lynis

lynis est un outil de vérification de sécurité open source.   
Il est principalement utilisé par les administrateurs système, les professionnels de la sécurité et les auditeurs, pour évaluer les défenses de sécurité de leurs systèmes Linux et Unix.   
Puisque lynis tourne sur l'hôte lui-même, il effectue des analyses de sécurité plus étendues que les balayeurs (*scanners*) de vulnérabilité.

Fonctionnement

lynis effectue des centaines de tests individuels.   
Chacun de ces tests aide à déterminer l'état de sécurité du système.

Étapes …

* Déterminer le système d'exploitation ;
* Rechercher des outils et des utilitaires disponibles ;
* Vérifier la mise à jour de lynis ;
* Exécuter des tests à partir de greffons (*plugins*) activés ;
* Exécuter des tests de sécurité par catégorie ;
* Signaler l'état de l'analyse de sécurité ;

Outre les données affichées à l'écran, tous les détails techniques sur la numérisation se retrouvent dans un fichier journal.   
Les résultats (avertissements, suggestions, collecte de données) se retrouvent dans un fichier de rapport.

**Numérisation opportuniste**

Le balayage lynis (*scanning*) est dit opportuniste.   
Cela signifie qu'il n'utilise que ce qu'il peut trouver. Aucune installation d'autres outils n’est nécessaire.

Par exemple, s'il voit que le système exécute Apache, il effectuera une première série de tests liés à Apache.   
Lors de l'analyse d'Apache, lorsqu’il découvre également une configuration SSL/TLS, il effectuera des étapes d'audit supplémentaires à ce sujet.   
Il recueillera ensuite ces certificats découverts afin qu'ils puissent être aussi vérifiés.

**Balayages de sécurité approfondis**

En effectuant une analyse opportuniste, lynis peut fonctionner avec peu de dépendances. Plus il trouve, plus la vérification sera approfondie. En d'autres termes, lynis effectuera toujours des analyses personnalisées sur chaque système.

**Greffons (*plugins*) lynis**

Les greffons (*plug-ins*) permettent à lyris d'effectuer des tests supplémentaires.   
Ils peuvent être considérés comme une extension (ou complément) à lynis, améliorant ainsi ses fonctionnalités.   
Un exemple est le greffon de vérification de la conformité. Il effectue des tests spécifiques liés à une ou plusieurs normes.

Installation de lyris  
La façon la plus rapide d'isstaller lynis est de le récupérer à partir des dépôts officiels ...  
**>> sudo apt update && sudo apt update -y  
>> sudo apt install apt-transport-https ca-certificates host  
>> sudo echo "deb https://packages.cisofy.com/community/lynis/deb/ stable main" | \  
 sudo tee /etc/apt/sources.list.d/cisofy-lynis.list  
>> sudo apt update  
>> sudo apt install lynis host**

Pour vérifier la version de lyris …  
**>>** **sudo lynis show version  
3.0.2**

Mise à jour des signatures …  
**>>** **sudo lynis update info** **== Lynis ==  
 Version: 3.0.2  
 Status: Outdated  
 Installed version: 302  
 Latest version: 308  
 Release date: 2020-12-24  
 Project page: https://cisofy.com/lynis/  
 Source code: https://github.com/CISOfy/lynis  
 Latest package: https://packages.cisofy.com/  
2007-2020, CISOfy - https://cisofy.com/lynis/**

Démarrage d’une vérification du système …  
**>>** **sudo lynis audit system**

Pour de l’aide …  
**>>** **lynis --help**

**lynis et les pauses**  
Par défaut, Lynis démarre et fait une pause après la première section.

* Avec CTRL + C, Il est possible d'arrêter le programme ;
* Avec la touche RETOUR (ENTER), il continuera à la prochaine série de tests.

Si on souhaite exécuter Lynis sans pause, il est possible de lui donner le paramètre supplémentaire --quick.

Pour effectuer une analyse rapide ...  
**>>** **lynis audit system --quick**

Liste des paramètres vérifiés …

[+] Initializing program

[+] System Tools

[+] Plugins (phase 1)

[+] Boot and services

[+] Kernel

[+] Mémoire et Processus  
[+] Users, Groups and Authentication  
[+] Insecure services  
[+] Banners and identification  
[+] Scheduled tasks  
[+] Accounting  
[+] Time and Synchronization  
[+] Cryptography  
[+] Virtualization  
[+] Containers  
[+] Security frameworks  
[+] Software: file integrity  
[+] Software: System tooling  
[+] Software: Malware  
[+] File Permissions  
[+] Home directories  
[+] Kernel Hardening  
[+] Hardening  
[+] Tests Personnalisés  
[+] Plugins (phase 2

Sortie d’une analyse stardard

Voici la liste des principaux points à vérifier.  
Ce rapport est une vue rapide.

