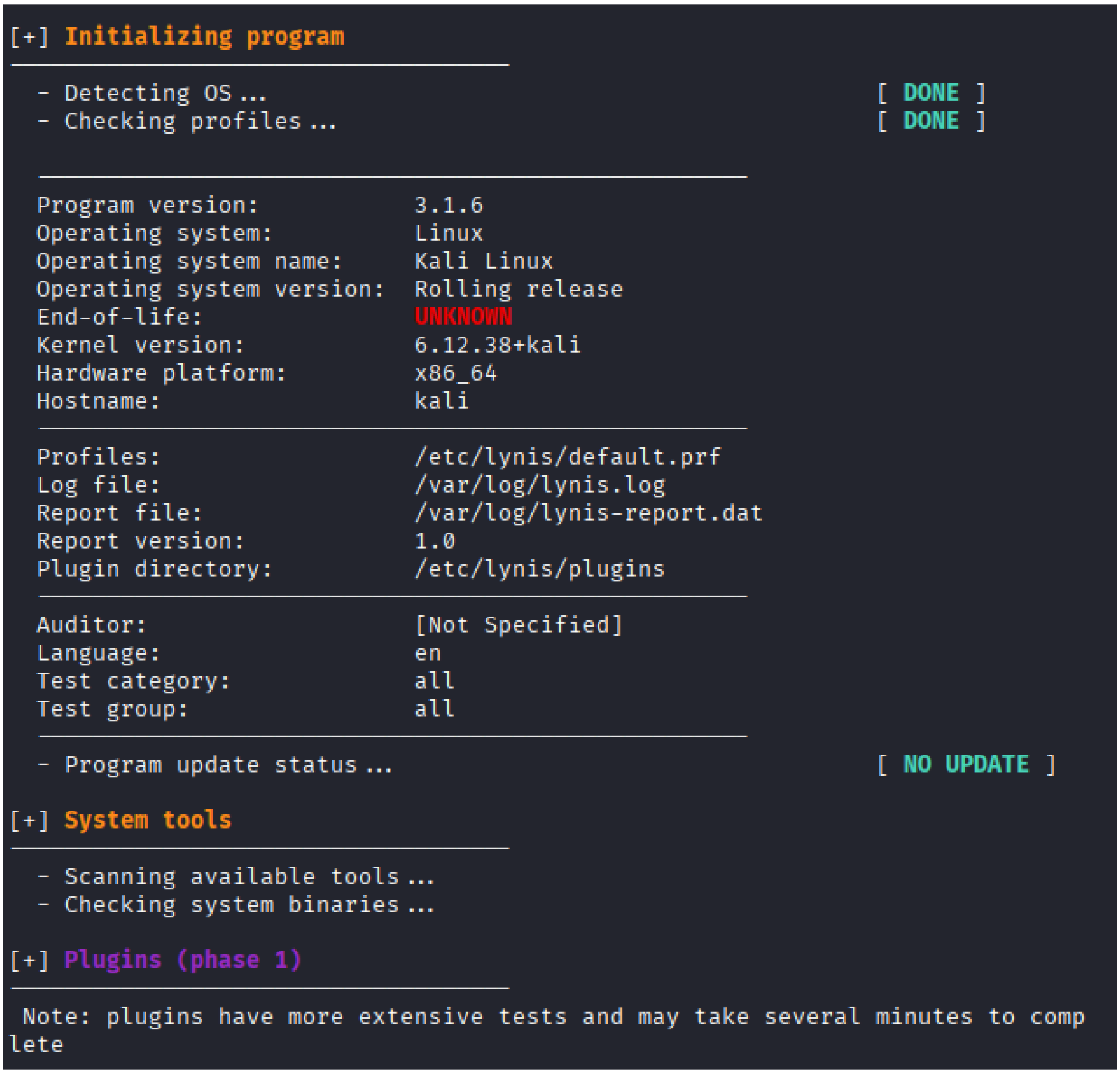
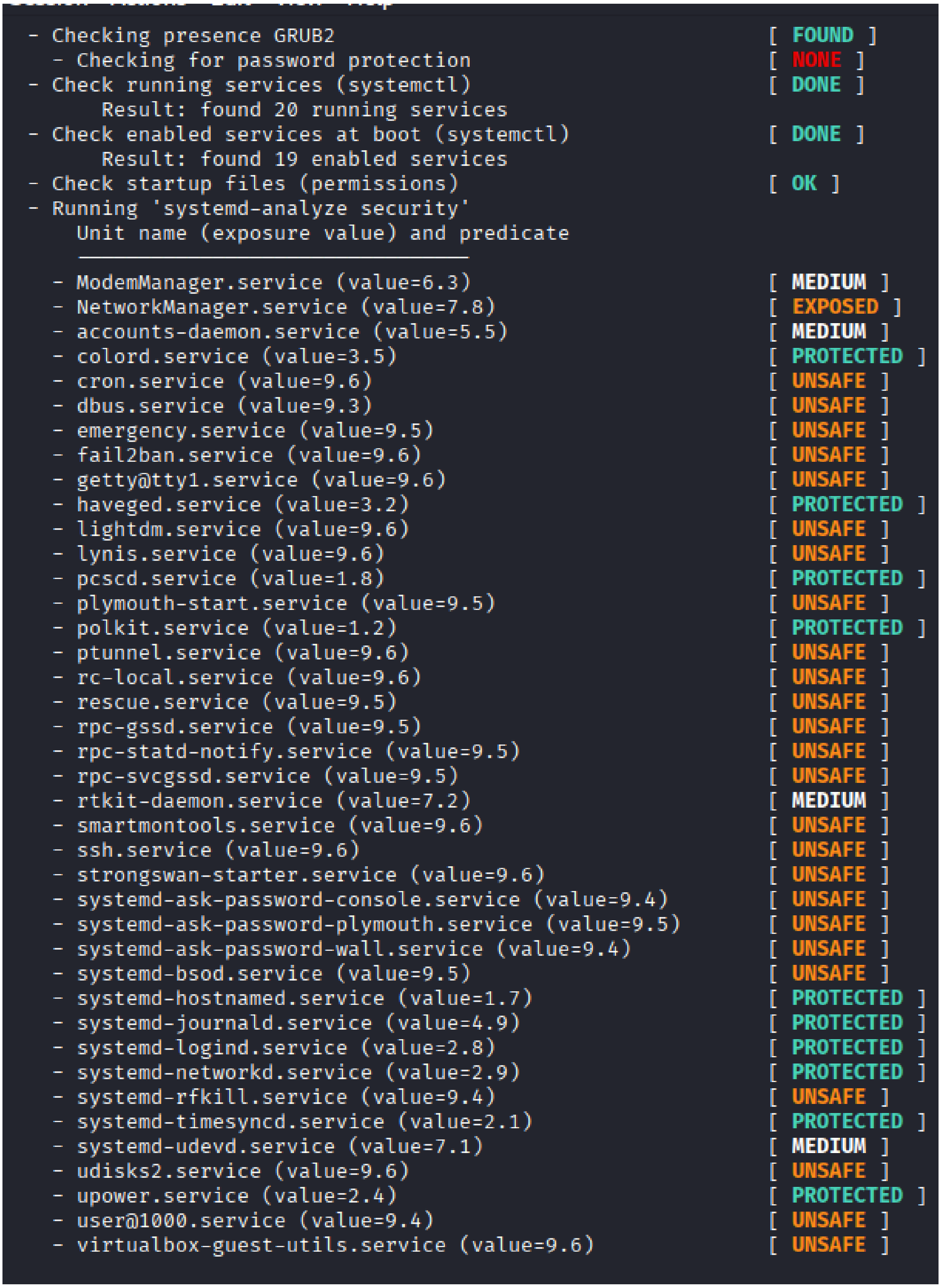
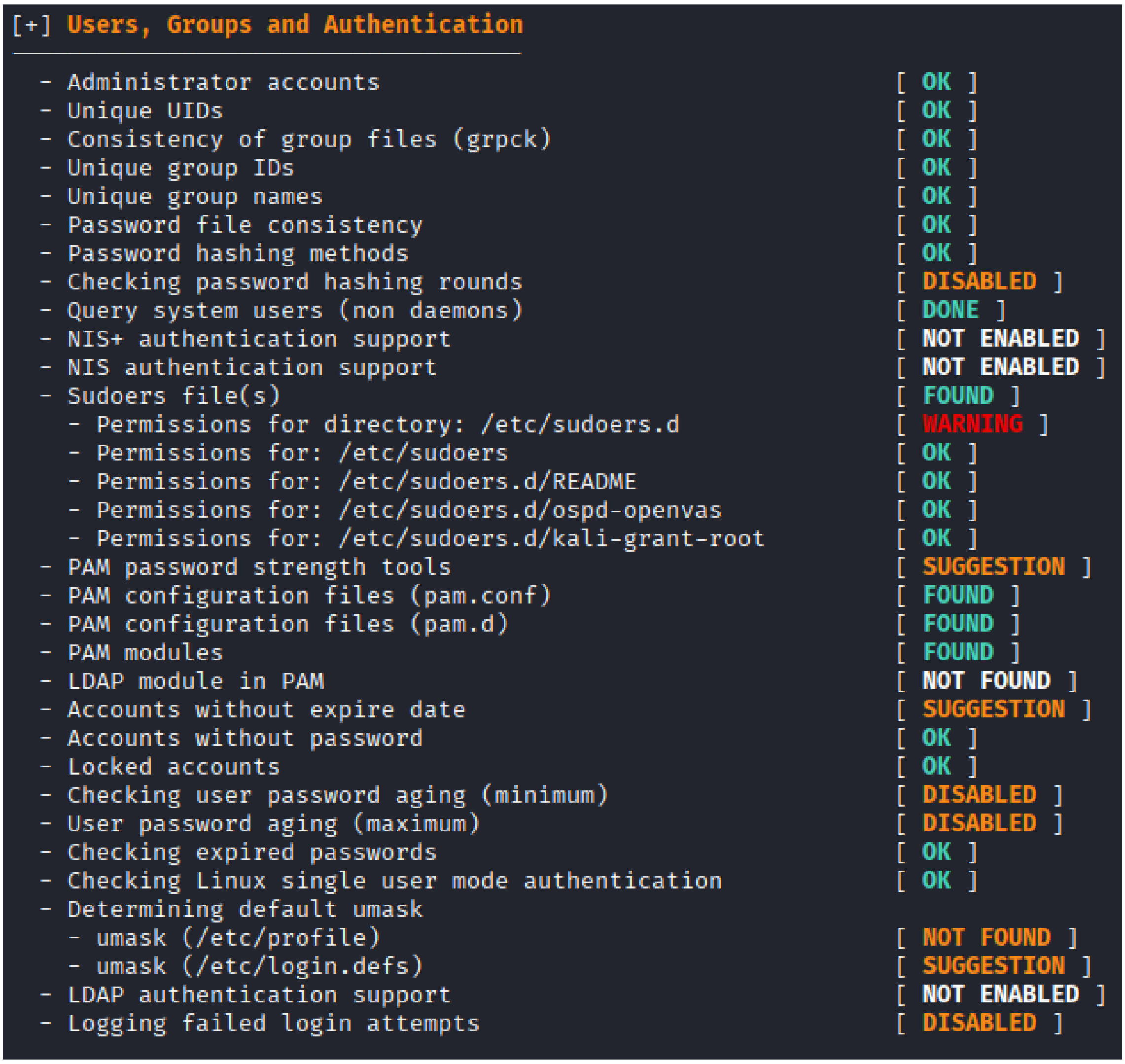
Parte 1: Auditoría del Sistema con Lynis



