Laboratorio de Telemetría y Auditoría

Entorno

Kali Linux (10.0.2.10)

Wazuh Server (10.0.2.20)

Suricata IDS

Chrony/NTP

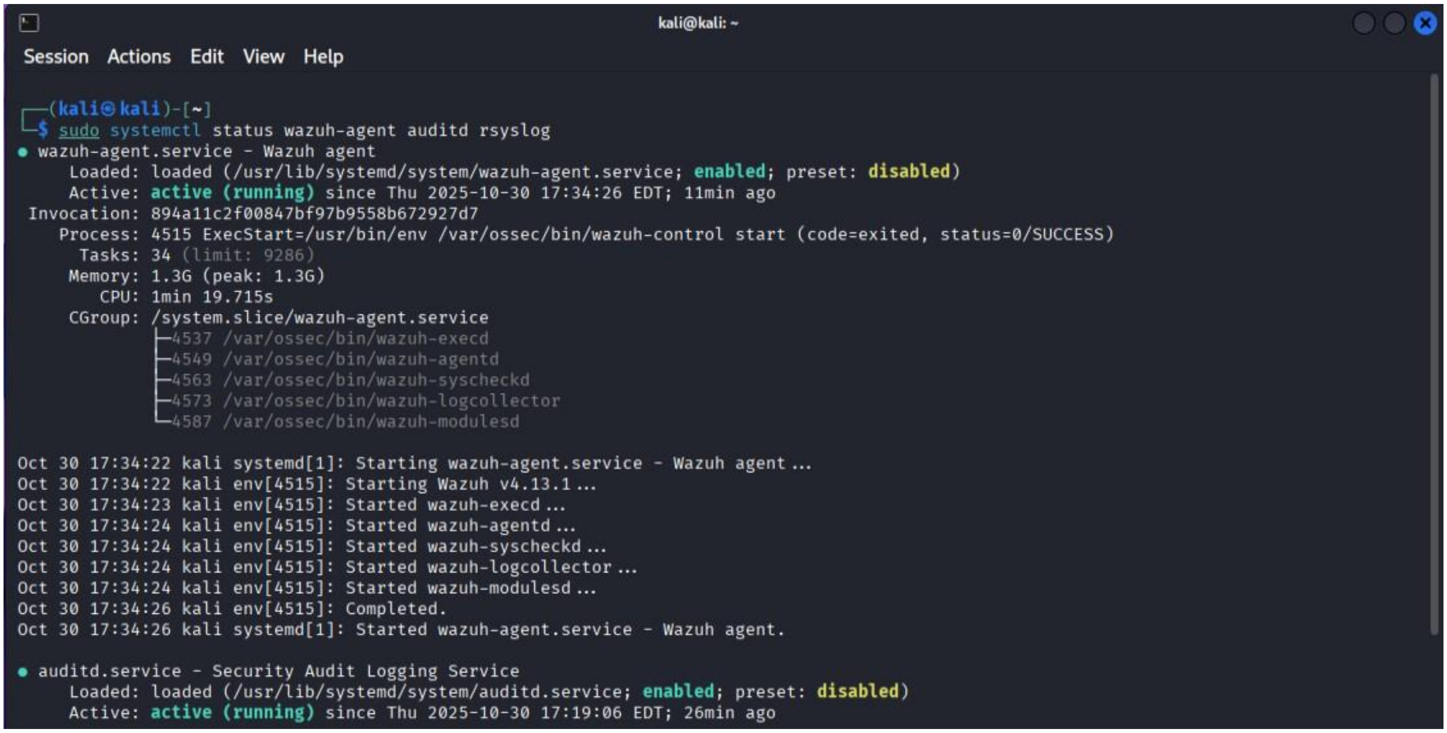
Índice

1. Introducción

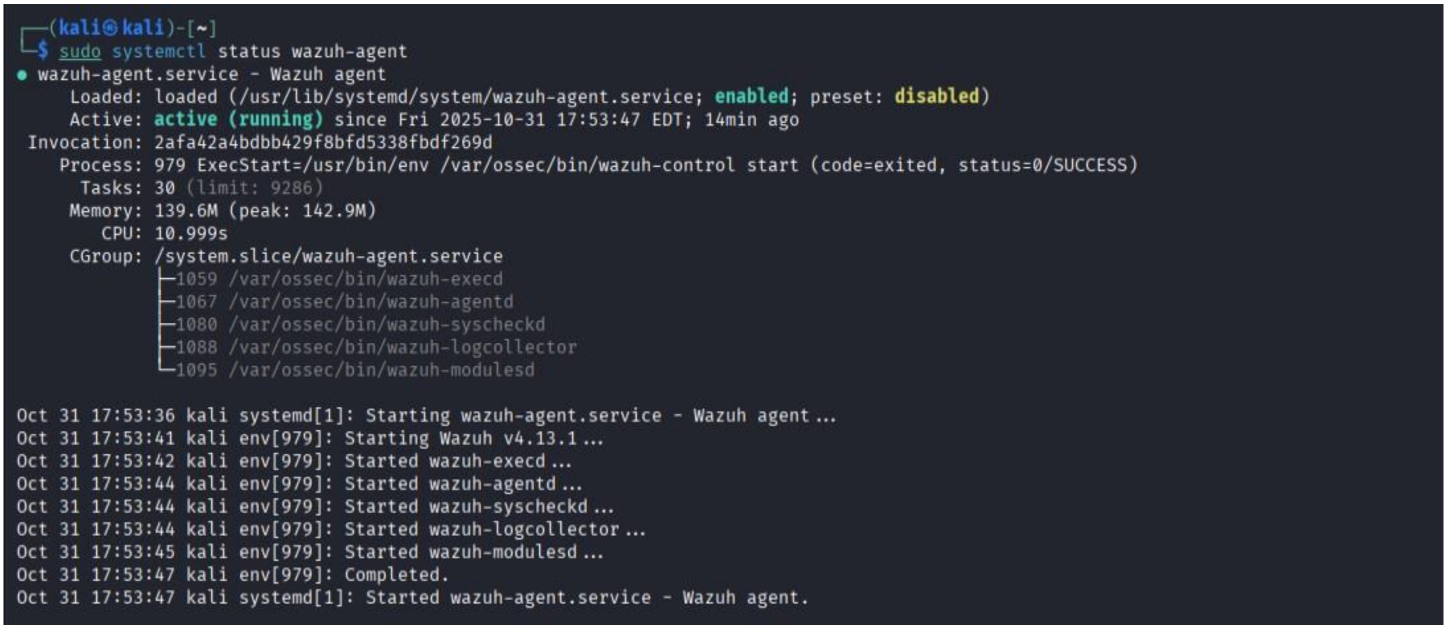
Se implementó un entorno completo de telemetría de seguridad, unificando:

- Auditd → auditoría de sistema y archivos críticos
- Suricata IDS → detección de actividad de red
- Wazuh SIEM → correlación, centralización y análisis de alertas

