



Hardening con Lynis

27/11/23

—

Jose Almirón Lopez

Índice

¿Qué es Lynis?	2
Instalación de Lynis	2
Funcionamiento básico	3
Advertencia (Warning)	4
Sugerencia (Suggestion)	5
Peligro (Danger)	6

¿Qué es Lynis?

Se trata de una herramienta de auditoría diseñada para sistemas Unix y otros paquetes de software, como servidores de bases de datos, demonios de tiempo y servidores web. Su propósito principal es facilitar la automatización de auditorías, la gestión de parches de seguridad, así como la detección de vulnerabilidades y malware.

Esta herramienta está diseñada para ser utilizada por especialistas en seguridad, penetration testers, auditores de sistemas y gestores de sistemas/redes. Es de código abierto, posibilita un escaneo exhaustivo, y destaca por su rapidez y facilidad de uso. Esto permite a los usuarios identificar y mejorar de manera eficiente los aspectos de fortalecimiento del sistema.

Algunos ejemplos de pruebas de auditoría que lleva a cabo incluyen:

- Métodos de autenticación disponibles.
- Certificados SSL que han expirado.
- Software desactualizado.
- Cuentas de usuario sin clave.
- Permisos de archivos incorrectos.
- Auditoría de cortafuegos.

Instalación de Lynis

Podemos instalarlo desde los repositorios de nuestra distribución o descargar las fuentes de la última versión desde su página oficial. En mi caso, optaré por la instalación a través de los repositorios utilizando el comando '***sudo apt install lynis***'.

```
jose@jose-almiron:~$ sudo apt install lynis
[sudo] contraseña para jose:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  linux-headers-6.2.0-26-generic linux-hwe-6.2-headers-6.2.0-26 linux-image-6.2.0-26-generic
  linux-modules-6.2.0-26-generic linux-modules-extra-6.2.0-26-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  menu
Paquetes sugeridos:
  apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu | kde-runtime | ktsuss
Se instalarán los siguientes paquetes NUEVOS:
  lynis menu
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 581 kB de archivos.
Se utilizarán 3.164 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Funcionamiento básico

Después de su instalación, podemos realizar un análisis exhaustivo del sistema ejecutando el comando `'sudo lynis audit system'`. Este comando realizará una auditoría, proporcionando informes sobre diversos niveles de endurecimiento de seguridad.

```
jose@jose-almiron:~$ sudo lynis audit system
[sudo] contraseña para jose:

[ Lynis 3.0.7 ]

#####
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.

2007-2021, 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 [ es ]

-----
Program version: 3.0.7
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 22.04
Kernel version: 6.2.0
Hardware platform: x86_64
Hostname: jose-almiron
-----
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: es
Test category: all
Test group: all
```

Advertencia (Warning)

Estos son hallazgos más significativos y pueden representar riesgos potenciales para la seguridad. Se deben abordar para mejorar la postura de seguridad, pero no son necesariamente emergencias.

```
[+] Kernel
-----
- Checking default run level [ RUNLEVEL 5 ]
- Checking CPU support (NX/PAE) [ ENCONTRADO ]
  CPU support: PAE and/or NoeXecute supported
- Checking kernel version and release [ HECHO ]
- Checking kernel type [ HECHO ]
- Checking loaded kernel modules [ HECHO ]
  Found 62 active modules
- Checking Linux kernel configuration file [ ENCONTRADO ]
- Checking default I/O kernel scheduler [ NO ENCONTRADO ]
- Checking for available kernel update [ OK ]
- Checking core dumps configuration
  - configuration in systemd conf files [ POR DEFECTO ]
  - configuration in etc/profile [ POR DEFECTO ]
  - 'hard' configuration in security/limits.conf [ POR DEFECTO ]
  - 'soft' configuration in security/limits.conf [ POR DEFECTO ]
  - Checking setuid core dumps configuration [ PROTEGIDO ]
- Check if reboot is needed [ NO ]

[+] Memoria y procesos
-----
- Checking /proc/meminfo [ ENCONTRADO ]
- Searching for dead/zombie processes [ NO ENCONTRADO ]
- Searching for IO waiting processes [ NO ENCONTRADO ]
- Search prelink tooling [ NO ENCONTRADO ]

[+] Usuarios, grupos y autenticación
-----
- Administrator accounts [ OK ]
- Unique UIDs [ OK ]
- Consistency of group files (grpck) [ OK ]
- Unique group IDs [ OK ]
- Unique group names [ OK ]
- Password file consistency [ OK ]
- Password hashing methods [ OK ]
- Checking password hashing rounds [ DESHABILITADO ]
- Query system users (non daemons) [ HECHO ]
- NIS+ authentication support [ NO HABILITADO ]
```

Sugerencia (Suggestion)

Estas son recomendaciones para mejorar la seguridad, pero no se consideran críticas. Son sugerencias para optimizar la configuración y fortalecer la seguridad.