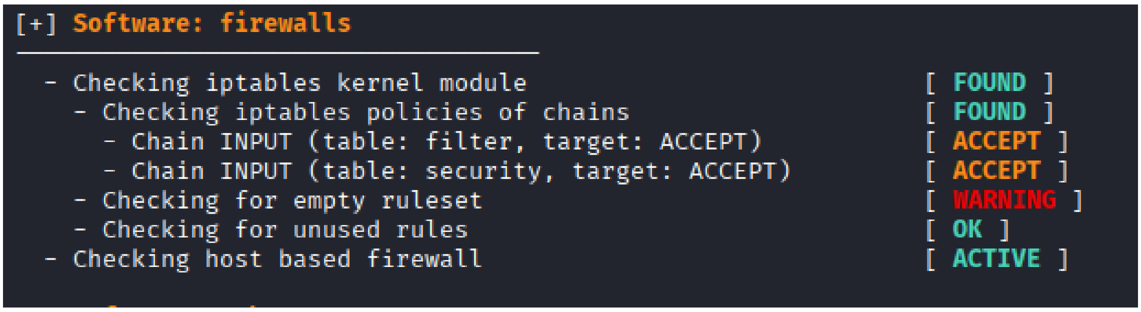
```
[+] Initializing program
------------------------------------
  - Detecting OS ...                                           [ DONE ]
  - Checking profiles ...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Kali Linux
  Operating system version:  Rolling release
  End-of-life:               UNKNOWN
  Kernel version:            6.12.38+kali
  Hardware platform:         x86_64
  Hostname:                  kali
  ---------------------------------------------------
  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:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status ...                                  [ NO UPDATE ]

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

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to comp
lete
```



