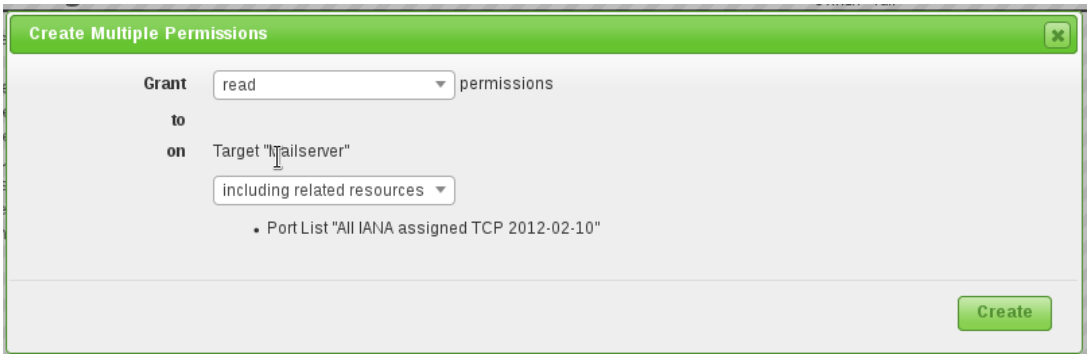


Fig. 8.11: Regular users can not create observers.

For regular users to assign read permission to their tasks to other users they require the permission *get_users* to access the user database. This permission is not granted by default but can be easily added using a special role.

The following steps explain the creation of this special role GrantReadPriv (see figure *The role GrantReadPriv allows to manage read access.* (page 73)). In a second step the role needs to be assigned the permission gos:perm:*get_users*. Every user with this additional role is assigned the permission to read the userdatabase. He then may share read access to their own tasks.

Then, in addition, this role must only be assigned to the respective users.

Note: In case the user is also allowed to share read access to groups or roles the *get_groups* and *get_roles* permissions must be assigned respectively.

8.3 Groups

Aside of the roles group management is also part of the Greenbone Security Assistant. These groups are used to logically group users. Additionally through the groups permissions can be assigned as well (see section *Permissions* (page 73)). By default no groups are set up. Indefinite groups can be created.

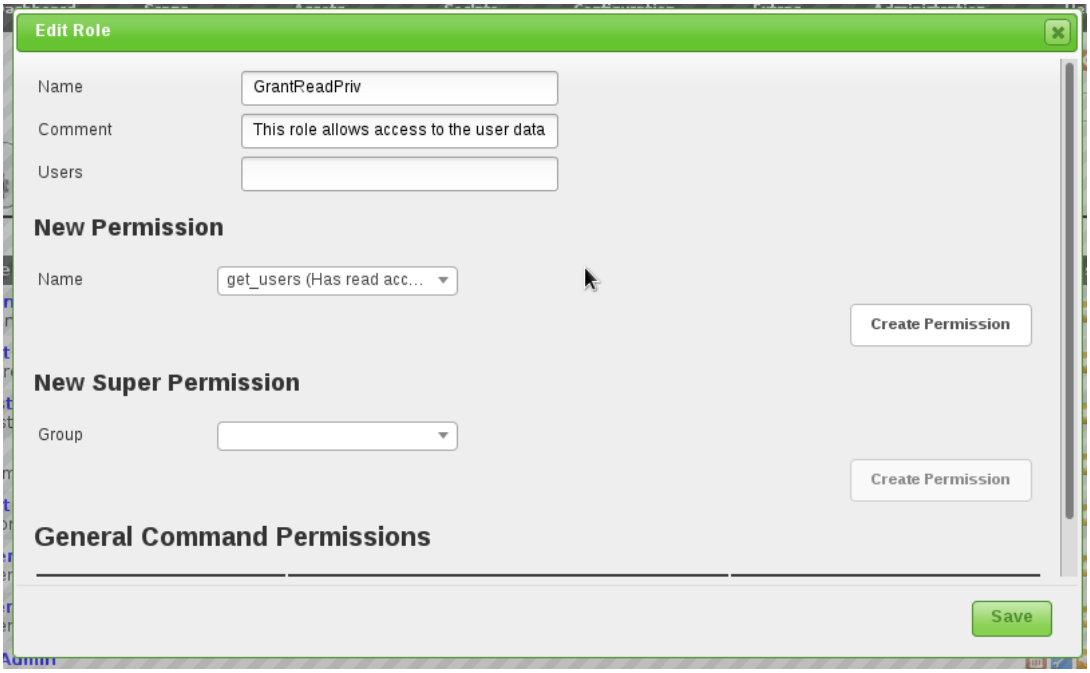


Fig. 8.12: The role GrantReadPriv allows to manage read access.

The following information must be included:

- Name: The name of the Group can be a maximum of 80 characters and can contain letters and numbers.
- Comment: An optional comment that describes the group in more detail.
- Users: The members of the group can be selected directly. The members can be separated by a space or comma. The length of the entry can be a maximum of 1000 characters. Alternatively, group memberships can be managed in the user profile directly.

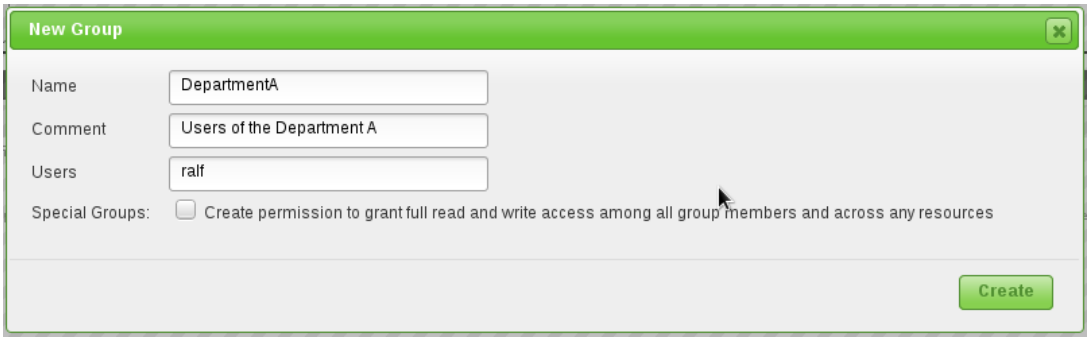


Fig. 8.13: Groups can be used to manage permissions.

8.4 Permissions

Under the menu option *Configuration/Permissions* every single permission assigned on the system can be viewed. This can easily reach hundreds of permissions if multiple roles are created. Each individual permission displayed always relates to exactly one subject.

A subject can be either

- a user

- a role
- or a group.

Normally permissions are being managed using the web interface vie the roles (see section *User Roles* (page 67)). Thereby the permissions of the role can be managed in the role management as well as here. Alternatively permissions can be assigned directly to users and groups.

This option gives you the most possible flexibility when managing permissions. However adding and managing permissions using this dialog is only recommended for experienced users who are looking for a specific permission or who want to delete a specific user, for example.

Note: It is also possible to modify the permissions of the default roles with this dialog. This could have unwanted effects when updating and the permissions are reset again.

8.4.1 Sharing Individual Objects for Other Users

Every user can share indefinite objects created by himself. However, the user must be assigned the permission *get_users*. Otherwise the user will not have permission to determine the name of other users (see section *GetUsers Role for Observers* (page 72)).

To share an object, first determine the Object-ID. Sharing by name is not possible. To acquire the ID display the object that is to be shared in the browser (i.e. a filter). At the top right of the display you can find and copy the ID.

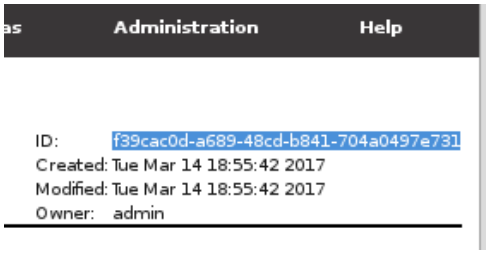


Fig. 8.14: Copying of the ID of an object to be shared.

Afterwards switch into the menu *Configuration/Permissions*. Create a new permission . Then select the proper permission for the object to be shared:

- Filter: *get_filters*
- Scan configuration: *get_configs*
- Alert: *get_alerts*
- Notes: *get_notes*
- Overrides: *get_overrides*
- Tags: *get_tags*
- Targets: *get_targets*
- Task with report: *get_tasks*
- Schedules: *get_schedules*

Select the appropriate subject (user, role or group) and paste the copied Resource ID into the respective field.

Fig. 8.15: Copying of the ID of an object to be shared.

8.5 Central User Management

Especially in larger environments with multiple users it is often difficult to achieve password synchronization. The effort to create new or reset passwords is often very high. To avoid this, the GSM appliance supports the usage of a central password store via LDAP or RADIUS. The GSM will use the service only for authentication on a per user basis. This means that users who should be able to authenticate through the service have to exist on the GSM as well and have to be configured for authentication through the service as well.

Prerequisite for using central authentication is the naming of the users with the same name as the object in the LDAP tree or the RADIUS server.

8.5.1 LDAP

Below the connection to a LDAP tree is covered. Thereby the GSM appliance uses a very simple interface. While other most systems supporting LDAP first search for the matching object in the LDAP tree and subsequently log in as this object afterwards (Search&Bind), the GSM appliance uses a simple bind with a hard coded object path.

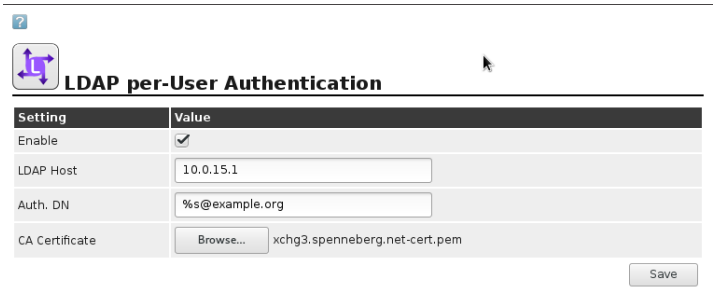


Fig. 8.16: Central LDAP authentication requires entering the DN.

Then the distinguishedName of the objects can be defined distinctively. Thereby the wildcard %s replaces the username. Examples for the *Auth. DN* are:

- `cn=%s,ou=people,dc=domain,dc=de`
- `uid=%s,ou=people,dc=domain,dc=de`
- `%s@domain.de`
- `domain.de\%s`

While the two first examples should work for any LDAP server with the correct attributes, the third and fourth example are typical formats used by Active Directory. Hereby the exact location of the user object is irrelevant.

The first example does not support users in different sub trees or different recursive depths of an LDAP tree. All users that need to log into the GSM must be in the same branch and in the same level of the LDAP tree! The second example uses the *uid* attribute. In this case, *uid=user* will be used as filter, and *ou=people,dc=domain,dc=org* will be used as base object to perform a search and to retrieve the corresponding DN for the authentication. Hereby the *uid* attribute location becomes relevant and should be at the first position.

The other information required is the *LDAP Host*. Only one system with its IP address or name can be entered here. The GSM accesses the LDAP host via SSL. To verify the host the certificate of the host must be uploaded to the GSM. Without SSL the LDAP authentication will not be accepted. Further information is available in the section *LDAP with SSL/TLS* (page 76).

Once you have enabled LDAP authentication, you will notice a new option LDAP Authentication Only in the New User section which will be off by default. Checked it if the new user should be able to login with the credentials configured in the directory service. For existing users you may enable this option through the Edit User dialog.

Please note that the user has to exist with this name in your directory service prior to use with the GSM. The GSM will not add, modify or remove users in your directory service. It will also not grant any user from your directory service automatically access to the GSM. You have to authorize every user separately by adding a user with the same name to the GSM with Allow LDAP-Authentication only checked as described above.

Also note that a locally configured user (i.e. a user which is not enabled for LDAP authentication) “Smith” on the GSM takes precedence over a user “Smith” in the connected directory service.

8.5.2 LDAP with SSL/TLS

The GSM appliance uses either the command StartTLS via the LDAP protocol on port 389 or SSL via LDAPS on port 636. Therefore the LDAP server must make its services available via SSL. The exact configuration of all available LDAP servers is out of scope for this manual. Therefore the following are just a couple of references:

- Microsoft: http://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx
- OpenLDAP: http://www.openldap.org/doc/admin24/tls.html

In order for the GSM appliance to verify the identity of the LDAP server it must trust its certificate. For this the certificate of the issuing certificate authority must be stored on the GSM. To do so the certificate of the certificate authority must be exported as a Base64 encoded file. A Base64 encoded certificate is often using the file extension `.pem`. The file itself starts with `------BEGIN CERTIFICATE-------`.

If the certificate authority is an intermediate certificate authority the complete certificate chain needs to be imported. This is often true if an official certificate authority is used because the Root CA is separated from the Issuing Certificate Authority. In these cases the contents of the file looks like:

```
-----BEGIN CERTIFICATE-----
......
Issuing Certificate Authority
......
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
......
Root CA
......
-----END CERTIFICATE-----
```

The actual place where you may find this certificate may vary based on your environment.

- Univention Corporate Server (UCS)

  Here you may retrieve the CA certificate from the file `/etc/univention/ssl/ucsCA/CAcert.pem`. This file already contains the certificate in the correct format and may be used by the command `ldapcertdownload`.

- Active Directory LDAP

  If your Active Directory LDAP service does not yet use LDAPS, you may find the following article helpful: http://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx The Active Directory LDAP — CA certificates can then be exported using the following procedure which must be performed from a desktop or server that has access to the Certification Authority console.

  - Open the Certification Authority console from any domain-joined computer or server.
  - Right-click the name of the certification authority and then select Properties.
  - In the CA certificates dialog box, choose the General tab, and then select the certificate for the certification authority you want to access.
  - Choose View Certificate.
  - In the Certificate dialog box, choose the Certification Authority tab. Select the name of the root certification authority and then choose View Certificate.
  - In the Certificate dialog box, choose the Details tab and then choose Copy to File.
  - The Certificate Export Wizard appears. Choose Next.
  - On the Export File Format page, select the Base-64 encoded X.509 (.CER) option.
  - Choose Next.
  - In the File to Export box, choose the path and name for the certificate, and then choose Next.
  - Choose Finish. The .cer file will be created in the location that you specified in the previous step.
  - A dialog box appears to inform you that the export was successful. Choose OK to finish.

  The contents of the file must be uploaded when enabling LDAP.

If the LDAP authentication does not work please verify that the entry in *LDAP Host* matches the commonName of the certificate of the LDAP server. If there are deviations the GSM appliance will refuse using the LDAP server.

8.5.3 RADIUS

Using a RADIUS server for central authentication is very simple. Navigate to the *Administration/Radius* menu.

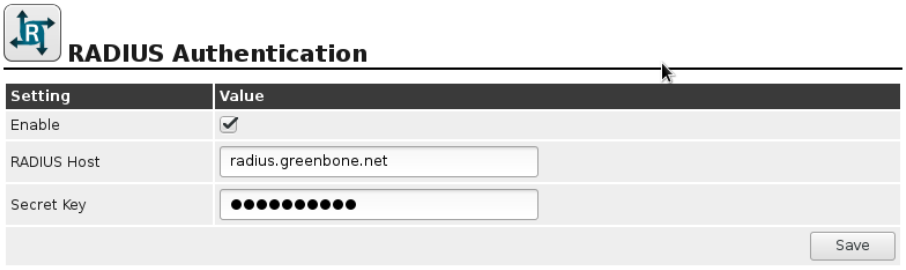


Fig. 8.17: RADIUS just requires a common preshared secret key.

Enable the RADIUS authentication and enter the hostname or IP address of the RADIUS server and the common preshared secret key to authenticate to and subsequently encrypt the communication with the RADIUS service.

Once the RADIUS service is enabled any user can be configured to authenticate via the RADIUS service.

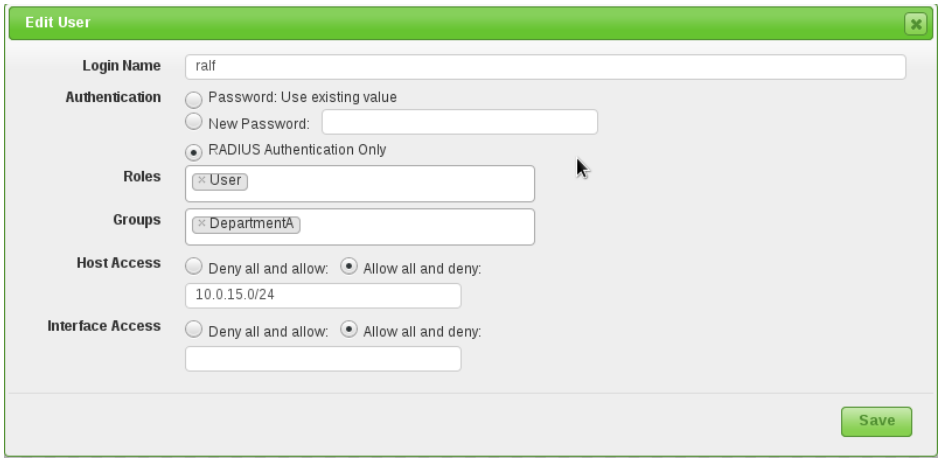


Fig. 8.18: Enable RADIUS for a user

CHAPTER 9

Vulnerability Management

9.1 Scanning

This chapter covers the set up and execution of the actual scans of your systems for vulnerability management. The chapter describes basic first steps. Later sections show the more detailed use and configuration of scan configurations and the analysis of the results.

Generally speaking the GSM may use two different approaches to scan a target:

- Remote Scan
- Authenticated Scan using local security checks

The remote scan is explained in the following sections while the authorized scan is handled in section *Authenticated Scan using Local Security Checks* (page 91). This chapter also covers the differences and advantages of both scan approaches (see section *Pros and Cons of Authenticated Scans* (page 92)).

9.1.1 Simple Scan

This first section describes the first steps of the configuration of the first scan. Basically two options are available. The web interface of the GSM appliance, the Greenbone Security Assistant, provides a wizard that creates all required configurations for a first scan with only very little input. Alternatively these configurations can be created manually step by step. The following two sections cover both options. Ideally the individual steps should be followed directly on a GSM appliance.

 These steps are also explained in a video based on GOS 3.1 at http://docs.greenbone.net/Videos/gos-3.1/en/GSM-FirstScan-GOS-3.1-en-20150716.mp4.

Wizard

When logging into the web interface of the GSM appliance for the first time after initial set up the empty dashboard will be displayed.

To configure a new task the admin has to select the menu *Scans* followed by *Tasks*. To ease the setup of the tasks an overlay promoting the wizard will be displayed.

By default, this will happen as long as less than four scan tasks were created. The wizard can be started at any time by clicking the  icon in the upper left corner on the screen. Three different options are available:

- Task Wizard
- Advanced Task Wizard
- Modify Task Wizard

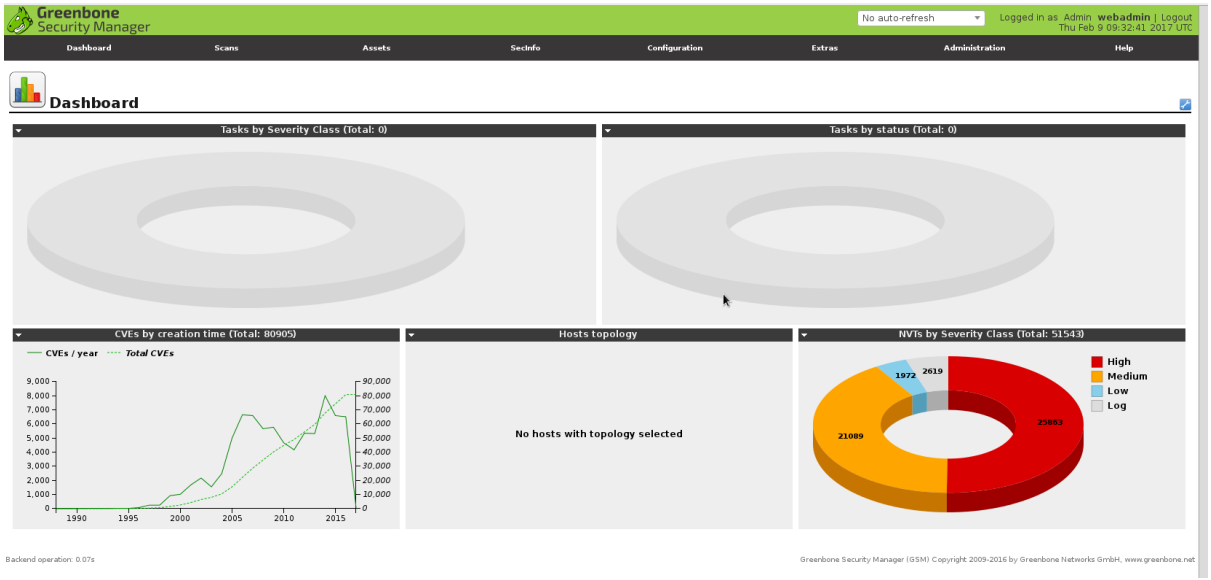


Fig. 9.1: The dashboard is displayed first by default

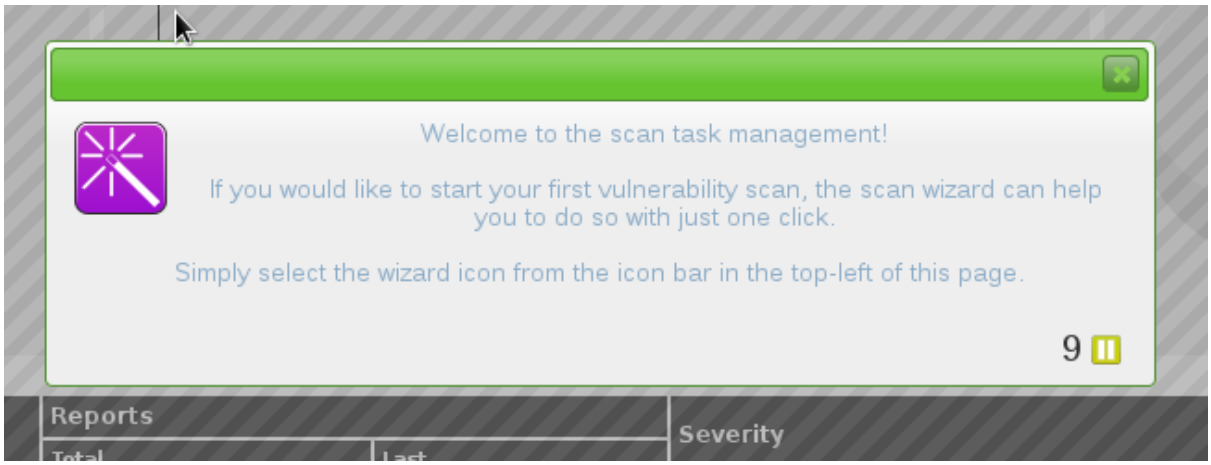


Fig. 9.2: The wizard is promoted using an overlay

To scan a simple system using the wizard first select the *Task Wizard*. For an immediate scan it is enough to enter the IP address or DNS name of the target system. When using a DNS name however, the GSM appliance must be able to resolve the name.

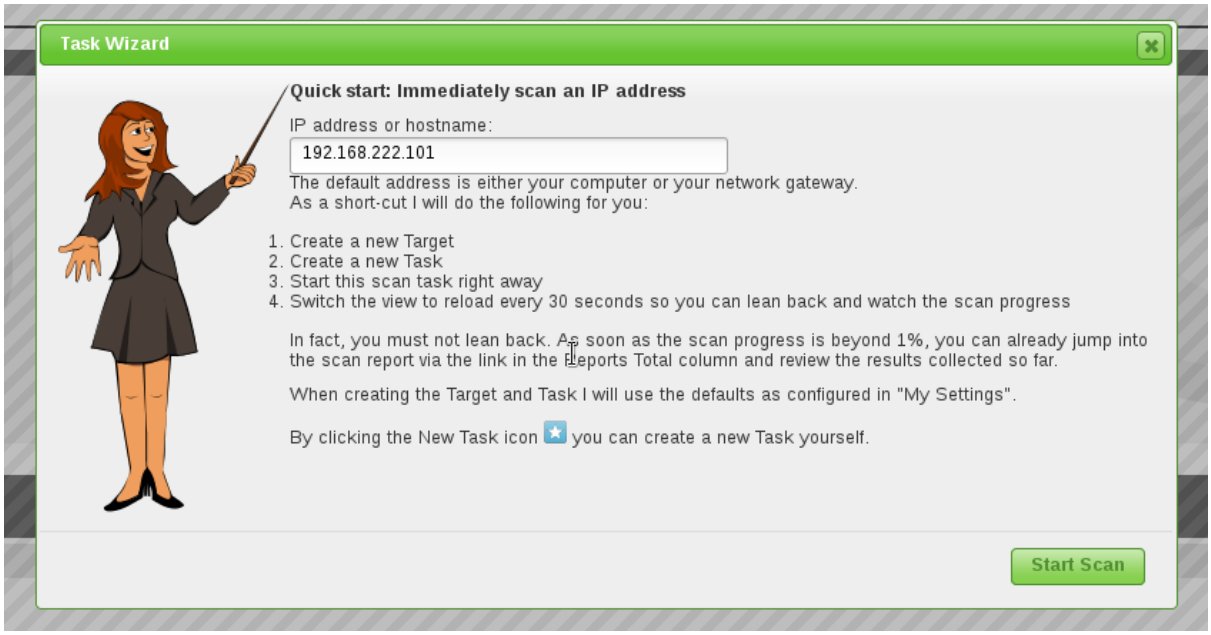


Fig. 9.3: The task wizard simplifies the first steps

The task wizard then automatically performs the following steps:

1. Creates a new scan target (Target) in the GSM.
2. Creates a new scan task (Task) in the GSM.
3. Starts the scan task immediately.
4. Changes the view and reloads it every 30 seconds in order to monitor the progress of the task.

After the task is started the progress can be monitored. The Greenbone Security Assistant displays the overview page. The new task can be seen there as well.

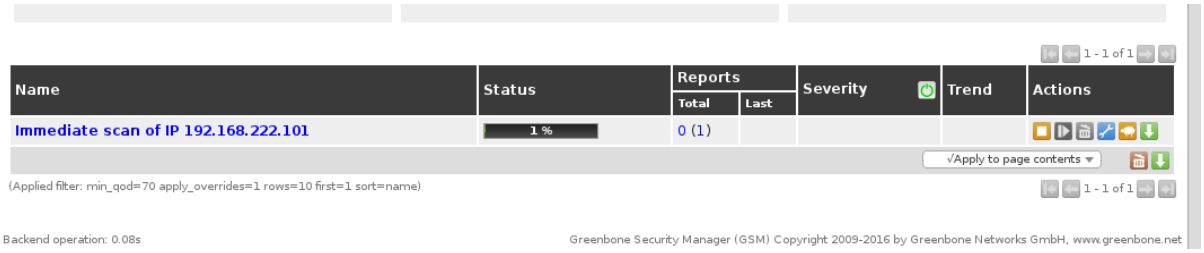


Fig. 9.4: After the start the progress is being displayed.

The colour and the fill level of the status bar display the state of the scan (see also section *Starting a Task* (page 90)).

The task can be managed via the actions in the right column:

- Starting of a currently not running task.
- Stopping of a currently running task. All discovered results will be written to the database.
- Resuming of a stopped task.
- Moving of a task to the trashcan.

- Editing of a task.
- Cloning of a task.
- Exporting of a task as XML object. The object can be imported again on another GSM.

During the scan and after its completion the admin can view the report by clicking the progress bar. The column Severity displays the criticality of any vulnerabilities found. The prior column Solution Type shows the type of any solution available. Usually the most common solution is the VendorFix .

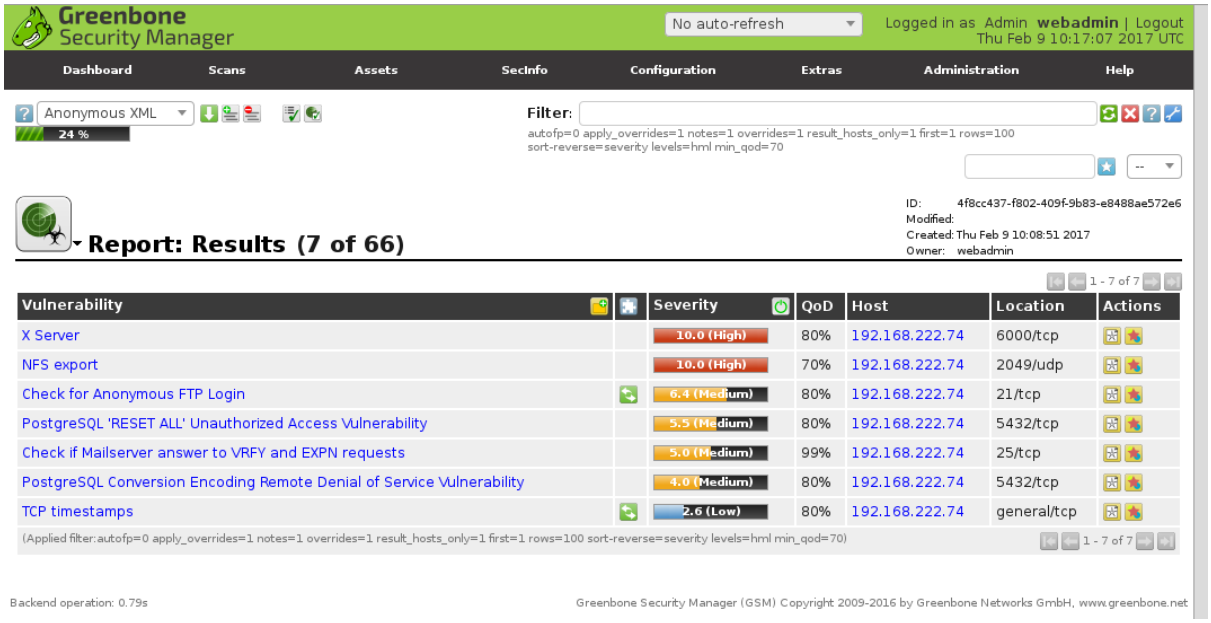


Fig. 9.5: The results are already available before the scan is completed.

The progress can be continued to be monitored at the top right via the progress bar. This page, however, is not reloaded automatically.

In order to obtain different representations of the results, you can move the mouse over the title bar. It opens a pull-down menu where you can choose different presentations of the results.

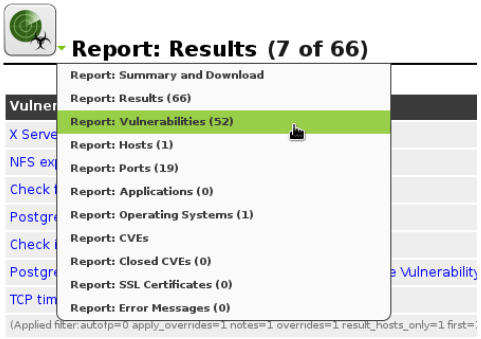


Fig. 9.6: Furthermore a report can be displayed using different presentations

Furthermore the report can be exported in various different formats as well. The export formats are selected in the in the right column on the Summary and Download view. Afterwards the report can be downloaded by clicking the button. Reports and report formats are discussed in more detail in section *Reports and Vulnerability Management* (page 124).

Advanced Wizard

Next to the simple wizard the GSM also provides an advanced wizard that allows for more configuration options. This wizard allows for shortcutting the manual configuration of the individual parameters and still allows for a more granular configuration.

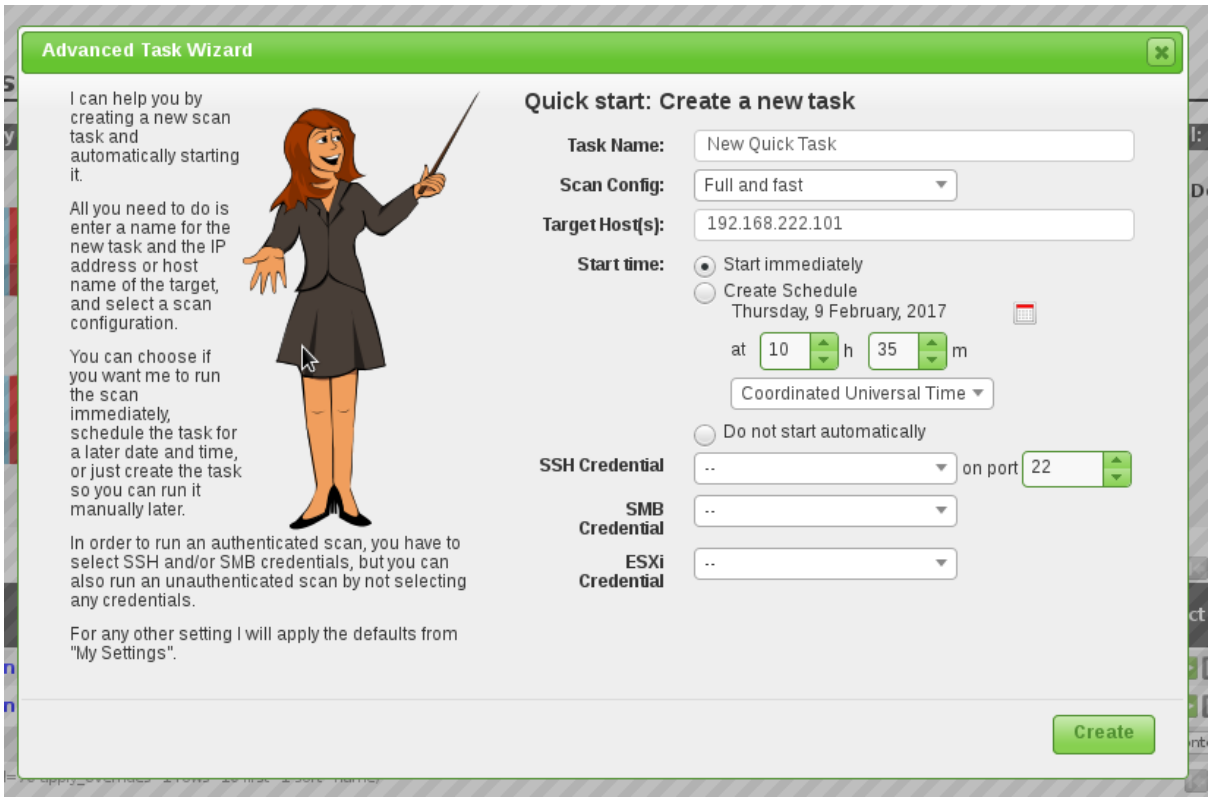


Fig. 9.7: The advanced wizard offers more options.

This wizard can be started by clicking on the wizard icon in the upper left corner of the task view.

An additional wizard allows the modification of a task (Modify Task Wizard). The task may be renamed and scheduled.

Manual Configuration

The upcoming section covers the creation of a simple scan with its individual steps that the wizard performs as well. This way meaningful names may be selected for both the scan targets (Targets) and the scan task (Task).

These steps are also explained in a video based on GOS 3.1 at http://docs.greenbone.net/Videos/gos-3.1/en/GSM-FirstScan-GOS-3.1-en-20150716.mp4.

Creating a Target

The first step is to define a scan target. This is called Target by the Greenbone Security Assistant.

First chose one or more systems in your network you want to scan. The IP address or the DNS name is required. In both cases it is necessary that the GSM can connect to the system. When using the DNS name the GSM appliance must also be able to resolve the name.

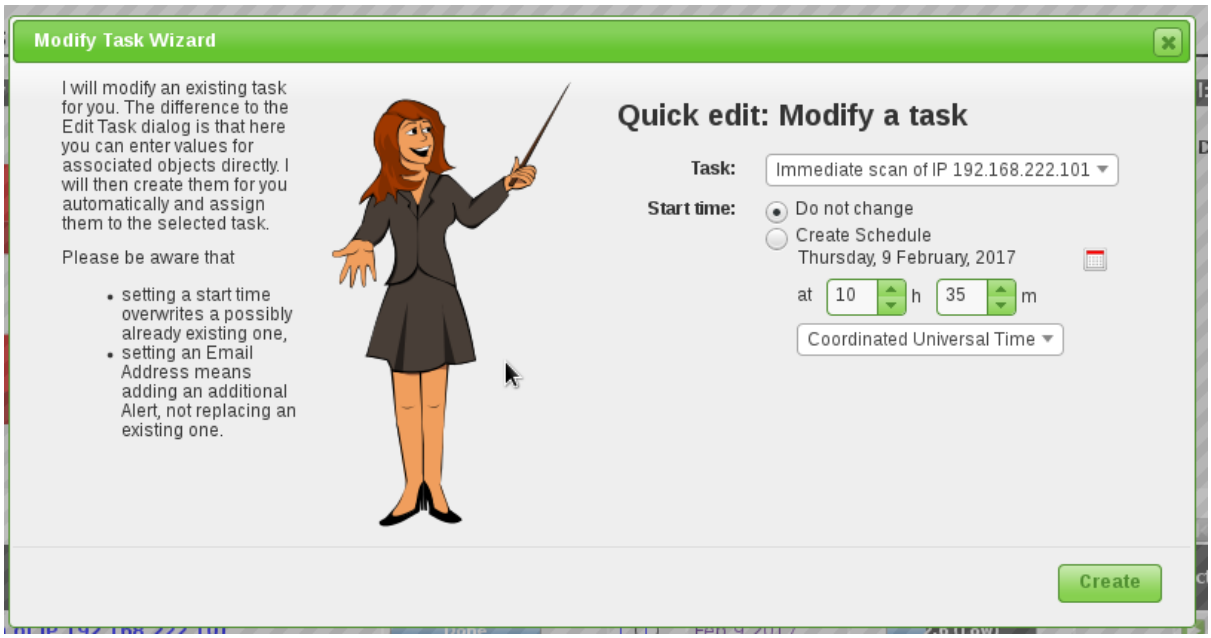


Fig. 9.8: The wizard may be used to schedule an existing task

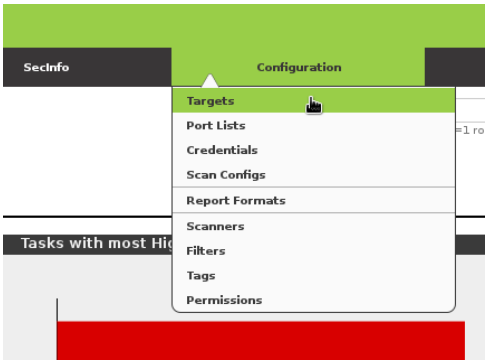


Fig. 9.9: Selecting the target menu.

Fig. 9.10: Creating a new target.

Choose *Targets* from the menu *Configuration*. Select the *New Target* icon (the white star on blue background:) in the upper left corner. This icon is always used to represent the creation of a new object within its respective context.

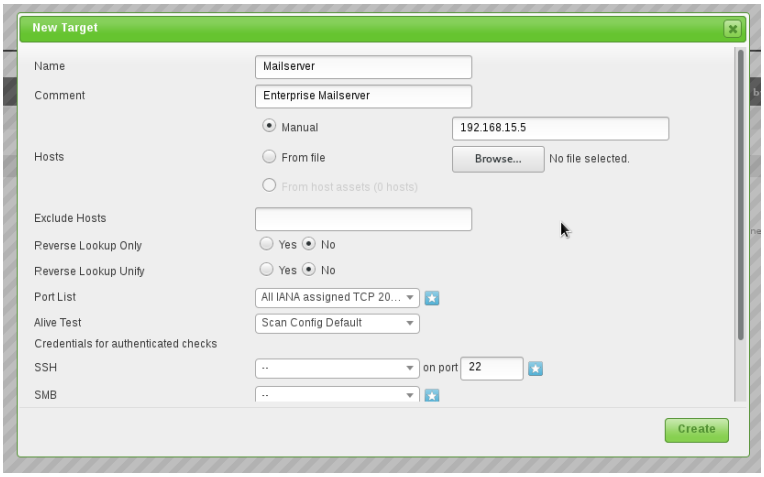


Fig. 9.11: Enter the details for the target.

A new overlay, in which the target can be configured in more detail, will open.

Enter the following information:

- Name The name can be freely chosen. A descriptive name should be chosen if possible. Possibilities are Mailserver, ClientNetwork, Webserverfarm, DMZ or the like, describing the entered systems in more detail.
- **Comment** The optional comment allows to specify background information. It simplifies understanding the configured targets later.
- **Hosts** Manual entry of the system or importing of a list of systems. When entering manually the following options are available:
  - Single IP address, i.e. 192.168.15.5
  - System name, i.e. mail.example.com
  - IPv4 address range, i.e. 192.168.15.5-192.168.15.27 or 192.168.55.5-27
  - IPv4 network in CIDR notation, i.e. 192.168.15.0/24 [5]
  - Single IPv6 address
  - IPv6 address range in long format, i.e. ::12:fe5:fb50-::12:fe6:100
  - IPv6 address range in short format, i.e. ::13:fe5:fb50-fb80
  - IPv6 address range in CIDR notation, i.e. fe80::222:64ff:fe76:4cea/120
  - multiple entries can be entered separated with commas

  When importing from a file the same syntax can be used. The entries can be stored in the file on multiple lines. When using long lists of systems to be scanned this way is usually the simpler one.

  Alternatively the systems may be imported from the host asset database.
- **Exclude Hosts** Systems that should be excluded from the lists mentioned above.
- **Reverse Lookup Only** Only scan IP addresses that can be resolved into a DNS name.
- **Reverse Lookup Unify** If multiple IP addresses resolve to the same DNS name the DNS name will only get scanned once.

[5] The maximum netmask is /20. This equals 4096 addresses.

- **Port list** The TCP and UDP protocols support 65535 ports respectively. Scanning all ports in many cases takes too long. Many ports are usually not used. A manufacturer developing a new application often reserves the respective port with the IANA (Internet Assigned Numbers Association). For most scans it is often enough to scan the ports registered with the IANA. But keep in mind that the registered ports differentiate from the privileged ports. Privileged ports are ports smaller than 1024 [6]. But the ports 1433/tcp (MS-SQL) and 3306/tcp (MySQL) are also registered and included in the appropriate lists. Nmap by default uses a different list and doesn't check all ports either. OpenVAS uses a different default as well.

  The scan of TCP ports is usually performed simply and fast. Operating system without firewall features always reply to a TCP request and as such advertise a port as being open (TCP-ACK) or closed (TCP-RST). With UDP this is not the case. The operating system only responds reliably when the port is closed (ICMP-Port-Unreachable). An open port is deducted by the scanner by a missing response. Therefore the scanner has to wait for an internal timeout. This behaviour is only true for systems not protected by a firewall. When a firewall exists the discovery of open or closed ports is much more difficult.

  If applications run on unusual ports and they should be monitored and tested with the GSM, the default port lists should be verified and adapted using *Configuration* submenu *Port Lists*. If necessary create your own list that includes your port. A new port list may be directly created using the icon  . The default port lists can not be modified.

- **Alive Test** This options specifies the method to check if a target (Targets) is reachable. Options are:
  - ICMP Ping
  - TCP Service Ping
  - ARP Ping
  - ICMP & TCP Service Ping
  - ICMP & ARP Ping
  - TCP Service & ARP Ping
  - ICMP, TCP Service & ARP Ping

In the real world there are problems with this test from time to time. In some environments routers and firewall systems respond to a TCP Service Ping with a TCP-RST even though the host is actually not alive (see also *Obstacles while Scanning* (page 119)).

Network components exist that support Proxy-ARP and respond to an ARP-Ping. Therefore this test often requires local customization to your environment.

- **SSH Credential** Selection of a user that can log into the target system of a scan if it is a Linux or UNIX system. This allows for an *Authenticated Scan* using local security checks (see section *Credentials* (page 92) and *Authenticated Scan using Local Security Checks* (page 91)).
- **SMB Credential** Selection of a user that can log into the target system of a scan if it is a Microsoft Windows system. This allows for an *Authenticated Scan* using local security checks (see section *Credentials* (page 92) and *Authenticated Scan using Local Security Checks* (page 91)).
- **ESXi Credential** Selection of a user that can log into the target system of a scan if it is a VMWare ESXi system. This allows for an *Authenticated Scan* using local security checks (see section *Credentials* (page 92) and *Authenticated Scan using Local Security Checks* (page 91)).
- **SNMP Credential** Selection of a user that can log into the target system of a scan if it is a SNMP aware system. This allows for an *Authenticated Scan* using local security checks (see section *Credentials* (page 92) and *Authenticated Scan using Local Security Checks* (page 91)).

[6] In UNIX access to these privileged ports is only allowed for privileged users (i.e. root). Ports starting at 1024 are also available to unprivileged users.

All credentials can be created on the fly using the icon next to the credential.

Creating a Task

The GSM controls the execution of a scan using Tasks. These tasks can be repeated regularly or run at specific times. The scheduling is discussed in more detail in section *Scheduled Scan* (page 120). For now the basic creation of a task is covered in this section.

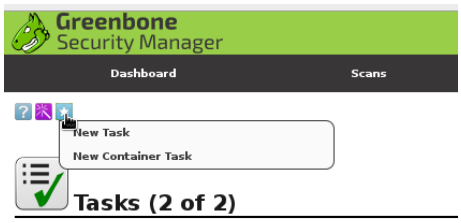


Fig. 9.12: Creation of tasks.

To access the tasks select menu option *Scans* from the menu bar. From there select the *Tasks*. On the following page select the white star on blue background to choose *New Task* to create a new task. An overlay opens which can be used to configure the additional options of the task.

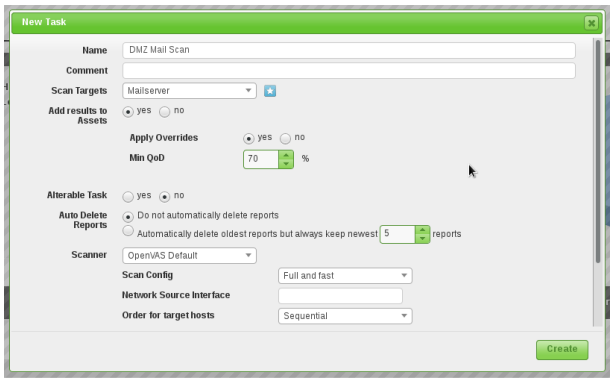


Fig. 9.13: Creation of a new task.

The following information can be entered:

- **Name** The name can be chosen freely. A descriptive name should be used if possible. Possibilities to describe the entered task are *Scan Mailserver*, *Test ClientNetwork*, *Check DMZ for new ports and systems* or the like.
- **Comment** The optional comment allows for the entry of background information. It simplifies understanding the configured task later.
- **Scan Targets** Select a previously configured Target from the drop down menu. Additionally you can create the target on the fly using the icon next to the drop down list.
- **Alerts** Select a previously configured Alert. Status changes of a task can be communicated to the world via email, Syslog, HTTP or a connector. Additionally you can create an alert on the fly using the icon next to the drop down list.
- **Schedule** Select a previously configured Schedule. The task can be run once or repeatedly at a predetermined time. It is possible to scan the network every Monday morning at 6:00 am for example. You can create the schedule on the fly using the icon next to the drop down list.

- **Add results to Asset Management** Selecting this option will make the systems available to the Asset Management of the GSM automatically (see chapter *Asset Management* (page 133)). This selection can be changed at a later point as well.
  - **Apply Overrides** Overrides may be directly applied when adding the results to the asset database.
  - **Min QoD** Here the minimum quality of detection can be specified for the addition of the results to the asset database.
- **Alterable Task** Allow for modification of the task even though reports were already created. The consistency between reports can no longer be guaranteed if tasks are altered.
- **Auto Delete Reports** This option may automatically delete old reports. The maximum number of reports to store can be configured. If the maximum is violated the oldest report is automatically deleted. The factory setting is `Do not automatically delete reports`.
- Scanner
  - **OpenVAS Scanner** By default only the built-in OpenVAS and the CVE scanning engines are supported. Satellite GSM formerly known as slaves or sensors may be used as additional scanning engines. These need to be configured first using the *Configuration/Scanners* menu. The following options are only relevant for the OpenVAS scanning engine. The CVE scanner does not support any options.
  - **Scan Config** The GSM comes by default with seven pre-configured scan configurations for the OpenVAS scanner.
    - **Discovery** Only NVTs are used that provide the most possible information of the target system. No vulnerabilities are being detected.
    - **Host Discovery** Only NVTs are used that discover target systems. This scan only reports the list of systems discovered.
    - **System Discovery** Only NVTs are used that discover target systems including installed operating systems and hardware in use.
    - **Full and Fast** This is the default and for many environments the best option to start with. This configuration is based on the information gathered in the prior port scan and uses almost all NVTs. Only NVTs are used that will not damage the target system. Plugins are optimized in the best possible way to keep the potential false negative rate especially low. The other configurations only provide more value only in rare cases but with much more required effort.
    - **Full and fast ultimate** This configuration expands the first configuration with NVTs that could disrupt services or systems or even cause shut downs.
    - **Full and very deep** This configuration differs from the **Full and Fast** configuration in the results of the port scan not having an impact on the selection of the NVTs. Therefore NVTs will be used that will have to wait for a timeout. This scan is very slow.
    - **Full and very deep ultimate** This configuration adds the dangerous NVTs that could cause possible service or system disruptions to the **Full and very deep** configuration.
  - **Network Source Interface** Here you can choose the source interface of the GSM for the scan.
  - **Order for target hosts** Select how the specified network area should be searched. Options available are:
    - Sequential
    - Random
    - Reverse

This is interesting if for example a network, i.e. 192.168.0.0/24, is being scanned that has lots of systems at the beginning or end of the IP address range. With the selection of the `Random` mode the progress view is more meaningful.

– **Maximum concurrently executed NVTs per host / Maximum concurrently scanned hosts**
Select the speed of the scan on one host. The default values are chosen sensibly. If more NVTs run simultaneously on a system or more systems are scanned at the same time, the scan might have a negative impact on either the performance of the scanned systems, the network or the GSM appliance itself. These values maxhosts and maxchecks may be tweaked.

Permissions

Once the task is saved it will be displayed in the list of scans (see figure *A newly created task.* (page 90)).

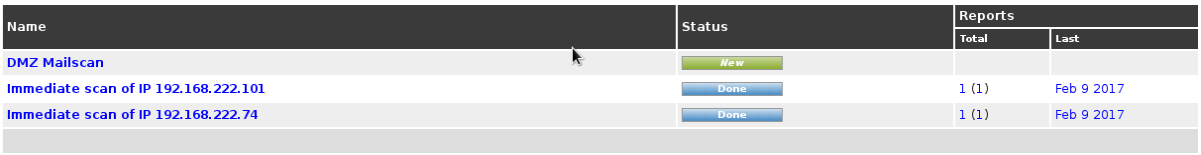


Fig. 9.14: A new task once it is created.

Selecting the name of the task using the mouse displays the details of the task. At the bottom of the page the permissions for the task can be managed. To add a permission click the icon in the *Permissions* title line.

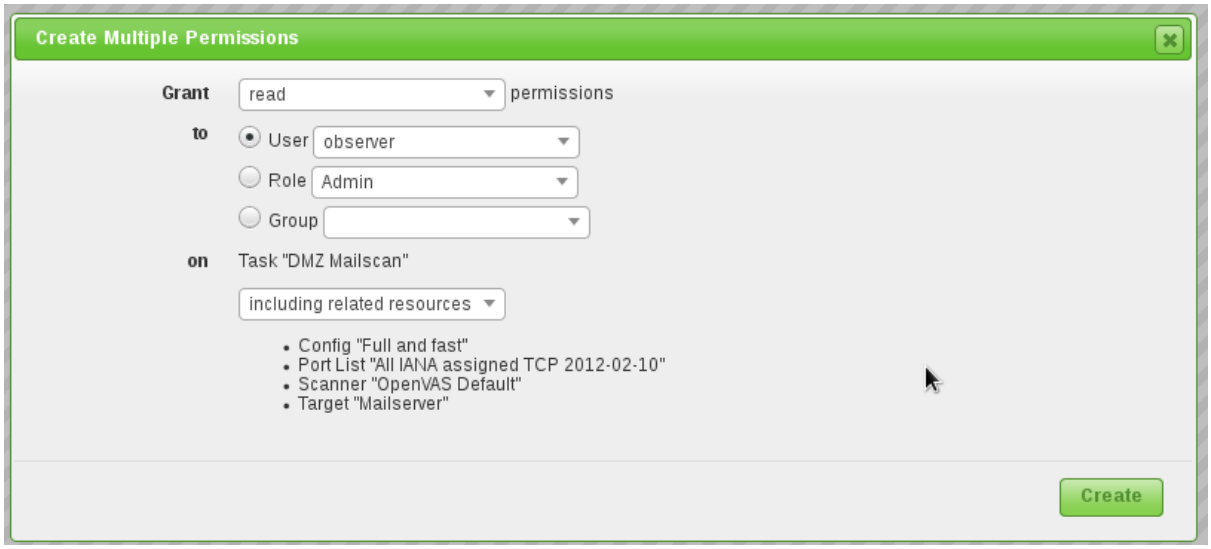


Fig. 9.15: Read permissions can be managed directly in the task.

Note: By default normal users can not create permissions for other users as they do not have read permission to the user database. To do this a user must specifically have the *get_users* permission. It makes most sense to create an additional role (see section *GetUsers Role for Observers* (page 72)).

Select *User*, *Group* or *Role* respectively and enter the respective name. After clicking on *Create* the permissions are created.

This is now displayed in the task overview.

Fig. 9.16: The read permissions of a task are displayed in the overview.

After logging in the user can see those tasks and can access the respective reports.

This is now displayed in the task overview.

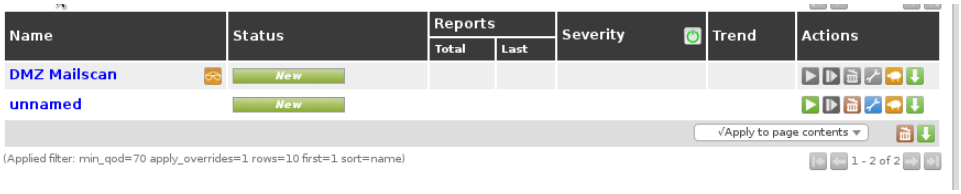


Fig. 9.17: After logging in the observer can view the tasks but cannot change them.

Starting a Task

Once a task is saved it will in the list of tasks (see figure *A newly created task.* (page 90)).

Fig. 9.18: A newly created task.

The task can be managed via the action icons in the right column:

- Starting of a currently not running task.
- Stopping of a currently running task. All discovered results will be written to the database.
- Resuming of a stopped task.
- Moving of a task to the trashcan.
- Editing of a task.
- Cloning of a task.
- Exporting of a task as XML object.

The status bar shows information about the status of a scan. The following colours and states are possible:

- New The task has not been run since it was created.

- 42 % The task is currently running and 42% completed. The information is based on the number of NVTs executed on the selected hosts. For this reason the information does not necessarily correlate with the time spent.
- Requested The task was just started. The GSM is preparing the scan.
- Delete Requested The task was deleted. The actual deletion process can take some time as reports need to be deleted as well.
- Stop Requested The task was stopped recently. However, the scan engine has not reacted respectively yet.
- Stopped at 15 % The last scan was stopped by the user at 15%. The latest report is possibly not yet complete. Other reasons for this status could be the reboot of the GSM or a power outage. After restarting the scanner the task will be resumed automatically.
- Internal Error An error has occurred. The latest report is possibly not yet complete or is missing completely.
- Done The task has been completed successfully.
- Container The task is a container task.

Container Task

A Container Task can be used to import and provide reports created on other GSMs. To create a container task use the icon in the top left corner and choose *New Container Task*. When creating the *Container Task* only the name and a comment may be specified. Afterwards reports may be imported. If several reports are imported they may be compared creating a delta report as well.

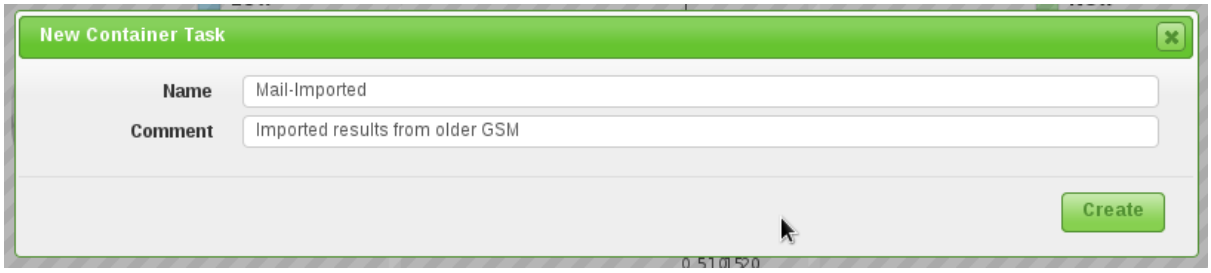


Fig. 9.19: Container tasks are used to import external reports.

The reports need to be in the GSM XML report format.

9.1.2 Authenticated Scan using Local Security Checks

An authenticated scan may provide more vulnerability details on the scanned system. During an authenticated scan the target is both scanned from the outside via the network and from the inside via a valid user login.

During an authenticated scan the GSM logs in to the target system in order to run these local security checks (LSC). The scan therefore requires the prior setup of user credentials. These credentials are used to authenticate to different services on the target system. In some circumstances the results could be limited by the permissions of the users used.

The NVTs in the corresponding NVT families (local security checks) will only be executed if the GSM was able to log in to the target system. The local security check NVTs in the resulting scan are minimally invasive.

The GSM only determines the risk level but does not introduce any changes on the target system. However the login by the GSM is probably being logged in the protocols of the target system.

The GSM can use different credentials based on the nature of the target. However, the most important ones are:

- **SMB** On Windows systems the GSM can check the patch level and locally installed software such as Adobe Acrobat Reader or the Java suite.
- **SSH** This access is used to check the patch level on UNIX and Linux systems.
- **ESXi** This access is used for testing of VMWare ESXi servers locally.
- **SNMP** Network components like routers and switches may be tested via SNMP.

Pros and Cons of Authenticated Scans

The extent and success of the testing routines for authenticated scans depend heavily on the permissions of the account used. On Linux systems an unprivileged user is sufficient and may access most interesting information while especially on Windows systems unprivileged users are very restricted and administrative users provide more results. An unprivileged user does not have access to the Windows registry, the Windows system folder `\windows`, which contains the information on updates and patchlevels, etc.

Local security checks are the most gentle method to scan for vulnerability details. While remote security checks try to be least invasive as well, they might have some impact.

Simply stated an authenticated scan is similar to a Whitebox approach. The GSM has access to prior information and may access the target from within. Especially the registry, software versions and patchlevel are accessible.

A remote scan is similar to a Blackbox approach. Here the GSM uses the same techniques and protocols as a potential attacker to access the target from the outside. The only information available was collected by the GSM itself. During the test the GSM may provoke malfunctions to extract any available information on the used software. The scanner might for example send a malformed request to a service to trigger a response containing further information on the deployed product.

During a remote scan using the scan configuration `Full and Fast` all remote checks are safe. The used NVTs might have some invasive components but none of the used NVTs try to trigger a defect of malfunction in the target (see example below). This is ensured by the scan preference `safe_checks=yes` in the scan configuration. All NVTs with very invasive components or which might trigger a denial of service (DoS) are automatically excluded from the test.

Example of an invasive NVT

An example for an invasive but save NVT is the Heartbleed NVT. This is executed even with `safe_checks` enabled because the NVT does not have any negative impact on the target. But the NVT is still invasive because it does test the memory leakage of the target. If the target is vulnerable actual memory of the target is leaked. The GSM does not evaluate the leaked information but just the fact that the memory was leaked. The information is immediately discarded.

Credentials

To access the credentials select the submenu *Credentials* from the *Configuration* menu. To create new credentials use the  icon in th upper left corner. An overlay is displayed where the following information can be entered:

- **Name** An arbitrary name for the credentials.
- **Comment** A freely selectable comment.
- **Type** The following types may be chosen:
  - Username + Password

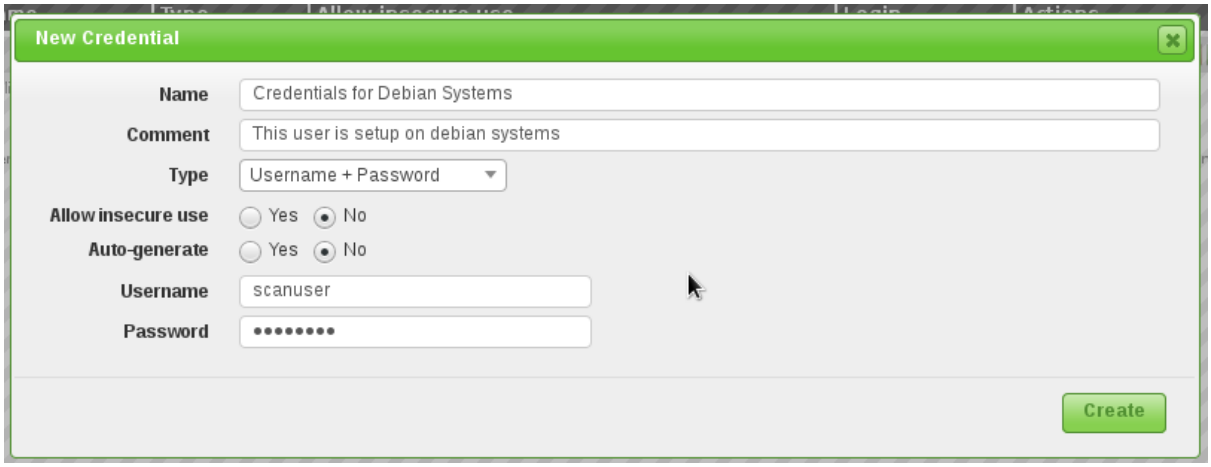


Fig. 9.20: SSH keys can be utilized with credentials as well.

  - Username + SSH Key
  - Client Certificate
  - SNMP

- **Allow insecure use** The GSM will only use the credentials using encrypted protocols by default.
- **Autogenerate Credentials** The GSM itself is creating a random password.
- **Username** The login name used by the GSM to authenticate on the scanned target system.
- **Password** The password can be entered.

Depending on the Type further options might be shown:

- SSH
  - **Private Key** If authentication is performed via SSH the private key can be uploaded.
  - **Passphrase** If required the passphrase of the private ssh key can be entered.
- Client Certificate
  - **Certificate** If authentication is performed via a client certificate the certificate file may be uploaded.
  - **Private Key** The corresponding private key can be uploaded.
- SNMP
  - **SNMP Community** If the protocols SNMPv1 or SNMPv2c are used the community can be entered.
  - **Username** For SNMPv3 the username may be specified.
  - **Password** For SNMPv3 the password may be specified.
  - **Privacy password** For SNMPv3 the password for the encryption may be specified.
  - **Auth algorithm** The authentication algorithm may be chosen. Supported are either MD5 or SHA1.
  - **Privacy algorithm** The encryption algorithm may be chosen. Supported are AES128, DES or none.

Autogenerate Credentials

To simplify the installation and creation of accounts for authenticated scans the GSM option *Autogenerate Credential* offers an install package for the respective target system. This package creates the user and the most important permissions for the authenticated scan and re-sets them again during uninstallation.

The install package is provided for:

- Debian based systems
- RPM based systems
- Windows
- Public Key

Requirements on Target Systems with Windows

General notes on configuration

- The remote registry service must be started in order to access the registry

  You can achieve this by configuring the service to automatically start up. If you do not prefer the automatic start, you could configure manual start up. In that case the service will be started while the system is scanned by GSM and afterwards it will be disabled again. To ensure this behaviour the following item about LocalAccountTokenFilterPolicy must be considered.

- It is necessary that for all scanned systems the file and printer sharing is activated. When using Windows XP, take care to disable the setting "Use Simple File Sharing".

- For individual systems not attached to a domain the following registry key must be set:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\
DWORD: LocalAccountTokenFilterPolicy = 1
```

- On systems with domain controller the user account in use must be a member of the group **Domain Administrators** to achieve the best possible results. Due to the permission concept it is not possible to discover all vulnerabilities using the **Local Administrator** or the administrators assigned by the domain. Alternatively follow the instructions below under *Configuring a domain account for authenticated scans* (page 95).

- Should a **Local Administrator** be selected – which we explicitly do not recommend – it is mandatory to set the following registry key as well:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\
DWORD: LocalAccountTokenFilterPolicy = 1
```

- Generated install package for credentials: The installer sets the `Remote Registry` service to auto start. If the installer is executed on a Domain Controller the user account will be assigned to the Group **BUILTIN/Administrators** (`SID S-1-5-32-544`).

- An exception rule for the GSM on the Windows firewall must be created. Additionally on XP systems the **File and Printer Sharing** must be set to `enabled`.

- Generated install package for credentials: During the installation the installer offers a dialog to enter the IP address of the GSM. If the entry is confirmed the firewall rule is configured. The **File and Printer Sharing** service will be enabled in the firewall rules.

Configuring a domain account for authenticated scans

In order to use a domain account for host based remote audits on a windows target this must be performed under Windows XP Professional, Windows Vista, Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 7, Windows 8, Windows 8.1 or Windows 10 and also be part of a domain.

Taking security into consideration the following eight steps should be implemented to create these scans.

Step 1: Create a security group First create a security group called `Greenbone Local Scan`:

- Log into a domain controller and open `Active Directory Users and Computers`.
- Now create the security group in the menu. Select *Action* > *New* > *Group*.
- Call the group `Greenbone Local Scan`. It is important that the Global is selected for the Group Scope and Security as the Group Type.
- Add the account, that is being used for the local authenticated scans under Windows by the Greenbone Appliance, to the group `Greenbone Local Scan`.

Step 2: Create a Group Policy Now create a group policy with called `Greenbone Local SecRights`.

- Open the Group Policy Management console.
- Right click on Group Policy Objects and select New.
- Enter `Greenbone Local SecRights` as the name of the policy.

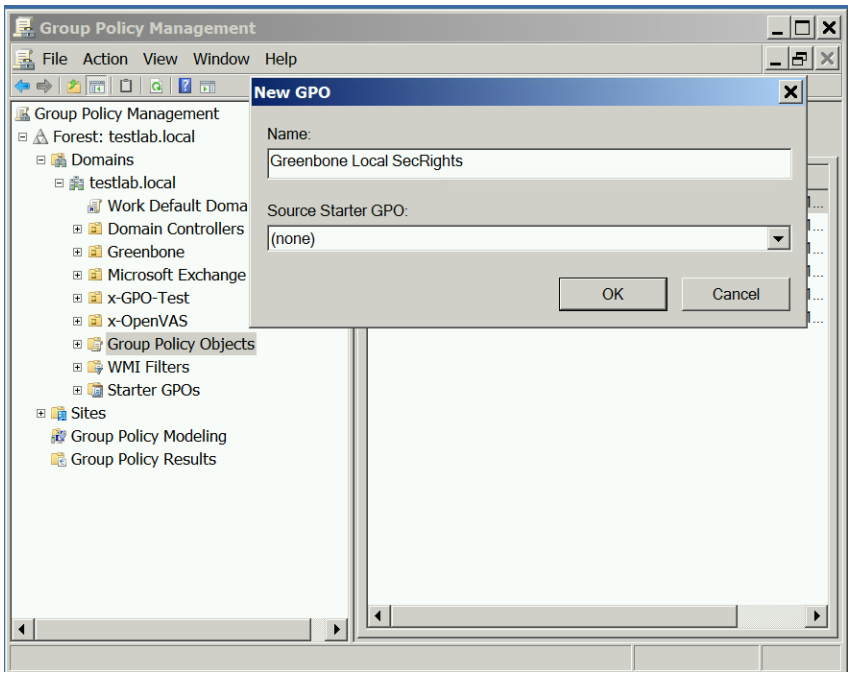


Fig. 9.21: A new Windows Group Policy Object for Greenbone scans.

Step 3: Configuration of the Policy Add the group `Greenbone Local Scan` to the `Greenbone Local SecRights` policy and insert local administrators to the groups.

Please note that this setting still exists after the GPO has been removed (*Tattooing GPO*). This changes fundamental privileges which might not be simply reversed by removing the GPO. Please research first whether these settings are compatible with your environement!

- Click on the policy `Greenbone Local SecRights` and select `Edit`.
- Open:

```
Computer Configuration\Policies\Windows Settings\
Security Settings\Restricted Groups
```

- In the left pane right click on Restricted Groups and select `Add Group`
- Now select `Browse` in the `Add Group` dialog, enter `Greenbone Local Scan`, afterwards click `Check Names`.

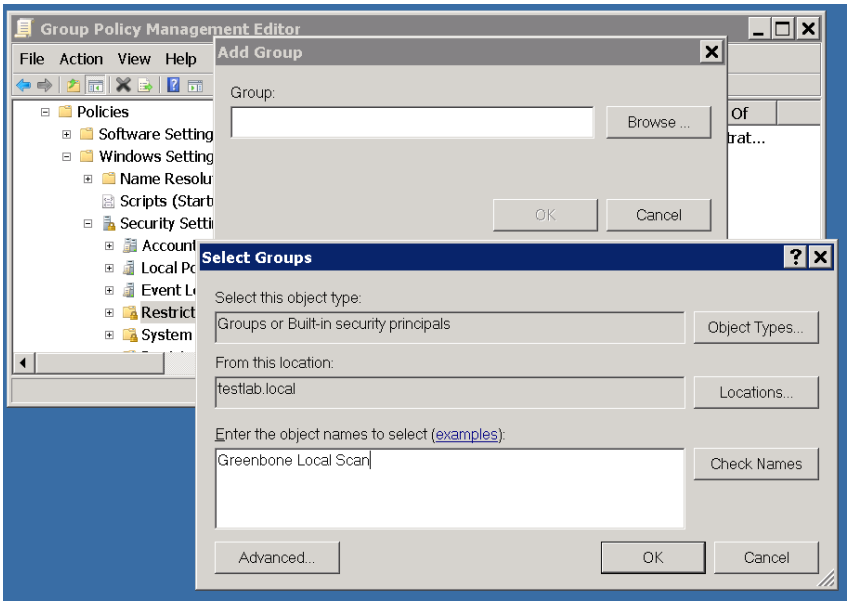


Fig. 9.22: Check Windows Group Name.

- Click OK twice to close the opened dialog.
- Under `This group is member of:` click on `Add`.
- Add the group `Administrators`. Additionally on non-English systems enter the respective name of the local administrator group.
- Click OK twice.

Step 4: Configuration of the policy, to deny local log on systems of the `Greenbone Local Scan` group

Add the `Greenbone Local Scan` to the `Greenbone Local SecRights` group and deny the local log in of group members.

- Click on the `Greenbone Local SecRights` and then select `Edit`.
- Open:

```
Computer Configuration\Policies\Windows Settings\Security Settings\
Local Policies\User Rights Assignment
```

- In the right pane double click on `Deny log on locally`
- Set the checkmark in `Define these policy settings:`
- Click on `Add User or Group`
- Now select `Browse`, enter `Greenbone Local Scan` and then click on `Check Names`.
- Now click twice on OK to close the opened dialog.

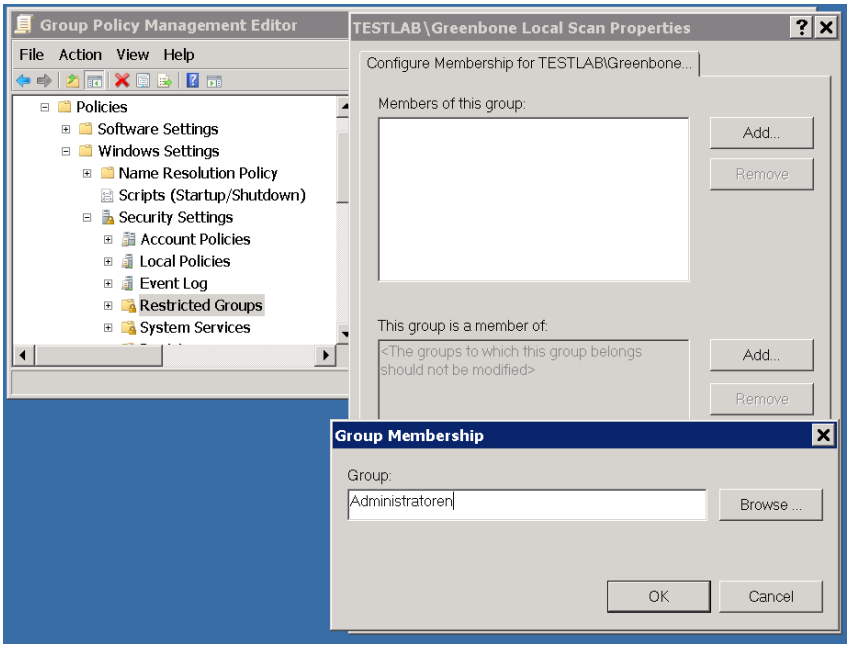


Fig. 9.23: Add Group Membership.

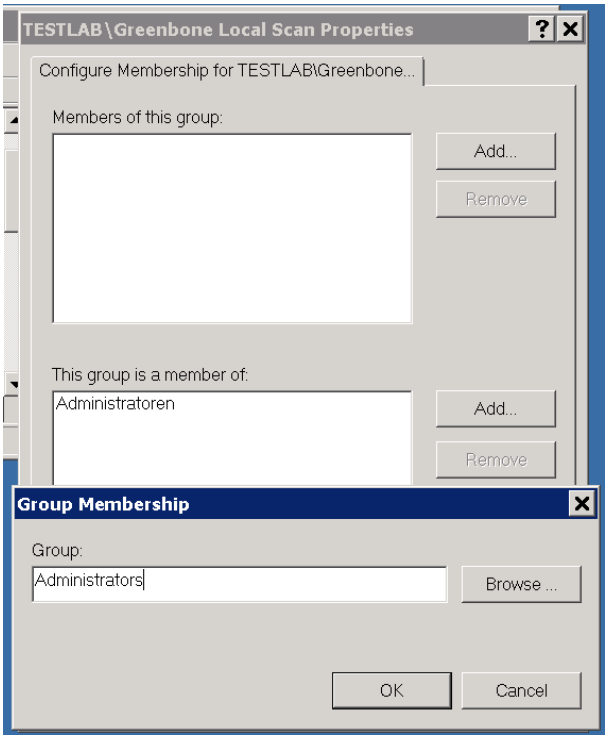


Fig. 9.24: Add another Group Membership.

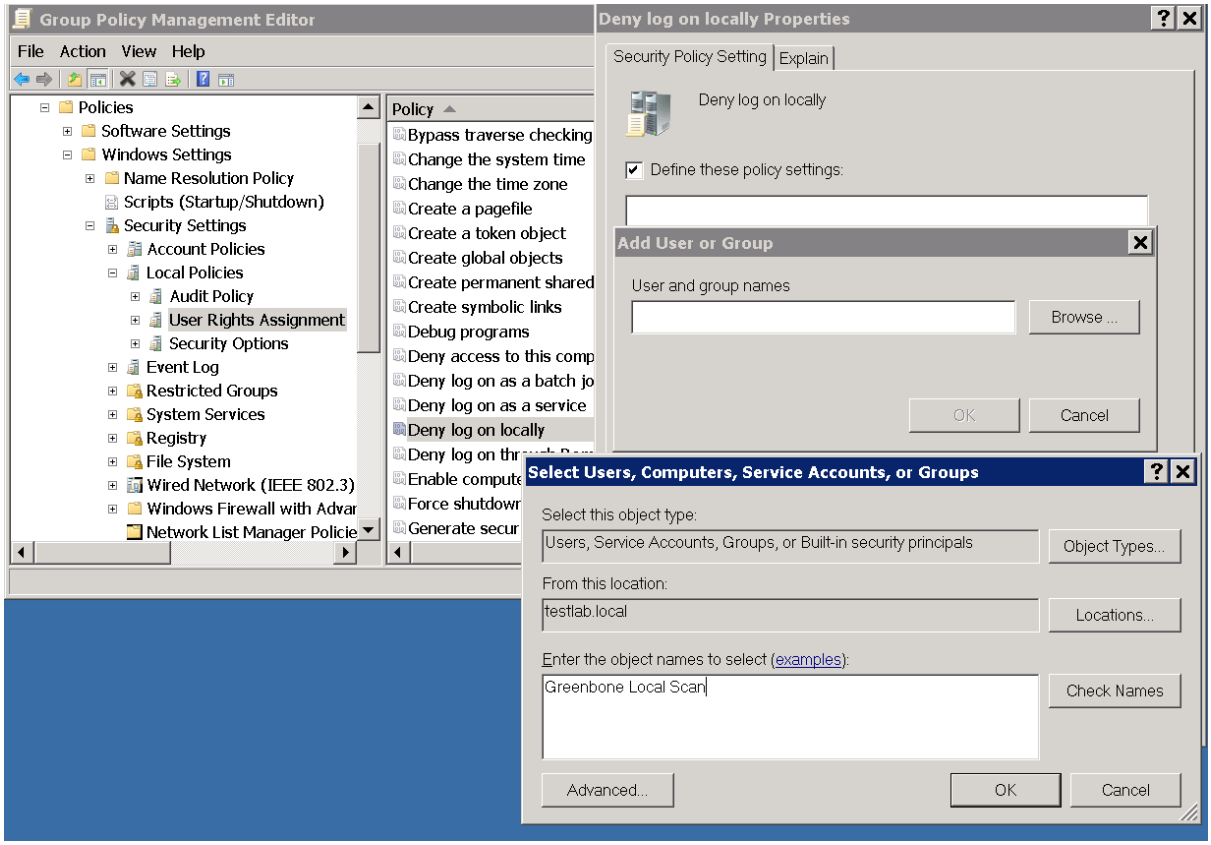


Fig. 9.25: Edit the policy for local log on.

