Hardening con Lynis

27/11/23

Jose Almirón Lopez

Índice

¿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 autoría 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.

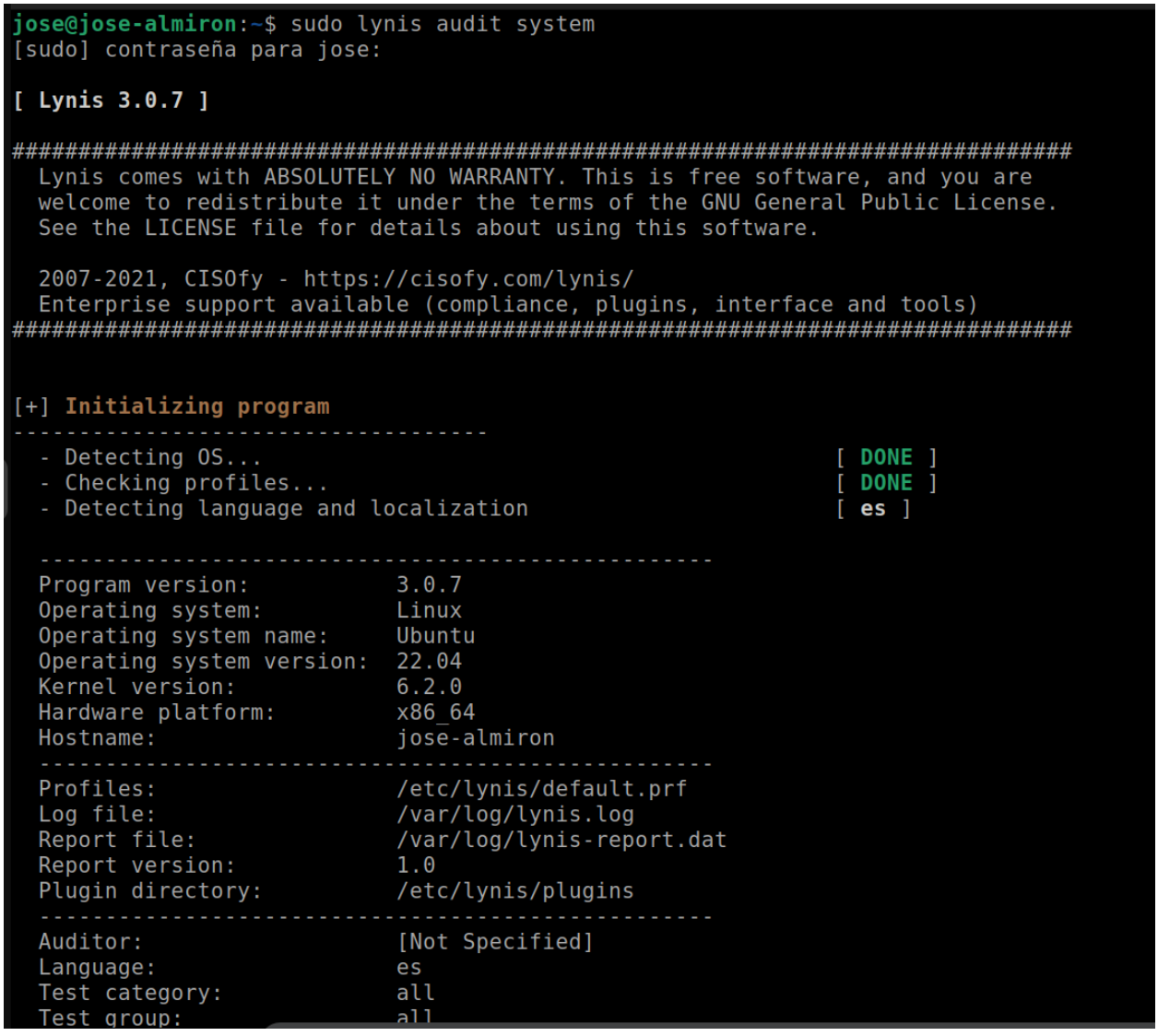