**Remarque** …  
Il est aussi possible, suite à un audit, de consulter, à l’aide de la commande less, le fichier /var/log/lynis-report.dat.

Pour un exemple de résultat complet voir la sortie (version longue en annexe).

|  |
| --- |
|  |
| [ Lynis 2.5.5 ]  ##############################################################################  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.  2007-2017, 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: 2.5.5  Operating system: Linux  Operating system name: Debian  Operating system version: 9.1  Kernel version: 4.9.33  Hardware platform: x86\_64  Hostname: ns532043  ---------------------------------------------------  Profiles: /etc/lynis/default.prf  Log file: /var/log/lynis.log  Report file: /var/log/lynis-report.dat  Report version: 1.0  Plugin directory: /usr/share/lynis/plugins  ---------------------------------------------------  Auditor: Not Specified]  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  - Plugins actives **[ NONE ]** |
|  |
| **[+] Boot and services**  ------------------------------------  - Service Manager **[ systemd ]**  - Checking UEFI boot **[ DÉSACTIVÉ ]**  - Checking presence GRUB2 **[ TROUVÉ ]**  - Checking for password protection **[ ATTENTION ]**  - Check running services (systemctl) **[ FAIT ]**  Result: found 16 running services  - Check enabled services at boot (systemctl) **[ FAIT ]**  Result: found 20 enabled services  - Check startup files (permissions) **[ OK ]** |
|  |
| [+] Kernel  ------------------------------------  - Checking default run level **[ RUNLEVEL 5 ]**  - Checking CPU support (NX/PAE)  CPU support: PAE and/or NoeXecute supported **[ TROUVÉ ]**  - Checking kernel version and release **[ FAIT ]**  - Checking kernel type **[ FAIT ]**  - Checking loaded kernel modules **[ FAIT ]**  - Checking Linux kernel configuration file **[ TROUVÉ ]**  - Checking for available kernel update **[ INCONNU ]**  - Checking core dumps configuration **[ DÉSACTIVÉ ]**  - Checking setuid core dumps configuration **[ DEFAULT ]**  - Check if reboot is needed **[ INCONNU ]** |
| [+] 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  **[ NON TROUVÉ ]**  - 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 ]**  - LDAP authentication support **[ NOT ENABLED ]**  - Logging failed login attempts **[ ACTIVÉ ]** |
|  |
| [+] Shells  ------------------------------------  - Checking shells from /etc/shells  Result: found 5 shells (valid shells: 5).  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 **[ OK ]**  - 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 ]**  - ACL support root file system **[ ACTIVÉ ]**  **- Mount options of / [ NON DEFAULT ]**  - Mount options of /boot  **[ NON DEFAULT ]**  - Mount options of /dev/shm **[ NON DEFAULT ]**  - Mount options of /home **[ NON DEFAULT ]**  - Checking Locate database **[ TROUVÉ ]**  - Disable kernel support of some filesystems |
| … |
| [+] NFS  ------------------------------------  - Check running NFS daemon **[ NON TROUVÉ ]** |
| [+] Name services  ------------------------------------  - Checking search domains **[ TROUVÉ ]**  - Searching DNS domain name  **[ TROUVÉ ]**  Domain name: ip-198-245-62.net  - Checking BIND status **[ TROUVÉ ]**  - Checking BIND configuration file **[ TROUVÉ ]**  - Checking BIND configuration consistency **[ OK ]**  - Checking BIND version in banner **[ ATTENTION ]**  - 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 **[ AUCUN ]**  - Checking security repository in sources.list file **[ OK ]**  W: The repository 'http://ppa.launchpad.net/wireguard/wireguard/ubuntu artful Release' does not have a Release file.  E: Failed to fetch http://ppa.launchpad.net/wireguard/wireguard/ubuntu/dists/artful/main/binary-amd64/Packages 404 Not Found  E: Some index files failed to download. They have been ignored, or old ones used instead.  - Checking vulnerable packages (apt-get only)  **[ ATTENTION ]**  - 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 ]**  Nameserver: 213.186.33.99 **[ OK ]**  - Checking default gateway **[ FAIT ]**  - Getting listening ports (TCP/UDP) **[ FAIT ]**  \* Found 12 ports  - Checking promiscuous interfaces  **[ OK ]**  - Checking waiting connections  **[ OK ]**  - Checking status DHCP client **[ NOT ACTIVE ]**  - Checking for ARP monitoring software **[ NON TROUVÉ ]** |
| … |
| … |
| [+] Software: firewalls  ------------------------------------  - Checking iptables support **[ TROUVÉ ]**  - Checking iptables policies of chains **[ TROUVÉ ]**  - Checking chain INPUT (table: nfilter, policy **[ other ]**  - Checking for empty ruleset  **[ OK ]**  - Checking for unused rules **[ TROUVÉ ]**  - Checking host based firewall  **[ ACTIVE ]** |
| … |