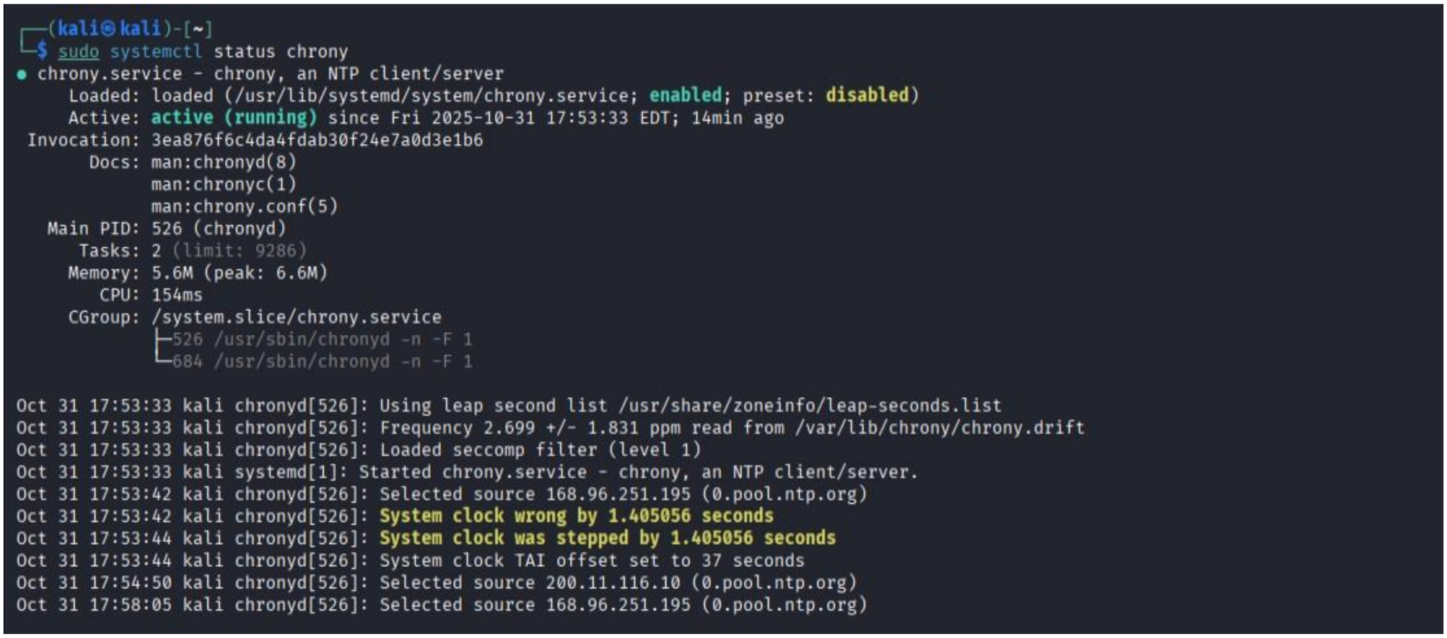
El foco estuvo en generar eventos reales (sudo, cambios en archivos, comandos, tráfico de red) y validar su detección en tiempo real)



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status wazuh-agent auditd rsyslog
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; preset: disabled)
     Active: active (running) since Thu 2025-10-30 17:34:26 EDT; 11min ago
 Invocation: 894a11c2f00847bf97b9558b672927d7
    Process: 4515 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 34 (limit: 9286)
     Memory: 1.3G (peak: 1.3G)
        CPU: 1min 19.715s
     CGroup: /system.slice/wazuh-agent.service
             ├─4537 /var/ossec/bin/wazuh-execd
             ├─4549 /var/ossec/bin/wazuh-agentd
             ├─4563 /var/ossec/bin/wazuh-syscheckd
             ├─4573 /var/ossec/bin/wazuh-logcollector
             └─4587 /var/ossec/bin/wazuh-modulesd

Oct 30 17:34:22 kali systemd[1]: Starting wazuh-agent.service - Wazuh agent...
Oct 30 17:34:22 kali env[4515]: Starting Wazuh v4.13.1...
Oct 30 17:34:23 kali env[4515]: Started wazuh-execd...
Oct 30 17:34:24 kali env[4515]: Started wazuh-agentd...
Oct 30 17:34:24 kali env[4515]: Started wazuh-syscheckd...
Oct 30 17:34:24 kali env[4515]: Started wazuh-logcollector...
Oct 30 17:34:24 kali env[4515]: Started wazuh-modulesd...
Oct 30 17:34:26 kali env[4515]: Completed.
Oct 30 17:34:26 kali systemd[1]: Started wazuh-agent.service - Wazuh agent.

● auditd.service - Security Audit Logging Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: disabled)
     Active: active (running) since Thu 2025-10-30 17:19:06 EDT; 26min ago
```



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-10-31 17:53:47 EDT; 14min ago
 Invocation: 2afa42a4bdbb429f8bfd5338fbdf269d
    Process: 979 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 30 (limit: 9286)
     Memory: 139.6M (peak: 142.9M)
        CPU: 10.999s
     CGroup: /system.slice/wazuh-agent.service
             ├─1059 /var/ossec/bin/wazuh-execd
             ├─1067 /var/ossec/bin/wazuh-agentd
             ├─1080 /var/ossec/bin/wazuh-syscheckd
             ├─1088 /var/ossec/bin/wazuh-logcollector
             └─1095 /var/ossec/bin/wazuh-modulesd

Oct 31 17:53:36 kali systemd[1]: Starting wazuh-agent.service - Wazuh agent...
Oct 31 17:53:41 kali env[979]: Starting Wazuh v4.13.1...
Oct 31 17:53:42 kali env[979]: Started wazuh-execd...
Oct 31 17:53:44 kali env[979]: Started wazuh-agentd...
Oct 31 17:53:44 kali env[979]: Started wazuh-syscheckd...
Oct 31 17:53:44 kali env[979]: Started wazuh-logcollector...
Oct 31 17:53:45 kali env[979]: Started wazuh-modulesd...
Oct 31 17:53:47 kali env[979]: Completed.
Oct 31 17:53:47 kali systemd[1]: Started wazuh-agent.service - Wazuh agent.
```



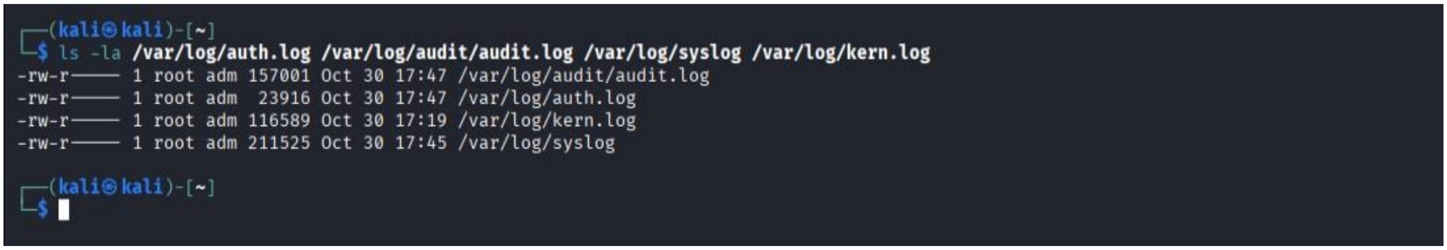
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status chrony
● chrony.service - chrony, an NTP client/server
     Loaded: loaded (/usr/lib/systemd/system/chrony.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-10-31 17:53:33 EDT; 14min ago
 Invocation: 3ea876f6c4da4fdab30f24e7a0d3e1b6
       Docs: man:chronyd(8)
             man:chronyc(1)
             man:chrony.conf(5)
   Main PID: 526 (chronyd)
      Tasks: 2 (limit: 9286)
     Memory: 5.6M (peak: 6.6M)
        CPU: 154ms
     CGroup: /system.slice/chrony.service
             ├─526 /usr/sbin/chronyd -n -F 1
             └─684 /usr/sbin/chronyd -n -F 1

