TEST DE LYNIS , logiciel d'audit système et réseau
sur une distrib Backbox 5 (ubuntu) desktop

```
root@backbox:~/Bureau/lynis# ./lynis

[ Lynis 2.7.1 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2019, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------


  Usage: lynis command [options]


  Command:

    audit
       audit system                : Perform local security scan
       audit system remote <host>  : Remote security scan
       audit dockerfile <file>     : Analyze Dockerfile

    show
       show                      : Show all commands
       show version                : Show Lynis version
       show help                 : Show help

    update
       update info               : Show update details


  Options:

    --no-log                    : Don't create a log file
    --pentest                   : Non-privileged scan (useful for pentest)
    --profile <profile>           : Scan the system with the given profile file
    --quick (-Q)                : Quick mode, don't wait for user input

    Layout options
    --no-colors                 : Don't use colors in output
    --quiet (-q)                : No output
    --reverse-colors              : Optimize color display for light backgrounds
```

```
  Misc options
  --debug                       : Debug logging to screen
  --view-manpage (--man)        : View man page
  --verbose                     : Show more details on screen
  --version (-V)                : Display version number and quit

  Enterprise options
  --plugindir <path>            : Define path of available plugins
  --upload                      : Upload data to central node

  More options available. Run './lynis show options', or use the man page.

 No command provided. Exiting..


root@backbox:~/Bureau/lynis# ./lynis audit system --quick

[ Lynis 2.7.1 ]

################################################################################
 Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
 welcome to redistribute it under the terms of the GNU General Public License.
 See the LICENSE file for details about using this software.

 2007-2019, CISOfy - https://cisofy.com/lynis/
 Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
 - Detecting OS...                                     [ DONE ]
 - Checking profiles...                                [ DONE ]
 - Detecting language and localization                 [ fr ]

 ---------------------------------------------------
 Program version:           2.7.1
 Operating system:          Linux
 Operating system name:     Ubuntu Linux
 Operating system version:  16.04
 Kernel version:            4.15.0
 Hardware platform:         i686
 Hostname:                  backbox
 ---------------------------------------------------
 Profiles:                  /etc/lynis/default.prf
 Log file:                  /var/log/lynis.log
 Report file:               /var/log/lynis-report.dat
 Report version:            1.0
 Plugin directory:          /etc/lynis/plugins
 ---------------------------------------------------
 Auditor:                   [Not Specified]
 Language:                  fr
```

```
  Test category:            all
  Test group:               all
  ------------------------------------------------
  - Program update status...                    [ NO UPDATE ]

[+] System Tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: les plugins ont des tests plus poussés et peuvent prendre plusieurs minutes

  - Plugin: debian
    [
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                          [ FOUND ]
    - Checking /sbin...                         [ FOUND ]
    - Checking /usr/bin...                      [ FOUND ]
    - Checking /usr/sbin...                     [ FOUND ]
    - Checking /usr/local/bin...                [ FOUND ]
    - Checking /usr/local/sbin...               [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):
      - libpam-tmpdir                           [ Not Installed ]
      - libpam-usb                              [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
    - Ecryptfs                                  [ NOT INSTALLED ]
  - Software:
    - apt-listbugs                              [ Not Installed ]
    - apt-listchanges                           [ Not Installed ]
    - checkrestart                              [ Not Installed ]
    - debsecan                                  [ Not Installed ]
    - debsums                                   [ Not Installed ]
    - fail2ban                                  [ Not Installed ]
]

[+] Boot and services
------------------------------------
  - Service Manager                             [ upstart ]
  - Checking UEFI boot                          [ DÉSACTIVÉ ]
  - Checking presence GRUB2                     [ TROUVÉ ]
    - Checking for password protection          [ ATTENTION ]
  - Check running services (systemctl)          [ FAIT ]
        Result: found 34 running services
  - Check enabled services at boot (systemctl)  [ FAIT ]
        Result: found 52 enabled services
  - Check startup files (permissions)           [ OK ]
```