| [+] 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: Protocol **[ NON TROUVÉ ]**  - 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: AllowUsers **[ NON TROUVÉ ]**  - SSH option: AllowGroups **[ 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 **[ IGNORÉ ]** |
| … |
| [+] 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 ]**  … |
| [+] Cryptography  ------------------------------------  - Checking for expired SSL certificates [0/7] **[ AUCUN ]**  … |
| [+] Containers  ------------------------------------  - Docker  Docker daemon **[ EN COURS: ]**  Docker info output (warnings) **[ 2 ]**  Containers  - Total containers [ 4 ]  Running containers **[ 2 ]**  Unused containers **[ 2 ]**  - File permissions **[ OK ]**  … |
| [+] Software: file integrity  ------------------------------------  - Checking file integrity tools  - Checking presence integrity tool **[ NON TROUVÉ ]**  … |
| [+] File Permissions  ------------------------------------  - Starting file permissions check  /root/.ssh **[ OK ]** |
| … |
| [+] Kernel Hardening  ------------------------------------  - Comparing sysctl key pairs with scan profile  - fs.protected\_hardlinks (exp: 1) **[ DIFFERENT ]**  - fs.protected\_symlinks (exp: 1) **[ DIFFERENT ]**  - fs.suid\_dumpable (exp: 0) **[ OK ]**  - kernel.core\_uses\_pid (exp: 1) **[ DIFFERENT ]**  kernel.ctrl-alt-del (exp: 0) **[ OK ]**  - kernel.dmesg\_restrict (exp: 1)  **[ DIFFERENT ]**  - kernel.kptr\_restrict (exp: 2) **[ DIFFERENT ]**  - kernel.randomize\_va\_space (exp: 2)  **[ DIFFERENT ]**  - kernel.sysrq (exp: 0)  **[ DIFFERENT ]**  - net.ipv4.conf.all.accept\_redirects (exp: 0) **[ OK ]**  - net.ipv4.conf.all.accept\_source\_route (exp: 0) **[ OK ]**  - net.ipv4.conf.all.bootp\_relay (exp: 0)  **[ OK ]**  - net.ipv4.conf.all.forwarding (exp: 0) **[ DIFFERENT ]**  - net.ipv4.conf.all.log\_martians (exp: 1) **[ DIFFERENT ]**  - net.ipv4.conf.all.mc\_forwarding (exp: 0) **[ OK ]**  - net.ipv4.conf.all.proxy\_arp (exp: 0) **[ OK ]**  - net.ipv4.conf.all.rp\_filter (exp: 1) **[ DIFFERENT ]**  - net.ipv4.conf.all.send\_redirects (exp: 0) **[ DIFFERENT ]**  - net.ipv4.conf.default.accept\_redirects (exp: 0) **[ DIFFERENT ]**  - net.ipv4.conf.default.accept\_source\_route (exp: 0) **[ DIFFERENT ]**  - net.ipv4.conf.default.log\_martians (exp: 1) [ **DIFFERENT ]**  - net.ipv4.icmp\_echo\_ignore\_broadcasts (exp: 1) **[ OK ]**  - net.ipv4.icmp\_ignore\_bogus\_error\_responses (exp: 1)**[ OK ]**  - net.ipv4.tcp\_syncookies (exp: 1) **[ OK ]**  - net.ipv4.tcp\_timestamps (exp: 0) **[ DIFFERENT ]**  - net.ipv6.conf.all.accept\_redirects (exp: 0) **[ DIFFERENT ]**  - net.ipv6.conf.all.accept\_source\_route (exp: 0) **[ OK ]**  - net.ipv6.conf.default.accept\_redirects (exp: 0) **[ DIFFERENT ]**  - net.ipv6.conf.default.accept\_source\_route (exp: 0) **[ OK ]** |
| … |
| [+] Tests Personnalisés  ------------------------------------  - Running custom tests… **[ NONE ]** |
| [+] Plugins (phase 2)  ------------------------------------  ============================================================================  -[ Lynis 2.5.5 Results ]- |
| **Warnings (1):**  ----------------------------  ! Found BIND version in banner [NAME-4210]  https://cisofy.com/controls/NAME-4210/ |
| **Suggestions (38):**  ----------------------------  \* 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/controls/BOOT-5122/  …  \* The version in BIND can be masked by defining 'version none' in the configuration file [NAME-4210]  https://cisofy.com/controls/NAME-4210/  \* Install debsums utility for the verification of packages with known good database. [PKGS-7370]  https://cisofy.com/controls/PKGS-7370/  …  \* Check iptables rules to see which rules are currently not used [FIRE-4513]  https://cisofy.com/controls/FIRE-4513/  …  \* Consider hardening SSH configuration [SSH-7408]  - Details : AllowTcpForwarding (YES --> NO)  https://cisofy.com/controls/SSH-7408/  \* Consider hardening SSH configuration [SSH-7408]  - Details : ClientAliveCountMax (3 --> 2)  https://cisofy.com/controls/SSH-7408/  …  \* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]  https://cisofy.com/controls/BANN-7130/  …  \* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]  https://cisofy.com/controls/FINT-4350/  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 : 66 [############# ]  Tests performed : 213  Plugins enabled : 0  Components:  - Firewall [**V**]  - 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  ============================================================================  Exceptions trouvées  Des événements ou informations exceptionnels ont été trouvés!  Que faire:  Vous pouvez aider en envoyant votre fichier journal (/var/log/lynis.log).  Go to https://cisofy.com/contact/ and send your file to the e-mail address listed  ============================================================================  … |