- Click OK.

Step 5: Configure the policy to deny the group `Greenbone Local Scan` logging into systems remotely

Add the `Greenbone Local Scan` to the `Greenbone Local SecRights` group and deny group members logging in via RDP.

- Click the policy `Greenbone Local SecRights` and then select `Edit`.
- Open:

```
Computer Configuration\Polices\Windows Settings\Security Settings\
Local Policies\User Rights Assignment
```

- In the right pane double click on `Deny log on through Remote Desktop Services`.
- Set the checkmark in `Define these policy settings:`
- Click on `Add User or Group`
- Now select `Browse` in the dialog, enter `Greenbone Local Scan`, then click on `Check Names`.
- Now click twice on OK to close the opened dialog.
- Click OK.

Step 6 (Optional): Configure the policy to give only read permissions to the local drive for the `Greenbone Local Scan` group.

Restrict the permissions to the system drive in the `Greenbone Local SecRights` policy for the `Greenbone Local Scan` group. Please note that this setting still exists after the GPO has been removed (`Tattooing GPO`). This changes fundamental privileges which might not be simply reversed

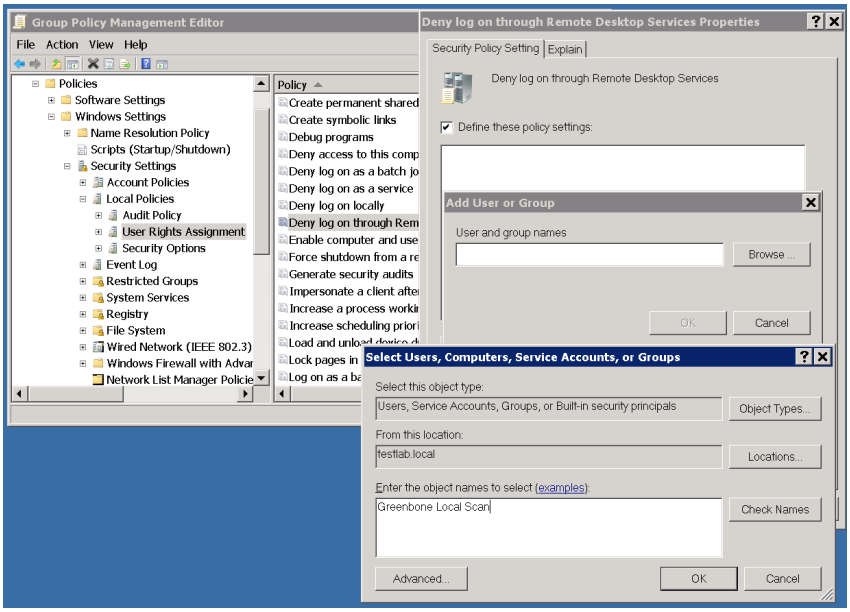


Fig. 9.26: Edit Policy for remote log in.

by removing the GPO. Please research first whether these settings are compatible with your environement!

- Click on the `Greenbone Local Sec Rights` policy and then select `Edit`.
- Open:

```
Computer Configuration\Polices\Windows Settings\Security Settings\File Systems
```

- In the left pane right click on File System and select `Add File...`.
- In the Folder field enter: `%SystemDrive%` and click OK.

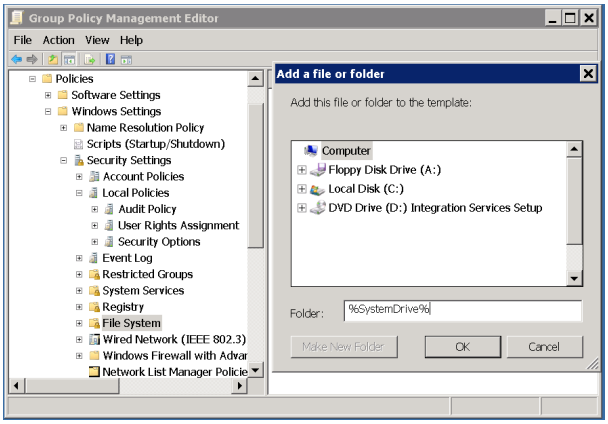


Fig. 9.27: Specifying the `%SystemDrive%` folder.

- Click on Add under `Group or user names:`
- In the dialog that opens enter `Greenbone Local Scan` and click OK.
- Now select the user `Greenbone Local Scan`.
- Deactivate all checkmarks under `Allow` and activate the checkmarks under *Deny* > *Write*.
- Afterwards click on OK and confirm the warning message with `Yes`.

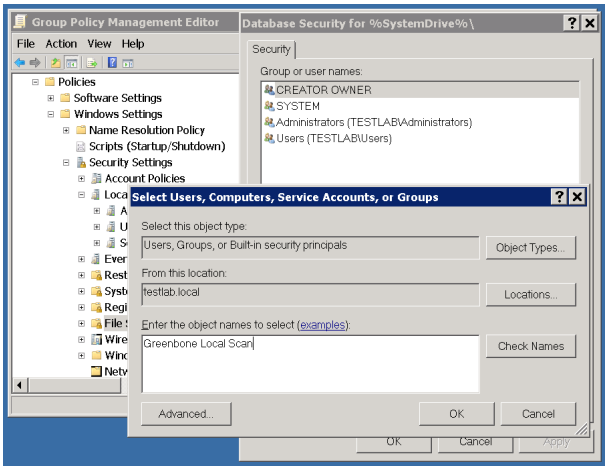


Fig. 9.28: Select the `Greenbone Local Scan` group.

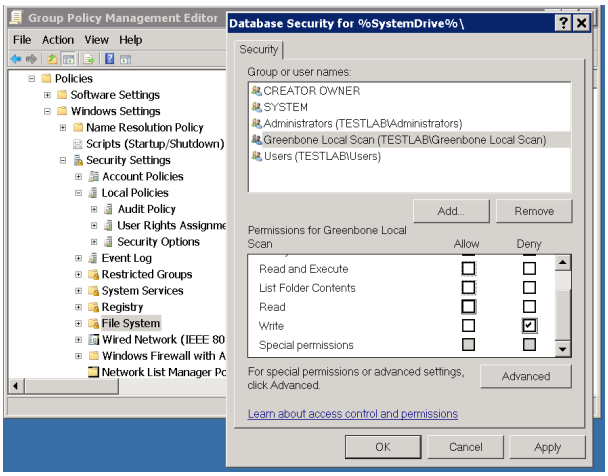


Fig. 9.29: Deny Write access to the group.

- Now select `Configure this file or folder then` and `Propagate inheritable permissions to all subfolders and files` and then click on OK.

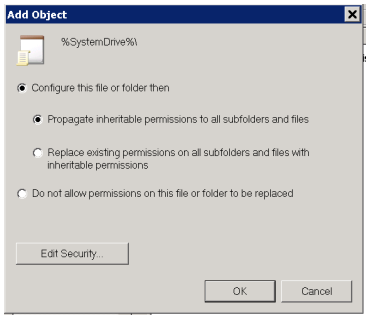


Fig. 9.30: Make the permissions recursive.

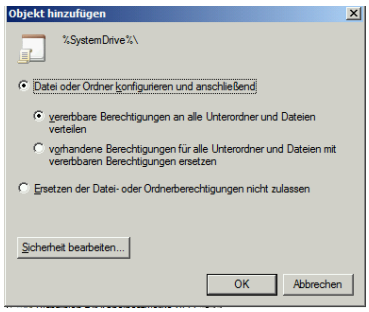


Fig. 9.31: Policy for read permissions on the system drive.

Step 7 (Optional): Configure the policy to give only read permissions to the registry for the `Greenbone Local Scan` group.

To achieve complete restriction is very difficult and possible with a lot of effort. If necessary critical branches can be secured additionally by adding the branches manually.

Please note that this setting still exists after the GPO has been removed (*Tattooing GPO*). This changes fundamental privileges which might not be simply reversed by removing the GPO. Please research first whether these settings are compatible with your environement!

- In the left pane right click `Registry` and select `Add Key`.
- Select `Users` and click OK

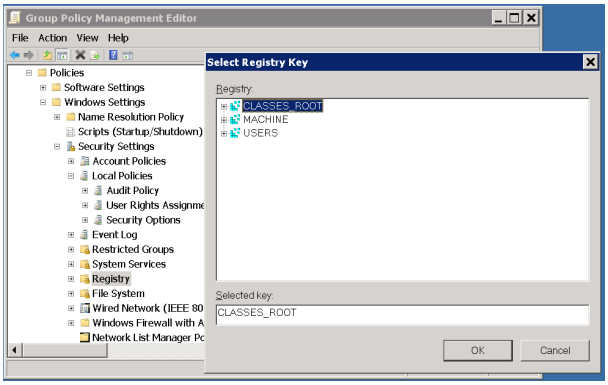


Fig. 9.32: Select the `USERS` registry key.

- Click on Advanced and then Add.
- Enter `Greenbone Local Scan` in the dialog that opens and click on OK.

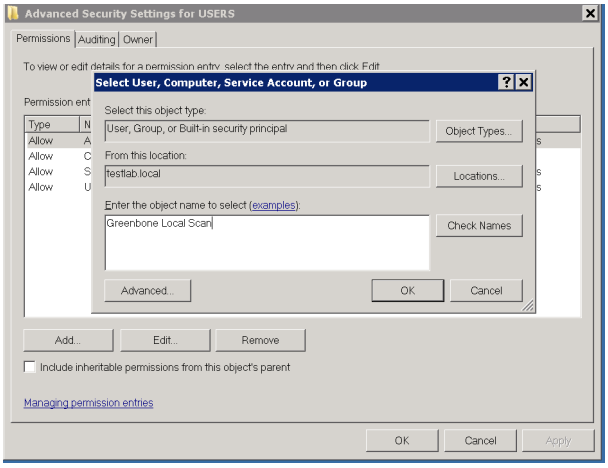


Fig. 9.33: Select the `Greenbone Local Scan` group.

- In the following dialog select for `Apply to: This object and child objects`
- Under Permissions select Deny for `Set Value`, `Create Subkey`, `Create Link`, `Delete`, `Change Permissions` and `Take Ownership`.

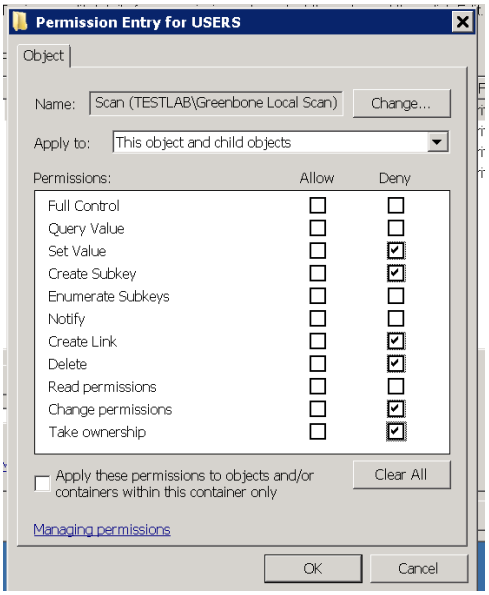


Fig. 9.34: Disallow edition of the registry.

- Do not select anything under `Allow`!
- Afterwards click OK twice and confirm the warning message with `Yes`.
- Click OK again.
- Now select `Configure this key then` and `Propagate inheritable permissions to all subkeys` and then click OK.
- Repeat the above mentioned steps also for MACHINE and CLASSES_ROOT by clicking on Registry in the right pane and then select `Add key...`.

Step 8 (Optional): Allow WMI access on Windows Vista, 7, 8, 10, 2008, 2008R2, 2012 and 2016 Windows Firewall

- Click on the `Greenbone Local Sec Rights` policy and then select `Edit`.

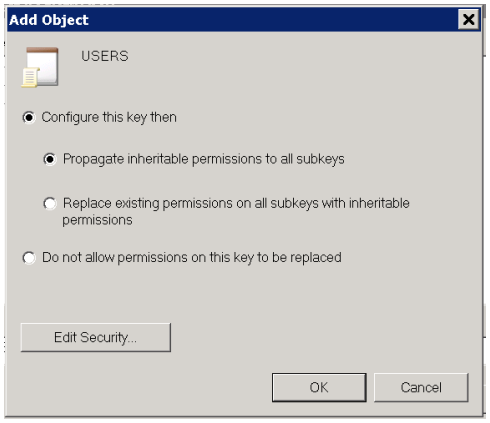


Fig. 9.35: Propagate the new settings recursively.

- Open:

  ```
  Computer configuration\Policies\Windows Settings\Security
  Settings\Windows Firewall with Advanced Security\Windows
  Firewall with Advanced Security\Inbound Rules
  ```

- Right mouse click in the working area and choose New Rule...?
- Choose the Predefined option, and click on Windows Management Instrumentation (WMI) from the drop-down list.

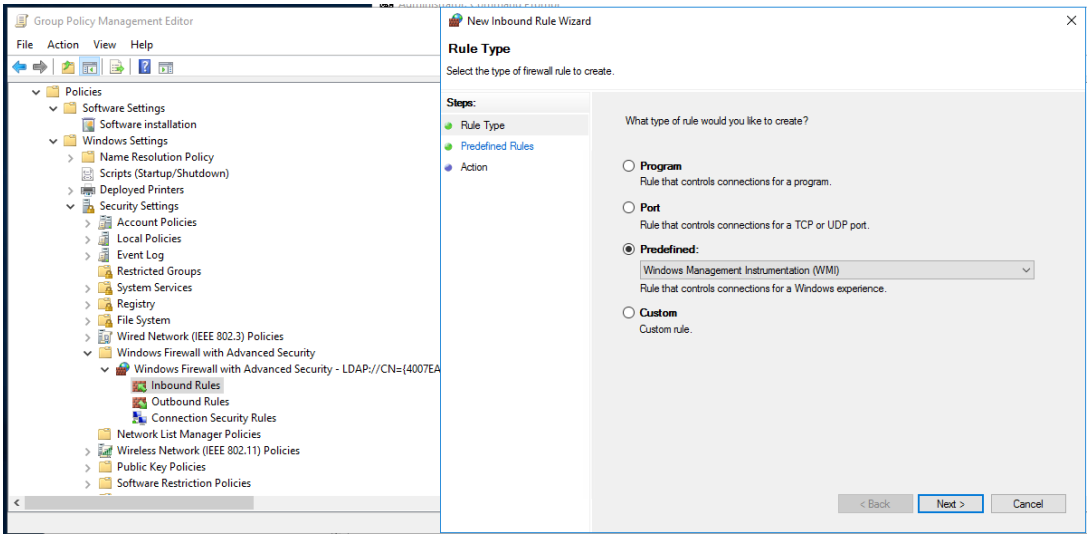


Fig. 9.36: Configuring the firewall via GPO

- Click on Next.
- Click the check boxes for:
  - Windows Management Instrumentation (ASync-In)
  - Windows Management Instrumentation (WMI-In)
  - Windows Management Instrumentation (DCOM-In)
- Click on Next.
- Click on Finish.

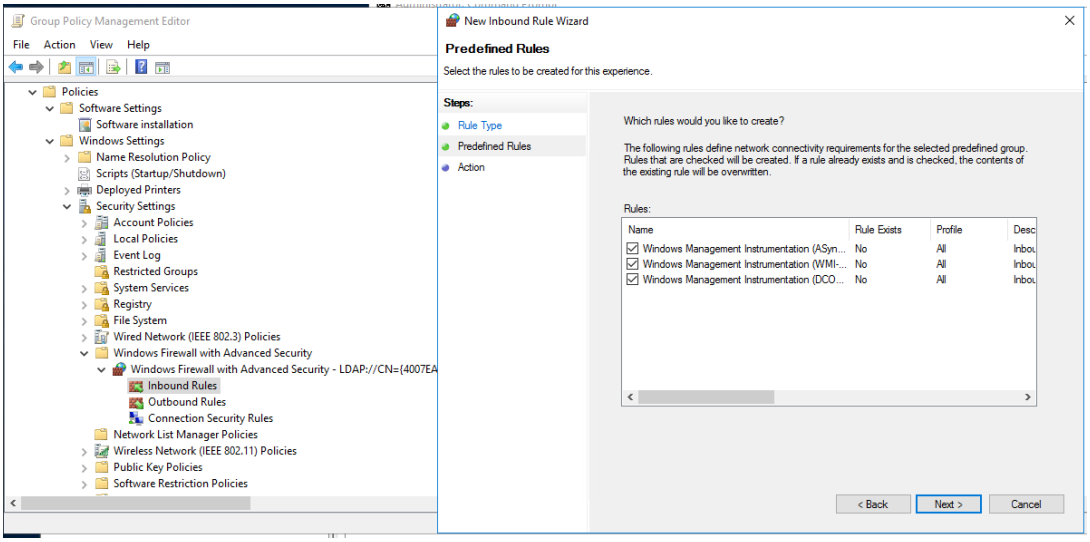


Fig. 9.37: Configuring the firewall via GPO

Step 9: Linking of the Group Policy Object

- On the right pane in the Group Policy Management console right click on the domain or Organizational Unit `Link an Existing GPO` and select `Link an Existing GPO`....
- Now select the group policy object `Greenbone Local SecRights`. The values shown in the figure only serve as example.

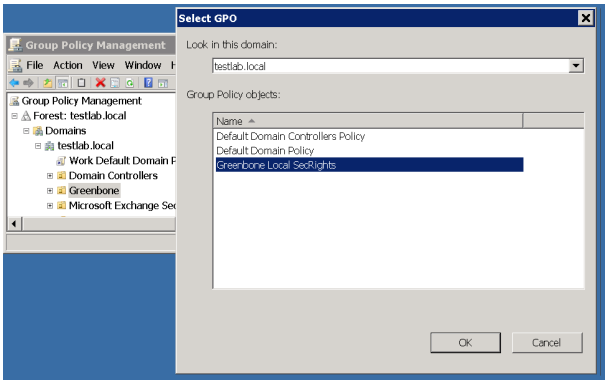


Fig. 9.38: Linking the policy.

Restrictions Based on the fact that write permissions to the registry and system drive have been removed, the following two tests will no longer work:

- **`Leave information on scanned Windows hosts` OID 1.3.6.1.4.1.25623.1.0.96171** This test, if desired, creates information about the start and end of a scan under HKLMSoftwareVulScanInfo. Due to denying write access to HKLM this is no longer possible. If you continue to desire this the GPO must be adjusted here respectively.
- **`Windows file Checksums` OID 1.3.6.1.4.1.25623.1.0.96180** This test, if desired, when executed saves the tool ReHash under C:\Windows\system32 (for 32-bit systems) or c:\Windows\SysWOW64 (for 64-bit systems). Due to denying write access this is no longer possible. The tool must be saved separately or the GPO must be adjusted respectively.

  More information can be found in section *File Checksums* (page 163).

Scanning without domain admin and local admin permissions

Theoretically it is possible to build a GPO in which the user also does not have any local admin permissions. But the effort to add respective read permissions to each registry branch and folder as well, is enormous. Unfortunately inheriting of permissions is deactivated for many folders and branches. Additionally these changes can be set by GPO but cannot be removed again (Tattooing GPO). Also specific permissions could possibly be overwritten so that additional problems could occur.

To go this route does not make a lot of sense from a technical and administrative perspective.

Requirements on Target Systems with Linux/UNIX

- For authenticated scans on Linux or UNIX systems regular user access is usually enough. The log in is performed via SSH. The authentication is done wither with passwords or an SSH key stored on the GSM.
- Generated install package for credentials: The install package for Linux Debian or Linux RedHat is a `.deb` or a `.rpm` respectively, creating a new user without any specific permissions. A SSH Key that is created on the GSM is stored in the users home folder. For users of other Linux distributions or UNIX derivatives the key is offered for download. The creation of a user and saving the key with the proper file permissions is the responsibility of the user.
- In both cases it needs to be made sure that Public Key authentication is not prohibited by the SSH daemon. The line `PubkeyAuthentication no` can not be present.
- Already existing SSH keys protected by an optional passphrase can be used as well. It is recommended to use the RSA and DSA formats as created by the command **`ssh-keygen`**.
- For scans that include policy testing root permission or the membership in specific groups (often `wheel`) might be necessary. For security reasons many configuration files are only readable by super user or members of specific groups.

Requirements on Target Systems with ESXi

By default, local ESXi users are limited to read-only roles. Either an administrative account or a read-only role with permission to global settings must be used.

The following steps will guide you through the process.

Start the Vsphere client.

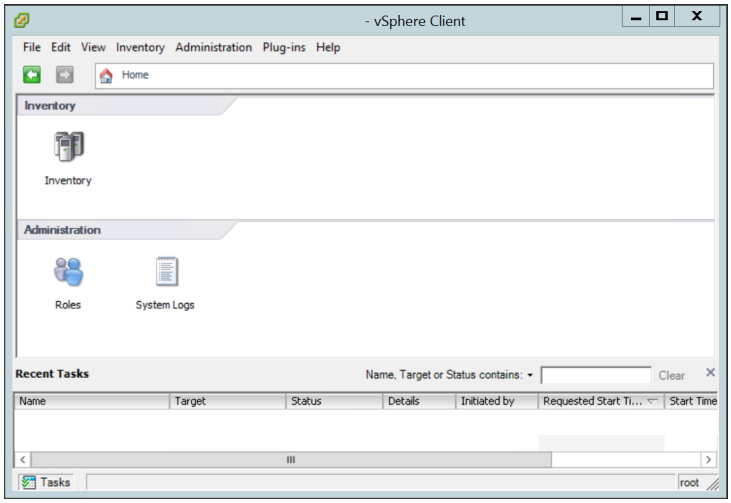


Fig. 9.39: The vsphere client offers access to the roles.

On the Home screen click `Roles`.

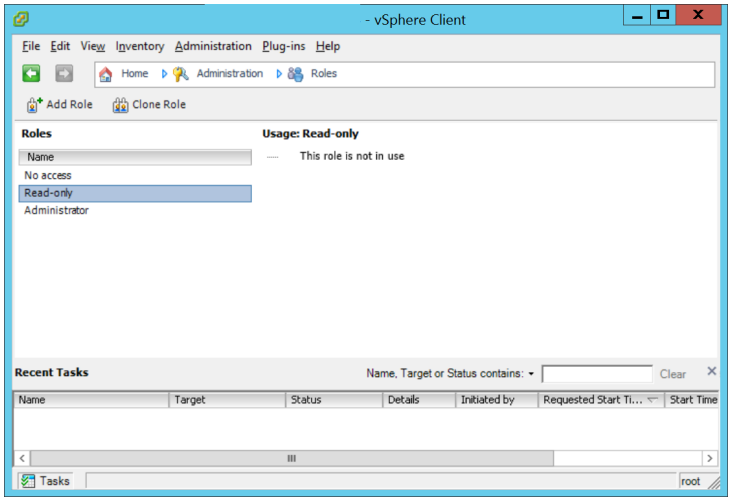


Fig. 9.40: The roles are displayed.

Select the Role `ReadOnly` by right-clicking with the mouse. Clone the role. The list will now contain the Clone as well.

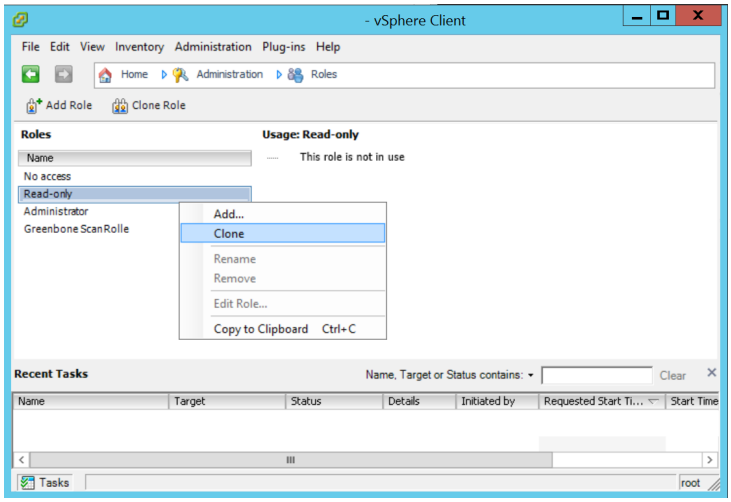


Fig. 9.41: The clone is added.

Rename the cloned role appropriately. In this case `Greenbone Scan Role` is used.

Now modify the new role by right-clicking the role again with the mouse

Add the privilege `Global > Settings` to the role.

Finally assign the new role to the scan user account used by the GSM. Choose the appropriate user from the list of local users and groups.

Go to the permissions tab and click the empty space. Choose `Add Permission`.

Select the created role in the right column. Add the appropriate user in the left column and apply the change using the `OK` Button.

Requirements on Target Systems with Cisco OS

The GSM may check network components like routers and switches for vulnerabilities as well. While the usual network services are discovered and checked via the network some vulnerabilities may only

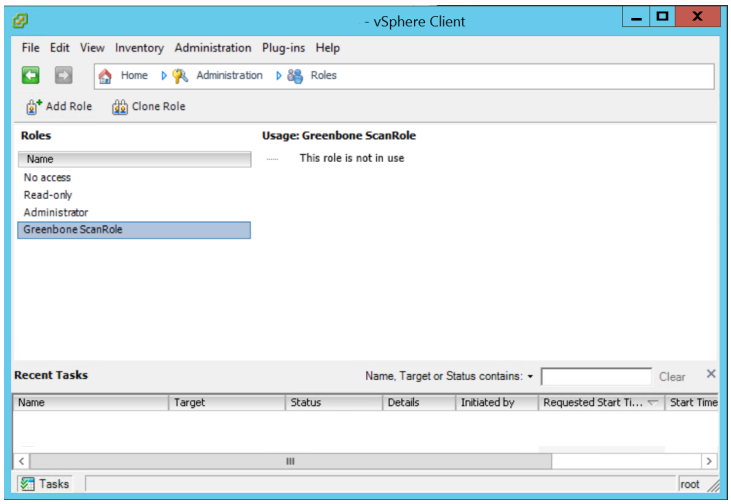


Fig. 9.42: The clone may be renamed.

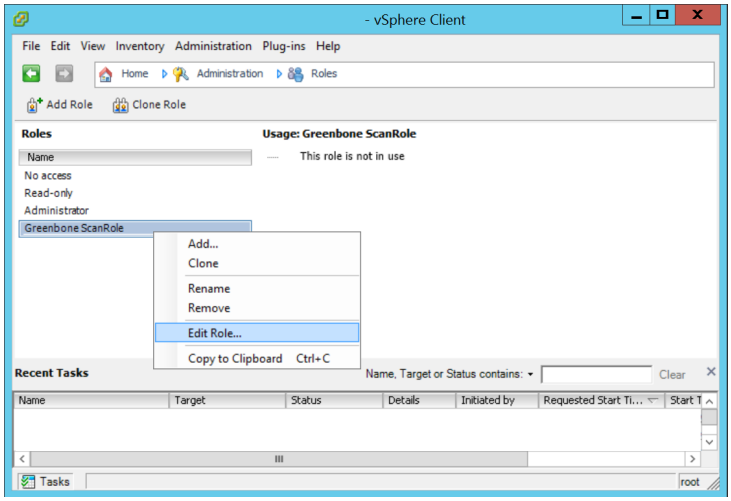


Fig. 9.43: Modify the new Greenbone role.

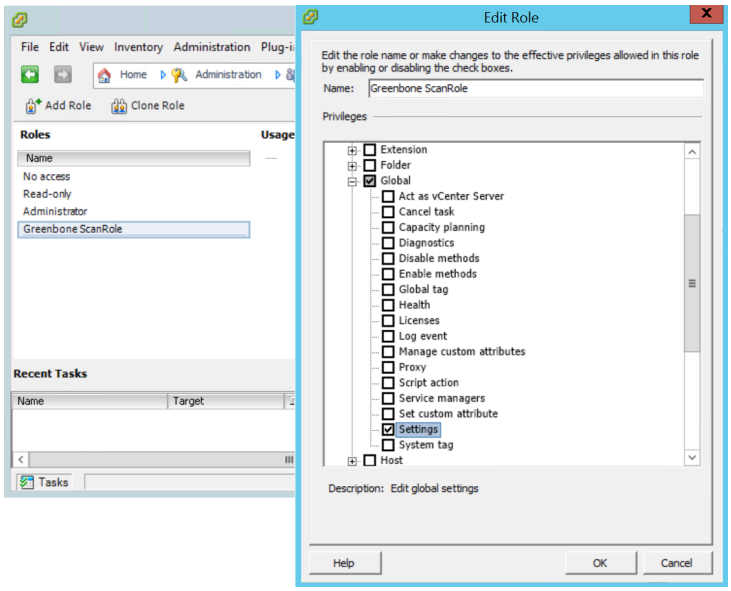


Fig. 9.44: Add Global>Settings to the role.

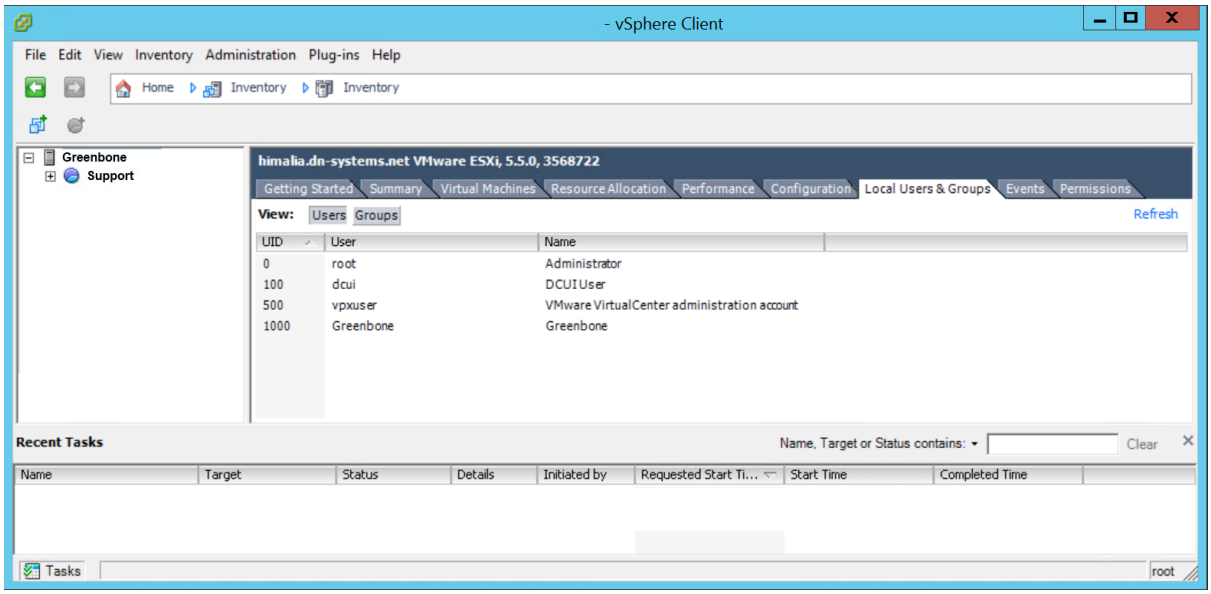


Fig. 9.45: Access the list of local users.

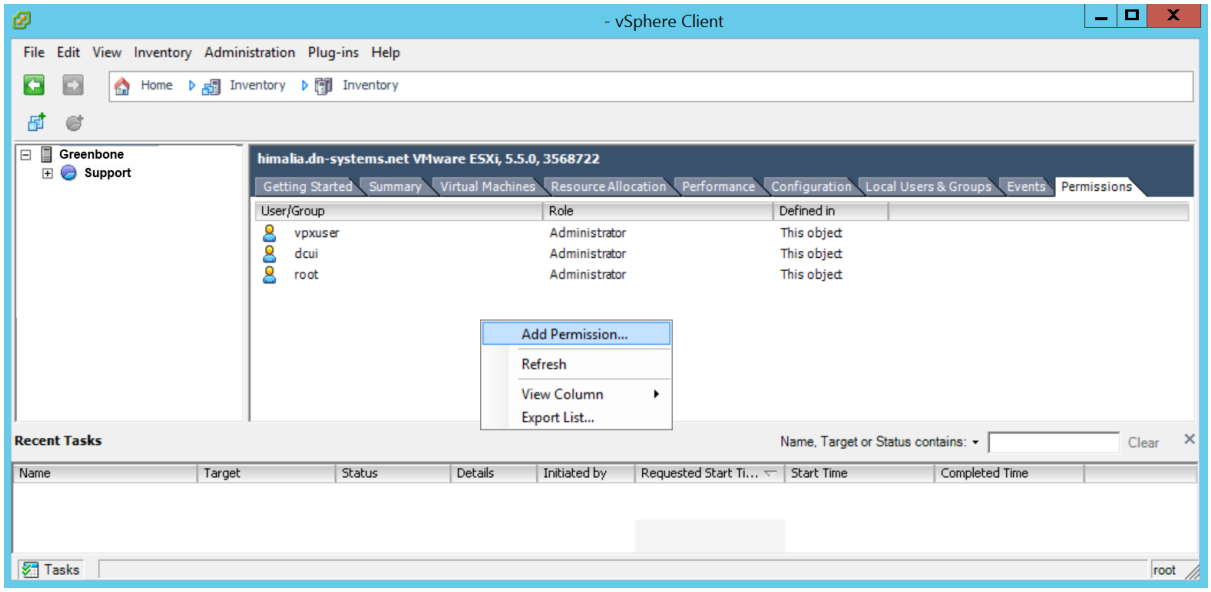


Fig. 9.46: Add a permission on the privileges tab.

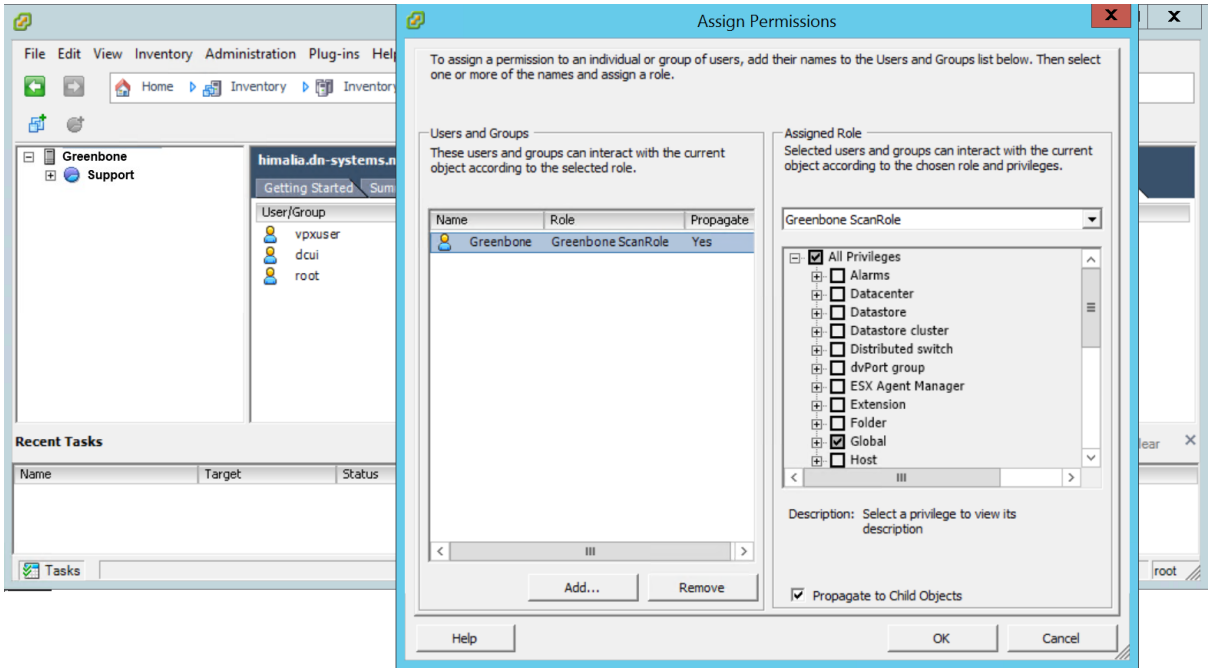


Fig. 9.47: Assign the role to the user.

be discovered by an authenticated Scan. For the authenticated scan the GSM may use either SNMP or SSH. This section will cover both approaches.

SNMP

The GSM may use the SNMP protocol to access the Cisco network component. The GSM support SNMPv1, v2c and v3. SNMP uses the port 161/udp. The default port list does not include any UDP port. Therefore this port is ignored during the vulnerability test using `Full and Fast` and no SNMP check is enabled. To scan network components the port list should be modified to include at least the following ports:

- 22/tcp SSH
- 80/tcp 8080/tcp HTTP
- 443/tcp 8443/tcp HTTPS
- 2000/tcp SCCP
- 2443/tcp SCCPS
- 5060/tcp 5060/udp SIP
- 5061/tcp 5061/udp SIPS
- 67/udp DHCP Server
- 69/udp TFTP
- 123/udp NTP
- 161/udp SNMP
- 162/udp SNMP Traps
- 500/udp IKE
- 514/udp Syslog
- 546/udp DHCPv6

- 6161/udp 6162/udp Unified CM

The admin might want to setup special port list to be used just for such network components.

The GSM needs to access only very few objects from the SNMP tree. For least privilege access a SNMP view should be used to constrain the visibility of the SNMP tree for the GSM. The following two examples explain how to setup the view using either a community string or a SNMPv3 user.

To use a SNMP community string the following commands are required on the target:

```
# configure terminal
```

Using an access list the usage of the community may be restricted. The IP address of the GSM is 192.168.222.74 in this example:

```
(config) # access-list 99 permit 192.168.222.74
```

The view `gsm` should only allow accessing the system description:

```
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
```

The last command links the community `gsm-community` with the view `gsm` and the access-list 99:

```
(config) # snmp-server community gsm-community view gsm RO 99
```

When using a SNMPv3 user including encryption the following configuration lines are required on the target:

```
# configure terminal
(config) # access-list 99 permit 192.168.222.74
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
```

SNMPv3 requires the setup of a group first. Here the group `gsmgroup` is linked to the view `gsm` and the access-list 99:

```
(config) # snmp-server group gsmgroup v3 priv read gsm access 99
```

Now the user may be created supplying the password `gsm-password` and the encryption key `gsm-encrypt`. The authentication is done using md5 while the encryption is handled by AES128:

```
(config) # snmp-server user gsm-user gsm-group v3 auth md5 gsm-password priv aes 128 gsm-encrypt
```

To configure either the community or the SNMPv3 user in the GSM the admin uses *Configuration/Credentials* (see section *Credentials* (page 92)).

SSH

The authenticated scan may be performed via SSH as well. When using SSH the usage of a special unprivileged user is recommended. The GSM currently only requires the command `show version` to retrieve the current version of the firmware of the device.

To setup a least privilege user which is only able to run this command several approaches are possible. The following example uses the Role-Based-Access-Control feature.

Tip: Before using the following example, make sure you understand all side effects of the configuration. If used without verification the system may restrict further logins via SSH or Console.

To use role based access control AAA and views have to be enabled:

```
> enable
# configure terminal
(config)# aaa new-model
(config)# exit
> enable view
# configure terminal
```

The following lines create a restricted view including just the command `show version`. The supplied password `view-pw` is not critical:

```
(config)# parser view gsm-view
(config-view)# secret 0 view-pw
(config-view)# commands exec include show version
(config-view)# exit
```

Now the user `gsm-user` with the password `gsm-pw` is created and linked to the view `gsm-view`:

```
(config)# username gsm-user view gsm-view password 0 gsm-pw
(config)# aaa authorization console
(config)# aaa authorization exec default local
```

If SSH is not yet enabled the following lines take care of that. Use the appropriate hostname and domain:

```
(config)# hostname switch
(config)# ip domain-name greenbone.net
(config)# crypto key generate rsa general-keys modulus 2048
```

Finally enable SSH logins using the following commands:

```
(config)# line vty 0 4
(config-line)# transport input ssh
(config-line)# Crtl-Z
```

Now the credentials of the user need to be entered on the GSM. Navigate to *Configuration* followed by *Credentials* and create the appropriate user. Then link the credentials to the target to be used as SSH-credentials.

9.2 Scan Configuration

The GSM appliance comes with various pre-defined scan configurations. However, they can be customized and expanded by your on configurations. The following configurations are already available from Greenbone:

Empty This is an empty template.

Discovery Only NVTs are used that provide information of the target system. No vulnerabilities are being detected.

Host Discovery Only NVTs are used that discover target systems. This scan only reports the list of systems discovered.

System Discovery Only NVTs are used that discover target systems including installed operating systems and hardware in use.

Full and Fast For many environments this is the best option to start with. This configuration is based on the information gathered in the prior port scan and uses almost all plugins. Only plugins are used that will not damage the target system. Plugins are optimized in the best possible way to keep the potential false negative rate especially low. The other configurations only provide more value only in rare cases but with much more required effort.

Full and fast ultimate This configuration expands the **Full and Fast** configuration with plugins that could disrupt services or systems or even cause shut downs.

Full and very deep This configuration differs from the **Full and Fast** configuration in the results of the port scan not having an impact on the selection of the plugins. Therefore plugins will be used that will have to wait for a timeout. This scan is very slow.

Full and very deep ultimate This configuration adds the dangerous plugins that could cause possible service or system disruptions to the **Full and very deep** configuration. This scan is also very slow.

The available scan configurations can be viewed under *Configuration/Scan Configs*. Remember that by default only the first 10 configurations are always displayed.

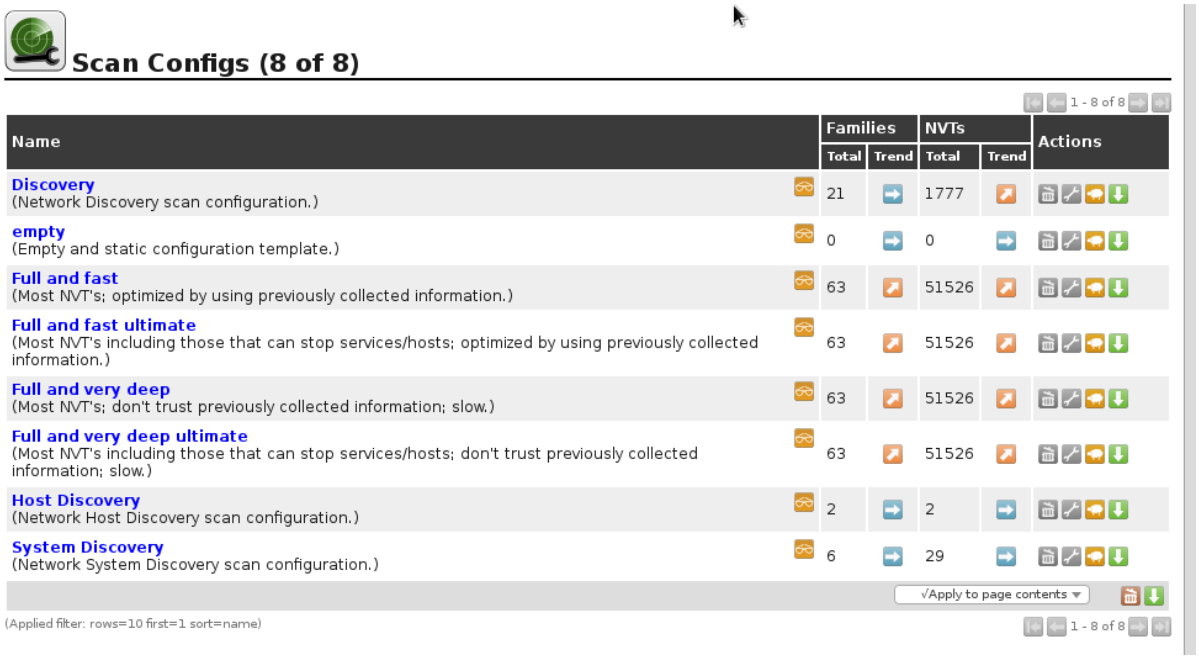


Fig. 9.48: The GSM comes with various scan configurations.

In figure *The GSM comes with various scan configurations.* (page 112) one can identify how many NVT families and how many NVTs are activated in a configuration. Additionally it shows the trend if a scan configuration was configured dynamically or statically.

Greenbone publishes new plugins regularly (NVTs). Also new NVT families can be introduced through the Greenbone Security Feed.

- dynamic

  Scan configurations that are configured dynamically will include and activate new NVT families and new NVTs of the respective activated families automatically after a NVT Feed update. This ensures that new NVTs are available immediately and without any interaction by the administrator.

- static

  Scan configurations that are configured statically will not change after an NVT Feed update.

The icon indicates if the scan configuration is available to and can be used by other users.

Fig. 9.49: User's scan configurations are only visible to them.

To make a configuration available the respective user, role or group must be assigned the *get_configs* permission. Then this configuration will be visible to the respective users as well.

Fig. 9.50: With the appropriate permissions other users can use the configuration.

9.2.1 Creating a New Scan Configuration

To create a new scan configuration first select *Configuration/Scan Configs*. Then by clicking on in the upper left corner a new scan configuration can be created.

Alternatively a scan configuration can be imported using the icon. Greenbone themselves offer different scan configurations on their web site. In addition scan configurations can be exported on other GSM appliances and then imported.

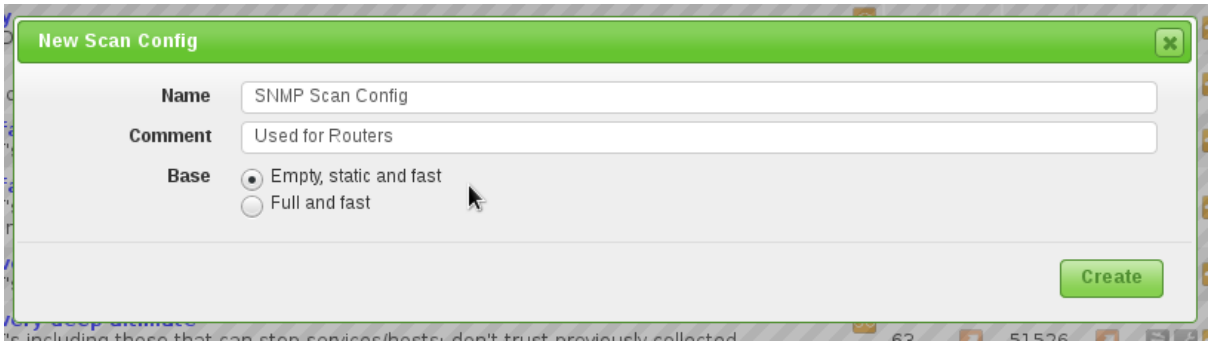


Fig. 9.51: A new scan configuration can be created manually.

When manually creating a scan configuration enter the name and an optional comment and decide which scan configuration to use as a template. You can choose between:

- Empty, static and fast
- Full and fast

If another scan configuration should be used as a template it may be cloned on the overview page . After cloning the configuration can be edited and given its own name and comment and can be further customized.

The next overlay will display the starting configuration. The configuration can be edited right away.

Of importance are the following settings:

Family Trend This option decides whether a newly introduced family will be activated in this scan configuration.

NVT Trend In every family it can be decided if all NVTs in this family should be activated automatically.

Select all NVTs In this column all NVTs of a family may be selected.

Action With this icon the NVTs within a family may be individually selected if you do not want to use all of them.

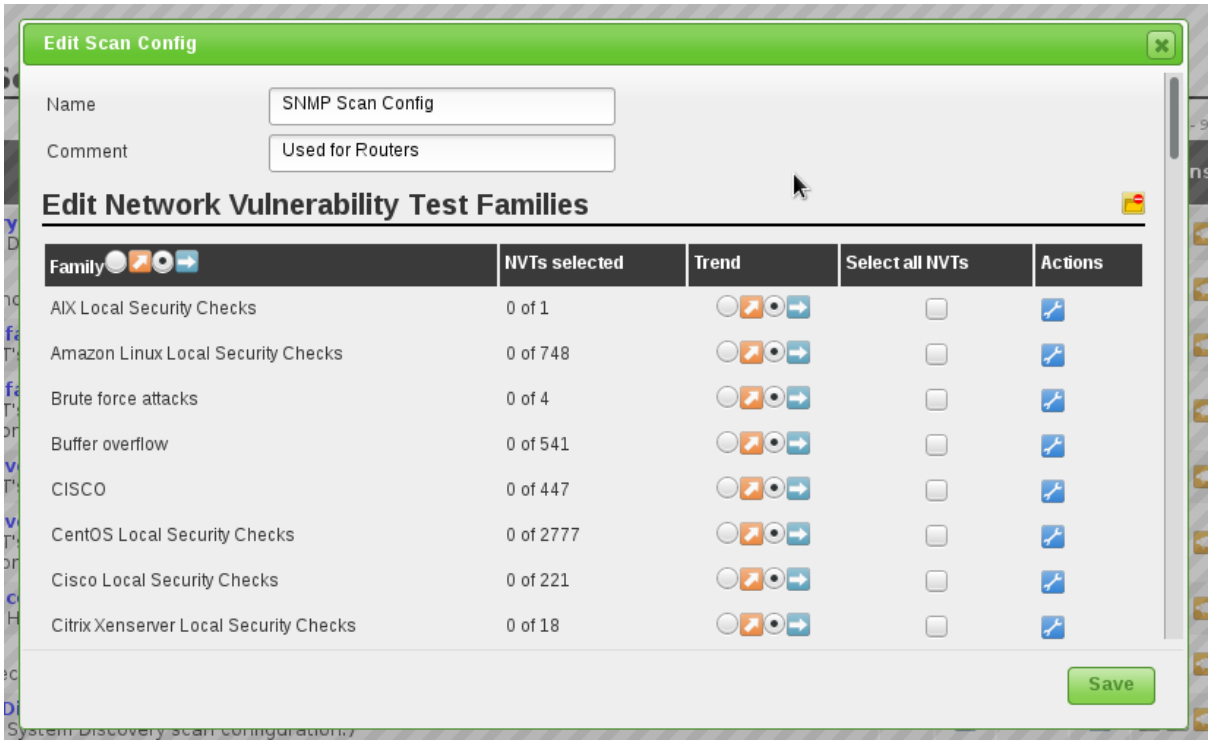


Fig. 9.52: The configuration offers many customization options.

When scrolling further down the *Edit Scanner Preferences* will appear (see section *Scanner Preferences* (page 114)). Here additional settings for the scan can be customized after unfolding using . Also, there are the *Network Vulnerability Test Preferences* that are being used by the NVTs. They can be customized here after unfolding using . Furthermore there is the possibility to define the settings directly within the respective NVTs.

To make changes to the NVTs you must switch into the respective family.

After selecting a family the individual NVTs can be accessed. The NVTs that are part of a family and their severity can be viewed.

Also the status (enabled/disabled) and the timeout of the NVT plugin can be viewed and verified as well if the NVT can be configured further via a configuration (column Prefs). If this is the case, the configuration can be accessed via the respective wrench icon . The settings can be found all the way at the bottom of the page the opens next.

The customized settings of the NVTs are then visible on the overview page of the scan configuration (see figure *The configuration offers many customization options.* (page 114) and *The configuration allows for specific customization of the NVTs as well.* (page 115)).

For practical use especially the settings of the Port Scanner in use are of interest. The GSM appliance utilizes Nmap and Ping as port scanner. Nmap is being used via the NASL wrapper. This allows for the greatest flexibility.

9.2.2 Scanner Preferences

To document all scanner and NVT preferences is out of scope of this document. Therefore only the most important general settings and specific settings of the Ping and Nmap-scanners will be covered.

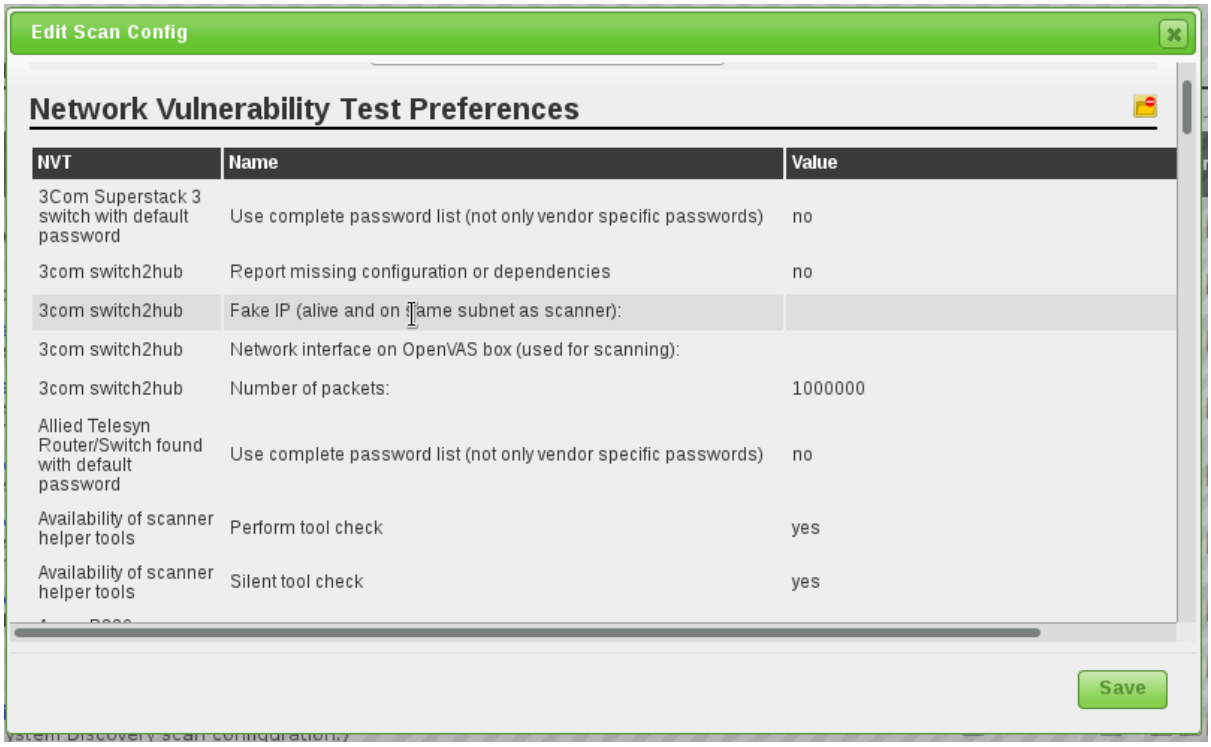


Fig. 9.53: The configuration allows for specific customization of the NVTs as well.

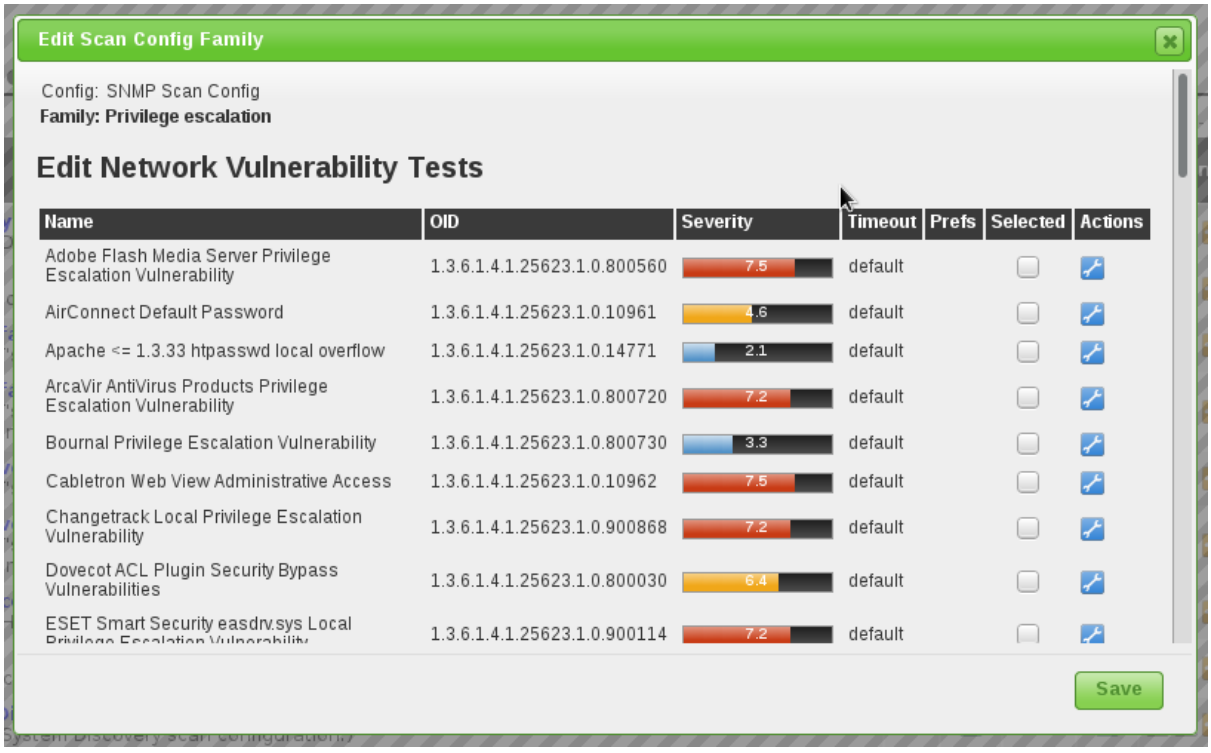


Fig. 9.54: When accessing a family the individual NVTs can be seen.

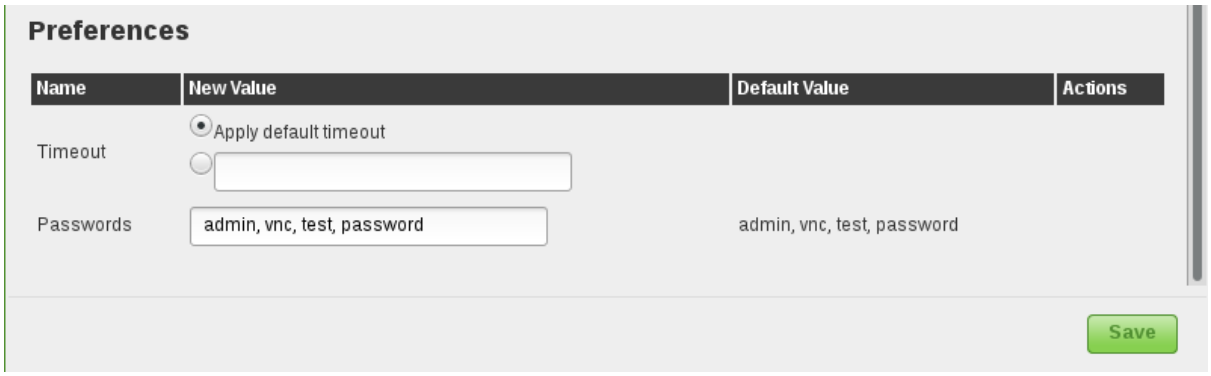


Fig. 9.55: The preferences can be configured for each NVT individually.

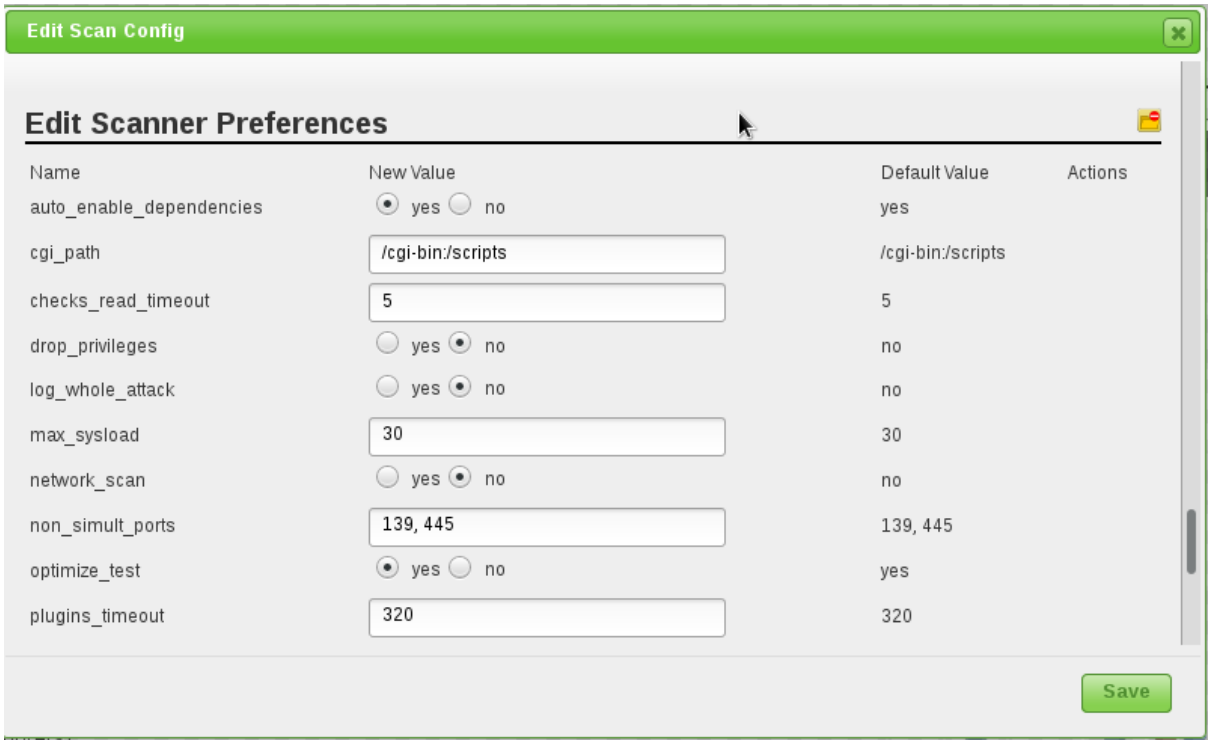


Fig. 9.56: These settings will be used in general by the configuration.

General Preferences

- *auto_enable_dependencies*: NVTs that are required by other NVTs will be activated automatically.
- *cgi_path*: This is the path that will be used by the NVTs to access CGI scripts.
- *checks_read_timeout*: This is the timeout for the network sockets during a scan.
- *drop_privileges*: With this parameter the OpenVAS scanner gives up *root* privileges before the start of the NVTs. This increases the security but results in fewer findings with some NVTs.
- *log_whole_attack*: If this option is enabled the system logs the run time of each individual NVT. Otherwise only that start and completion of a scan is being logged. This reduces required storage space on the hard disk.
- *max_sysload*: This option specifies the maximum load on the GSM. Once this load is reached no further NVTs are used until the load drops below this value again.
- *network_scan*: Experimental option, which scans the entire network all at once instead of starting Nmap for each individual host. This can save time in specific environments.
- *non_simult_ports*: These ports are not being tested simultaneously by NVTs.
- *optimize_test*: NVTs will only be started if specific pre-requisites are met (i.e. open port).
- *plugins_timeout*: Maximum run time of a NVT.
- *report_host_details*: Detailed information of the host are being saved to the report.
- *safe_checks*: Some NVTs can cause damage on the host system. This setting disables those respective NVTs.
- *scanner_plugins_timeout*: This is the maximum lifetime (in seconds) for all NVTs from the Port scanners family. If a NVT runs longer the plugin is terminated.
- *timeout_retry*: number of retries when a socket connection attempt times out.
- *unscanned_closed*: This parameter defines if TCP ports that were not scanned should be treated like closed ports.
- *unscanned_closed_udp*: This parameter defines if UDP ports that were not scanned should be treated as closed ports.
- *use_mac_addr*: Systems will be identified by MAC address and not by IP address. This could be beneficial in a DHCP environment.
- *vhosts*: If the GSM is to scan a web server with name based virtual hosts then the settings *vhosts* and *vhosts_ip* can be used. In the setting *vhosts* the names of the virtual hosts a entered comma separated.
- *vhosts_ip*: If the GSM is to scan a web server with name based virtual hosts then the settings *vhosts* and *vhosts_ip* can be used. In the setting *vhosts_ip* the IP address of the web server is being entered. In the report it can not be referenced in which virtual instance a NVT discovered a vulnerability.

Ping Preferences

The Ping-Scanner-NVT from the Port Scanners family contains the following configurations parameters.

Remember that the `Alive Test` settings of a target object can overwrite some settings of the Ping-Scanner.

- *Do a TCP ping*: Here it can be selected if the reachability of a host should be tested using TCP. In this case the following ports will be tested: 21,22,23,25,53,80,135,137,139,143,443,445. Default: No.

- *Do an ICMP ping*: Here it can be selected if the reachability of host should be tested using ICMP. Default: Yes.
- *Mark unreachable Hosts as dead*: Here it can be selected if a system that are not discovered by this NVT should be tested by other NVTs later. Default: No.
- *Report about reachable Hosts*: Here it can be selected if the systems discovered by this NVT should be listed. Default: No.
- *Report about unreachable Hosts*: Here it can be selected if the systems that are not discovered by this system should be listed. Default: No.
- *TCP ping tries also TCP-SYN ping*: The TCP ping uses by default a TCP-ACK packet. Here a TCP-SYN packet can be used additionally. Default: No.
- *Use ARP*: Here it can be selected if hosts should be searched for in the local network using the ARP protocol. Default: No.
- *Use Nmap*: Here it can be selected if the Ping-NVT should use Nmap. Default: Yes.
- *nmap: try also with only –sP*: If Nmap is used the Ping-Scan will be performed using the –sP option.
- *nmap additional ports for –PA*: Here additional ports for the TCP-Ping-Test can be specified. This is only the case if *Do a TCP ping* is selected. Default: 137,587,3128,8080.

Nmap NASL Preferences

The following options from the Nmap (NASL Wrapper) NVT from the family of Port Scanners will be directly translated into options for the execution of the nmap command. Therefore additional information can be found in the documentation for nmap[7].

- *Do not randomize the order in which ports are scanned*: Nmap will scan the ports in ascending order.
- *Do not scan targets not in the file*: Only meaningful in conjunction with *File containing grepable results*.
- *Fragment IP packets*: Nmap fragments the packets for the attack. This allows to bypass simple packet filters.
- *Identify the remote OS*: Nmap tried to identify the operating system.
- *RPC port scan*: Nmap tests the system for Sun RPC ports.
- *Run dangerous ports even if safe checks are set*: UDP and RPC scans can cause problems and usually are disabled with the setting *safe_checks*.
- *Service scan*: Nmap will try to identify services.
- *Use hidden option to identify the remote OS*: Nmap will try to identify more aggressively.
- *Data length*: Nmap adds random data of specified length to the packet.
- *Host Timeout*: Defines the host timeout.
- *Initial RTT timeout*: This is the initial round trip timeout. Nmap can adjust this timeout dependent on the results.
- *Max RTT timeout*: This is the maximum RTT.
- *Min RTT timeout*: This is the minimum RTT.
- *Max Retries*: Maximum number of retries.
- *Maximum wait between probes*: This regulates the speed of the scan.
- *Min RTT Timeout*: This regulates the speed of the scan.

[7] http://nmap.org/docs.html

- *Minimum wait between probes*: This regulates the speed of the scan.
- *Ports scanned in parallel (max)*: Defines how many ports should be scanned simultaneously.
- *Ports scanned in parallel (min)*: see above
- *Source port*: Defines the source port. This is of interest when scanning through a firewall if connections are in general allowed from a specific port.
- *File containing grepable results*: Allows for the specification of a file in which line entries in the form of `Host: IP address` can be found. If the option *Do not scan targets not in the file* is set at the same time only systems contained in the file will be scanned.
- *TCP scanning technique*: Define the actual scan technique.
- *Timing policy*: Instead of changing the timing values individually the timing policy can be modified.

The timing policy uses the following values:

	initial_rtt_timeout	min_rtt_timeout	max_rtt_timeout	max_parallelism	scan_delay	max_scan_delay
Paranoid	5 min	100 ms	10 sec	Serial	5 min	1 sec
Sneaky	15 sec	100 ms	10 sec	Serial	15 sec	1 sec
Polite	1 sec	100 ms	10 sec	Serial	400 ms	1 sec
Normal	1 sec	100 ms	10 sec	Parallel	0 sec	1 sec
Aggressive	500 ms	100 ms	1250 ms	Parallel	0 sec	10 ms
Insane	250 ms	50 ms	300 ms	Parallel	0 sec	5 ms

9.3 Obstacles while Scanning

This section will highlight and explain several typical problems which might occur during a scan using the default values of the GSM. While the default values of the GSM are valid for most environments and customers, depending on the actual environment and the configuration of the scanned hosts they might require some tweaking.

The following sections will cover typical problems, explain why they occur and will give some advice to overcome these problems.

9.3.1 Hosts not found

During a typical Scan (either a Discovery Scan or a Full and Fast Scan) the GSM will by default first use the ping command to check the availability of the configured targets. If the target does not reply the ping request the target is presumed to be dead and will not be scanned by the port scanner or any NVT.

In most LAN environments this does not pose any problems because all devices will respond to a ping request. But sometimes (local) firewalls or other configuration might suppress the ping response. If this happens the target will not be scanned and will not be included in the results and the scan report.

To remediate this problem the both the target configuration and the scan configuration support the setting of the Alive Test (see *Alive Test* (page 86)).

If the target does not respond to a ping request you may want to test a `TCP Ping`. If the target is located within the same broadcast domain you may want to try a `ARP Ping` as well.

9.3.2 Long Scanperiods

Once the target is discovered to be alive using the ping command the GSM uses a port scanner to scan the target. By default a TCP port list containing around 5000 ports is used. If the target is protected by a (local) firewall dropping most of these packets the port scan will need to wait for the timeout of each individual port. If your hosts are protected by (local) firewalls you may want to tune the port lists or your firewalls. If the firewall does not drop the request but rejects the request the port scanner does not have to wait for the timeout. This is especially true if you include UDP ports in the scan.

9.3.3 NVT not used

This happens especially very often if you use UDP based NVTs like NVTs using the SNMP protocol. If you use the default configuration `Full and Fast` the SNMP NVTs are included. But if the target is configured using the default port list the NVTs are not executed. This happens because the default port list does not include any UDP ports. Therefore the port 161/udp (snmp) is not discovered and excluded from further scans. Both the discovery scans and the recommended `Full and Fast` scan configuration optimize the scan based on the discovered services. If the UDP port is not discovered no SNMP NVTs are executed.

Please do not enable all ports per default in your port lists. This will prolong the scans considerably. Best practice is the tuning of the port lists to the ports which are used in your environment and are supported by your firewalls.

9.4 Scheduled Scan

For continuous vulnerability management the manual execution of task is cumbersome. The GSM supports the scheduling of tasks for their automation. This is done via *Schedules*. This option can be found in the *Configuration* menu.

The GSM does not provide any schedules by default. To add a new schedule use the|new| button in the upper left corner.

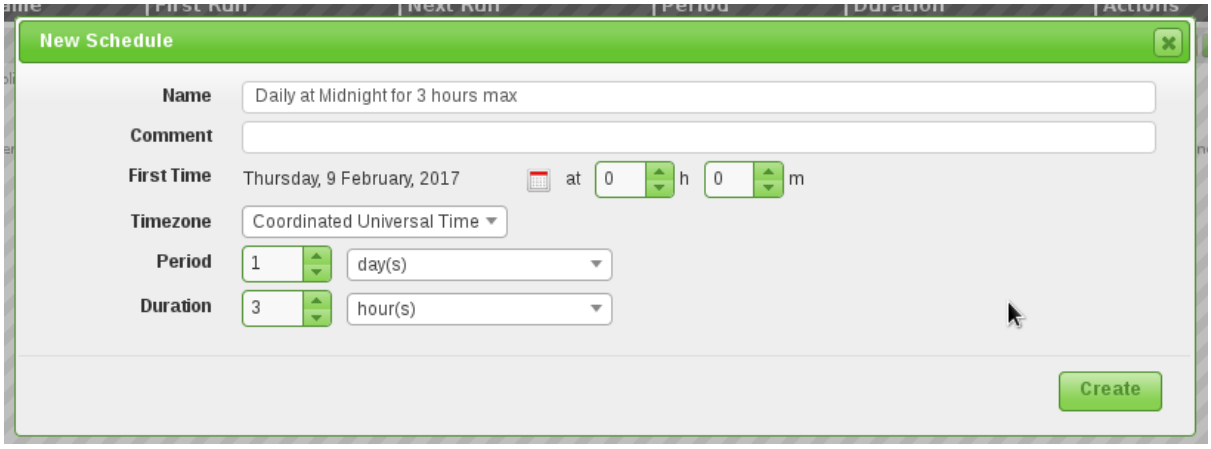


Fig. 9.57: Schedules support time controlled scans.

The Greenbone Security Manager refers to Schedules as automatic scans at a specific time. They can be run once or repeatedly. The intervals can be configured:

- hourly
- daily
- weekly

- monthly

Since the GSM runs in the UTC timezone internally the time zone chosen in the schedule is very important. A drop down menu provides the available timezones. For Eastern Standard Time (EST) you will likely choose `America/New York`. Finally the maximum duration of the scan can be limited. If the scan takes longer it will aborted. This way it can be ensured that the scan will always run with a specific (maintenance) time window.

The following options are configurable in the dialog:

- **Name** This is a descriptive name. Meaningful are entries such as `Daily 5:15pm` or `Every 2nd monthly 4:15am`.
- **Comment** Enter a comment again.
- **First Time** Enter the time of the first run.
- **Timezone** The timezone the time refers to. UTC is default.
- **Period** This is the interval between two runs. It can be selected between hourly, daily, weekly and monthly. If left blank the interval is a single instance.
- **Duration** This is the maximum duration a task can take for its execution. After expiration of the of the time allotted the task is aborted.

9.5 Alerts

With the use of alerts the state and results of a scan can be sent to others systems automatically. Alerts are anchored within the system in a way that each configured event will trigger an action, for example, when a task is started or completed. Additionally this can be tied to a condition. Such a condition could be the discovery of a vulnerability with a severity greater than 9. If met, an email or a SNMP trap can be triggered.

To create a new alert change to *Configuration/Alerts*. Now add a new alert using the button  in the upper left corner.

Using the overlay the following details of the alert can be defined:

Name: The name, describing the alert, can be freely chosen

Comment: The optional comment can contain additional information.

Event: Here the event, for which the alert message is being sent, is being defined. For example, this can occur when the status of a task changes.

Condition: Here additional conditions, that have to be met, may be defined. The alert message can occur:

- Always
- Only when at minimum a specific severity level is reached.
- If the severity level changes, increases or decreases.
- If a powerfilter matches at least the specified number of results.
- If a powerfilter matches at least the specified number of results more than in the previous scan.

Report Result Filter Finally the results can be limited with an additional filter. A filter must be created and saved prior (see section *Powerfilter* (page 57)).

Method: Here the method for the alert is selected. Only one method per alert can be chosen. If different alerts for the same event should be triggered, multiple alerts must be created and linked to the same task.