Oct 31 17:53:33 kali chronyd[526]: Using leap second list /usr/share/zoneinfo/leap-seconds.list
Oct 31 17:53:33 kali chronyd[526]: Frequency 2.699 +/- 1.831 ppm read from /var/lib/chrony/chrony.drift
Oct 31 17:53:33 kali chronyd[526]: Loaded seccomp filter (level 1)
Oct 31 17:53:33 kali systemd[1]: Started chrony.service - chrony, an NTP client/server.
Oct 31 17:53:42 kali chronyd[526]: Selected source 168.96.251.195 (0.pool.ntp.org)
Oct 31 17:53:42 kali chronyd[526]: System clock wrong by 1.405056 seconds
Oct 31 17:53:44 kali chronyd[526]: System clock was stepped by 1.405056 seconds
Oct 31 17:53:44 kali chronyd[526]: System clock TAI offset set to 37 seconds
Oct 31 17:54:50 kali chronyd[526]: Selected source 200.11.116.10 (0.pool.ntp.org)
Oct 31 17:58:05 kali chronyd[526]: Selected source 168.96.251.195 (0.pool.ntp.org)
```

2. Implementación y configuración

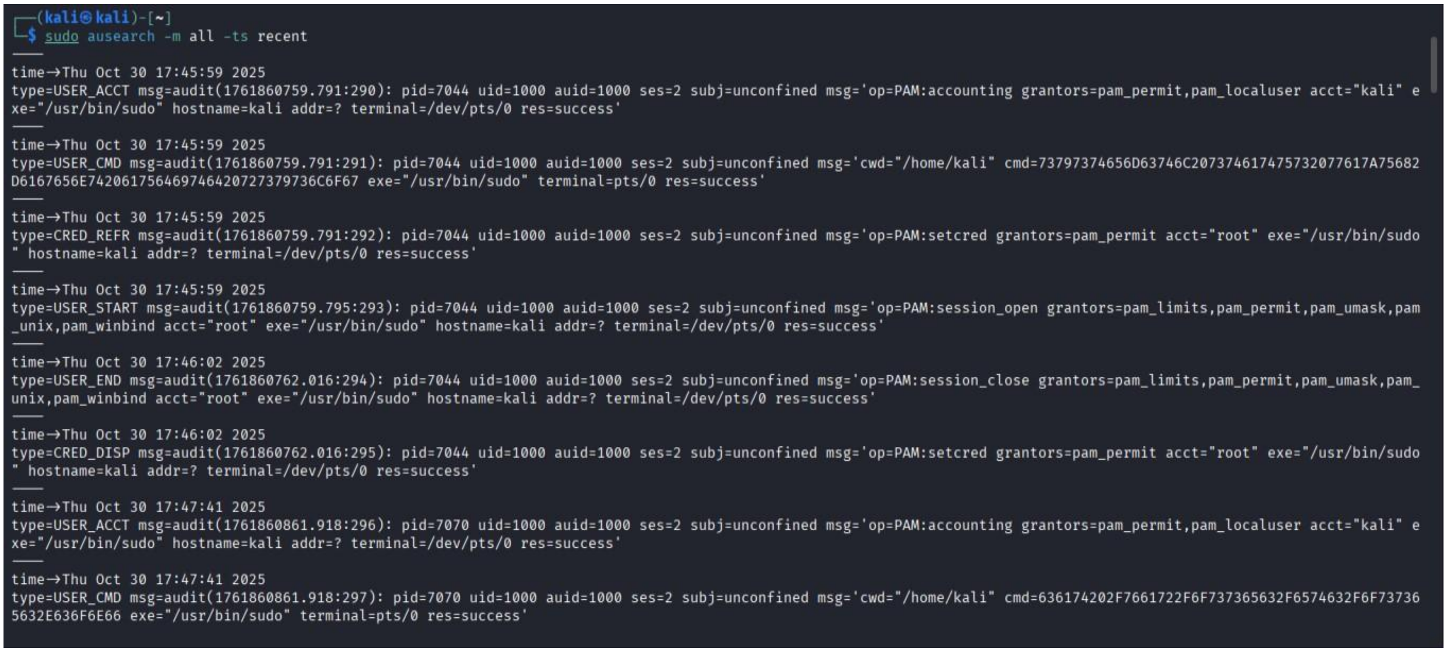
Auditd - Auditoría del sistema

Activación de reglas para:

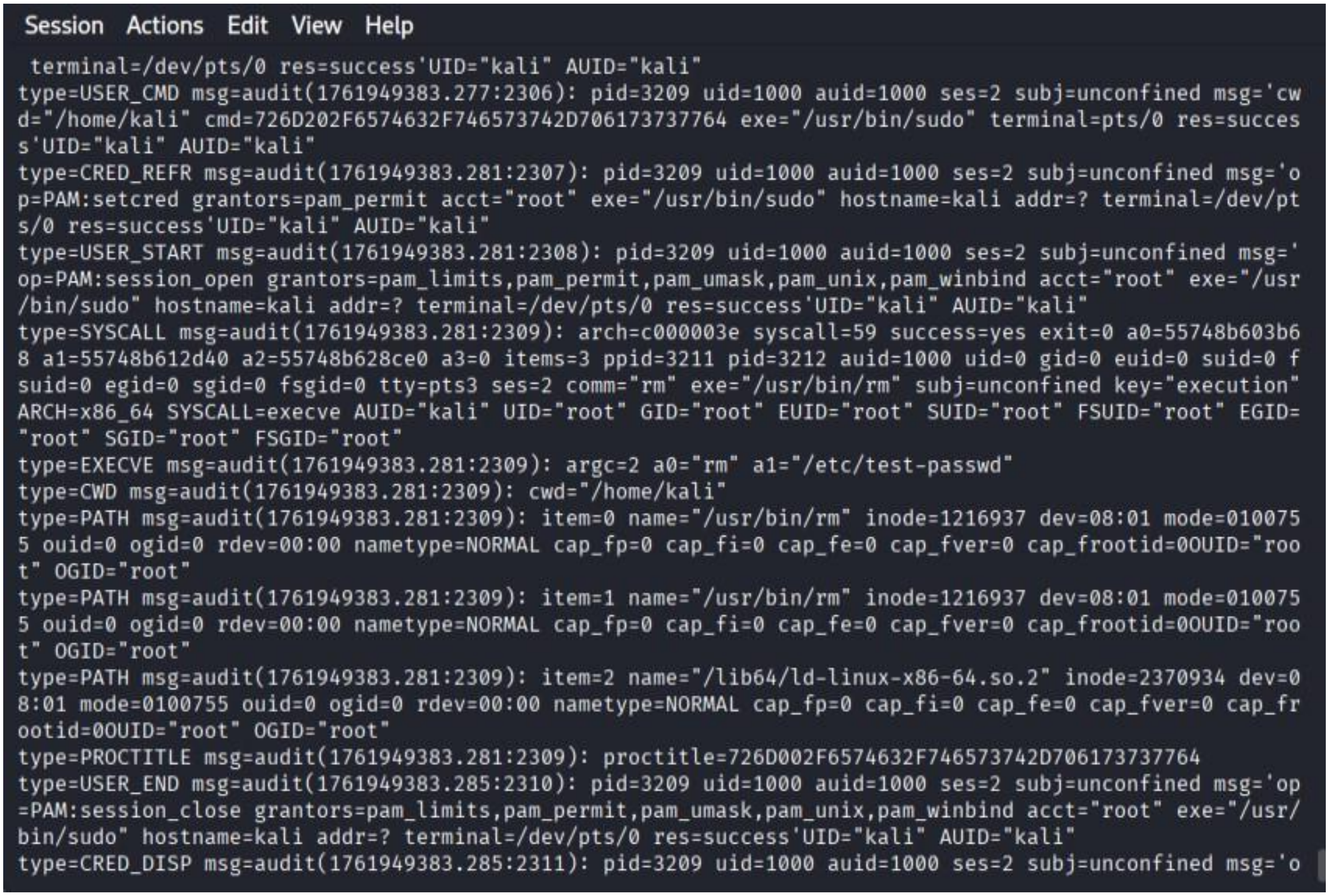
- Autenticación (auth.log, sudo)
- Ejecución de comandos
- Acceso a archivos críticos
- Acciones sospechosas (ej. rm /etc/test-passwd)
- Verificación con ausearch y audit.log
- Eventos enviados correctamente a Wazuh