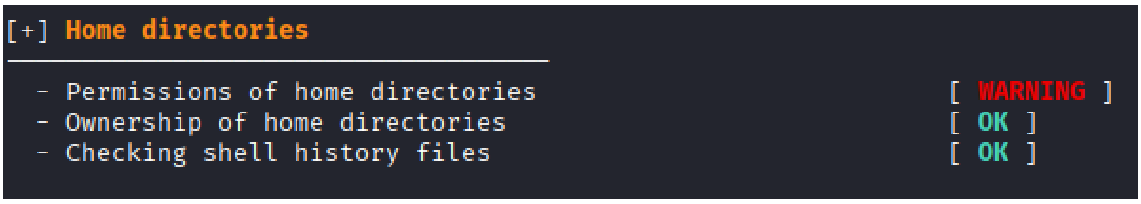
```
  - Checking presence GRUB2                                   [ FOUND ]
    - Checking for password protection                        [ NONE ]
  - Check running services (systemctl)                        [ DONE ]
        Result: found 20 running services
  - Check enabled services at boot (systemctl)                [ DONE ]
        Result: found 19 enabled services
  - Check startup files (permissions)                         [ OK ]
  - Running 'systemd-analyze security'
      Unit name (exposure value) and predicate
      ────────────────────────────────
    - ModemManager.service (value=6.3)                        [ MEDIUM ]
    - NetworkManager.service (value=7.8)                      [ EXPOSED ]
    - accounts-daemon.service (value=5.5)                     [ MEDIUM ]
    - colord.service (value=3.5)                              [ PROTECTED ]
    - cron.service (value=9.6)                                [ UNSAFE ]
    - dbus.service (value=9.3)                                [ UNSAFE ]
    - emergency.service (value=9.5)                           [ UNSAFE ]
    - fail2ban.service (value=9.6)                            [ UNSAFE ]
    - getty@tty1.service (value=9.6)                          [ UNSAFE ]
    - haveged.service (value=3.2)                             [ PROTECTED ]
    - lightdm.service (value=9.6)                             [ UNSAFE ]
    - lynis.service (value=9.6)                               [ UNSAFE ]
    - pcscd.service (value=1.8)                               [ PROTECTED ]
    - plymouth-start.service (value=9.5)                      [ UNSAFE ]
    - polkit.service (value=1.2)                              [ PROTECTED ]
    - ptunnel.service (value=9.6)                             [ UNSAFE ]
    - rc-local.service (value=9.6)                            [ UNSAFE ]
    - rescue.service (value=9.5)                              [ UNSAFE ]
    - rpc-gssd.service (value=9.5)                            [ UNSAFE ]
    - rpc-statd-notify.service (value=9.5)                    [ UNSAFE ]
    - rpc-svcgssd.service (value=9.5)                         [ UNSAFE ]
    - rtkit-daemon.service (value=7.2)                        [ MEDIUM ]
    - smartmontools.service (value=9.6)                       [ UNSAFE ]
    - ssh.service (value=9.6)                                 [ UNSAFE ]
    - strongswan-starter.service (value=9.6)                  [ UNSAFE ]
    - systemd-ask-password-console.service (value=9.4)        [ UNSAFE ]
    - systemd-ask-password-plymouth.service (value=9.5)       [ UNSAFE ]
    - systemd-ask-password-wall.service (value=9.4)           [ UNSAFE ]
    - systemd-bsod.service (value=9.5)                        [ UNSAFE ]
    - systemd-hostnamed.service (value=1.7)                   [ PROTECTED ]
    - systemd-journald.service (value=4.9)                    [ PROTECTED ]
    - systemd-logind.service (value=2.8)                      [ PROTECTED ]
    - systemd-networkd.service (value=2.9)                    [ PROTECTED ]
    - systemd-rfkill.service (value=9.4)                      [ UNSAFE ]
    - systemd-timesyncd.service (value=2.1)                   [ PROTECTED ]
    - systemd-udevd.service (value=7.1)                       [ MEDIUM ]
    - udisks2.service (value=9.6)                             [ UNSAFE ]
    - upower.service (value=2.4)                              [ PROTECTED ]
    - user@1000.service (value=9.4)                           [ UNSAFE ]
    - virtualbox-guest-utils.service (value=9.6)              [ UNSAFE ]
```