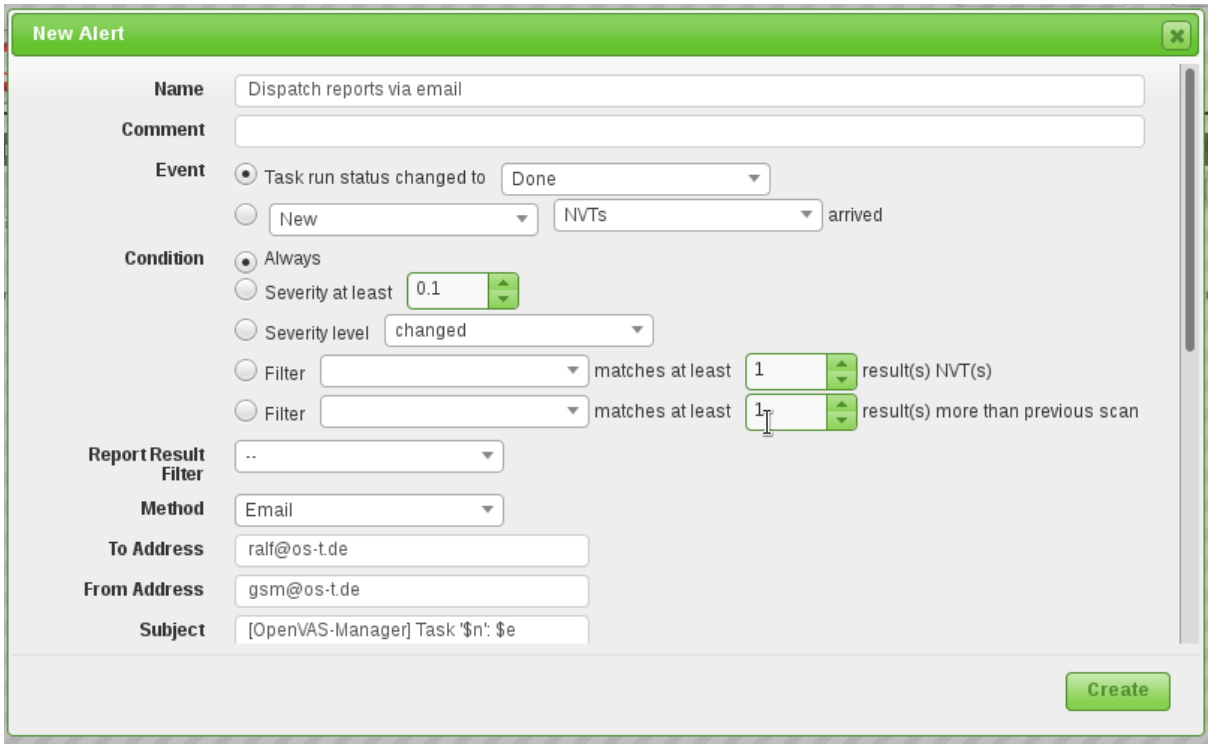


Fig. 9.58: Alerts offer various alerting options.

Email This is the most powerful and most used method. To use this method the mailserver to be used must be configured using the GSM console (see section *Mail Server* (page 43)). The following options may be specified:

To Address: This is the email address to which the email should be sent to.

From Address: This is the sender address of the generated email.

Subject: This is the subject of the email. You can use variables like $n (task name) and $e (event description).

Content: Here the content of the email can be defined:

Simple Notice: This is only a simple description of the event.

Include Report: If the event for the completion of the task (Default: Done) is selected the report can be included in the email. Here a report format that uses the content type `text/*` can be chosen as an email does not support binary content directly. Additionally you can modify the contents of the email message. Within the message you may use variables:

- $c condition description
- $e event description
- $F name of filter
- $f filter term
- $H host summary
- $i report text
- $n task name
- $r report format name
- $t a note if the report was truncated

- $z timezone

Attach Report: If the event for the completion of the task (Default: Done) is selected the report can be attached to the email. Here any report format can be chosen. The report will be attached in its correct MIME type to the generated email. PDF is possible as well. Additionally you can modify the contents of the email message. The same variables may be used.

System Logger This method sends the alert to a Syslog daemon. The Syslog server is defined via the console (see section *Central Logging Server* (page 44)).

HTTP Get With the HTTP Get method, an SMS text message or a message to a trouble ticket system can be sent automatically, for example. The following variables can be used when specifying the URL:

- `$n`: Name of the task
- `$e`: Description of the event (Start, Stop, Done)
- `$c`: Description of the condition that occurred
- `$$`: The $ symbol

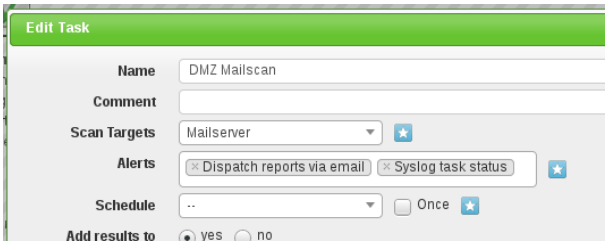


Fig. 9.59: Tasks need to be configured with the appropriate alerts.

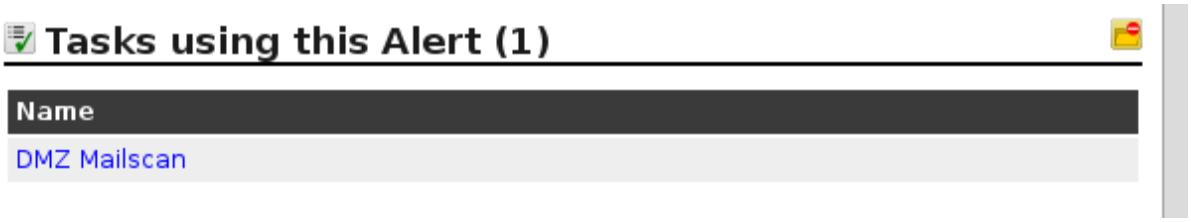


Fig. 9.60: In an alert is in use the corresponding tasks are referenced.

Sourcefire Connector Here the data can be sent automatically to a Cisco Firepower Management Center (formerly known as Sourcefire Defense Center). For more information see section *Firepower Management Center* (page 236).

verinice.PRO Connector Here the data can be sent automatically to a verinice.PRO installation. For more information see section *Verinice* (page 224).

Send to Host Here the report may be send via tcp to an arbitrary host/port combination.

SCP

The report may be copied to a host via scp. Within the filename you can use the following variables:

- $$: $
- $n: task name

SNMP

An SNMP trap is send to the given agent. Within the message you can use the following variables:

- $$: $
- $e: event description
- $n: task name

Start Task Here the alert may start an additional task. The available tasks are selected using a drop down menu.

For the alert to be used afterwards, a specific task definition must be created (see figure *Tasks need to be configured with the appropriate alerts.* (page 123)). To do so edit the respective task. This change of the task is also allowed for already defined and used tasks as it does not have any effect on already created reports.

Afterwards the respective alert references the tasks using the alert (see figure *In an alert is in use the corresponding tasks are referenced.* (page 123)).

9.6 Reports and Vulnerability Management

The results of a scan are summarized in a report. Reports can be viewed with a browser and downloaded from the GSM in different formats. Once a scan has been started the report of the results found so far, can be viewed. Once a scan is complete its status changed to `Done`. From now on no additional results will get added. For more information on reports please refer to the Reports (page 151) chapter as well.

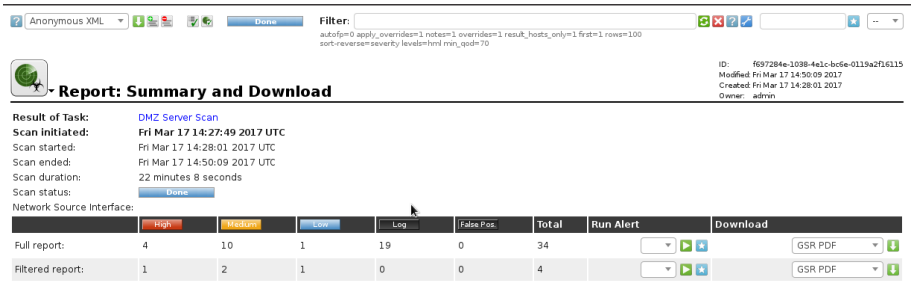


Fig. 9.61: The report summary gives an overview over vulnerabilities found.

The report summary gives a quick overview over the current state. It shows if a scan is complete and how many vulnerabilities have already been found. From the summery a report can be downloaded directly in many different formats. The following formats are supported (see also section *Report Plugins* (page 152))

Anonymous XML Like XML but anonymous.

ARF: Asset Reporting Format v1.0.0 This format creates a report that represents the NIST Asset Reporting Format.

CPE - Common Enumeration CSV Table This report selects all CPE tables and creates a single comma separated file.

CSV hosts This report creates a comma separated file containing the systems discovered.

CSV Results This report creates a comma separated file with the results of a scan.

GSR PDF - Greenbone Security Report (recommended) This is the complete Greenbone Security report with all vulnerabilities.

GXR PDF - Greenbone Executive Report (recommended) This is a shortened report for management.

HTML This report is in HTML format.

ITG - IT-Grundschutz catalogue This report is guided by the BSI IT-Grundschutz catalogue.

LaTeX This report is offered as LaTeX source text.

NBE This is the old OpenVAS/Nessus report format.

Verinice ISM, ITG For Import into veri.nice.

XML A single XML file is created from the report details. This should be the basis for creating your own style for a report or post-process the results in other ways.

Details of a report can be viewed in the web UI as well.

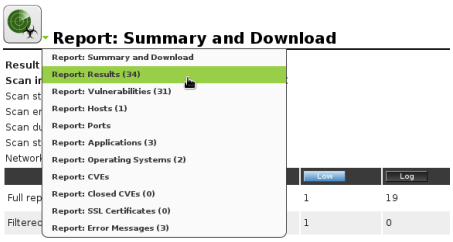


Fig. 9.62: Different views of the same report.

Since a report often contains a lot of findings, the complete report as well as only filtered results can be viewed and downloaded. In the default setting only the `High` and `Medium` risks are being displayed. This can be changed very easily.

Fig. 9.63: Report Filtering.

In the Filtered Results section shows the filtered results. As long as the scan is still running can cause rearrangements here.

To interpret the results please note the following information:

- False Positives False Pos.

  A false positive is a finding that describes a problem that does not exists in reality. Vulnerability scanners often find evidence that point at a vulnerability. However, a final judgment cannot be made. There are two options available:

  - Reporting of a potentially nonexistent vulnerability (False Positive).
  - Ignoring reporting of a potentially existing vulnerability (False Negative).

  Since a user can identify, manage and as such deal with false positives compared to false negatives, the GSM Vulnerability Scanner reports all potentially existing vulnerabilities. The GSM assists with several automatic and semi-automatic to categorize them.

This problem is very common with Enterprise Linux distributions. If, for example, a SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner, that knows of a vulnerability in this version, will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If the user knows of this circumstance an Override can be configured (see section *Overrides and False Positives* (page 130)). The AutoFP function (see section *Automatic False Positives* (page 131)) can assist here as well.

Note: Consider the new concept of Quality of Detection (see sections *Reading of the Reports* (page 126) and *Network Vulnerability Tests* (page 141)).

- Multiple findings can have the same cause. Is an especially old software package installed often multiple vulnerabilities exist. Each of these vulnerabilities is tested by an individual NVT and causes an alert. The installation of a current package will then remove a lot of vulnerabilities at once.
- Important are findings of the levels High and Medium. Address these findings in order of priority. Before addressing medium level findings, high level findings should get addressed. Only in exceptional cases, when it is known that the high alerts need to be less considered (because the service cannot be reached through the firewall) should this approach be deviated from.
- Low and Log are mostly interesting for detail understanding. This is why these findings are filtered out by default. These findings can hold very interesting information however and considering them will increase the security of your network and systems. For their understanding often a deeper knowledge of the applications is required. Typical for an alert at the log level is that a service uses a banner with its name and version number. This could be useful for an attacker during an attack if this version has a known vulnerability.
- To simplify the remediation of vulnerabilities every alert offers a solution for problems directly. In most cases it will be referred to the latest vendor software package. In some cases a configuration change will be mentioned.
- References explain the vulnerabilities further. Even though the alerts contain a lot of information external references are always listed. These refer to web sites on which the vulnerability was already discussed. Additional background information is available such as who discovered the vulnerability, what effects it could have and how the vulnerability can be remediated.

9.6.1 Reading of the Reports

The report contains a list of all of the vulnerabilities detected by the GSM (see figure *List of discovered vulnerabilities* (page 126))

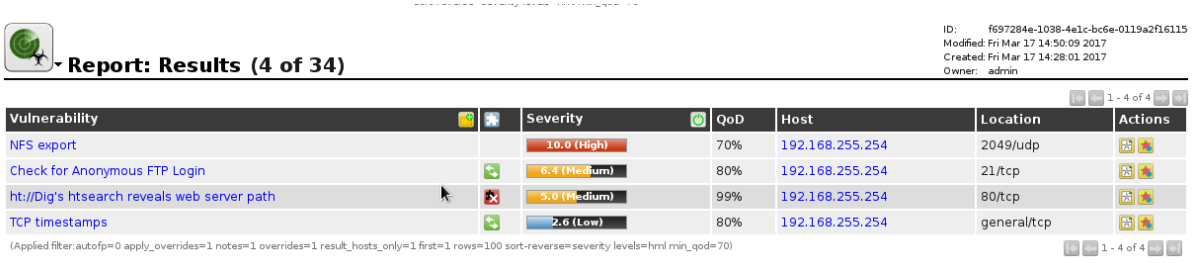


Fig. 9.64: List of discovered vulnerabilities

To support the administrator with the analysis of the results the severity of a vulnerability (CVSS, see also section *CVSS* (page 146))is displayed directly as a bar.

To point the administrator to a simple solution the column Solution-Type displays the existence of a solution. The column will display if a vendor patch exists or a workaround is available. It will also be displayed if no solution for a vulnerability exists . If the column of the respective vulnerability still appears empty then the respective NVT has not been updated yet.

The column Quality of Detection (QoD) provides information in regards to the reliability of the successful detection of a vulnerability. This assessment is implemented into all existing NVTs step by step (see section *Network Vulnerability Tests* (page 141)). This column allows to be filtered as well. You can use the *min_qod* in the Powerfilter. By default only NVTs with a QoD of 70% are displayed.Vulnerabilities with a lower reliability of detection are not displayed in the report. The possibility of false positives is thereby lower.

In the respective vulnerability view, additional, more detailed information is available.

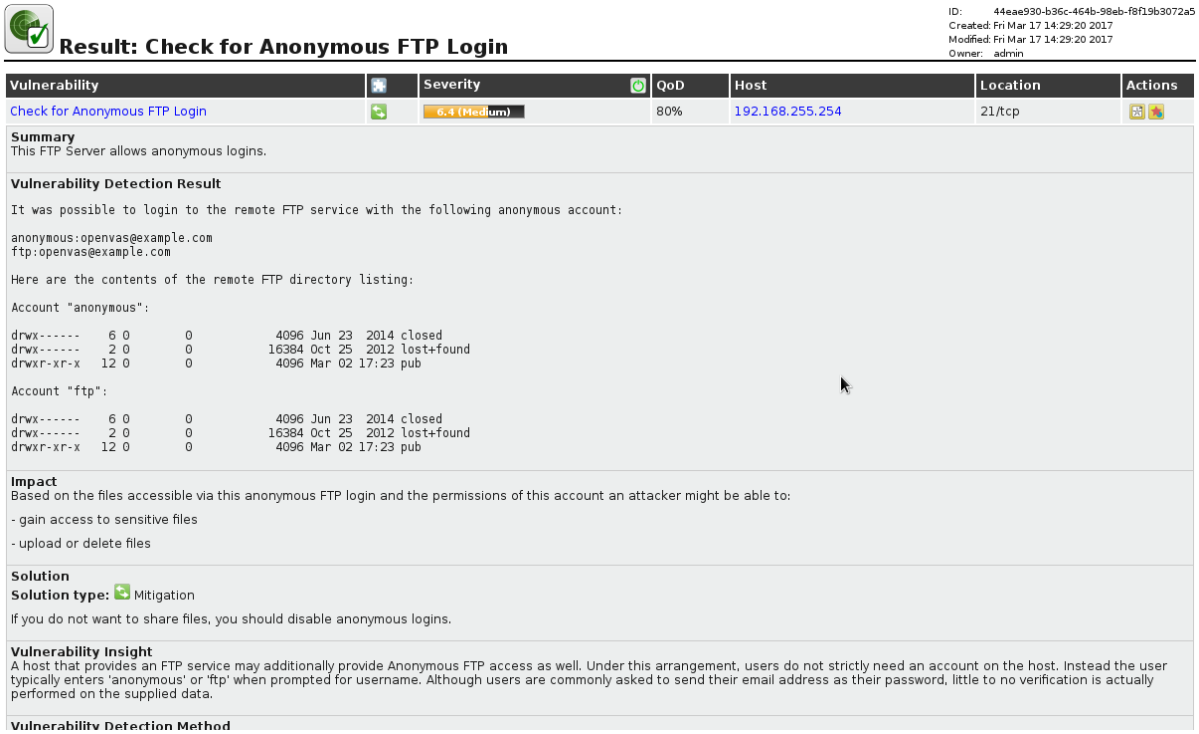


Fig. 9.65: Detailed information about the vulnerability and solution options.

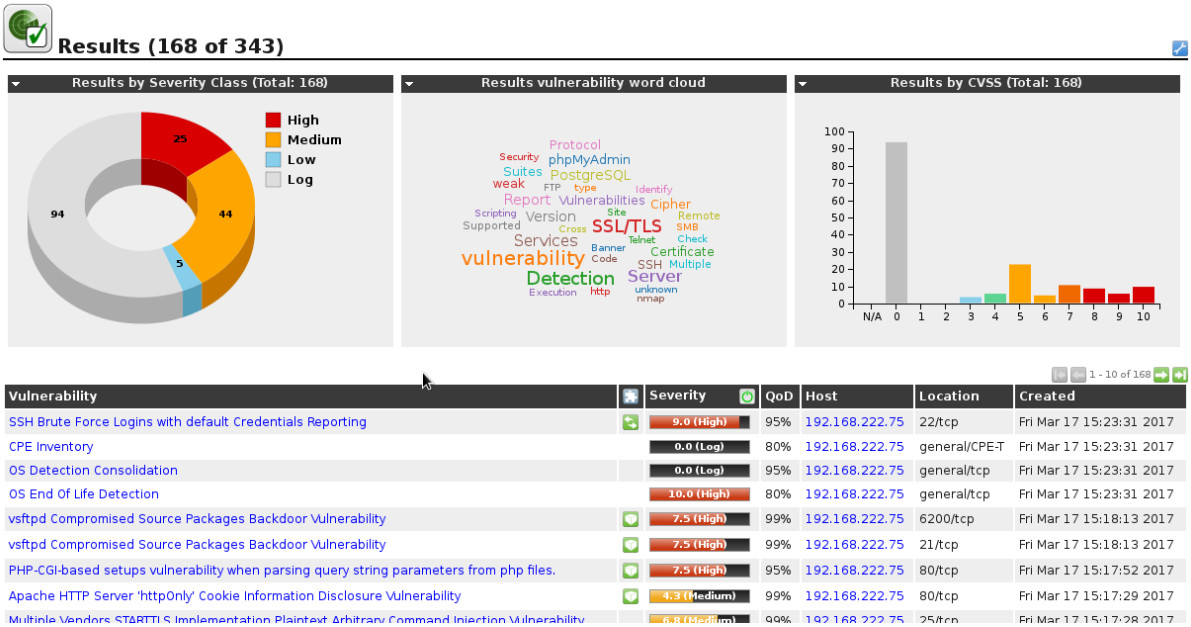
9.6.2 Results

While the reports only contain the results of one single run of a task all results are saved in the internal database and can be viewed using *Scan Management/Results*.

By default the view is sorted by the creation time of the results. But the results may be sorted by severity, QoD, solution type or host as well. Additionally powerfilters (see section *Powerfilter* (page 57)) may be used to view just the interesting results.

9.6.3 Notes

Notes allow adding comments to a Network Vulnerability Test (NVT). They will also be displayed in the reports. A Note can be added to a specific result, a specific task, a risk level, port or host and as such will only appear in specific reports. A Note can be generalized just as well so that it will be displayed in all reports.



Creating notes

To create a new note select the finding in the report you want to add a note to and click *New Note* . Alternatively you can create a note without relation to a finding. However, the GSM can not suggest any meaningful values for the different fields in the following dialogue.

A new window opens in which exactly those criteria of the selected vulnerability are pre-set.

Fig. 9.66: A new note

Individual values can be selected and unselected to generalize or the note even further or make it more specific. Additionally the note can be activated for a specific period of time. This allows adding of information to a note that a security update is uploaded in the next seven days. For the next seven days the note will be displayed in the report that the vulnerability is being worked on.

Generalizing Notes

Any note can be generalized. In this example a quite extensive generalization is configured, matching any target host, port and task.

From this moment on the note is always shown in the results view if this NVT matches.

This applies for all previously created scan reports and for all future scan reports until the note is deleted.

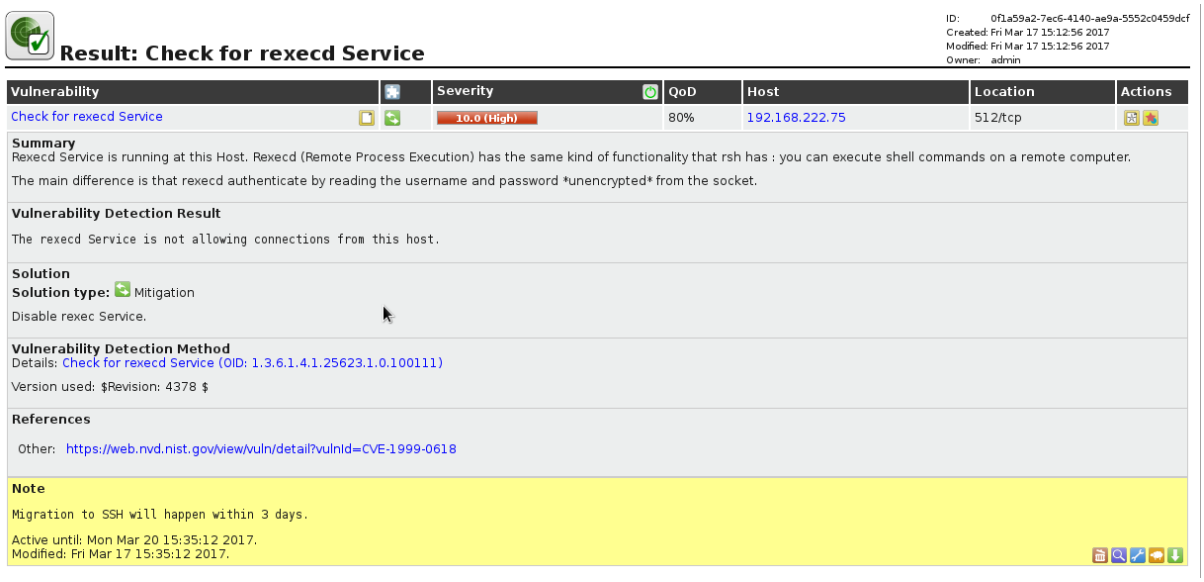


Fig. 9.67: A note in a report

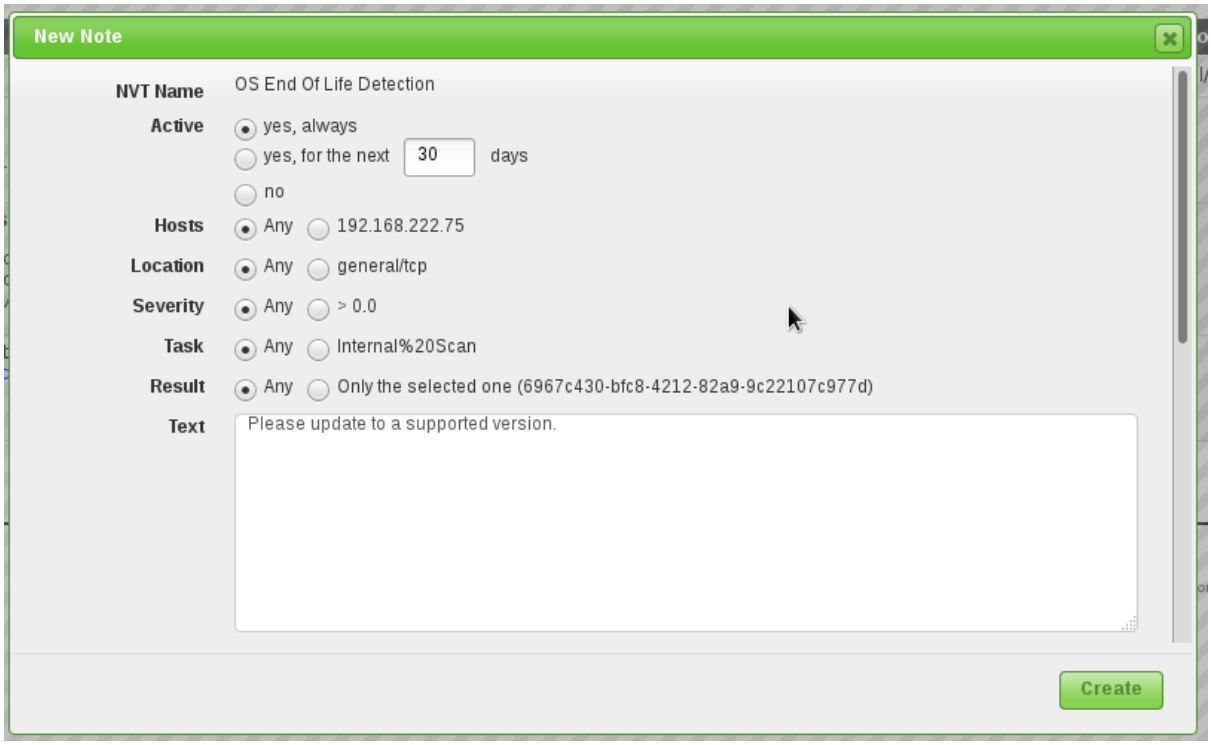


Fig. 9.68: A generalized note

Managing Notes

The created notes can be displayed under *Scan Management* and *Notes*. Here completely new notes can be added as well.

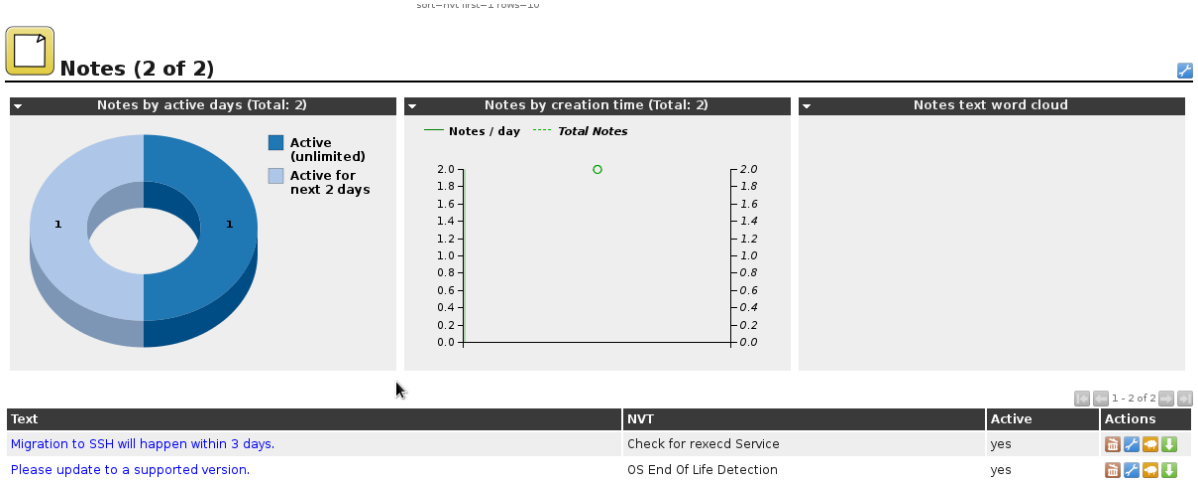


Fig. 9.69: Notes can be managed individually.

Among others it is being displayed if created notes are currently active. Additionally notes can be edited . To search for a specific note a search filter can be used respectively. This will make it easier to find a specific note when especially a great deal of notes is available. The search filter can be opened respectively end text entered appropriately or it can be entered directly into the filter window at the top. These filters can, of course, be saved for later use as well.

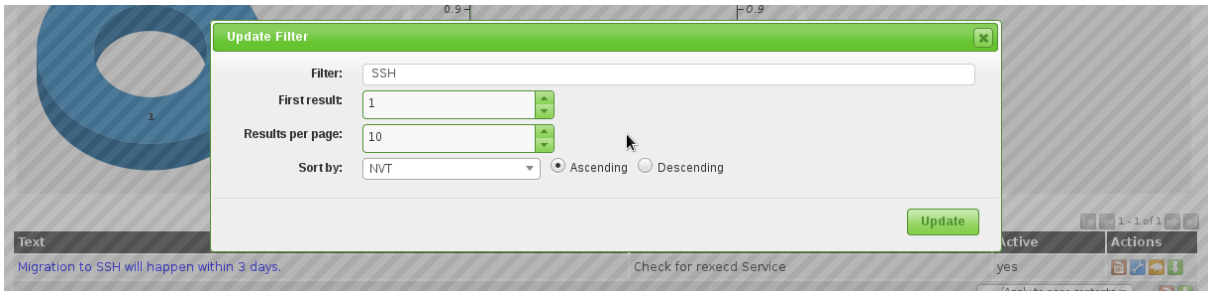


Fig. 9.70: Notes can be limited by a search filter.

9.6.4 Overrides and False Positives

The results of a report can not only be supplemented through meaningful or helpful data but the severity of the results can be modified. This is called Override by the GSM.

These overrides are especially useful to manage results that are discovered as a false positive and that have been given a critical severity but should be given a different severity (i.e. False Positive) in the future. The same is true for results that only have been given the severity Log but should be assigned a higher severity locally. These can be managed with an override as well.

The use of overrides makes also sense to manage acceptable risks. The risk of a vulnerability can be ranked new and as such the risks that, in your opinion, are not critical can be re-evaluated in the results.

What is a false positive?

A false positive is a result that describes a problem that does not exist in reality. Often vulnerability scanners find proof that point to a security issue. A final prediction is not possible, however. Two options are now available:

- Reporting of a potentially non-existent vulnerability (False Positive).
- Omission of the reporting of the potentially existing vulnerability (False Negative).

Since a user is able to recognize, manage and handle these as it is not the case with false negatives, the GSM vulnerability scanner reports all potentially existing vulnerabilities. The GSM assists with several automatic and semi-automatic to categorize them.

Note: Consider the new concept of Quality of Detection (see sections *Reading of the Reports* (page 126) and *Network Vulnerability Tests* (page 141)).

This problem is especially typical with Enterprise Linux distributions. If, for example, a SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner, that knows of a vulnerability in this version, will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If the scan administrator knows of this circumstance an override can ensure that these results are no longer being displayed.

Creating an Override

Overrides like notes can be created in different ways. The simplest way to get to this option is through the respective scan result in a report. At the top right of each finding the *Add Override* icon can be found.

Overrides have the same function as notes, however, they add the possibility to adjust the severity:

- High
- Medium
- Low
- Log
- False Positive

Vulnerabilities with the level False Positive are not being displayed in the reports. But special reports for findings of this level can be created. As with overrides they can have a time limitation.

Note: If several overrides apply to the same NVT in the same report the most recent override is actually used and applied.

Disabling and Enabling Overrides

Wherever overrides may change the display of the results, the overrides may be enabled or disabled. This may be done using the icon in the title bar.

Automatic False Positives

The GSM is able to detect false positives automatically and can assign an override automatically. However the target system must be analyzed internally and externally with an authenticated scan.

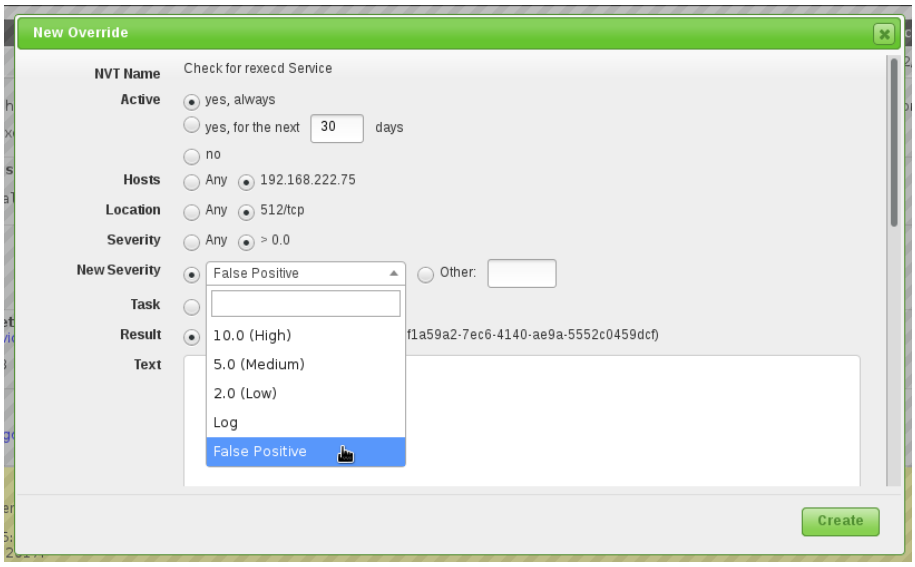


Fig. 9.71: Overrides allow for the customization of the severity level.

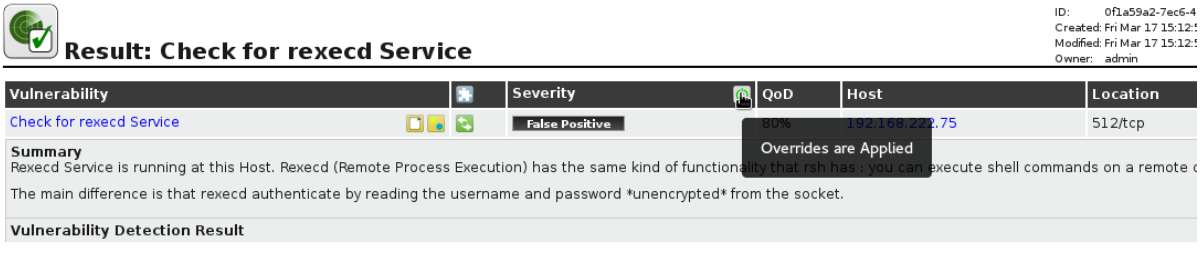


Fig. 9.72: Overrides may be enabled and disabled.

An authenticated scan can identify vulnerabilities in locally installed software. As such vulnerabilities can be identified that can be exploited by local users or are available to an attacker if he already gained local access as an unprivileged user for example. In many cases an attack occurs in different phases and an attacker exploits multiple vulnerabilities to increase his privileges.

An authenticated scan offers a second more powerful function justifying its execution. In many cases by scanning the system externally, it can not be properly identified if a vulnerability really exists. In doubt, the Greenbone Security Manager reports all potential vulnerabilities. With the authenticated scan many of these potential vulnerabilities can be recognized and filtered as false positives.

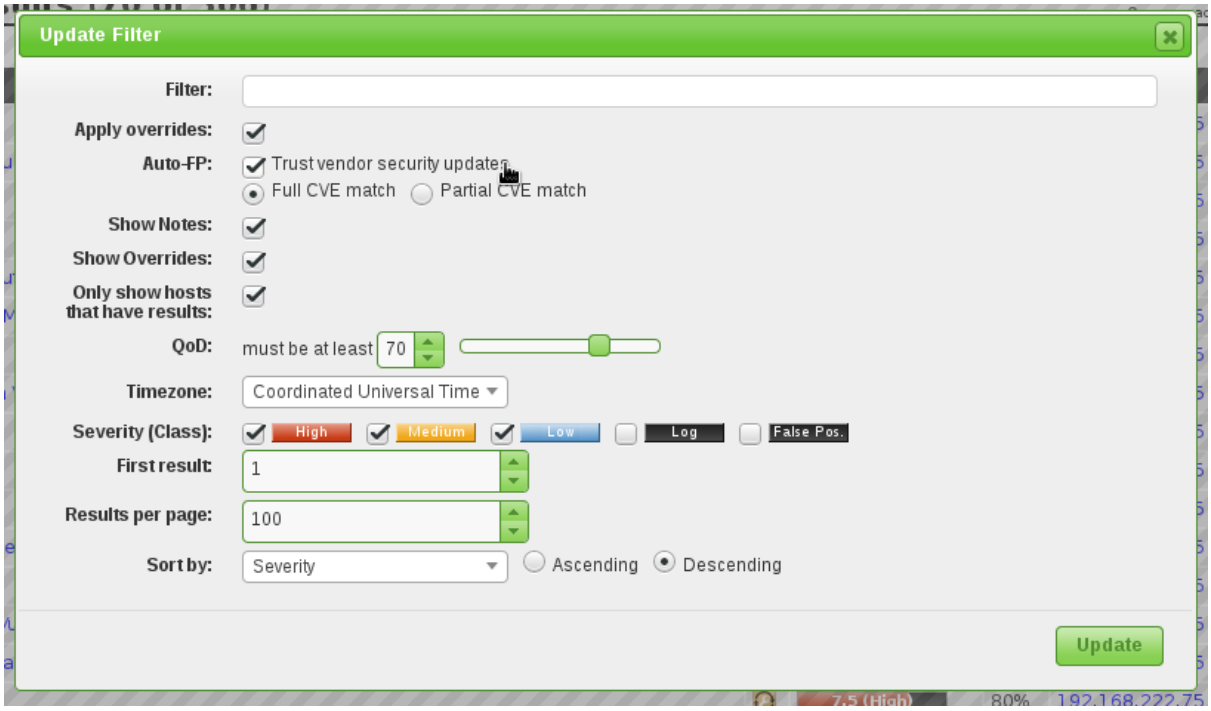


Fig. 9.73: Automatic False Positives

This problem is especially typical with Enterprise Linux distributions. If, for example, a SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner, that knows of a vulnerability in this version, will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If an authenticated scan was performed the GSM can recognize that the version 4.4-p1 is installed and no longer contains this vulnerability.

Automatic false positives are enabled with the Report-Filter function (see section *Powerfilter* (page 57)). This functionality gives the best results when using the `Partial CVE match`.

9.7 Asset Management

The GSM may store all results of all scans in the Asset-Management. When defining a task it can be determined if the results of a scan should be recorded in the asset management (see section *Creating a Task* (page 87)).

While the asset management of older GOS versions is still available (see section *Classic Asset Management* (page 136)) the new asset management offers additional features.

9.7.1 Dashboard

The dashboard provides a quick overview on the found and scanned systems including their operating systems, vulnerabilities and severities. The Dashboard may be accessed via *Assets* followed by *Dashboard*.

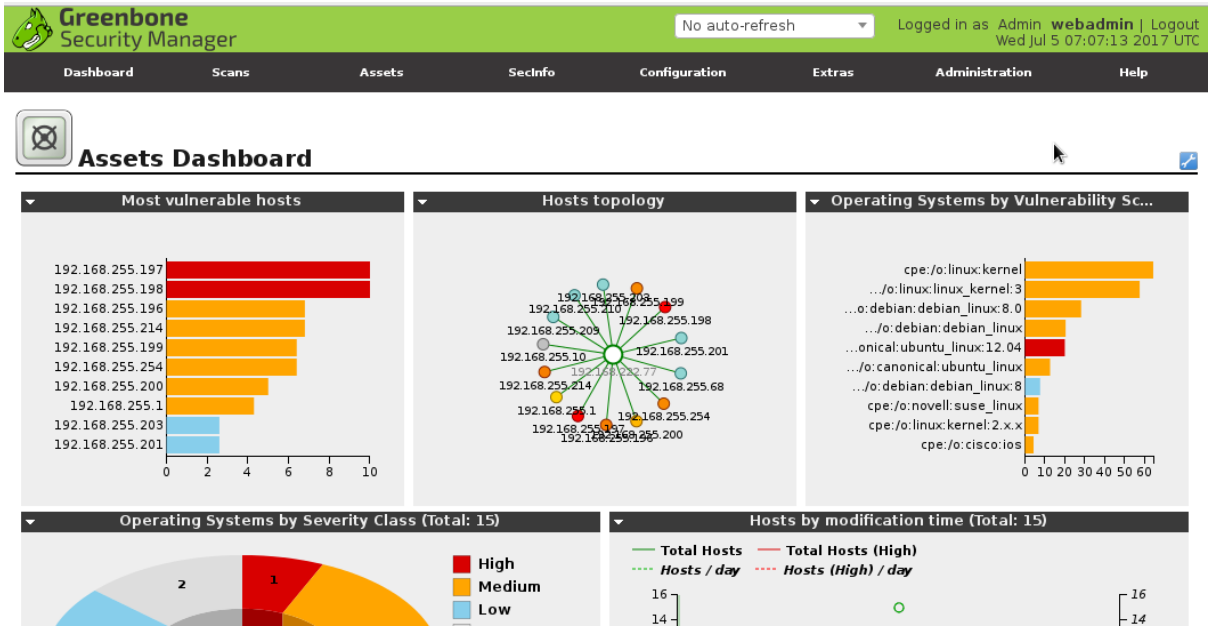


Fig. 9.74: The asset dashboard provides a quick overview on the scanned systems.

9.7.2 Hosts View

The hosts view displays all scanned hosts individually.

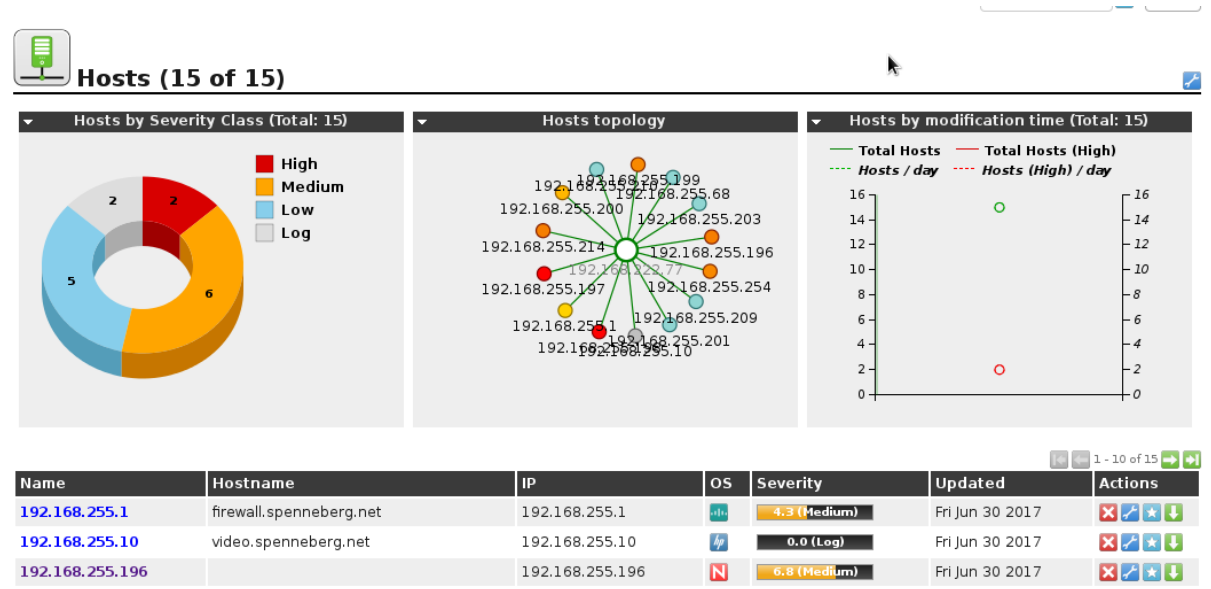


Fig. 9.75: The hosts view presents the hosts individually.

While displaying the main information on the hosts like IP addresses, hostname, operating system, and maximum severity this view may also be used to alter the stored information.

9.7.3 Modifying Hosts

The rightmost column contains four buttons allowing the following operations:

- Delete the host from the asset management
- Edit the host. Currently only comments may be added. Further options may be available in future releases.
- Create a scan target based on the asset. You will be redirected to the target creation and the hosts field will be prefilled.
- You may download the XML presentation of the asset.

The delete, create and download option are also available at the bottom of the page. These options apply then to all currently displayed hosts.

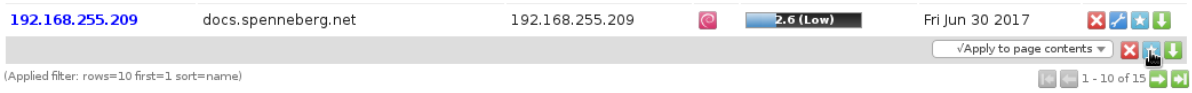


Fig. 9.76: The hosts view support the creation of targets based on the displayed hosts.

This may be used by first filtering the hosts. For example, you could create a filter to display only Microsoft Windows hosts. Then a new scan target could be defined based on the filtered hosts using the button at the bottom of the screen.

This will create a fixed set of hosts. If additional Microsoft Windows hosts show up in further scans they will not be added to the target!

9.7.4 Adding Hosts

If you want to add hosts to the asset management this is possible as well. Currently you may only provide the IP address and a comment. Further options will be added in future GOS releases.

To add a host use the button at the left top of the page. An overlay is displayed supporting the entry of the IP address and a comment.

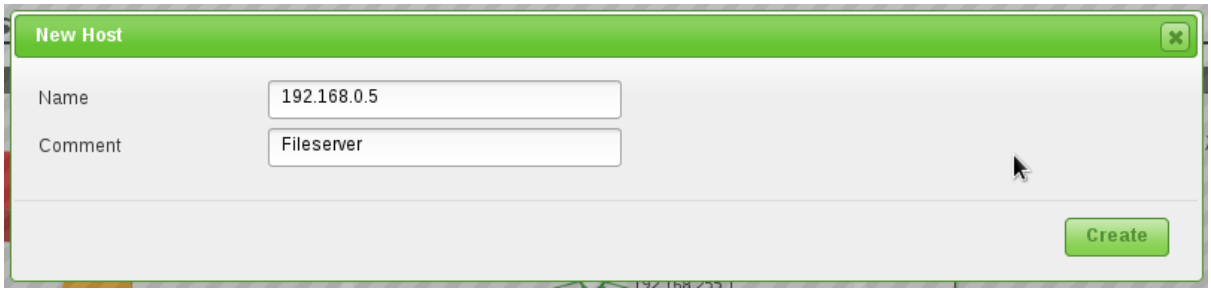


Fig. 9.77: Adding hosts is possible using the WebUI.

Of course this feature is also available via GMP (see section *GMP* (page 34)). The import of hosts from a configuration management database may be achieved using this option.

9.7.5 Host Details

When selecting a host the host details are displayed. These include:

- Comment
- IP address

- Hostname
- Operating System
- Route
- Maximum Severity

Additionally the identifiers of the system are displayed. Especially SSH keys and X.509 certificates will be presented.

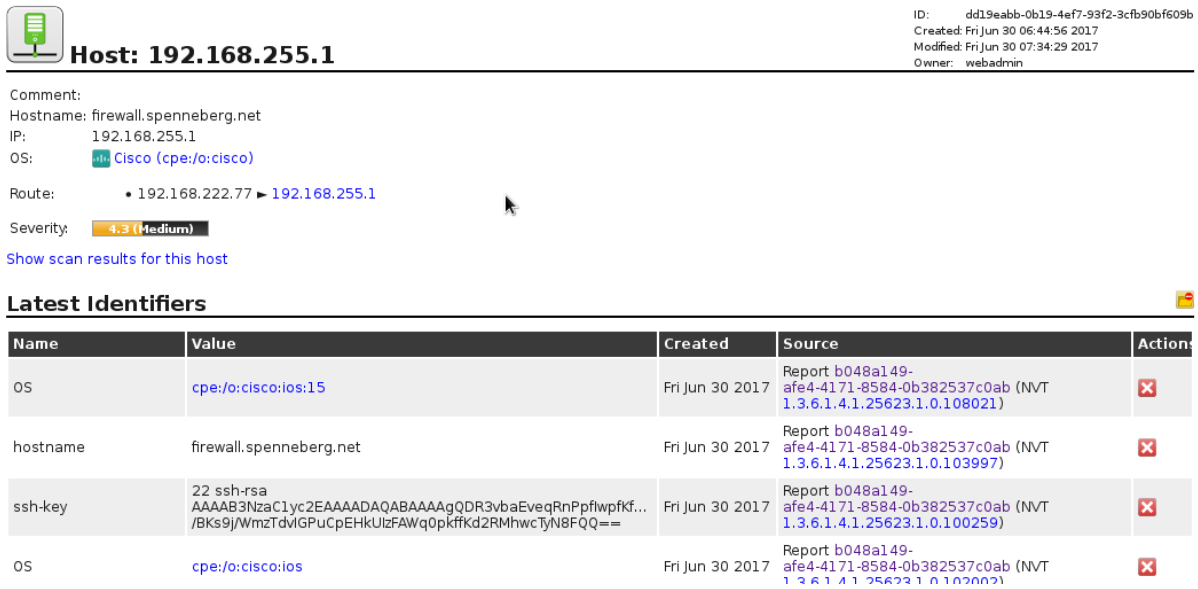


Fig. 9.78: The hosts details present the identifiers of the host.

Operating Systems View

The operating systems view within the asset management provides a different view on the stored data. While the hosts view is centered on the individual hosts this view concentrates on the used operating systems.

This view provides the average maximum severity of all hosts using the same OS and adds the latest and highest severity as well to the picture.

By selecting an operating system you can directly access the hosts using the OS.

Classic Asset Management

The classic asset management can be accessed via *Assets* followed by *Hosts (Classic)*.

Here you can see how many security holes were discovered on the systems. In addition the overview displays the operating system with a logo (OS column) and the discovered ports and applications. Also it is being displayed how a scan of the system would possible turn out in this moment (Prognosis column, see also section *Prognosis* (page 139)). Via the a prognostic report can be created as well. Through the asset management you can always access the last report of the host. The date of the report is visible and can be accessed directly by clicking on the link. If multiple reports exist older reports can be accessed in the host details. By clicking on the host IP address the host details can be accessed. Here the amount of discovered vulnerabilities, the identified operating system, the discovered ports and the amount of detected applications on the system can be viewed

The host details contain additional information of the system:

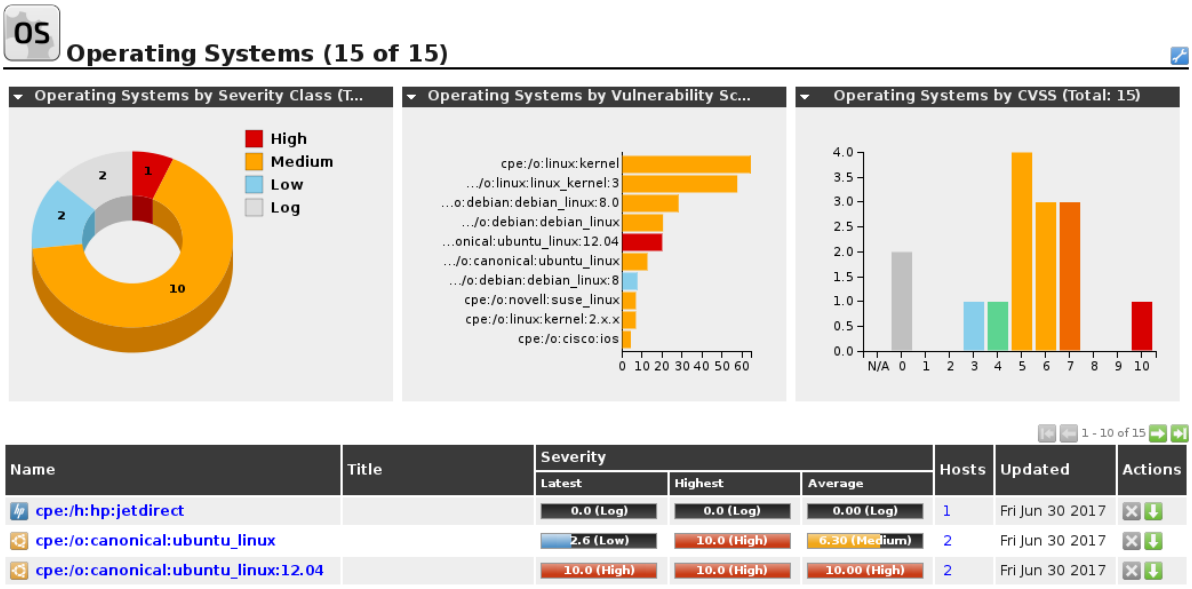


Fig. 9.79: The OS view clusters the operating systems.

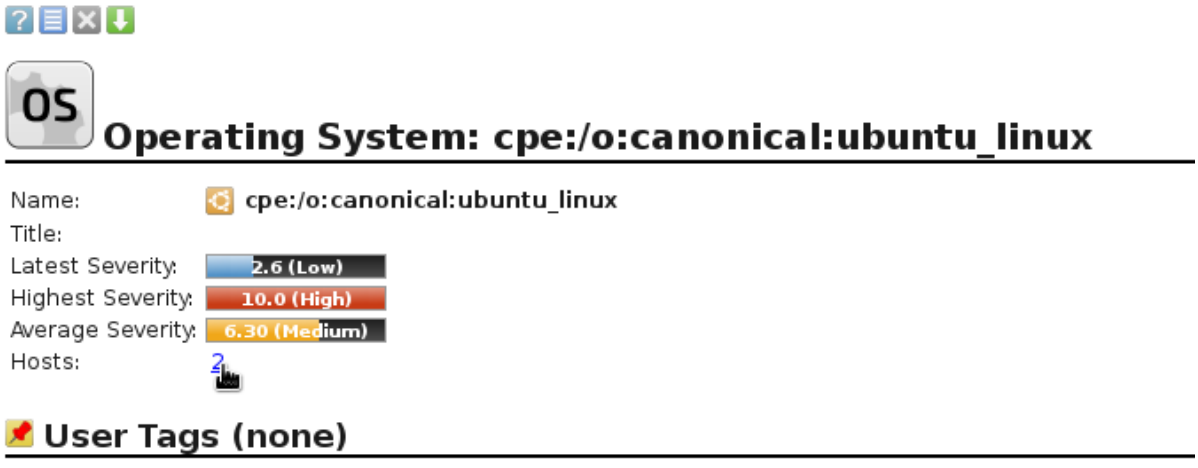


Fig. 9.80: From the OS details the hosts using the OS may be displayed.

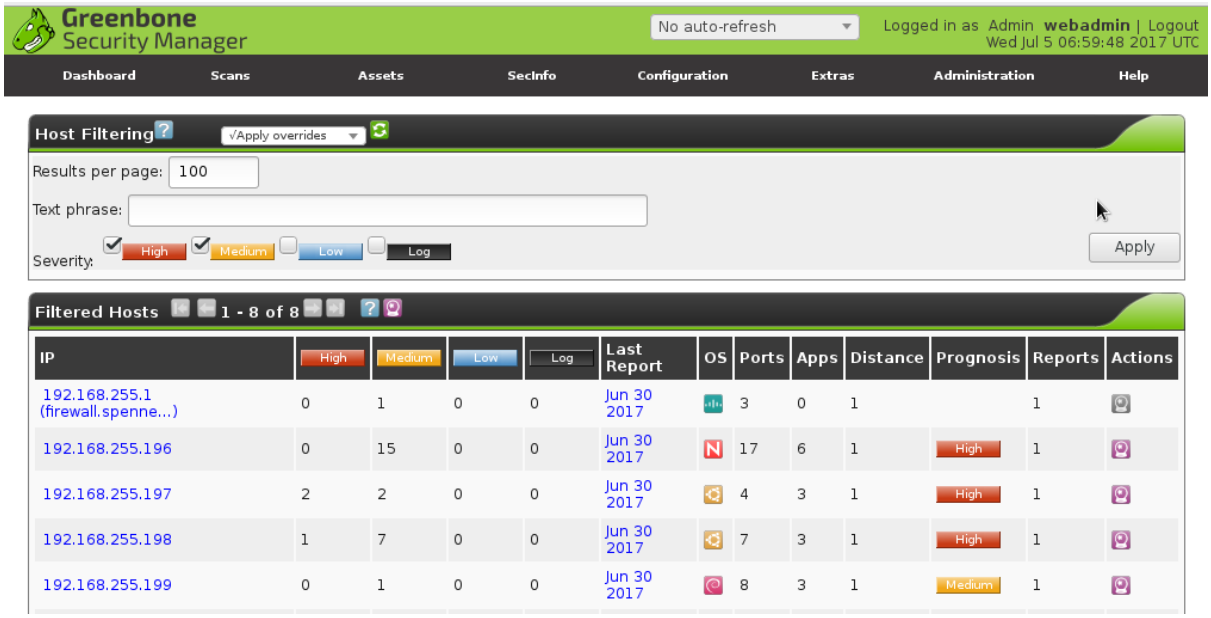


Fig. 9.81: The asset database displays the stored systems.

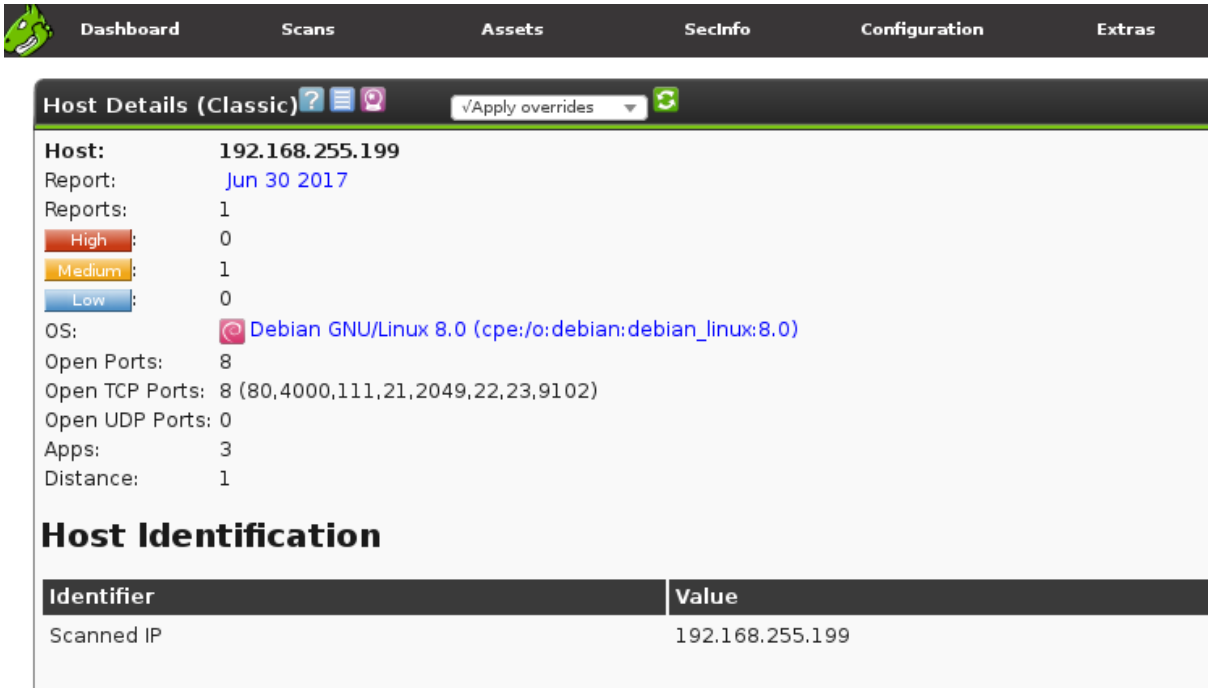


Fig. 9.82: The host details contain further information on the host.

Hardware: The GSM stores information about the hardware. If known then the MAC address is listed here. It can only be displayed though if the target system is on the same LAN as the GSM.

Detected Applications: Especially of interest are the detected applications. With this the Greenbone Security Manager can give a prognosis based on its SecInfo database without re-scanning if additional security risks would be found. This is especially of interest for systems that currently do not have any vulnerability and new scans are not being performed regularly.

9.7.6 Prognosis

The prognosis allows to forecast possible security risks without a new scan based on current information about known security holes from the *SecInfo Management* (SCAP, Security Content Automation Protocol) (see chapter *SecInfo Management* (page 139)). This is especially interesting for environments where by the use of the GSM most vulnerabilities have been removed or remediated. Of course new vulnerabilities are being discovered daily. Not every vulnerability justifies a new scan of the network or of individual systems. Due to the fact that the GSM has this information, based on the knowledge of the detected applications it can make a prognosis which security risks exist. If security risks become known it justifies the actual running of a scan to verify the prognosis. For this the asset database requires current data of course. This is why a scan of the systems should occur regularly in weekly or monthly intervals.

A prognostic scan can be performed as well. It will determine probable existing vulnerabilities

9.8 SecInfo Management

The *SecInfo Management* offers central access to different information relating to IT-Security. This includes the following information:

NVTs: These are the Network Vulnerability Tests. These tests test the target system for potential vulnerabilities.

CVEs: The Common Vulnerability and Exposures are vulnerabilities published by vendors and security researchers.

CPEs: The Common Platform Enumeration offers standardized names of the products that are being used information technology.

OVAL Definition: The Open Vulnerability Assessment Language offers a standardized language for the testing of vulnerabilities. OVAL definitions use this language to concretely discover vulnerabilities.

CERT-Bund Advisories: The CERT-Bund Advisories are published by the emergency response team[8] of the Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik, abbreviated as BSI). The main task of the CERT-Bund is the operation of a warning and information service publishing information regarding new vulnerabilities and security risks as well as threats for IT systems.

DFN-CERT Advisories: The DFN-CERT[9] is the emergency response team of the German Research Network (German: Deutsches Forschungsnetz, abbreviated as DFN).

The CVEs, CPEs and OVAL definitions are published and made accessible by NIST as part of the National Vulnerability Database (NVD) (see also section *Security Content Automation Protocol (SCAP)* (page 141)).

To get a quick overview over this information the Secinfo dashboard (see figure *The SecInfo Dashboard allows displaying data graphically.* (page 140)) exists. It allows for the graphical display of different information grouped by different aspects.

[8] https://www.cert-bund.de/
[9] https://www.cert.dfn.de/

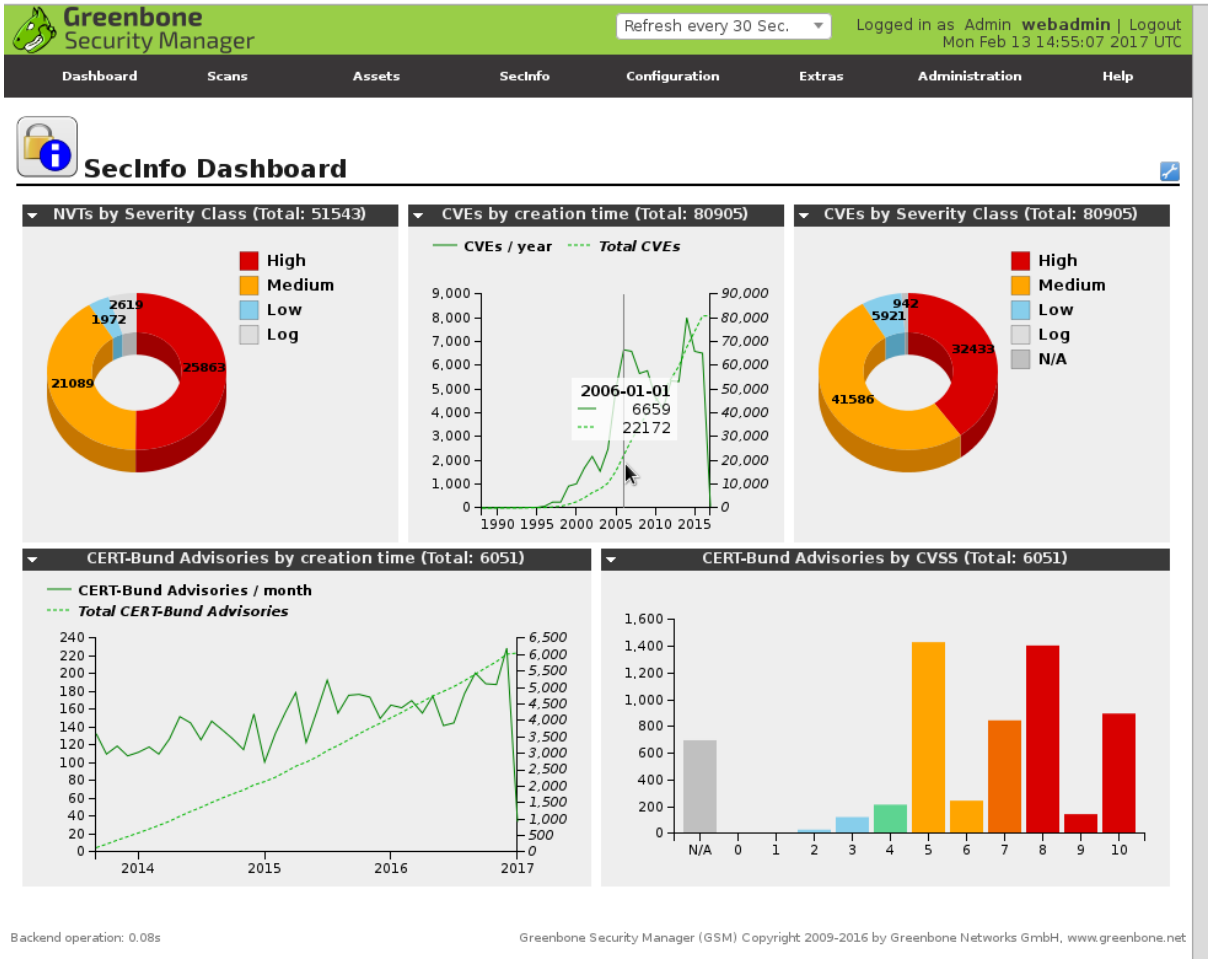


Fig. 9.83: The SecInfo Dashboard allows displaying data graphically.

9.8.1 SecInfo Portal

SecInfo Data is being provided by Greenbone Networks online as well. This portal[10] can be accessed directly through the Internet. It corresponds to data that can be displayed in the GSM as well. The SecInfo Portal is a GSM ONE that has been configured especially for anonymous guest access. Contrary to a full-fledged GSM only the SecInfo management and the CVSS online calculator are available for the guest user.

The SecInfo portal achieves a multitude of functions:

- Anonymous access to details of the Greenbone vulnerability tests as well as SCAP data (CVE, CPE, OVAL) and messages of different CERTs. The data itself is referenced thus offering the possibility to browse by Security-Information regarding a product, a vendor or a specific vulnerability.
- Demo of the respective upcoming version of the Greenbone OS as soon as the SecInfo section reached beta status.
- Service for embedded diagrams as they are used on the Greenbone website for feed statistics for example.
- Service for direct links to details or specific selections, for example for a specific CVE (CVE-2014-0160, *Heartbleed*) or an overview: All published CVE notices in 2013.
- Service for links to CVSS vulnerability rating including CVSS online calculator: AV:N/AC:L/Au:N/C:P/I:P/A:P
- Example of how a GSM can be configured by yourself on an Intranet to allow direct links in internal reports and platforms.

Such access can be provided yourself by activating guest access (see section *Guest Log in* (page 69))

9.8.2 Network Vulnerability Tests

The abbreviation NVT stands for Network Vulnerability Test. These are test routines the GSM utilizes and that are updated regularly with the Greenbone Security Feed. Here you can find information when the test was developed, which systems are affected, what impact the vulnerabilities have and how they can be remediated.

Compared to the Greenbone OS 3.0 there are two new pieces of information, the Solution Type (see *Solution Type* (page 275)) and the Quality of Detection (QoD, see *Quality of Detection (QoD)* (page 273)).

With the introduction of the QoD the parameter `Paranoid` in the scan configuration (see chapter *Scan Configuration* (page 111)) is being removed without replacement. In the past a scan configuration without this parameter only used NVTs with a QoD of a minimum of 70%. Only with this parameter all NVTs were used. Now all NVTs are being used and executed in a scan configuration. The filtering of the results is done on based on QoD. That way all the results are always available in the database and can be turned on or off respectively.

9.8.3 Security Content Automation Protocol (SCAP)

The National Institute of Standards and Technology (NIST) in the USA provides the National Vulnerability Database[11] (NVD). NVD is a data repository for the vulnerability management of the US government. The goal is the standardized provision of the data for the automated processing and support for the function of vulnerability management and the implementation of compliance guide lines. The NVD provide different databases. They include

- check lists
- vulnerabilities

[10] https://secinfo.greenbone.net
[11] https://nvd.nist.gov/

- misconfigurations
- products
- threat metrics

For this the NVD utilizes the Security Content Automation Protocol[12] (SCAP). The Security Content Automation Protocol is a combination of different interoperable standards. Many standards were developed or derived from public discussion. The public participation of the community in the development is an important aspect for accepting and spreading of the SCAP standards. The SCAP protocol is currently specified in version 1.2 and includes the following components:

- Languages
  - XCCDF: The Extensible Configuration Checklist Description Format
  - OVAL: Open Vulnerability and Assessment Language
  - OCIL: Open Checklist Interactive Language
  - Asset Identification
  - ARF: Asset Reporting Format
- Collections
  - CCE: Common Configuration Enumeration
  - CPE: Common Platform Enumeration
  - CVE: Common Vulnerabilities and Exposure
- Metrics:
  - CVSS: Common Vulnerability Scoring System
  - CCSS: Common Configuration Scoring System
- Integrity
  - TMSAD: Trust Model for Security Automation Data

OVAL, CCE, CPE and CVE are trademarks of NIST.

The Greenbone vulnerability scanner uses the OVAL standard, CVE, CPE and CVSS. By utilizing these standards the interoperability with other systems is guaranteed. These standards also allow comparing of the results.

Vulnerability scanners such as the Greenbone Security Manager can be validated by NIST respectively. The Greenbone Security Manager has been validated with respect to SCAP version 1.0[13].

Following, the standards utilized by the Greenbone Security Manager are being covered in more detail.

CVE

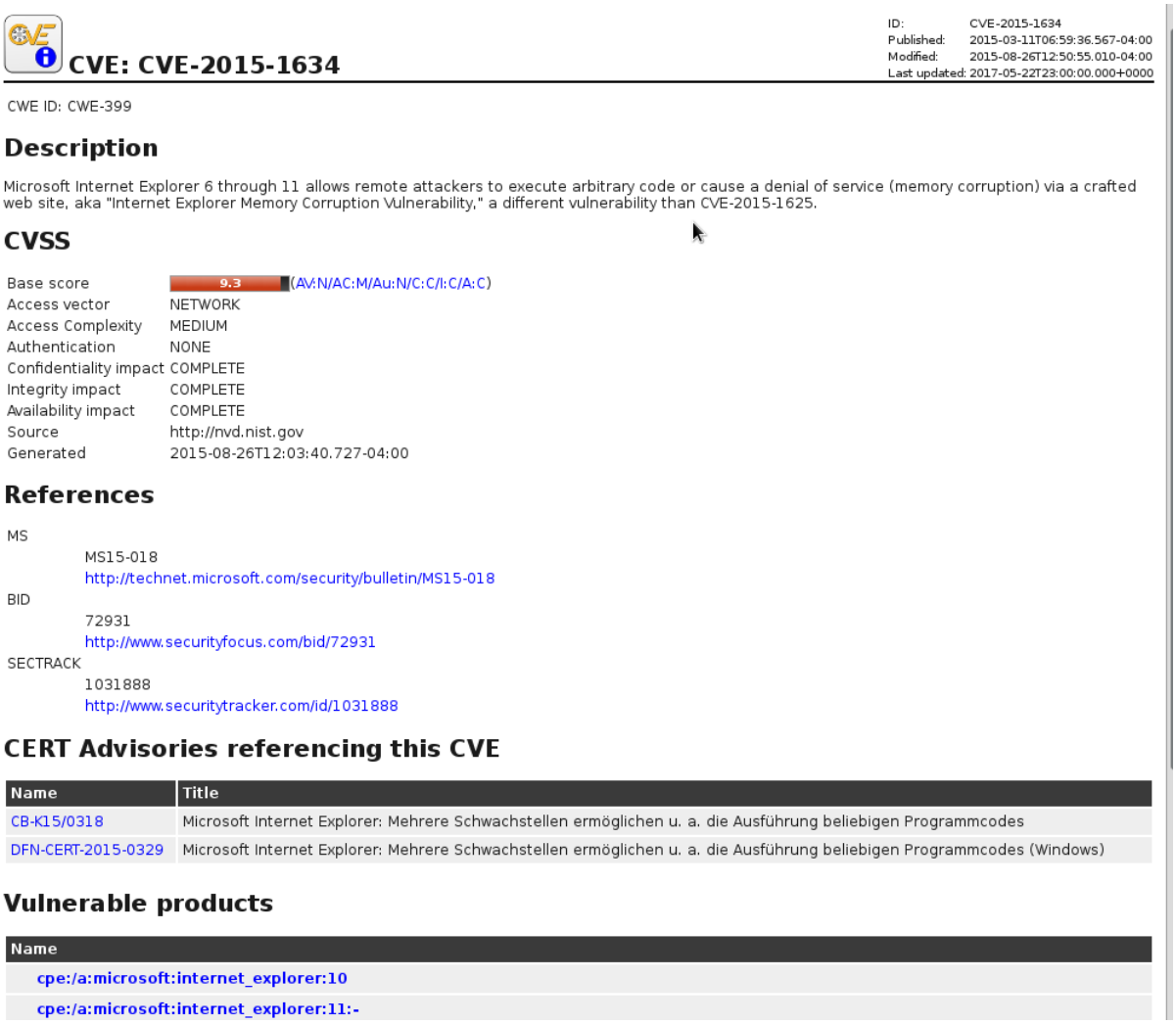
Due to the fact that in the past often multiple organizations discovered and reported vulnerabilities at the same time and assigned them different names, communication and comparison of the results was not easy. Different scanners reported the same vulnerability under different names. As a matter of fact instead of two different vulnerabilities it was actually the same vulnerability.

To address this, MITRE [15], sponsored by the US-CERT, founded the CVE project in 1999. Every vulnerability is assigned a unique identifier consisting of the year and a simple number. This number then serves as central reference.

[12] http://scap.nist.gov/

[13] https://nvd.nist.gov/scapproducts.cfm

[15] MITRE (Massachusetts Institute of Technology Research & Engineering) Corporation is an organization for the management of research institutions for the United States government that was formed by splitting off from the Massachusetts Institute of Technology (MIT).



CVE: CVE-2015-1634

ID: CVE-2015-1634
Published: 2015-03-11T06:59:36.567-04:00
Modified: 2015-08-26T12:50:55.010-04:00
Last updated: 2017-05-22T23:00:00.000+0000

CWE ID: CWE-399

Description

Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1625.

CVSS

Base score	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Access vector	NETWORK
Access Complexity	MEDIUM
Authentication	NONE
Confidentiality impact	COMPLETE
Integrity impact	COMPLETE
Availability impact	COMPLETE
Source	http://nvd.nist.gov
Generated	2015-08-26T12:03:40.727-04:00

References

MS
MS15-018
http://technet.microsoft.com/security/bulletin/MS15-018
BID
72931
http://www.securityfocus.com/bid/72931
SECTRACK
1031888
http://www.securitytracker.com/id/1031888

CERT Advisories referencing this CVE

Name	Title
CB-K15/0318	Microsoft Internet Explorer: Mehrere Schwachstellen ermöglichen u. a. die Ausführung beliebigen Programmcodes
DFN-CERT-2015-0329	Microsoft Internet Explorer: Mehrere Schwachstellen ermöglichen u. a. die Ausführung beliebigen Programmcodes (Windows)

Vulnerable products

Name
cpe:/a:microsoft:internet_explorer:10
cpe:/a:microsoft:internet_explorer:11:-

Fig. 9.84: The CVEs include information regarding the severity and affected products.