[+] Kernel

- Checking default run level [RUNLEVEL 5]
- Checking kernel version and release [FAIT]
- Checking kernel type [FAIT]
- Checking loaded kernel modules [FAIT]
  Found 104 active modules
- Checking Linux kernel configuration file [TROUVÉ]
- Checking default I/O kernel scheduler [TROUVÉ]
- Checking for available kernel update [OK]
- Checking core dumps configuration [DÉSACTIVÉ]
  - Checking setuid core dumps configuration [DEFAULT]
- Check if reboot is needed [NON]

[+] Mémoire et Processus

- Checking /proc/meminfo [TROUVÉ]
- Searching for dead/zombie processes [OK]
- Searching for IO waiting processes [OK]

[+] Users, Groups and Authentication

- Administrator accounts [OK]
- Unique UIDs [OK]
- Consistency of group files (grpck) [OK]
- Unique group IDs [OK]
- Unique group names [OK]
- Password file consistency [OK]
- Query system users (non daemons) [FAIT]
- NIS+ authentication support [NOT ENABLED]
- NIS authentication support [NOT ENABLED]
- sudoers file [TROUVÉ]
  - Check sudoers file permissions [OK]
- PAM password strength tools [SUGGESTION]
- PAM configuration files (pam.conf) [TROUVÉ]
- PAM configuration files (pam.d) [TROUVÉ]
- PAM modules [TROUVÉ]
- LDAP module in PAM [NON TROUVÉ]
- Accounts without expire date [OK]
- Accounts without password [OK]
- Checking user password aging (minimum) [DÉSACTIVÉ]
- User password aging (maximum) [DÉSACTIVÉ]
- Checking expired passwords [OK]
- Checking Linux single user mode authentication [OK]
- Determining default umask
  - umask (/etc/profile) [NON TROUVÉ]
  - umask (/etc/login.defs) [SUGGESTION]
  - umask (/etc/init.d/rc) [SUGGESTION]
- LDAP authentication support [NOT ENABLED]
- Logging failed login attempts [ACTIVÉ]

[+] Shells

  - Checking shells from /etc/shells
    Result: found 4 shells (valid shells: 4).
    - Session timeout settings/tools [AUCUN]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc [AUCUN]
    - Checking default umask in /etc/profile [AUCUN]

[+] File systems

  - Checking mount points
    - Checking /home mount point [SUGGESTION]
    - Checking /tmp mount point [SUGGESTION]
    - Checking /var mount point [SUGGESTION]
  - Query swap partitions (fstab) [OK]
  - Testing swap partitions [OK]
  - Testing /proc mount (hidepid) [SUGGESTION]
  - Checking for old files in /tmp [OK]
  - Checking /tmp sticky bit [OK]
  - Checking /var/tmp sticky bit [OK]
  - ACL support root file system [ACTIVÉ]
  - Mount options of / [NON DEFAULT]
  - Checking Locate database [TROUVÉ]
  - Disable kernel support of some filesystems
    - Discovered kernel modules: cramfs freevxfs hfs hfsplus jffs2

[+] USB Devices

  - Checking usb-storage driver (modprobe config) [NOT DISABLED]
  - Checking USB devices authorization [ACTIVÉ]
  - Checking USBGuard [NON TROUVÉ]

[+] Storage

  - Checking firewire ohci driver (modprobe config) [DÉSACTIVÉ]

[+] NFS

  - Query rpc registered programs [FAIT]
  - Query NFS versions [FAIT]
  - Query NFS protocols [FAIT]
  - Check running NFS daemon [NON TROUVÉ]

[+] Name services

  - Searching DNS domain name [INCONNU]
  - Checking /etc/hosts
    - Checking /etc/hosts (duplicates) [OK]
    - Checking /etc/hosts (hostname) [OK]
    - Checking /etc/hosts (localhost) [OK]
    - Checking /etc/hosts (localhost to IP) [OK]

[+] Ports and packages

- Searching package managers
  - Searching dpkg package manager [TROUVÉ]
    - Querying package manager
  - Query unpurged packages [TROUVÉ]
- Checking security repository in sources.list file [OK]
- Checking APT package database [OK]

W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: http://deb.torproject.org/torproject.org xenial InRelease: The following signatures were invalid: KEYEXPIRED 1535644863 KEYEXPIRED 1535644863 KEYEXPIRED 1535644863 KEYEXPIRED 1535644863

W: Failed to fetch http://deb.torproject.org/torproject.org/dists/xenial/InRelease The following signatures were invalid: KEYEXPIRED 1535644863 KEYEXPIRED 1535644863 KEYEXPIRED 1535644863 KEYEXPIRED 1535644863

W: Some index files failed to download. They have been ignored, or old ones used instead.