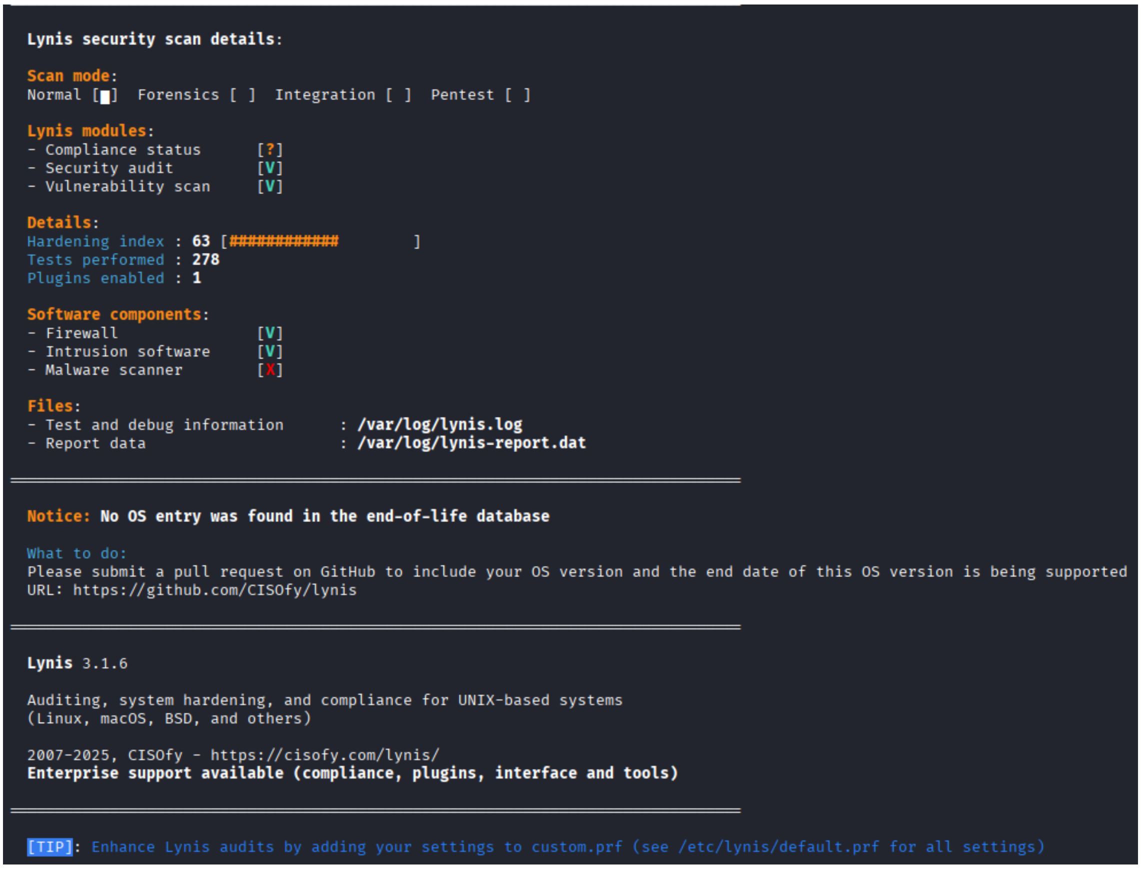
```
[+] Users, Groups and Authentication
------------------------------------
  - Administrator accounts                                     [ OK ]
  - Unique UIDs                                                [ OK ]
  - Consistency of group files (grpck)                         [ OK ]
  - Unique group IDs                                           [ OK ]
  - Unique group names                                         [ OK ]
  - Password file consistency                                  [ OK ]
  - Password hashing methods                                   [ OK ]
  - Checking password hashing rounds                           [ DISABLED ]
  - Query system users (non daemons)                           [ DONE ]
  - NIS+ authentication support                                [ NOT ENABLED ]
  - NIS authentication support                                 [ NOT ENABLED ]
  - Sudoers file(s)                                            [ FOUND ]
    - Permissions for directory: /etc/sudoers.d                [ WARNING ]
    - Permissions for: /etc/sudoers                            [ OK ]
    - Permissions for: /etc/sudoers.d/README                   [ OK ]
    - Permissions for: /etc/sudoers.d/ospd-openvas             [ OK ]
    - Permissions for: /etc/sudoers.d/kali-grant-root          [ OK ]
  - PAM password strength tools                                [ SUGGESTION ]
  - PAM configuration files (pam.conf)                         [ FOUND ]
  - PAM configuration files (pam.d)                            [ FOUND ]
  - PAM modules                                                [ FOUND ]
  - LDAP module in PAM                                         [ NOT FOUND ]
  - Accounts without expire date                               [ SUGGESTION ]
  - Accounts without password                                  [ OK ]
  - Locked accounts                                            [ OK ]
  - Checking user password aging (minimum)                     [ DISABLED ]
  - User password aging (maximum)                              [ DISABLED ]
  - Checking expired passwords                                 [ OK ]
  - Checking Linux single user mode authentication             [ OK ]
  - Determining default umask
    - umask (/etc/profile)                                     [ NOT FOUND ]
    - umask (/etc/login.defs)                                  [ SUGGESTION ]
  - LDAP authentication support                                [ NOT ENABLED ]
  - Logging failed login attempts                              [ DISABLED ]
```



```
[+] Software: firewalls
------------------------------------
  - Checking iptables kernel module                            [ FOUND ]
    - Checking iptables policies of chains                     [ FOUND ]
      - Chain INPUT (table: filter, target: ACCEPT)            [ ACCEPT ]
      - Chain INPUT (table: security, target: ACCEPT)          [ ACCEPT ]
    - Checking for empty ruleset                               [ WARNING ]
    - Checking for unused rules                                [ OK ]
  - Checking host based firewall                               [ ACTIVE ]
```



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



```
  Lynis security scan details:

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

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Details:
  Hardening index : 63 [############        ]
  Tests performed : 278
  Plugins enabled : 1

  Software components:
  - Firewall               [V]
  - Intrusion software     [V]
  - Malware scanner        [X]

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

================================================================================

  Notice: No OS entry was found in the end-of-life database

  What to do:
  Please submit a pull request on GitHub to include your OS version and the end date of this OS version is being supported
  URL: https://github.com/CISOfy/lynis

================================================================================

  Lynis 3.1.6

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

  2007-2025, 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)
```

Instalar un file integrity checker (FINT-4350)

Como AIDE, Wazuh, OSSEC o rkhunter.