```
┌──(kali㉿kali)-[~]
└─$ ls -la /var/log/auth.log /var/log/audit/audit.log /var/log/syslog /var/log/kern.log
-rw-r───── 1 root adm 157001 Oct 30 17:47 /var/log/audit/audit.log
-rw-r───── 1 root adm  23916 Oct 30 17:47 /var/log/auth.log
-rw-r───── 1 root adm 116589 Oct 30 17:19 /var/log/kern.log
-rw-r───── 1 root adm 211525 Oct 30 17:45 /var/log/syslog

┌──(kali㉿kali)-[~]
└─$ █
```



```
┌──(kali㉿kali)-[~]
└─$ sudo ausearch -m all -ts recent
----
time->Thu Oct 30 17:45:59 2025
type=USER_ACCT msg=audit(1761860759.791:290): pid=7044 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:accounting grantors=pam_permit,pam_localuser acct="kali" e
xe="/usr/bin/sudo" hostname=kali addr=? terminal=/dev/pts/0 res=success'
----
time->Thu Oct 30 17:45:59 2025
type=USER_CMD msg=audit(1761860759.791:291): pid=7044 uid=1000 auid=1000 ses=2 subj=unconfined msg='cwd="/home/kali" cmd=73797374656D63746C20737461747573207617A75682
D6167656E742061756469746420727379736C6F67 exe="/usr/bin/sudo" terminal=pts/0 res=success'
----
time->Thu Oct 30 17:45:59 2025
type=CRED_REFR msg=audit(1761860759.791:292): pid=7044 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sudo
" hostname=kali addr=? terminal=/dev/pts/0 res=success'
----
time->Thu Oct 30 17:45:59 2025
type=USER_START msg=audit(1761860759.795:293): pid=7044 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:session_open grantors=pam_limits,pam_permit,pam_umask,pam
_unix,pam_winbind acct="root" exe="/usr/bin/sudo" hostname=kali addr=? terminal=/dev/pts/0 res=success'
----
time->Thu Oct 30 17:46:02 2025
type=USER_END msg=audit(1761860762.016:294): pid=7044 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:session_close grantors=pam_limits,pam_permit,pam_umask,pam_
unix,pam_winbind acct="root" exe="/usr/bin/sudo" hostname=kali addr=? terminal=/dev/pts/0 res=success'
----
time->Thu Oct 30 17:46:02 2025
type=CRED_DISP msg=audit(1761860762.016:295): pid=7044 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sudo
" hostname=kali addr=? terminal=/dev/pts/0 res=success'
----
time->Thu Oct 30 17:47:41 2025
type=USER_ACCT msg=audit(1761860861.918:296): pid=7070 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:accounting grantors=pam_permit,pam_localuser acct="kali" e
xe="/usr/bin/sudo" hostname=kali addr=? terminal=/dev/pts/0 res=success'
----
time->Thu Oct 30 17:47:41 2025
type=USER_CMD msg=audit(1761860861.918:297): pid=7070 uid=1000 auid=1000 ses=2 subj=unconfined msg='cwd="/home/kali" cmd=636174202F7661722F6F737365632F6574632F6F73736
5632E636F6E66 exe="/usr/bin/sudo" terminal=pts/0 res=success'
```

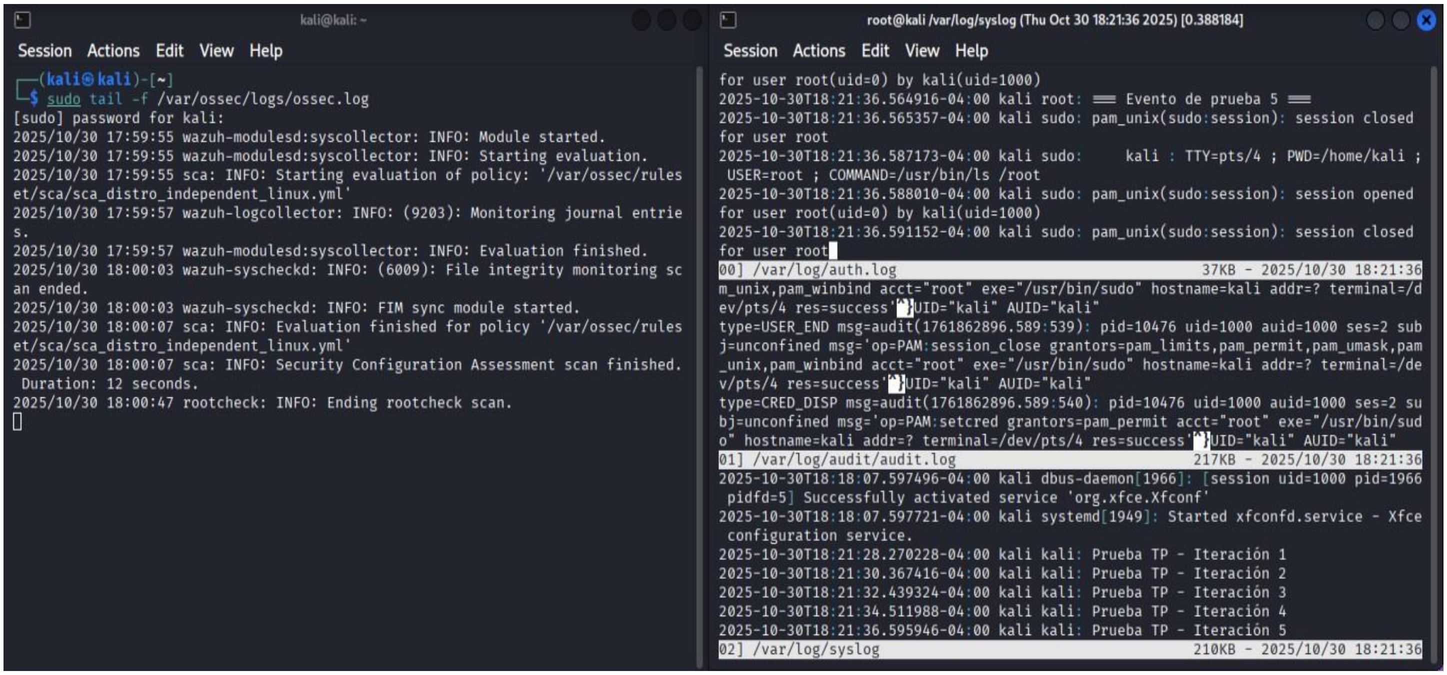