Annexe  
Fichier de sortie complet

|  |
| --- |
|  |
| [ Lynis 2.5.5 ]  ##############################################################################  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.  2007-2017, 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: 2.5.5  Operating system: Linux  Operating system name: Debian  Operating system version: 9.1  Kernel version: 4.9.33  Hardware platform: x86\_64  Hostname: ns532043  ---------------------------------------------------  Profiles: /etc/lynis/default.prf  Log file: /var/log/lynis.log  Report file: /var/log/lynis-report.dat  Report version: 1.0  Plugin directory: /usr/share/lynis/plugins  ---------------------------------------------------  Auditor: Not Specified]  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  - Plugins actives **[ NONE ]** |
|  |
| **[+] Boot and services**  ------------------------------------  - Service Manager **[ systemd ]**  - Checking UEFI boot **[ DÉSACTIVÉ ]**  - Checking presence GRUB2 **[ TROUVÉ ]**  - Checking for password protection **[ ATTENTION ]**  - Check running services (systemctl) **[ FAIT ]**  Result: found 16 running services  - Check enabled services at boot (systemctl) **[ FAIT ]**  Result: found 20 enabled services  - Check startup files (permissions) **[ OK ]** |
|  |
| [+] Kernel  ------------------------------------  - Checking default run level **[ RUNLEVEL 5 ]**  - Checking CPU support (NX/PAE)  CPU support: PAE and/or NoeXecute supported **[ TROUVÉ ]**  - Checking kernel version and release **[ FAIT ]**  - Checking kernel type **[ FAIT ]**  - Checking loaded kernel modules **[ FAIT ]**  - Checking Linux kernel configuration file **[ TROUVÉ ]**  - Checking for available kernel update **[ INCONNU ]**  - Checking core dumps configuration **[ DÉSACTIVÉ ]**  - Checking setuid core dumps configuration **[ DEFAULT ]**  - Check if reboot is needed **[ INCONNU ]** |
| [+] 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  **[ NON TROUVÉ ]**  - 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 ]**  - LDAP authentication support **[ NOT ENABLED ]**  - Logging failed login attempts **[ ACTIVÉ ]** |
|  |
| [+] Shells  ------------------------------------  - Checking shells from /etc/shells  Result: found 5 shells (valid shells: 5).  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 **[ OK ]**  - 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 ]**  - ACL support root file system **[ ACTIVÉ ]**  **- Mount options of / [ NON DEFAULT ]**  - Mount options of /boot  **[ NON DEFAULT ]**  - Mount options of /dev/shm **[ NON DEFAULT ]**  - Mount options of /home **[ NON DEFAULT ]**  - Checking Locate database **[ TROUVÉ ]**  - Disable kernel support of some filesystems |
| [+] Storage  ------------------------------------  - Checking usb-storage driver (modprobe config) **[ NOT DISABLED ]**  - Checking USB devices authorization **[ ACTIVÉ ]**  - Checking firewire ohci driver (modprobe config) **[ NOT DISABLED ]** |
| [+] NFS  ------------------------------------  - Check running NFS daemon **[ NON TROUVÉ ]** |
| [+] Name services  ------------------------------------  - Checking search domains **[ TROUVÉ ]**  - Searching DNS domain name  **[ TROUVÉ ]**  Domain name: ip-198-245-62.net  - Checking BIND status **[ TROUVÉ ]**  - Checking BIND configuration file **[ TROUVÉ ]**  - Checking BIND configuration consistency **[ OK ]**  - Checking BIND version in banner **[ ATTENTION ]**  - 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 **[ AUCUN ]**  - Checking security repository in sources.list file **[ OK ]**  W: The repository 'http://ppa.launchpad.net/wireguard/wireguard/ubuntu artful Release' does not have a Release file.  