```
[+] Frameworks de seguridad
-----
- Checking presence AppArmor [ ENCONTRADO ]
- Checking AppArmor status [ HABILITADO ]
  Found 123 unconfined processes
- Checking presence SELinux [ NO ENCONTRADO ]
- Checking presence TOMOYO Linux [ NO ENCONTRADO ]
- Checking presence grsecurity [ NO ENCONTRADO ]
- Checking for implemented MAC framework [ OK ]

[+] Software: integridad de ficheros
-----
- Checking file integrity tools
- Checking presence integrity tool [ NO ENCONTRADO ]

[+] Software: Herramientas del sistema
-----
- Checking automation tooling
- Automation tooling [ NO ENCONTRADO ]
- Checking for IDS/IPS tooling [ NINGUNO ]

[+] Software: Malware
-----
- Malware software components [ NO ENCONTRADO ]

[+] Permisos de ficheros
-----
- Starting file permissions check
  File: /boot/grub/grub.cfg [ SUGERENCIA ]
  File: /etc/crontab [ SUGERENCIA ]
  File: /etc/group [ OK ]
  File: /etc/group- [ OK ]
  File: /etc/hosts.allow [ OK ]
  File: /etc/hosts.deny [ OK ]
  File: /etc/issue [ OK ]
  File: /etc/issue.net [ OK ]
  File: /etc/passwd [ OK ]
  File: /etc/passwd- [ OK ]
  Directory: /etc/cron.d [ SUGERENCIA ]
  Directory: /etc/cron.daily [ SUGERENCIA ]
  Directory: /etc/cron.hourly [ SUGERENCIA ]
  Directory: /etc/cron.weekly [ SUGERENCIA ]
  Directory: /etc/cron.monthly [ SUGERENCIA ]

[+] Directorios de inicio
```

Peligro (Danger)

Estos son los problemas más críticos y deben abordarse de inmediato. Los hallazgos de nivel de peligro representan riesgos graves para la seguridad y la integridad del sistema.

```
[+] Directorios de inicio
-----
- Permissions of home directories          [ OK ]
- Ownership of home directories           [ OK ]
- Checking shell history files             [ OK ]

[+] Bastionado del kernel
-----
- Comparing sysctl key pairs with scan profile
- dev.tty.ldisc_autoload (exp: 0)         [ DIFERENTE ]
- fs.protected_fifos (exp: 2)              [ DIFERENTE ]
- fs.protected_hardlinks (exp: 1)          [ OK ]
- fs.protected_regular (exp: 2)            [ OK ]
- fs.protected_symlinks (exp: 1)           [ OK ]
- fs.suid_dumpable (exp: 0)                [ DIFERENTE ]
- kernel.core_uses_pid (exp: 1)            [ OK ]
- kernel.ctrl-alt-del (exp: 0)             [ OK ]
- kernel.dmesg_restrict (exp: 1)           [ OK ]
- kernel.kptr_restrict (exp: 2)            [ DIFERENTE ]
- kernel.modules_disabled (exp: 1)         [ DIFERENTE ]
- kernel.perf_event_paranoid (exp: 3)      [ DIFERENTE ]
- kernel.randomize_va_space (exp: 2)       [ OK ]
- kernel.sysrq (exp: 0)                   [ DIFERENTE ]
- kernel.unprivileged_bpf_disabled (exp: 1) [ DIFERENTE ]
- kernel.yama.ptrace_scope (exp: 1 2 3)    [ OK ]
- net.core.bpf_jit_harden (exp: 2)         [ DIFERENTE ]
- net.ipv4.conf.all.accept_redirects (exp: 0) [ DIFERENTE ]
- 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)    [ OK ]
- net.ipv4.conf.all.log_martians (exp: 1)  [ DIFERENTE ]
- 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)     [ DIFERENTE ]
- net.ipv4.conf.all.send_redirects (exp: 0) [ DIFERENTE ]
- net.ipv4.conf.default.accept_redirects (exp: 0) [ DIFERENTE ]
- net.ipv4.conf.default.accept_source_route (exp: 0) [ OK ]
- net.ipv4.conf.default.log_martians (exp: 1) [ DIFERENTE ]
- 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 1)       [ OK ]
- net.ipv6.conf.all.accept_redirects (exp: 0) [ DIFERENTE ]
- net.ipv6.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv6.conf.default.accept_redirects (exp: 0) [ DIFERENTE ]
- net.ipv6.conf.default.accept_source_route (exp: 0) [ OK ]