```
 terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=USER_CMD msg=audit(1761949383.277:2306): pid=3209 uid=1000 auid=1000 ses=2 subj=unconfined msg='cw
d="/home/kali" cmd=726D202F6574632F746573742D706173737764 exe="/usr/bin/sudo" terminal=pts/0 res=succes
s'UID="kali" AUID="kali"
type=CRED_REFR msg=audit(1761949383.281:2307): pid=3209 uid=1000 auid=1000 ses=2 subj=unconfined msg='o
p=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sudo" hostname=kali addr=? terminal=/dev/pt
s/0 res=success'UID="kali" AUID="kali"
type=USER_START msg=audit(1761949383.281:2308): pid=3209 uid=1000 auid=1000 ses=2 subj=unconfined msg='
op=PAM:session_open grantors=pam_limits,pam_permit,pam_umask,pam_unix,pam_winbind acct="root" exe="/usr
/bin/sudo" hostname=kali addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=SYSCALL msg=audit(1761949383.281:2309): arch=c000003e syscall=59 success=yes exit=0 a0=55748b603b6
8 a1=55748b612d40 a2=55748b628ce0 a3=0 items=3 ppid=3211 pid=3212 auid=1000 uid=0 gid=0 euid=0 suid=0 f
suid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=2 comm="rm" exe="/usr/bin/rm" subj=unconfined key="execution"
ARCH=x86_64 SYSCALL=execve AUID="kali" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID=
"root" SGID="root" FSGID="root"
type=EXECVE msg=audit(1761949383.281:2309): argc=2 a0="rm" a1="/etc/test-passwd"
type=CWD msg=audit(1761949383.281:2309): cwd="/home/kali"
type=PATH msg=audit(1761949383.281:2309): item=0 name="/usr/bin/rm" inode=1216937 dev=08:01 mode=010075
5 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="roo
t" OGID="root"
type=PATH msg=audit(1761949383.281:2309): item=1 name="/usr/bin/rm" inode=1216937 dev=08:01 mode=010075
5 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="roo
t" OGID="root"
type=PATH msg=audit(1761949383.281:2309): item=2 name="/lib64/ld-linux-x86-64.so.2" inode=2370934 dev=0
8:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_fr
ootid=0OUID="root" OGID="root"
type=PROCTITLE msg=audit(1761949383.281:2309): proctitle=726D002F6574632F746573742D706173737764
type=USER_END msg=audit(1761949383.285:2310): pid=3209 uid=1000 auid=1000 ses=2 subj=unconfined msg='op
=PAM:session_close grantors=pam_limits,pam_permit,pam_umask,pam_unix,pam_winbind acct="root" exe="/usr/
bin/sudo" hostname=kali addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=CRED_DISP msg=audit(1761949383.285:2311): pid=3209 uid=1000 auid=1000 ses=2 subj=unconfined msg='o
```

Wazuh - Recolección y correlación

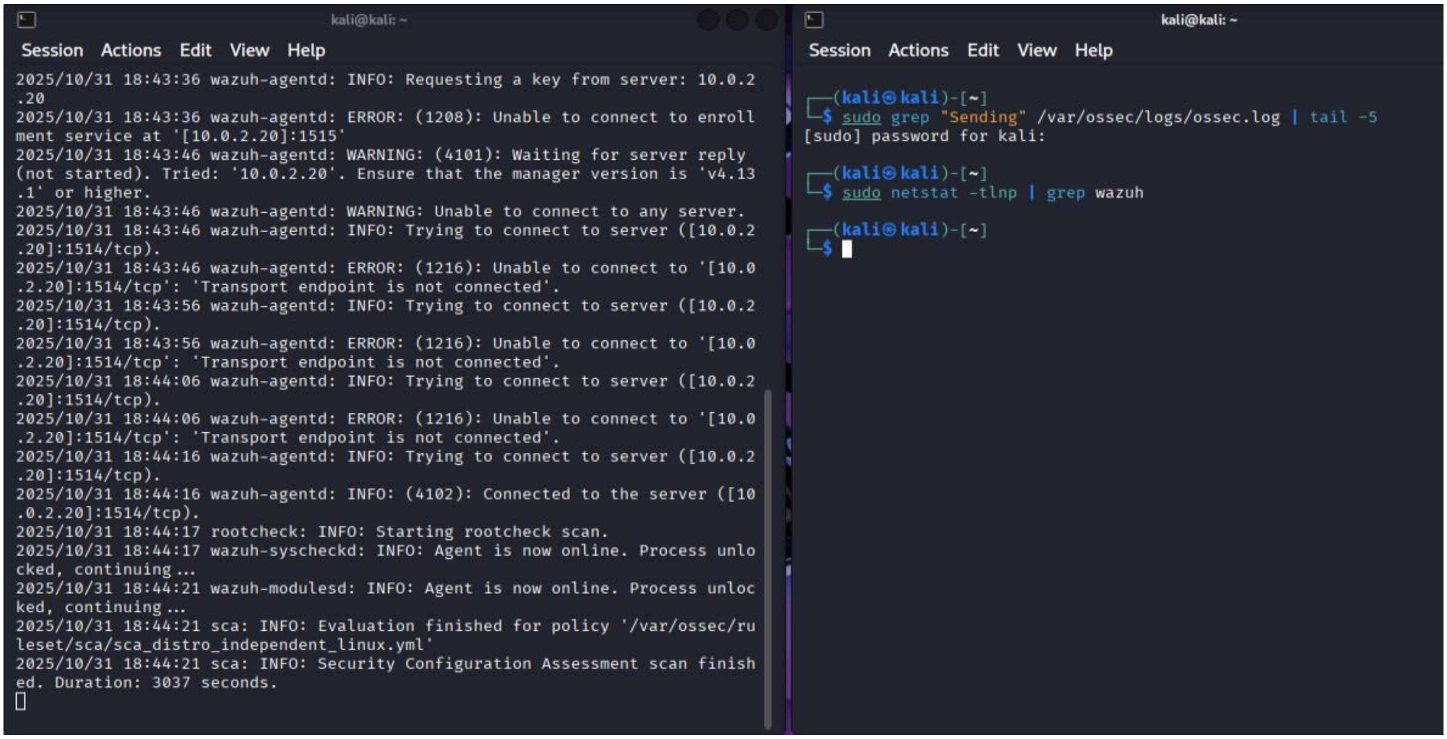
Configuración de localfile para logs locales. Detección en tiempo real de:

- Sesiones sudo
- Comandos logger
- Fallos de autenticación
- Cambios en integridad


kali@kali: ~
Session Actions Edit View Help
root@kali /var/log/syslog (Thu Oct 30 18:21:36 2025) [0.388184]
Session Actions Edit View Help

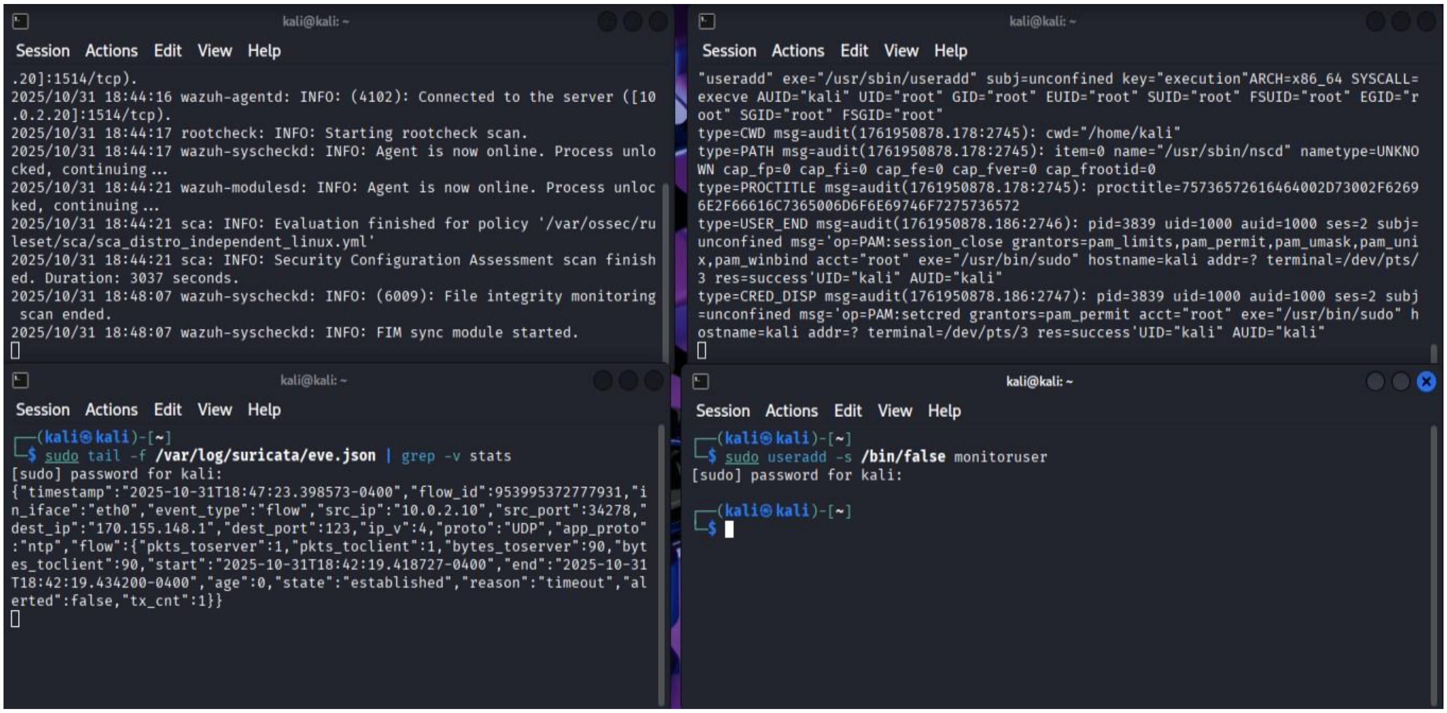
```
┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/ossec/logs/ossec.log
[sudo] password for kali:
2025/10/30 17:59:55 wazuh-modulesd:syscollector: INFO: Module started.
2025/10/30 17:59:55 wazuh-modulesd:syscollector: INFO: Starting evaluation.
2025/10/30 17:59:55 sca: INFO: Starting evaluation of policy: '/var/ossec/rules
et/sca/sca_distro_independent_linux.yml'
2025/10/30 17:59:57 wazuh-logcollector: INFO: (9203): Monitoring journal entrie
s.
2025/10/30 17:59:57 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2025/10/30 18:00:03 wazuh-syscheckd: INFO: (6009): File integrity monitoring sc
an ended.
2025/10/30 18:00:03 wazuh-syscheckd: INFO: FIM sync module started.
2025/10/30 18:00:07 sca: INFO: Evaluation finished for policy '/var/ossec/rules
et/sca/sca_distro_independent_linux.yml'
2025/10/30 18:00:07 sca: INFO: Security Configuration Assessment scan finished.
 Duration: 12 seconds.
2025/10/30 18:00:47 rootcheck: INFO: Ending rootcheck scan.
▯
```