E: Failed to fetch http://ppa.launchpad.net/wireguard/wireguard/ubuntu/dists/artful/main/binary-amd64/Packages 404 Not Found  E: Some index files failed to download. They have been ignored, or old ones used instead.  - Checking vulnerable packages (apt-get only)  **[ ATTENTION ]**  - 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 ]**  Nameserver: 213.186.33.99 **[ OK ]**  - Checking default gateway **[ FAIT ]**  - Getting listening ports (TCP/UDP) **[ FAIT ]**  \* Found 12 ports  - Checking promiscuous interfaces  **[ OK ]**  - Checking waiting connections  **[ OK ]**  - Checking status DHCP client **[ NOT ACTIVE ]**  - Checking for ARP monitoring software **[ NON TROUVÉ ]** |
| [+] Printers and Spools  ------------------------------------  - Checking cups daemon **[ NON TROUVÉ ]**  - Checking lp daemon **[ NON LANCÉ ]** |
| [+] Software: e-mail and messaging |
| [+] Software: firewalls  ------------------------------------  - Checking iptables support **[ TROUVÉ ]**  - Checking iptables policies of chains **[ TROUVÉ ]**  - Checking chain INPUT (table: nfilter, policy **[ other ]**  - Checking for empty ruleset  **[ OK ]**  - Checking for unused rules **[ TROUVÉ ]**  - Checking host based firewall  **[ ACTIVE ]** |
| [+] Software: webserver  ------------------------------------  - Checking Apache (binary /usr/sbin/apache2) **[ TROUVÉ ]**  Info: Found 2 virtual hosts  \* Loadable modules **[ TROUVÉ (114) ]**  - Found 114 loadable modules  mod\_evasive: anti-DoS/brute force **[ NON TROUVÉ ]**  mod\_reqtimeout/mod\_qos  **[ TROUVÉ ]**  ModSecurity: web application firewall  **[ NON TROUVÉ ]**  - Checking nginx **[ NON TROUVÉ ]** |
| [+] 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: Protocol **[ NON TROUVÉ ]**  - 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: 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 **[ IGNORÉ ]** |
| [+] 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 [0/7] **[ AUCUN ]** |
| [+] Virtualization  ------------------------------------ |
| [+] Containers  ------------------------------------  - Docker  Docker daemon **[ EN COURS: ]**  Docker info output (warnings) **[ 2 ]**  Containers  - Total containers [ 4 ]  Running containers **[ 2 ]**  Unused containers **[ 2 ]**  - File permissions **[ OK ]** |
| [+] Security frameworks  ------------------------------------  - Checking presence AppArmor **[ NON TROUVÉ ]**  - Checking presence SELinux **[ NON TROUVÉ ]**  - Checking presence grsecurity **[ NON TROUVÉ ]**  - Checking for implemented MAC framework **[ AUCUN ]** |
| [+] Software: file integrity  ------------------------------------  - Checking file integrity tools  - Checking presence integrity tool **[ NON TROUVÉ ]** |
| [+] Software: System tooling  ------------------------------------  - Checking automation tooling  - Automation tooling **[ NON TROUVÉ ]**  - Checking presence of Fail2ban **[ TROUVÉ ]**  - Checking Fail2ban jails **[ ACTIVÉ ]**  - Checking for IDS/IPS tooling **[ TROUVÉ ]** |
| [+] Software: Malware  ------------------------------------ |
| [+] File Permissions  ------------------------------------  - Starting file permissions check  /root/.ssh **[ OK ]** |
| [+] Home directories  ------------------------------------  - Checking shell history files **[ OK ]** |