The CVE database of MITRE is not a vulnerability database. CVE was developed in order to connect the vulnerability database and other systems with each other. This allows for the comparison of security tools and services. This is why the CVE database does not contain any information regarding risk, impact or remediation of the vulnerability. Detailed technical information is also not included. A CVE only contains the identification number with status, a short description and references to reports and advisories.

The National Vulnerability Database (NVD) refers to MITRE's CVE database and supplements this information with information in regards to remediation of the vulnerability, the severity, affected products and possible impact. Greenbone refers to the CVE database of the NVD so that information is included. At the same time does the GSM combine the information with the NVTs and the CERT-Bund and DFN-CERT advisories.

This information can be displayed comfortably in the web interface.

CPE

The abbreviation CPE stands for Common Platform Enumeration, modelled after CVE and started by MITRE as well, as an industry standard for a common naming convention for information technology systems. Hereby common naming exists for operating systems and applications allowing for global referencing.

Originally the Common Platform Enumeration (CPE) was initiated by MITRE. Today the CPE standard is maintained by the US American National Institute for Standards and Technology NIST as part of the National Vulnerability Database (NVD). NIST already had maintained the official CPE dictionary and the CPE specifications for many years. CPE is a structured naming schema for applications, operating systems and hardware devices. It is based on the generic syntax of the Uniform Resource Identifier (URI).

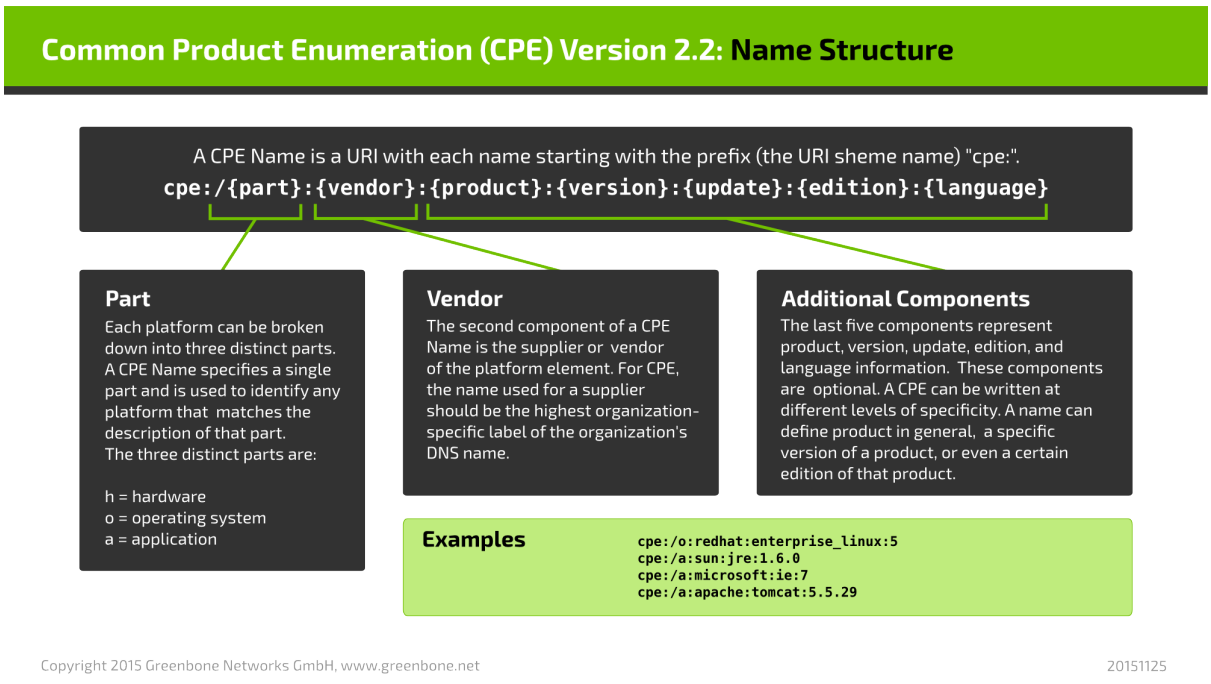


Fig. 9.85: Common Product Enumeration: Name Structure

Due to the fact that the CPE standard is closely tied to the CVE standard, their combination allows for conclusion of existing vulnerabilities when discovering a platform or product.

CPE is composed of the following components:

Naming: The name specification describes the logical structure of well-formed names (WFNs), its binding to URIs and formatted character strings and the conversion of the WFNs and their bindings.

Name Matching: The name matching specification describes the methods to compare WFNs with each other. This allows for the testing if some or all refer to the same product.

Dictionary: The dictionary is a repository of CPE names and meta data. Every name defines an single class of an IT product. The dictionary specification describes the processes for the use of the dictionary, like the search for a specific name or entries, which belong to a more general class.

Applicability Language: The applicability language specification describes the creation of complex logical expressions with the help of the WFNs. These applicability statements can be used for the tagging of check lists, guide lines or other documentation and as such describe for which products these documents are relevant for.

OVAL

The Open Vulnerability and Assessment Language is also a Mitre project. It is a language to describe vulnerabilities, configuration settings (compliance), patches and applications (inventory). The XML based definitions allow for simple processing by automated systems. As such the OVAL definition `oval:org.mitre.oval:def:22127` of the inventory class describes the Adobe Flash Player 12 while the OVAL definition `oval:org.mitre.oval:def:22272` describes a vulnerability of Google Chrome under Windows.

OVAL Definition: oval:org.mitre.oval:def:22272

ID: oval:org.mitre.oval:def:22272
Created: 2014-02-03T12:56:06Z
Modified: 2014-03-17T08:00:17Z

Title:	Vulnerability in Google Chrome before 32.0.1700.76 on Windows allows attackers to trigger a sync with an arbitrary Google account by leveraging improper handling of the closing of an untrusted signin confirm dialog
Version:	4
Definition class:	vulnerability
Referenced CVEs:	1
Severity:	7.5
File:	oval/5.10/org.mitre.oval/v/family/windows.xml

Description

The OneClickSigninBubbleView::WindowClosing function in browser/ui/views/sync/one_click_signin_bubble_view.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows attackers to trigger a sync with an arbitrary Google account by leveraging improper handling of the closing of an untrusted signin confirm dialog.

Affected

Family: windows

Type	Name
platform	Microsoft Windows 2000
platform	Microsoft Windows XP
platform	Microsoft Windows Server 2003
platform	Microsoft Windows Server 2008
platform	Microsoft Windows Server 2008 R2
platform	Microsoft Windows Vista
platform	Microsoft Windows 7
platform	Microsoft Windows 8
platform	Microsoft Windows 8.1
platform	Microsoft Windows Server 2012
platform	Microsoft Windows Server 2012 R2
product	Google Chrome

Criteria

- Google Chrome is installed (oval:org.mitre.oval:def:11914)

Fig. 9.86: OVAL describes the discovery of vulnerabilities.

These OVAL definitions are created made available in XML and describe the discovery of individual systems and vulnerabilities. The above mentioned OVAL definition 22272 has the following structure:

```
<definition id="oval:org.mitre.oval:def:22272" version="4" class="vulnerability">
  <metadata>
    <title>Vulnerability in Google Chrome before 32.0.1700.76 on Windows allows
           attackers to trigger a sync with an arbitrary Google account by
           leveraging improper handling of the closing of an untrusted signin
           confirm dialog</title>
    <affected family="windows">
      <platform>Microsoft Windows 2000</platform>
      <platform>Microsoft Windows XP</platform>
      <platform>Microsoft Windows Server 2003</platform>
      <platform>Microsoft Windows Server 2008</platform>
      <platform>Microsoft Windows Server 2008 R2</platform>
      <platform>Microsoft Windows Vista</platform>
      <platform>Microsoft Windows 7</platform>
      <platform>Microsoft Windows 8</platform>
      <platform>Microsoft Windows 8.1</platform>
      <platform>Microsoft Windows Server 2012</platform>
      <platform>Microsoft Windows Server 2012 R2</platform>
      <product>Google Chrome</product>
    </affected>
    <reference source="CVE" ref_id="CVE-2013-6643"
     ref_url="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6643"/>
    <description>The OneClickSigninBubbleView::WindowClosing function in
      browser/ui/views/sync/one_click_signin_bubble_view.cc in Google
      Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac
      OS X and Linux allows attackers to trigger a sync with an arbitrary
      Google account by leveraging improper handling of the closing of an
      untrusted signin confirm dialog.</description>
    <oval_repository>
      <dates>
        <submitted date="2014-02-03T12:56:06">
          <contributor organization="ALTX-SOFT">Maria Kedovskaya</contributor>
        </submitted>
        <status_change date="2014-02-04T12:25:48.757-05:00">DRAFT</status_change>
        <status_change date="2014-02-24T04:03:01.652-05:00">INTERIM</status_change>
        <status_change date="2014-03-17T04:00:17.615-04:00">ACCEPTED</status_change>
      </dates>
      <status>ACCEPTED</status>
    </oval_repository>
  </metadata>
  <criteria>
    <extend_definition comment="Google Chrome is installed"
     definition_ref="oval:org.mitre.oval:def:11914"/>
    <criteria operator="AND" comment="Affected versions of Google Chrome">
      <criterion comment="Check if the version of Google Chrome is greater than
        or equals to  32.0.1651.2" test_ref="oval:org.mitre.oval:tst:100272"/>
      <criterion comment="Check if the version of Google Chrome is less than
        or equals to  32.0.1700.75" test_ref="oval:org.mitre.oval:tst:99783"/>
    </criteria>
  </criteria>
</definition>
```

This information are being processed graphically by the web interface and presented easily readable (see figure *OVAL describes the discovery of vulnerabilities.* (page 145)).

CVSS

A big problem for regular administrators is the interpretation of vulnerability with their own environment. How critical does he have to rate a vulnerability? To support personnel that do not work with

the analysis and rating of vulnerabilities constantly the Common Vulnerability Scoring System (CVSS) was invented. CVSS is an industry standard for the description of the severity of security risks in computer systems. In the CVSS security risks are rated and compared using different criteria. This allows for the creation of a priority list of counter measures.

The CVSS score is continuously improved upon. Currently in general the CVSS score version 2 is being used. Version 3 is being developed by the CVSS Special Interest Group (CVSS-SIG) of the Forum of Incident Response and Security Teams[14] (FIRST).

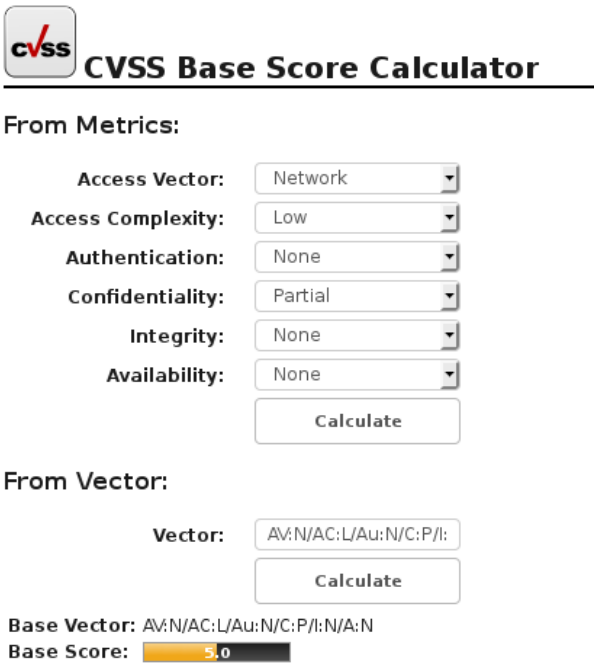


Fig. 9.87: The CVSS calculator allows for the calculation of scores conveniently.

The CVSS score in version 2 supports Base Score Metrics, Temporal Score Metrics and Environmental Score Metrics.

The Base Score Metrics in general test the exploitability of a vulnerability and their impact on the target system. Hereby access, complexity and requirement of authentication are rated. At the same time they rate if the confidentiality, integrity or availability is threatened.

The Temporal Score Metrics test if completed example code exists, the vendor already supplied a patch and confirmed the vulnerability. The score will be changing drastically in the course of time.

The Environmental Score Metrics review if control damage has to be suspected, the target distribution, and if confidentiality, integrity of availability is required. This assessment is strongly depended on the environment in which the vulnerable product is being used.

Since the Base Score Metrics are merely meaningful in general and can be determined permanently the GSM provides them as part of the SecInfo data.

Hereby the following formula is being used and can be calculated with the CVSS calculator of the GSM as well (*Extras/CVSS-Calculator*, see figure *The CVSS calculator allows for the calculation of scores conveniently.* (page 147)).

$$BaseScore = roundTo1Decimal(((0.6 * Impact) + (0.4 * Exploitability) - 1.5) * f(Impact))$$

Hereby the impact is calculated as follows:

$$Impact = 10.41 * (1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 - AvailImpact))$$

[14] https://www.first.org/cvss

The exploitability is calculated as:

$$Exploitability = 20 * AccessVector * AccessComplexity * Authentication$$

The function $f(Impact)$ is 0, if the impact is 0. In all other cases the value is 1.176. The other values are constants:

- Access Vector
  - requires local access: 0.395
  - adjacent network accessible: 0.646
  - network accessible: 1.0
- Access Complexity:
  - high: 0.35
  - medium: 0.61
  - low: 0.71
- Authentication
  - requires multiple instances of authentication: 0.45
  - requires single instance of authentication: 0.56
  - requires no authentication: 0.704
- ConfImpact:
  - none: 0.0
  - partial: 0.275
  - complete: 0.660
- IntegImpact
  - none: 0.0
  - partial: 0.275
  - complete: 0.660
- AvailImpact
  - none: 0.0
  - partial: 0.275
  - complete: 0.660

9.8.4 DFN-CERT

While the individual NVTs, CVEs, CPEs and OVAL definitions are being created primarily for processing by computer systems, the DFN-CERT publishes, like many other Computer Emergency Report Teams (CERTs), new advisories regularly.

The DFN-CERT is responsible for hundreds of universities and research institutions that are associated with the German Research Network (German: Deutsches Forschungsnetz, abbreviated as DFN). An Advisory describes especially critical security risks that require fast reacting. These are being obtained by the GSM as well and stored to the database for reference. They can be displayed directly as well.

9.8.5 CERT-Bund

CERT-Bund offers a warning and information service (German: Warn- und Informationsdienst, abbreviated as WID). Currently this service offers two different types of Information (Excerpt from the website https://www.cert-bund.de/):

Advisories: This information service is only available to federal agencies as a closed list! The advisories describe current information about security critical incidents in computer systems and detailed measures to remediate security risks.

Short Information: Short information features the short description of current information regarding security risks and vulnerabilities. Please note that information sometimes is not verified and under some circumstances could be incomplete or even inaccurate.

The Greenbone Security Feed contains the CERT-Bund Short Information. They can be identified by the K in the message (`CB-K14/1296`).

CHAPTER 10

Reports

The GSM saves all reports of all scans in a local database. Not only is the last report of a scan saved but all reports of all scans ever run. This allows also access to information from the past. The reports contain the discovered vulnerabilities and information of a scan (see section *Reports and Vulnerability Management* (page 124)).

If a scan has been performed multiple times the trend of discovered vulnerabilities will be displayed. However, the trend information can not be found on the report page but under *Scan Management/Tasks*.

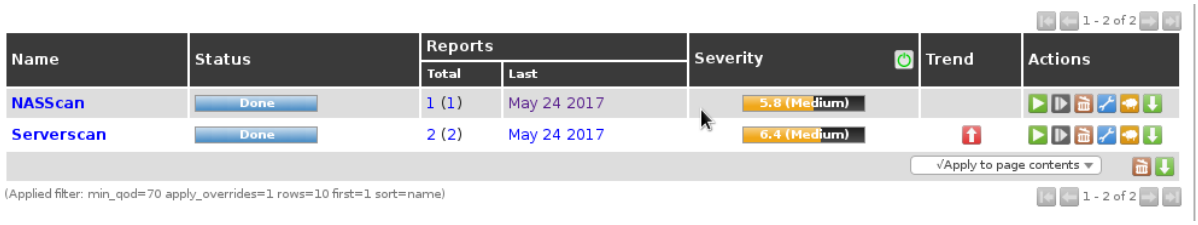


Fig. 10.1: The trend of discovered vulnerabilities can be found in the respective column in the task overview.

In this view only reports of a specific scan can be accessed. To do so use the column Reports/Total (see figure *The Reports column contains the amount of reports saved in total and the date of the last report.* (page 151)).

Fig. 10.2: The Reports column contains the amount of reports saved in total and the date of the last report.

Here you can find the date of the last saved report as well as the amount of reports available in total. The first value represents the number of all completed scans and the second the amount of reports including the not yet completed ones. By clicking on one of the values you will get a list of the respective reports. By clicking on the date the latest report will be displayed.

10.1 Delta Reports

If more than one report of a task can be displayed (see *Now, for comparison the second report needs to be selected.* (page 152)) a Delta-Report can be created. Use the compare option in the Action column. The first report is being selected for comparison.

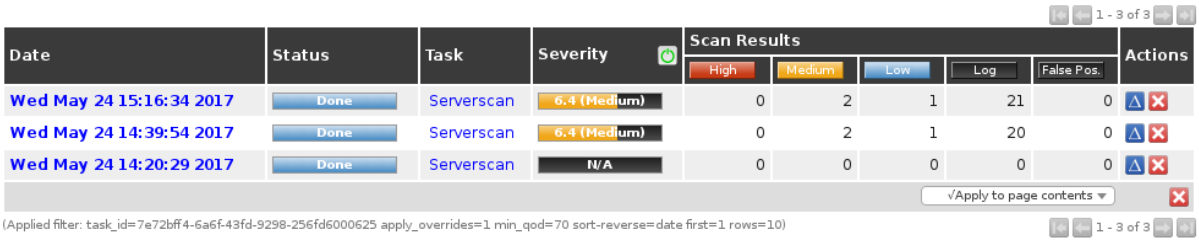


Fig. 10.3: Two reports of the same task can be compared in a delta report.

Afterwards the respective icon is greyed out for the selected report. The compare icons of the other reports have now changed in their appearance. Use the icon to select the second report for comparison.

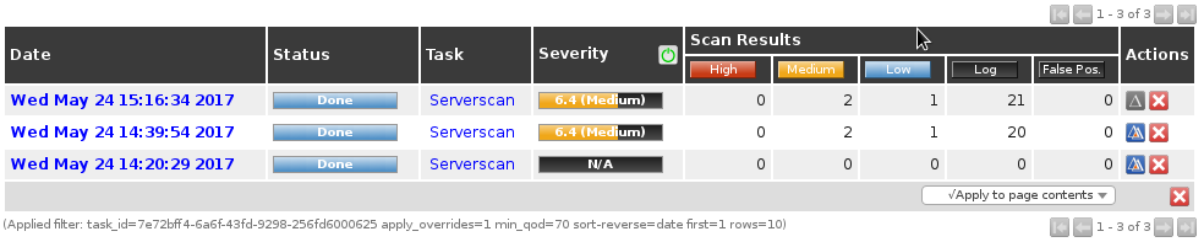


Fig. 10.4: Now, for comparison the second report needs to be selected.

Subsequently you will receive the delta report. As usual, it can be displayed in different formats and exported as PDF.

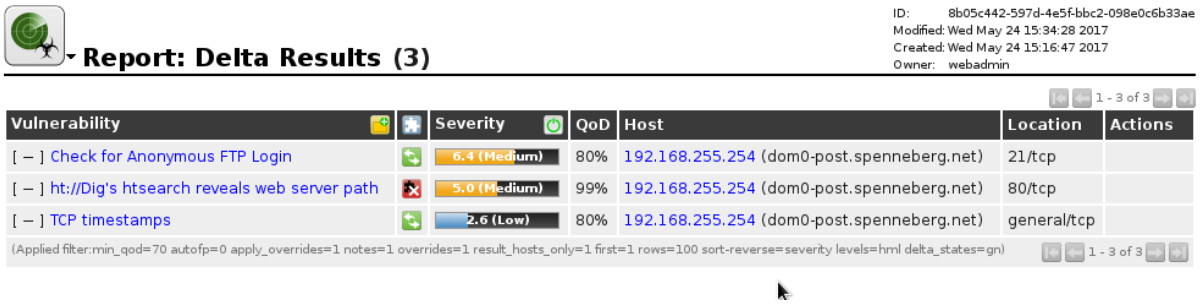


Fig. 10.5: The delta report can be exported as PDF as well.

The report contains information as to which run times are being compared with each other and how many results have been added or were removed.

10.2 Report Plugins

Report plugins are defined as the formats a report is created from, based on the scan results. This ranges from PDF documents as per corporate identity to interactive reports like the Greenbone Security Explorer. These plugins can be used to export report information into other document formats so they can be processed by other third party applications (Connectors).

The name of the exported report is configurable in the user settings (see section *My Settings* (page 62)). Greenbone supports the creation of additional plugins. Requests, suggestions and concrete templates are welcome.

The report plugin framework has the following properties:

Simple Import/Export: A report plugin is always a single XML file. The import is easily performed (see section *Import of additional plugins* (page 154)).

Parameterized: Plugins can contain parameters that can be customized to specific requirements in the graphical interface.

Content Type: For every plugin it is determined of which type the result is. The well-known HTTP descriptors are being used, for example, `application/pdf`, `graphics/png` or `text/plain`. Depending on the content type the plugins are displayed in contextual relation. For example, the types `text/*` for the sending as email inline.

Signature Support: Through the Greenbone Security Feed signatures for trusted plugins are being provided. That way it can be verified that an imported plugin was verified by Greenbone.

The Reports can be exported in different formats:

ARF: Asset Reporting Format v1.0.0 This format creates a report that represents the NIST Asset Reporting Format.

CPE - Common Enumeration CSV Table This report selects all CPE tables and creates a single comma separated file.

CSV hosts This report creates a comma separated file containing the systems discovered.

CSV Results This report creates a comma separated file with the results of a scan.

GSR PDF - Greenbone Security Report (recommended) This is the complete Greenbone Security report with all vulnerabilities in graphical format as a PDF file. The topology graph is not included when more than 100 hosts are covered in the report. The language is English.

GXR PDF - Greenbone Executive Report (recommended) This is a shortened report with all vulnerabilities in graphical format as a PDF file for management. The topology graph is not included when more than 100 hosts are covered in the report. The language of the report is in English.

HTML This report is in HTML format and as such can be opened in a web browser. It is a detailed listing containing the complete description of vulnerabilities including note and overrides with all references and cross references. It is a neutral document without any further references to Greenbone or the Greenbone Security Manager. The document can also be used off-line and the language being used is English.

ITG - IT-Grundschutz catalogue This report is guided by the BSI IT-Grundschutz catalogue. It provides an overview of the discovered results in table view in CSV format and in German.

LaTeX This report is offered as LaTeX source text. The language is English.

NBE This is the old OpenVAS/Nessus report format. It does not have support for notes, overrides and some additional information.

PDF This is a complete report in PDF. Like the HTML format it is neutral. The language is English.

Topology SVG This presents the results in a SVG picture.

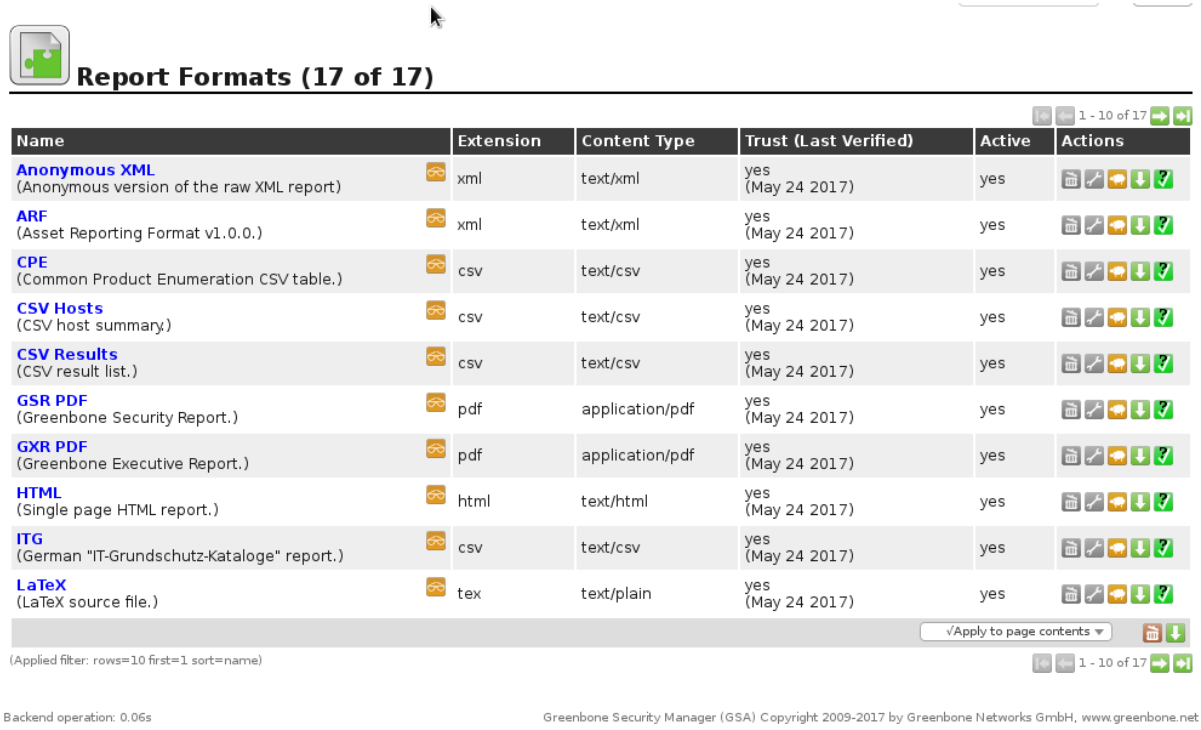
TXT This creates a text file. This format is especially useful when being sent by Email. The language is English.

Verinice ISM Creates an import file for the ISMS tool *Verinice*.

Verinice ITG Creates an import file for the ISMS tool *Verinice*.

XML The report is being exported in the native XML format. Contrary to the other formats this format contains all results and does not format them at all.

The report plugins define the format of the reports to be exported. Many report plugins reduce the available data in order to display it in a meaningful way. However, the native GSM XML format contains all data and can be used to import exported reports on another GSM. To do so use the Container Task (see also section *Container Task* (page 91)).



Report Formats (17 of 17)

1 - 10 of 17

Name	Extension	Content Type	Trust (Last Verified)	Active	Actions
Anonymous XML (Anonymous version of the raw XML report)	xml	text/xml	yes (May 24 2017)	yes	
ARF (Asset Reporting Format v1.0.0.)	xml	text/xml	yes (May 24 2017)	yes	
CPE (Common Product Enumeration CSV table.)	csv	text/csv	yes (May 24 2017)	yes	
CSV Hosts (CSV host summary.)	csv	text/csv	yes (May 24 2017)	yes	
CSV Results (CSV result list.)	csv	text/csv	yes (May 24 2017)	yes	
GSR PDF (Greenbone Security Report.)	pdf	application/pdf	yes (May 24 2017)	yes	
GXR PDF (Greenbone Executive Report.)	pdf	application/pdf	yes (May 24 2017)	yes	
HTML (Single page HTML report.)	html	text/html	yes (May 24 2017)	yes	
ITG (German "IT-Grundschutz-Kataloge" report.)	csv	text/csv	yes (May 24 2017)	yes	
LaTeX (LaTeX source file.)	tex	text/plain	yes (May 24 2017)	yes	

√Apply to page contents

(Applied filter: rows=10 first=1 sort=name)

1 - 10 of 17

Backend operation: 0.06s

Greenbone Security Manager (GSA) Copyright 2009-2017 by Greenbone Networks GmbH, www.greenbone.net

Fig. 10.6: Greenbone includes many report plugins by default.

The overview (see figure *Greenbone includes many report plugins by default.* (page 154)) shows additional details of the report plugins. For every plugin in the individual columns the following information is being displayed:

Extension: The file name of the downloaded report through the respective plugin is comprised of the UUID (unique internal ID of the report) and this extension. Among others, the extension supports the browser to start a compatible application in case the specified content type is not recognized.

Content Type: The content type specifies the format in use and is being transmitted when being downloaded. That way a compatible application can be launched by the browser directly. Additionally the content type is important internally: It is being used to offer suitable plugins within its context. For example, when sending a report via Email all plugins of the type `text/\*` are being offered as they can be embedded in an email in a humanly readable way.

Trust: Some plugins only consist of a data transformation while others execute more complex operations and also use support programs. To avoid misuse the plugins are digitally signed. If the signature is authentic and the publisher trusted, it is ensured that the plugin exists in the exact format as certified by the publisher. The verification does not occur automatically rather than manually with the verify icon . The date of the verification is saved automatically. This function should definitely be used for all newly imported plugins before they are being activated. This is not required for the supplied default plugins .

Active: The plugins are only available in the respective selection menus if they were activated. Newly imported plugins are always deactivated at first.

10.2.1 Import of additional plugins

Other report formats can be imported easily. Greenbone offers the following additional report format plugins on the following web page: http://greenbone.net/technology/report_formats.html:

- Sourcefire Host Input Import (see also section *Firepower Management Center* (page 236))

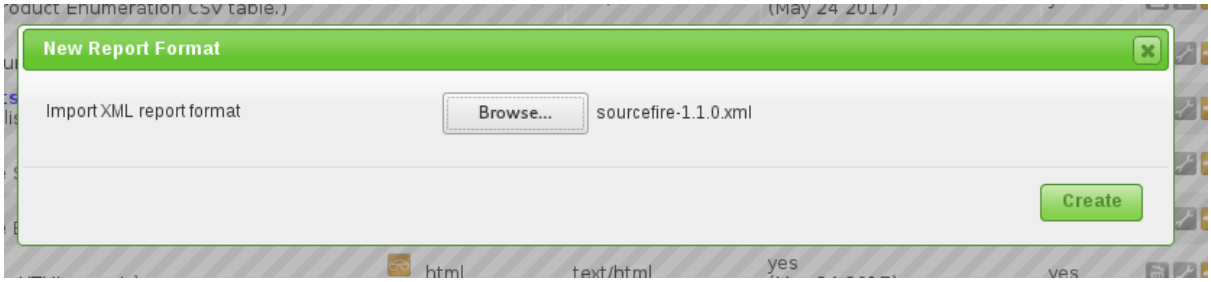


Fig. 10.7: New report formats plugins can be imported easily.

- OVAL System Characteristics
- OVAL System Characteristics Archive

Note: The report format plugins for the verinice connector are now already shipped with the Greenbone operating system. They do not need to be manually imported anymore.

To import a report plugin the respective XML file must be downloaded from Greenbone. Afterwards change to *Configuration/Report Formats*. Select the icon to add the new format.

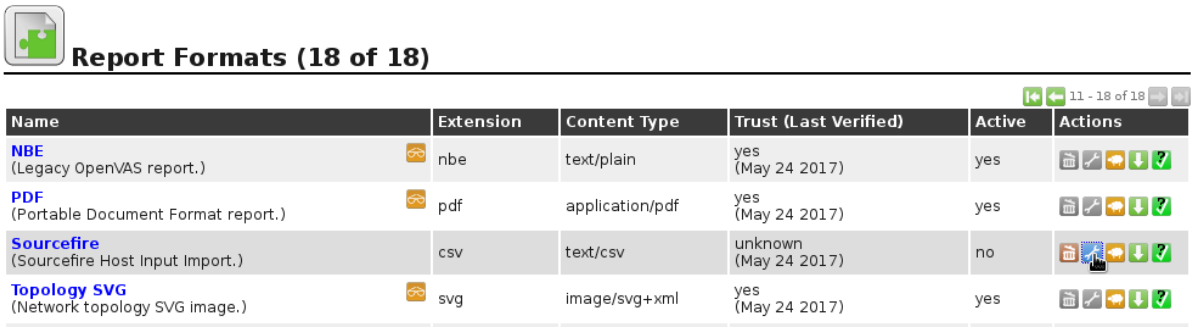


Fig. 10.8: Imported formats should be verified before activation.

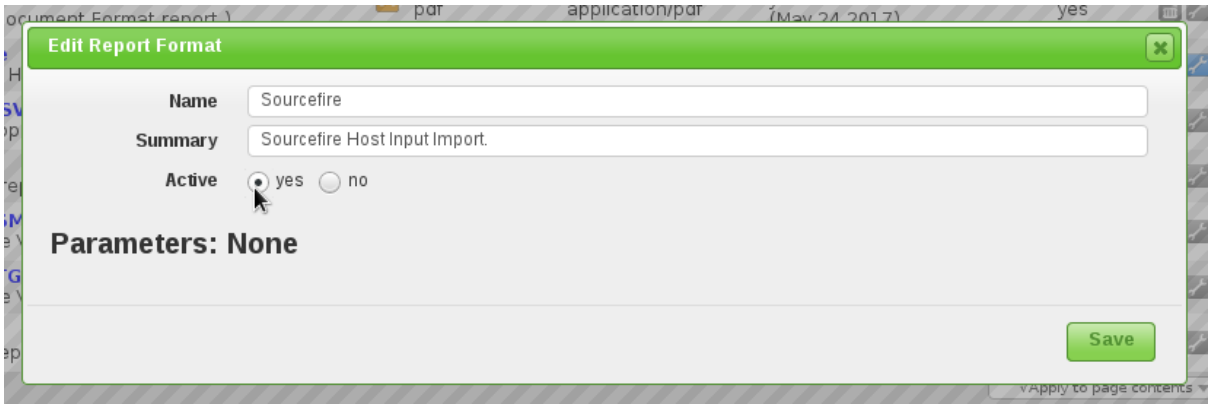


Fig. 10.9: New report formats plugins can be activated easily.

Select the respective file and then import the format. After importing the new format is not active yet. Report plugins can be signed by the publisher. This signature should get verified before activation . This verification is being done automatically when importing. The result with the date of the verification is being displayed in the Trust column. If the report plugin is trusted it can be activated afterwards. To do so, edit the report plugin by clicking the edit icon in the Actions column.

CHAPTER 11

Compliance and special scans

Compliance in the IT security world is the primary approach for organizations to keep their information and assets protected and secure.

With cybercrime on the rise, governments see the need to protect their citizens and pass rules and regulations on privacy and IT security in the hopes to protect our identities and assets. Information Security bodies such as the Information Systems Audit and Control Association (ISACA) or the International Organization for Standardization (ISO) publish IT security standards, frameworks and guidelines such as the Control Objectives for Information and Related Technology (COBIT) or the ISO 27000 series which cover information security standards. The German Federal Office for Security in Information Technology (BSI), for example, publishes the IT Baseline Protection Catalogs, or IT-Grundschutz-Kataloge. This is a collection of documents that provide useful information for detecting weaknesses and combating attacks on IT environments. To better protect against credit card data theft the Payment Card Industry Security Standards Council publishes the payment Card Industry Data Security Standard (PCI DSS).

All these privacy laws, standards, frameworks, rules and regulations are to force and assist organizations to implement the appropriate safeguards to protect themselves and their information assets from attacks. In order to implement these laws, standards, frameworks, rules and regulations within an organization the organization will have to create an IT security framework consisting of policies, standards, baselines, guidelines and detailed procedures.

Security scanners such as the Greenbone Security Manager (GSM) can assist IT security professionals to check their IT security safeguards against the aforementioned regulations, standards and frameworks for compliance.

In the following sections we will describe how the GSM can be utilized to perform certain compliance checks.

11.1 Generic Policy Scans

When performing policy scans there are several groups each with four NVTs that can be configured accordingly. In the policy section of the NVTs database at least two of these four policy NVTs are required to run a policy scan. The four NVT types are:

- ***Base*** This NVT performs the actual scan/function of the actual policy scan.
- ***Matches*** This NVT summarizes any items which match the checks performed by the base NVT.
- ***Violations*** This NVT summarizes any items which did not match the checks performed by the base NVT.
- ***Errors*** This NVT summarizes any items where some error occurred when running the policy scan.

The base NVT must be selected for a policy check since it performs the actual tests. The other three plugins may be selected according to your needs. For example, if matching patterns are of no concern then only the violations plugin should be selected additionally.

11.1.1 File Content

File content checks belong to policy audits which don't explicitly test for vulnerabilities but rather test the compliance of file contents (e.g. configuration files) regarding a given policy.

GSM provides a policy module to check if a file content is compliant with a given policy.

In general this is an authenticated check, i.e. the scan engine will have to log into the target system to perform the check.

The file content check can only be performed on systems supporting the command `grep`. Normally this means Linux or Linux-like systems.

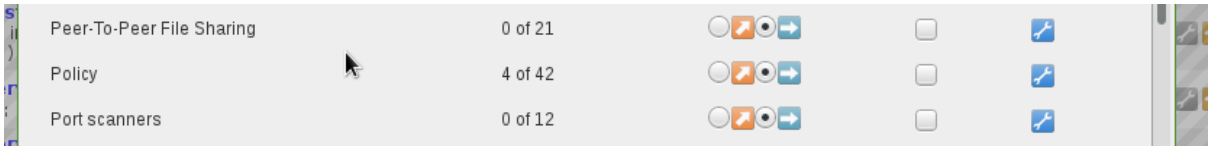


Fig. 11.1: The NVTs are in the „Policy“ family

Four different NVTs provide the file content check:

- *File Content*: This NVT performs the actual file content check.
- *File Content: Matches*: This NVT shows the patterns and files which passed the file content check (the predefined pattern matches in the file)
- *File Content: Violations*: This NVT shows the patterns and files which didn't pass the file content check (the predefined pattern doesn't match in the file)
- *File Content: Errors*: This NVT shows the files where some error occurred (e.g. the file is not found on the target system)

The NVT *File Content* must be selected for a file content check since it performs the actual tests. The other three plugins may be selected according to your needs. E.g. if just not matching patterns are of concern then only the plugin *File Content: Violations* should be additionally selected.

Patterns

A reference file with the patterns to check and some other entries must be created. Following is an example:

```
filename|pattern|presence/absence
/tmp/filecontent_test|^paramter1=true.*$|presence
/tmp/filecontent_test|^paramter2=true.*$|presence
/tmp/filecontent_test|^paramter3=true.*$|absence
/tmp/filecontent_test_notthere|^paramter3=true.*$|absence
```

This file must contain the row `filename|pattern|presence/absence`. The subsequent rows contain each a test entry. Each row contains three elements which are separated by `|`. The first field contains the path and file name, the second field the pattern to check and the third field indicates if a pattern has to be present or absent.

The pattern to check, the second element in the row, is defined as a regular expression and will be checked in the file accordingly.

Select the file with *Browse* and select *Upload file*. The file upload will be started by clicking *Save Config*.

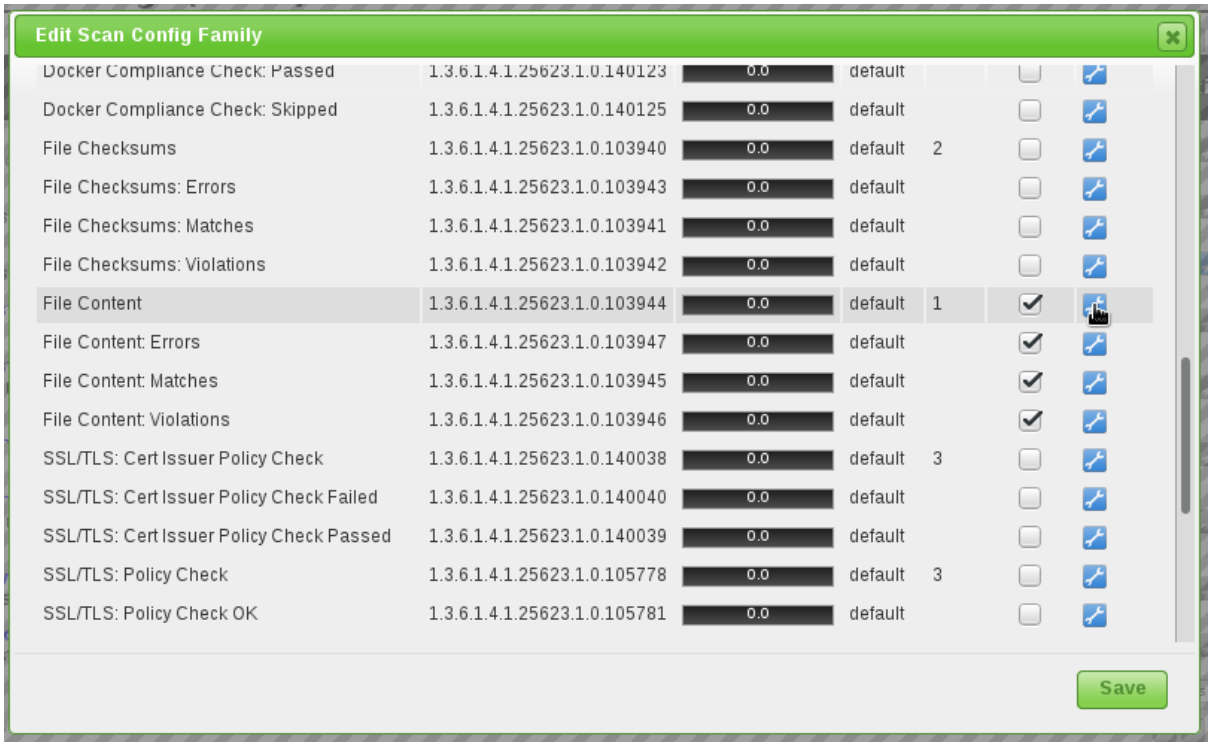


Fig. 11.2: Afterwards import this file in the properties of the NVT

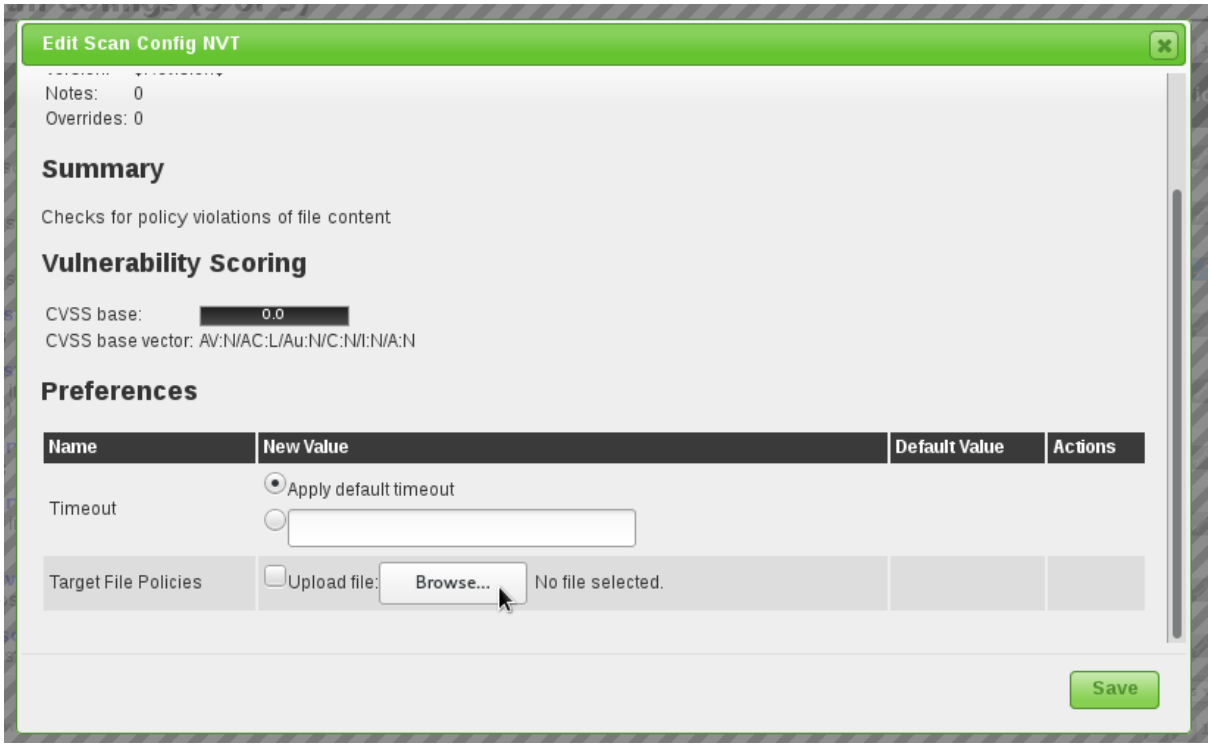


Fig. 11.3: The mask will change if there is already a file uploaded

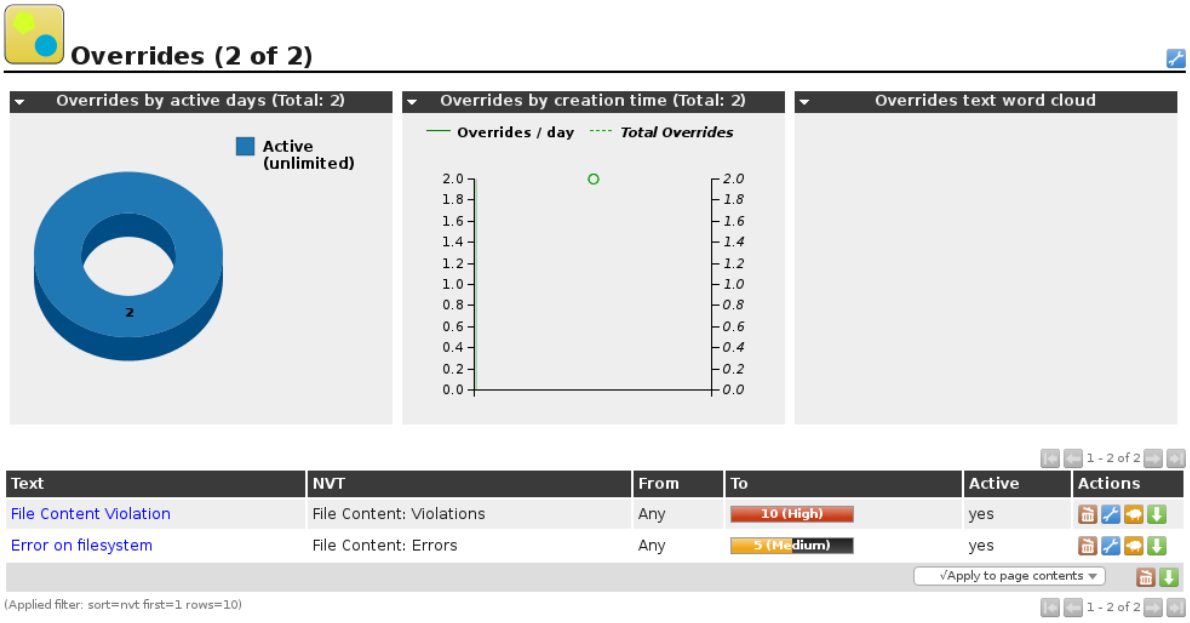
By clicking on the icon it is possible to download the already uploaded reference file. Select *Replace existing file with:* to upload a new reference file. The possibilities to change is only available if the scan configuration is not in use. This is done to ensure immutable audit-compliant scan results.

Severity

The severity of the NVTs depend on the GOS version used. Since GOS 4.2 the violation NVTs have a default score of 10. In the past these NVTs had a default score of 0 (log message) and overrides were required for different scores. The new default score of 10 can be changed using overrides as well.

By sectioning the reporting plugins in three different NVTs it is now possible to create distinct overrides on the severity according your needs.

In the following picture the severities of *File Content: Violations* and *File Content: Errors* have been changed which will be shown in the reports accordingly.



Example

Here (policy_file_content_example.xml[16]) is an example scan configuration with all the relevant NVTs for the file content test to download. The corresponding test file (filecontent_test[17]) should be downloaded and extracted to the /tmp/ directory on the target system.

Now create an new task and start it for the target system where you saved test files. Please note that this has to be an authenticated scan with the appropriate SSH Credentials.

The overrides can be created either before or after a scan. The latter is easier since you can create the appropriate reference through a simple click in the result page.

11.1.2 Registry Content

The registry is a database in Windows that contains important information about system hardware, installed programs and settings, and profiles of each of the user accounts on your computer. Windows continually refers to the information in the registry [110].

[16] http://download.greenbone.net/scanconfigs/policy_file_content_example.xml
[17] http://download.greenbone.net/misc/filecontent_test
[110] http://windows.microsoft.com/en-ca/windows-vista/what-is-the-registry

Due to the nature of the Windows registry every program/application installed under windows will register itself in the Windows registry and as such has a registry entry. Even malware and other malicious code usually leaves traces within the windows registry. The registry now can be utilized to search for specific application or malware related information such as version levels and numbers. Also missing or changed registry settings could point to a potential security policy violation on an endpoint. GSM provides a policy auditing module to verify registry entries on target systems. This module checks for the presence or absence of registry settings as well as registry violations. Since the registry is unique to Windows systems this check can only be run on Windows systems. To access the registry on the target system the check needs to authenticate on the target system.

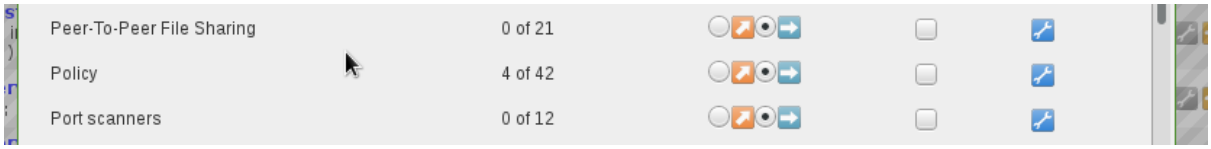


Fig. 11.4: The NVTs are in the „Policy“ family.

Four different NVTs provide the registry content check:

- *Windows Registry Check*: This NVT performs the actual registry content check on the files.
- *Windows Registry Check: OK*: This NVT shows the registry setting which passed the registry check (registry content OK).
- *Windows Registry Check: Violations*: This NVT shows the registry content which didn't pass the registry check (wrong registry content).
- *Windows Registry Check: Errors*: This NVT shows the registry entries where some error occurred (e.g. registry content not found on the target system).

The plugin *Windows Registry Check* must be selected for a registry check since it performs the actual tests. The other three plugins may be selected according to the needs. E.g. just entries with wrong registry content are of concern then only the plugin *Windows Registry Check: Violations* should be additionally selected.

Registry Content Pattern

A file with the reference registry content must be created: Following is an example:

```
Present|Hive|Key|Value|ValueType|ValueContent
TRUE|HKLM|SOFTWARE\Macromedia\FlashPlayer\SafeVersions|8.0|REG_DWORD|33
TRUE|HKLM|SOFTWARE\Microsoft\Internet Explorer
TRUE|HKLM|SOFTWARE\Microsoft\Internet Explorer|Version|REG_SZ|9.11.10240.16384
TRUE|HKLM|SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system|LocalAccountTokenFilterPolicy
FALSE|HKLM|SOFTWARE\Virus
TRUE|HKLM|SOFTWARE\ShouldNotBeHere
TRUE|HKLM|SOFTWARE\Macromedia\FlashPlayer\SafeVersions|8.0|REG_DWORD|*
```

This file must contain the row `Present|Hive|Key|Value|ValueType|ValueContent`. The subsequent rows contain each a test entry. Each row contains a registry entry to be checked. Each row contains six elements which are separated by `|`. The first field sets if a registry entry should be present or not, the second the hive the registry entry is located in, the third the key, the fourth the value, the fifth the value type and the sixth the value content. If a star `*` is uesd in the last column any value is valid and accepted for existance or non-existance.

Select the file with *Browse* and select *Upload file*. The file upload will be started by clicking *Save Config*.

By clicking on the ⬇ icon it is possible to download the already uploaded reference file. Select *Replace existing file with:* to upload a new reference file. The option to change is only available if the scan configuration is not in use. This is done to ensure immutable audit-compliant scan results.

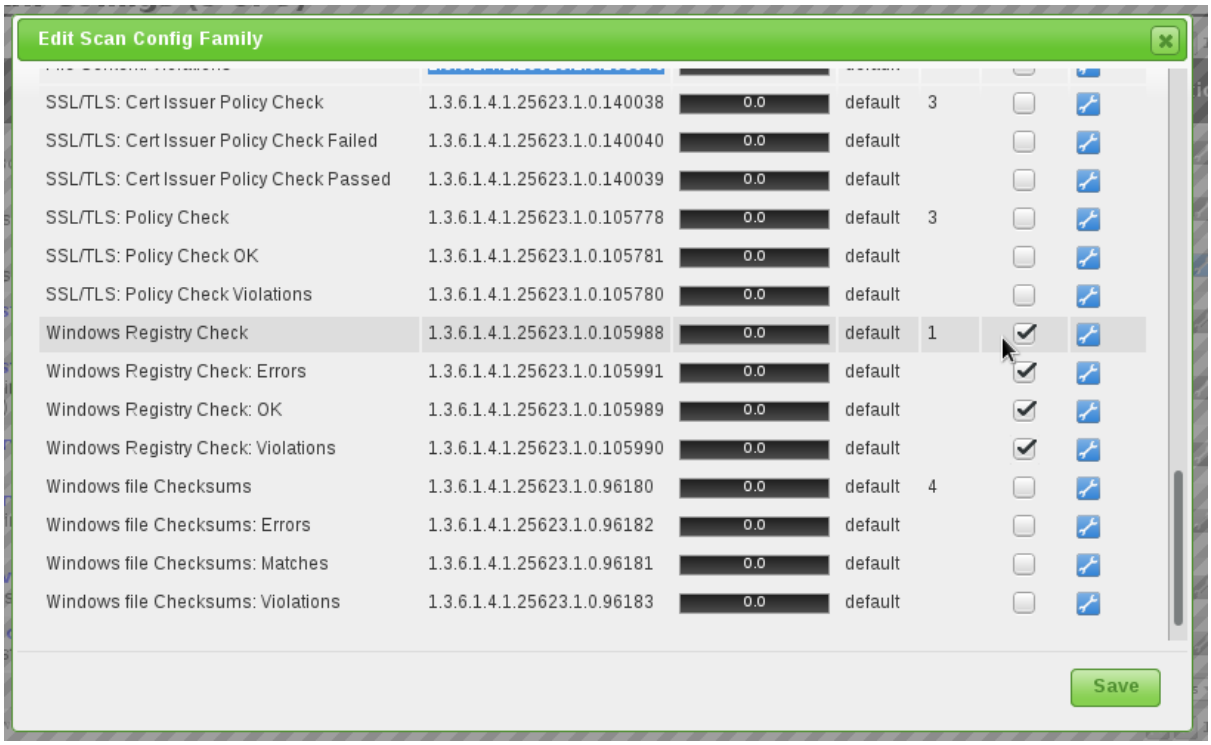


Fig. 11.5: Afterwards import this file in the properties of the NVT.

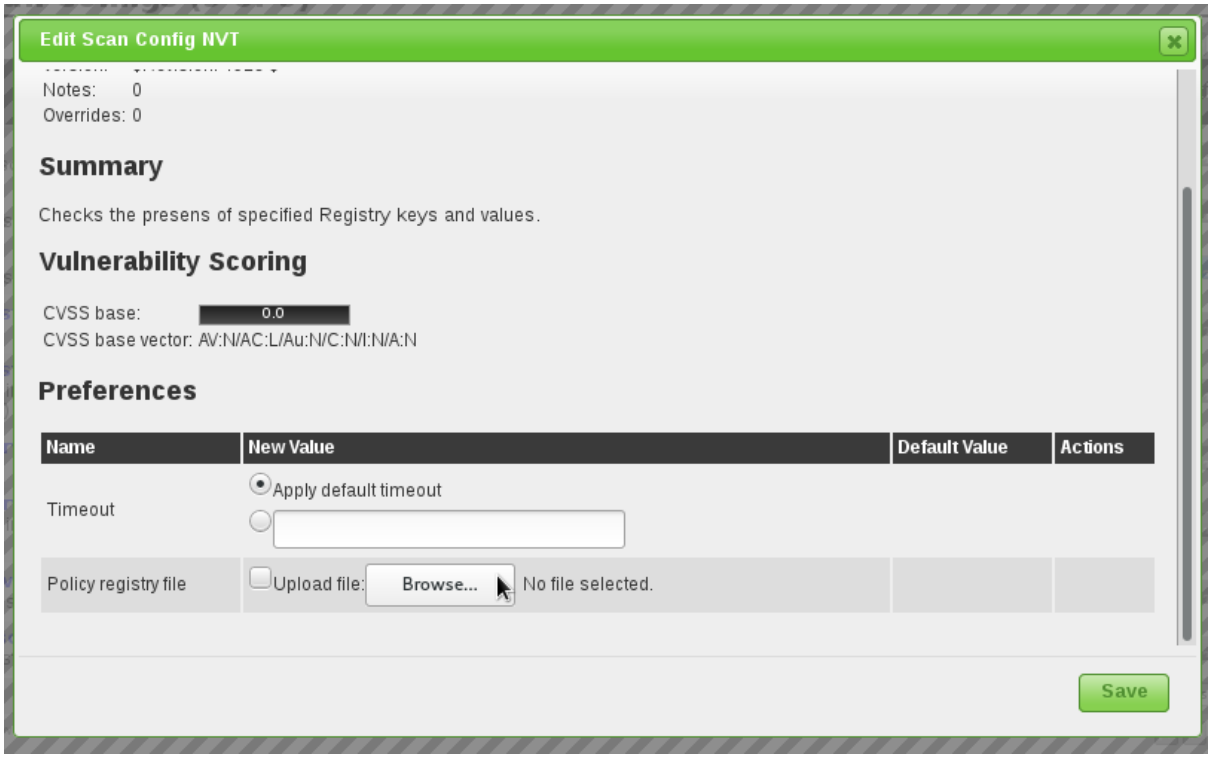


Fig. 11.6: The mask will change if there is already a file uploaded.

Severity

The severity of the NVTs depend on the GOS version used. Since GOS 4.2 the violation NVTs have a default score of 10. In the past these NVTs had a default score of 0 (log message) and overrides were required for different scores. The new default score of 10 can be changed using overrides as well.

By sectioning the reporting plugins in three different NVTs it is now possible to create distinct overrides on the severity according your needs.

In the figure *Severity overrides applied for Windows registry checks.* (page 163) the severities of *Registry Content: Violations* and *Registry Content: Errors* have been changed which will be shown in the reports accordingly.

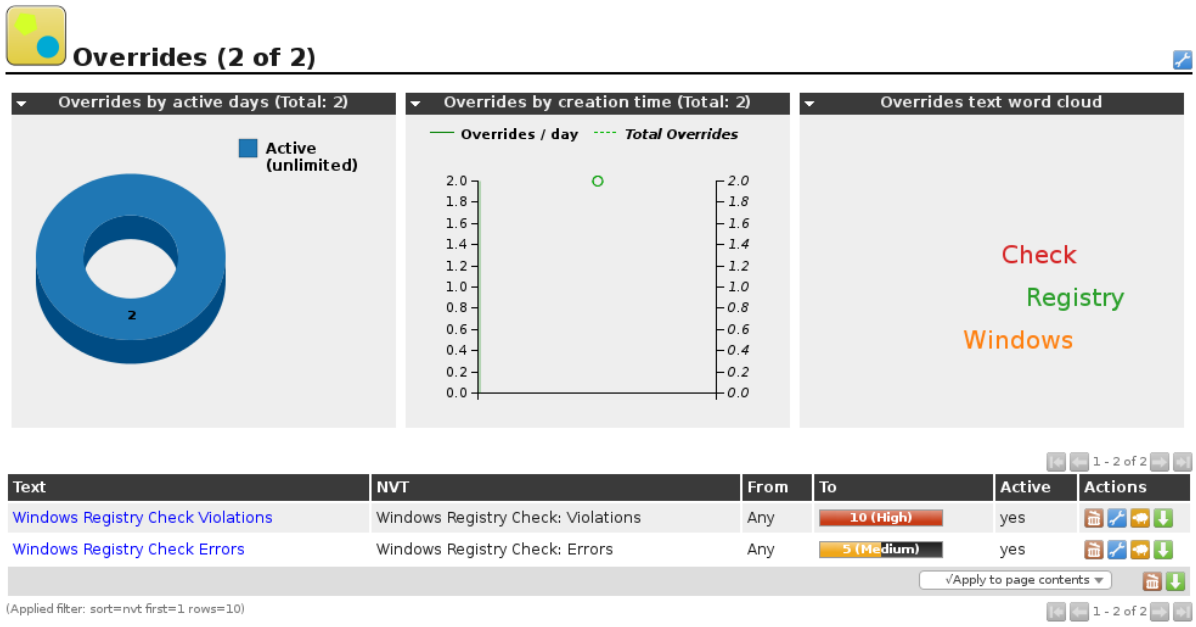


Fig. 11.7: Severity overrides applied for Windows registry checks.

Example

Here (policy_registry_ScanConfig.xml[18]) is an example scan configuration with all relevant NVTs for the registry test to download.

Now create a new task and start it for the target system where you saved test files.

The overrides can be created either before or after a scan. The latter is easier since you can create the appropriate reference through a simple click in the result page.

11.1.3 File Checksums

File checksum checks belong to policy audits which don't explicitly test for vulnerabilities but rather test the integrity of files. GSM provides a policy auditing module to verify file integrity on target systems. This module checks the file content by MD5 or SHA1 checksums. In general this is an authenticated check, i.e. the scan engine will have to log into the target system to perform the check. The file checksum check can only be performed on systems supporting checksums. Normally this means Linux or Linux-like systems. GSM provides however as well a module for checksum checks for Windows systems (see *Windows* (page 166)).

[18] http://download.greenbone.net/misc/policy_registry_ScanConfig.xml

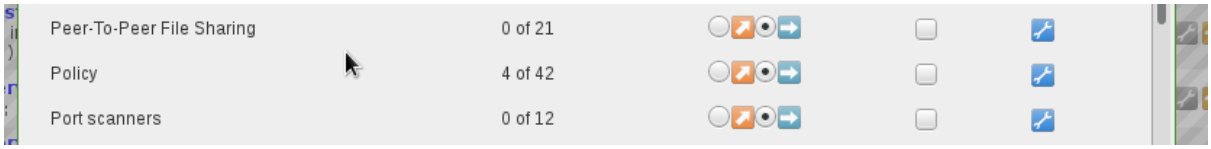


Fig. 11.8: The NVTs are in the „Policy“ family.

Four different NVTs provide the file checksum check:

- *File Checksums*: This NVT performs the actual checksum check on the files.
- *File Checksums: Matches*: This NVT shows the files which passed the checksum check (checksum matches).
- *File Checksums: Violations*: This NVT shows the files which didn't pass the checksum check (wrong checksum).
- *File Checksums: Errors*: This NVT shows the files where some error occurred (e.g. file not found on the target system).

The plugin *File Checksums* must be selected for a file checksum check since it performs the actual tests. The other three plugins may be selected according to the needs. E.g. just files with wrong checksums are of concern then only the plugin *File Checksums: Violations* should be additionally selected.

Checksum Patterns

A file with the reference checksums must be created. Following is an example:

```
Checksum|File|Checksumtype
6597ecf8208cf64b2b0eaa52d8169c07|/bin/login|md5
ed3ed98cb2efa9256817948cd27e5a4d9be2bdb8|/bin/bash|sha1
7c59061203b2b67f2b5c51e0d0d01c0d|/bin/pwd|md5
```

This file must first contain the row `Checksum|File|Checksumtype`. The subsequent rows contain each a test entry. Each row contain three elements which are separated by `|`. The first field contains the checksum in hex, the second field the path and file name and the third field the checksum type. Currently MD5 and SHA1 checksums are supported.

Note: Checksums and checksum type must be lowercase.

Select the file with *Browse* and select *Upload file*. The file upload will be started by clicking *Save Config*.

By clicking on the ⬇ icon it is possible to download the already uploaded reference file. Select *Replace existing file with:* to upload a new reference file. The possibilities to change is only available if the scan configuration is not in use. This is done to ensure immutable audit-compliant scan results.

Severity

The severity of the NVTs depend on the GOS version used. Since GOS 4.2 the violation NVTs have a default score of 10. In the past these NVTs had a default score of 0 (log message) and overrides were required for different scores. The new default score of 10 can be changed using overrides as well.

By sectioning the reporting plugins in three different NVTs it is now possible to create distinct overrides on the severity according your needs.

In the figure *Severity overrides applied for file checksum checks.* (page 166) the severities of *File Checksum: Violations* and *File Checksum: Errors* have been changed which will be shown in the reports accordingly.

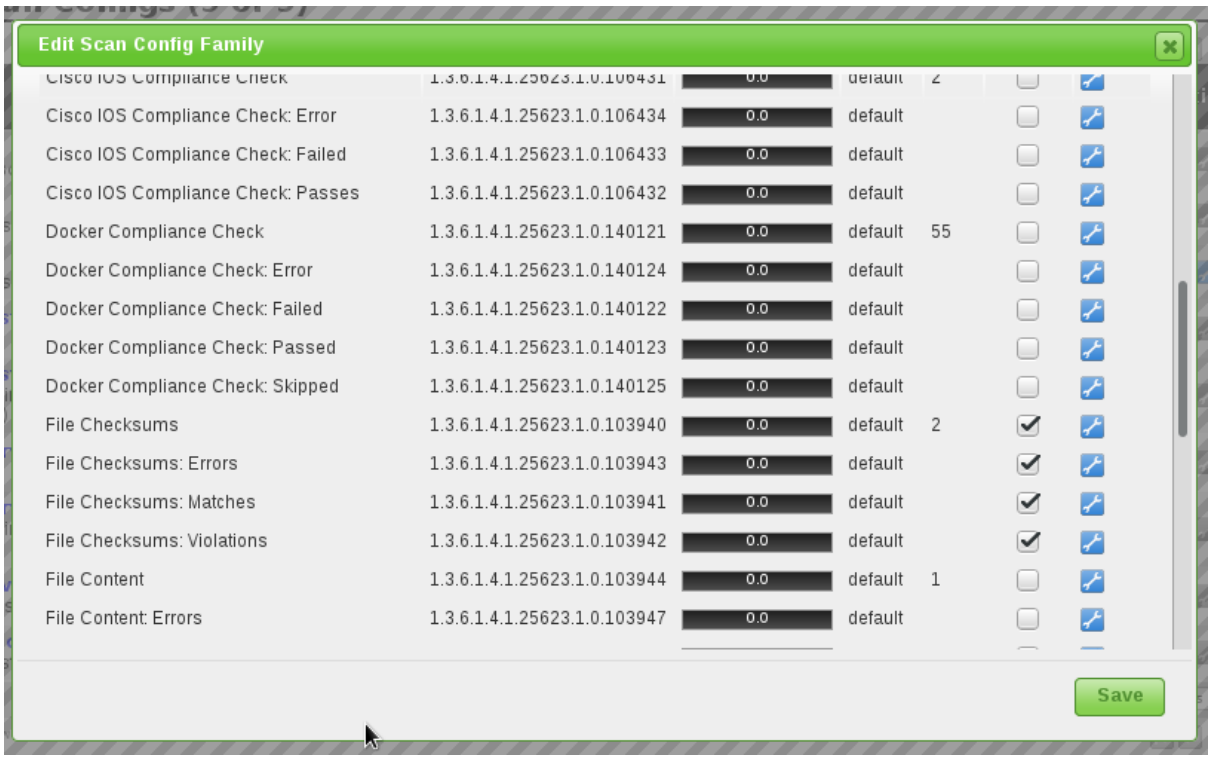


Fig. 11.9: Afterwards import this file in the properties of the NVT.

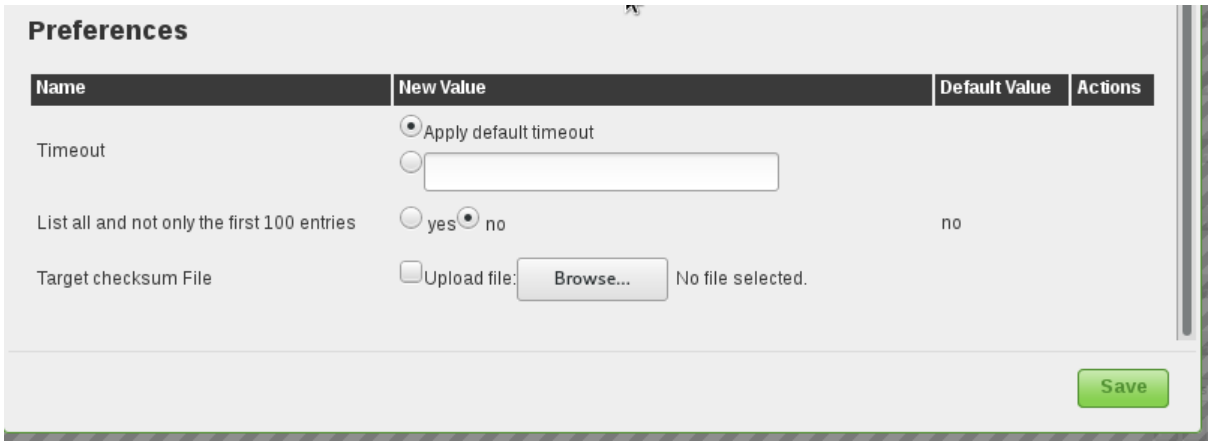


Fig. 11.10: The mask will change if there is already a file uploaded.

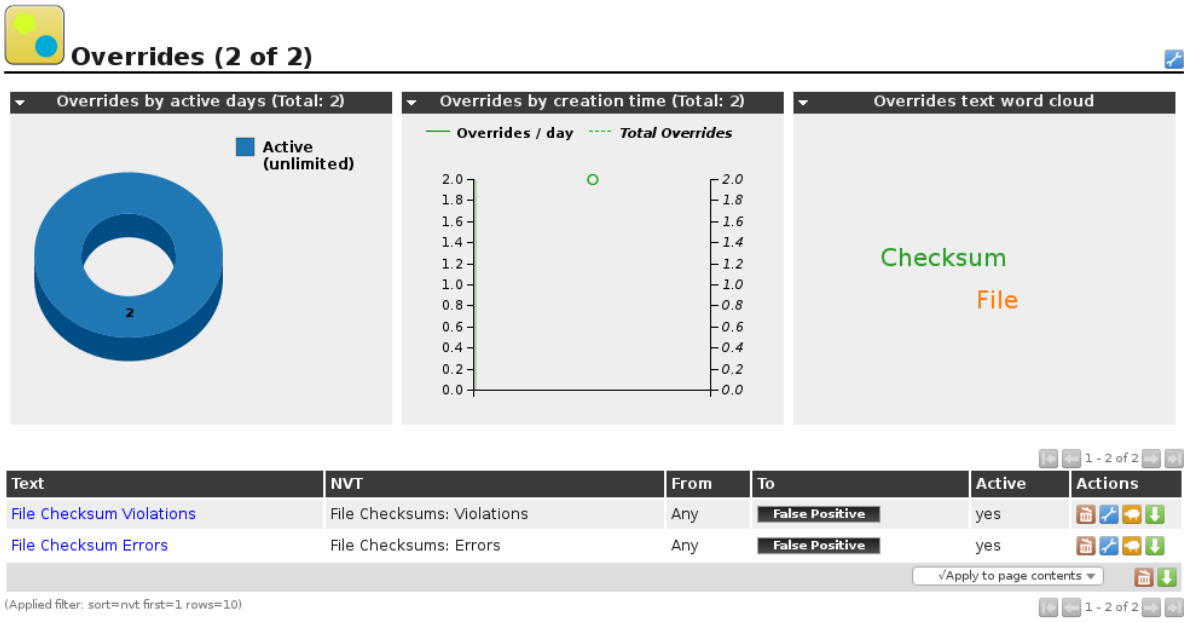


Fig. 11.11: Severity overrides applied for file checksum checks.

Example

Here (policy_file_checksums_example.xml[19]) is an example scan configuration with all relevant NVTs for the checksum test to download. The corresponding testfiles (policy_file_checksums_testfiles[20]) should be downloaded and extracted to the `/tmp/` directory on the target system. This can be done e.g. by `tar -xvC /tmp/ -f policy_file_checksums_testfiles.tar.gz`.

Now create a new task and start it for the target system where you saved test files. Please note that this has to be an authenticated scan with the appropriate SSH Credentials.

The overrides can be created either before or after a scan. The latter is easier since you can create the appropriate reference through a simple click in the result page.

Windows

GSM provides a similar module for Windows systems for checksum checks. Since Windows doesn't provide an internal program for creating checksums it has to be installed one either manually or automatically by the NVT. GSM uses ReHash (http://rehash.sourceforge.net/) for creating checksums on Windows systems.

As for Linux systems the NVTs for checksum checks are located under the *Policy* family.

Please note the two operating modes for these checks: Either a before manually on the target system installed tool will be used or the tool ReHash will automatically be installed and if requested as well deinstalled on the target system during the checking routine.

Through the preferences it can be set if the checksum program ReHash should be deleted after the check or not. The program can be left on the target system to e.g. speed up recurring tests and therefore don't have to be transferred each time. It can further be set if the checksum program should be installed automatically on the target system. If not it has to be manually installed (under `C:\\Windows\\system32` on 32-bit system) or `C:\\Windows\\SysWOW64` (on 64-bit systems)) and has to be executable for the authenticated user. The file with the reference checksums must be uploaded in the preferences as it is done for the Linux checksum check. The file has the same structure as the one for Linux.