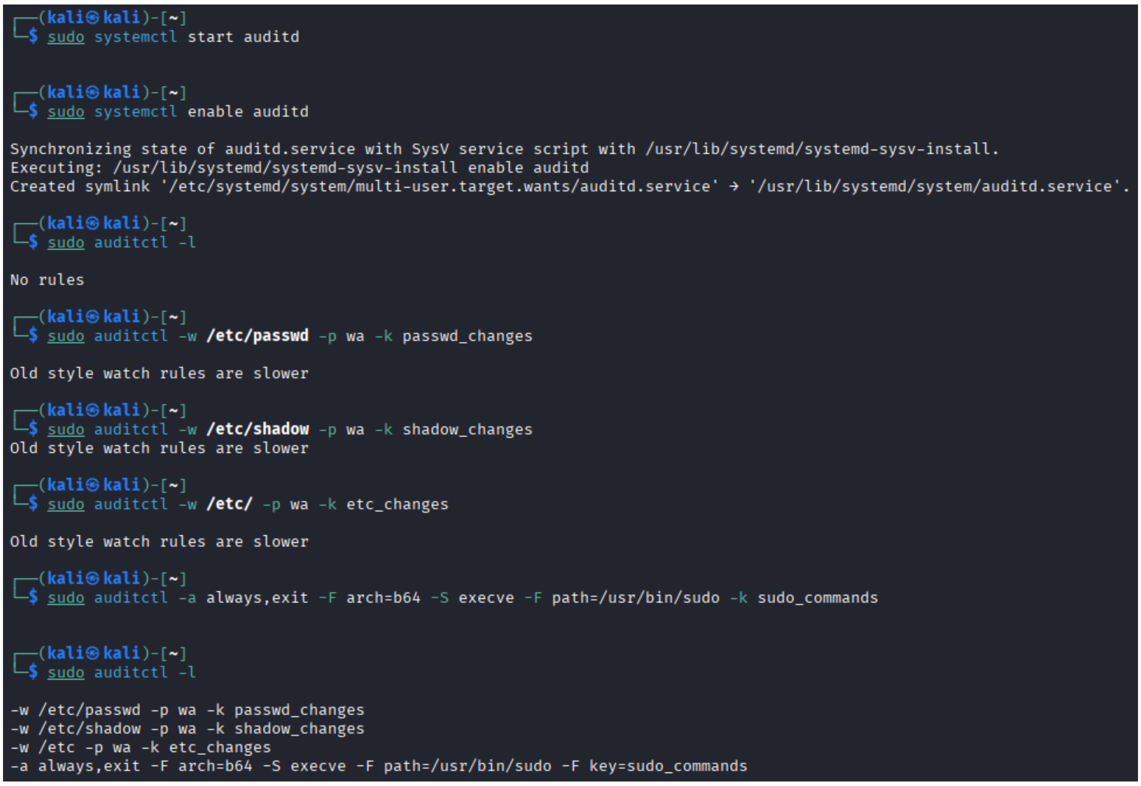
Por qué:

- Detecta modificaciones sospechosas en archivos críticos.
- Sirve para saber si un atacante ha cambiado configuración, binarios o contraseñas.
- Es fundamental para detectar intrusiones que ya han ocurrido.

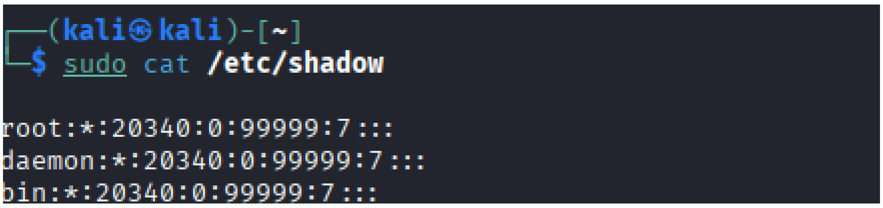
Una auditoría automatizada como Lynis sirve para:

- Detectar vulnerabilidades, configuraciones débiles o malas prácticas de seguridad en un sistema Linux.
- Evaluar el estado general de seguridad del sistema según estándares y buenas prácticas (CIS, NIST, etc.).
- Revisar:
    - configuraciones del kernel
    - permisos de archivos
    - servicios activos
    - autenticación (PAM, contraseñas, SSH)
    - firewall
    - software instalado
- Generar recomendaciones automáticas para fortalecer el sistema.

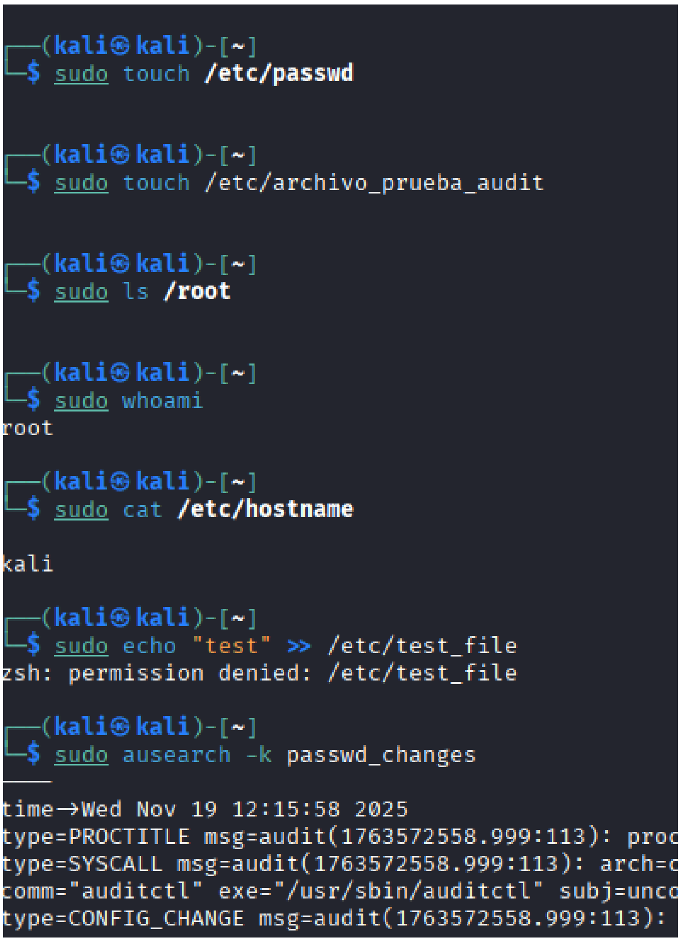
Parte 2: Auditoría y Monitorización con auditd