[+] Bastionado
-----
- Installed compiler(s)                   [ NO ENCONTRADO ]
- Installed malware scanner               [ NO ENCONTRADO ]
- Non-native binary formats               [ ENCONTRADO ]

[+] Pruebas personalizadas
-----
- Running system tests
```

Al concluir la auditoría, Lynis proporcionará consejos para mejorar nuestro endurecimiento de seguridad y señalará un nivel de endurecimiento. Cuanto más alto sea este nivel, mayor será la fortificación de nuestro sistema.

```
=====
Lynis security scan details:

Hardening index : 60 [#####          ]
Tests performed : 247
Plugins enabled : 1

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

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

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
=====
```

He realizado algunas modificaciones para mejorar las alertas que indican el nivel más alto de peligro, con el fin de evaluar cómo ha mejorado la fortificación del sistema. Ahora procedo a ejecutar otro informe para revisar los resultados


```
Directory: /etc/cron.weekly [ SUGERENCIA ]
Directory: /etc/cron.monthly [ SUGERENCIA ]
```

[+] Directorios de inicio

```
-----
- Permissions of home directories [ OK ]
- Ownership of home directories [ OK ]
- Checking shell history files [ OK ]
```

[+] Bastionado del kernel

```
-----
- Comparing sysctl key pairs with scan profile
  - dev.tty.ldisc_autoload (exp: 0) [ OK ]
  - fs.protected_fifos (exp: 2) [ OK ]
  - fs.protected_hardlinks (exp: 1) [ OK ]
  - fs.protected_regular (exp: 2) [ OK ]
  - fs.protected_symlinks (exp: 1) [ OK ]
  - fs.suid_dumpable (exp: 0) [ OK ]
  - kernel.core_uses_pid (exp: 1) [ OK ]
  - kernel.ctrl-alt-del (exp: 0) [ OK ]
  - kernel.dmesg_restrict (exp: 1) [ OK ]
  - kernel.kptr_restrict (exp: 2) [ OK ]
  - kernel.modules_disabled (exp: 1) [ OK ]
  - kernel.perf_event_paranoid (exp: 3) [ OK ]
  - kernel.randomize_va_space (exp: 2) [ OK ]
  - kernel.sysrq (exp: 0) [ OK ]
  - kernel.unprivileged_bpf_disabled (exp: 1) [ OK ]
  - kernel.yama.ptrace_scope (exp: 1 2 3) [ OK ]
  - net.core.bpf_jit_harden (exp: 2) [ OK ]
  - 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) [ OK ]
  - net.ipv4.conf.all.log_martians (exp: 1) [ OK ]
  - 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) [ OK ]
  - net.ipv4.conf.all.send_redirects (exp: 0) [ OK ]
  - net.ipv4.conf.default.accept_redirects (exp: 0) [ OK ]
  - net.ipv4.conf.default.accept_source_route (exp: 0) [ OK ]
  - net.ipv4.conf.default.log_martians (exp: 1) [ OK ]
  - 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 1) [ OK ]
  - net.ipv6.conf.all.accept_redirects (exp: 0) [ OK ]
  - net.ipv6.conf.all.accept_source_route (exp: 0) [ OK ]
  - net.ipv6.conf.default.accept_redirects (exp: 0) [ OK ]
  - net.ipv6.conf.default.accept_source_route (exp: 0) [ OK ]
```

[+] Bastionado

```
-----
- Installed compiler(s) [ ENCONTRADO ]
- Installed malware scanner [ ENCONTRADO ]
- Non-native binary formats [ ENCONTRADO ]
```

Como podemos observar, nuestro endurecimiento ha mejorado de 60 a 72.

```
=====
Lynis security scan details:

Hardening index : 72 [#####          ]
Tests performed : 253
Plugins enabled : 1

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

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

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
=====
```

También nos indica la ubicación donde se almacenarán los informes, que se encuentra en la ruta ***'/var/log/lynis.log'***.