[19] http://download.greenbone.net/scanconfigs/policy_file_checksums_example.xml
[20] http://download.greenbone.net/misc/policy_file_checksums_testfiles.tar.gz

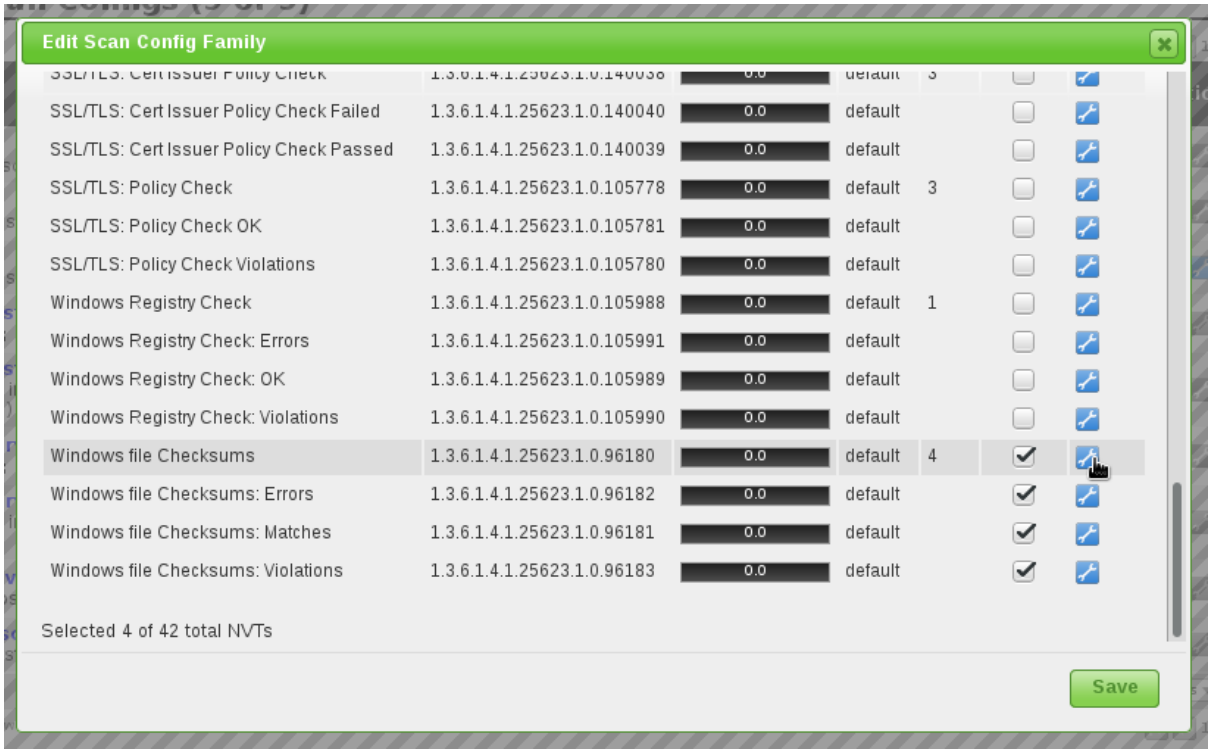


Fig. 11.12: Four NVTs are responsible for the checksum checks under Windows

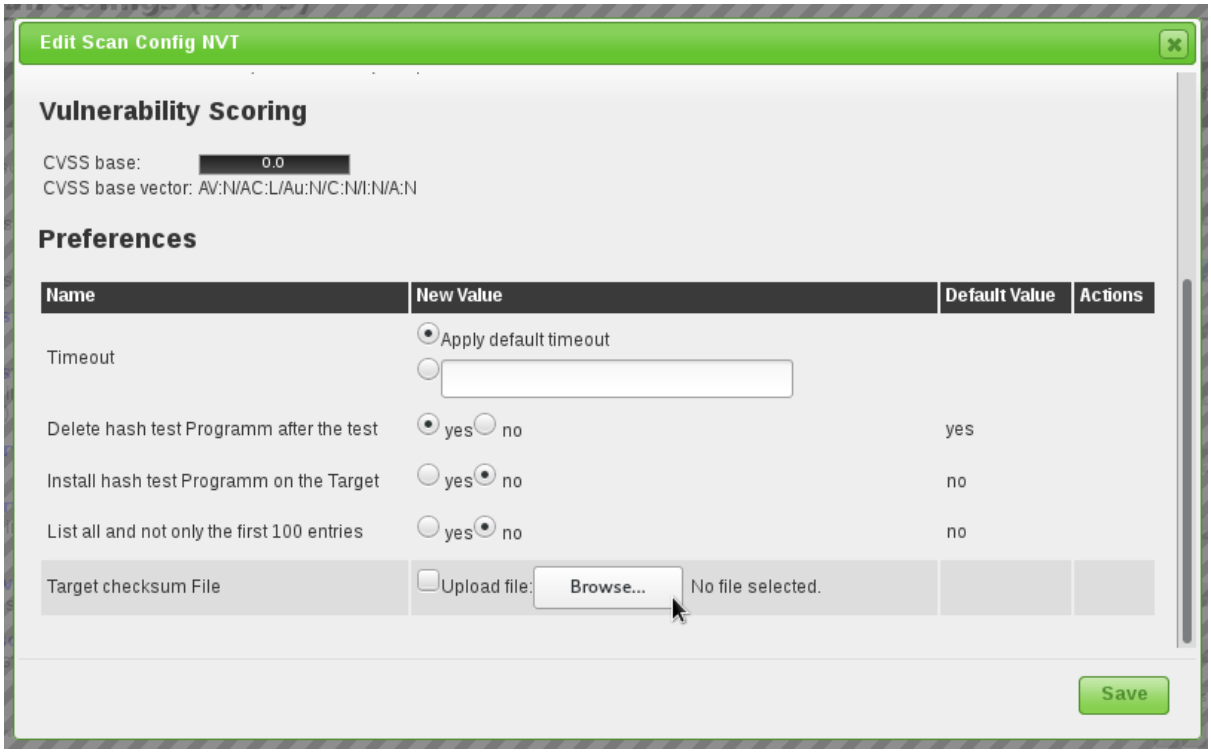


Fig. 11.13: The preferences must be set then in the „Windows file Checksums“ NVT.

Example Windows

A sample configuration (sample_config-Windows_file_Policy.xml[21]) with all needed NVTs for the Windows checksum check can be downloaded here. The corresponding example files (windows_checksums_testfiles.zip[22]) can be downloaded and must be saved and extracted on the target system on filesystem C:.

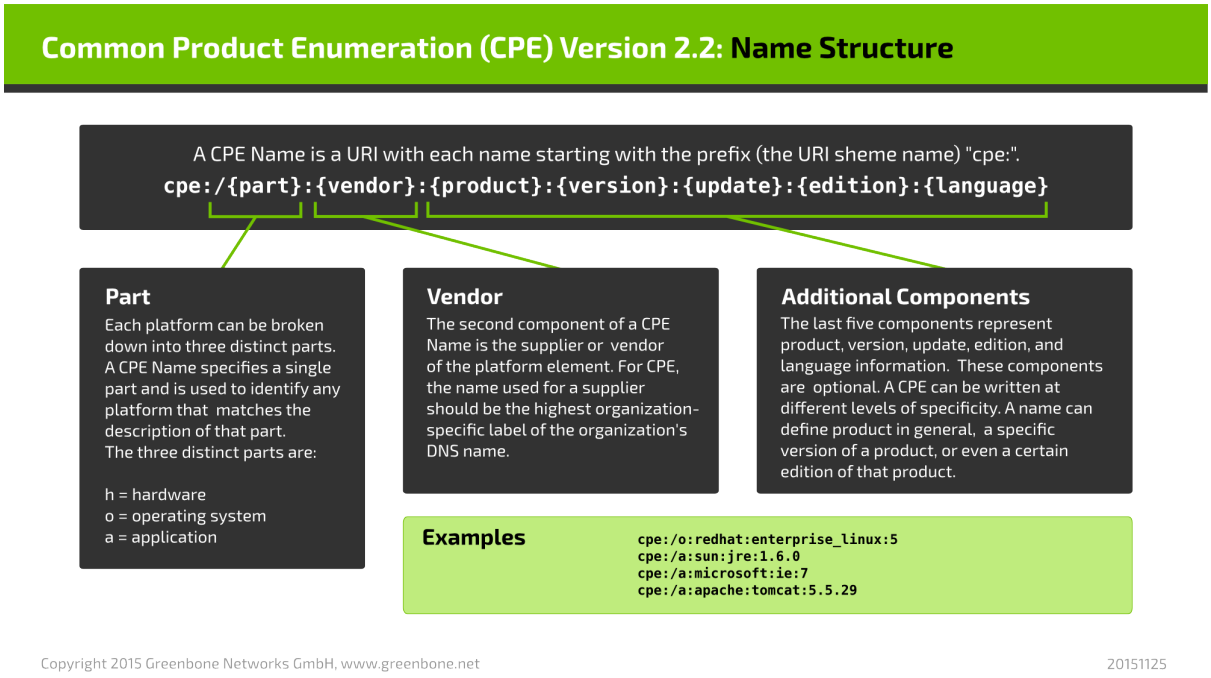
For Tasks and Overrides please proceed as described above.

11.1.4 CPE-based

CPE stands for Common Product Enumeration[23]. It is a structured naming scheme for information technology systems, platforms, and packages.

In other words: CPE provides a unique identifier for virtually any software product that is known for a vulnerability.

The CPE dictionary is maintained by U.S. National Institute for Standards and Technology (NIST)[24] and was developed by the MITRE Corporation (MITRE)[25] and NIST. Close to the end of 2014 MITRE announced that all intellectual property associated with CPE has been transferred to NIST. MITRE still maintains CVE (Common Vulnerability Enumeration) and other relevant security standards.



CPE-based, simple checks for security policies

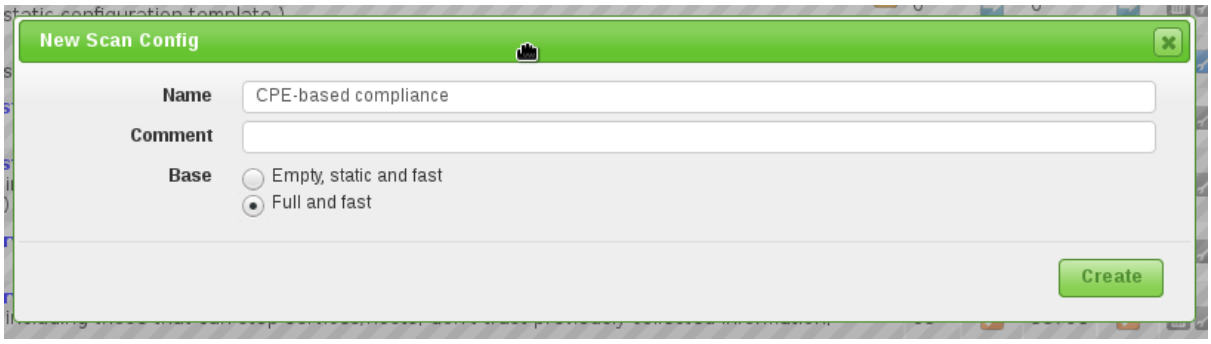
With any executed scan, CPEs for the identified products are stored. This happens independently of whether the product actually reveals a security problem or not. On this basis it is possible to describe simple security policies and the checks for compliance with these. With the Greenbone Security Manager it is possible to describe policies to check for the presence as well as for the absence of a product. These cases can be associated with a severity to appear in the scan report.

[21] http://download.greenbone.net/scanconfigs/sample_config-Windows_file_Policy.xml
[22] http://download.greenbone.net/misc/windows_checksums_testfiles.zip
[23] http://scap.nist.gov/specifications/cpe/
[24] http://www.nist.org
[25] http://www.mitre.org/

Checking policy compliance

This example demonstrates how to check the compliance of a policy regarding specific products in a IT infrastructure and how the reporting with the corresponding severity can be done.

1. The information about whether a certain product is present on the target system is gathered by a single Network Vulnerability Test (NVT) or even independently by a number of special NVTs. This means that for a certain product you can specify an optimized scan configuration that only concentrates on this product and does not do any other scan activity. The advantage of such a special scan configuration is a considerably faster execution of the scan compared to a comprehensive scan configuration such as *Full and Fast*. The disadvantage of a special scan configuration is that some experience is required to select the right set of NVTs to maximize the probability of success. Initially it is easier to apply a comprehensive scan configuration. In this case it is not necessary to care about the product character, you just enter its CPE identifier. This example follows the simple approach. First, a copy of *Full and Fast* is created. This is necessary because *Full and Fast* is a pre-configured scan configuration and thus can not be modified.



2. On the overview page for this scan configuration you will find a section *Network Vulnerability Test Preferences*. You will need to unfold this section using . Here, all NVTs that allow special configuration are listed. With you can jump directly to the edit dialog for a specific NVT. This short-cut avoids having to click through the family structures to get to the desired NVT (the here used NVTs are in the family *Policy*).

3. You can either specify a single CPE directly or a list of CPEs in a file which must be imported afterwards (through clicking on *Browse* to select the file and selecting *Upload file*). Below is an example for checking for Internet Explorer 9 and ClamAV 0.98:

```
cpe:/a:microsoft:ie:9
cpe:/a:clamav:clamav:0.99
```

For this example we have a policy where the stated CPEs must be present to comply. This means we want to know especially if there are some installations which violate this policy (e.g. missing or not wrong products/versions).

Confirm your changes with *Save*.

4. The severity of the NVTs depend on the GOS version used. Since GOS 4.2 the violation NVTs have a default score of 10. In the past these NVTs had a default score of 0 (log message) and overrides were required for different scores. The new default score of 10 can be changed using overrides as well. If you want to change this you have to create an override. In this example violations of the policy should be reported with different severity.

   For this a new override has to be created through the *Scan Management*. The OID in this case will be "1.3.6.1.4.1.25623.1.0.103964" (for the NVT *CPE-based Policy Check Violations*) and a new severity of 5.0 (Medium) will be set.

5. In case the detection efficiency should be increased by applying local security checks it is required to configure remote access via the *Credentials* feature. If not done yet, create a corresponding user account on the Windows systems (a low privileged user account is sufficient).

6. Define the target systems (targets) and, if applicable, choose the respective credentials.

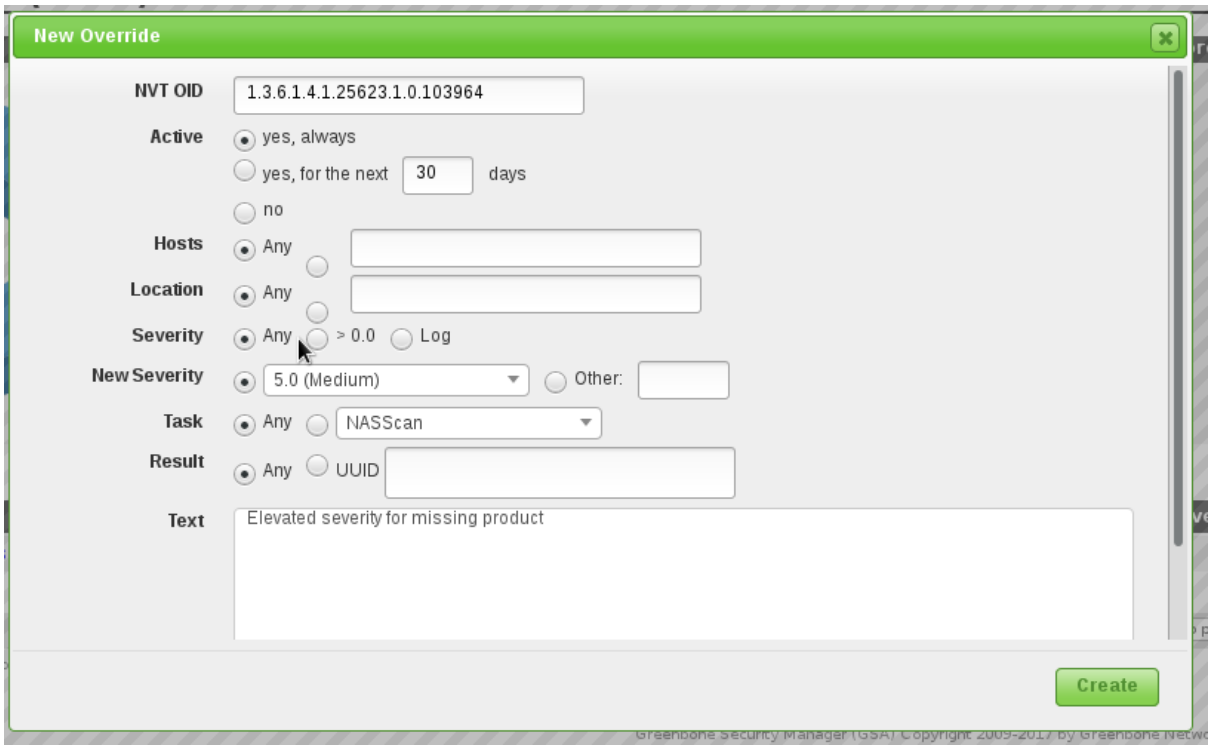
7. Now you can create the actual task. This means to combine the newly created scan configuration with the newly created targets.

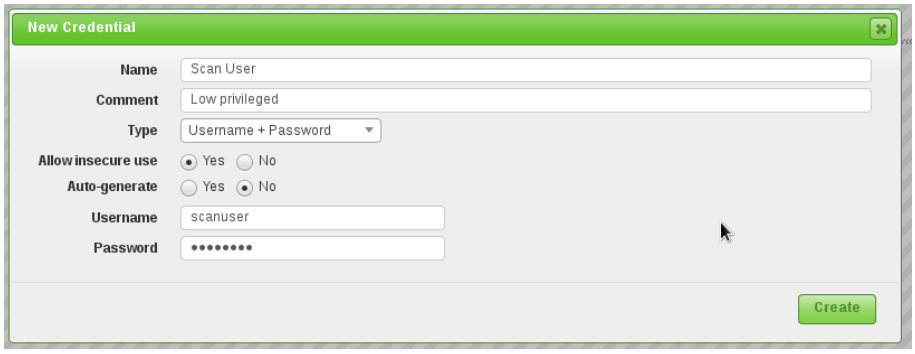
8. The scan is started by clicking on of the respective task. It can take a while for the scan to complete. To update the view with the current progress, click on .

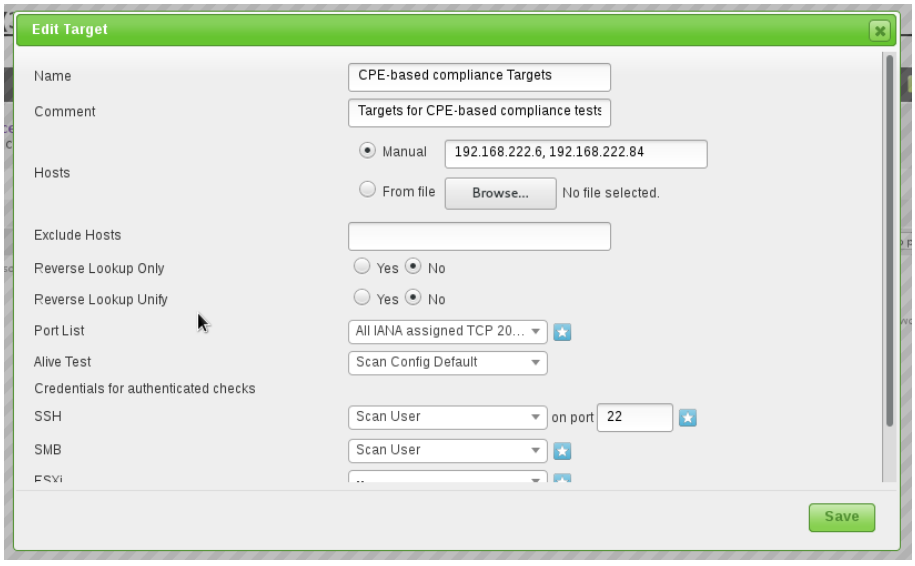
9. **As soon as the status changes to *Done* the complete report is available.** At any time you can review the intermediate results. To only show the results of the CPE-based policy checks, you can apply a suitable filter (search text "cpe").

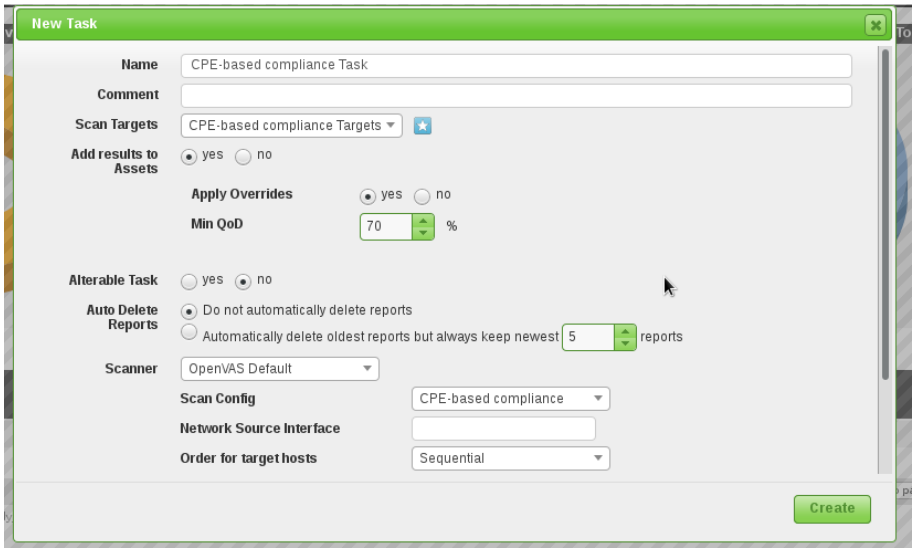
10. In this example ClamAV 0.99 was found on one of the target systems and reported as a log message.

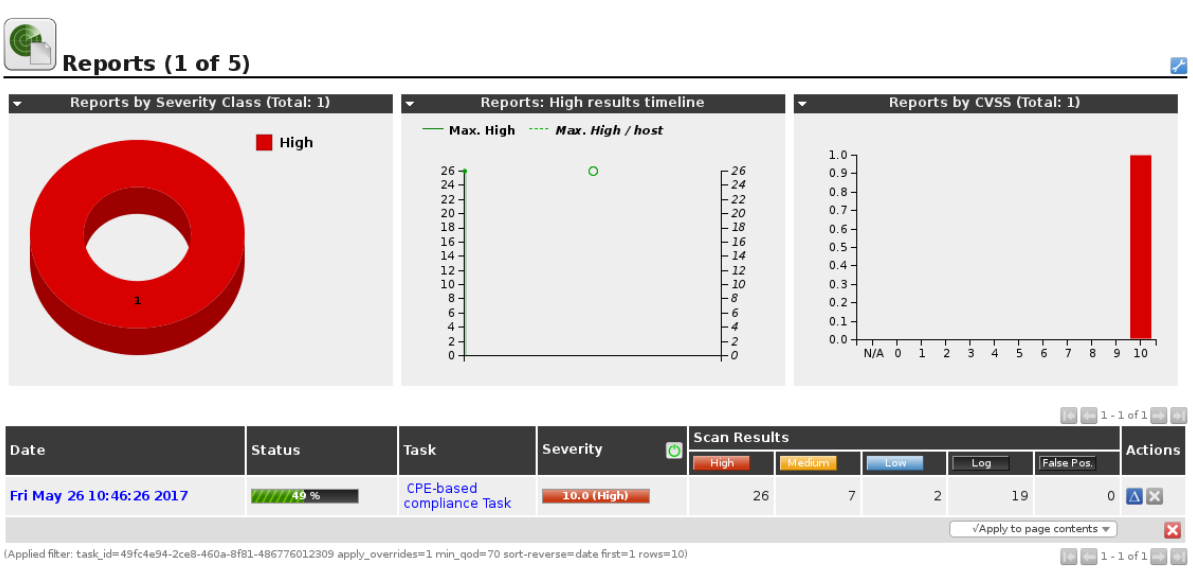
Internet Explorer 9 on the other hand haven't been found on the target system which will be reported as a medium risk as defined in the override.

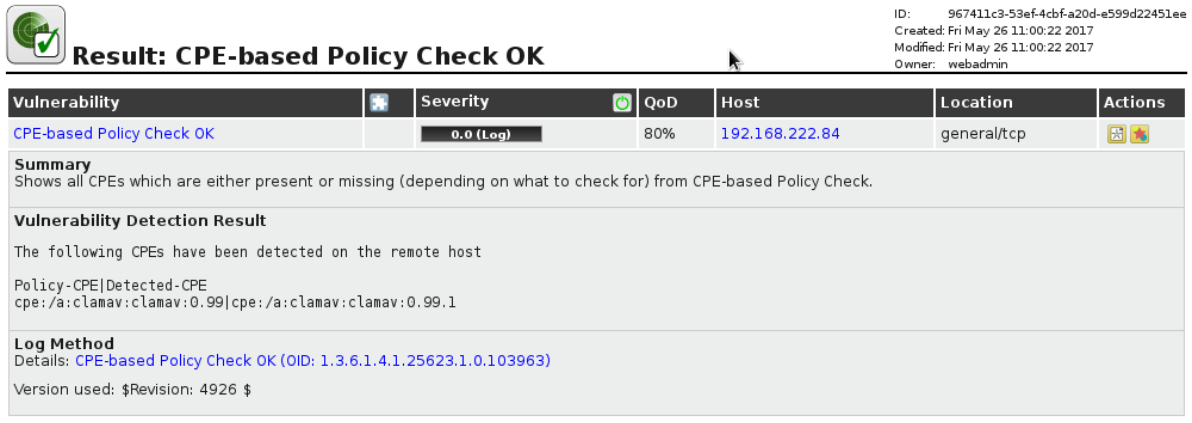

New Override
NVT OID
1.3.6.1.4.1.25623.1.0.103964
Active
yes, always
yes, for the next
30
days
no
Hosts
Any
Location
Any
Severity
Any
> 0.0
Log
New Severity
5.0 (Medium)
Other:
Task
Any
NASScan
Result
Any
UUID
Text
Elevated severity for missing product
Create


New Credential
Name
Scan User
Comment
Low privileged
Type
Username + Password
Allow insecure use
Yes
No
Auto-generate
Yes
No
Username
scanuser
Password
Create


Edit Target
Name
CPE-based compliance Targets
Comment
Targets for CPE-based compliance tests
Hosts
Manual
192.168.222.6, 192.168.222.84
From file
Browse...
No file selected.
Exclude Hosts
Reverse Lookup Only
Yes
No
Reverse Lookup Unify
Yes
No
Port List
All IANA assigned TCP 20...
Alive Test
Scan Config Default
Credentials for authenticated checks
SSH
Scan User
on port
22
SMB
Scan User
Save


New Task
Name
CPE-based compliance Task
Comment
Scan Targets
CPE-based compliance Targets
Add results to Assets
yes
no
Apply Overrides
yes
no
Min QoD
70
%
Alterable Task
yes
no
Auto Delete Reports
Do not automatically delete reports
Automatically delete oldest reports but always keep newest
5
reports
Scanner
OpenVAS Default
Scan Config
CPE-based compliance
Network Source Interface
Order for target hosts
Sequential
Create


Reports (1 of 5)
Reports by Severity Class (Total: 1)
High
Reports: High results timeline
Max. High
Max. High / host
Reports by CVSS (Total: 1)
Date
Status
Task
Severity
Scan Results
High
Medium
Low
Log
False Pos.
Actions
Fri May 26 10:46:26 2017
49 %
CPE-based compliance Task
10.0 (High)
26
7
2
19
0
Apply to page contents


Result: CPE-based Policy Check OK
ID: 967411c3-53ef-4cbf-a20d-e599d22451ee
Created: Fri May 26 11:00:22 2017
Modified: Fri May 26 11:00:22 2017
Owner: webadmin
Vulnerability
Severity
QoD
Host
Location
Actions
CPE-based Policy Check OK
0.0 (Log)
80%
192.168.222.84
general/tcp
Summary
Shows all CPEs which are either present or missing (depending on what to check for) from CPE-based Policy Check.
Vulnerability Detection Result
The following CPEs have been detected on the remote host
Policy-CPE|Detected-CPE
cpe:/a:clamav:clamav:0.99|cpe:/a:clamav:clamav:0.99.1
Log Method
Details: CPE-based Policy Check OK (OID: 1.3.6.1.4.1.25623.1.0.103963)
Version used: $Revision: 4926 $

Finding problematic products

This example demonstrates how the presence of a certain product in an IT infrastructure is classified as a severe problem and reported as such.

1. Execute steps 1 to 3 of the above described method for finding checking policy compliance.

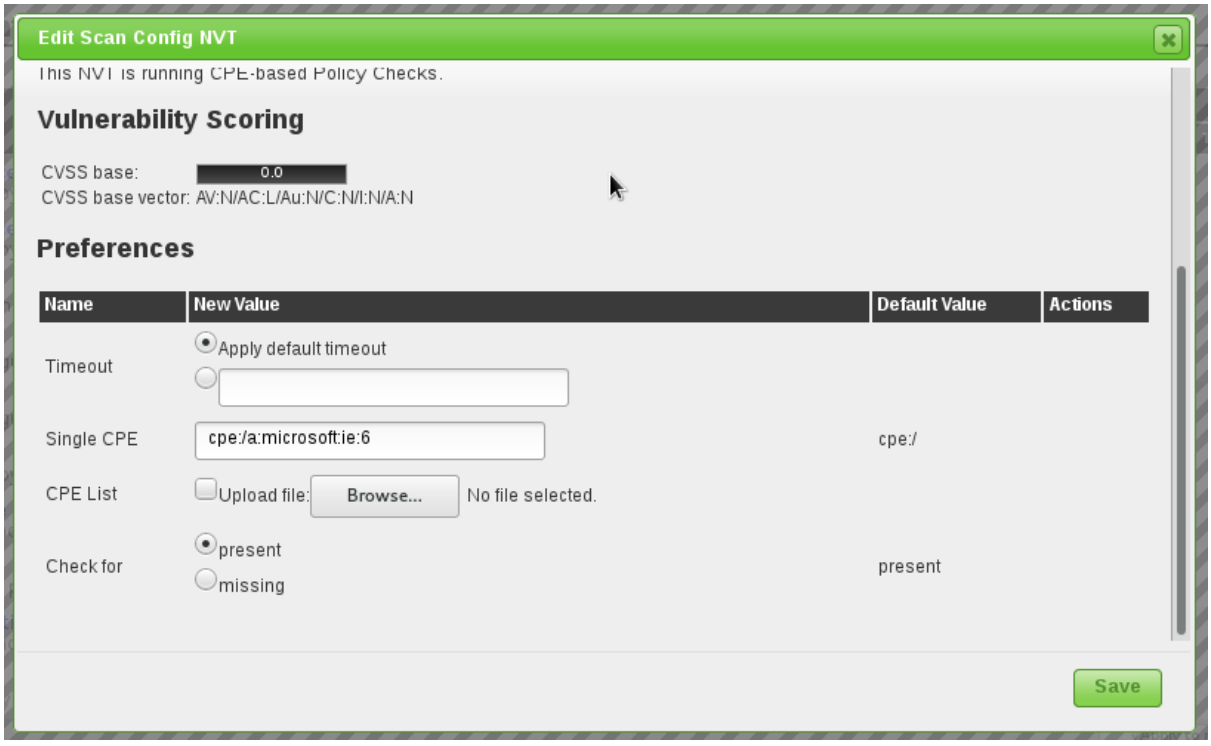
   Note that when choosing a general scan like *Full and Fast* both cases are treated the same, presence of the product as a running service and presence of the product on a hard drive.

   This essentially means that if you want to ensure the desired product indeed runs as a service you should avoid running NVTs that check for the simple presence on the file system or in a registry. If you don't want to go into such details right now, you still have the option to look into the report details in order to check for false positives and false negatives.

2. This time a single CPE (Internet Explorer 6) will be searched.

   In this case we have to set that the entered CPE must be “present”.

   Confirm your changes with *Save*.

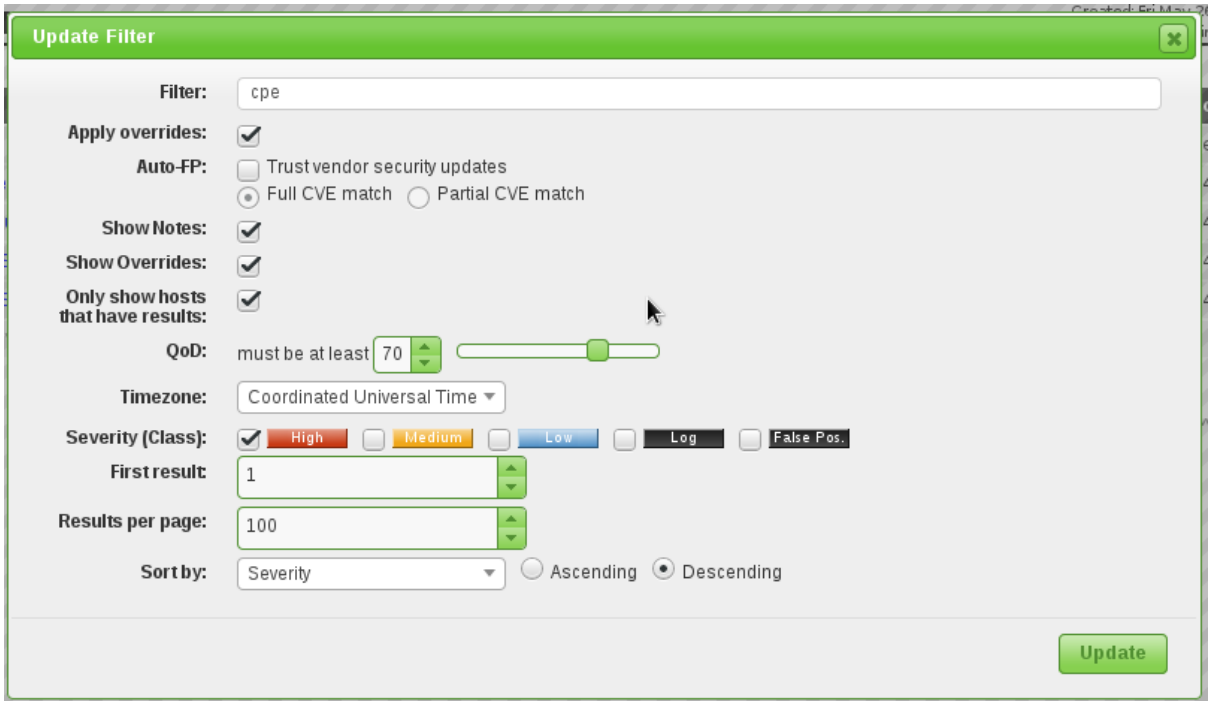


3. The severity of the NVTs depend on the GOS version used. Since GOS 4.2 the violation NVTs have a default score of 10. In the past these NVTs had a default score of 0 (log message) and overrides were required for different scores. The new default score of 10 can be changed using overrides as well. If you want to change this you have to create an override.

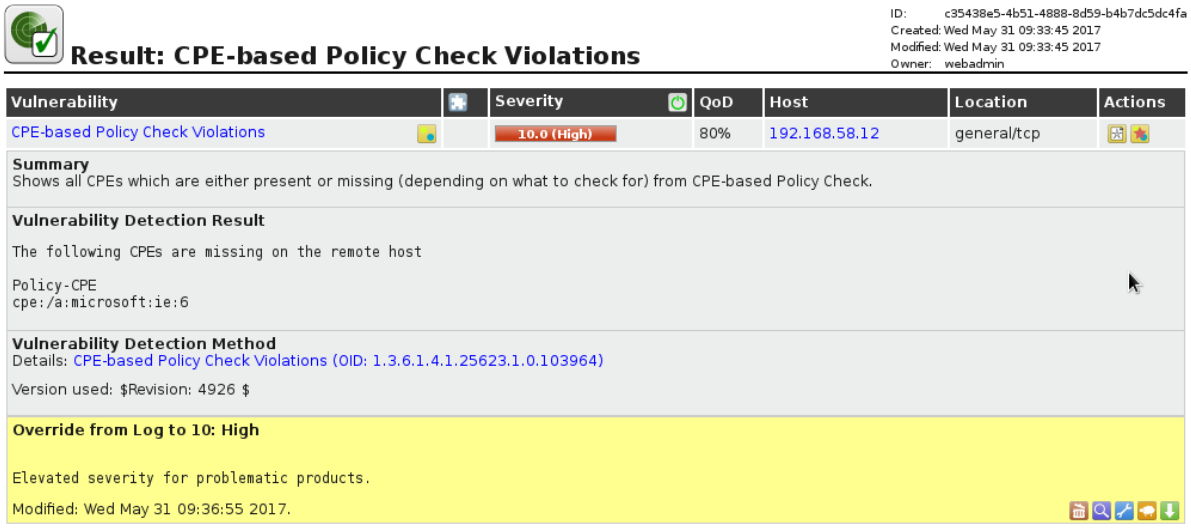
4. In case the pure presence of a product should be considered, you should apply local security checks by configuring remote access via the *Credentials* feature. Execute step 6 to 9 in the example above to enable local security checks, to create a new task with the target systems and to start it.

5. As soon as the status changes to *Done* the complete report is available. At any time you can review the intermediate results.

   To only show the results of the CPE-based policy checks, you can apply a suitable filter (search text "cpe").



6. In this example Internet Explorer 6 was found on one of the target systems and reported as a severe problem as defined in the override.



Detecting absence of important products

This example shows how the absence of a certain product in your IT infrastructure is defined as a severe problem and reported as such.

1. Execute steps 1 to 3 of the above described method for finding problematic products.

   Note that when choosing a general scan like *Full and Fast* both cases are treated the same, presence of the product as a running service and presence of the product on a hard drive.

   This essentially means that if you want to ensure the desired product indeed runs as a service you should avoid running NVTs that check for the simple presence on the file system or in a registry. If you don't want to go into such details right now, you still have the option to look into the report details in order to check for false positives and false negatives.

2. This time the configuration of *CPE-based Policy Check* will be set up to check if Norton Antivirus is present on the target system. In this case it will be reported if it is "missing".

3. The severity of the NVTs depend on the GOS version used. Since GOS 4.2 the violation NVTs have a default score of 10. In the past these NVTs had a default score of 0 (log message) and overrides were required for different scores. The new default score of 10 can be changed using overrides as well. If you want to change this you have to create an override.

4. For checking simply the availability of a product installation, local security checks can improve the detection rate. If just running network services should be searched it normally doesn't help but rather increase the number of false positives.

   Execute step 6 to 9 in the example *Checking policy compliance* (page 169) to enable local security checks, to create a new task with the target systems and to start it.

5. As soon as the status changes to *Done* the complete report is available. At any time you can review the intermediate results.

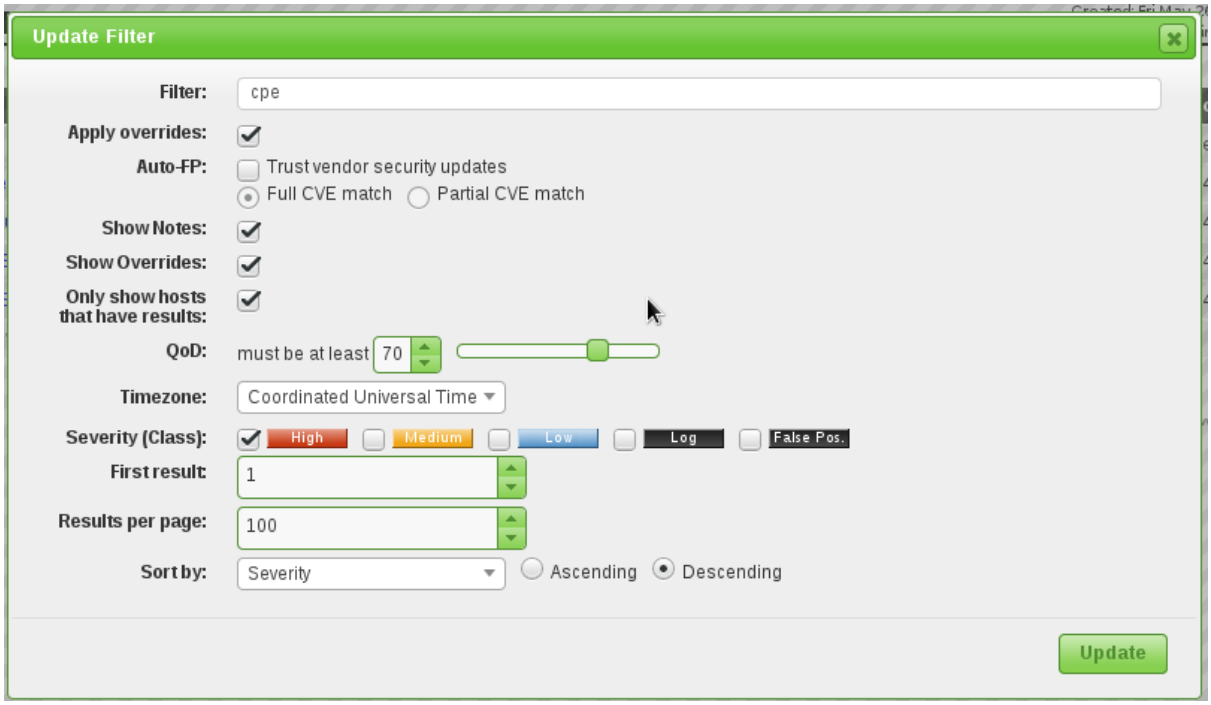
   To only show the results of the CPE-based policy checks, you can apply a suitable filter (search text "cpe").

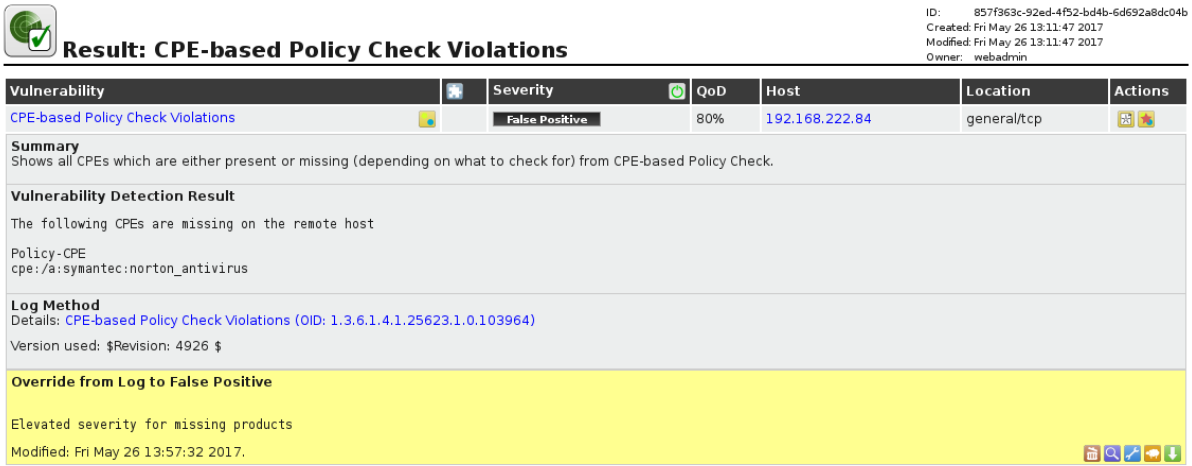
6. In this example Norton Antivirus was not found on one of the target systems.

11.2 Standard Policies

11.2.1 IT-Grundschutz

With the Greenbone Security Manager it is possible to automatically check either the German "IT-Grundschutz-Kataloge" or the modernized "IT-Grundschutz-Kompendium" as published and main-


Update Filter
Filter:
cpe
Apply overrides:
Auto-FP:
Trust vendor security updates
Full CVE match
Partial CVE match
Show Notes:
Show Overrides:
Only show hosts that have results:
QoD:
must be at least
70
Timezone:
Coordinated Universal Time
Severity (Class):
High
Medium
Low
Log
False Pos.
First result:
1
Results per page:
100
Sort by:
Severity
Ascending
Descending
Update


Result: CPE-based Policy Check Violations
ID: 857f363c-92ed-4f52-bd4b-6d692a8dc04b
Created: Fri May 26 13:11:47 2017
Modified: Fri May 26 13:11:47 2017
Owner: webadmin
Vulnerability
Severity
QoD
Host
Location
Actions
CPE-based Policy Check Violations
False Positive
80%
192.168.222.84
general/tcp
Summary
Shows all CPEs which are either present or missing (depending on what to check for) from CPE-based Policy Check.
Vulnerability Detection Result
The following CPEs are missing on the remote host
Policy-CPE
cpe:/a:symantec:norton_antivirus
Log Method
Details: CPE-based Policy Check Violations (OID: 1.3.6.1.4.1.25623.1.0.103964)
Version used: $Revision: 4926 $
Override from Log to False Positive
Elevated severity for missing products
Modified: Fri May 26 13:57:32 2017.

tained by the Bundesamt für Sicherheit in der Informationstechnik[26] (German Federal Office for IT Security, BSI).

The current "15. Ergänzungslieferung" with tests for over 80 measures is supported for the "IT-Grundschutz-Kataloge". That is the maximum number of measures which is possible to support with automatic tests.

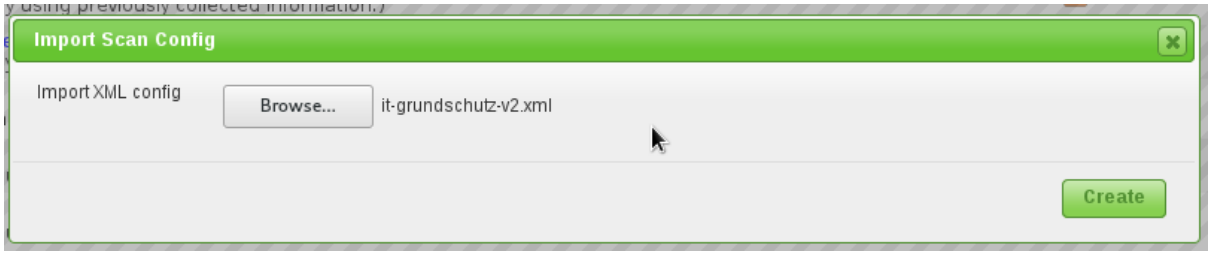
Some measures are quite comprehensive so that and actually consist of several single tests. A couple of measures address a specific operating system ans hence will only be applied to those. The number and type of tested systems remains irrelevant for the Greenbone Security Manager.

This makes the Greenbone Security Manager the fastest co-worker for executing a IT-Grundschutz audit. And it opens the opportunity to install a check for breaches as a permanent background process.

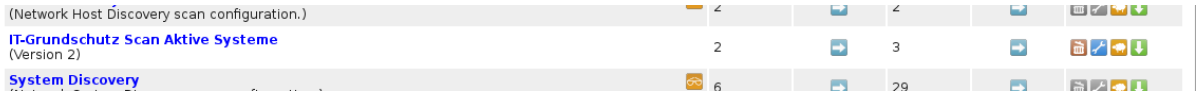
Checking IT-Grundschutz

This example executes a check according to the German "IT-Grundschutz", where you can select between "IT-Grundschutz-Kataloge" and "IT-Grundschutz-Kompendium".

1. Import the scan configuration using the Upload Button IT-Grundschutz Scan[27]. For verinice integration use the following configuration: IT-Grundschutz Scan incl. Discovery for verinice[28]



This covers the settings to execute all of the checks. The actual checks are not explicitly selected so that rather a summary result is generated.



1.1. To test for "IT-Grundschutz-Kataloge", please click the Edit Button of the scan configuration and click again the Edit Button to edit the family "Compliance". Two NVTs are selected per default ("IT-Grundschutz, 15. EL" and "Compliance Tests").

In "Compliance Tests", turn "Launch IT-Grundschutz (15. EL)" to "yes".

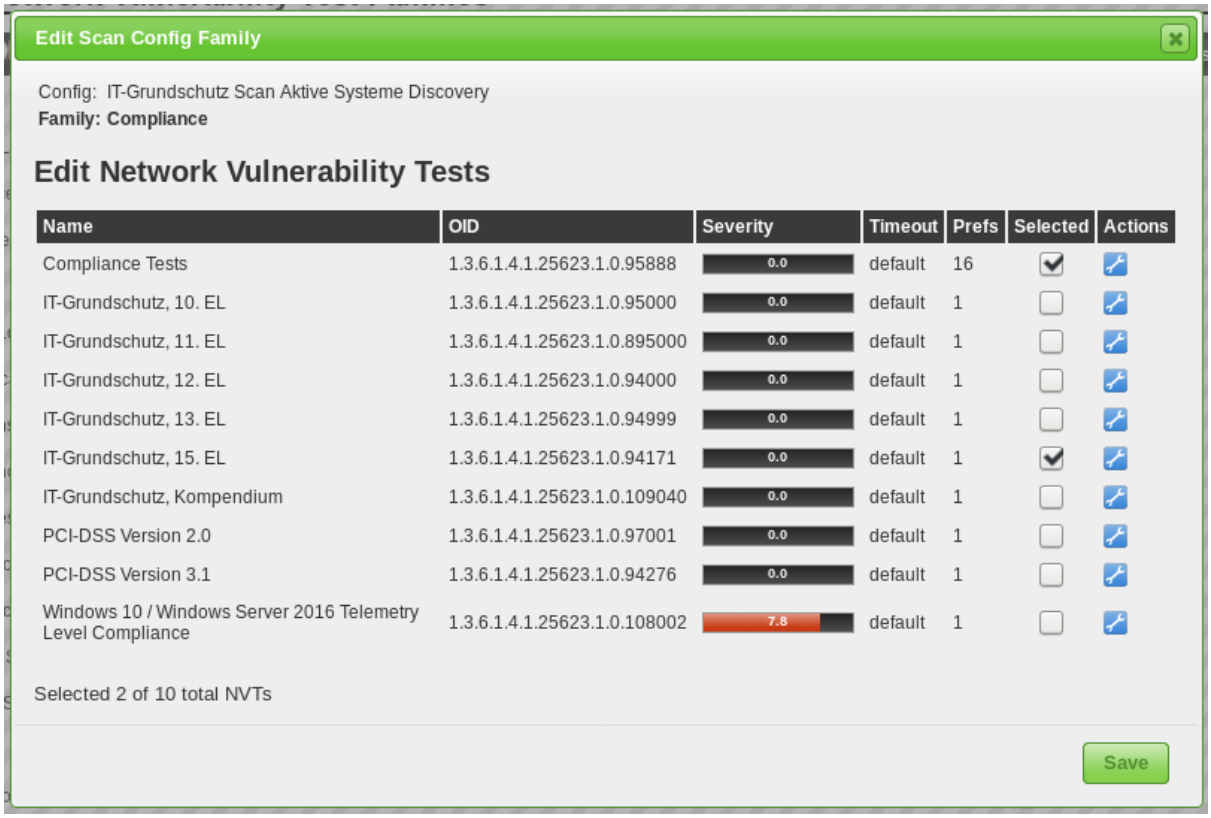
1.2. To test for "IT-Grundschutz-Kompendium", please click the Edit Button of the scan configuration and click again the Edit Button to edit the family "Compliance". Select "IT-Grundschutz, Kompendium" and "Compliance Tests".

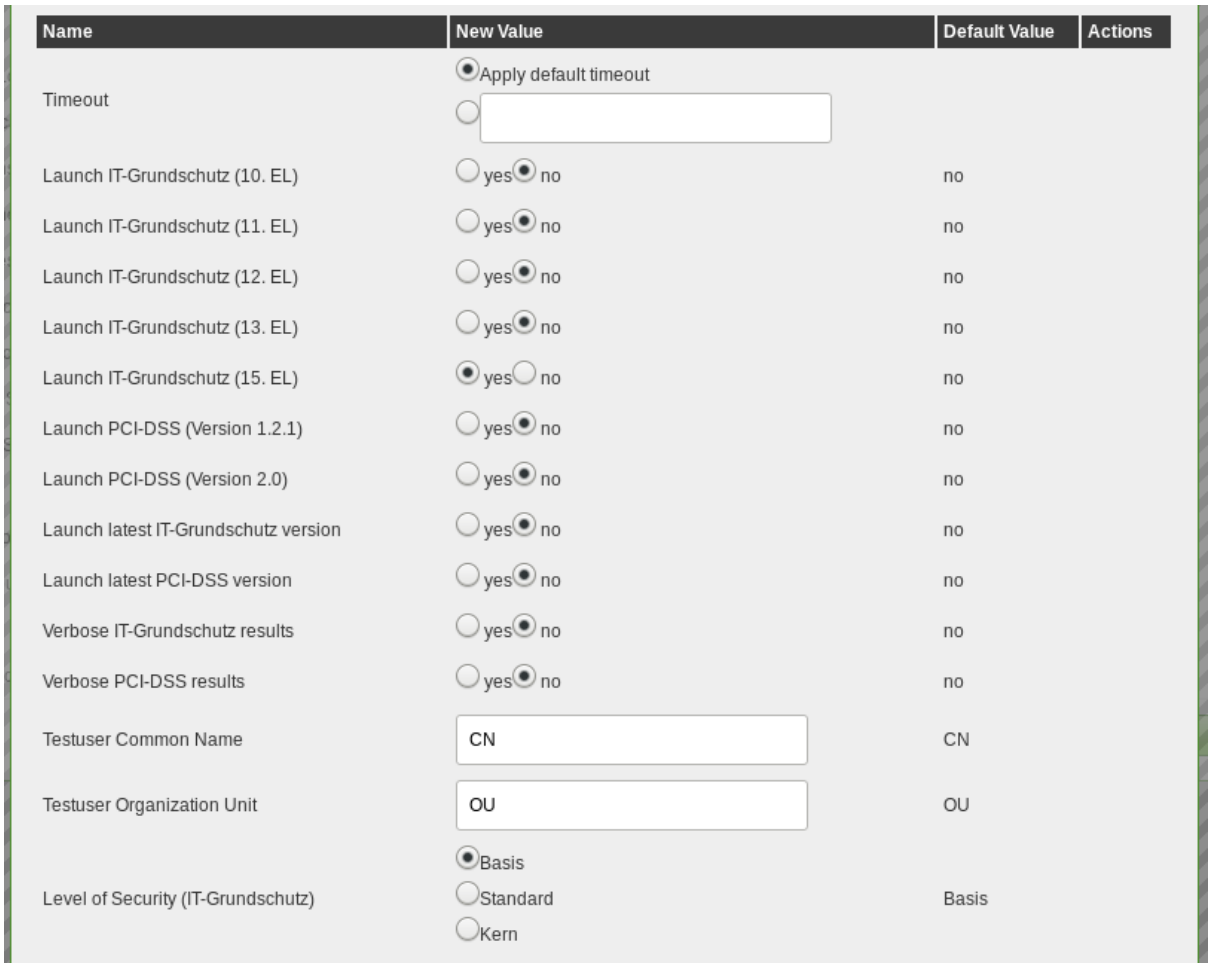
In "Compliance Tests", select "Launch latest IT-Grundschutz version" and choose the "Level of Security" (Basis, Standard, Kern), which was introduced in the modernized "IT-Grundschutz-Kompendium".

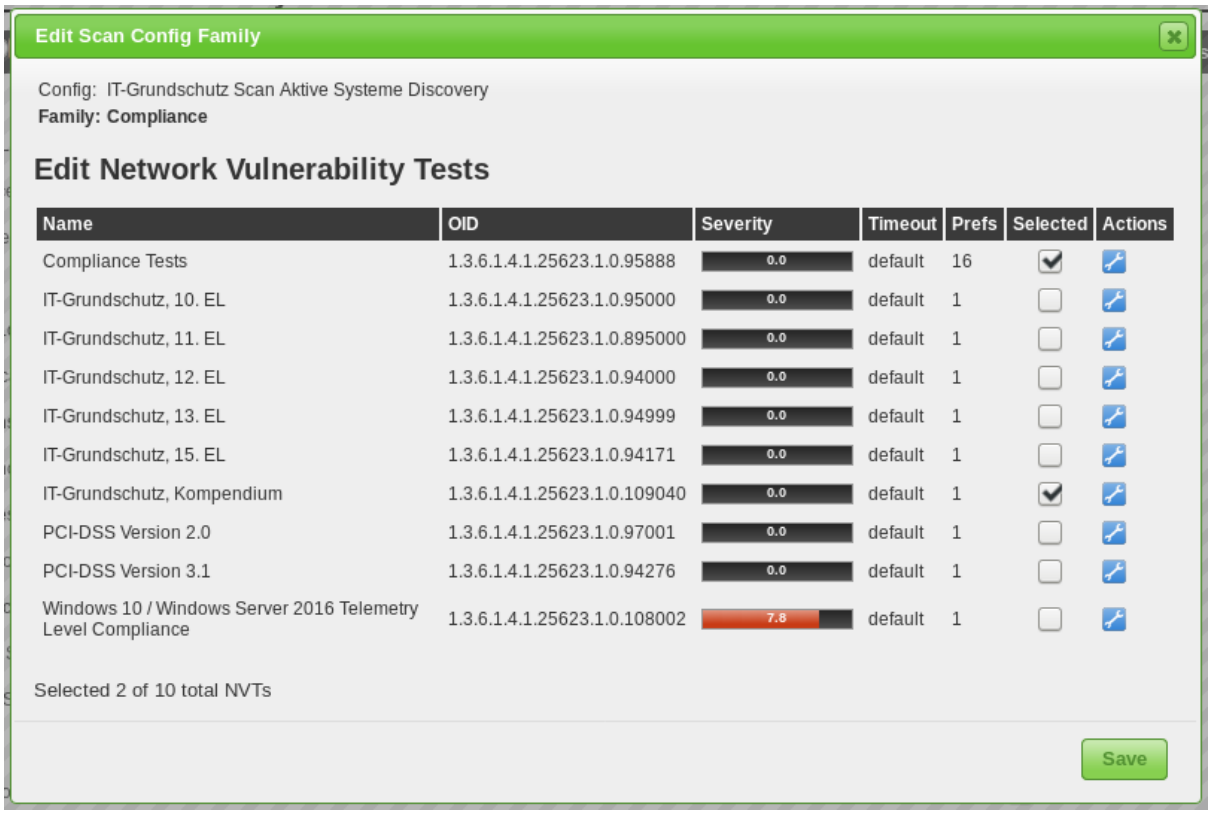
Regardless if you scan for "IT-Grundschutz-Kataloge" or "IT-Grundschutz-Kompendium", you can choose the report format by clicking the Edit Button of the selected NVT ("IT-Grundschutz, Kompendium" or "IT-Grundschutz, 15. EL"). Select "Text" to get a textual report format, "Tabellarisch" to get a tabular report format or "Text und Tabellarisch" to get both report formats.

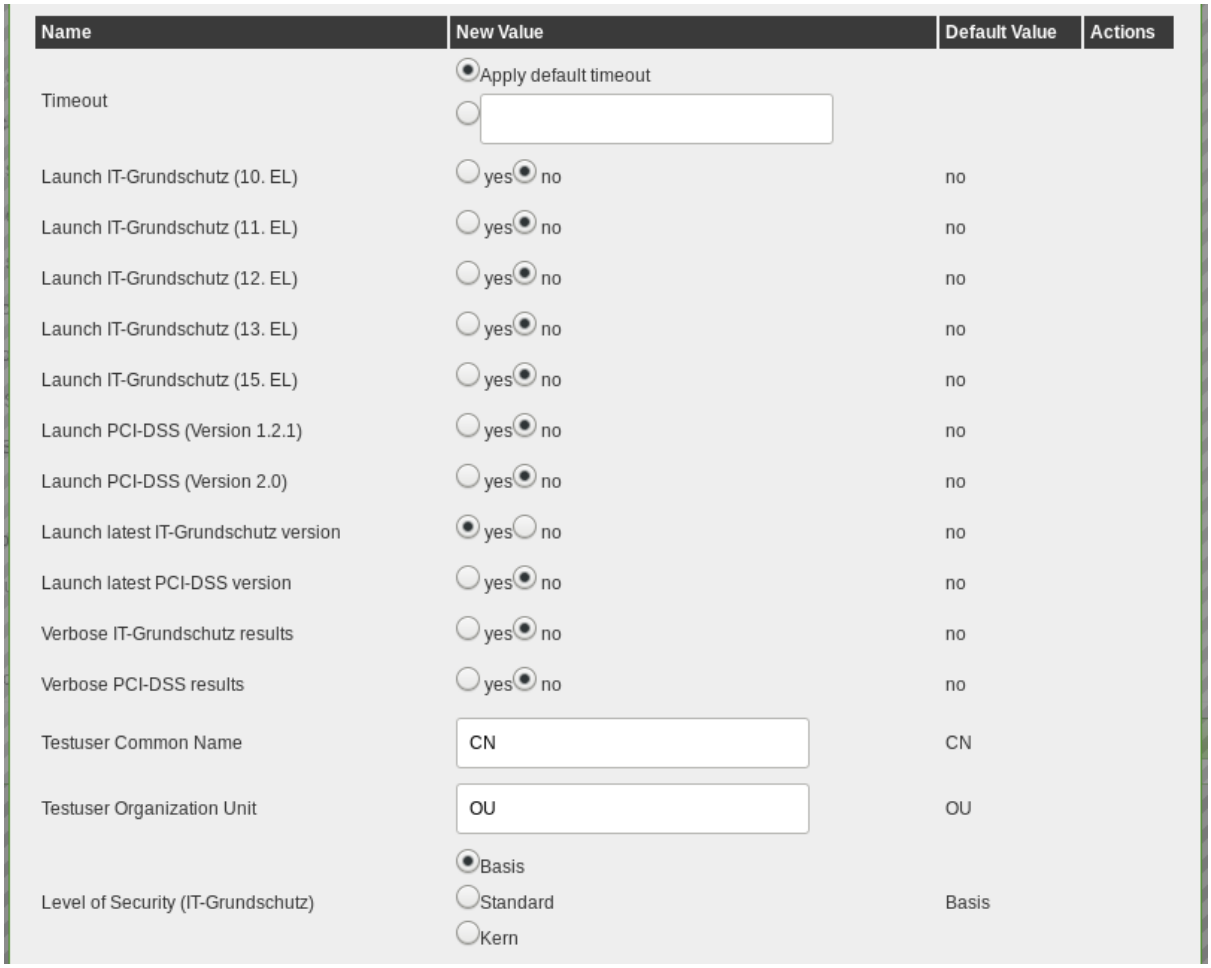
The following example executes a simple check according to the German "IT-Grundschutz-Kataloge", but is similar to the "IT-Grundschutz-Kompendium".

[26] http://www.bsi.de
[27] http://download.greenbone.net/scanconfigs/it-grundschutz-v2.xml
[28] http://download.greenbone.net/scanconfigs/it-grundschutz-discovery-v2.xml

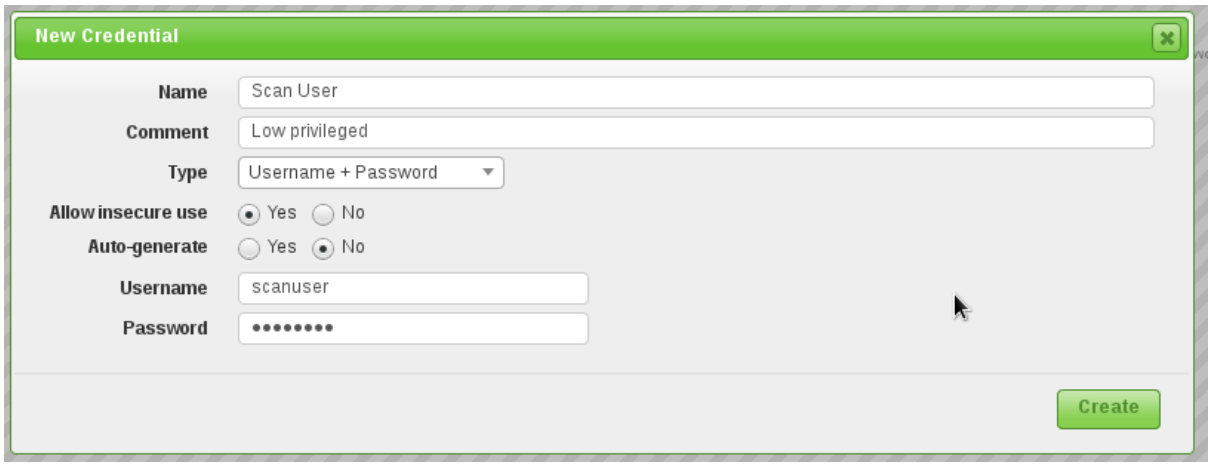

Edit Scan Config Family
Config: IT-Grundschutz Scan Aktive Systeme Discovery
Family: Compliance
Edit Network Vulnerability Tests
Name
OID
Severity
Timeout
Prefs
Selected
Actions
Compliance Tests 1.3.6.1.4.1.25623.1.0.95888 0.0 default 16
IT-Grundschutz, 10. EL 1.3.6.1.4.1.25623.1.0.95000 0.0 default 1
IT-Grundschutz, 11. EL 1.3.6.1.4.1.25623.1.0.895000 0.0 default 1
IT-Grundschutz, 12. EL 1.3.6.1.4.1.25623.1.0.94000 0.0 default 1
IT-Grundschutz, 13. EL 1.3.6.1.4.1.25623.1.0.94999 0.0 default 1
IT-Grundschutz, 15. EL 1.3.6.1.4.1.25623.1.0.94171 0.0 default 1
IT-Grundschutz, Kompendium 1.3.6.1.4.1.25623.1.0.109040 0.0 default 1
PCI-DSS Version 2.0 1.3.6.1.4.1.25623.1.0.97001 0.0 default 1
PCI-DSS Version 3.1 1.3.6.1.4.1.25623.1.0.94276 0.0 default 1
Windows 10 / Windows Server 2016 Telemetry Level Compliance 1.3.6.1.4.1.25623.1.0.108002 7.8 default 1
Selected 2 of 10 total NVTs
Save


Name
New Value
Default Value
Actions
Timeout
Apply default timeout
Launch IT-Grundschutz (10. EL) yes no no
Launch IT-Grundschutz (11. EL) yes no no
Launch IT-Grundschutz (12. EL) yes no no
Launch IT-Grundschutz (13. EL) yes no no
Launch IT-Grundschutz (15. EL) yes no no
Launch PCI-DSS (Version 1.2.1) yes no no
Launch PCI-DSS (Version 2.0) yes no no
Launch latest IT-Grundschutz version yes no no
Launch latest PCI-DSS version yes no no
Verbose IT-Grundschutz results yes no no
Verbose PCI-DSS results yes no no
Testuser Common Name CN CN
Testuser Organization Unit OU OU
Level of Security (IT-Grundschutz) Basis Standard Kern Basis


Edit Scan Config Family
Config: IT-Grundschutz Scan Aktive Systeme Discovery
Family: Compliance
Edit Network Vulnerability Tests
Name
OID
Severity
Timeout
Prefs
Selected
Actions
Compliance Tests 1.3.6.1.4.1.25623.1.0.95888 0.0 default 16
IT-Grundschutz, 10. EL 1.3.6.1.4.1.25623.1.0.95000 0.0 default 1
IT-Grundschutz, 11. EL 1.3.6.1.4.1.25623.1.0.895000 0.0 default 1
IT-Grundschutz, 12. EL 1.3.6.1.4.1.25623.1.0.94000 0.0 default 1
IT-Grundschutz, 13. EL 1.3.6.1.4.1.25623.1.0.94999 0.0 default 1
IT-Grundschutz, 15. EL 1.3.6.1.4.1.25623.1.0.94171 0.0 default 1
IT-Grundschutz, Kompendium 1.3.6.1.4.1.25623.1.0.109040 0.0 default 1
PCI-DSS Version 2.0 1.3.6.1.4.1.25623.1.0.97001 0.0 default 1
PCI-DSS Version 3.1 1.3.6.1.4.1.25623.1.0.94276 0.0 default 1
Windows 10 / Windows Server 2016 Telemetry Level Compliance 1.3.6.1.4.1.25623.1.0.108002 7.8 default 1
Selected 2 of 10 total NVTs
Save


Name
New Value
Default Value
Actions
Timeout
Apply default timeout
Launch IT-Grundschutz (10. EL) yes no no
Launch IT-Grundschutz (11. EL) yes no no
Launch IT-Grundschutz (12. EL) yes no no
Launch IT-Grundschutz (13. EL) yes no no
Launch IT-Grundschutz (15. EL) yes no no
Launch PCI-DSS (Version 1.2.1) yes no no
Launch PCI-DSS (Version 2.0) yes no no
Launch latest IT-Grundschutz version yes no no
Launch latest PCI-DSS version yes no no
Verbose IT-Grundschutz results yes no no
Verbose PCI-DSS results yes no no
Testuser Common Name CN CN
Testuser Organization Unit OU OU
Level of Security (IT-Grundschutz) Basis Standard Kern Basis

2. The majority of checks for the measures is based on local security checks. For these a respective access needs to be configured. If not done yet, create a corresponding user account on the Windows systems (the higher the privileges of this user account, the more measures can be checked).



3. Define the target systems (targets) and, if applicable, choose the respective credentials.
4. Now you can create the actual task. This means to combine the imported scan configuration with the newly created targets.
5. The search is started by clicking on of the respective task. It can take a while for the scan to complete. To update the view with the current progress, click on .
6. As soon as the status changes to “Done” the complete report is available. At any time you can review the intermediate results. Please note, that for the textual form of the reports you need to enable category “Low” in the filter.

   With the imported scan configuration 2 versions of the results will be created: an overview in textual form (under “general/IT-Grundschutz”) and a table for further processing (under “general/IT-Grundschutz-T”). For the latter, you need to enable category “Log” in the report filter

Import of results into a spreadsheet application

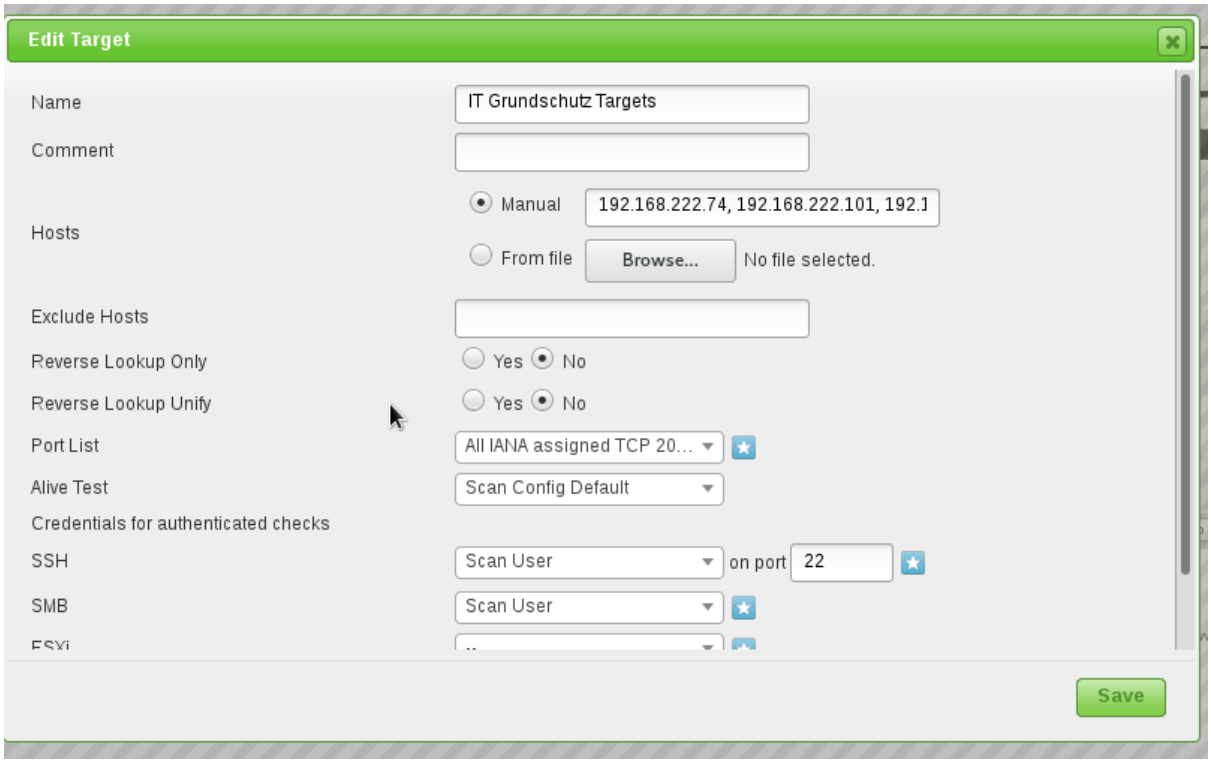
1. Choose download format “ITG” either in the report filter or in the task overview. *Note*: Using the report filter it is necessary to enable the category “Log”.

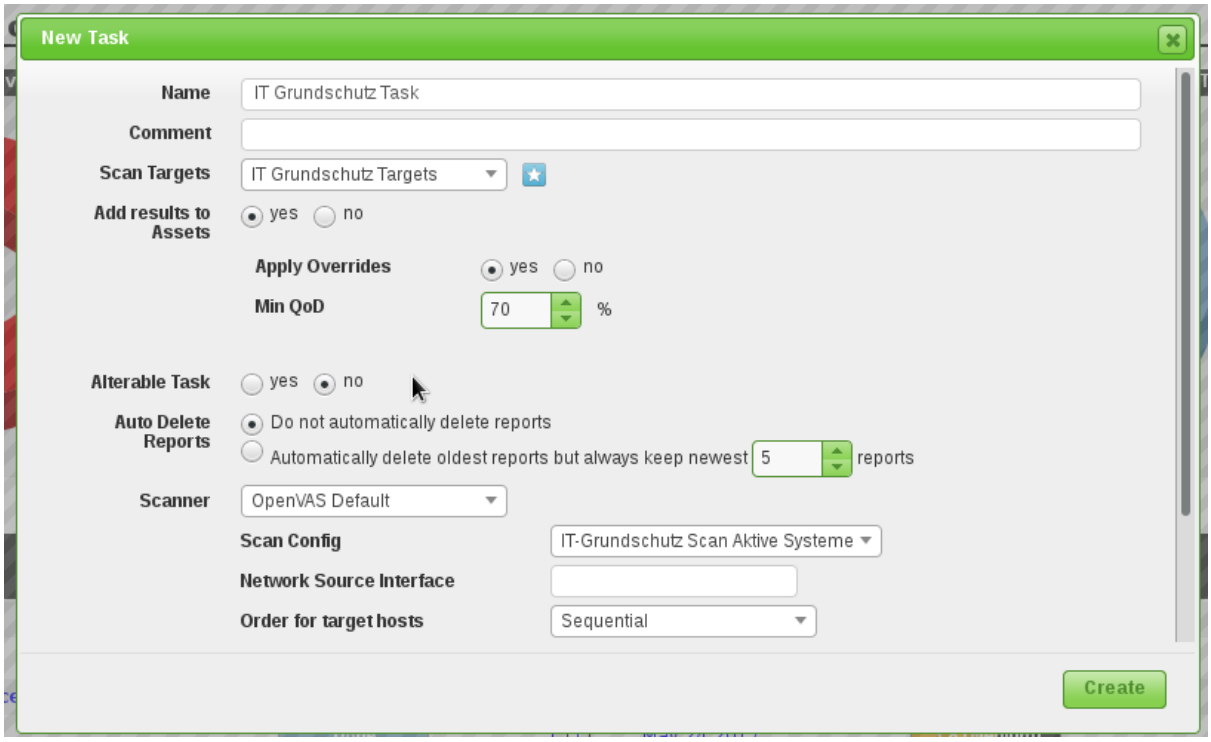
For this download format suitable tabular results for all target systems are automatically collected and joined.

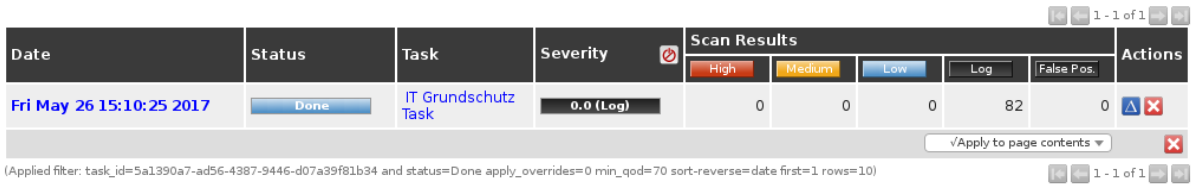
2. Import the ITG file as so called CSV table into your spreadsheet application.