```
for user root(uid=0) by kali(uid=1000)
2025-10-30T18:21:36.564916-04:00 kali root: ══ Evento de prueba 5 ══
2025-10-30T18:21:36.565357-04:00 kali sudo: pam_unix(sudo:session): session closed
for user root
2025-10-30T18:21:36.587173-04:00 kali sudo:     kali : TTY=pts/4 ; PWD=/home/kali ;
 USER=root ; COMMAND=/usr/bin/ls /root
2025-10-30T18:21:36.588010-04:00 kali sudo: pam_unix(sudo:session): session opened
for user root(uid=0) by kali(uid=1000)
2025-10-30T18:21:36.591152-04:00 kali sudo: pam_unix(sudo:session): session closed
for user root
00] /var/log/auth.log                                  37KB - 2025/10/30 18:21:36
m_unix,pam_winbind acct="root" exe="/usr/bin/sudo" hostname=kali addr=? terminal=/d
ev/pts/4 res=success'^]UID="kali" AUID="kali"
type=USER_END msg=audit(1761862896.589:539): pid=10476 uid=1000 auid=1000 ses=2 sub
j=unconfined msg='op=PAM:session_close grantors=pam_limits,pam_permit,pam_umask,pam
_unix,pam_winbind acct="root" exe="/usr/bin/sudo" hostname=kali addr=? terminal=/de
v/pts/4 res=success'^]UID="kali" AUID="kali"
type=CRED_DISP msg=audit(1761862896.589:540): pid=10476 uid=1000 auid=1000 ses=2 su
bj=unconfined msg='op=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sud
o" hostname=kali addr=? terminal=/dev/pts/4 res=success'^]UID="kali" AUID="kali"
01] /var/log/audit/audit.log                          217KB - 2025/10/30 18:21:36
2025-10-30T18:18:07.597496-04:00 kali dbus-daemon[1966]: [session uid=1000 pid=1966
 pidfd=5] Successfully activated service 'org.xfce.Xfconf'
2025-10-30T18:18:07.597721-04:00 kali systemd[1949]: Started xfconfd.service - Xfce
 configuration service.
2025-10-30T18:21:28.270228-04:00 kali kali: Prueba TP - Iteración 1
2025-10-30T18:21:30.367416-04:00 kali kali: Prueba TP - Iteración 2
2025-10-30T18:21:32.439324-04:00 kali kali: Prueba TP - Iteración 3
2025-10-30T18:21:34.511988-04:00 kali kali: Prueba TP - Iteración 4
2025-10-30T18:21:36.595946-04:00 kali kali: Prueba TP - Iteración 5
02] /var/log/syslog                                   210KB - 2025/10/30 18:21:36
```


kali@kali: ~
Session Actions Edit View Help
kali@kali: ~
Session Actions Edit View Help