- Checking vulnerable packages [ATTENTION]
- Checking upgradeable packages [IGNORÉ]
- Checking package audit tool [INSTALLED]
  Found: apt-get

[+] Networking

- Checking IPv6 configuration [ACTIVÉ]
  Configuration method [AUTO]
  IPv6 only [NO]
- Checking configured nameservers
  - Testing nameservers
    Nameserver: 127.0.0.1 [OK]
- Checking default gateway [FAIT]
- Getting listening ports (TCP/UDP) [FAIT]
  * Found 102 ports
- Checking promiscuous interfaces [OK]
- Checking waiting connections [OK]
- Checking status DHCP client [EN COURS:]
- Checking for ARP monitoring software [NON TROUVÉ]

[+] Printers and Spools

- Checking cups daemon [EN COURS:]
- Checking CUPS configuration file [OK]
  - File permissions [ATTENTION]
- Checking CUPS addresses/sockets [TROUVÉ]
- Checking lp daemon [NON LANCÉ]

[+] Software: e-mail and messaging

- Postfix status [EN COURS:]
  - Postfix configuration [TROUVÉ]
    - Postfix banner [ATTENTION]
- Dovecot status [EN COURS:]

[+] Software: firewalls

- Checking iptables kernel module [NON TROUVÉ]
- Checking host based firewall [NOT ACTIVE]

[+] Software: webserver

- Checking Apache (binary /usr/sbin/apache2) [TROUVÉ]
  Info: No virtual hosts found
  * Loadable modules [TROUVÉ (106)]
    - Found 106 loadable modules
      mod_evasive: anti-DoS/brute force [NON TROUVÉ]
      mod_reqtimeout/mod_qos [TROUVÉ]
      ModSecurity: web application firewall [NON TROUVÉ]
- Checking nginx [TROUVÉ]
  - Searching nginx configuration file [TROUVÉ]
    - Found nginx includes [2 FOUND]
  - Parsing configuration options
    - /etc/nginx/nginx.conf
    - /etc/nginx/sites-enabled/default
    - SSL configured [NON]
    - Checking log file configuration
      - Missing log files (access_log) [NON]
      - Disabled access logging [NON]
      - Missing log files (error_log) [NON]
      - Debugging mode on error_log [NON]

[+] SSH Support

- Checking running SSH daemon [TROUVÉ]
  - Searching SSH configuration [TROUVÉ]
  - SSH option: AllowTcpForwarding [SUGGESTION]
  - SSH option: ClientAliveCountMax [SUGGESTION]
  - SSH option: ClientAliveInterval [OK]
  - SSH option: Compression [SUGGESTION]
  - SSH option: FingerprintHash [OK]
  - SSH option: GatewayPorts [OK]
  - SSH option: IgnoreRhosts [OK]
  - SSH option: LoginGraceTime [OK]
  - SSH option: LogLevel [SUGGESTION]
  - SSH option: MaxAuthTries [SUGGESTION]
  - SSH option: MaxSessions [SUGGESTION]
  - SSH option: PermitRootLogin [OK]
  - SSH option: PermitUserEnvironment [OK]
  - SSH option: PermitTunnel [OK]
  - SSH option: Port [SUGGESTION]
  - SSH option: PrintLastLog [OK]
  - SSH option: StrictModes [OK]
  - SSH option: TCPKeepAlive [SUGGESTION]
  - SSH option: UseDNS [OK]
  - SSH option: VerifyReverseMapping [NON TROUVÉ]

- SSH option: X11Forwarding [SUGGESTION]
- SSH option: AllowAgentForwarding [SUGGESTION]
- SSH option: Protocol [OK]
- SSH option: UsePrivilegeSeparation [SUGGESTION]
- SSH option: AllowUsers [NON TROUVÉ]
- SSH option: AllowGroups [NON TROUVÉ]