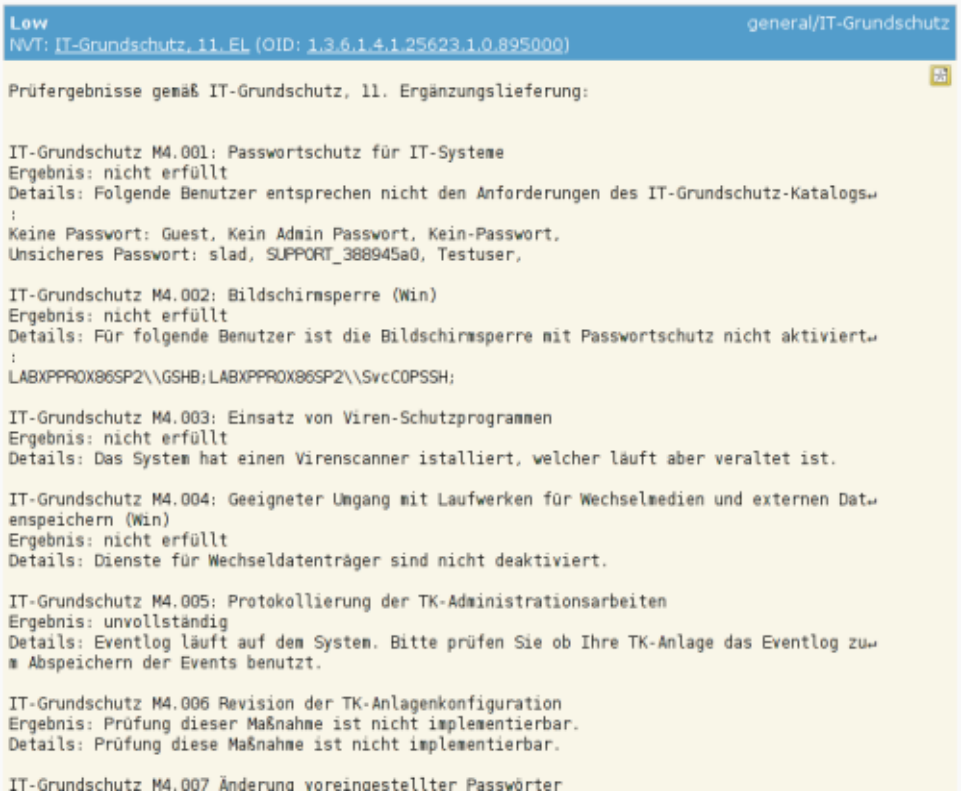
The example above shows an import for OpenOffice 3.2. Please take care that the following settings are adjusted for the import (if not already default):

- Charset: UTF-8


Edit Target
Name
IT Grundschutz Targets
Comment
Hosts
Manual
192.168.222.74, 192.168.222.101, 192.1
From file
Browse...
No file selected.
Exclude Hosts
Reverse Lookup Only
Yes
No
Reverse Lookup Unify
Yes
No
Port List
All IANA assigned TCP 20...
Alive Test
Scan Config Default
Credentials for authenticated checks
SSH
Scan User
on port
22
SMB
Scan User
Save

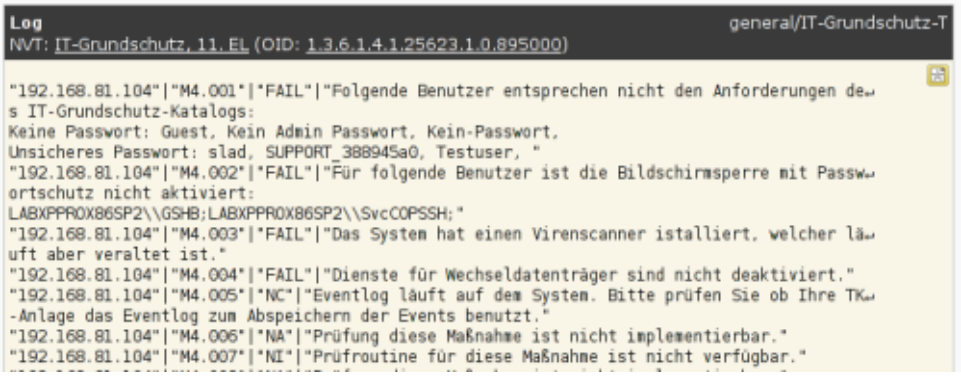

New Task
Name
IT Grundschutz Task
Comment
Scan Targets
IT Grundschutz Targets
Add results to Assets
yes
no
Apply Overrides
yes
no
Min QoD
70
%
Alterable Task
yes
no
Auto Delete Reports
Do not automatically delete reports
Automatically delete oldest reports but always keep newest
5
reports
Scanner
OpenVAS Default
Scan Config
IT-Grundschutz Scan Aktive Systeme
Network Source Interface
Order for target hosts
Sequential
Create


1 - 1 of 1
Date
Status
Task
Severity
Scan Results
High
Medium
Low
Log
False Pos.
Actions
Fri May 26 15:10:25 2017
Done
IT Grundschutz Task
0.0 (Log)
0
0
0
82
0
√Apply to page contents
(Applied filter: task_id=5a1390a7-ad56-4387-9446-d07a39f81b34 and status=Done apply_overrides=0 min_qod=70 sort-reverse=date first=1 rows=10)
1 - 1 of 1



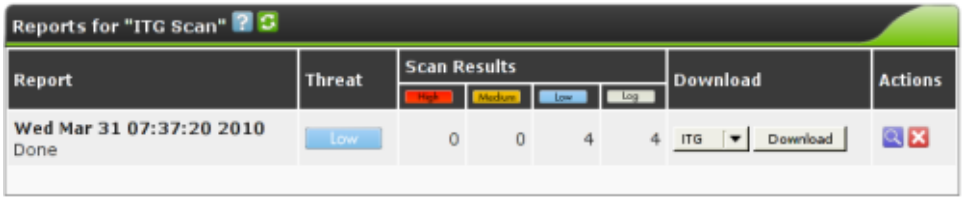
Low general/IT-Grundschutz
NVT: IT-Grundschutz, 11. EL (OID: 1.3.6.1.4.1.25623.1.0.895000)

```
Prüfergebnisse gemäß IT-Grundschutz, 11. Ergänzungslieferung:


IT-Grundschutz M4.001: Passwortschutz für IT-Systeme
Ergebnis: nicht erfüllt
Details: Folgende Benutzer entsprechen nicht den Anforderungen des IT-Grundschutz-Katalogs
:
Keine Passwort: Guest, Kein Admin Passwort, Kein-Passwort,
Unsicheres Passwort: slad, SUPPORT_388945a0, Testuser,

IT-Grundschutz M4.002: Bildschirmsperre (Win)
Ergebnis: nicht erfüllt
Details: Für folgende Benutzer ist die Bildschirmsperre mit Passwortschutz nicht aktiviert
:
LABXPPROX86SP2\\GSHB;LABXPPROX86SP2\\SvcCOPSSH;

IT-Grundschutz M4.003: Einsatz von Viren-Schutzprogrammen
Ergebnis: nicht erfüllt
Details: Das System hat einen Virenscanner istalliert, welcher läuft aber veraltet ist.

IT-Grundschutz M4.004: Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Dat
enspeichern (Win)
Ergebnis: nicht erfüllt
Details: Dienste für Wechseldatenträger sind nicht deaktiviert.

IT-Grundschutz M4.005: Protokollierung der TK-Administrationsarbeiten
Ergebnis: unvollständig
Details: Eventlog läuft auf dem System. Bitte prüfen Sie ob Ihre TK-Anlage das Eventlog zu
m Abspeichern der Events benutzt.

IT-Grundschutz M4.006 Revision der TK-Anlagenkonfiguration
Ergebnis: Prüfung dieser Maßnahme ist nicht implementierbar.
Details: Prüfung diese Maßnahme ist nicht implementierbar.

IT-Grundschutz M4.007 Änderung voreingestellter Passwörter
```



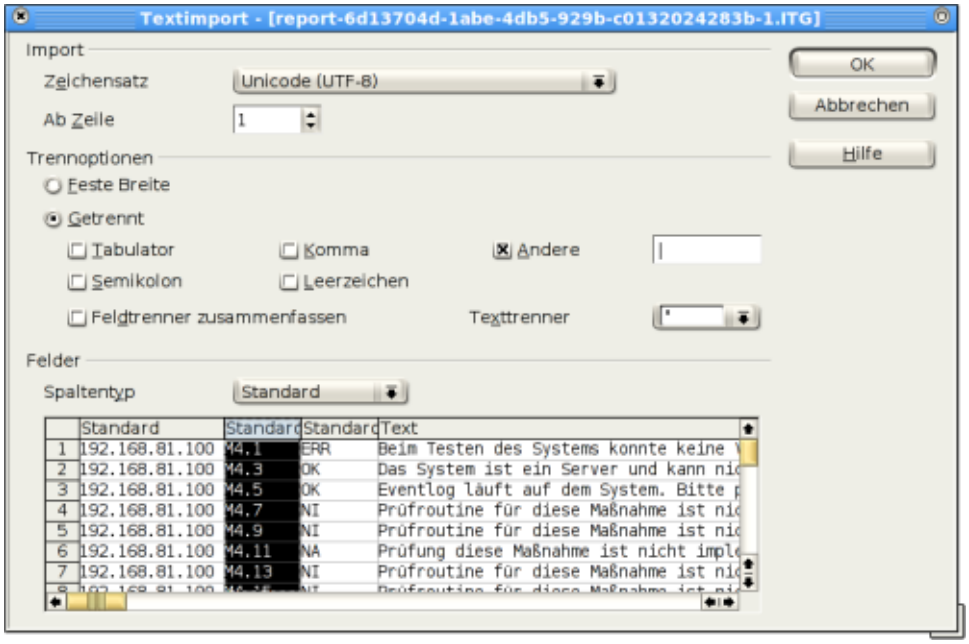
Log general/IT-Grundschutz-T
NVT: IT-Grundschutz, 11. EL (OID: 1.3.6.1.4.1.25623.1.0.895000)

```
"192.168.81.104"|"M4.001"|"FAIL"|"Folgende Benutzer entsprechen nicht den Anforderungen de
s IT-Grundschutz-Katalogs:
Keine Passwort: Guest, Kein Admin Passwort, Kein-Passwort,
Unsicheres Passwort: slad, SUPPORT_388945a0, Testuser, "
"192.168.81.104"|"M4.002"|"FAIL"|"Für folgende Benutzer ist die Bildschirmsperre mit Passw
ortschutz nicht aktiviert:
LABXPPROX86SP2\\GSHB;LABXPPROX86SP2\\SvcCOPSSH;"
"192.168.81.104"|"M4.003"|"FAIL"|"Das System hat einen Virenscanner istalliert, welcher lä
uft aber veraltet ist."
"192.168.81.104"|"M4.004"|"FAIL"|"Dienste für Wechseldatenträger sind nicht deaktiviert."
"192.168.81.104"|"M4.005"|"NC"|"Eventlog läuft auf dem System. Bitte prüfen Sie ob Ihre TK
-Anlage das Eventlog zum Abspeichern der Events benutzt."
"192.168.81.104"|"M4.006"|"NA"|"Prüfung diese Maßnahme ist nicht implementierbar."
"192.168.81.104"|"M4.007"|"NI"|"Prüfroutine für diese Maßnahme ist nicht verfügbar."
```



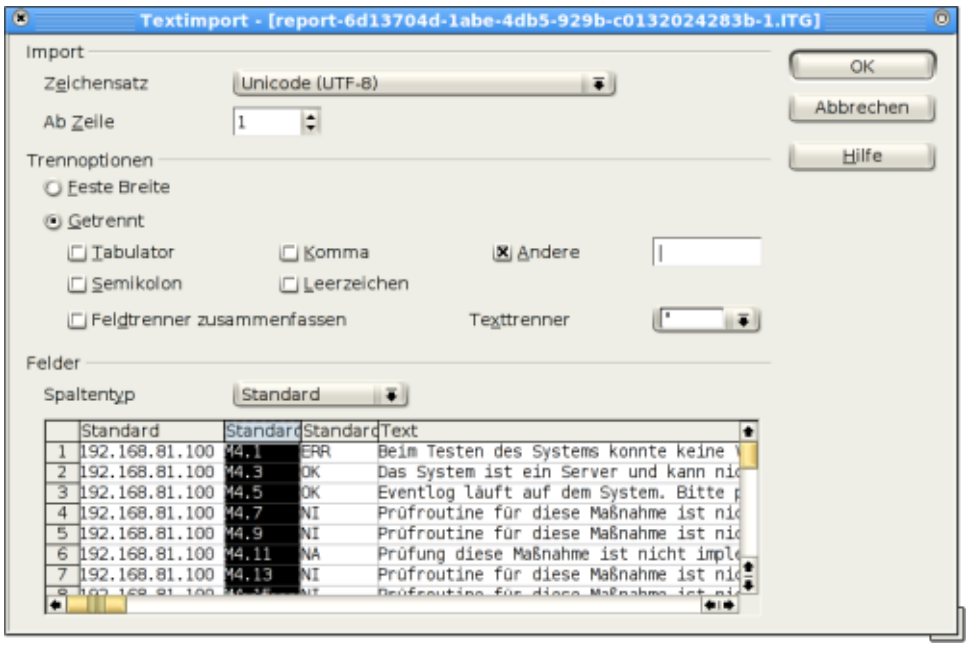
Reports for "ITG Scan"

Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Wed Mar 31 07:37:20 2010 Done	Low	0	0	4	4	ITG Download	



- Field separator: The “pipe” symbol (vertical line)
- Text separator: The double quote
- Last column: Type “Text”

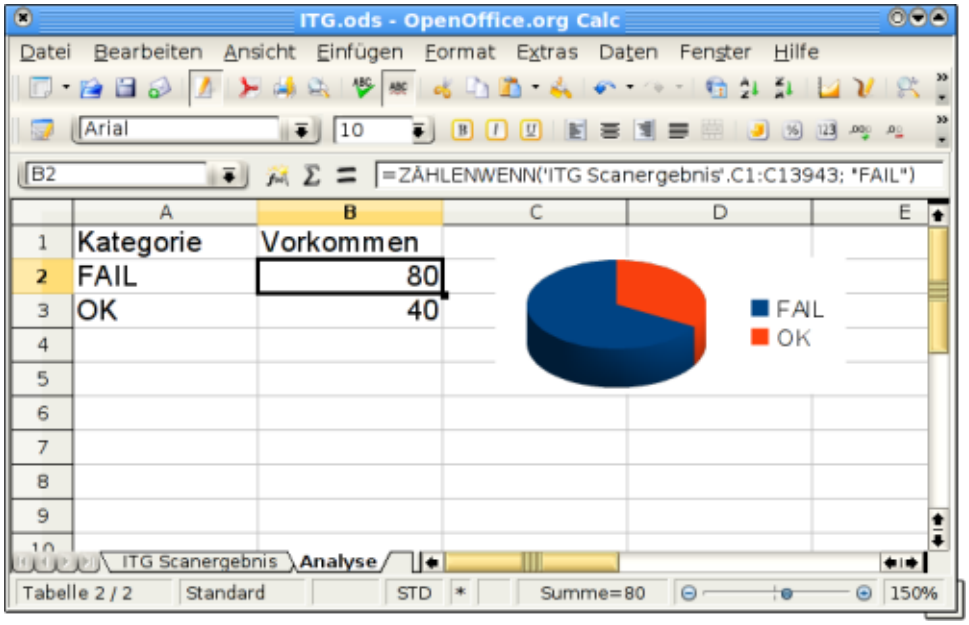
3. Now the scan results are available in the spreadsheet application:



4. From this point you can create simple (like in the screen shot below) or, of course, your individual comprehensive analysis or report.

Import of results into IT-Grundschutz tools

A number of tools is available to help IT-Grundschutz processes with structured approach, data entries and management.



The German federal agency for IT security (Bundesamt für Sicherheit in der Informationstechnik, BSI) offers on its website an overview on IT-Grundschutz tools[29].

For an import of the results of a IT-Grundschutz scan into one of these tools please contact the vendor of the corresponding tool. For additional questions please don't hesitate to contact the Greenbone Support.

Result classes of IT-Grundschutz checks

The following result classes can occur for a check:

- ***Not fulfilled (FAIL)*:** It was detected that the target system does not fulfill the measure.
- ***Fulfilled (OK)*:** It was detected that the target system does fulfill the measure.
- ***Error (ERR)*:** It was not possible to execute the test routine properly. For example, some checks require credentials. If the credentials are missing, the check can not be executed for technical reasons. In case no credentials are provided many of the checks will have this status.
- ***Check of this measure is not available (NI)*:** In general it is assumed this measure can be automatically checked for, but an implementation is not yet available. For newly released "Ergänzungslieferungen" this is initially true for a number of measures. However, the Greenbone Security Feed is updated continuously, and eventually all measures will be implemented.
- ***Check of the measure is not implemented (NA)*:** A number of measures of the "IT-Grundschutzkataloge" are kept too general to create an explicit automatic check. Other measures describe checks that can only be done physically and thus also belong to this class of test that can't be implemented at all.
- ***Check not suited for the target system (NS)*:** Some measures refer exclusively to a special type of operating system. If the target system runs another operating system type, the measure does not apply and the result class is set to NS.
- ***This measure is deprecated (DEP)*:** Some updates ("Ergänzungslieferungen") removed some measures without a replacement. Old IDs of such deprecated measures are never re-used. So, the results marked as DEP can be safely ignored but the entries remain for completeness.

[29] https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/GSTOOL/AndereTools/anderetools_node.html

Supported measures

This overview refers to the current Ergänzungslieferung. The measure ID's link to the corresponding detailed information available on the website of BSI.

The following test types are distinguished:

- Remote: For the check it is only necessary to have network connection to the target system.
- Credentials: For the check is is required to use a account on the target system.

BSI reference	Title	Test type	Note
M4.2[30]	Screen lock	Credentials	Windows: Can only test for local accounts. Linux: Only default screen savers in Gnome and KDE.
M4.3[31]	Use of anti virus protection software	Credentials	
M4.4[32]	Compliant handling of drives for removable media and external data storage devices	Credentials	
M4.5[33]	Logging of telecommunication equipment	Credentials	
M4.7[34]	Changing of default passwords	Remote	Test only via SSH and Telnet.
M4.9[35]	Use of the security mechanisms of XWindows	Credentials	
M4.14[36]	Mandatory password protection in Unix	Credentials	
M4.15[37]	Secure login	Credentials	
M4.16[38]	Access restrictions of user IDs and / or terminals	Credentials	
M4.17[39]	Locking and deleting unneeded accounts and terminals	Credentials	
M4.18[40]	Administrative and technical securing of access to monitoring and single-user mode	Credentials	
M4.19[41]	Restrictive allocation of attributes for UNIX system files and directories	Credentials	
M4.20[42]	Restrictive allocation of attributes for UNIX user files and directories	Credentials	
M4.21[43]	Preventing of unauthorized escalation of administrator rights	Credentials	
M4.22[44]	Preventing of loss of confidentiality of sensitive data in the UNIX system	Credentials	
M4.23[45]	Safe access of executable files	Credentials	
M4.33[46]	Use of a virus scanning program for storage media exchange and data transfer	Credentials	
M4.36[47]	Disabling of certain fax receiving phone numbers	Credentials	Cisco devices can only be tested via telnet because they do not support blowfish-cbc encryption.

Continued on next page

Table 11.1 – continued from previous page

BSI reference	Title	Test type	Note
M4.37[48]	Disabling of certain fax sending phone numbers	Credentials	Cisco devices can only be tested via telnet because they do not support blowfish-cbc encryption.
M4.40[49]	Preventing the unauthorized use of the computer microphone	Credentials	Only implemented for Linux. Under Windows it is not possible to determine the status of the microphone via registry/WMI.
M4.48[50]	Password protection if Windows systems	Credentials	
M4.49[51]	Securing of the boot process of Windows systems	Credentials	
M4.52[52]	Equipment protection under Windows NT-based systems	Credentials	
M4.57[53]	Deactivation of automatic CD-ROM recognition	Credentials	
M4.80[54]	Sichere Zugriffsmechanismen bei Fernadministration	Remote	
M4.94[55]	Protection of web server files	Remote	
M4.96[56]	Disabling of DNS	Credentials	
M4.97[57]	One service per server	Remote	
M4.98[58]	Limit communication though a packet filter to a minimum	Credentials	Microsoft Windows Firewall is being tested. For Vista and newer any firewall that is installed comforming to the system.
M4.106[59]	Activation of system wide logging	Credentials	
M4.135[60]	Restrictive assigning of access rights to system files	Credentials	
M4.147[61]	Secure use of EFS under Windows	Credentials	
M4.200[62]	Use of USB storage media	Credentials	
M4.227[63]	Use of a local NTP server for time synchronization	Credentials	
M4.238[64]	Use of a local packet filter	Credentials	Microsoft Windows Firewall is being tested. For Vista and newer any firewall that is installed comforming to the system.
M4.244[65]	Secure system configuration of Windows client operating systems	Credentials	
M4.277[66]	Securing of the SMB, LDAP and RCP communication of Windows servers	Credentials	
M4.284[67]	Handling of services of Windows Server 2003	Credentials	
M4.285[68]	Uninstallation of unneeded client services of Windows Server 2003	Credentials	
M4.287[69]	Secure administration of VoIP middleware	Remote	

Continued on next page

Table 11.1 – continued from previous page

BSI reference	Title	Test type	Note
M4.300[70]	Information protection of printers, copies and multi-function equipment	Remote	
M4.305[71]	Use of storage quotas	Credentials	
M4.310[72]	Implementation of LDAP access to file services	Remote	
M4.313[73]	Providing of secure domain controllers	Credentials	
M4.325[74]	Deletion of swap files	Credentials	
M4.326[75]	Providing the NTFS properties on a Samba file server	Credentials	
M4.328[76]	Secure base configuration of a Samba server	Credentials	
M4.331[77]	Secure configuration of the operating system for a samba server	Credentials	
M4.332[78]	Secure configuration of access controls of a Samba server	Credentials	
M4.333[79]	Secure configuration of Winbind under Samba	Credentials	
M4.334[80]	SMB message signing and Samba	Credentials	
M4.338[81]	Use of Windows Vista and new file and registry virtualization	Credentials	Only a general test if file and registry virtualization is enabled.
M4.339[82]	Avoidance of unauthorized use of portable media under Windows Vista and later	Credentials	
M4.340[83]	Use of the Windows user account control UAC starting with Windows Vista	Credentials	
M4.341[84]	Integrity protection starting with Windows Vista	Credentials	Where possible technically implemented (active UAC and protected mode in different zones).
M4.342[85]	Activation of last access certificate stamp starting with Windows Vista	Credentials	
M4.344[86]	Monitoring of Windows Vista-, Windows 7 and Windows Server 2008-Systems	Credentials	
M4.368[87]	Regular audits of the terminal server environment	Credentials	
M5.8[88]	Regular security check of the network	Remote	Only a message is being displayed that tests should be performed with up-to date plugins.
M5.17[89]	Use of the security mechanisms of NFS	Credentials	
M5.18[90]	Use of the security mechanisms of NIS	Credentials	
M5.19[91]	Use of the security mechanisms of sendmail	Remote	
M5.19[92]	Use of the security mechanisms of sendmail	Credentials	

Continued on next page

Table 11.1 – continued from previous page

BSI reference	Title	Test type	Note
M5.20[93]	Use of the security mechanisms of rlogin, rsh and rcp	Credentials	
M5.21[94]	Secure use of telnet, ftp, tftp and rexec	Credentials	
M5.34[95]	Use of one time passwords	Credentials	
M5.59[96]	Protection from DNS-spoofing with authentication mechanisms	Credentials	
M5.63[97]	Use of GnuPG or PGP	Credentials	
M5.64[98]	Secure shell	Remote	
M5.66[99]	Use of TLS/SSL	Remote	
M5.72[100]	Deactivation of not required net services	Credentials	Only displays the services in question.
M5.90[101]	Use of IPSec under Windows	Credentials	
M5.91[102]	Use of personal firewalls for clients	Credentials	Microsoft Windows Firewall is being tested. For Vista and newer any firewall that is installed conforming to the system. On Linux systems, displaying if the iptables rules, if possible.
M5.109[103]	Use of a e-mail scanners on the mailserver	Remote	
M5.123[104]	Securing of the network communication under Windows	Credentials	
M5.131[105]	Securing of the IP protocols under Windows Server 2003	Credentials	
M5.145[106]	Secure use of CUPS	Credentials	
M5.147[107]	Securing of the communication with directory services	Remote	

[30] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04002.html
[31] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04003.html
[32] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04004.html
[33] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04005.html
[34] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04007.html
[35] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04009.html
[36] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04014.html
[37] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04015.html
[38] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04016.html
[39] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04017.html
[40] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04018.html
[41] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04019.html
[42] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04020.html
[43] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04021.html
[44] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04022.html
[45] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04023.html
[46] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04033.html
[47] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04036.html
[48] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04037.html
[49] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04040.html
[50] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html
[51] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04049.html
[52] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04052.html
[53] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04057.html
[54] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04080.html
[55] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04094.html
[56] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04096.html
[57] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04097.html
[58] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04098.html
[59] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04106.html
[60] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04135.html
[61] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04147.html
[62] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04200.html
[63] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04227.html
[64] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04238.html
[65] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
[66] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04277.html
[67] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04284.html
[68] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04285.html
[69] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04287.html
[70] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04300.html
[71] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04305.html
[72] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04310.html
[73] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04313.html
[74] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04325.html
[75] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04326.html
[76] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04328.html
[77] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04331.html
[78] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04332.html
[79] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04333.html
[80] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04334.html
[81] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04338.html
[82] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04339.html
[83] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
[84] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04341.html
[85] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04342.html
[86] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
[87] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04368.html
[88] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05008.html
[89] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05017.html

11.2.2 PCI DSS

Introduction into vulnerability analysis and policy monitoring for the Payment Card Industry Data Security Standard (PCI DSS) with the Greenbone Security Manager.

Payment Card Industry Data Security Standard

The PCI DSS is a security standard for payment card transactions and is supported by the major payment systems MasterCard, Visa, AMEX, Discover and JCB.

All organizations that process card payments, store or transfer card data are required to perform compliance validation according to PCI DSS. Non-compliance or lack of validation means the risk of being fined or, ultimately, losing the ability to process payment cards.

The validation of compliance depends on the volume of card transactions. Here, service providers are usually classified as Level 1 Service Provider and they must, on a quarterly basis, validate their cardholder data environment by an independent scanning vendor approved by the PCI Security Standards Council (PCI SSC). In addition, an annual on-site PCI Security Audit has to be performed by an independent Qualified Security Assessor (QSA), also approved by the PCI SSC.

The "Approved Scanning Vendor" (ASV) is a service provider who performs a vulnerability scan of the cardholder data environment visible to the internet. As such the vulnerability scanners themselves can not be classified or certified as ASVs. However, they are tools for the ASV to perform the vulnerability scan using the approved process.

Greenbone Security Manager and PCI DSS

According to PCI DSS (Version 3.1, Requirement 11.2) two types of vulnerability scans are to be performed on a quarterly basis and after significant changes to the cardholder data environment. This includes the vulnerability scan conducted by the ASV explained above and an internal scan of the cardholder data environment. The latter scan may be performed by employees of the organization and requires no approval by the PCI SSC.

The Greenbone Security Manager (GSM) can perform both of these scans. The false positive management features help avoid significant work load of manual elimination of wrong alerts.

A merchant can use the GSM to check the security requirements prior to the ASV vulnerability scan in order to avoid costly re-scans.

This way, a merchant can use the GSM to check for PCI compliance on an ongoing basis even between the scans performed by the ASV.

Since security changes are stored immutable for audit compliance within the GSM, the correct security and compliance status can even be verified at all times in between the quarterly ASV scans.

[90] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05018.html
[91] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05019.html
[92] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05019.html
[93] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05020.html
[94] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05021.html
[95] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05034.html
[96] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05059.html
[97] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05063.html
[98] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05064.html
[99] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05066.html
[100] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05072.html
[101] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05090.html
[102] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05091.html
[103] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05109.html
[104] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
[105] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05131.html
[106] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05145.html
[107] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05147.html

Escalation methods can inform an external auditor as well as internal experts continuously about the security status. Summaries are sent to the responsible parties.

Policy Monitoring

In the same way the GSM checks the technical aspects of other policies periodically it can also check the system parameters according to the PCI DSS policy.

With a permanent background policy scan it is ensured that antivirus tools are not outdated or firewalls don't get deactivated without notice. Such parameters can be monitored and escalated in the same way as software vulnerabilities.

Advantages for merchant:

- Permanent policy monitoring
- Flexible escalation
- "False Positive" management
- Internal and external vulnerability scanning
- Complete vulnerability analysis according to PCI DSS for internal scans

Advantages for the ASV:

- "False Positive" Management
- Static scan configuration for re-scans
- Complete vulnerability analysis according to PCI DSS for external scans via internet
- Flexible reporting framework for individual scan reports

Greenbone Networks GmbH as the vendor of the GSM does not act as an ASV. But among Greenbone's business partners you will find security consultants that as an ASV at the same time and can introduce the GSM into your security process.

11.2.3 BSI TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung

The "Bundesamt für Sicherheit in der Informationstechnik (BSI)" published a technical guideline TR-03116 "Kryptographische Vorgaben für Projekte der Bundesregierung". Part 4 of this guideline describes the security requirements for services of the federal government using the cryptographic protocols SSL/TLS, S/MIME and OpenPGP.

The requirements are based on forecasts on the security of the algorithms and key length for the next seven years including 2022.

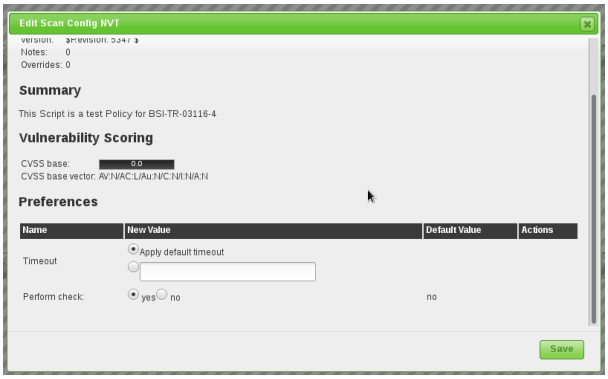
Greenbone Networks provides a scan configuration to test the compliance of services with the technical guideline TR-03116. The configuration may be downloaded from http://download.greenbone.net/scanconfigs/policy_BSI-TR-03116-4.xml. This configuration needs to be imported to the GSM subsequently.

The scan configuration has to be modified to be effective. The BSI-TR-03116-4 Policy NVT must be configured to perform the check.

This scan configuration tests if the scanned hosts and services use SSL/TLS. If this is the case the compliance with the guideline is tested.

At least the following ciphers must be supported to pass the test:

- TLS_ECDHE_ECDSA-WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

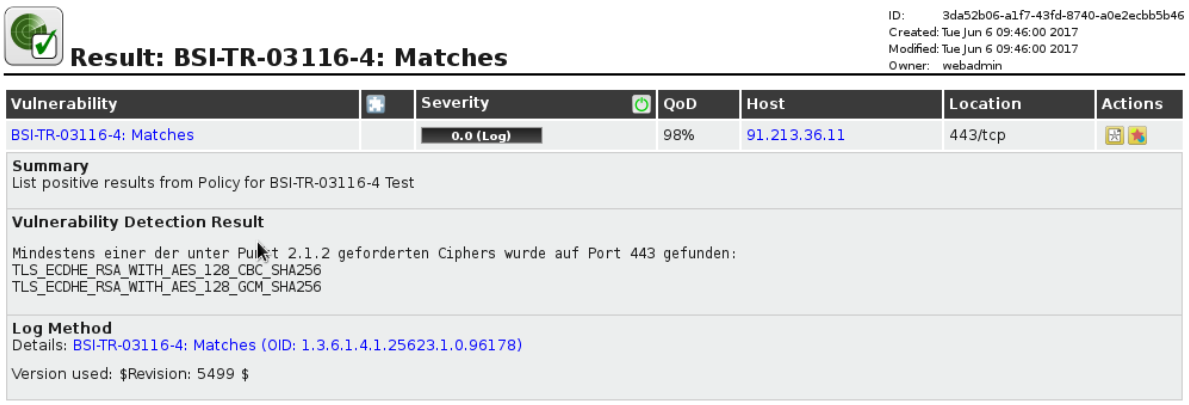


- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

If a preshared-key is used by the application in addition to the SSL/TLS algorithm one of the following ciphers is required:

- TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256

Once the target is scanned the scan report will show either matches or violations:



The severity of the NVTs depend on the GOS version used. Since GOS 4.2 the violation NVTs have a default score of 10. In the past these NVTs had a default score of 0 (log message) and overrides were required for different scores. The new default score of 10 can be changed using overrides as well. If you want to change this you have to create an override.

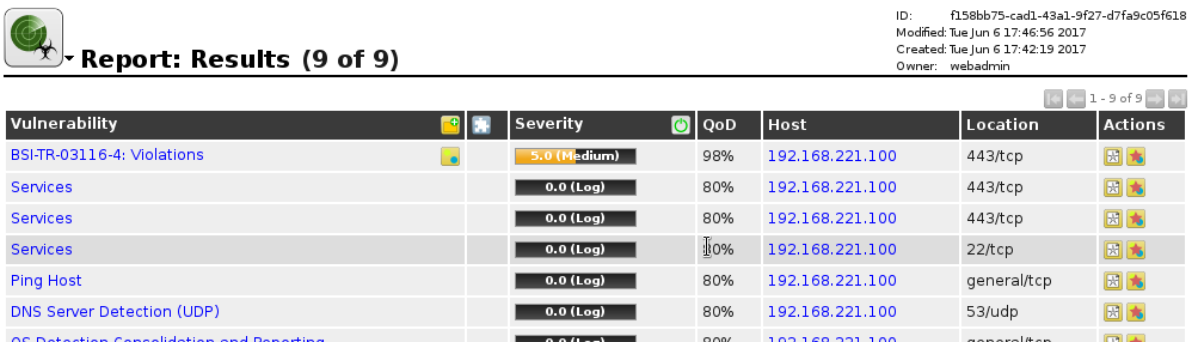


Fig. 11.14: The violation is reported with a high severity.

11.3 Special Policies

11.3.1 Mailserver Online Test

In September 2014 the Bavarian State Office for Data Protection performed an online test "Mailserver regarding STARTTLS, Perfect Forward Secrecy and Heartbleed[108]". The organizations that were found to be affected by this test were asked to remove the security risks.

Using Greenbone Security Manager or OpenVAS respectively an organization can test themselves if their own mail servers comply with the security criteria. For this follow these steps:

1. Import the following scan config: onlinepruefung-mailserver-scanconfig.xml[109].
2. Configure a new port with the port range `T:25`.
3. Configure a target containing the mailservers to be tested and select the port list created in the previous step. Depending on the network settings it could make sense to use "Consider Alive" as Alive Test.
4. Create a task with the target created above and the imported scan config.
5. Start the scan. It can take 30-40 Minutes because generally the scanner has to wait for some data from the mailservers a bit longer.
6. Finally you will get a scan report with different log entries for each mailserver. The missing StartTLS will initially only be displayed as a log message as it is a policy question how it should be assessed. For Example an override for this NVT can be created defining it as a high risk. The override can then be expanded to all hosts and possibly all tasks.
7. Should monitoring be established, a schedule for this task can be created (i.e. every week on Sundays) as well as an alert (i.e. an email). Combined with the respective overrides an automated warning system is being created in the background.

11.4 TLS-Map

The TLS (Transport Layer Security) protocol ensures the confidentiality, authenticity and integrity of communication in insecure networks. It establishes confidential communication between sender and receiver, for example web server and web browser. In the past years various security holes were detected for the often used protocol TLS 1.0 and used by attackers to actually read the communication.

With the GSM it is possible to identify systems that offer services using SSL/TLS protocols. Additionally GSM detects the protocol versions and offered encryption algorithms. Further details about the service can be achieved in case it can be properly identified.

11.4.1 Preparations

For a simplified export of your scan results we prepared a special Report Format Plugin. The resulting data file makes it easy to further process the data.

Please download and import the TLS-Map Report Format Plugin[111].

Remind that you need to activate the plugin after import for making it available. For this, click on the wrench icon and set "Active" to "yes" in the dialog. Finally click "Save Report Format".

[108] http://www.lda.bayern.de/onlinepruefung/emailserver.html
[109] http://download.greenbone.net/scanconfigs/onlinepruefung-mailserver-scanconfig.xml
[111] http://download.greenbone.net/rfps/tls-map-1.0.0.xml

11.4.2 Checking for TLS

For an overview on TLS usage in your network or on single systems we recommend to use one of the following scan configurations:

- TLS-Map Scan Config[112]

  This scan configuration identifies the used protocol versions and the offered encryption algorithms, but does not try to identify in-depth details of the service.

- TLS-Map with service detection[113]

  This scan configuration identifies the used protocol versions and the offered encryption algorithms and additionally tries to identify in-depth details of the service. This identification takes more time and produces more network traffic compared to the above simple scan configuration.

Import one or both of these scan configurations according to your needs.

Now choose a suitable list of ports to be scanned. Pay attention that all ports your are interested in are covered by the list. The more extensive the list the longer the scan will take, but this may also detect services at unusual ports.

Via menu “Port Lists” you can choose from the pre-configured lists or create you own.

Consider for the choice that the TLS protocol is based on the TCP protocol. A port list with UDP port hence will slow down the scan without benefits. If you want to cover any TCP port, then you should choose “All TCP”.

Next, create a target covering the systems and/or networks you want to check. Link this target with the port list you have chosen in the “New Target” dialog.

Create a new task and configure the imported scan configuration and the target. Start the new task.

11.4.3 Exporting the scan results

As soon as the status of the started task changes to “Done”, the scan is complete and the results can be exported.

For the export, open the report of the task, for example by clicking on the date in column “Last” in the task overview.

Change to the “Report: Summary and Download” page via the report menu and then select the “TLS Map” report format plugin for the “Full report” and select download.

The report will be prepared in CSV format. You can open this file with convenient application, for example with a spreadsheet tool.

The file contains one line per port and systems where a SSL/TLS protocol is offered:

```
IP,Host,Port,TLS-Version,Ciphers,Application-CPE
192.168.12.34,www.local,443,TLSv1.0;SSLv3,SSL3_RSA_RC4_128_SHA;TLS1_RSA_RC4_128_SHA,
  cpe:/a:apache:http_server:2.2.22;cpe:/a:php:php:5.4.4
192.168.56.78,www2.local,443,TLSv1.0;SSLv3,SSL3_RSA_RC4_128_SHA;TLS1_RSA_RC4_128_SHA,
  cpe:/a:apache:http_server:2.2.22
```

Separated by commas, each line contains the following information:

- IP: The IP address of the system where the service was detected.
- Host: The DNS name of the system in case it is available
- Port: The port where the service was detected.
- TLS-Version: The protocol version offered by the service. In case more than one is offered, the versions are separated with semicolons.

[112] http://download.greenbone.net/scanconfigs/tls-map-scan-config.xml
[113] http://download.greenbone.net/scanconfigs/tls-map-app-detection-scan-config.xml

- Ciphers: The encryption algorithms offered by the service. In case more than one is offered, the algorithms are separated with semicolons.
- Application-CPE: The detected application in CPE format. In case more than one is identified, the applications are separated with semicolons.

11.5 Conficker Search

Conficker[114] is a computer worm that occurred in fall 2008. It threatens Windows operating systems and caused numerous network failures with significant financial damage. The worm takes advantage of a security hole in the operating system and is self-updating.

Microsoft Bulletin MS08-067[115] describes the most important security hole that is exploited by Conficker to attack the corresponding systems.

11.5.1 Search methods for vulnerability and infection

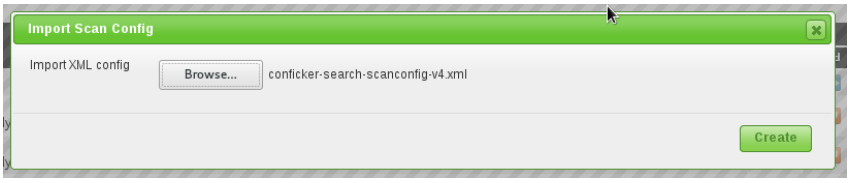
Using the Greenbone Security Manager two methods are recommended for the search:

- Non-invasive search for the security holes described by Microsoft in Bulletin MS08-067, including the Conficker worm.
- Invasive search for the security holes described by Microsoft in Bulletin MS08-067, including the Conficker worm.

The first method is able to detect the presence of the vulnerability. The second method goes as far as exploiting the vulnerability to be certain that it is indeed present. Admittedly, this may cause outages of the corresponding systems and thus should be executed with appropriate prudence.

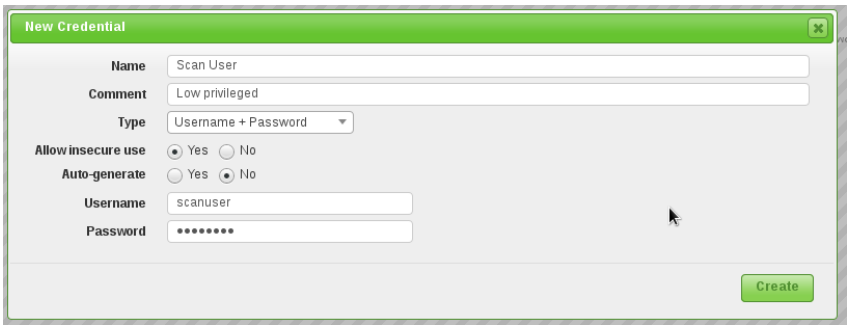
11.5.2 Execute search for vulnerability and Conficker

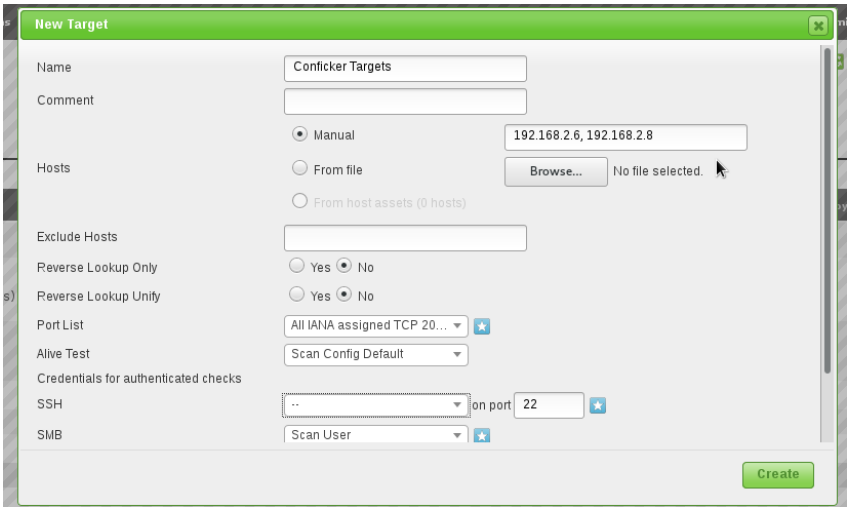
- Import the scan configuration Conficker Search[116] or, for the invasive search, the scan configuration Invasive Conficker Search[117].

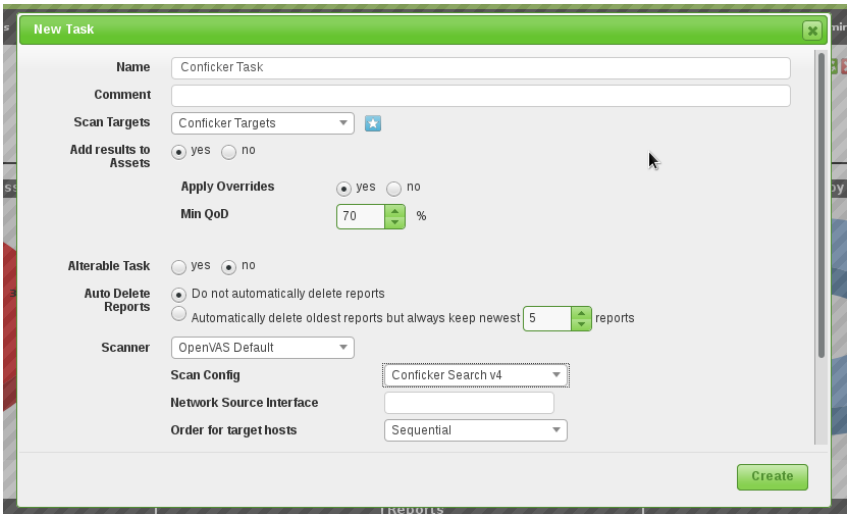


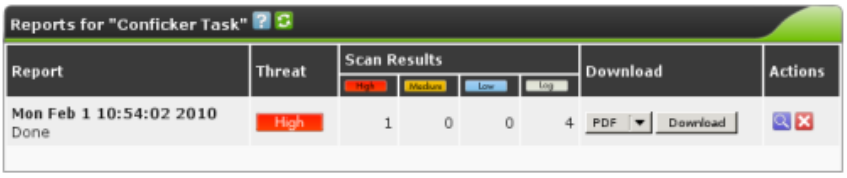
- If the target systems do not allow anonymous access, create credentials to provide the scan engine with access to the target systems. If not done yet, create a corresponding user account on the Windows systems (a low privileged user account is sufficient).
- Define the target systems (targets) and, if applicable, choose the respective credentials.
- Now you can create the actual task. This means to combine the imported scan configuration with the newly created targets.
- The search is started by clicking on ▶ of the respective task. It can take a while for the scan to complete. To update the view with the current progress, click on 🔄.
- As soon as the status changes to "Done" the complete report is available. At any time you can review the intermediate results. Here is an example for a system where the vendor security update for MS08-67 has not been installed.

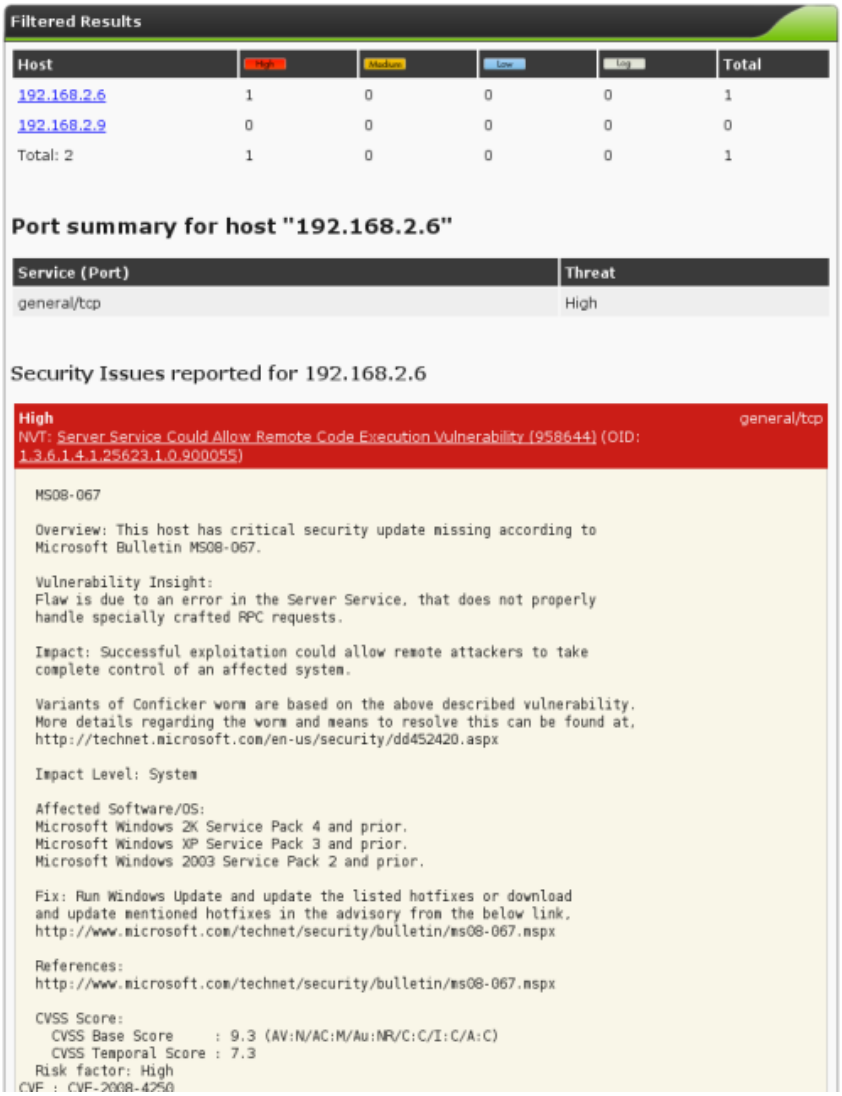
[114] http://en.wikipedia.org/wiki/Conficker
[115] http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
[116] http://download.greenbone.net/scanconfigs/conficker-search-scanconfig-v4.xml
[117] http://download.greenbone.net/scanconfigs/conficker-search-scanconfig-invasive-v4.xml


New Credential
Name
Scan User
Comment
Low privileged
Type
Username + Password
Allow insecure use
Yes
No
Auto-generate
Yes
No
Username
scanuser
Password
Create


New Target
Name
Conficker Targets
Comment
Manual
192.168.2.6, 192.168.2.8
Hosts
From file
Browse...
No file selected.
From host assets (0 hosts)
Exclude Hosts
Reverse Lookup Only
Yes
No
Reverse Lookup Unify
Yes
No
Port List
All IANA assigned TCP 20...
Alive Test
Scan Config Default
Credentials for authenticated checks
SSH
on port
22
SMB
Scan User
Create


New Task
Name
Conficker Task
Comment
Scan Targets
Conficker Targets
Add results to Assets
yes
no
Apply Overrides
yes
no
Min QoD
70
%
Alterable Task
yes
no
Auto Delete Reports
Do not automatically delete reports
Automatically delete oldest reports but always keep newest
5
reports
Scanner
OpenVAS Default
Scan Config
Conficker Search v4
Network Source Interface
Order for target hosts
Sequential
Create


Reports for "Conficker Task"
Report
Threat
Scan Results
Download
Actions
Mon Feb 1 10:54:02 2010
Done
High
1
0
0
4
PDF
Download



Filtered Results

Host	High	Medium	Low	Log	Total
192.168.2.6	1	0	0	0	1
192.168.2.9	0	0	0	0	0
Total: 2	1	0	0	0	1

Port summary for host "192.168.2.6"

Service (Port)	Threat
general/tcp	High

Security Issues reported for 192.168.2.6

High general/tcp
NVT: Server Service Could Allow Remote Code Execution Vulnerability (958644) (OID: 1.3.6.1.4.1.25623.1.0.900055)

```
MS08-067

Overview: This host has critical security update missing according to
Microsoft Bulletin MS08-067.

Vulnerability Insight:
Flaw is due to an error in the Server Service, that does not properly
handle specially crafted RPC requests.

Impact: Successful exploitation could allow remote attackers to take
complete control of an affected system.

Variants of Conficker worm are based on the above described vulnerability.
More details regarding the worm and means to resolve this can be found at,
http://technet.microsoft.com/en-us/security/dd452420.aspx

Impact Level: System

Affected Software/OS:
Microsoft Windows 2K Service Pack 4 and prior.
Microsoft Windows XP Service Pack 3 and prior.
Microsoft Windows 2003 Service Pack 2 and prior.

Fix: Run Windows Update and update the listed hotfixes or download
and update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

References:
http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

CVSS Score:
  CVSS Base Score     : 9.3 (AV:N/AC:M/Au:NR/C:C/I:C/A:C)
  CVSS Temporal Score : 7.3
Risk factor: High
CVE : CVE-2008-4250
```

11.6 OVAL System Characteristics

The Open Vulnerability and Assessment Language (OVAL)[118] is an approach for a standardized description of the (security) state of an IT system. OVAL files describe a vulnerability and define tests to identify the state in which a system is vulnerable. They usually refer to specific version of software products for which a known vulnerability exists.

This means that in order to check for vulnerabilities described in an OVAL definition, information about the current state of the system is needed. This information is collected in a standardized format as well — the OVAL System Characteristics (SC).

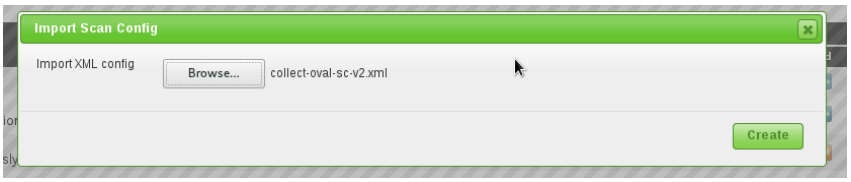
There are a number of solutions which perform checks based on OVAL definitions and SC files. OVAL definitions are provided by various vendors[119]. MITRE provides the OVAL Repository[120] with more than 13,000 entries.

11.6.1 Collecting Scan Results as OVAL SCs

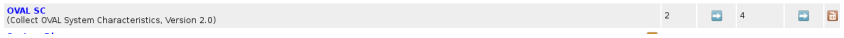
During a scan the Greenbone Security Manager collects large amounts of data about the target system. This information is managed in an optimized data pool. Parts of this information are usable as a component of an OVAL System Characteristics.

The creation of OVAL SC files is not enabled by default but has to be explicitly enabled. The following scan configuration can be used to achieve this: collect-oval-sc-v2.xml[121].

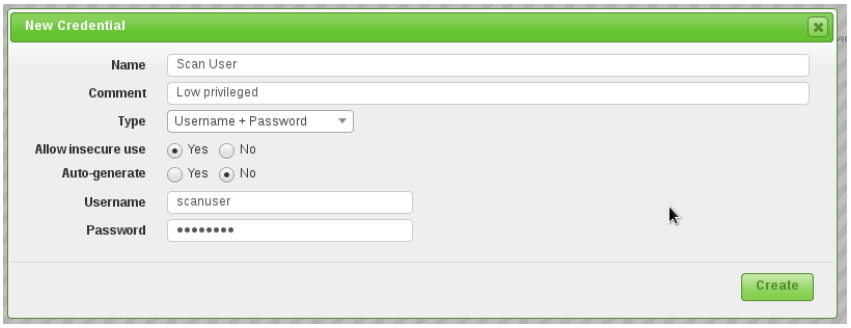
Import the scan configuration in the GSM:



The new scan configuration is now shown in the list:

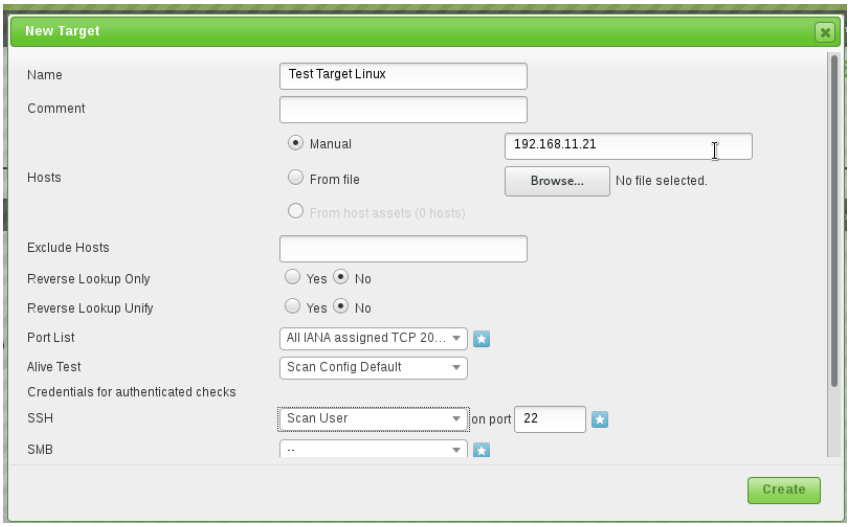


The most comprehensive results of a target system can be collected using authenticated scans. For this you need to create an account on the target system. Ensure that the account has the necessary privileges. For unixoid systems an account with low privileges is usually sufficient, for Windows system administrative privileges are required.

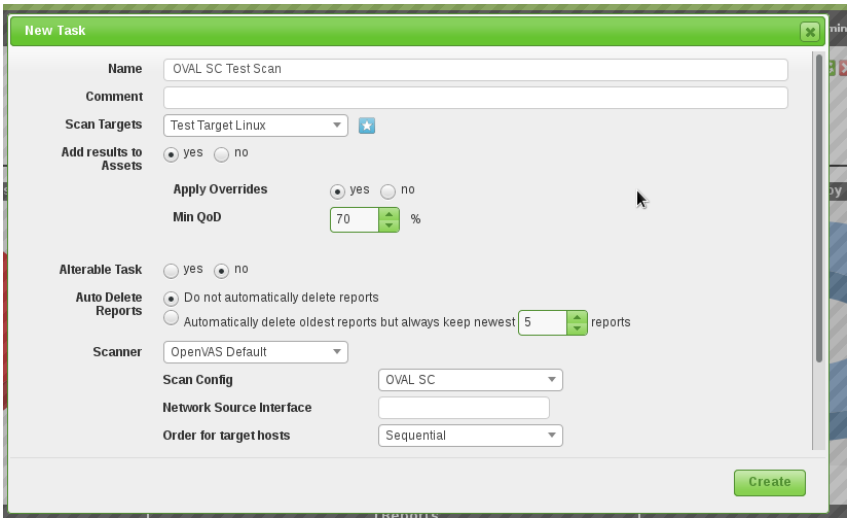


The following example shows the creation of a Linux target. For a Windows target the credential must be set in the SMB field instead of SSH.

[118] http://oval.mitre.org/
[119] http://oval.mitre.org/repository/about/other_repositories.html
[120] http://oval.mitre.org/repository/
[121] http://download.greenbone.net/scanconfigs/collect-oval-sc-v2.xml



Now create the task, which you can start immediately.



The scan itself is quite fast because the scan configuration is optimized to collect only the specific data needed for generating the System Characteristics file.

The results are returned a log information. By default these messages are suppressed.

If you adjust your filter you can see the OVAL System Characteristics in XML formatted for easy readability:

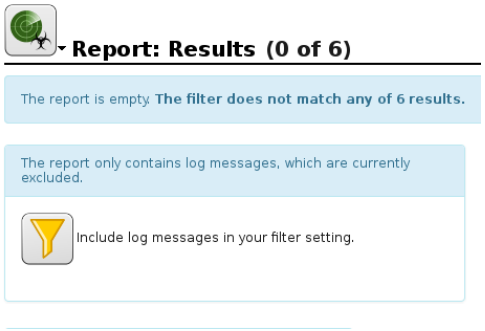
Please note: If you have collected data from a large number of target systems this view may become hard to read.

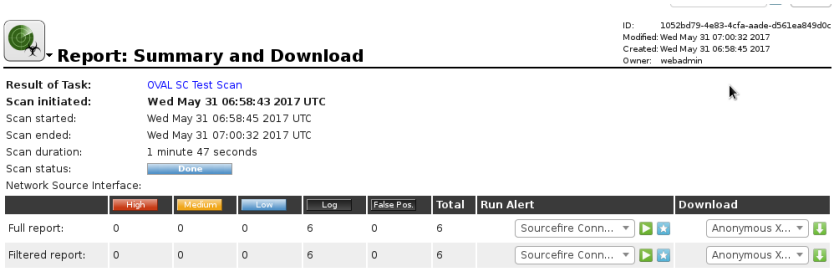
11.6.2 Exporting OVAL SCs

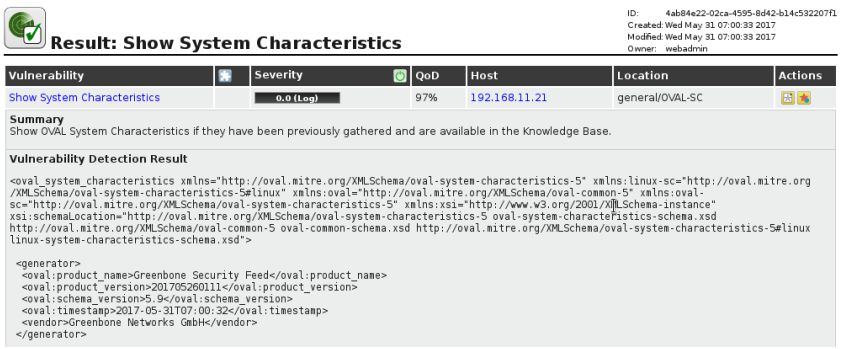
OVAL SC files are defined in a way that one file can contain only information about one system. Using the Greenbone Security Manager you can collect a large number of System Characteristics from many different systems in one single step.

Because of this we provide two Report Format Plugins:

- OVAL System Characteristics: Produces a single SC file in the XML format.
- OVAL System Characteristics Archive: Can be used for an arbitrary number of System Characteristics, which will be collected in a ZIP file. The names of the individual SC files will contain the IP


Report: Results (0 of 6)
The report is empty. The filter does not match any of 6 results.
The report only contains log messages, which are currently excluded.
Include log messages in your filter setting.


Report: Summary and Download
ID: 1052bd79-4a83-4cfa-aade-d561ea849d0c
Modified: Wed May 31 07:00:32 2017
Created: Wed May 31 06:58:45 2017
Owner: webadmin
Result of Task: OVAL SC Test Scan
Scan initiated: Wed May 31 06:58:43 2017 UTC
Scan started: Wed May 31 06:58:45 2017 UTC
Scan ended: Wed May 31 07:00:32 2017 UTC
Scan duration: 1 minute 47 seconds
Scan status: Done
Network Source Interface:
High Medium Low Log False Pos. Total Run Alert Download
Full report: 0 0 0 6 0 6 Sourcefire Conn... Anonymous X...
Filtered report: 0 0 0 6 0 6 Sourcefire Conn... Anonymous X...

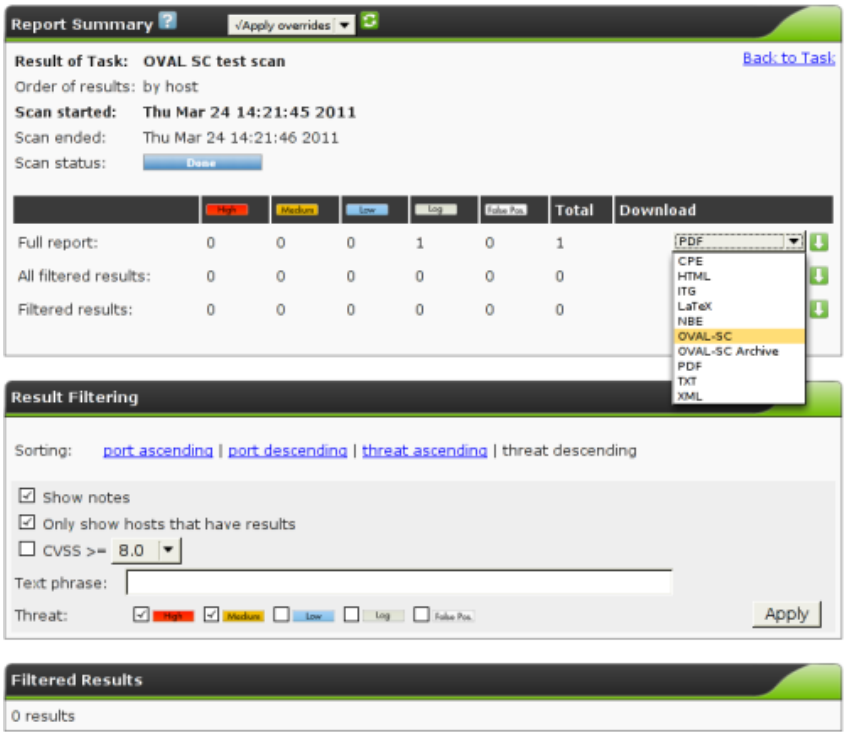

Result: Show System Characteristics
ID: 4ab84e22-02ca-4595-8d42-b14c532207f1
Created: Wed May 31 07:00:33 2017
Modified: Wed May 31 07:00:33 2017
Owner: webadmin
Vulnerability Severity QoD Host Location Actions
Show System Characteristics 0.0 (Log) 97% 192.168.11.21 general/OVAL-SC
Summary
Show OVAL System Characteristics if they have been previously gathered and are available in the Knowledge Base.
Vulnerability Detection Result
<oval_system_characteristics xmlns="http://oval.mitre.org/XMLSchema/oval-system-characteristics-5" xmlns:linux-sc="http://oval.mitre.org/XMLSchema/oval-system-characteristics-5#linux" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:oval-sc="http://oval.mitre.org/XMLSchema/oval-system-characteristics-5" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-system-characteristics-5 oval-system-characteristics-schema.xsd http://oval.mitre.org/XMLSchema/oval-common-5 oval-common-schema.xsd http://oval.mitre.org/XMLSchema/oval-system-characteristics-5#linux linux-system-characteristics-schema.xsd">
<generator>
<oval:product_name>Greenbone Security Feed</oval:product_name>
<oval:product_version>201705260111</oval:product_version>
<oval:schema_version>5.9</oval:schema_version>
<oval:timestamp>2017-05-31T07:00:32</oval:timestamp>
<vendor>Greenbone Networks GmbH</vendor>
</generator>

address of the target system.

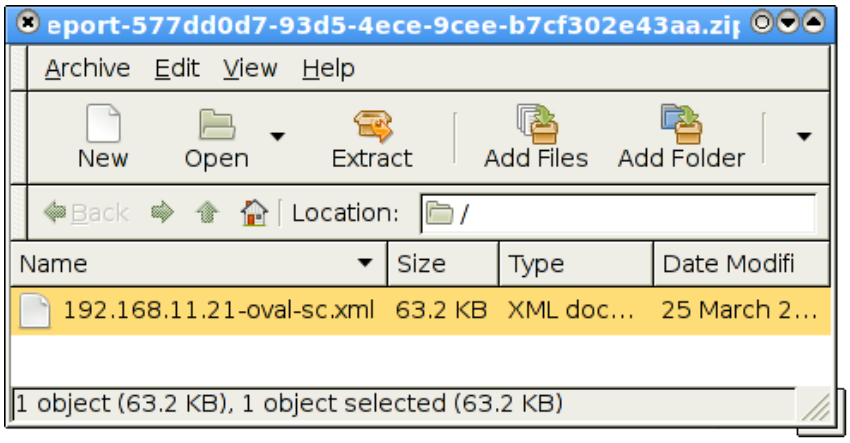
Both plugins are available for download on the Report Formats page[122].

Import the report format plugins, verify the signature and activate them. For detailed information about this process, please refer to: *Report Plugins* (page 152).

You can now download the results in the format you require for further processing. Select the format "OVAL-SC" or "OVAL-SC archive" in the "Full report" line:



The ZIP archives look as follows:



11.6.3 Example: Using OVAL SCs with ovaldi

The MITRE organization not only provides the OVAL standard but also provides a reference implementation for local OVAL checks. The OVAL Interpreter ovaldi[123] is available under an Open Source license.

[122] http://www.greenbone.net/technology/report_formats.html
[123] http://oval.mitre.org/language/interpreter.html

By using the Greenbone Security Manager to provide OVAL System Characteristics it is easy to use ovaldi on Linux to check a Windows system — or the other way round.

For example, if the target system you tested above was a Debian Linux system, you can now download the official Debian OVAL definitions 2010[124] and execute the test ("false" means that a condition was not met, i.e. a vulnerability does not exist on the target).

Ovaldi automatically creates a HTML and XML version of the plain text output as shown below: oval-sc-debian-squeeze-sample-ovaldi-results.html[125] (102 KByte) and oval-sc-debian-squeeze-sample-ovaldi-results.xml[126] (4.2 MByte). To run the tests additionally download the files oval-definitions-2010.xml[127] and oval-sc-debian-squeeze-sample.xml[128].

```
$ cd /tmp
$ ovaldi -m -o /tmp/oval-definitions-2010.xml \
  -i /tmp/oval-sc-debian-squeeze-sample.xml \
  -a /usr/share/ovaldi/xml/

-----------------------------------------------------
OVAL Definition Interpreter
Version: 5.10.1 Build: 2
Build date: Sep 11 2012 07:49:59
Copyright (c) 2002-2012 - The MITRE Corporation
-----------------------------------------------------

Start Time: Tue Sep 11 12:12:52 2012

 ** parsing /tmp/oval-definitions-2010.xml file.
    - validating xml schema.
 ** checking schema version
    - Schema version - 5.3
 ** skipping Schematron validation
 ** parsing /tmp/oval-sc-debian-lenny-sample.xml for analysis.
    - validating xml schema.
 ** running the OVAL Definition analysis.
      Analyzing definition:  FINISHED
 ** applying directives to OVAL results.
 ** OVAL definition results.

  OVAL Id                                  Result
  ------------------------------------------------------
  oval:org.debian:def:1965                 false
  oval:org.debian:def:1966                 false
  oval:org.debian:def:1967                 false
  oval:org.debian:def:1968                 false
  oval:org.debian:def:1969                 false
  oval:org.debian:def:1970                 false
  oval:org.debian:def:1971                 false
  oval:org.debian:def:1972                 false
  oval:org.debian:def:1973                 false
  oval:org.debian:def:1974                 false
  ...
  oval:org.debian:def:2124                 false
  oval:org.debian:def:2125                 false
  oval:org.debian:def:2126                 false
  oval:org.debian:def:2127                 false
  oval:org.debian:def:2128                 false
  oval:org.debian:def:2129                 false
  oval:org.debian:def:2130                 false
```

[124] http://www.debian.org/security/oval/oval-definitions-2010.xml
[125] http://download.greenbone.net/misc/oval-sc-debian-squeeze-sample-ovaldi-results.html
[126] http://download.greenbone.net/misc/oval-sc-debian-squeeze-sample-ovaldi-results.xml
[127] http://www.debian.org/security/oval/oval-definitions-2010.xml
[128] http://download.greenbone.net/misc/oval-sc-debian-squeeze-sample.xml

```
  oval:org.debian:def:2131                false
  oval:org.debian:def:2132                false
  oval:org.debian:def:2133                false
  ------------------------------------------------------


 ** finished evaluating OVAL definitions.

 ** saving OVAL results to results.xml.
 ** running OVAL Results xsl: /usr/share/ovaldi/xml//results_to_html.xsl.

 ------------------------------------------------------
```

If the target system was a Microsoft Windows system, you can use the definitions provided by MITRE[129] and execute the test ("false" means that a condition was not met, i.e. a vulnerability does not exist on the target).

Ovaldi automatically creates a HTML and XML version of the plain text output as shown below: oval-sc-windows-xp-sample-ovaldi-results.html[130] (23 KByte) and oval-sc-windows-xp-sample-ovaldi-results.xml[131] (159 KByte).

To run the tests additionally download the files windows.xml[132] and oval-sc-windows-xp-sample.xml[133].

```
$ cd /tmp
$ ovaldi -m -o /tmp/windows.xml \
  -i /tmp/oval-sc-windows-xp-sample.xml \
  -a /usr/share/ovaldi/xml/

------------------------------------------------------
OVAL Definition Interpreter
Version: 5.10.1 Build: 2
Build date: Sep 11 2012 07:49:59
Copyright (c) 2002-2012 - The MITRE Corporation
------------------------------------------------------

Start Time: Tue Sep 11 15:57:55 2012

 ** parsing /tmp/windows.xml file.
    - validating xml schema.
 ** checking schema version
    - Schema version - 5.10
 ** skipping Schematron validation
 ** parsing /tmp/oval-sc-windows-xp-sample.xml for analysis.
    - validating xml schema.
 ** running the OVAL Definition analysis.
      Analyzing definition:  FINISHED
 ** applying directives to OVAL results.
 ** OVAL definition results.

  OVAL Id                                  Result
  ------------------------------------------------------
  oval:org.mitre.oval:def:754              true
  oval:org.mitre.oval:def:15339            false
  oval:org.mitre.oval:def:15465            false
  oval:org.mitre.oval:def:15452            false
  oval:org.mitre.oval:def:15377            false
  oval:org.mitre.oval:def:15346            false
```

[129] http://oval.mitre.org/rep-data/5.10/org.mitre.oval/p/family/windows.xml
[130] http://download.greenbone.net/misc/oval-sc-windows-xp-sample-ovaldi-results.html
[131] http://download.greenbone.net/misc/oval-sc-windows-xp-sample-ovaldi-results.xml
[132] http://oval.mitre.org/rep-data/5.10/org.mitre.oval/p/family/windows.xml
[133] http://download.greenbone.net/misc/oval-sc-windows-xp-sample.xml

```
 oval:org.mitre.oval:def:15173          false
 oval:org.mitre.oval:def:15057          false
 oval:org.mitre.oval:def:15546          false
 oval:org.mitre.oval:def:14566          false
 oval:org.mitre.oval:def:720            false
 oval:org.mitre.oval:def:627            false
 oval:org.mitre.oval:def:286            false
 oval:org.mitre.oval:def:748            false
 oval:org.mitre.oval:def:684            false
 oval:org.mitre.oval:def:396            false
 oval:org.mitre.oval:def:1205           false
 oval:org.mitre.oval:def:679            false
 oval:org.mitre.oval:def:165            false
 oval:org.mitre.oval:def:565            false
 oval:org.mitre.oval:def:289            false
 oval:org.mitre.oval:def:730            false
 oval:org.mitre.oval:def:1162           false
 oval:org.mitre.oval:def:2041           false
 oval:org.mitre.oval:def:1946           false
 oval:org.mitre.oval:def:1815           false
 oval:org.mitre.oval:def:1282           false
 oval:org.mitre.oval:def:1804           false
 oval:org.mitre.oval:def:1469           false
 oval:org.mitre.oval:def:718            false
 oval:org.mitre.oval:def:347            false
 oval:org.mitre.oval:def:283            false
 oval:org.mitre.oval:def:282            false
 ------------------------------------------------------


** finished evaluating OVAL definitions.

** saving OVAL results to results.xml.
** running OVAL Results xsl: /usr/share/ovaldi/xml/results_to_html.xsl.

-------------------------------------------------
```

CHAPTER 12

Greenbone Management Protocol

The entire control of the GSM appliance is done via the Greenbone Management Protocol (GMP). The web interface is an GMP client as well and accesses the GSM functions via GMP.

GMP is formerly known as OMP. Greenbone provides new tools to use the features of the GMP protocol. While the gvm-tools (see section *GVM-Tools* (page 243)) may be used to connect to both GOS 4 and older GOS 3.1 appliances the older omp.exe (see http://docs.greenbone.net/GSM-Manual/gos-3.1/en/omp.html) tool is not compatible with GOS 4.

The GMP protocol is documented at the Greenbone TechDoc portal: http://docs.greenbone.net/API/OMP/omp-7.0.html

This chapter covers the activation and use of the protocol by third party applications.

12.1 Activating the GMP Protocol

To be able to use the GMP protocol it first needs to be activated on the GSM appliance. The web interfaces uses the GMP protocol only locally on the appliance and not through the network. Activating the GMP protocol can either be performed directly through a variable on the command line (see section *GMP* (page 34)) or via the GOS-Admin-Menu under *Remote* and then *GMP*. It is important that in both cases the GSM appliance needs to be rebooted to activate this setting. Access to the GMP protocol is done in general SSL encrypted and authenticated. The same users as in the web interface are being used. The users are subject to the same restrictions and have the exact same permissions.

12.2 Access with `gvm-cli.exe`

While with the help of the documentation of the GMP protocol your own application for access can be developed, Greenbone has developed a command line application for easy access and a Python shell and makes both available on the website for Linux and Windows. The tool and the download locations are described in section *GVM-Tools* (page 243).

The GMP protocol is XML based. Every command and every response is a GMP object.

The command line tool `gvm-cli.exe` supplied by Greenbone Networks offers for one the direct sending and receiving of XML commands and XML responses.

The tool supports the following connections:

- tls
- ssh
- socket

The commandline tool supports several switches. These can be displayed using:

```
$ gvm-cli -h
usage: gvm-cli [-h] [-V] [connection_type] ...

  gvm-cli 1.2.0 (C) 2017 Greenbone Networks GmbH

  This program is a command line tool to access services via
  GMP (Greenbone Management Protocol).

  Examples:
  gvm-cli --xml "<get_version/>"
  gvm-cli --xml "<commands><authenticate><credentials><username>myuser</username><password>mypass
...
```

While the tool supports more switches the additional options are only displayed when the connection_type is specified:

```
$ gvm-cli ssh -h
usage: gvm-cli ssh [-h] [-c [CONFIG]] [--timeout TIMEOUT]
                   [--log [{DEBUG,INFO,WARNING,ERROR,CRITICAL}]]
                   [--gmp-username GMP_USERNAME] [--gmp-password GMP_PASSWORD]
                   [-X XML] --hostname HOSTNAME [--port PORT]
                   [--ssh-user SSH_USER]
                   [infile]

positional arguments:
  infile

optional arguments:
  -h, --help            show this help message and exit
  -c [CONFIG], --config [CONFIG]
                        Configuration file path. Default: ~/.config/gvm-
                        tools.conf

...
```

While the current GSM Appliances (GOS 4) use ssh to protect the GMP protocol, older appliances used TLS and Port 9390 to transport the GMP protocol. The gvm tools may be used with both the older and the current Greenbone OS.

The tools are mostly helpful for batch mode (`batch processing`, `scripting`).

With this tool the GMP protocol can be used in a simple way:

```
gvm-cli --xml "<get_version/>"
gvm-cli --xml "<get_tasks/>"
gvm-cli < file
```

12.2.1 Configuring the Client

To use the `gvm-cli` command you need to log into the appliance. For this the required information is supplied either using command line switches or a configuration file (~/.config/gvm-tools.conf).

To provide the GMP user using command line switches use:

- `--gmp-username`
- `--gmp-password`

Alternatively a configuration file ~/.config/gvm-tools.conf containing these informations may be created:

```
[Auth]
gmp_username=webadmin
gmp_password=kennwort
```

This configuration file is not read be default. You will have to add the commandline switch `--config` or `-c` to read the configuration file.

12.2.2 Starting a Scan using gvm-cli

A typical example for using the GMP protocol is the automatic scan of a new system. Below we assume that an Intrusion Detection System is in use that monitors the systems in the DMZ and immediately discovers new systems and unusual TCP ports not used up to now. If such an event is being discovered the IDS should automatically initiate a scan of the new system. This should be done with the help of a script. For the this `gvm-cli` can be used although the `gvm-pyshell` or using self written python scripts might be more suitable. The processing of the XML output is better supported by python then by using the shell. This is explained in the following sections.

Starting point is the IP address of the new suspected system. For this IP address a target needs to be created in the GSM.

Under http://docs.greenbone.net/API/OMP/omp-7.0.html#command_create_target the command `create_target` is described.