```
2025/10/31 18:43:36 wazuh-agentd: INFO: Requesting a key from server: 10.0.2
.20
2025/10/31 18:43:36 wazuh-agentd: ERROR: (1208): Unable to connect to enroll
ment service at '[10.0.2.20]:1515'
2025/10/31 18:43:46 wazuh-agentd: WARNING: (4101): Waiting for server reply
(not started). Tried: '10.0.2.20'. Ensure that the manager version is 'v4.13
.1' or higher.
2025/10/31 18:43:46 wazuh-agentd: WARNING: Unable to connect to any server.
2025/10/31 18:43:46 wazuh-agentd: INFO: Trying to connect to server ([10.0.2
.20]:1514/tcp).
2025/10/31 18:43:46 wazuh-agentd: ERROR: (1216): Unable to connect to '[10.0
.2.20]:1514/tcp': 'Transport endpoint is not connected'.
2025/10/31 18:43:56 wazuh-agentd: INFO: Trying to connect to server ([10.0.2
.20]:1514/tcp).
2025/10/31 18:43:56 wazuh-agentd: ERROR: (1216): Unable to connect to '[10.0
.2.20]:1514/tcp': 'Transport endpoint is not connected'.
2025/10/31 18:44:06 wazuh-agentd: INFO: Trying to connect to server ([10.0.2
.20]:1514/tcp).
2025/10/31 18:44:06 wazuh-agentd: ERROR: (1216): Unable to connect to '[10.0
.2.20]:1514/tcp': 'Transport endpoint is not connected'.
2025/10/31 18:44:16 wazuh-agentd: INFO: Trying to connect to server ([10.0.2
.20]:1514/tcp).
2025/10/31 18:44:16 wazuh-agentd: INFO: (4102): Connected to the server ([10
.0.2.20]:1514/tcp).
2025/10/31 18:44:17 rootcheck: INFO: Starting rootcheck scan.
2025/10/31 18:44:17 wazuh-syscheckd: INFO: Agent is now online. Process unlo
cked, continuing ...
2025/10/31 18:44:21 wazuh-modulesd: INFO: Agent is now online. Process unloc
ked, continuing ...
2025/10/31 18:44:21 sca: INFO: Evaluation finished for policy '/var/ossec/ru
leset/sca/sca_distro_independent_linux.yml'
2025/10/31 18:44:21 sca: INFO: Security Configuration Assessment scan finish
ed. Duration: 3037 seconds.
▯
```

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "Sending" /var/ossec/logs/ossec.log | tail -5
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo netstat -tlnp | grep wazuh

┌──(kali㉿kali)-[~]
└─$ █
```



```
.20]:1514/tcp).
2025/10/31 18:44:16 wazuh-agentd: INFO: (4102): Connected to the server ([10
.0.2.20]:1514/tcp).
2025/10/31 18:44:17 rootcheck: INFO: Starting rootcheck scan.
2025/10/31 18:44:17 wazuh-syscheckd: INFO: Agent is now online. Process unlo
cked, continuing ...
2025/10/31 18:44:21 wazuh-modulesd: INFO: Agent is now online. Process unloc
ked, continuing ...
2025/10/31 18:44:21 sca: INFO: Evaluation finished for policy '/var/ossec/ru
leset/sca/sca_distro_independent_linux.yml'
2025/10/31 18:44:21 sca: INFO: Security Configuration Assessment scan finish
ed. Duration: 3037 seconds.
2025/10/31 18:48:07 wazuh-syscheckd: INFO: (6009): File integrity monitoring
 scan ended.
2025/10/31 18:48:07 wazuh-syscheckd: INFO: FIM sync module started.
```

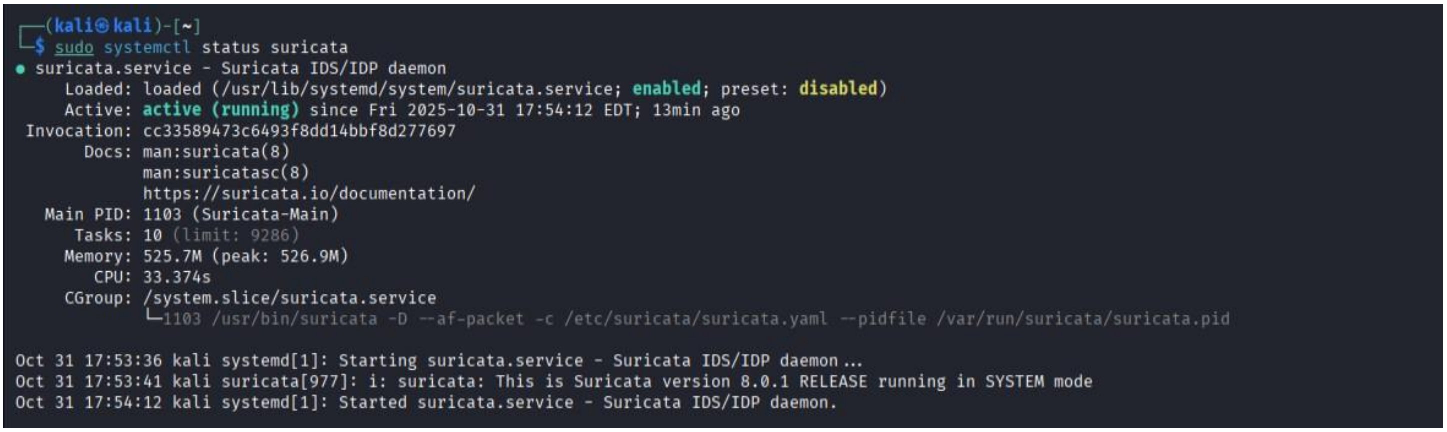
```
"useradd" exe="/usr/sbin/useradd" subj=unconfined key="execution"ARCH=x86_64 SYSCALL=
execve AUID="kali" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="r
oot" SGID="root" FSGID="root"
type=CWD msg=audit(1761950878.178:2745): cwd="/home/kali"
type=PATH msg=audit(1761950878.178:2745): item=0 name="/usr/sbin/nscd" nametype=UNKNO
WN cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PROCTITLE msg=audit(1761950878.178:2745): proctitle=757365726164002D73002F6269
6E2F66616C7365006D6F6E69746F7275736572
type=USER_END msg=audit(1761950878.186:2746): pid=3839 uid=1000 auid=1000 ses=2 subj=
unconfined msg='op=PAM:session_close grantors=pam_limits,pam_permit,pam_umask,pam_uni
x,pam_winbind acct="root" exe="/usr/bin/sudo" hostname=kali addr=? terminal=/dev/pts/
3 res=success'UID="kali" AUID="kali"
type=CRED_DISP msg=audit(1761950878.186:2747): pid=3839 uid=1000 auid=1000 ses=2 subj
=unconfined msg='op=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sudo" h
ostname=kali addr=? terminal=/dev/pts/3 res=success'UID="kali" AUID="kali"
```

```
┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/suricata/eve.json | grep -v stats
[sudo] password for kali:
{"timestamp":"2025-10-31T18:47:23.398573-0400","flow_id":953995372777931,"i
n_iface":"eth0","event_type":"flow","src_ip":"10.0.2.10","src_port":34278,"
dest_ip":"170.155.148.1","dest_port":123,"ip_v":4,"proto":"UDP","app_proto"
:"ntp","flow":{"pkts_toserver":1,"pkts_toclient":1,"bytes_toserver":90,"byt
es_toclient":90,"start":"2025-10-31T18:42:19.418727-0400","end":"2025-10-31
T18:42:19.434200-0400","age":0,"state":"established","reason":"timeout","al
erted":false,"tx_cnt":1}}
```