| [+] Kernel Hardening  ------------------------------------  - Comparing sysctl key pairs with scan profile  - fs.protected\_hardlinks (exp: 1) **[ DIFFERENT ]**  - fs.protected\_symlinks (exp: 1) **[ DIFFERENT ]**  - fs.suid\_dumpable (exp: 0) **[ OK ]**  - kernel.core\_uses\_pid (exp: 1) **[ DIFFERENT ]**  kernel.ctrl-alt-del (exp: 0) **[ OK ]**  - kernel.dmesg\_restrict (exp: 1)  **[ DIFFERENT ]**  - kernel.kptr\_restrict (exp: 2) **[ DIFFERENT ]**  - kernel.randomize\_va\_space (exp: 2)  **[ DIFFERENT ]**  - kernel.sysrq (exp: 0)  **[ DIFFERENT ]**  - net.ipv4.conf.all.accept\_redirects (exp: 0) **[ OK ]**  - net.ipv4.conf.all.accept\_source\_route (exp: 0) **[ OK ]**  - net.ipv4.conf.all.bootp\_relay (exp: 0)  **[ OK ]**  - net.ipv4.conf.all.forwarding (exp: 0) **[ DIFFERENT ]**  - net.ipv4.conf.all.log\_martians (exp: 1) **[ DIFFERENT ]**  - net.ipv4.conf.all.mc\_forwarding (exp: 0) **[ OK ]**  - net.ipv4.conf.all.proxy\_arp (exp: 0) **[ OK ]**  - net.ipv4.conf.all.rp\_filter (exp: 1) **[ DIFFERENT ]**  - net.ipv4.conf.all.send\_redirects (exp: 0) **[ DIFFERENT ]**  - net.ipv4.conf.default.accept\_redirects (exp: 0) **[ DIFFERENT ]**  - net.ipv4.conf.default.accept\_source\_route (exp: 0) **[ DIFFERENT ]**  - net.ipv4.conf.default.log\_martians (exp: 1) [ **DIFFERENT ]**  - net.ipv4.icmp\_echo\_ignore\_broadcasts (exp: 1) **[ OK ]**  - net.ipv4.icmp\_ignore\_bogus\_error\_responses (exp: 1)**[ OK ]**  - net.ipv4.tcp\_syncookies (exp: 1) **[ OK ]**  - net.ipv4.tcp\_timestamps (exp: 0) **[ DIFFERENT ]**  - net.ipv6.conf.all.accept\_redirects (exp: 0) **[ DIFFERENT ]**  - net.ipv6.conf.all.accept\_source\_route (exp: 0) **[ OK ]**  - net.ipv6.conf.default.accept\_redirects (exp: 0) **[ DIFFERENT ]**  - net.ipv6.conf.default.accept\_source\_route (exp: 0) **[ OK ]** |
| [+] Hardening  ------------------------------------  - Installed compiler(s) [ **TROUVÉ ]**  - Installed malware scanner **[ NON TROUVÉ ]** |
| [+] Tests Personnalisés  ------------------------------------  - Running custom tests… **[ NONE ]** |
| [+] Plugins (phase 2)  ------------------------------------  ============================================================================  -[ Lynis 2.5.5 Results ]- |
| **Warnings (1):**  ----------------------------  ! Found BIND version in banner [NAME-4210]  https://cisofy.com/controls/NAME-4210/ |
| **Suggestions (38):**  ----------------------------  \* 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/controls/BOOT-5122/  \* Determine why /vmlinuz is missing on this Debian/Ubuntu system. [KRNL-5788]  Details : /vmlinuz  https://cisofy.com/controls/KRNL-5788/  \* Check the output of apt-cache policy manually to determine why output is empty [KRNL-5788]  https://cisofy.com/controls/KRNL-5788/  \* Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc [AUTH-9262]  https://cisofy.com/controls/AUTH-9262/  \* Configure minimum password age in /etc/login.defs [AUTH-9286]  https://cisofy.com/controls/AUTH-9286/  \* Configure maximum password age in /etc/login.defs [AUTH-9286]  https://cisofy.com/controls/AUTH-9286/  \* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]  https://cisofy.com/controls/AUTH-9328/  \* To decrease the impact of a full /tmp file system, place /tmp on a separated partition [FILE-6310]  https://cisofy.com/controls/FILE-6310/  \* To decrease the impact of a full /var file system, place /var on a separated partition [FILE-6310]  https://cisofy.com/controls/FILE-6310/  \* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]  https://cisofy.com/controls/STRG-1840/  \* Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]  https://cisofy.com/controls/STRG-1846/  \* The version in BIND can be masked by defining 'version none' in the configuration file [NAME-4210]  https://cisofy.com/controls/NAME-4210/  \* Install debsums utility for the verification of packages with known good database. [PKGS-7370]  