If the IP address is saved in the variable `IPADDRESS` the respective target can be created with the following command:

```
$ gvm-cli ssh --gmp-username webadmin --gmp-password kennwort \
--hostname 192.168.222.115 \
--xml "<create_target><name>Suspect Host</name>\
<hosts>$IPADDRESS</hosts></create_target>"

<create_target_response status="201" status_text="OK, resource
created" id="4574473f-a5d0-494c-be6f-3205be487793"/>
```

Now the task can be created.

```
$ gvm-cli ssh --gmp-username webadmin --gmp-password kennwort \
--hostname 192.168.222.115 \
--xml "<create_task><name>Scan Suspect Host</name> \
<target id=\"4574473f-a5d0-494c-be6f-3205be487793\"></target> \
<config id=\"daba56c8-73ec-11df-a475-002264764cea\"></config></create_task>"


<create_task_response status="201" status_text="OK, resource created" id="ce225181-c836-4ec1-b83f
```

The output us the ID of the task. It is required to start and monitor the task.

The other IDs used by the command may be retrieved using the following commands displaying the available targets and scan configs:

```
$ gvm-cli ssh --gmp-username webadmin --gmp-password kennwort \
--hostname 192.168.222.115 --xml "<get_targets/>"

$ gvm-cli ssh --gmp-username webadmin --gmp-password kennwort \
--hostname 192.168.222.115 --xml "<get_configs/>"
```

The output of the above commands is XML.

Now the task needs to be started:

```
$ gvm-cli ssh --gmp-username webadmin --gmp-password kennwort \
--hostname 192.168.222.115 \
--xml '<start_task task_id="ce225181-c836-4ec1-b83f-a6fcba70e17d"/>'
```

The connection will be closed by the GSM.

Now the task is running. The status of the task can be displayed with the following command:

```
$ gvm-cli ssh --gmp-username webadmin --gmp-password kennwort \
--hostname 192.168.222.115 \
--xml '<get_tasks task_id="ce225181-c836-4ec1-b83f-a6fcba70e17d"/>'

<get_tasks_response status="200" status_text="OK"><apply_overrides>
...<status>Running</status><progress>98<host_progress>
<host>192.168.255.254</host>98</host_progress></progress>.../>
```

As soon as the scan is completed the report can be downloaded. For this the ID that was output when the task was started is required. Also a meaningful report format must be entered. The IDs for the report formats can be displayed via:

```
$ $ gvm-cli ssh --gmp-username webadmin --gmp-password kennwort \
--hostname 192.168.222.115 --xml '<get_report_formats/>'
```

Now the report can be loaded:

```
$ gvm-cli ssh --gmp-username webadmin --gmp-password kennwort \
--hostname 192.168.222.115 \
--xml '<get_reports report_id="23a335d6-65bd-4be2-a83e-be330289eef7" \
format_id="35ba7077-dc85-42ef-87c9-b0eda7e903b6"/>'
```

For a complete automatic processing of the data the task could be combined with an alert that could send out the report automatically at a specific severity level.

12.3 gvm-pyshell

The command line tool `gvm-pyshell.exe` supplied by Greenbone Networks offers for one the direct sending and receiving of XML commands and XML responses using python commands. These commands take care of the generation and parsing of the XML data.

The tool supports the following connections:

- tls
- ssh
- socket

While the current GSM Appliances (GOS 4) use ssh to protect the GMP protocol, older appliances used TLS and Port 9390 to transport the GMP protocol. The gvm tools may be used with both the older and the current Greenbone OS.

The tools are mostly helpful for batch mode (`batch processing`, `scripting`).

The authentication configuration of the `gvm-pyshell` can be stored in a file in the home directory of the user. The syntax is explained in section *Configuring the Client* (page 206).

The Python implementation follows the GMP API. Under http://docs.greenbone.net/API/OMP/omp-7.0.html the API is described. Optional arguments in the API are identified by a ?. The following example explains the usage of the Python functions:

```
gmp.create_task("Name","Config","Scanner","Target",comment="comment")
```

While mandatory arguments may be supplied in the correct order and are identified automatically they may also be specified using their identifier:

```
gmp.create_task(name="Name",config_id="Config",scanner_id="Scanner",target_id="Target",comment="c
```

12.3.1 Starting a Scan using gvm-pyshell

A typical example for using the GMP protocol is the scan of a new system. Below we assume that an Intrusion Detection System is in use that monitors the systems in the DMZ and immediately discovers new systems and unusual TCP ports not used up to now. If such an event is being discovered the IDS should automatically initiate a scan of the new system. This should be done with the help of a script. For the this the `gvm-pyshell` is very suitable. The processing of the XML output is better supported by python then by using the shell.

Starting point is the IP address of the new suspected system. For this IP address a target needs to be created in the GSM.

Under http://docs.greenbone.net/API/OMP/omp-7.0.html#command_create_target the command `create_target` is described.

The following lines will first step through the required commands using the interactive python shell:

```
$ gvm-pyshell ssh \
--gmp-username webadmin --gmp-password kennwort\
--hostname 192.168.222.115
GVM Interactive Console. Type "help" to get information about functionality.
>>> res=gmp.create_target("Suspect Host", True, hosts="192.168.255.254")
>>> target_id = res.xpath('@id')[0]
```

The variable target_id contains now the id of the created target. This id can now be used to create the corresponding task.

The task creation requires the following input:

- target_id
- config_id
- scanner_id
- task_name
- task_comment

To display all available scan configurations the following code may be used:

```
>>> res = gmp.get_configs()
>>> for i, conf in enumerate(res.xpath('config')):
...     id = conf.xpath('@id')[0]
...     name = conf.xpath('name/text()')[0]
...     print('\n({0}) {1}: ({2})'.format(i, name, id))
```

The scanners can be discovered using the same technique. But if only the built in scanners are used the following id are hard-coded:

- OpenVAS 08b69003-5fc2-4037-a479-93b440211c73
- CVE 6acd0832-df90-11e4-b9d5-28d24461215b

To create the task use the following command:

```
>>> res=gmp.create_task(name="Scan Suspect Host",
... config_id="daba56c8-73ec-11df-a475-002264764cea",
... scanner_id="08b69003-5fc2-4037-a479-93b440211c73",
... target_id=target_id)
>>> task_id = res.xpath('@id')[0]
```

To start the task use:

```
>>> gmp.start_task(task_id)
```

The current version of the GSM (4.1.7) closes the connection in the gvm-pyshell imediately. Further commands are not possible.

All these commands may be put in a python script which may be invoked by the gvm-pyshell:

```
len_args = len(args.script) - 1
if len_args is not 2:
    message = """
    This script creates a new task with specific host and nvt!
    It needs two parameters after the script name.
    First one is name of the target and the second one is the
    chosen host. The task is called target-task

    Example:
        $ gvm-pyshell ssh newtask target host
    """
    print(message)
    quit()

target = args.script[1]
host = args.script[2]
task = target + " Task"

# Full and Fast
myconfig_id = "daba56c8-73ec-11df-a475-002264764cea"

# OpenVAS Scanner
myscanner_id = "08b69003-5fc2-4037-a479-93b440211c73"

res=gmp.create_target(target, True, hosts=host)
mytarget_id = res.xpath('@id')[0]

res=gmp.create_task(name=task,
                    config_id=myconfig_id,
                    scanner_id=myscanner_id,
                    target_id=mytarget_id)
mytask_id = res.xpath('@id')[0]

gmp.start_task(mytask_id)
```

12.4 Example Scripts

The gvm-tools come with a collection of example scripts which may be used by the `gvm-pyshell.exe` tool. Currently the following scripts are shipped in the Bitbucket repository:

- application-detection.gmp

  This script will display all hosts with the searched application.

- cfg-gen-for-certs.gmp

  This script creates a new scan config with nvts based on a given CERT-Bund Advisory.

- clean-slave.gmp

  This script removes all resources from a slave except active tasks.

- create-dummy-data.gmp

  This script generates dummy data.

- DeleteOverridesByFilter.gmp

  This script deletes overrides using a filter.

- monthly-report2.gmp

This script will display all vulnerabilities based on the reports of a given months. Made for GOS 4.x.

- monthly-report.gmp

  This script will display all vulnerabilities based on the reports of a given months. Made for GOS 3.1.

- nvt-scan.gmp

  This script creates a new task with specific host and nvt using hardcoded base config.

- startNVTScan.gmp

  This script interactively creates a new task with specific host and nvt.

- SyncAssets.gmp

  This script will upload assets to the asset db.

- SyncReports.gmp

  This script will pull reports and upload these to a second GSM using container tasks.

These scripts may serve as a starting point for the development of private scripts.

12.4.1 Status Codes

The GMP protocol uses status codes for communication. These status codes can be displayed in the web interface.

Fig. 12.1: The GMP protocol uses status codes and alerts to display statuses.

The status codes are similar to HTTP status codes. The following codes are being used:

2xx: The command was sent, understood and accepted successfully.

- 200: OK
- 201: Resource created
- 202: Request submitted

4xx: A user error occurred.

400: Syntax error This could be different syntax errors. Often elements or attributes in the OMP command are missing. The status text shows additional information. Currently this status code is also used for missing or wrong authentication.

401: Authenticate First This is the error code that is being used for missing or wrong authentication. Currently the value 400 is still being used.

403: Access to resource forbidden This is the error code that is being used for having not enough permissions. Often `400: Permission denied` will be displayed instead as well.

404: Resource missing The resource could not be found. The Resource ID was empty or wrong.

409: Resource busy This error code happens, for example, if the feed synchronization is being started while it is already in progress.

5xx: A server error occurred

500: Internal Error This could be entries that exceed an internal buffer size.

503: Scanner loading NVTs The scanner is currently busy loading the NVTs from its cache. Try again later.

503: Service temporarily down Possibly the scanner daemon is not running. Often the problem could be expired certificates.

503: Service unavailable: The OMP command is blocked on the GSM.

CHAPTER 13

Master Setup

The Greenbone Security Manager allows for the building of a distributed scan system. Hereby it is possible that one GSM remotely controls another GSM for this purpose.

Thereby the controlling GSM is called a master device and the controlled GSM a remote scanner. As soon as two GSMs are configured as master and remote scanner a user can individually configure a scan for the remote scanner via the web interface of the scan master depending on requirements and permissions. Every GSM starting from the midrange models upwards can be used as scan master and control one or more scanners. Every GSM can function as a remote scanner.

The remote scanners are independent GSMs. This is why the administrator must configure the feed updates and release updates locally on the remote scanners as well and ensure their execution. A remote scanner also provides their own graphical interface and own management. This allows for it being able to be used completely independently, however some scans being executed from the master.

Additionally the remote scanner can be configured as sensor. A scan sensor is a GSM that exclusively is being used for the function of scan slave and also completely being managed by the assigned master. This management includes automatic updates of the feeds as well as the automatic updates of release updates. A sensor does not require any network connectivity other than to a sensor master and after initial setup no further administrative tasks.

Remote scanners and slaves can be integrated into a scan master, in order to test those network segments for vulnerabilities that are not accessible in any other way.

Basically the master establishes the connection to the delegated remote scanners. The connection is established by using the Greenbone management protocol (GMP) which uses TCP port 22 (ssh). The feed and release updates send to sensors use the port 22/tcp (ssh) as well. Thus only this one port is required for remote scanners and sensor setup.

But it is very important to distinguish these two features:

- Remote Scanners: This feature requires the enabling of the GMP protocol on the remote scanner via the console and the setup of the remote scanner via the web GUI on the master. This feature then support the execution of scans via the remote scanner.
- Sensors: This feature requires the setup of the master-sensor relationship via the console on both the master and the sensor. This feature then supports the synchronization of the feed and GOS updates from the master to the sensor and the sensors management.

13.1 Setup of the remote scanner

Like with any other GSM the basic setup of a remote scanner is being performed via the serial port. In addition to the network configuration and the administrative access two other basic parameters for the use as slave are required:

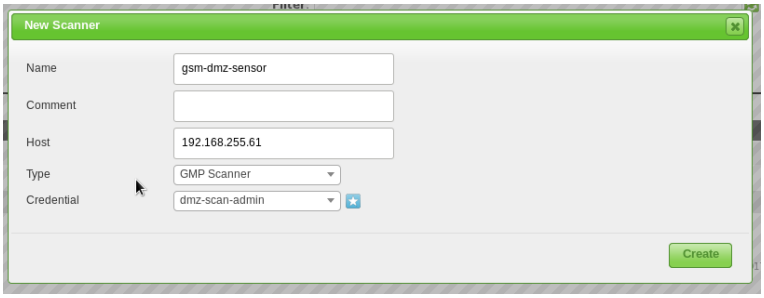


Fig. 13.1: Configuring the remote scanner on the master

- Configuring of a scan administrator on the slave that allows the master to control the slave. This scan administrator is configured using the console menu. It is being enabled on the remote scanner GSM using *Setup/User/Users* followed by *Admin User*.
- Activation of the remote GMP features. This can be enabled in the menu using *Setup/Services* followed by *GMP*.

Afterwards the remote scanners can be set up on the master and a task may be delegated to the remote scanner.

- To setup the remote scanner on the master navigate to *Configuration/Scanners*. Create a new remote scanner using .
- Choose `GMP-Scanner` in the Overlay and enter the IP address and the credentials of the scan user generated on the remote scanner.
- When configuring a new task on the master the new scanner may be chosen to run the task.
- Verify the scanner using the button. If the setup was correctly it will be successfully verified.

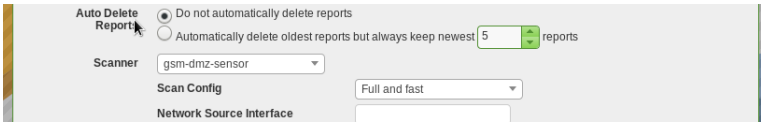


Fig. 13.2: Running a task on the remote scanner

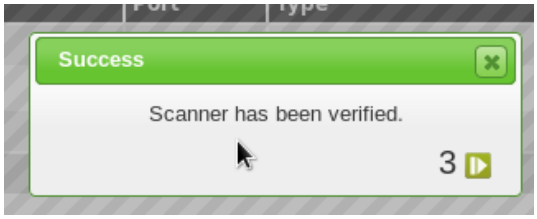


Fig. 13.3: Successful verification of the scanner

13.2 Sensor

For security reasons often it is not possible to scan network segments directly. Most of the time direct access of this segment to the Internet is not desired. In order for a sensor to have the latest NVTs available, the Greenbone Security Feed from the master may be pushed to the sensor and as such allow for a feed synchronization with the sensor. After the initial setup this occurs automatically. As soon as the master synchronized itself with the feed server it will transfer the information to the sensor as well.

To achieve this the master uses the SSH protocol. The following steps are required to setup the communication between the master and the sensor.

- First login to the console of both the master and the sensor
- On the master navigate to *Setup/Master/Master Identifier* followed by *Download*.

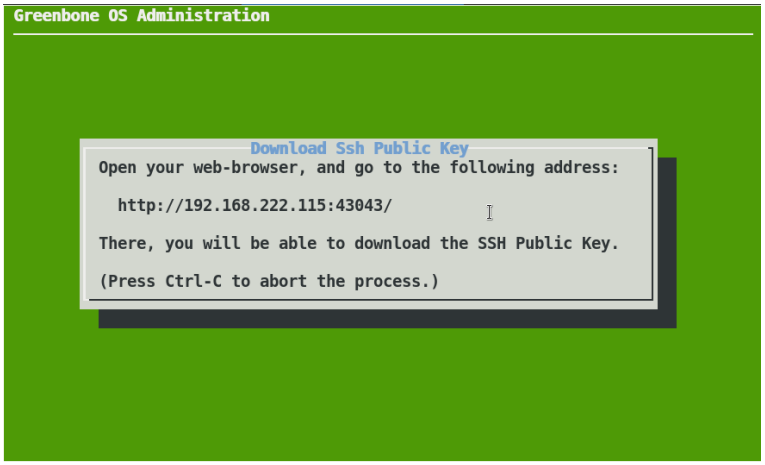


Fig. 13.4: Download the master identifier.

- Enter the URL in a browser and download the public ssh key of the master (id.pub). Once the key is downloaded the master displays the fingerprint in the console. Do not confirm the fingerprint before uploading the key to the sensor.
- On the sensor navigate to *Setup/Sensor/Configure Master* followed by *Upload*.
- Enter the URL shown on the console within a browser and upload the file downloaded from the master. After the successful upload the fingerprint of the uploaded key is displayed on the console of the sensor. Compare this fingerprint with the fingerprint displayed on the master. If the fingerprints match confirm the fingerprint both on the master and the sensor.
- Save the pending modifications on the sensor.
- Check whether the SSH service is already enabled. On the GSM25V this service is disabled by default. Enable the SSH service by navigating to *Setup/Services/SSH* followed by *State*. Save the pending modifications.
- On the master navigate to *Setup/Master*.
- Choose *Sensors* followed by *Add a new sensor*.
- Enter the IP address of the sensor.
- The master requires the identifier of the sensor. This identifier may either be entered manually or retrieved automatically. To automatically retrieve the identifier choose *Auto* in the sensor configuration menu on the master. The master will now connect to the sensor and retrieve and display the identifier.
- Compare the identifier displayed on the master with the identifier on the sensor. The identifier on the sensor may be displayed using *Setup/Sensor* followed by *Fingerprint*. If the strings match confirm the identifier on the master.
- Save the pending modification on the master.
- Check the successful configuration of this sensor by choosing the appropriate menu option. If any warning is displayed enable the appropriate settings on the sensor.

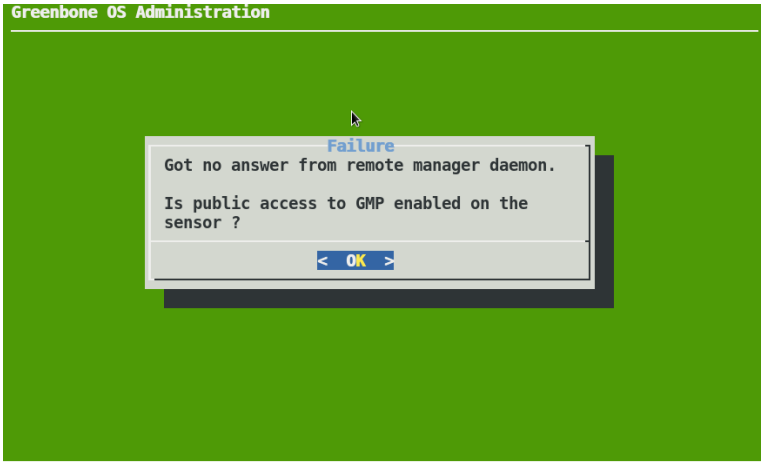


Fig. 13.5: If GMP is not enabled on the sensor a warning is displayed.

13.2.1 Communicating with the Sensors

The remote scanners and sensors communicate using SSH. This protocol must be allowed through possible existing firewall systems. Hereby the master always establishes the connection to the sensor. For backward compatibility the master also tries to connect to the sensor using the port 9390/tcp. The availability of the port may be switch on the sensor.

The feed update of the delegated scan sensors is being performed selectively either directly from the Greenbone Update Servers or through the master. For updates from the master to the scan sensor SSH (TCP per 22) is being used. If this option is not being used it has to be remembered that a possible firewall situated between the master and the scan sensor blocks this connection without notification (*Drop* or *Deny* setting). Instead the establishing of the connection should be allowed (*Accept* or *Permit*) or rejected (*Reject*) with notification as the master will always try to transfer the feed updates to the scan sensor.

CHAPTER 14

Performance

When operating the Greenbone Security Manager a considerable amount of data can be transmitted by the target systems. The available scan results are also being analyzed, filtered and processed by the GSM. On larger GSM models this occurs generally at the same time and by many users and processes.

This chapter covers the diverse questions regarding performance and discusses optimization options.

14.1 Scan Performance

The speed of a scan depends on many parameters This section points out the most important settings and makes some recommendations.

14.1.1 Selecting a Port List for a Scan

Which port list being configured for a target and as such for the tasks and the scans has a big impact, for one on the discovery performance and on the other hand regarding the scan duration.

One needs to weigh up between those two aspects when planning the vulnerability testing.

About Ports

Ports are the connection points of network communication whereby each port of the one system connects with the port port on another system.

Every system has 65535 TCP ports and 65535 UDP ports. To be precise there is one more namely the special port 0. In a connection between two ports data transmission occurs in both directions for UDP only in one direction. Due to the fact that data received by UDP are not necessarily confirmed, the testing of UDP ports usually takes longer.

Ports 0 to 1023 need to be highlighted as so called privileged or system ports and usually can not be opened by user applications.

At the IANA (Internet Assigned Numbers Authority) standard protocol ports can be reserved that then are assigned a protocol name like port 80 for `http` or port 443 for `https`.

At IANA over 5000 ports are registered. However it is absolutely possible for software to use one of these ports for different purposes if the port is not being used on the respective system.

From analysis, in which all ports of all systems of all internet accessible systems were analyzed, lists of the most used ports were created. Those do not necessarily reflect the IANA list because there is no obligation to register a specific service type for a respective port.

Typically desktop systems have fewer ports open than servers. Active network components such as routers, printers and IP phones in general have only very few ports open, namely only those they require for their actual task and for their maintenance.

Which Port List for which Scan Task

The choice of the port list always needs to be weighed up between discovery performance and scan duration.

The duration of a scan is mostly determined by the amount of ports to be tested and the network configuration. For example, starting with a certain amount of ports to be tested, throttling by the network elements or the tested systems could occur.

For the discovery performance it is obvious that services that are not bound to ports on the list, are not being tested for vulnerabilities. Additionally malicious applications that are bound to such ports won't be discovered of course. The malicious application mostly open ports that are usually not being used and are far form the system ports.

Other criteria are the defence mechanisms that are being activated by often exhaustive port scans and initiate counter measures or alerts. Even with normal scans firewalls can simulate that all 65535 ports are active and as such slow down the actual scan of those ports that are being scanned for nothing, with so called time outs.

Also to remember that for every port that is being queried the service behind it reacts at least with one log entry. For organizational reasons some services possibly should be scanned or at at least at a specific time only.

The following table outlines which port list could be most meaningful for which task.

Task/Problem	Port List
Initial Suspicion, Penetration Test, High Security, First scan of unknown systems in limited numbers	• All TCP and All UDP
Background test of an environment with known or defined environment (servers) in large numbers or with high frequency	• Specific List of Known Services • All IANA TCP
First scan of unknown systems in large numbers or with high frequency	• All IANA TCP • Nmap Top 1000 TCP and Top 100 UDP

The final decision needs to be made by the person(s) responsible for the scans. There should be at least documentation of the targets or problem to justify the selection of the ports.

On the one hand one can *play it safe*, meaning always scan all ports, will not achieve the desired outcome because all systems simply can not be scanned in time or because it will interrupt business operations.

On the other hand *super fast*, meaning only scan all privileged ports, will seem inadequate for unknown systems with high security requirements if during a later incident a vulnerability is being discovered that was rather easy to be identified. Examples for this are database services.

Also to be remembered, some systems do not use a static port allocation rather than constantly changing them even during operation. This, of course, makes it more difficult for a specific port list.

Scan Duration

In some situations with port throttling scanning all TCP and UDP ports can take 24 hours or more for a single system. Since the scans are being performed in parallel two systems will of course only take marginally more time than a single system. However the parallelizing has its limits due to system resources or network performance.

However all IANA TCP ports do usually take no more than a couple of minutes.

Since some counter measures can increase the duration of a scan there is the option to prevent throttling by making configuration changes on the defense system.

All in all at the end one will learn over time network ranges to be scanned and how they will react to scans and routine tasks can be optimized in that regard.

In suspected cases of a compromise or highest security breaches a fully inclusive scan is unavoidable.

Total Security

For port scans the basic principle that no total security exists is also true. This means that even when `All TCP and All UDP` are being used the pre set timeout of the port testing can be too short to coax a hidden malicious application into a response.

Or especially with a large amount of ports it comes directly down to defense through infrastructure. Less could sometimes even mean more.

If an initial suspicion exists an experienced penetration tester who combines the use of the actual scan tools with experience and professionally related intuition and has a good command of detailed parameterization should be consulted.

14.1.2 Scan Configuration

The scan configuration has an impact on the scan duration as well. The GSM offers four different scan configurations for vulnerability scans:

- Full and fast
- Full and fast ultimate
- Full and very deep
- Full and very deep ultimate

Both the `Full and fast` and `Full and fast ultimate` scan configurations optimize their process using already found information. This allows for the optimization of many NVTs and in doubt do not need to be tested. The two other scan configurations ignore already discovered information and therefore will execute all NVTs. This includes those NVTs as well that are not useful based on previously discovered information.

14.1.3 Tasks

During the progress of a scan a progress bar is being created. This progress bar should reflect the progress of the scan in percent. In most cases this is a rough estimate since it is difficult for the GSM to project how the systems or services that haven't been scanned yet behave compared to the already scanned systems and services.

This can be understood best when looking at an example. Assumed is a network 162.168.0.0/24 with 5 hosts: 192.168.0.250-254. A scan is being configured for this network. The scan will be performed in sequence. Due to the fact that the IP addresses at the beginning of the network are not being used the scan will run very quickly and reaches 95%. Then however, systems are being discovered that use many services. The scan will slow down respectively and since all these services are being tested. The progress bar only jumps very little. To adjust for this behaviour in the scanner dialog the `Order for target hosts` can be adjusted. The setting `Random` makes sense.

14.2 Backend Performance

The web interface accesses the GSM utilizing the OMP protocol. Some operations require more time than others. To allow an analysis and examination of the speed of the OMP backend every web page displays the time required to prepare the data at the bottom of the web page.

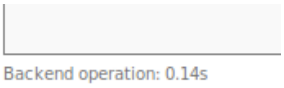


Fig. 14.1: The processing times of the backend are being displayed.

14.3 Appliance Performance

The overall performance of the GSM can be monitored with the integrated monitoring. Under *Extras* the GSM provides its own *Performance* monitoring. Here the resource utilization of the GSM for the last hour, day, week, month and year can be displayed.

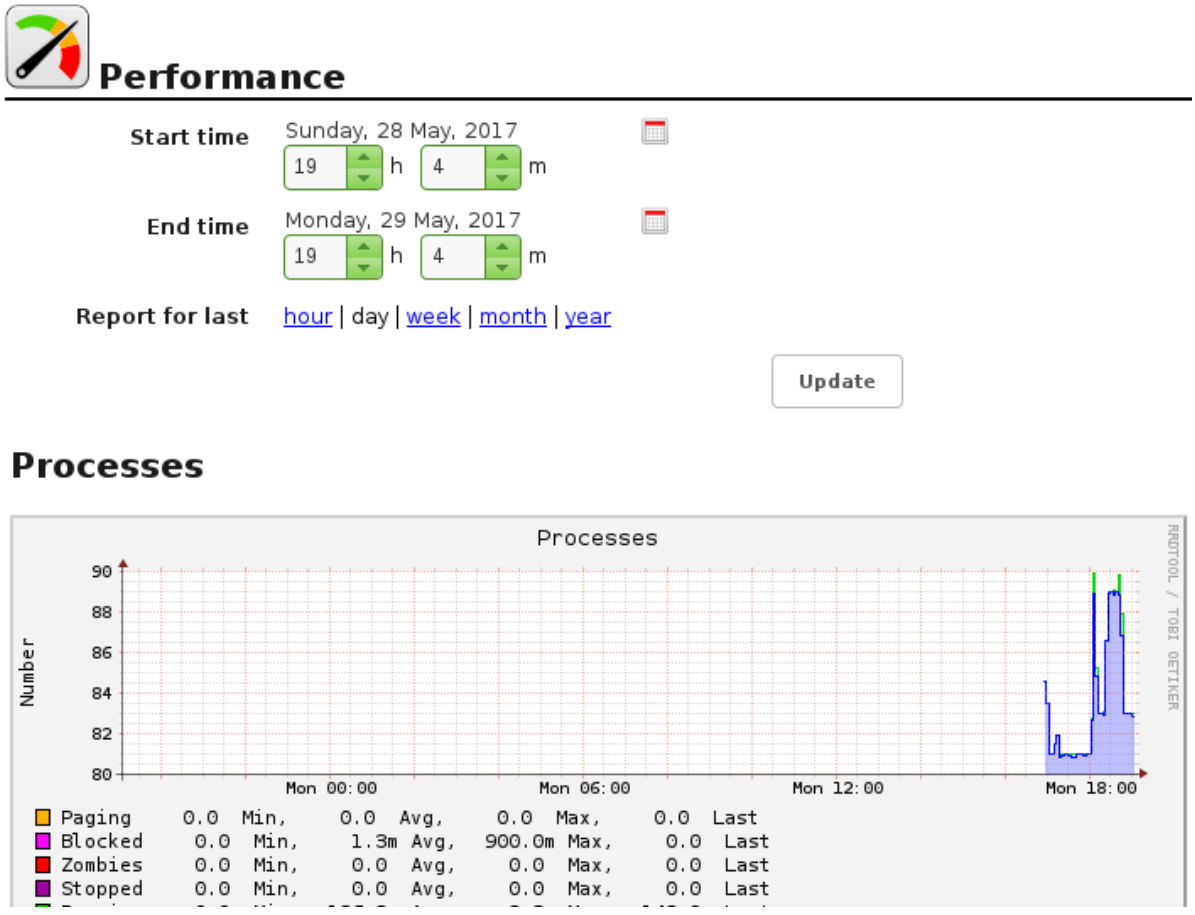


Fig. 14.2: The processing times of the backend are being displayed.

Here the following points are important:

Processes A high amount of processes is not critical. However, primarily only sleeping and running processes should be displayed.

System Load An ongoing high utilization is critical. Hereby a load of 4 on a system with 4 cores is considered ok.

CPU Usage Here especially a high Wait-IO is critical.

Memory Usage The GSM uses aggressive caching. The usage of most of the memory as cache is okay.

Swap A use of the Swap memory points to a potential system overload.

CHAPTER 15

Integration with other Systems

The Greenbone GSM appliance can be connected to other systems. This chapter covers the possible options. Some systems have been integrated already into the GSM by Greenbone Networks. This includes the verinice ITSM system, the Sourcefire IPS Defense Center and the Nagios Monitoring System. The following sections will instruct in these possibilities and give instructions for the configuration.

15.1 Integration with third-party vendors

The GSM has numerous interfaces that allow for the communication with third-party vendors. This section covers the options for an integration and connection with other systems.

Hereby the GSM offers the following interfaces:

Greenbone Management Protocol (GMP) The OpenVAS Management Protocol allows to completely remote control the GSM appliance. The protocol supports the creating of users, creating and starting of scan tasks and downloading reports, and so on.

Connecting additional scanners via OSP The OpenVAS Scanner Protocol (OSP) is a standardized interface for different vulnerability scanners. Arbitrary scanners can be integrated seamless into the GSM vulnerability management. Controlling the scanners and handling the results works in the same way for all scanners.

Report Format The GSM can present the scan results in any format. To do so the GSM already comes with a multitude of pre-installed report formats. Additional report formats can be downloaded from Greenbone or developed in collaboration with Greenbone.

Alert via Syslog, E-Mail, SNMP-Trap or HTTP.

Automatic result forwarding through connectors. These connectors are being created by Greenbone, verified and integrated into the GSM.

Monitoring via SNMP On the web site http://docs.greenbone.net/API/SNMP/snmp-gos-3.1.en.html provides the current MIB file (Management Information Base). MIB files describe the files that can be queried by SNMP about the equipment.

15.1.1 OSP Scanner

The OpenVAS Scanner Protocol resembles the Greenbone Management Protocol (GMP, see chapter Greenbone Management Protocol (page 205)). It is XML based, stateless and does not require a permanent connection for communication. The design allows for embedding of additional scanners seamlessly into GSM.

The open format allows to develop arbitrary own OSP scanners. Greenbone provides the protocol documentation and a base framework for programmers, see chapter `osp`.

15.2 Verinice

Verinice (see http://verinice.org/en/) is a free Open Source Information Security Management System (ISMS), developed by the company SerNet (see http://sernet.de/en/).

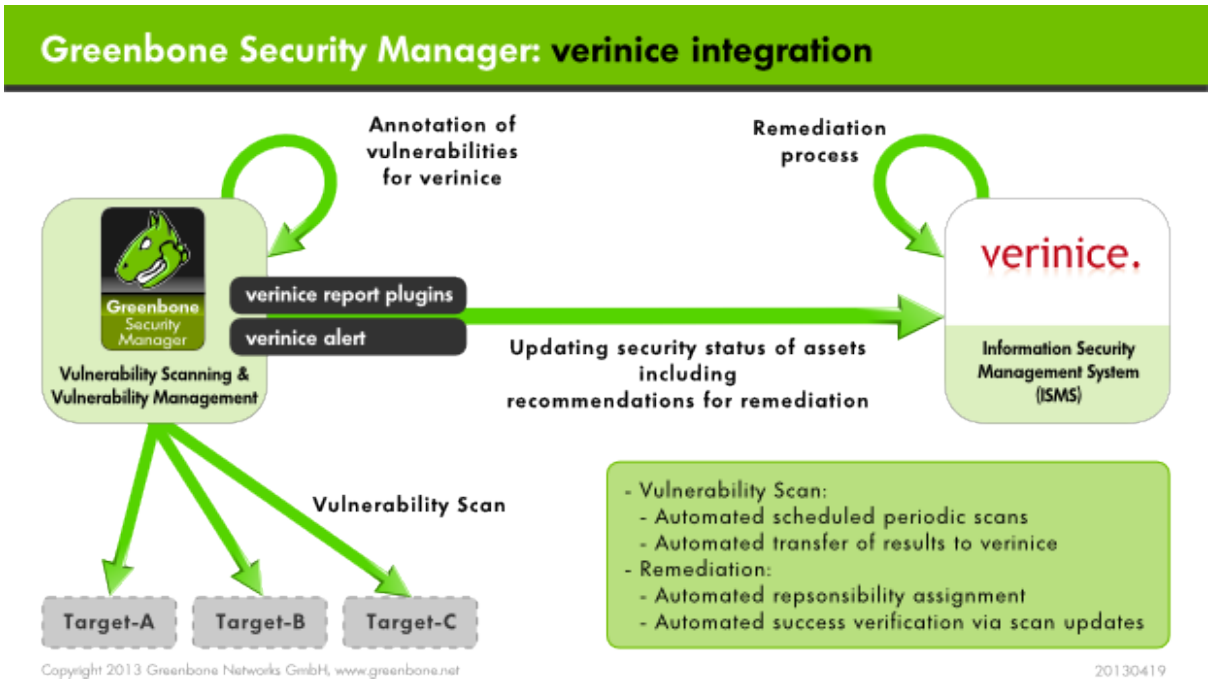


Fig. 15.1: The GSM may be integrated with verinice.

Verinice is suitable for:

- vulnerability remediation workflow
- implementing the BSI IT-Baseline Protection Catalogues
- performing risk analysis based on ISO 27005
- operating an ISMS based on ISO 27001
- performing an IS assessment per VDA specifications
- proof of Compliance with standards such as ISO 27002, IDW PS 330

The Greenbone Security Manager can support the modelling and implementation of IT Baseline Protection as well as the operation of an ISMS.

For this Greenbone offers two report plugins for the export of data from the GSM into verinice:

- `Verinice-ISM` containing all scan results
- `Verinice-ITG` containing the scan results of a BSI IT-Baseline Protection scan

The option exists to transfer data completely automated from the Greenbone Security Manager to verinicePRO, the server extension of verinice.

Following the manual import of reports from the GSM in the free verinice version is covered. For support with the use of the connector please contact SerNET or Greenbone.

15.2.1 IT Security Management

The report plugin for verinice is pre-configured and is available as `Verinice-ISM`.

With this report plugin Greenbone supports the vulnerability remediation workflow in verinice.

Hereby the notes (notes objects, see section *Notes* (page 127)) of the scan results play a central role for the `Verinice-ISM` plugin. Verinice uses the notes to create objects for processing. If there are no notes in a task only the assets will be imported as well as the complete vulnerability report. Exclusively such vulnerabilities that have a note will be imported by verinice as vulnerabilities. This allows controlling the import in fine detail.

Note: Why are only vulnerabilities transferred where a note is attached?

Within the entire security process for vulnerabilities, there must be a single point where the decision is made which vulnerability must be resolved and which are tolerable. This decision is made in the vulnerability management, by tagging the vulnerabilities accordingly.

The remediation workflow targets at solving any of the managed issues. Within the remediation workflow it is not allowed to decide about tolerating an issue.

Afterwards the report needs to be saved as `Verinice ISM-Report`. A `.vna` file will be created. This is a zip file containing the data of the GSM scan.

Start verinice to import. In verinice open the ISM perspective. Import the catalogue `Implementation Assistance for ISO27001`. Create an organization. Afterwards the screen should look like figure *Verinice offers an ISM perspective.* (page 225).

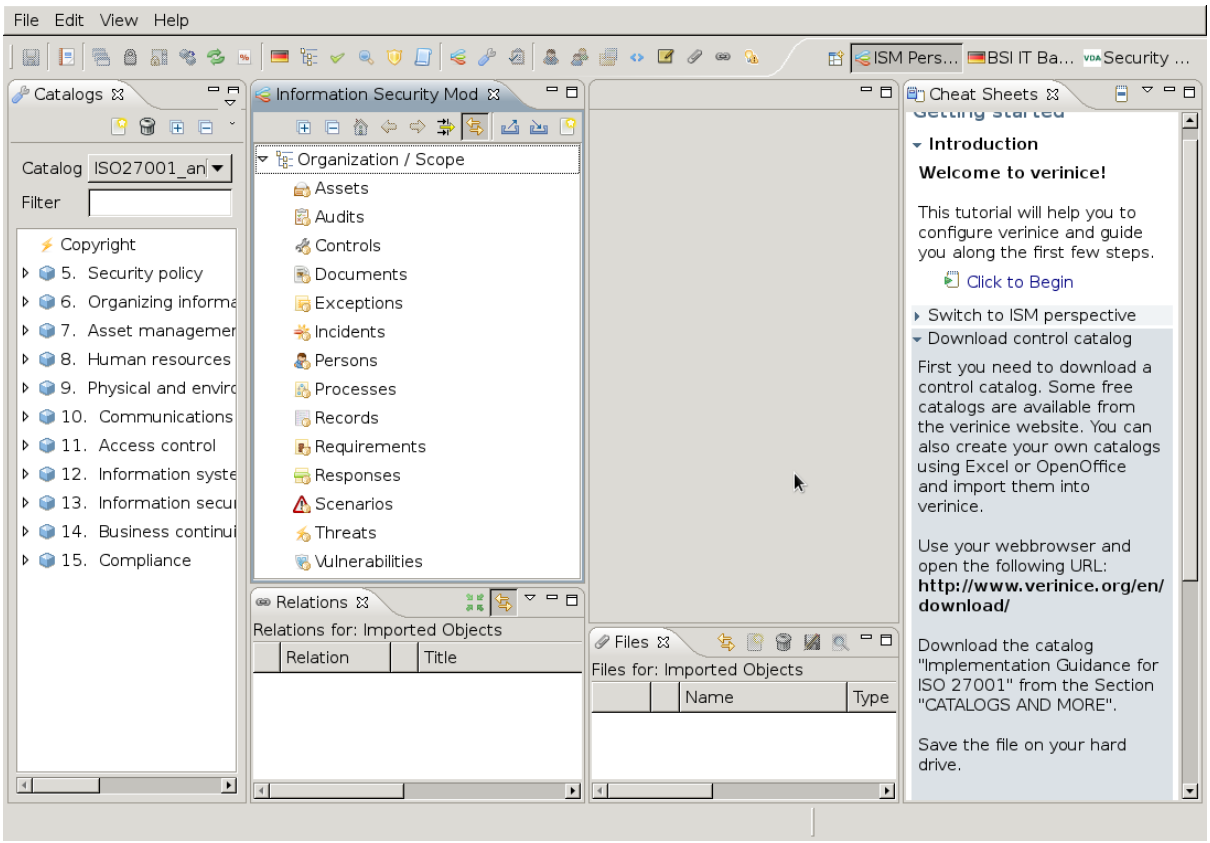


Fig. 15.2: Verinice offers an ISM perspective.

Importing of the ISM Scan

In the verinice interface chose the import option in the Information Security Model.

Now select your ISM report. The remaining parameters can be kept with their default settings.

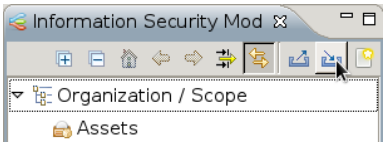


Fig. 15.3: The import button is located in the Information Security Model window.

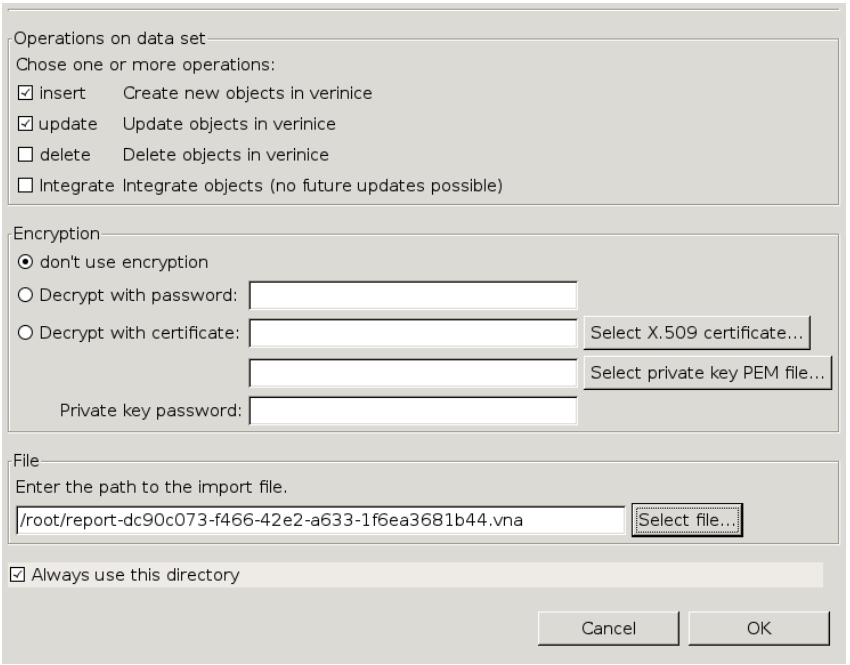


Fig. 15.4: Select the report in the dialog.

The results of the ISM report were imported and can be unfolded in Vernice. Thereby only the results were imported that had notes included in the GSM report.

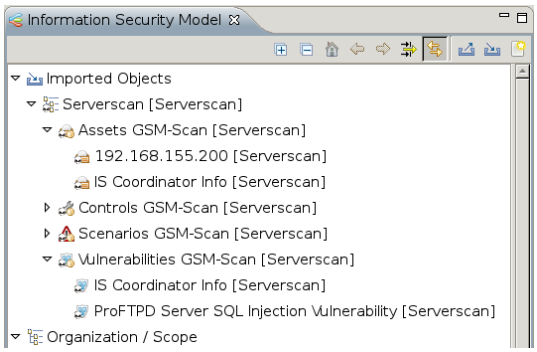


Fig. 15.5: Through the creation of notes the import of vulnerabilities can be controlled.

The process to track vulnerabilities for the imported organization can be separated into two sub processes:

- Creation of tasks
- Remediation of vulnerabilities

Creation of Tasks

Before creating tasks the data for the organization must be prepared with the following steps:

- After the first import of an organization it must be moved to the top level from the group of imported objects. Cut the organization and paste it back into the top level again.

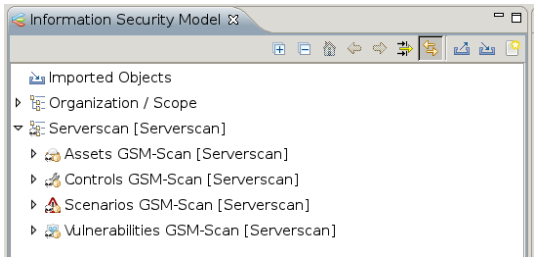


Fig. 15.6: The imported organization must be moved to the top level.

- The assets and controls must be grouped. In the context menu in the top most asset and control group select the option `Group with Tags...` In figure *The assets have already been grouped.* (page 228) this has already been done.
- All assets groups must be assigned a person responsible. Assign a person to one or more asset groups. Hereby create the person and assign them with drag&drop. The successful assignment is being displayed in the `Relations` window.
- After all the asset groups have been assigned to a person responsible, the process to remediate the vulnerabilities can be started from the context menu of the organization. Select from the context menu of an organization the task `Greenbone: Start Vulnerability Tracking`. First it will be verified if all asset groups are assigned to a person and controls are grouped. The result of the verification will be displayed in a dialog. The user can continue and create tasks or cancel the creation.

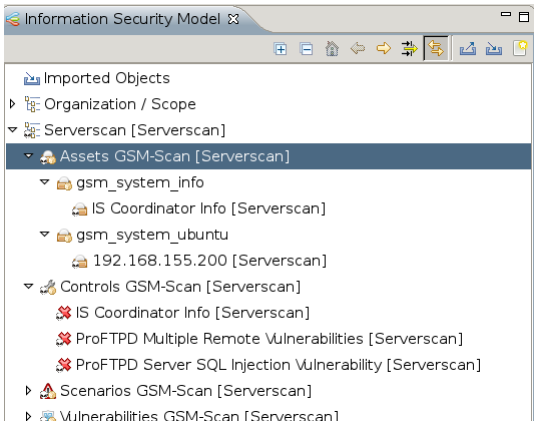


Fig. 15.7: The assets have already been grouped.

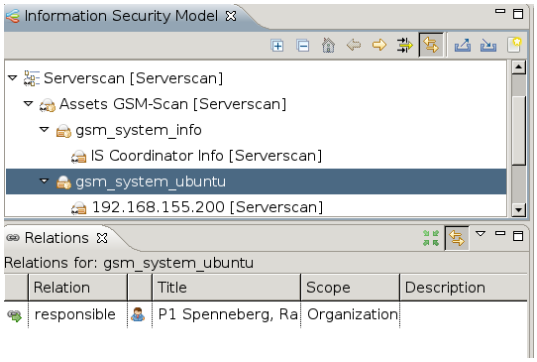


Fig. 15.8: The connection of individual objects can be confirmed in the in the Relations window.

Remediation of Vulnerabilities

The created tasks can be managed with the help of the task view or the web fronted of the verinice.Pro version (under: ISO 27000 tasks). The task to remediate vulnerabilities is called Remediate Vulnerabilities. A task contains controls, scenarios and assets that are connected to a control group and are assigned to a person responsible.

This process now takes place with the following steps:

- The person responsible must remediate the vulnerabilities for all assets.
- If the deadline for the task Remediate Vulnerabilities expires a reminder email will be sent to the person responsible.
- After completion of a task called Remediate Vulnerabilities all connection between assets and scenarios that were assigned to a task are being deleted.
- A control is marked as implemented if no asset is assigned to the scenario anymore. If other connections to assets still exist the status is being marked as partly. Afterwards the process is being completed.

15.2.2 IT Security Baseline

Greenbone provides a special configuration (IT Security Baseline scan including discovery for verinice) as well as an IT Security Baseline report plugin (Verinice ITG), which allows for the export of a report suited for verinice.

For optimum results the scan configuration needs to be imported. The report plugin is now shipped with the GSM. A manual import is not required anymore.

For optimum results in the scan it is helpful to perform an authenticated scan (see section *Authenticated Scan using Local Security Checks* (page 91)).

As soon as the scan is completed export it in the verinice ITG format. A file with the extension `.vna` is being created. This is a ZIP archive in which the results of the scans are stored. This file can be loaded by verinice directly.

Following for clarity purposes a scan is being used with only one host.

Open verinice and change into the IT Security Baseline start perspective (see figure *Verinice opens the already modelled IT bond.* (page 229)). If no IT bond has been created yet the middle view will still be empty.

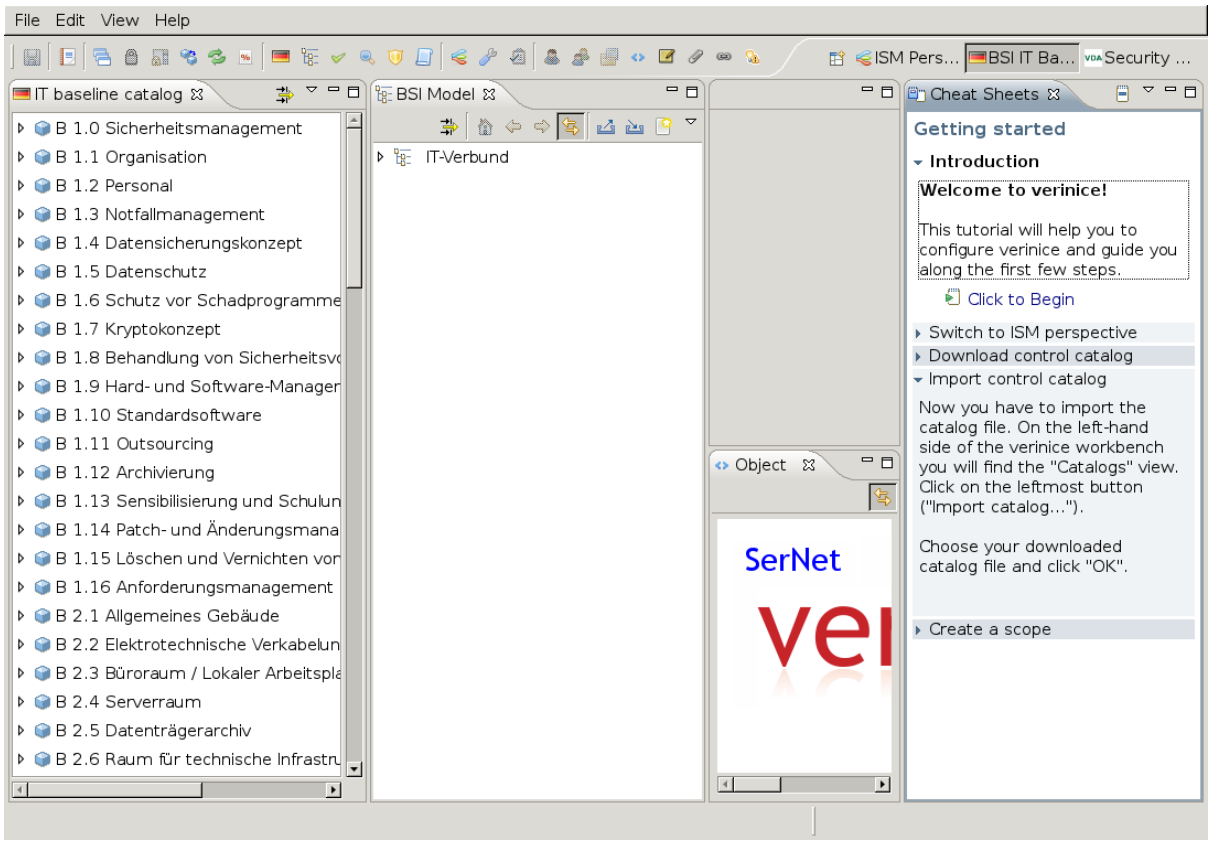


Fig. 15.9: Verinice opens the already modelled IT bond.

Importing of the ITG Scan

In the verinice interface select the import function in the IT Security Baseline model.

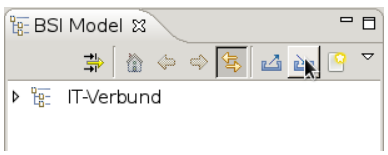


Fig. 15.10: The Import button is located in the BSI model window.

Now select the ITG report. The remaining parameters can be kept with their default settings.

The results of the ISM report were imported and can be unfolded in Vernice.

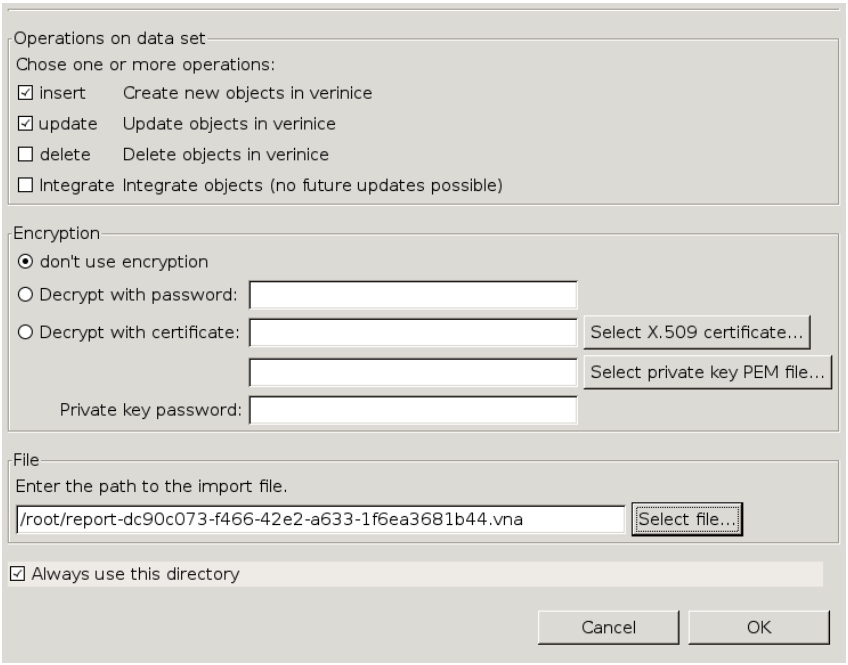


Fig. 15.11: Select the report on the dialog.

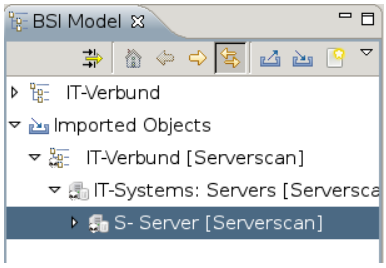


Fig. 15.12: The imported data can be unfolded in verinice.

The imported objects are named by the target in the GSM or their IP address. Every imported object has a sub-object GSM result with the activity results of the scan.

Now the IT Security Baseline modules can be added. For this select a server by right clicking on it. In the context menu select `Greenbone: Automatically assign components`. Verinice now will be choosing the appropriate components to model the system based on the tags set by the GSM.

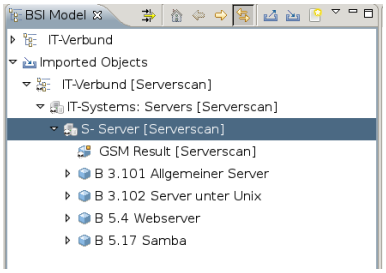
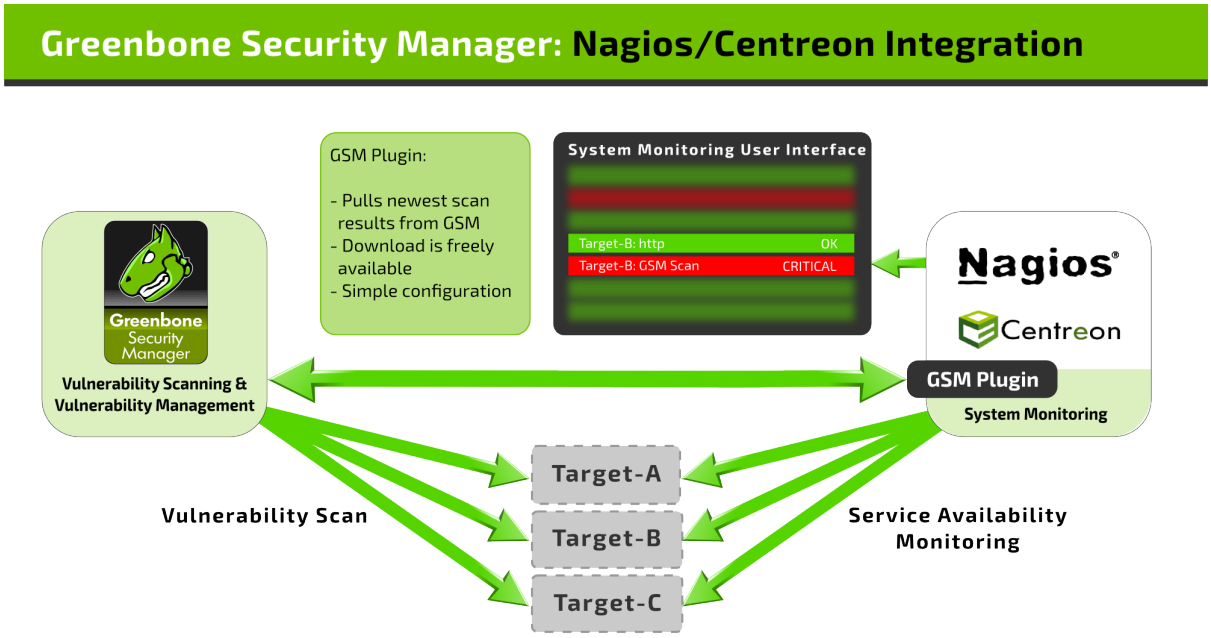


Fig. 15.13: Now the IT Security Baseline components can be selected automatically.

Now the results of the scans can be added into the control catalogue. Hereby select the server object and select the option `Greenbone: Automatic Base Security Check` from the context menu.

15.3 Nagios

Nagios can integrate the scan results in its monitoring tasks as additional test. In this case the scanned systems are automatically matched with the monitored systems. With this the scan results are eventually available for the alert rules and other processes of Nagios.



When linking Nagios with GSM, Nagios will assume the controlling role. Nagios regularly and automatically retrieves the newest scan results from Greenbone Security Manager. This is done via a Nagios plugin ("check_omp").

Follow the step-by-step instructions to connect the GSM to Nagios as part of the Open Monitoring Distribution[134] (OMD) are covered as an example. Other products like Icinga, Centreon etc. might re-

[134] http://omdistro.org/

quire small adjustments to the described steps.

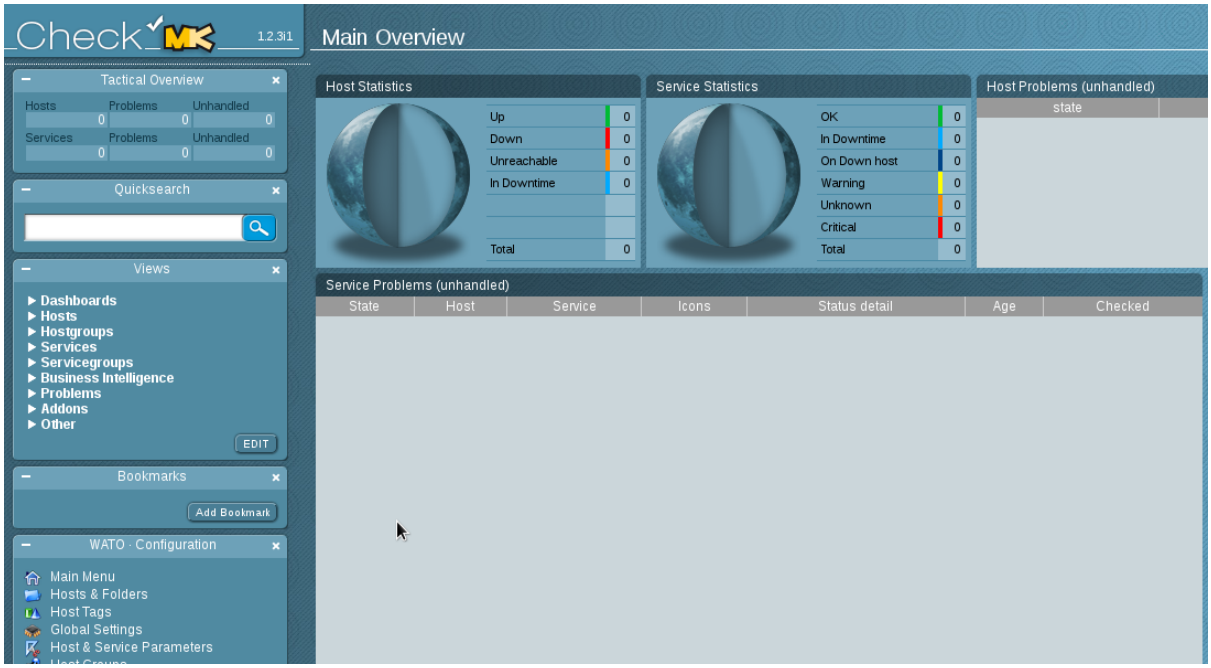


Fig. 15.14: The configuration is done by example on an empty sample site.

15.3.1 Configuration of the GSM User

For access the plugin requires a user used to login to the appliance. On the GSM and for this user, a scan target (or multiple ones) must be set up with all hosts of which the security status is to be monitored. The sample configuration used here assumes that there is only one relevant target but technically it is possible to link complex setups with multiple targets and multiple GSMs.

The GSM user account provided for queries by the Nagios plugin must be owner of the relevant scan targets or at least have unrestricted reading access to them. The tasks should be run as scheduled scans regularly.

In addition network access via OMP to the GSM appliance must be possible. Therefore the OMP access must be activated in the GOS-Admin-Menu via the command line (see sections *Activating the GMP Protocol* (page 205))

15.3.2 Configuring the Plugin

Greenbone provides the `check_gmp.py` plugin. This Nagios plugin may be called by the monitoring solution. Further information about this plugin and the download location are located in section *check_gmp.py* (page 243).

Copy the plugin to `/opt/omd/sites/site/local/lib/nagios/plugins/`.

First check if the plugin can reach the GSM through the network, OMP was activated and the user was created properly. In the following command replace the IP address with the IP address of your GSM and provide the user name and password you created.

```
omd-host# /opt/omd/sites/<site>/local/lib/nagios/plugins/check_gmp.py \
ssh --gmp-username=webadmin --gmp-password=kennwort \
--hostname 192.168.222.115 --ping
GMP OK: Ping successful
```

Next check if you also have access to the data. The easiest way is to do this via the command line.

```
omd-host# /opt/omd/sites/<site>/local/lib/nagios/plugins/check_gmp.py \
ssh --gmp-username=webadmin --gmp-password=kennwort \
--hostname 192.168.222.115 \
-F 192.168.255.254 --last-report -T "Scan Suspect Host" --status
GMP WARNING: 2 vulnerabilities found - High: 0 Medium: 1 Low: 1
|High=0 Medium=1 Low=1
```

The plugin supports several commandline switches. These can be displayed using:

```
./check_gmp.py -h
usage: check_gmp [-h] [-V] [-I MAX_RUNNING_INSTANCES] [--cache [CACHE]]
                 [--timeout TIMEOUT]
                 [connection_type] ...

Check-GMP Nagios Command Plugin 1.0 (C) 2017 Greenbone Networks GmbH
...
```

To display all available commandline switches the connection_type has to be specified:

```
./check_gmp.py ssh -h
usage: check_gmp ssh [-h] [--timeout TIMEOUT]
                     [--log [{DEBUG,INFO,WARNING,ERROR,CRITICAL}]]
                     [-u GMP_USERNAME] [-w GMP_PASSWORD] [-F HOSTADDRESS]
                     [-T TASK] [--ping | --status] [--trend | --last-report]
                     [--overrides] [-d] [-l] [--dfn] [--oid] [--descr]
                     [--showlog] [--scanend] [--autofp {0,1,2}] [-e] [-A]
                     --hostname HOSTNAME [--port PORT] [--ssh-user SSH_USER]

optional arguments:
  -h, --help            show this help message and exit
  --timeout TIMEOUT     Wait <seconds> for response. Default: 60
  --log [{DEBUG,INFO,WARNING,ERROR,CRITICAL}]
                        Activates logging. Default level: INFO.
  -u GMP_USERNAME, --gmp-username GMP_USERNAME
                        GMP username.
...
```

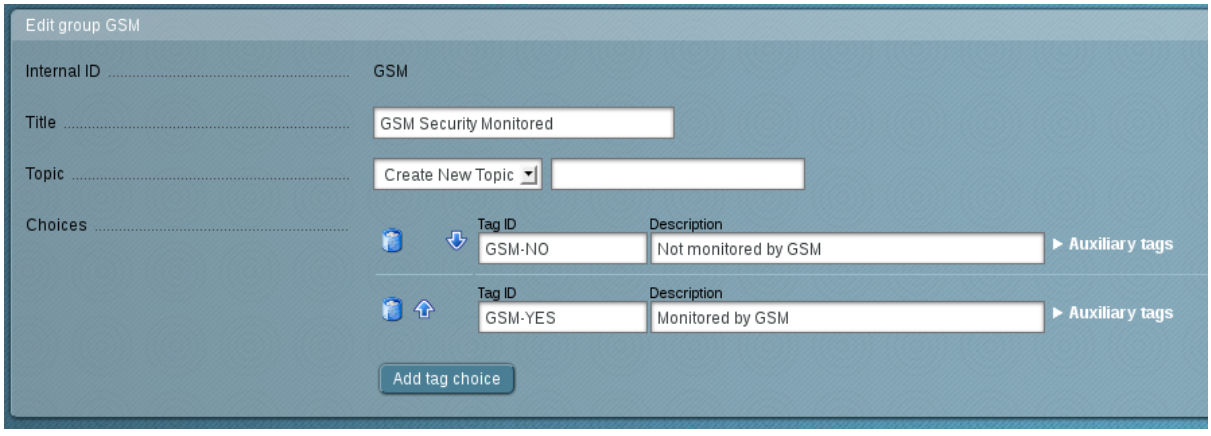


Fig. 15.15: The host tag labels the systems that are being monitored by the GSM.

If the tests were successful the check can be integrated into the web administration frontend WATO. For this switch to the web interface Multisite for your OMD page (see figure *The configuration is done by example on an empty sample site.* (page 232)).

First create the host tag (figure *The host tag labels the systems that are being monitored by the GSM.* (page 233)). It labels the hosts that are also being scanned by the GSM appliance. For this select `Host Tags` in the left menu and here create a new task.

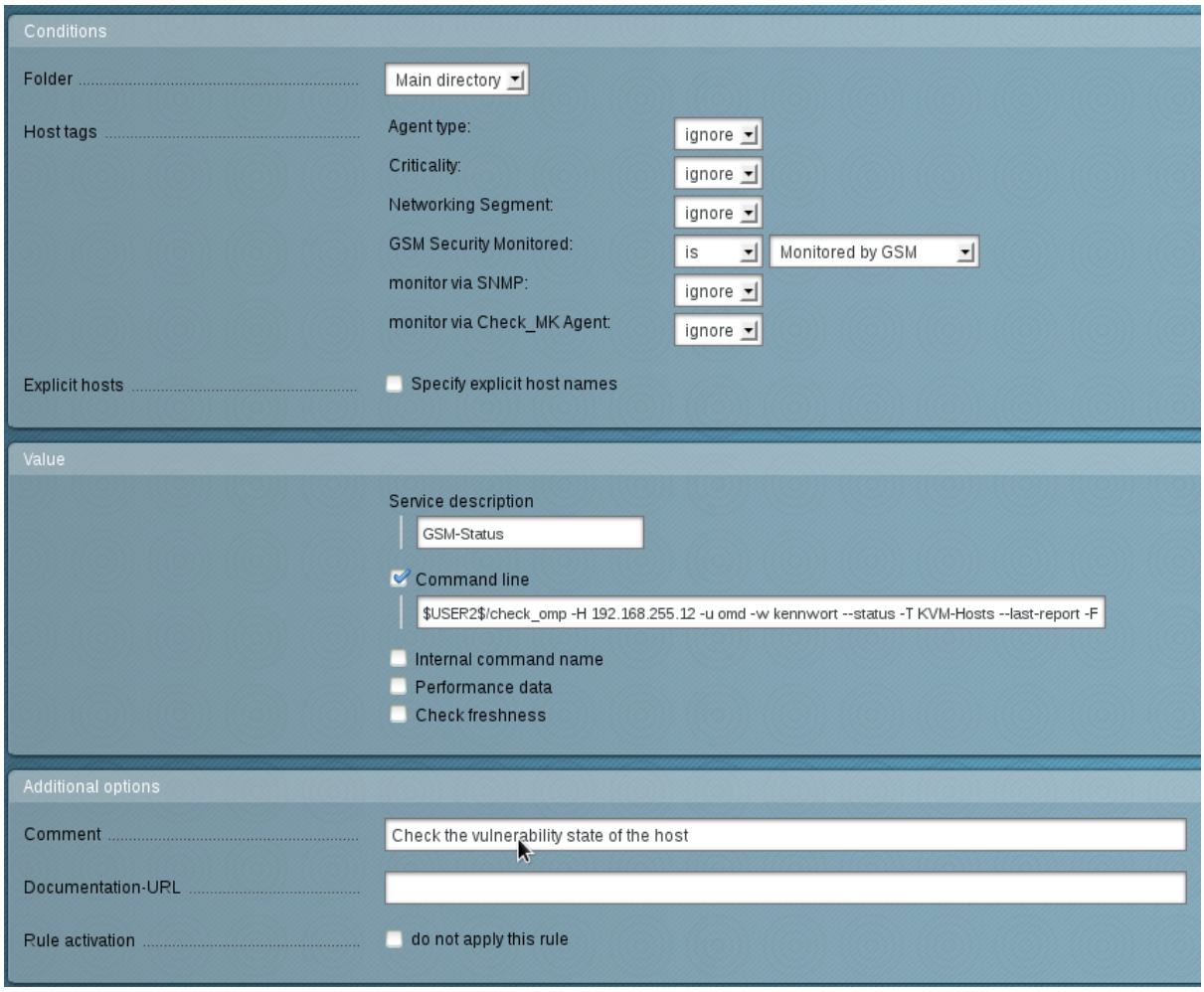


Fig. 15.16: This rule checks the status in the GSM for every host with the tag `Monitored by GSM`.

New create a new rule (figure *This rule checks the status in the GSM for every host with the tag Monitored by GSM.* (page 234)), that analyzes the host tag. For this select in the left menu in `Host & Service Parameters` the option `Active Checks`. In the next menu select `Classical Active and Passive Nagios Checks`. Then create a new rule (figure *This rule checks the status in the GSM for every host with the tag Monitored by GSM.* (page 234)) in the current folder (`Create Rule in Folder Main Directory`). Remember to use the following command:

```
$USER2$/check_gmp.py -H <gsm -ip> -u <user> -w <password> --status -T <report > \
--last-report -F $HOSTADDRESS$
```

Now the host has to be created or configure in a way that it has the respective host tag (see figure *Every host scanned by the GSM now must have the tag.* (page 235)).

Fig. 15.17: Every host scanned by the GSM now must have the tag.

After the changes have been activated in the multisite (`Activate Changes`) the status information is available in the graphical interface.

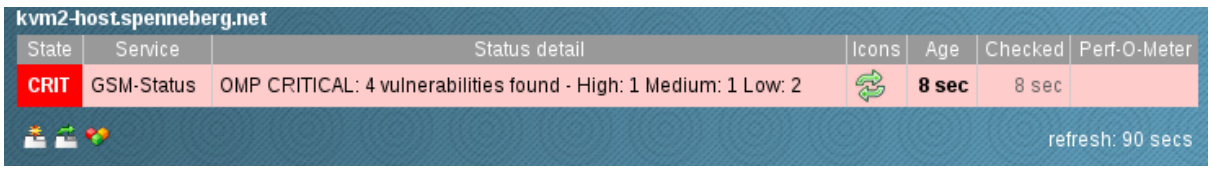


Fig. 15.18: The GSM status is now being displayed in the multisite.

So that the user name and password are not being displayed in the graphical interface they can be

saved as variables to the file `/opt/omd/sites/site/etc/nagios/resource.cfg`:

```
##########################################
# OMD settings, please use them to make your config
# portable, but dont change them
$USER1$=/omd/sites/produktiv/lib/nagios/plugins
$USER2$=/omd/sites/produktiv/local/lib/nagios/plugins
$USER3$=produktiv
$USER4$=/omd/sites/produktiv
##########################################
# set your own macros here:
$USER5$=omd
$USER6$=kennwort
```

Now the username and the password can be replaced with the variables USER5 and USER6 in WATO.

15.3.3 Caching and Multiprocessing

The `check_gmp.py` supports caching. All new reports will be cached in a sqlite database. The first call with an unknown host will take longer because the report needs to be retrieved from the GSM. Subsequent calls to the plugin will only retrieve the current report from the GSM if the end-time of the scan differs. Otherwise the information from the database is used. This will greatly reduce the load both on the monitoring server and the GSM.

The cache file is written to `/tmp/check_gmp/reports.db` by default. A different location of the database may be specified using the commandline switch `--cache`.

To further reduce the load both on the monitoring server and the GSM the plugin may restrict the maximum number of simultaneously running plugin instances. Further started instances are stopped and wait for their continuation. The default value of `MAX_RUNNING_INSTANCES` is 3. The default may be modified using the commandline switch `-I`.

15.4 Firepower Management Center

The Cisco Firepower Management Center (former Sourcefire Intrusion Prevention System) (IPS) is one of the leading solution for intrusion detection and defense in computer networks. As a Network Intrusion Detection System (NIDS) it is being tasked with the discovery, alerting and the defense against attacks on the network.

For the Firepower to correctly identify and classify attacks it requires as close as possible information about the systems in the network, the installed applications as well as their possible vulnerabilities. For this purpose the Firepower System has its own asset database that can be augmented with information from the GSM. Additionally the Sourcefire system can start an automatic scan if it suspects anything.

The connection methods are available:

1. **Automatic data transfer from the GSM to the NIDS/IDS** If the GSM and NIDS/IDS are configured respectively the data transfer from the GSM to the NIDS/IPS can be utilized easily, like any other alert functionality of the GSM. After completion of the scan it will be forwarded as an alert to the NIDS/IPS in respect to the desired criteria. If the scan task is being run automatically on a weekly basis you get a fully automated alerting and optimization system.
2. **Active control of the GSM by the NIDS/IPS** In the operation of the NIDS/IPS suspected incidents on systems with high risk can occur. In such a case the NIDS/IPS can instruct the GSM to check the system [135].

[135] This control does not exist as a finalized *Remediation* for the Sourcefire system but it can be implemented via OMP (see chapter Greenbone Management Protocol (page 205)).

To use the connection in the options 1 and 2 the GSM as well as the Sourcefire Defense Center must be prepared. In the GSM a report plugin must be installed and on the Defense Center receiving the data must be enabled.

15.4.1 Installation of the Report Plugin

The report plugin can be obtained from the Greenbone web site under http://download.greenbone.net/rfps/sourcefire-1.1.0.xml.

Download the plug in and install it on the GSM. Remember to verify and activate the plugin after importing (see section *Import of additional plugins* (page 154)).

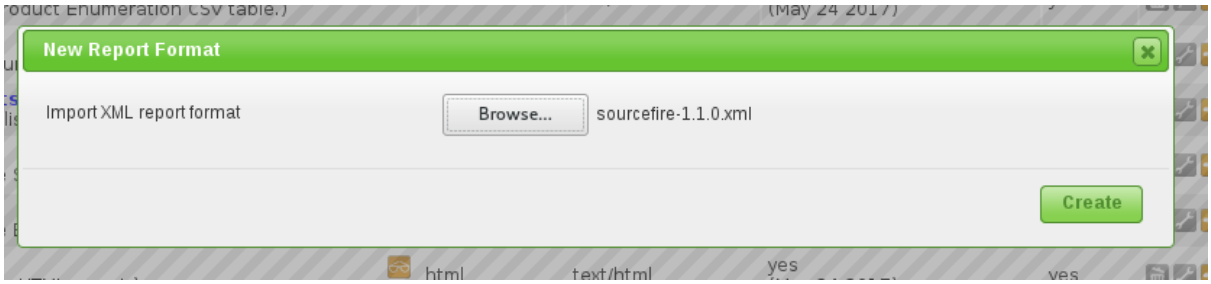


Fig. 15.19: The report plugin processes the data for Sourcefire.