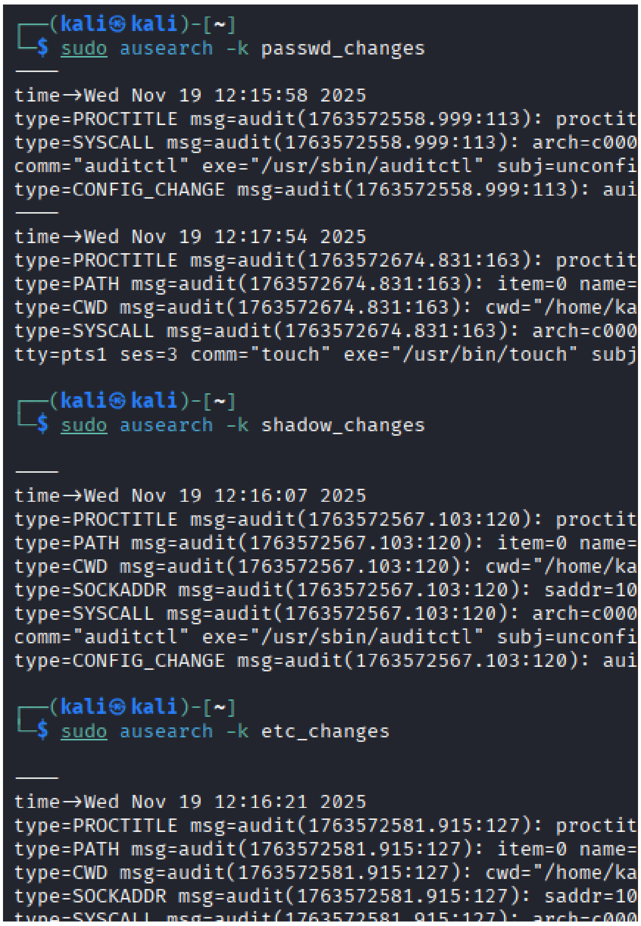
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start auditd


┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable auditd

Synchronizing state of auditd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable auditd
Created symlink '/etc/systemd/system/multi-user.target.wants/auditd.service' → '/usr/lib/systemd/system/auditd.service'.

┌──(kali㉿kali)-[~]
└─$ sudo auditctl -l

No rules

┌──(kali㉿kali)-[~]
└─$ sudo auditctl -w /etc/passwd -p wa -k passwd_changes

Old style watch rules are slower

┌──(kali㉿kali)-[~]
└─$ sudo auditctl -w /etc/shadow -p wa -k shadow_changes
Old style watch rules are slower

┌──(kali㉿kali)-[~]
└─$ sudo auditctl -w /etc/ -p wa -k etc_changes

Old style watch rules are slower

┌──(kali㉿kali)-[~]
└─$ sudo auditctl -a always,exit -F arch=b64 -S execve -F path=/usr/bin/sudo -k sudo_commands


┌──(kali㉿kali)-[~]
└─$ sudo auditctl -l

-w /etc/passwd -p wa -k passwd_changes
-w /etc/shadow -p wa -k shadow_changes
-w /etc -p wa -k etc_changes
-a always,exit -F arch=b64 -S execve -F path=/usr/bin/sudo -F key=sudo_commands
```



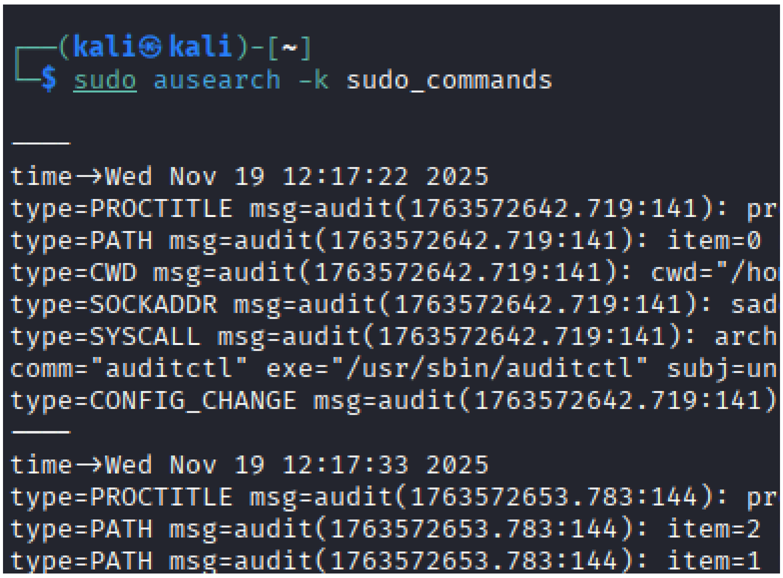
```
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/shadow

root:*:20340:0:99999:7:::
daemon:*:20340:0:99999:7:::
bin:*:20340:0:99999:7:::
```



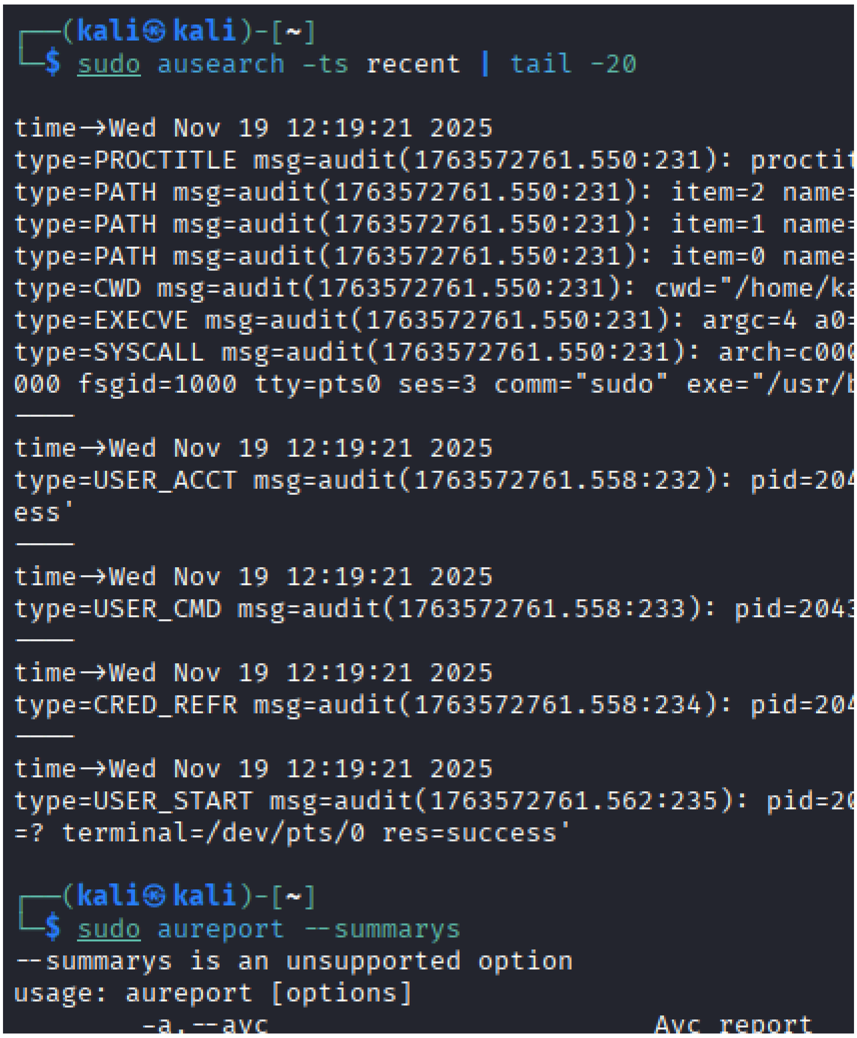
```
┌──(kali㉿kali)-[~]
└─$ sudo touch /etc/passwd