[+] SNMP Support

- Checking running SNMP daemon [NON TROUVÉ]

[+] Databases

No database engines found

[+] LDAP Services

- Checking OpenLDAP instance [NON TROUVÉ]

[+] PHP

- Checking PHP [NON TROUVÉ]

[+] Squid Support

- Checking running Squid daemon [NON TROUVÉ]

[+] Logging and files

- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NON TROUVÉ]
- Checking systemd journal status [TROUVÉ]
- Checking Metalog status [NON TROUVÉ]
- Checking RSyslog status [TROUVÉ]
- Checking RFC 3195 daemon status [NON TROUVÉ]
- Checking minilogd instances [NON TROUVÉ]
- Checking logrotate presence [OK]
- Checking log directories (static list) [FAIT]
- Checking open log files [FAIT]
- Checking deleted files in use [FILES FOUND]

[+] Insecure services

- Checking inetd status [NOT ACTIVE]

[+] Banners and identification

- /etc/issue [TROUVÉ]
- /etc/issue contents [WEAK]
- /etc/issue.net [TROUVÉ]
- /etc/issue.net contents [WEAK]

[+] Scheduled tasks

- Checking crontab/cronjob [FAIT]

[+] Accounting

- Checking accounting information [NON TROUVÉ]
- Checking sysstat accounting data [NON TROUVÉ]
- Checking auditd [NON TROUVÉ]

[+] Time and Synchronization

- NTP daemon found: systemd (timesyncd) [TROUVÉ]
- Checking event based ntpdate (if-up) [TROUVÉ]
- Checking for a running NTP daemon or client [OK]

[+] Cryptography

- Checking for expired SSL certificates [0/0] [AUCUN]

[+] Virtualization

[+] Containers

[+] Security frameworks

- Checking presence AppArmor [TROUVÉ]
  - Checking AppArmor status [ACTIVÉ]
- Checking presence SELinux [NON TROUVÉ]
- Checking presence TOMOYO Linux [NON TROUVÉ]
- Checking presence grsecurity [NON TROUVÉ]
- Checking for implemented MAC framework [OK]

[+] Software: file integrity

- Checking file integrity tools
- Checking presence integrity tool [NON TROUVÉ]

[+] Software: System tooling

- Checking automation tooling
- Automation tooling [NON TROUVÉ]
- Checking for IDS/IPS tooling [AUCUN]

[+] Software: Malware

[+] File Permissions

- Starting file permissions check

[+] Home directories

  - Checking shell history files [OK]

[+] Kernel Hardening

  - Comparing sysctl key pairs with scan profile

[+] Hardening

    - Installed compiler(s) [TROUVÉ]
    - Installed malware scanner [NON TROUVÉ]

[+] Tests Personnalisés

  - Running custom tests... [NONE]

[+] Plugins (phase 2)

==

  -[Lynis 2.7.1 Results]-

  Warnings (3):

  ! One or more deprecated options used [LYNIS]
    - Details : show_tool_tips
    - Solution : Update your profile
      https://cisofy.com/lynis/controls/LYNIS/

  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/lynis/controls/PKGS-7392/

  ! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
      https://cisofy.com/lynis/controls/MAIL-8818/

  Suggestions (53):
  ----
  * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
      https://your-domain.example.org/controls/CUST-0280/

  * Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]
      https://your-domain.example.org/controls/CUST-0285/

  * Install 'ecryptfs-utils' and configure for each user. [CUST-0520]
      https://your-domain.example.org/controls/CUST-0520/

  * Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]
      https://your-domain.example.org/controls/CUST-0810/

* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]
https://your-domain.example.org/controls/CUST-0811/

* Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting. [CUST-0830]
https://your-domain.example.org/controls/CUST-0830/

* Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]
https://your-domain.example.org/controls/CUST-0870/

* Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]
https://your-domain.example.org/controls/CUST-0875/

* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
https://cisofy.com/lynis/controls/DEB-0880/

* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
https://cisofy.com/lynis/controls/BOOT-5122/

* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
https://cisofy.com/lynis/controls/AUTH-9262/

* Configure minimum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/lynis/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/lynis/controls/AUTH-9286/

* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
https://cisofy.com/lynis/controls/AUTH-9328/