Instalación de Lynis

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]
```

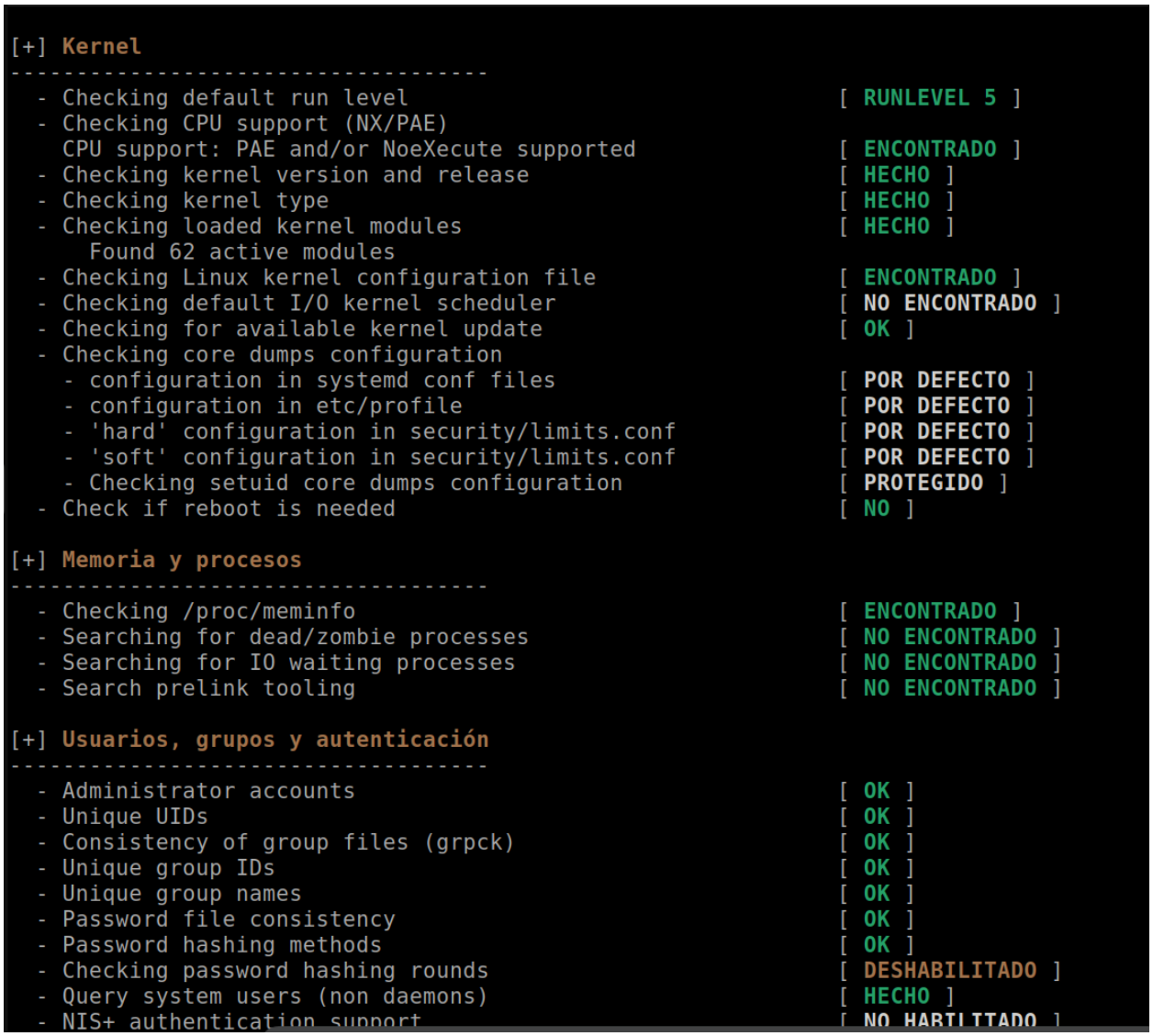
Funcionamiento básico

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.