┌──(kali㉿kali)-[~]
└─$ sudo touch /etc/archivo_prueba_audit

┌──(kali㉿kali)-[~]
└─$ sudo ls /root

┌──(kali㉿kali)-[~]
└─$ sudo whoami
root

┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/hostname

kali

┌──(kali㉿kali)-[~]
└─$ sudo echo "test" >> /etc/test_file
zsh: permission denied: /etc/test_file

┌──(kali㉿kali)-[~]
└─$ sudo ausearch -k passwd_changes
----
time→Wed Nov 19 12:15:58 2025
type=PROCTITLE msg=audit(1763572558.999:113): proc
type=SYSCALL msg=audit(1763572558.999:113): arch=c
comm="auditctl" exe="/usr/sbin/auditctl" subj=unco
type=CONFIG_CHANGE msg=audit(1763572558.999:113):
```



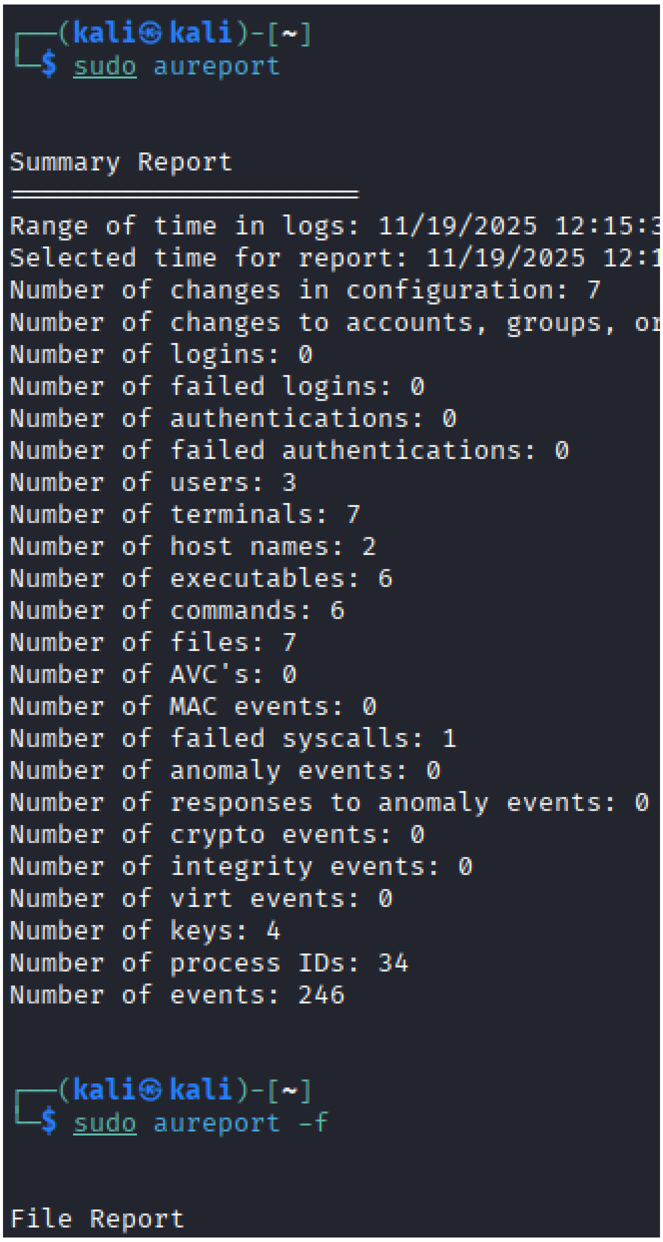
```
┌──(kali㉿kali)-[~]
└─$ sudo ausearch -k passwd_changes
----
time→Wed Nov 19 12:15:58 2025
type=PROCTITLE msg=audit(1763572558.999:113): proctit
type=SYSCALL msg=audit(1763572558.999:113): arch=c000
comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfi
type=CONFIG_CHANGE msg=audit(1763572558.999:113): aui
----
time→Wed Nov 19 12:17:54 2025
type=PROCTITLE msg=audit(1763572674.831:163): proctit
type=PATH msg=audit(1763572674.831:163): item=0 name=
type=CWD msg=audit(1763572674.831:163): cwd="/home/ka
type=SYSCALL msg=audit(1763572674.831:163): arch=c000
tty=pts1 ses=3 comm="touch" exe="/usr/bin/touch" subj

┌──(kali㉿kali)-[~]
└─$ sudo ausearch -k shadow_changes

----
time→Wed Nov 19 12:16:07 2025
type=PROCTITLE msg=audit(1763572567.103:120): proctit
type=PATH msg=audit(1763572567.103:120): item=0 name=
type=CWD msg=audit(1763572567.103:120): cwd="/home/ka
type=SOCKADDR msg=audit(1763572567.103:120): saddr=10
type=SYSCALL msg=audit(1763572567.103:120): arch=c000
comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfi
type=CONFIG_CHANGE msg=audit(1763572567.103:120): aui