* Default umask in /etc/init.d/rc could be more strict like 027 [AUTH-9328]
https://cisofy.com/lynis/controls/AUTH-9328/

* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
https://cisofy.com/lynis/controls/FILE-6310/

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]

https://cisofy.com/lynis/controls/STRG-1840/

* Check DNS configuration for the dns domain name [NAME-4028]
https://cisofy.com/lynis/controls/NAME-4028/

* Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]
https://cisofy.com/lynis/controls/PKGS-7346/

* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
https://cisofy.com/lynis/controls/PKGS-7370/

* Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]
https://cisofy.com/lynis/controls/PKGS-7392/

* Install package apt-show-versions for patch management purposes [PKGS-7394]
https://cisofy.com/lynis/controls/PKGS-7394/

* Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]
https://cisofy.com/lynis/controls/NETW-3032/

* Access to CUPS configuration could be more strict. [PRNT-2307]
https://cisofy.com/lynis/controls/PRNT-2307/

* You are advised to hide the mail_name (option: smtpd_banner) from your postfix configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf) [MAIL-8818]
https://cisofy.com/lynis/controls/MAIL-8818/

* Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
- Details : disable_vrfy_command=no
- Solution : run postconf -e disable_vrfy_command=yes to change the value
https://cisofy.com/lynis/controls/MAIL-8820/

* Configure a firewall/packet filter to filter incoming and outgoing traffic [FIRE-4590]
https://cisofy.com/lynis/controls/FIRE-4590/

* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
https://cisofy.com/lynis/controls/HTTP-6640/

* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
https://cisofy.com/lynis/controls/HTTP-6643/

* Add HTTPS to nginx virtual hosts for enhanced protection of sensitive data and privacy [HTTP-6710]
https://cisofy.com/lynis/controls/HTTP-6710/

* Consider hardening SSH configuration [SSH-7408]
- Details : AllowTcpForwarding (YES --> NO)
https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]

- Details : ClientAliveCountMax (3 --> 2)
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
 - Details : Compression (YES --> NO)
   https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
 - Details : LogLevel (INFO --> VERBOSE)
   https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
 - Details : MaxAuthTries (6 --> 2)
   https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
 - Details : MaxSessions (10 --> 2)
   https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
 - Details : Port (22 -->)
   https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
 - Details : TCPKeepAlive (YES --> NO)
   https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
 - Details : X11Forwarding (YES --> NO)
   https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
 - Details : AllowAgentForwarding (YES --> NO)
   https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
 - Details : UsePrivilegeSeparation (YES --> SANDBOX)
   https://cisofy.com/lynis/controls/SSH-7408/

* Check what deleted files are still in use and why. [LOGG-2190]
   https://cisofy.com/lynis/controls/LOGG-2190/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
   https://cisofy.com/lynis/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
   https://cisofy.com/lynis/controls/BANN-7130/

* Enable process accounting [ACCT-9622]
   https://cisofy.com/lynis/controls/ACCT-9622/

* Enable sysstat to collect accounting (no results) [ACCT-9626]

https://cisofy.com/lynis/controls/ACCT-9626/

* Enable auditd to collect audit information [ACCT-9628]
https://cisofy.com/lynis/controls/ACCT-9628/

* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
https://cisofy.com/lynis/controls/FINT-4350/

* Determine if automation tools are present for system management [TOOL-5002]
https://cisofy.com/lynis/controls/TOOL-5002/

* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/lynis/controls/HRDN-7222/

* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
- Solution : Install a tool like rkhunter, chkrootkit, OSSEC
https://cisofy.com/lynis/controls/HRDN-7230/

Follow-up:

- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

==========

Lynis security scan details:

Hardening index : 52 [##########   ]
Tests performed : 237
Plugins enabled : 1

Components:
- Firewall   [X]
- Malware scanner   [X]

Lynis Modules:
- Compliance Status   [?]
- Security Audit   [V]
- Vulnerability Scan   [V]

Files:
- Test and debug information   : /var/log/lynis.log
- Report data   : /var/log/lynis-report.dat

==========

Lynis 2.7.1

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2019, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

==

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

root@backbox:~/Bureau/lynis#