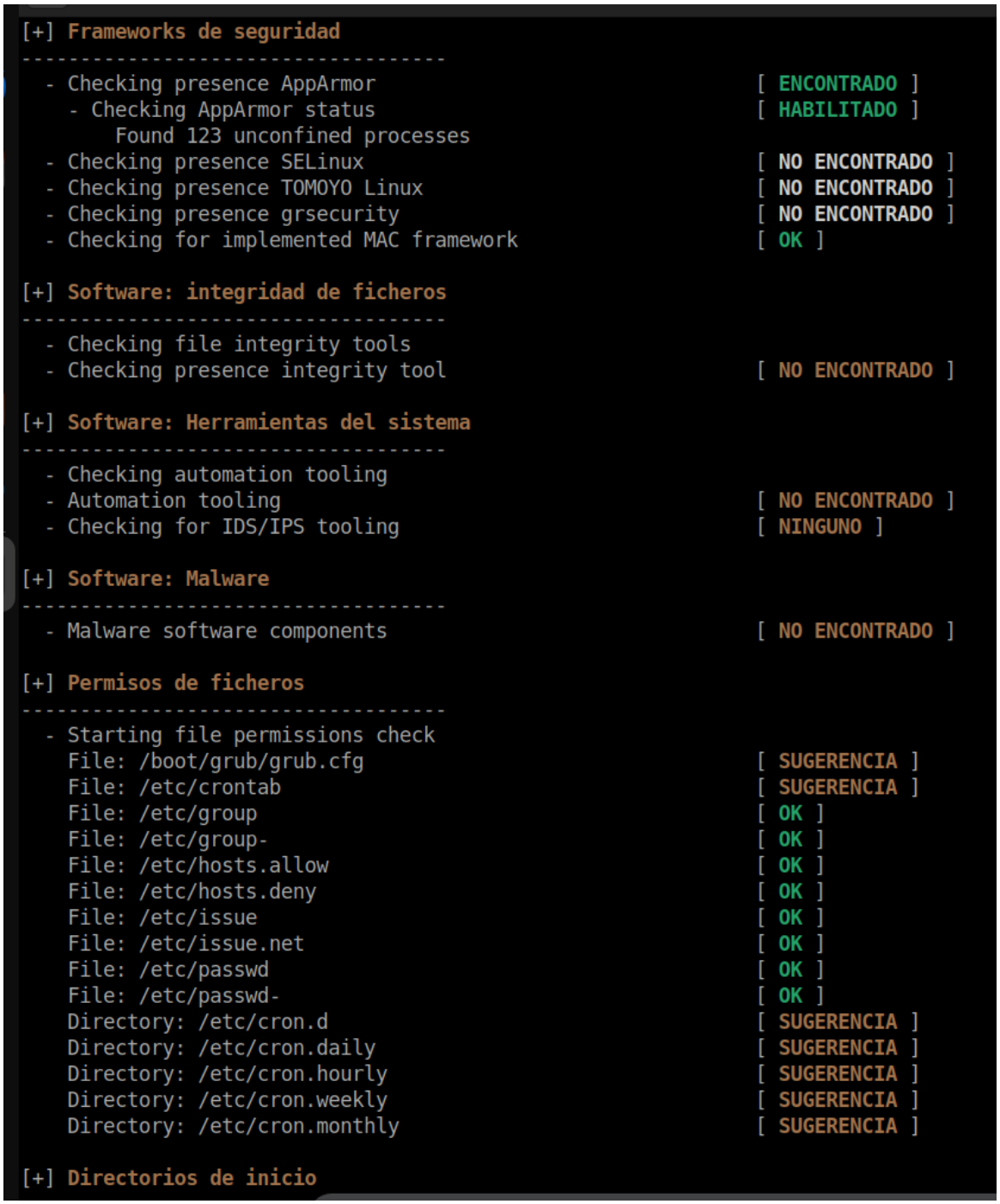
Advertencia (Warning)

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.



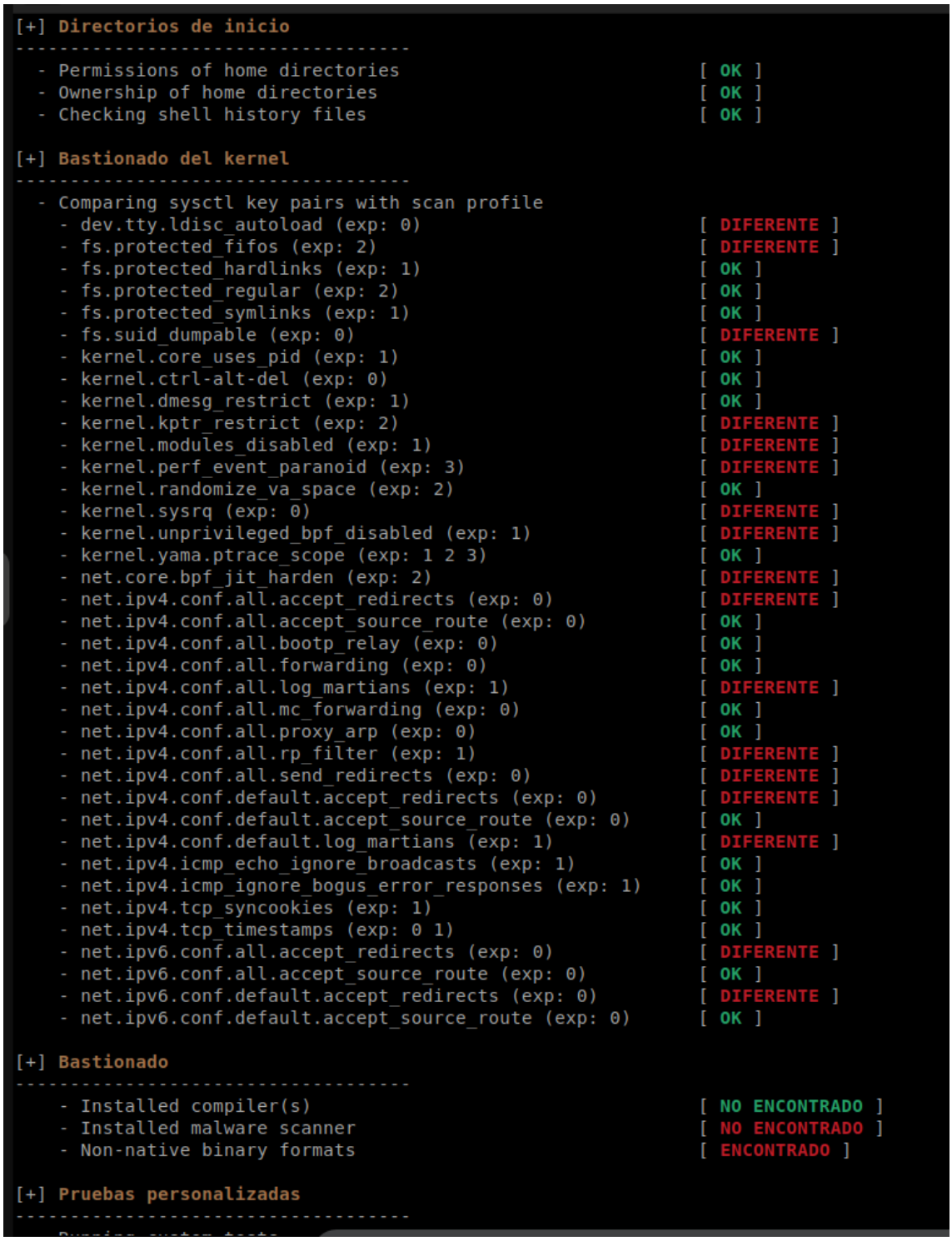
Sugerencia (Suggestion)