┌──(kali㉿kali)-[~]
└─$ sudo ausearch -k etc_changes

----
time→Wed Nov 19 12:16:21 2025
type=PROCTITLE msg=audit(1763572581.915:127): proctit
type=PATH msg=audit(1763572581.915:127): item=0 name=
type=CWD msg=audit(1763572581.915:127): cwd="/home/ka
type=SOCKADDR msg=audit(1763572581.915:127): saddr=10
type=SYSCALL msg=audit(1763572581.915:127): arch=c000
```



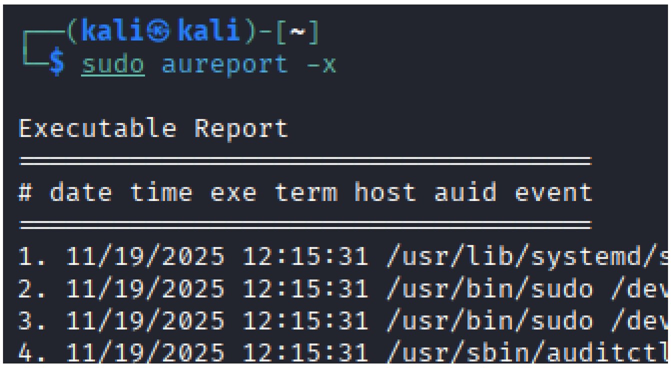
```
┌──(kali㉿kali)-[~]
└─$ sudo ausearch -k sudo_commands

----
time->Wed Nov 19 12:17:22 2025
type=PROCTITLE msg=audit(1763572642.719:141): pr
type=PATH msg=audit(1763572642.719:141): item=0
type=CWD msg=audit(1763572642.719:141): cwd="/ho
type=SOCKADDR msg=audit(1763572642.719:141): sad
type=SYSCALL msg=audit(1763572642.719:141): arch
comm="auditctl" exe="/usr/sbin/auditctl" subj=un
type=CONFIG_CHANGE msg=audit(1763572642.719:141)
----
time->Wed Nov 19 12:17:33 2025
type=PROCTITLE msg=audit(1763572653.783:144): pr
type=PATH msg=audit(1763572653.783:144): item=2
type=PATH msg=audit(1763572653.783:144): item=1
```



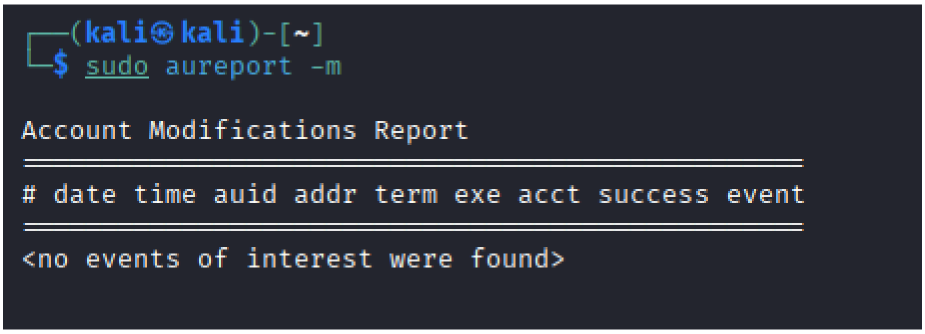
```
┌──(kali㉿kali)-[~]
└─$ sudo ausearch -ts recent | tail -20

time->Wed Nov 19 12:19:21 2025
type=PROCTITLE msg=audit(1763572761.550:231): procti
type=PATH msg=audit(1763572761.550:231): item=2 name=
type=PATH msg=audit(1763572761.550:231): item=1 name=
type=PATH msg=audit(1763572761.550:231): item=0 name=
type=CWD msg=audit(1763572761.550:231): cwd="/home/ka
type=EXECVE msg=audit(1763572761.550:231): argc=4 a0=
type=SYSCALL msg=audit(1763572761.550:231): arch=c000
000 fsgid=1000 tty=pts0 ses=3 comm="sudo" exe="/usr/b
----
time->Wed Nov 19 12:19:21 2025
type=USER_ACCT msg=audit(1763572761.558:232): pid=204
ess'
----
time->Wed Nov 19 12:19:21 2025
type=USER_CMD msg=audit(1763572761.558:233): pid=2043
----
time->Wed Nov 19 12:19:21 2025
type=CRED_REFR msg=audit(1763572761.558:234): pid=204
----
time->Wed Nov 19 12:19:21 2025
type=USER_START msg=audit(1763572761.562:235): pid=20
=? terminal=/dev/pts/0 res=success'

┌──(kali㉿kali)-[~]
└─$ sudo aureport --summarys
--summarys is an unsupported option
usage: aureport [options]
        -a,--avc                        Avc report
```



```
┌──(kali㉿kali)-[~]
└─$ sudo aureport


Summary Report
======================
Range of time in logs: 11/19/2025 12:15:3
Selected time for report: 11/19/2025 12:1
Number of changes in configuration: 7
Number of changes to accounts, groups, or
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 3
Number of terminals: 7
Number of host names: 2
Number of executables: 6
Number of commands: 6
Number of files: 7
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 1
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 4
Number of process IDs: 34
Number of events: 246


┌──(kali㉿kali)-[~]
└─$ sudo aureport -f


File Report
```



```
┌──(kali㉿kali)-[~]
└─$ sudo aureport -x

Executable Report
====================================
# date time exe term host auid event
====================================
1. 11/19/2025 12:15:31 /usr/lib/systemd/s
2. 11/19/2025 12:15:31 /usr/bin/sudo /dev
3. 11/19/2025 12:15:31 /usr/bin/sudo /dev
4. 11/19/2025 12:15:31 /usr/sbin/auditctl
```



```
┌──(kali㉿kali)-[~]
└─$ sudo aureport -m

Account Modifications Report
=================================================
# date time auid addr term exe acct success event
=================================================
<no events of interest were found>
```

auditd registró:

Acceso y modificación del fichero /etc/passwd

Solo se registró la configuración de la regla, pero no se detectaron accesos o modificaciones posteriores.

auditd registró estos eventos:

1. **sudo auditctl -l**
2. **sudo cat /etc/shadow**

En total se ven 2 ejecuciones reales de sudo después de configurar la regla.

Un sistema de auditoría como auditd sirve para monitorear y registrar actividades críticas del servidor para mejorar la seguridad, la trazabilidad y la capacidad de detectar incidentes.

Escenario 1 — Manipulación de archivos de sistema

auditd detecta:

- Intentos de modificar /etc/passwd, /etc/shadow, /etc/sudoers
- Cambios no autorizados en configuraciones críticas

Esto puede indicar un intento de escalada de privilegios o persistencia.

Escenario 2 — Uso sospechoso de sudo o ejecución de binarios peligrosos

auditd puede detectar:

- Muchos intentos de sudo fallidos
- Ejecución de herramientas como ncat, bash, curl como root
- Creación de shells inesperadas

Esto puede indicar un ataque interno o un intruso que consiguió acceso.