15.4.2 Configuration of the Host-Input-API clients

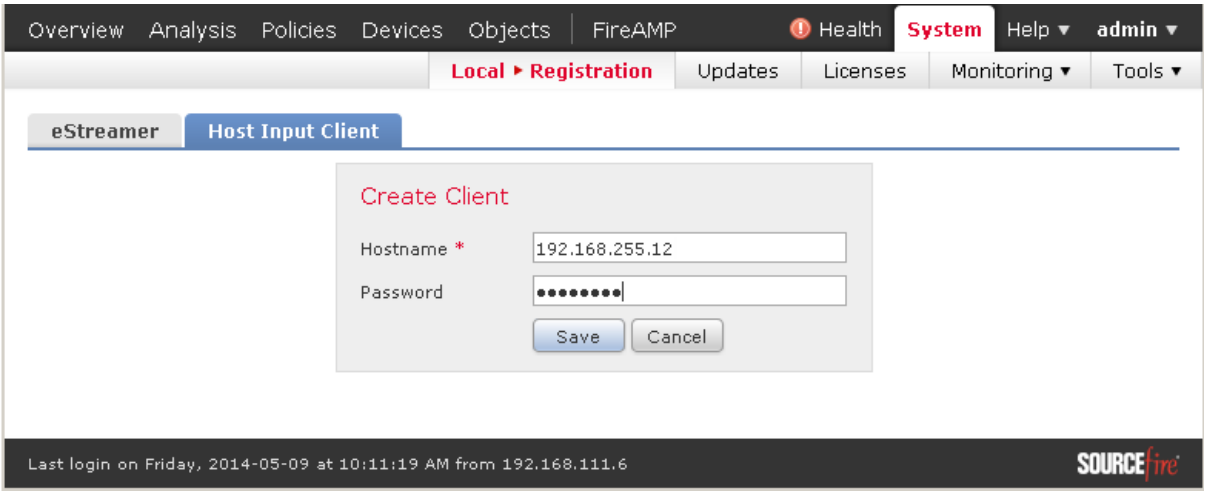


Fig. 15.20: The GSM must be set up in the Defense Center.

Log into the Sourcefire Defense Center and create a Host-Input-Client. The Host-Input-API is an interface through which the Defense Center accepts data from other applications for its asset database. This option can be found in the web interface under System->Local->Registration. There change into the `Host Input Client` register. Here create the GSM appliance. It is important to enter the IP address of the appliance that the appliance will use to connect to the Defense Center. The connection is TLS encrypted. The Defense Center creates a private key and certificate automatically. In the certificate the IP address entered above will be used as Common Name and verified when the client is establishing a connection. If the client uses a different IP address the connection fails.

The created PKCS12 file is optionally secured by a password.

Afterwards the certificate and the key are being created and made available as a download. Download this file.

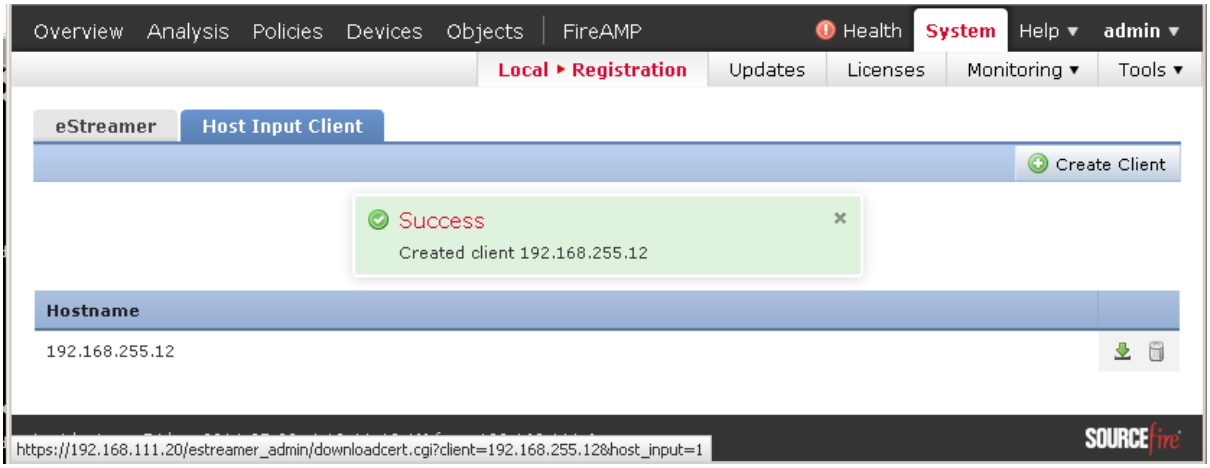


Fig. 15.21: The created PKCS12 file must be downloaded.

15.4.3 Configuration of Alerts on the GSM

Now the respective Alerts must be set up on the GSM. For this switch to *Configuration/Alerts*. Enter the data of the Sourcefire system and the supply the PKCS12 file.

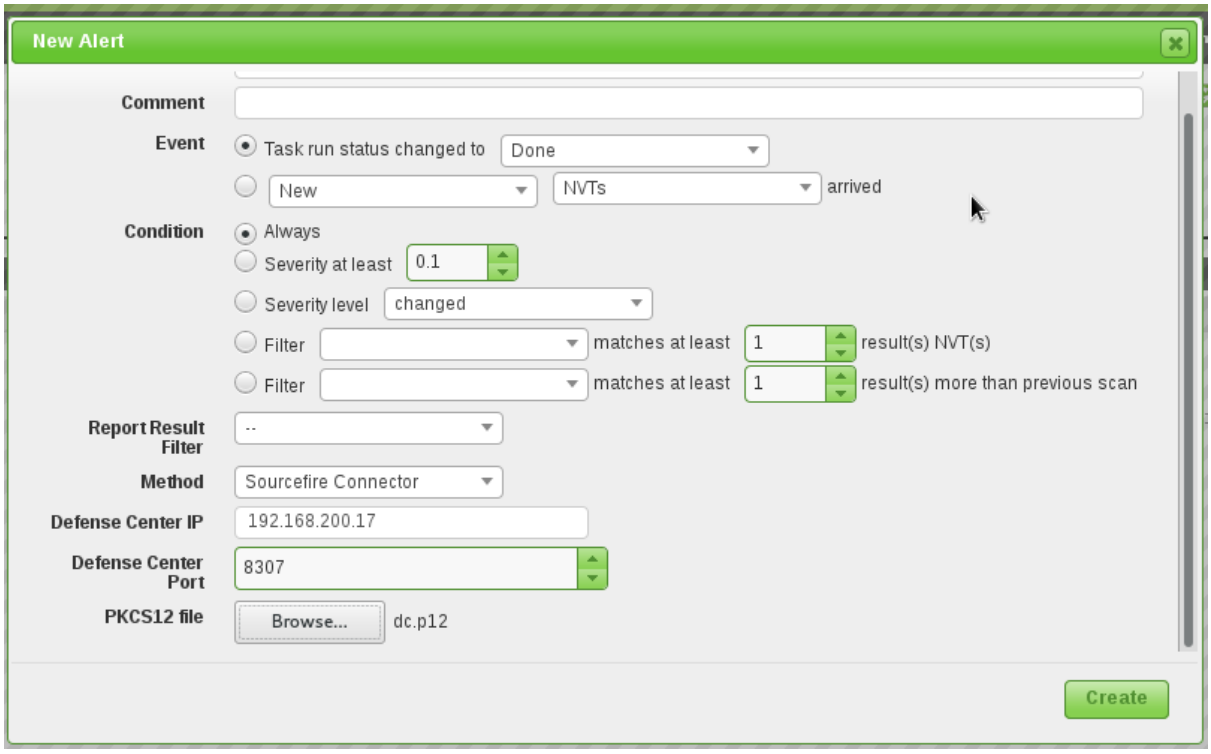


Fig. 15.22: The PKCS12 file is being used by the connector for authentication.

If a password was entered when the client was created the PKCS12 must be decrypted before loading it onto the GSM. For this you can use the following command under Linux:

```
$ openssl pkcs12 -in encrypted.pkcs12 -nodes -out decrypted.pcks12
Enter Import Password : password
MAC verified OK
$
```

15.5 Splunk

The Greenbone Security Manager may be configured to forward the scan results to a splunk enterprise installation for further analysis and correlation.

The Splunk integration requires the installation of the Greenbone-Splunk-App on the splunk server. The download and installation of the app are explained in section *Splunk Application* (page 244).

Once the app is installed on the splunk server the GSM may be instructed to send the results to the splunk server. This section will cover the configuration of the GSM.

15.5.1 Configuration of the Splunk Alert

To configure the GSM navigate to *Configuration* followed by *Alerts*. Create a new alert by clicking the icon .

Setup the alert and specify a name and a comment. Choose the event and the Condition for the forwarding of the results to the Splunk server. The defaults are probably appropriate for most environments.

Scroll down to the option *Send to host*. Fill in the IP address of the splunk server and the port of the Greenbone App. This tcp port is 7680 by default. This setting can be checked using the Splunk Web-Gui via Settings->Data inputs->TCP (see section *Splunk Application* (page 244)). Choose the XML format.

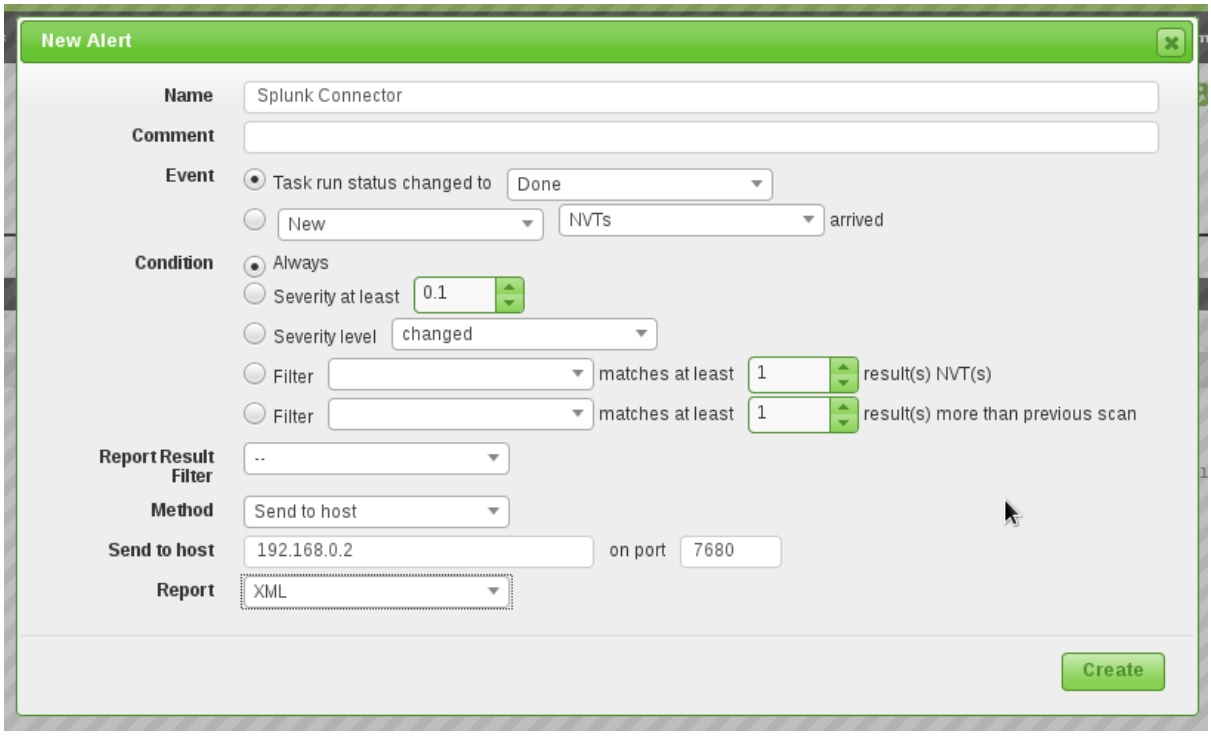


Fig. 15.23: Configuration of the splunk alert.

This alert can now be added to the appropriate tasks. Navigate to *Scan Management* and create a new task using the alert. The alert may even be added to already existing tasks because the alert does not modify the scan behavior.

For testing purposes existing reports may be processed by the alert. Navigate to *Scan Management* followed by *Reports*. Choose any existing report and switch to the *Summary and Download* view. Here you can process the report using any configured alert.

	High	Medium	Low	Log	False Pos.	Total	Run Alert
Full report:	5	0	1	11	0	17	Splunk Connector
Filtered report:	5	0	0	0	0	5	Splunk Connector

User Tags (none)

Fig. 15.24: Processing an existing report using the alert.

15.5.2 Accessing the Information in Splunk

To access the information in Splunk switch to the Greenbone dashboard. The Greenbone dashboard within the Splunk web interface will display the vulnerabilities found within the last 7 days.

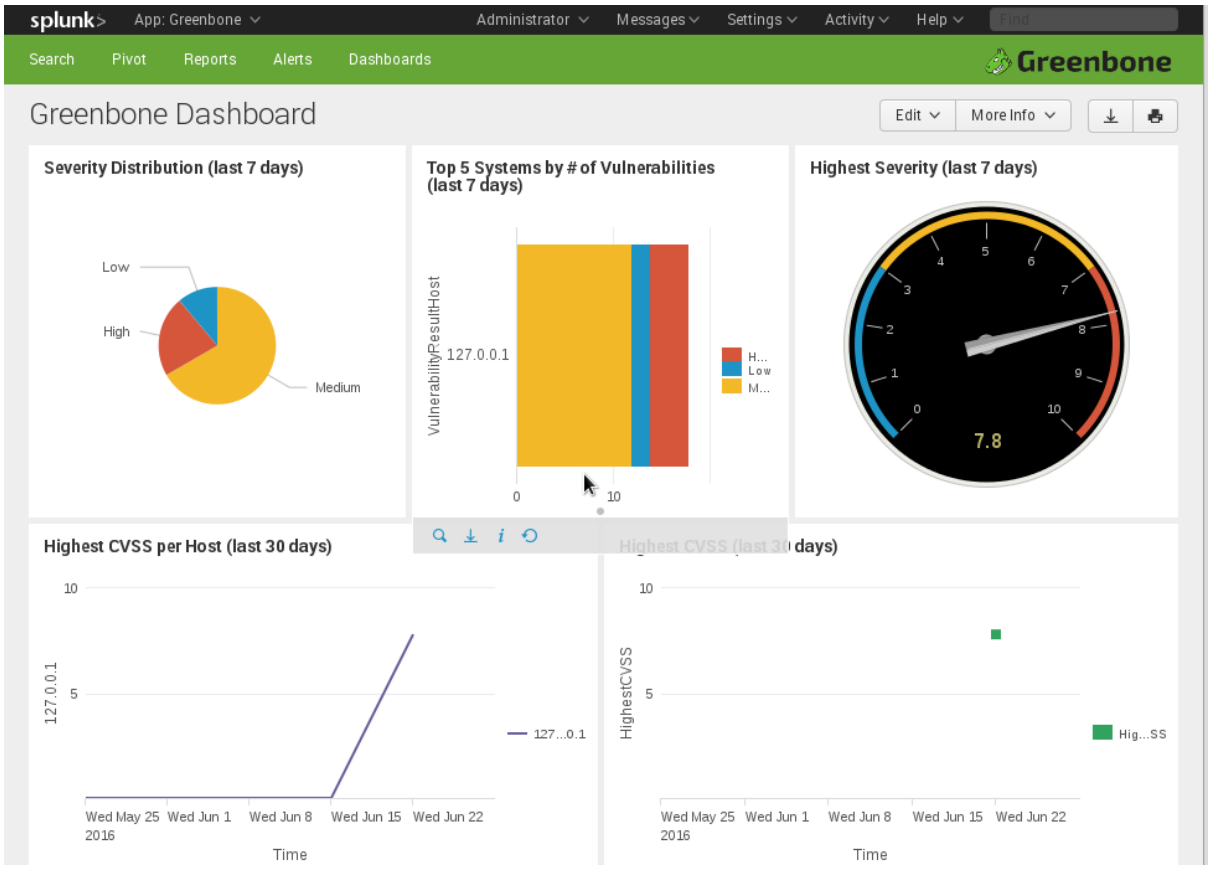


Fig. 15.25: The Greenbone dashboard provides a quick overview.

Since the information forwarded by the GSM is indexed by Splunk you can use the Search view to search for any data.

Some supported indexes are:

- host
- source, sourcetype
- date_hour, date_minute, date_month, date_year, date_mdate, date_wday, date_zone
- VulnerabilityResultNvtCVE
- VulnerabilityResultNvtCVSS
- VulnerabilityResultQod

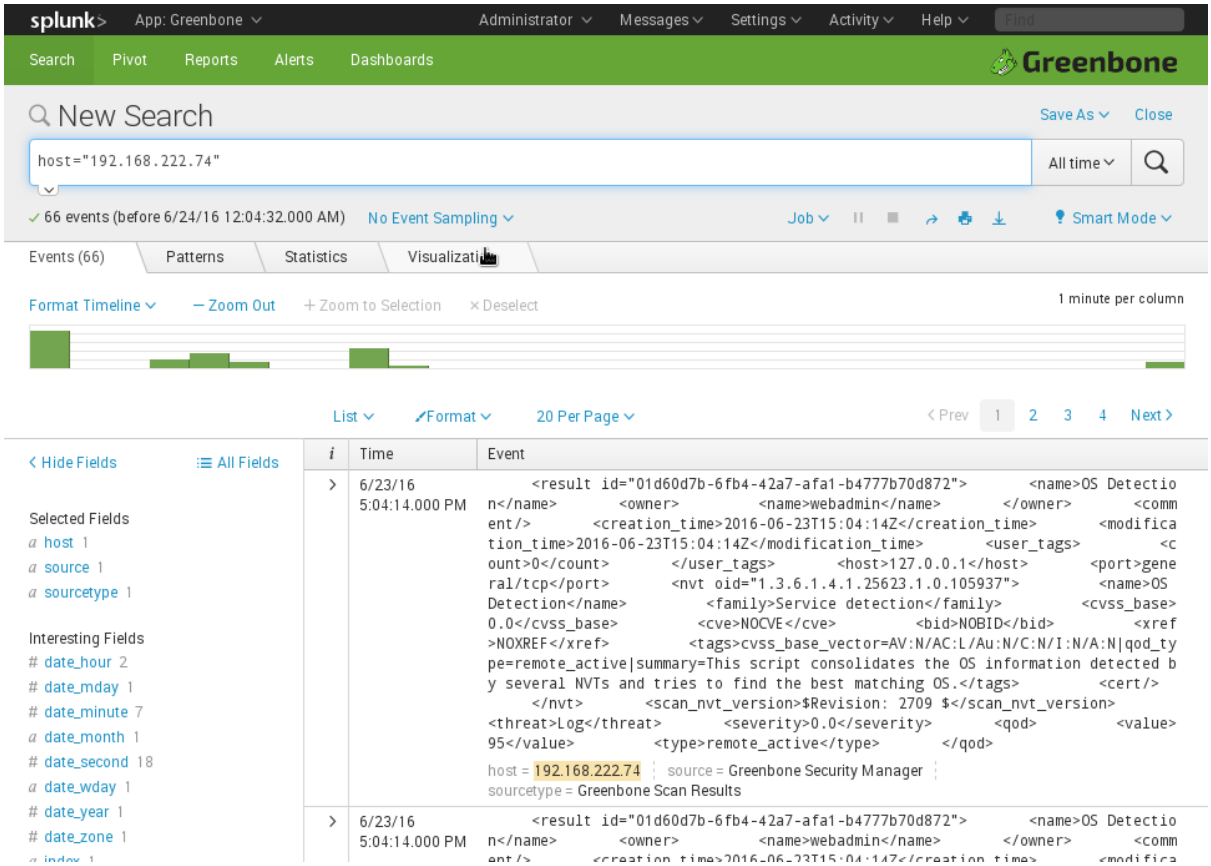


Fig. 15.26: The splunk server supports complex searches.

- VulnerabilityResultSeverity
- VulnerabilityResultThreat

CHAPTER 16

Tools

This chapter presents some additional tools which may be used with the GSM appliance.

16.1 GVM-Tools

The `gvm-tools` implement the Greenbone Management Protocol (GMP). These tools are supplied by Greenbone Networks for both the Linux and the Windows operating system. These tools are provided both as a commandline tool and a Python Python Shell. You can download the tools for Microsoft Windows at:

- CLI gvm-cli.exe[136]:
  - SHA256 checksum: dc1af9c7a715c738e124188a21dc02c2fa1c84bbc454ab1a2528e8f2a0a45989
- Python Shell gvm-pyshell.exe[137]:
  - SHA256 checksum: 9c65b595138c11f0d5e2684cf5dec73a9e4b725d1186614e231c0572ab46dc38

The listed checksums were checked and found to be valid on March 15th 2018 and may be outdated in the future. Please contact Greenbone support for current checksums if the checksums do not match.

The tool is a statically linked executable file that should work on most Microsoft systems. Greenbone has released all components as open source so you can build the tool for other systems like Linux as well:

- https://bitbucket.org/greenbone/gvm-tools

Please be aware of the fact, that the tools require Python3 to work. To install the tools first clone the repository and then install the tools using:

```
$ hg clone https://bitbucket.org/greenbone/gvm-tools
$ cd gvm-tools
$ sudo python3 setup.py install
```

Greenbone has already developed a small collection of scripts using these tools they may be found in the scripts directory at the BitBucket repository.

The usage of the tool is explained in section *Greenbone Management Protocol* (page 205).

16.2 `check_gmp.py`

Greenbone provides the `check_gmp.py` plugin for integration of the GSM appliance into network monitoring solutions like Nagios, Icinga and Check_MK. The tool may be downloaded from http://download.greenbone.net/tools/check_gmp.py.

[136] http://download.greenbone.net/tools/gvm-cli.exe
[137] http://download.greenbone.net/tools/gvm-pyshell.exe

The SHA256 checksum is:

- SHA256: 7d483bd2ad304872c5f4487a492ef6e4357b58aecd68f51fc7b363fa8273a9bb.

This checksum was validated on Sept 6th 2017. If the checksum of the downloaded file differs, please contact Greenbone Networks Support.

The tool is a python script that requires the installation of the gvm-tools. Greenbone has released all components as open source so you can build the tool for other systems as well

Download the plugin to your monitoring system and make it executable:

```
omd-host :~# wget -q http://download.greenbone.net/tools/check_gmp.py
omd-host :~# chmod 755 check_gmp.py
omd-host :~# $ /tmp/check_gmp.py --version
check_gmp 1.0
```

The usage of the plugin is described in section *Nagios* (page 231).

16.3 Splunk Application

Greenbone Networks offers a small application for the integration with Splunk. The application is currently available at http://download.greenbone.net/tools/Greenbone-Splunk-App-1.0.1.tar.gz. If you have problems downloading or testing the application please contact Greenbone Support.

The installation of the splunk app is quite simple. The following guide uses the splunk enterprise version 6.4.3. The installation of the app in splunk light is not supported.

To install the app first login to your splunk server. Navigate to Splunk->Apps->Manage Apps.

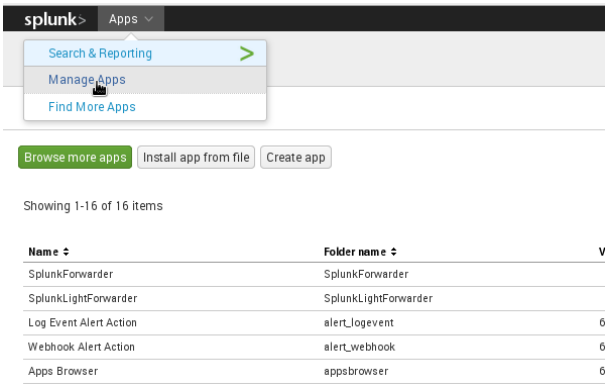


Fig. 16.1: Splunk support the installation of 3rd party add-ons.

Choose Install app from file. Browse to the downloaded Greenbone-Splunk-App and upload it to the splunk server.

Choose Upload. The next screen will show the successful installation of the plugin.

Please check the port of the Greenbone-Splunk-App after the installation. You can access the port in the Web-Gui via Settings->Data inputs->TCP.

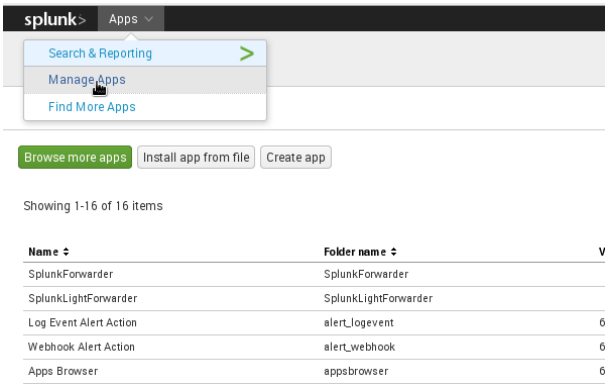


Fig. 16.2: 3rd party add-ons may be installed from file.

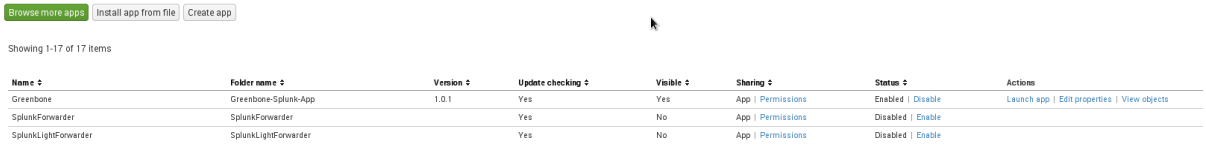


Fig. 16.3: Splunk lists the add-on after successful installation.

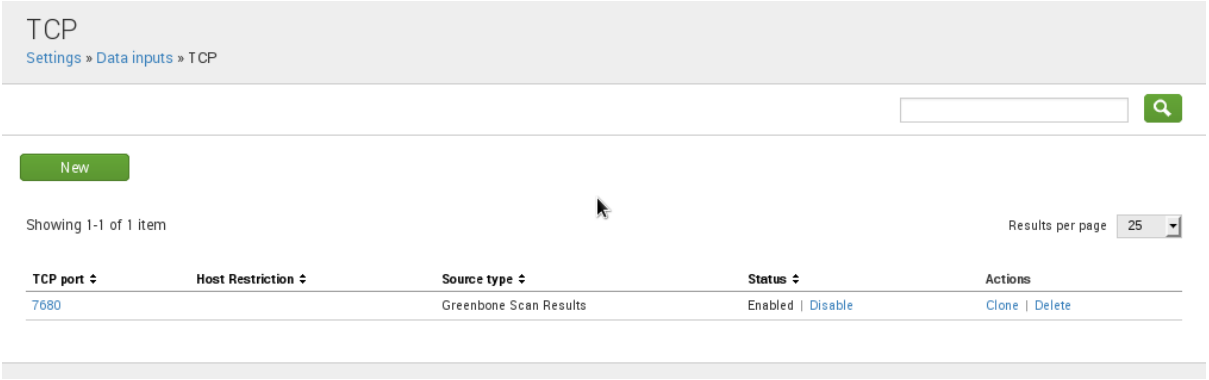


Fig. 16.4: The port of the app is required for the configuration on the GSM.

CHAPTER 17

Setup Guides

This chapter provides specific setup guides and trouble shooting for the different GSM appliances:

17.1 GSM ONE

This setup guide will show the steps required to put the GSM ONE appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
VirtualBox installed	
Integrity verification (optional)	
Import of the OVA	
Resources: 2 CPUs, 2GB Ram	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Web admin account	
SSL certificate	
Readiness	

17.1.1 Requirements

This section lists the requirements for the successful deployment of the GSM ONE appliance. Please ensure that all requirements are met.

Resources

The virtual appliance requires at least the following resources:

- 2 virtual CPUs

- 2 GB RAM

Supported Hypervisor

While the GSM ONE may be run on different hypervisors, only the following two hypervisors are currently supported:

- Oracle VirtualBox on GNU/Linux
- Oracle VirtualBox on Microsoft Windows

Verification of Integrity

The integrity of the virtual appliance may be verified. On request the Greenbone support provides an integrity checksum. To request the checksum please contact the Greenbone support via email (emailto:support@greenbone.net). Include your subscription number in the email. The integrity checksum may be provided via phone or via support portal at https://support.greenbone.net. Please specify the preferred channel in the email.

The local verification of the checksum depends on the host operating system.

On Linux systems use the following command to calculate the checksum:

```
sha256sum GSM-ONE-3.1.19-18-gsf201599999.ova
```

On Windows systems you first have to install an appropriate program. You may use rehash which can be found at http://rehash.sourceforge.net. To calculate the checksum, use:

```
rehash.exe -none -sha256 C:\<path>\GSM-ONE-3.1.19-18-gsf201599999.ova
```

If the checksum does not match the checksum provide by the Greenbone support the virtual appliance has been modified and should not be used.

Deployment

Each GSM ONE is activated using a unique subscription key. You may not clone the GSM ONE and use several instances in parallel. This may result in inconsistencies and unwanted side effects.

17.1.2 Importing of the Virtual Appliance

The virtual appliances are being provided by Greenbone in the Open Virtualization Appliance (OVA) format. These files are easily imported into VMWare or VirtualBox. The following scenarios are supported by Greenbone:

- GSM ONE: Oracle VirtualBox (Linux and Microsoft Windows)
- GSM 25V: ESXi 5.1 or higher

Import into VirtualBox

Install Oracle VirtualBox for your operating system. VirtualBox is often included with Linux distributions. Should this not be the case and for the different versions of Microsoft Windows, VirtualBox is available directly from Oracle http://virtualbox.org/wiki/Downloads.

Once installed, start VirtualBox. Now you can import the OVA-file via *File -> Import Appliance* (see figure *Import of the OVA-Appliance* (page 249))

Confirm the configuration of the virtual machine in the following window (see figure *Accepting the hardware configuration* (page 249)). If possible, select 4096 MB RAM (memory) for optimal configuration of the virtual appliance. Accept the remaining hardware settings.

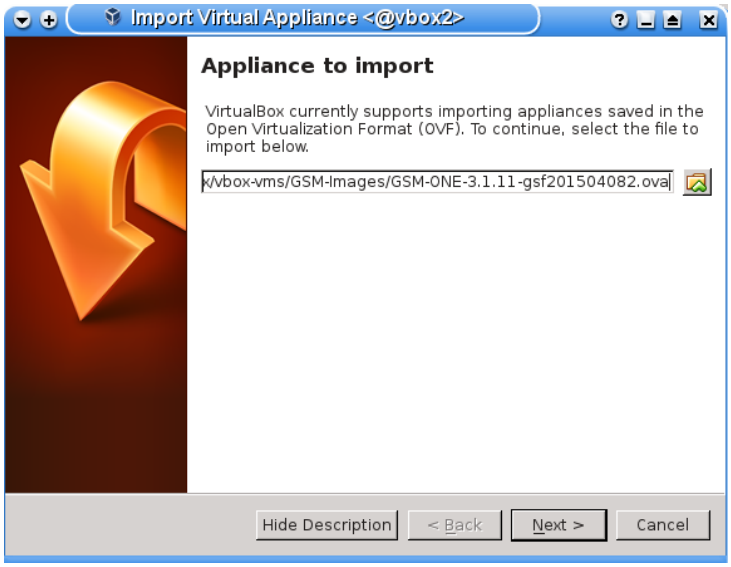


Fig. 17.1: Import of the OVA-Appliance

The actual import can take up to 10 minutes. Once imported you can start the virtual appliance.

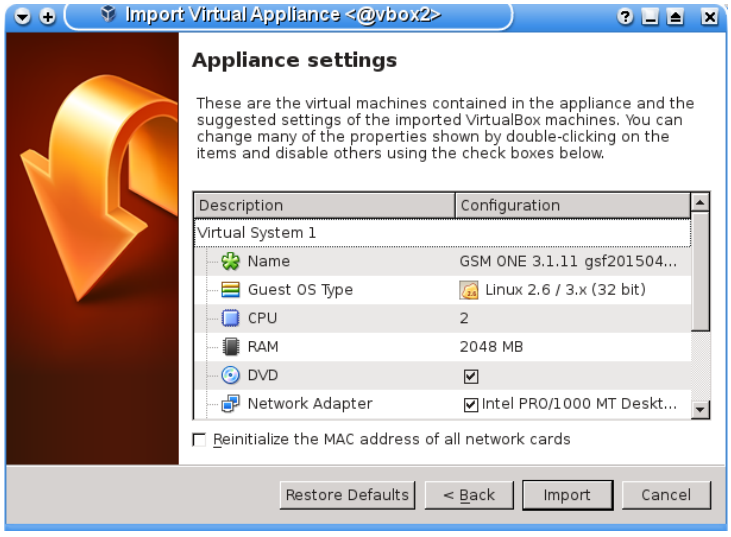


Fig. 17.2: Accepting the hardware configuration

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

Please follow the steps described in chapter *System Administration* (page 17) and then continue with the next sections for logging in or for troubleshooting.

17.1.3 Login to the Webinterface

The main interface of the GSM is the web gui. To access the web gui use a current web browser and access https://<ip-of-the-gsm>/.

The IP address of the GSM is displayed at the login prompt of the console.

Login using the web admin you created during the setup.

17.1.4 GSM ONE troubleshooting

The following warnings and problems are known and depend on your environment:

- On Linux host systems VirtualBox may warn during the import that the Host-I/O-Cache is activated if the virtual image is stored on a xfs partition. This warning is expected and may be accepted.
- On Linux host systems the warning "Failed to attach the network LUN (VERR_INTNET_FLT_IF_NOT_FOUND)" is displayed if the virtual machine does not discover any network card. The network card within the VirtualBox hypervisor needs to be configured. Usually the default can be accepted.

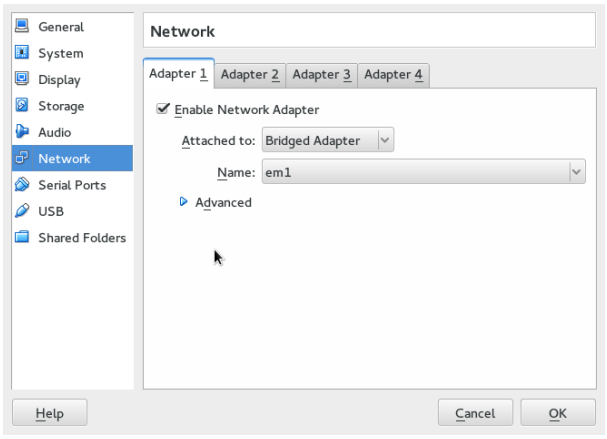


Fig. 17.3: Choose the correct network card in VirtualBox

- If the warning "AMD-V is disabled in the BIOS. (VERR_SVM_DISABLED)." is displayed, you need to enable the option "VT-X/AMD-V" in the BIOS of your host. An alternative solution is disabling of the acceleration in the system configuration of the virtual machine.

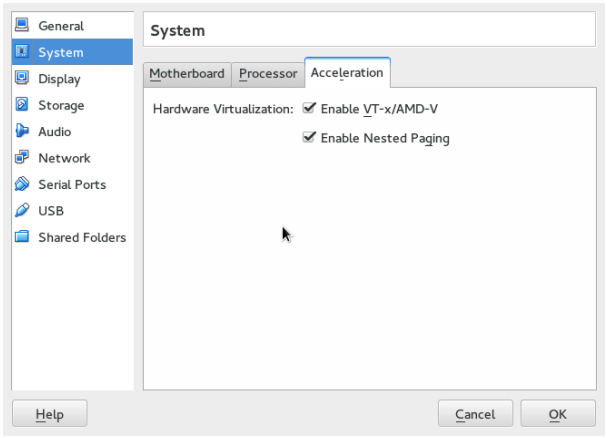


Fig. 17.4: Disabling the hardware acceleration in VirtualBox

17.2 GSM 25V

This setup guide will show the steps required to put the GSM 25V virtual appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
VMware ESXi 5.1 or higher	
Download of the ISO image	
Resources: 2 CPUs, 4GB Ram	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Scan user account	
SSL certificate	
Master key download	
Sensor setup on the master	
Readiness	

17.2.1 Requirements

This section lists the requirements for the successful deployment of the GSM 25V appliance. Please ensure that all requirements are met.

Resources

The virtual appliance requires at least the following resources:

- 2 virtual CPUs
- 4 GB RAM

Supported Hypervisor

The GSM 25V is only supported for the following hypervisor:

- VMware ESXi 5.1 or higher

Deployment

You will receive the GSM 25V as a ISO image for installation. Usually the image does not include the latest updates. Feeds are never included. You will need to update and synchronize the current feed using the sensor or the master GSM after deployment.

Each GSM 25V requires a unique subscription key. This key is not pre-installed and needs to be installed manually before using the GSM 25V. You may not clone the GSM 25V and use several instances in parallel with the same subscription key. This may result in inconsistencies and unwanted side effects.

17.2.2 Installation of the GSM 25V

The virtual appliances are being provided by Greenbone as ISO images for easy installation from a virtual CD drive. The following scenarios are supported by Greenbone:

- GSM 25V: ESXi 5.1 or higher

To install the GSM 25V setup a virtual machine using the following characteristics:

- 4 GB RAM
- 2 CPUs
- 20GB harddisk

- Choose the GSM 25V ISO image for the installation

Start the installation of the virtual machine.

- On the first screen choose Setup.

Fig. 17.5: Setup menu

- Confirm the warning message.

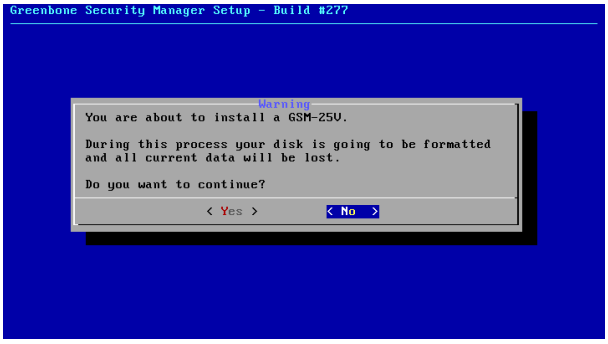


Fig. 17.6: The installation will overwrite the existing disk.

- The installation will take a few minutes to complete.
- After the installation of the operating system the username of the console user must be entered.

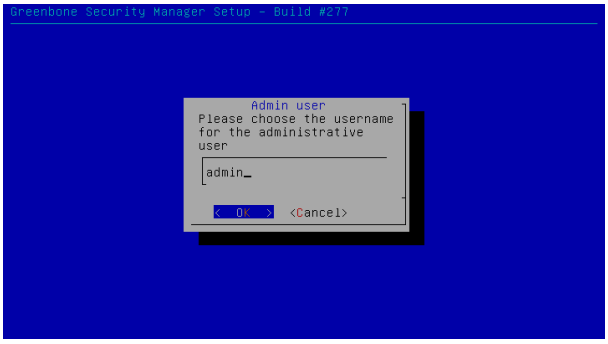


Fig. 17.7: Enter the name of the console user, e.g. admin.

- Enter the password of the console user.
- Now remove the virtual ISO image and reboot the virtual appliance.
- Do not login to the virtual appliance after the first reboot. The appliance will continue the setup of the system and will automatically reboot a second time within a few minutes.
- After the second reboot you may login to the virtual scan sensor using the configured console user and password.

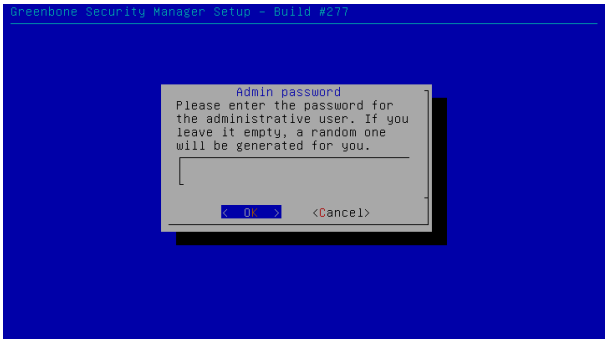


Fig. 17.8: Enter the password of the console user.

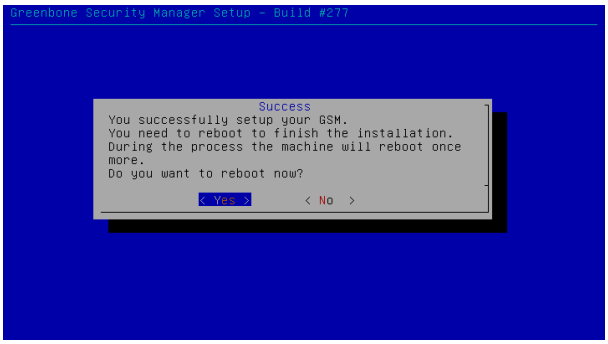


Fig. 17.9: Reboot the virtual appliance.

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

But being a sole sensor the GSM 25V differs in some steps from the other appliances:

- You do not add a web admin but a scan admin user account using *Setup/User/Users* followed by *Admin User*.
- You need to exchange the ssh keys with the master.

Please follow the steps described in chapter *System Administration* (page 17). Please remember to add the scan user account instead of a web admin account and then continue with the section *Sensor* (page 214) to exchange the keys with the master.

The GSM 25V sensor does not offer any web interface. You can login to the sensor using the console and SSH from the master. The sensor is solely managed from the master.

If the communication between the master and the sensor fails, you might need to adjust the rule-set of any internal firewall governing the network connection.

17.3 GSM 25

This setup guide will show the steps required to put a GSM 25 sensor appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
Powersupply	
Serial console cable / USB converter	
Putty/Screen setup	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Scan user account	
SSL certificate	
Master key download	
Sensor setup on the master	
Readiness	

17.3.1 Installation

The appliance GSM 25 is 19" mountable and requires 1 rack unit (RU). The optional RACKMOUNT25 kit provides the racking brackets for installation in a 19" rack. For stand-alone operation you will find 4 self-sticking rubber pads to be mounted on the corresponding bottom side embossments.

For cabling the GSM 25 appliance has corresponding connectors at the back:

- **back:**
  - Power supply +12V DC (one), external power supply and suitable cable enclosed
  - Network access (LAN1)
  - RS-232 console port, suitable cable is enclosed
  - Reset button

For the installation you have to use a terminal application and a serial cable to establish a connection.

17.3.2 Serial Port

To utilize the serial port use the enclosed console cable. Alternatively you can use a blue Cisco console cable (rollover-cable).

Should your system not come with a serial port you will require a USB-to-Serial adapter. Ensure the use of a quality adapter. Many cheap adapters can cause errors with the serial protocol. Additionally such adapters might not be compatible with the drivers that come with Microsoft Windows operating systems.

To access the serial port you require a terminal application. The application needs to be configured to a speed of 9600 Bits/s (Baud).

In Linux the command line command **`screen`** can be used. It is sufficient to run the command providing the serial port.

```
screen /dev/ttyS0  #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Sometimes it does not work with the first serial port. You have to experiment with the number (0, 1 or 2). You can quit the command by entering `CTRL-a \`. When starting the command it might be necessary to hit `RETURN` several times to get a command prompt.

In Windows you can use the Putty[138] application. After starting putty you will select the options as per Figure fig:putty-serial. Select the appropriate serial port also.

[138] http://www.chiark.greenend.org.uk/~sgtatham/putty/

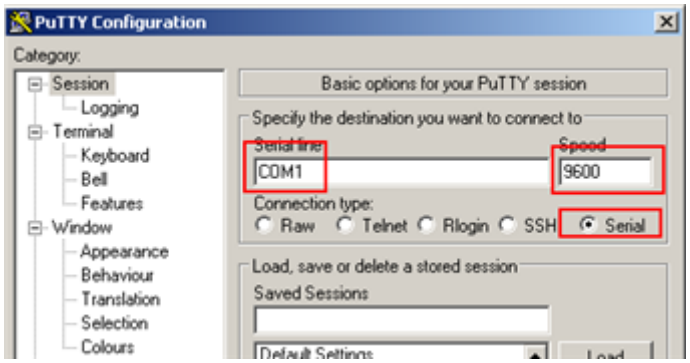


Fig. 17.10: Setting up the serial port in Putty

17.3.3 Startup

Once the appliance is fully wired and you are connected to the appliance via the console cable and have setup the terminal application (putty, screen or similar) you can power on the appliance. The appliance will boot and depending on the exact model the first messages will be displayed in the terminal application after a short time period.

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

But being a sole sensor the GSM 25 differs in some steps from the other appliances:

- You do not add a web admin but a scan user account.
- You need to exchange the masterkey with the sensor.

Please follow the steps described in chapter *System Administration* (page 17). Please remember to add the scan user account instead of a web admin account and then continue with the section *Sensor* (page 214) to exchange the keys with the master.

The GSM 25 sensor does not offer any web interface. You can login to the sensor using the console and SSH from the master. The sensor is solely managed from the master.

If the communication between the master and the sensor fails, you might need to adjust the rule-set of any internal firewall governing the network connection.

17.4 GSM 100

This setup guide will show the steps required to put a GSM 100 appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
Powersupply	
Serial console cable / USB converter	
Putty/Screen setup	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Web admin account	
SSL certificate	
Readiness	

17.4.1 Installation

The appliance GSM 100 is 19" mountable and requires 1 rack unit (RU). The optional RACKMOUNT100 kit provides the racking brackets for installation in a 19" rack. For stand-alone operation you will find 4 self-sticking rubber pads to be mounted on the corresponding bottom side embossments.

For cabling the GSM 100 appliance has corresponding connectors at the back:

- **back:**
  - Power supply +12V DC (one), external power supply and suitable cable enclosed
  - Network access (LAN1)
  - RS-232 console port, suitable cable is enclosed
  - Reset button

For the installation you have to use a terminal application and a serial cable to establish a connection.

17.4.2 Serial Port

To utilize the serial port use the enclosed console cable. Alternatively you can use a blue Cisco console cable (rollover-cable).

Should your system not come with a serial port you will require a USB-to-Serial adapter. Ensure the use of a quality adapter. Many cheap adapters can cause errors with the serial protocol. Additionally such adapters might not be compatible with the drivers that come with Microsoft Windows operating systems.

To access the serial port you require a terminal application. The application needs to be configured to a speed of 9600 Bits/s (Baud).

In Linux the command line command **`screen`** can be used. It is sufficient to run the command providing the serial port.

```
screen /dev/ttyS0  #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Sometimes it does not work with the first serial port. You have to experiment with the number (0, 1 or 2). You can quit the command by entering `CTRL-a \`. When starting the command it might be necessary to hit `RETURN` several times to get a command prompt.

In Windows you can use the Putty[139] application. After starting putty you will select the options as per Figure fig:putty-serial. Select the appropriate serial port also.

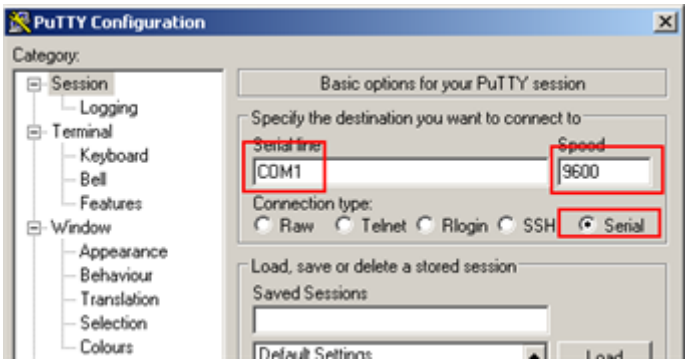


Fig. 17.11: Setting up the serial port in Putty

[139] http://www.chiark.greenend.org.uk/~sgtatham/putty/

17.4.3 Startup

Once the appliance is fully wired and you are connected to the appliance via the console cable and have setup the terminal application (putty, screen or similar) you can power on the appliance. The appliance will boot and depending on the exact model the first messages will be displayed in the terminal application after a short time period.

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

Please follow the steps described in chapter *System Administration* (page 17) and then continue with the next sections for logging in.

17.4.4 Login to the Webinterface

The main interface of the GSM is the web gui. To access the web gui use a current web browser and access https://<ip-of-the-gsm>/.

The IP address of the GSM is displayed at the login prompt of the console.

Login using the web admin you created during the setup.

17.5 GSM 500/510/550

This setup guide will show the steps required to put a GSM 500, 510 or 550 appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
Powersupply	
Serial console cable / USB converter	
Putty/Screen setup	
Firmware check (>= 2.0)	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Web admin account	
SSL certificate	
Readiness	

17.5.1 Installation

The appliances GSM 500, GSM 510 and GSM 550 are 19" mountable and require 1 rack unit (RU). For installation in a 19" this equipment comes with the respective racking brackets.

For cabling GSM 500, GSM 510 and GSM 550 appliances have corresponding connectors at the front and back:

- **back:**
  - Power supply (one)
  - VGA-monitor
  - Keyboard via USB
  - Serial Console

- **front:**
  - Keyboard via USB
  - Network port eth0
  - RS-232 console port (|0|0|0), Cisco compatible, suitable cable is enclosed

For the installation you have to use a terminal application and a console cable to establish a connection.

17.5.2 Serial Port

To utilize the serial port use the enclosed console cable. Alternatively you can use a blue Cisco console cable (rollover-cable).

Should your system not come with a serial port you will require a USB-to-Serial adapter. Ensure the use of a quality adapter. Many cheap adapters can cause errors with the serial protocol. Additionally such adapters might not be compatible with the drivers that come with Microsoft Windows operating systems.

To access the serial port you require a terminal application. The application needs to be configured to a speed of 9600 Bits/s (Baud).

In Linux the command line command **`screen`** can be used. It is sufficient to run the command providing the serial port.

```
screen /dev/ttyS0  #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Sometimes it does not work with the first serial port. You have to experiment with the number (0, 1 or 2). You can quit the command by entering `CTRL-a \`. When starting the command it might be necessary to hit `RETURN` several times to get a command prompt.

In Windows you can use the Putty[140] application. After starting putty you will select the options as per Figure fig:putty-serial. Select the appropriate serial port also.

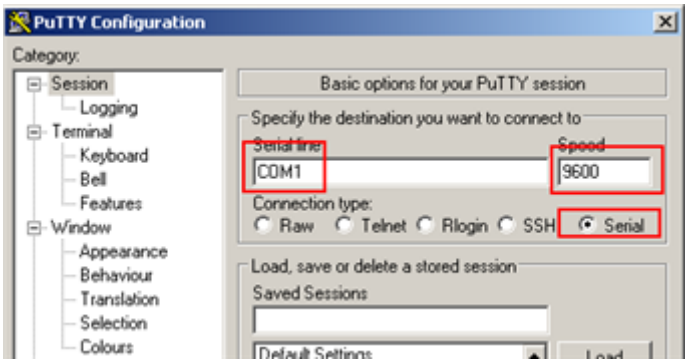


Fig. 17.12: Setting up the serial port in Putty

17.5.3 Startup

Once the appliance is fully wired and you are connected to the appliance via the console cable and have setup the terminal application (putty, screen or similar) you can power on the appliance. The appliance will boot and depending on the exact model the first messages will be displayed in the terminal application after a short time period.

[140] http://www.chiark.greenend.org.uk/~sgtatham/putty/

Firmware Notice

The appliances GSM 500, GSM 510 and GSM 550 are first generation devices. These devices were shipped with older firmware images which needs to be upgraded before the appliances are put into production. If the displayed flash version is < 2.0 please contact the Greenbone support (mailto:support@greenbone.net[141]) before continuing!

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

Please follow the steps described in chapter *System Administration* (page 17) and then continue with the next sections for logging in.

17.5.4 Login to the Webinterface

The main interface of the GSM is the web gui. To access the web gui use a current web browser and access https://<ip-of-the-gsm>/.

The IP address of the GSM is displayed at the login prompt of the console.

Login using the web admin you created during the setup.

17.6 GSM 400/600/650

This setup guide will show the steps required to put a GSM 400, 600 or 650 appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
Powersupply	
Serial console cable / USB converter	
Putty/Screen setup	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Web admin account	
SSL certificate	
Readiness	

17.6.1 Installation

The appliances GSM 400, GSM 600 and GSM 650 are 19" mountable and require 1 rack unit (RU). For installation in a 19" this equipment comes with the respective racking brackets.

For cabling GSM 400, GSM 600 and GSM 650 appliances have corresponding connectors at the front and back:

- **back:**
  - Power supply (one)
  - VGA-monitor
  - Keyboard via USB
  - Serial Console

[141] support@greenbone.net

- **front:**
  - Keyboard via USB
  - Network port eth0
  - RS-232 console port (|0|0|0), Cisco compatible, suitable cable is enclosed

For the installation you have to use a terminal application and a console cable to establish a connection.

17.6.2 Serial Port

To utilize the serial port use the enclosed console cable. Alternatively you can use a blue Cisco console cable (rollover-cable).

Should your system not come with a serial port you will require a USB-to-Serial adapter. Ensure the use of a quality adapter. Many cheap adapters can cause errors with the serial protocol. Additionally such adapters might not be compatible with the drivers that come with Microsoft Windows operating systems.

To access the serial port you require a terminal application. The application needs to be configured to a speed of 9600 Bits/s (Baud).

In Linux the command line command **`screen`** can be used. It is sufficient to run the command providing the serial port.

```
screen /dev/ttyS0  #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Sometimes it does not work with the first serial port. You have to experiment with the number (0, 1 or 2). You can quit the command by entering `CTRL-a \`. When starting the command it might be necessary to hit `RETURN` several times to get a command prompt.

In Windows you can use the Putty[142] application. After starting putty you will select the options as per Figure fig:putty-serial. Select the appropriate serial port also.

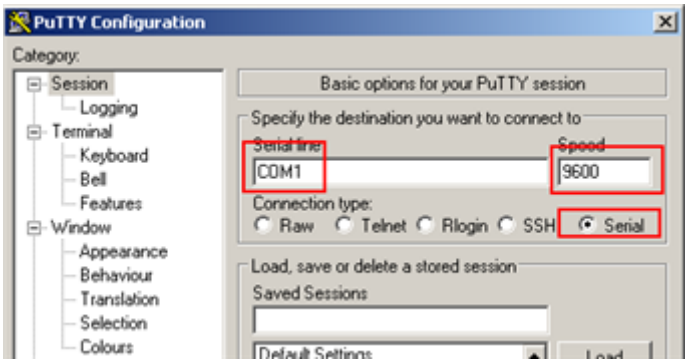


Fig. 17.13: Setting up the serial port in Putty

17.6.3 Startup

Once the appliance is fully wired and you are connected to the appliance via the console cable and have setup the terminal application (putty, screen or similar) you can power on the appliance. The appliance will boot and depending on the exact model the first messages will be displayed in the terminal application after a short time period.

[142] http://www.chiark.greenend.org.uk/~sgtatham/putty/

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

Please follow the steps described in chapter *System Administration* (page 17) and then continue with the next sections for logging in.

17.6.4 Login to the Webinterface

The main interface of the GSM is the web gui. To access the web gui use a current web browser and access https://<ip-of-the-gsm>/.

The IP address of the GSM is displayed at the login prompt of the console.

Login using the web admin you created during the setup.

17.7 GSM 5300/6400

This setup guide will show the steps required to put a GSM 5300 or 6400 appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
Powersupply (2 connectors)	
Serial console cable / USB converter	
Putty/Screen setup	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Web admin account	
SSL certificate	
Readiness	

17.7.1 Installation

The appliances GSM 5300 and GSM 6400 are 19" mountable and require 2 rack units (RU). For installation in a 19" this equipment comes with the respective racking brackets.

For cabling GSM 5300 and GSM 6400 appliances have corresponding connectors at the front and back:

- **back:**
  - Power supply (two)
  - VGA-monitor
- **front:**
  - Keyboard via USB
  - Network port labeled "MGMT" (eth0)
  - RS-232 console port (|O|O|O), Cisco compatible, suitable cable is enclosed

For the installation you have to use a terminal application and a console cable to establish a connection.

17.7.2 Serial Port

To utilize the serial port use the enclosed console cable. Alternatively you can use a blue Cisco console cable (rollover-cable).

Should your system not come with a serial port you will require a USB-to-Serial adapter. Ensure the use of a quality adapter. Many cheap adapters can cause errors with the serial protocol. Additionally such adapters might not be compatible with the drivers that come with Microsoft Windows operating systems.

To access the serial port you require a terminal application. The application needs to be configured to a speed of 9600 Bits/s (Baud).

In Linux the command line command **screen** can be used. It is sufficient to run the command providing the serial port.

```
screen /dev/ttyS0  #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Sometimes it does not work with the first serial port. You have to experiment with the number (0, 1 or 2). You can quit the command by entering `CTRL-a \`. When starting the command it might be necessary to hit `RETURN` several times to get a command prompt.

In Windows you can use the Putty[143] application. After starting putty you will select the options as per Figure fig:putty-serial. Select the appropriate serial port also.

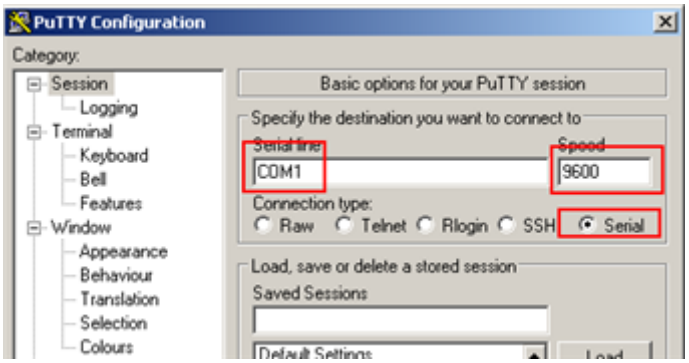


Fig. 17.14: Setting up the serial port in Putty

17.7.3 Startup

Once the appliance is fully wired and you are connected to the appliance via the console cable and have setup the terminal application (putty, screen or similar) you can power on the appliance. The appliance will boot and depending on the exact model the first messages will be displayed in the terminal application after a short time period.

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

Please follow the steps described in chapter *System Administration* (page 17) and then continue with the next sections for logging in.

[143] http://www.chiark.greenend.org.uk/~sgtatham/putty/

17.7.4 Login to the Webinterface

The main interface of the GSM is the web gui. To access the web gui use a current web browser and access https://<ip-of-the-gsm>/.

The IP address of the GSM is displayed at the login prompt of the console.

Login using the web admin you created during the setup.

Architecture

This chapter covers the architecture and the communication protocols used by the Greenbone Security Manager. Some protocols are mandatory and some protocols are optional. Some protocols are only used in specific setups.

18.1 Protocols

The GSM requires several protocols to fully function. These protocols provide the feed updates, DNS resolution, time, etc. The following protocols are used by a stand alone system or a GSM master to initiate connections being a client:

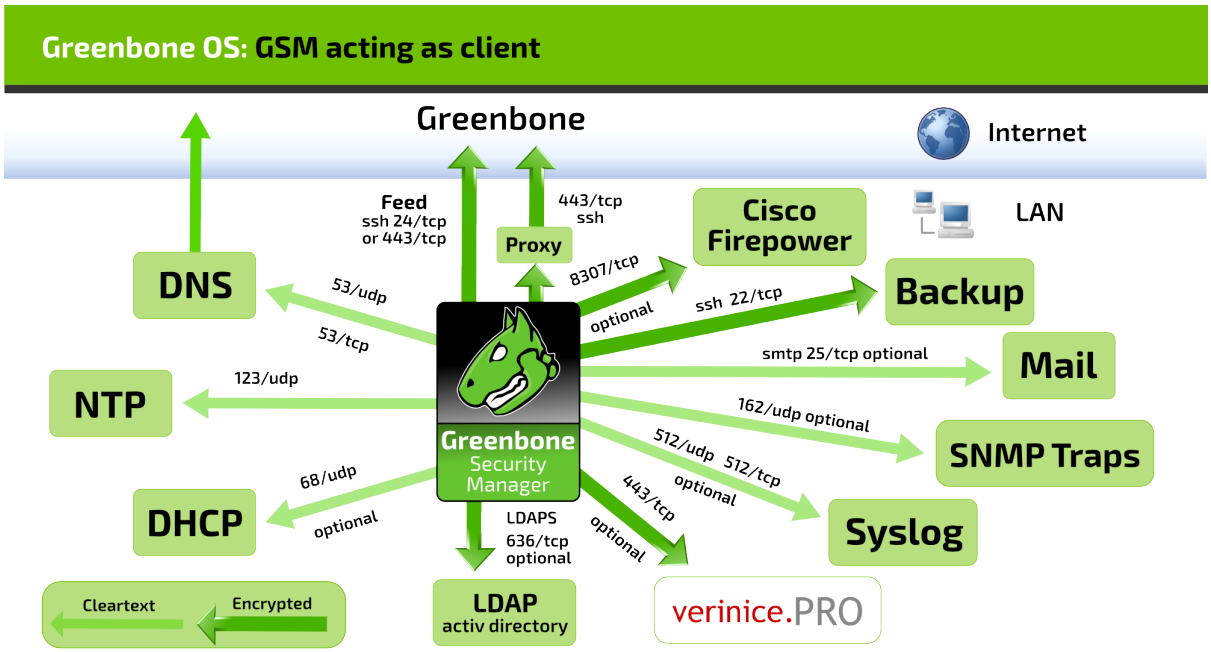


Fig. 18.1: GSM acting as client

- GSM is client
  - DNS - Name resolution
    * connecting to 53/udp and 53/tcp
    * mandatory
    * not encrypted

    * may use internal DNS server
- NTP - time synchronization
    * connecting to 123/udp
    * mandatory
    * not encrypted
    * may use internal NTP server
- Feeds (see below)
    * direct
        · connecting to 24/tcp or 443/tcp
        · direct Internet access required
    * via proxy
        · connecting to internal HTTP-Proxy supporting CONNECT method on configurable port
    * connecting to apt.greenbone.net and feed.greenbone.net
    * mandatory on stand-alone and master appliances
    * Protocol used is SSH
    * encrypted and bidirectionally authenticated via SSH
        · Server: public key
        · Client: public key
- DHCP
    * connecting to 67/udp and 68/udp
    * optional
    * not encrypted
- LDAPS - User authentication
    * connecting to 636/tcp
    * optional
    * encrypted and authenticated via SSL/TLS
        · Server: certificate
        · Client: username/password
- Syslog - Remote Logging and alerts
    * connecting to 512/udp or 512/tcp
    * optional
    * not encrypted
- SNMP Traps for alerts
    * connecting to 162/udp
    * optional
    * just SNMPv1
    * not encrypted
- SMTP for E-Mail alerts

    * connecting to 25/tcp
    * optional
    * not encrypted
  - SSH for Backup
    * connecting to 22/tcp
    * optional
    * encrypted and bidirectionally authenticated via SSH
      · Server: public key
      · Client: public key
  - Cisco Firepower (Sourcefire) for IPS integration
    * connecting to 8307/tcp
    * optional
    * encrypted and bidirectionally authenticated via SSL/TLS
      · Server: certificate
      · Client: certificate
  - verinice.PRO
    * connecting to 443/tcp
    * optional
    * encrypted via SSL/TLS
      · Server: optionally via certificate
      · Client: username/password

The following connection are accepted by a GSM acting as a server.

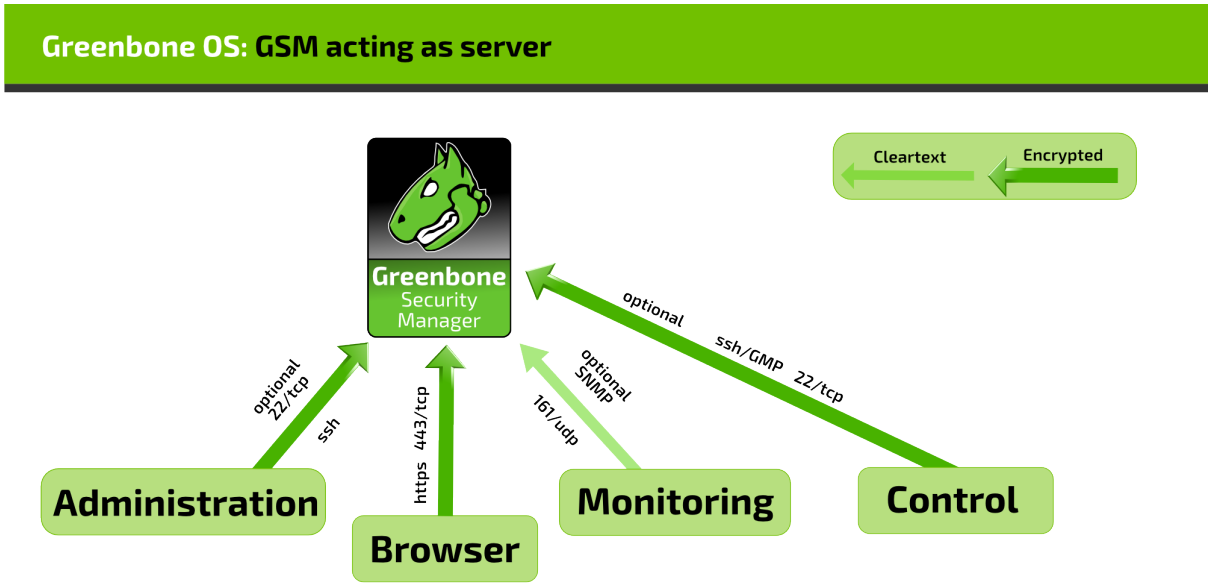


Fig. 18.2: GSM acting as server

- GSM is server
  - HTTPS - Web interface
    * 443/tcp
    * mandatory on stand-alone and master appliances
    * encrypted and authenticated via SSL/TLS
      · Server: optionally via certificate
      · Client: username/password
  - SSH - CLI access and GMP
    * 22/tcp
    * optional
    * encrypted and authenticated via SSH
      · Server: public key
      · Client: username/password
  - SNMP
    * 161/udp
    * optional
    * optionally encrypted when using SNMPv3

In a master/sensor setup the following additional requirements apply. The master (client) initiates two additional connections to the sensor (server):

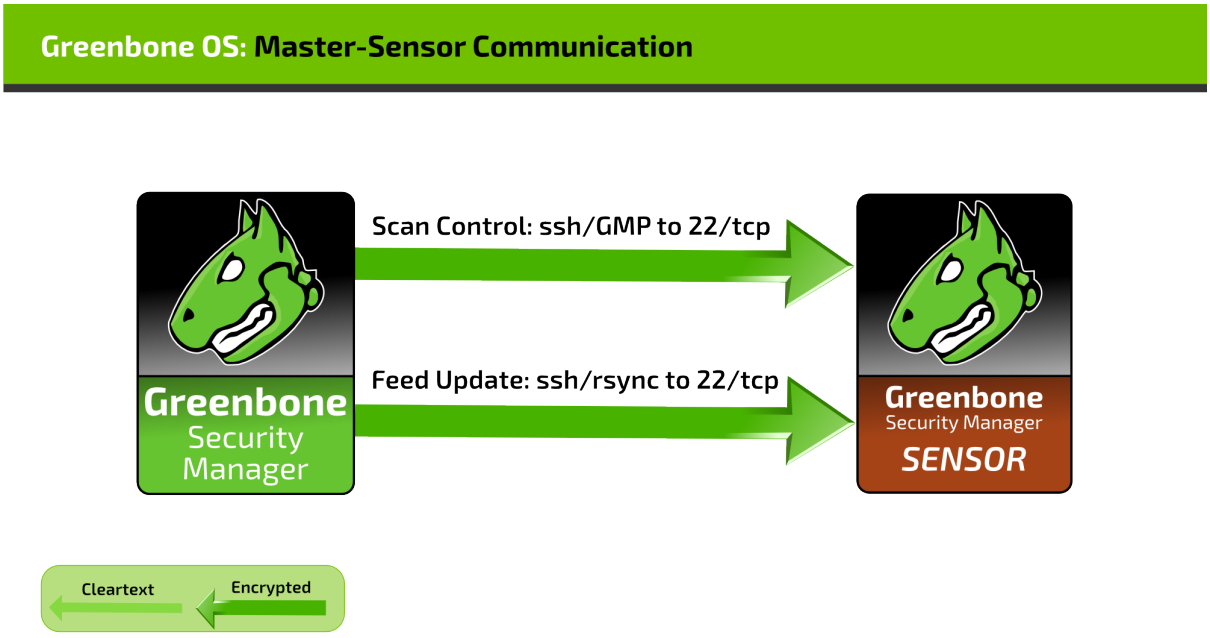


Fig. 18.3: GSM master and sensor

- SSH for Updates and Feeds and GMP
  - 22/tcp
  - mandatory

- encrypted and bidirectionally authenticated via SSH
  * Server: public key
  * Client: public key

18.2 Security Gateway Considerations

Many enterprises deploy security gateways to restrict the Internet access. These security gateways may operate as packet filters or application layer gateways. Some products support deep inspection and try to determine the actual protocol used in the communication channels. They might even try to decrypt and analyze any encrypted communication.

18.2.1 Standalone/Master GSM

While many protocols used by the GSM are only used internally, some protocols require access to the Internet. These might be filtered by such a security gateway. When deploying the GSM as standalone appliance or master the GSM needs to be able to access the Greenbone security feed. The Greenbone security feed may be access directly via port 24/tcp or 443/tcp or using a proxy. In all cases the actual protocol used is SSH. Even when using the port 443/tcp or a HTTP proxy the protocol used is SSH.

A deep inspection firewall might detect the usage of the SSH protocol running on port 443/tcp and could drop or block the traffic. If the security gateway would try to decrypt the traffic using man-in-the-middle techniques the communication of the GSM and the Feed server will fail. The SSH protocol using bidirectional authentication based on public keys will prevent any man-in-the-middle approach by terminating the communication.

Additional protocols which might need Internet access are DNS and NTP. Both DNS and NTP may be configured to use internal DNS and NTP servers.

18.2.2 Sensor GSM

If security gateways are deployed between the master and the sensor the security gateway must permit SSH (22/tcp) and GMP (9390/tcp) connections from the master to the sensor.

CHAPTER 19

Frequently Asked Questions

This section collects frequently asked questions with answers.

19.1 What is the difference between a scan sensor and a scan slave?

A scan slave is controlled by a scan master for doing vulnerability scans. Scans for scan slaves are configure on the scan master by each user as needed and permitted. GSMs from midrange upward can act as a master and control one or many scan slaves. Any GSM can act as a scan slave. Any scan slave has to take care on its own to update the feed and release.

A scan sensor is a GSM that solely works as scan slave but is also fully managed by the master unit. This management includes automatic feed and release updates. Essentially, a sensor does not require any other connection than to its master and, once installed, does not require any administrative works.

19.2 Scan process very slow

The performance of a scan depends on various aspects.

- Several port scanners were activated concurrently.

  If your are using a individual Scan Config please take care to select only a single port scanner in the family “Port Scanner”. Of course “Ping Host” can still be activated.

- Unused IP addresses are scanned very time-consuming.

  In a first phase for each IP address it is detected whether a active system is present. In case it is not, this IP will not be scanned. Firewalls and other systems can prevent a successful detection. The NVT “Ping Host” (1.3.6.1.4.1.25623.1.0.100315) offers to fine-tune detection.

19.3 Scan triggers alarm at other security tools

For many vulnerability tests the behaviour of real attacks is applied. Even though a real attack does not happen, some security tools will issue an alarm.

Known examples are:

- Symantec reports attack regarding CVE-2009-3103 if the NVT “Microsoft Windows SMB2 ‘_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability” (1.3.6.1.4.1.25623.1.0.100283) is executed. This NVT is only executed if “safe checks” is explicitly disabled in the Scan Configuration because it can affect the target system.

19.4 On scanned target systems appears a VNC dialog

When testing port 5900 or configured VNC port, a window appears on scanned target system that asks the user whether to allow the connection. This was observed for UltraVNC Version 1.0.2.

Solution: Exclude port 5900 or other configured VNC port from target specification. Alternatively upgrade to a newer version of UltraVNC would help (UltraVNC 1.0.9.6.1 only uses balloons to inform users).

19.5 After Factory Reset neither Feed-Update nor System-Upgrade works

(This is not relevant for virtual appliances where no factory reset is integrated anyway)

A Factory Reset deletes the whole system including the subscription key. The key is mandatory for Feed-Update and System-Upgrade.

1. Reactivate subscription key:

   A backup key is delivered with each GSM appliance, usually stored on a USB Stick and labelled with the key ID. Use this key to reactivate the GSM. The activation is described in the SetUp Guide of the respective GSM type.

2. Update system to current version:

   Depending on the age of the factors emergency system you now need to execute the respective upgrade procedure.

CHAPTER 20

Glossary

This section defines relevant terminology which is consistently used across the entire system.

20.1 Host

A Host is a single system that is connected to a computer network and that may be scanned. One or many hosts form the basis of a scan target.

A host is also an asset type. Any scanned or discovered host can be recorded in the asset database.

Hosts in scan targets and in scan reports are identified by their network address, either an IP address or a hostname.

20.2 Quality of Detection (QoD)

The Quality of Detection (QoD) is a value between 0% and 100% describing the reliability of the executed vulnerability detection or product detection.

This concept also solves the challenge of potential vulnerabilities. Such are always recorded and kept in the results database but are only visible on demand.

While the QoD range allows to express the quality quite fine-grained, in fact most of the test routines use a standard methodology. Therefore QoD Types are associate with a QoD value. The current list of types might be extended over time.

QoD	QoD Type	Description
100%	exploit	The detection happened via an exploit and therefore is fully verified.
99%	remote_vul	Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability.
98%	remote_app	Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.
97%	package	Authenticated package-based checks for Linux(oid) systems.
97%	registry	Authenticated registry-based checks for Windows systems.
95%	remote_active	Remote active checks (code execution, traversal attack, sql injection etc.) where the response shows the likely presence of the vulnerable application or of the vulnerability. "Likely" means that only rare circumstances are possible where the detection would be wrong.
80%	remote_banner	Remote banner check of applications that offer patch level in version. Many proprietary products do so.
80%	executable_version	Authenticated executable version checks for Linux(oid) or Windows systems where applications offer patch level in version.
75%		This value was assigned to any pre-qod results during system migration. However, some NVTs eventually might own this value for some reason.
70%	remote_analysis	Remote checks that do some analysis but which are not always fully reliable.
50%	remote_probe	Remote checks where intermediate systems such as firewalls might pretend correct detection so that it is actually not clear whether the application itself answered. This can happen for example for non-TLS connections.
30%	remote_banner_unreliable	Remote banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.
30%	executable_version_unreliable	Authenticated executable version checks for Linux(oid) systems where applications don't offer patch level in version identification.
1%	general_note	General note on potential vulnerability without finding any present application.

The value of 70% is the default minimum used for the default filtering to display the results in the reports.

20.3 Severity

The Severity is a value between 0.0 (no severity) and 10.0 (highest severity) and expresses also a Severity Class (None, Low, Medium or High).

This concept is based on CVSS but is applied also where no full CVSS Base Vector is available. For example, arbitrary values in that range are applied for Overrides and used by OSP scanners even without a vector definition.

Comparison, weighting, prioritisation is possible of any scan results or NVTs because the severity concept is strictly applied across the entire system. Not a single severity is just expressed as “High” for example. Any new NVT is assigned with a full CVSS vector even if CVE does not offer one and any results of OSP scanners is assigned a adequate severity value even if the respective scanner uses a different severity scheme.

The severity classes None, Low, Medium and High are defined by sub-ranges of the main range 0.0-10.0. Users can select to use different classifications. The default is the NVD classification which is the most commonly used one.

Scan results are assigned a severity while achieved. The severity of the related NVT may change over time though. Users can select Dynamic Severity to let the system always use the most current severity of NVTs for the results.

20.4 Solution Type

This information shows possible solutions for the remediation of the vulnerability. Currently three different variants are available:

- Workaround: Information is available about a configuration or specific deployment scenario that can be used to avoid exposure to the vulnerability. There may be none, one, or more workarounds available. This is typically the “first line of defense” against a new vulnerability before a mitigation or vendor fix has been issued or even discovered.
- Mitigation: Information is available about a configuration or deployment scenario that helps to reduce the risk of the vulnerability but that does not resolve the vulnerability on the affected product. Mitigations may include using devices or access controls external to the affected product. Mitigations may or may not be issued by the original author of the affected product, and they may or may not be officially sanctioned by the document producer.
- Vendor-Fix: Information is available about an official fix that is issued by the original author of the affected product. Unless otherwise noted, it is assumed that this fix fully resolves the vulnerability.
- None-Available: Currently there is no fix available. Information should contain details about why there is no fix.
- WillNotFix: There is no fix for the vulnerability and there never will be one. This is often the case when a product has been orphaned, end-of-lifed, or otherwise deprecated. Information should contain details about why there will be no fix issued.

H

I

L

M

N

O

P

Q

R

S

T

U

V

W