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

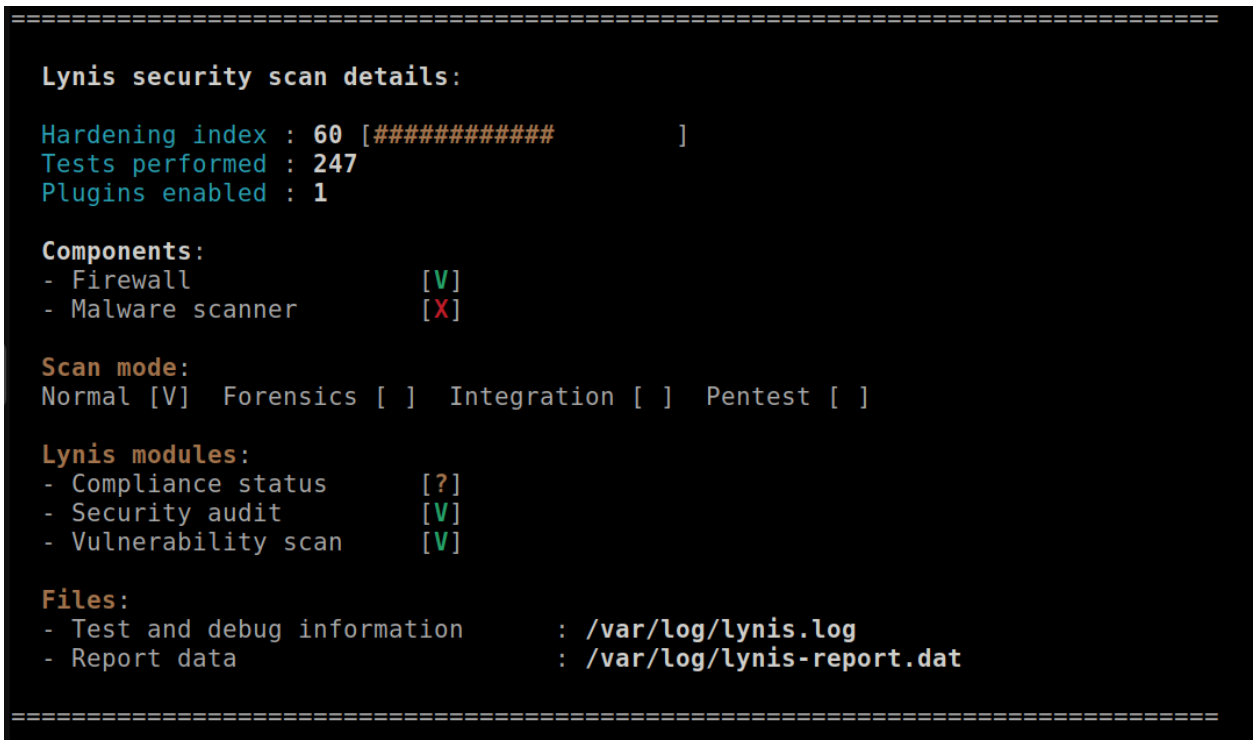


Peligro (Danger)

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.