https://cisofy.com/controls/PKGS-7370/  \* Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]  https://cisofy.com/controls/NETW-3032/  \* Check iptables rules to see which rules are currently not used [FIRE-4513]  https://cisofy.com/controls/FIRE-4513/  \* Install Apache mod\_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]  https://cisofy.com/controls/HTTP-6640/  \* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]  https://cisofy.com/controls/HTTP-6643/  \* Consider hardening SSH configuration [SSH-7408]  - Details : AllowTcpForwarding (YES --> NO)  https://cisofy.com/controls/SSH-7408/  \* Consider hardening SSH configuration [SSH-7408]  - Details : ClientAliveCountMax (3 --> 2)  https://cisofy.com/controls/SSH-7408/  \* Consider hardening SSH configuration [SSH-7408]  - Details : Compression (YES --> NO)  https://cisofy.com/controls/SSH-7408/  \* Consider hardening SSH configuration [SSH-7408]  - Details : LogLevel (INFO --> VERBOSE)  https://cisofy.com/controls/SSH-7408/  \* Consider hardening SSH configuration [SSH-7408]  - Details : MaxAuthTries (6 --> 2)  https://cisofy.com/controls/SSH-7408/  \* Consider hardening SSH configuration [SSH-7408]  - Details : MaxSessions (10 --> 2)  https://cisofy.com/controls/SSH-7408/  \* Consider hardening SSH configuration [SSH-7408]  - Details : Port (22 --> )  https://cisofy.com/controls/SSH-7408/  \* Consider hardening SSH configuration [SSH-7408]  - Details : TCPKeepAlive (YES --> NO)  https://cisofy.com/controls/SSH-7408/  \* Consider hardening SSH configuration [SSH-7408]  - Details : X11Forwarding (YES --> NO)  https://cisofy.com/controls/SSH-7408/  \* Consider hardening SSH configuration [SSH-7408]  - Details : AllowAgentForwarding (YES --> NO)  https://cisofy.com/controls/SSH-7408/  \* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]  https://cisofy.com/controls/BANN-7126/  \* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]  https://cisofy.com/controls/BANN-7130/  \* Enable process accounting [ACCT-9622]  https://cisofy.com/controls/ACCT-9622/  \* Enable sysstat to collect accounting (no results) [ACCT-9626]  https://cisofy.com/controls/ACCT-9626/  \* Enable auditd to collect audit information [ACCT-9628]  https://cisofy.com/controls/ACCT-9628/  \* Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]  https://cisofy.com/controls/CONT-8104/  \* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]  https://cisofy.com/controls/FINT-4350/  \* Determine if automation tools are present for system management [TOOL-5002]  https://cisofy.com/controls/TOOL-5002/  \* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]  https://cisofy.com/controls/KRNL-6000/  \* Harden compilers like restricting access to root user only [HRDN-7222]  https://cisofy.com/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/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 : 66 [############# ]  Tests performed : 213  Plugins enabled : 0  Components:  - Firewall [**V**]  - 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  ============================================================================  Exceptions trouvées  Des événements ou informations exceptionnels ont été trouvés!  Que faire:  Vous pouvez aider en envoyant votre fichier journal (/var/log/lynis.log).  Go to https://cisofy.com/contact/ and send your file to the e-mail address listed  ============================================================================  Lynis 2.5.5  Auditing, system hardening, and compliance for UNIX-based systems  (Linux, macOS, BSD, and others)  2007-2017, 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) |