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.



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

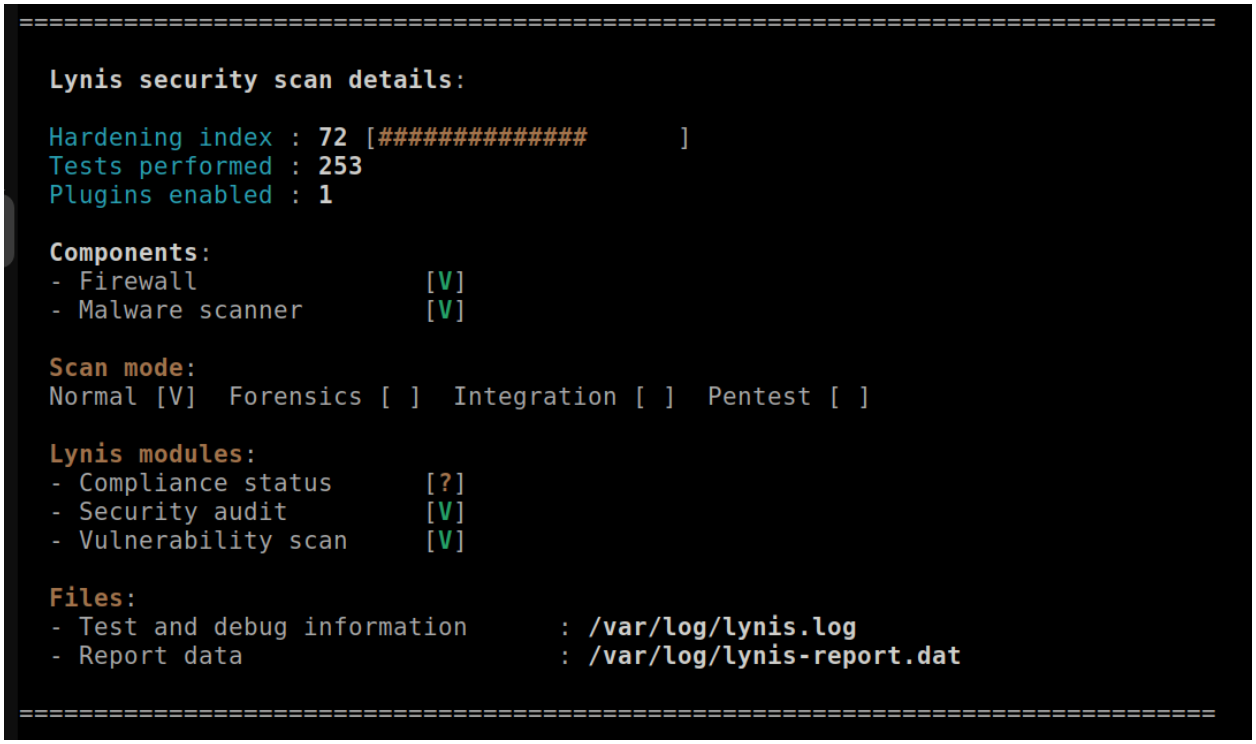
```
    Directory: /etc/cron.weekly                                [ SUGERENCIA ]
    Directory: /etc/cron.monthly                               [ SUGERENCIA ]

[+] 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.



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