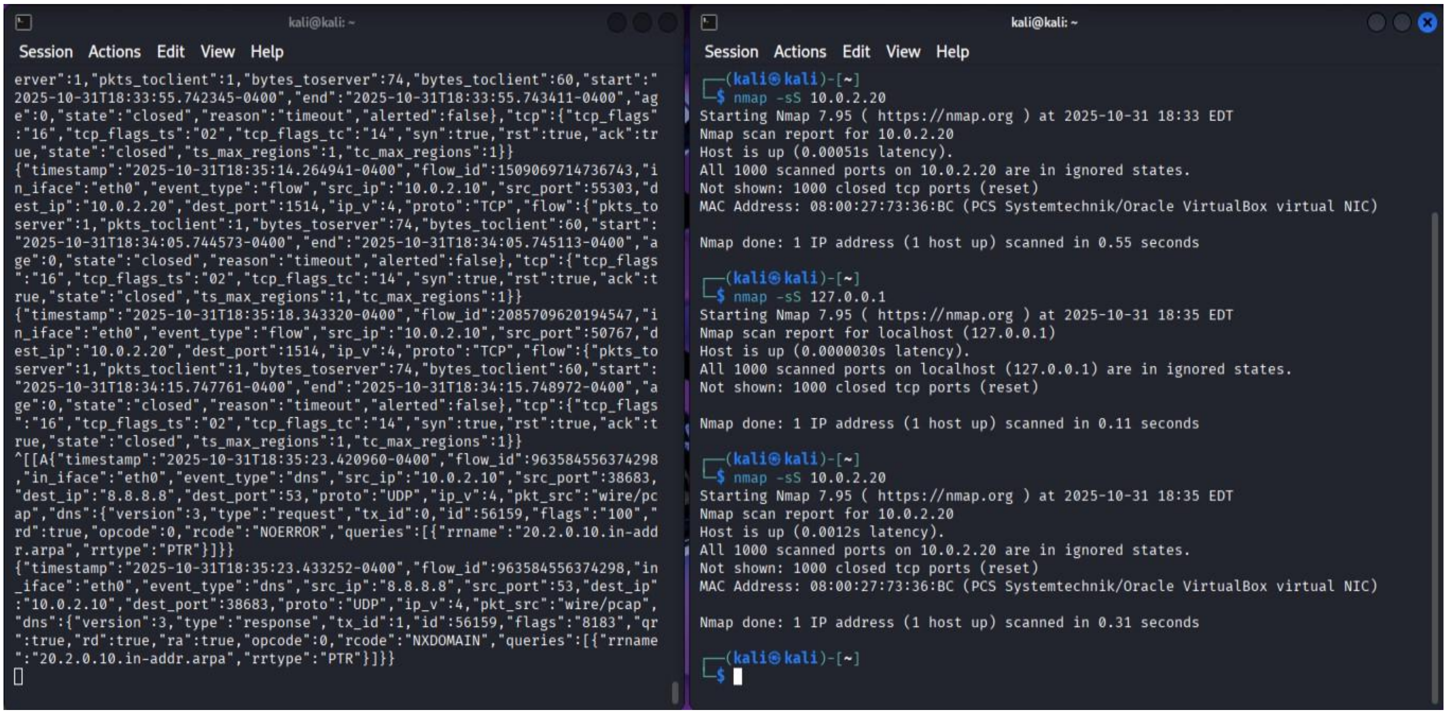
```
┌──(kali㉿kali)-[~]
└─$ sudo useradd -s /bin/false monitoruser
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ 
```

Suricata - Telemetría de red

- Activación del modo AF-Packet (eth0)
- Captura de tráfico TCP/UDP y eventos HTTP/HTTPS
- Generación de alertas de seguridad
- Integración con Wazuh para correlación



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-10-31 17:54:12 EDT; 13min ago
 Invocation: cc33589473c6493f8dd14bbf8d277697
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
   Main PID: 1103 (Suricata-Main)
      Tasks: 10 (limit: 9286)
     Memory: 525.7M (peak: 526.9M)
        CPU: 33.374s
     CGroup: /system.slice/suricata.service
             └─1103 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata/suricata.pid

Oct 31 17:53:36 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon ...
Oct 31 17:53:41 kali suricata[977]: i: suricata: This is Suricata version 8.0.1 RELEASE running in SYSTEM mode
Oct 31 17:54:12 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
```


kali@kali: ~
Session Actions Edit View Help
kali@kali: ~
Session Actions Edit View Help

```
erver":1,"pkts_toclient":1,"bytes_toserver":74,"bytes_toclient":60,"start":"
2025-10-31T18:33:55.742345-0400","end":"2025-10-31T18:33:55.743411-0400","ag
e":0,"state":"closed","reason":"timeout","alerted":false},"tcp":{"tcp_flags"
:"16","tcp_flags_ts":"02","tcp_flags_tc":"14","syn":true,"rst":true,"ack":tr
ue,"state":"closed","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-10-31T18:35:14.264941-0400","flow_id":1509069714736743,"i
n_iface":"eth0","event_type":"flow","src_ip":"10.0.2.10","src_port":55303,"d
est_ip":"10.0.2.20","dest_port":1514,"ip_v":4,"proto":"TCP","flow":{"pkts_to
server":1,"pkts_toclient":1,"bytes_toserver":74,"bytes_toclient":60,"start":
"2025-10-31T18:34:05.744573-0400","end":"2025-10-31T18:34:05.745113-0400","a
ge":0,"state":"closed","reason":"timeout","alerted":false},"tcp":{"tcp_flags
":"16","tcp_flags_ts":"02","tcp_flags_tc":"14","syn":true,"rst":true,"ack":t
rue,"state":"closed","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2025-10-31T18:35:18.343320-0400","flow_id":2085709620194547,"i
n_iface":"eth0","event_type":"flow","src_ip":"10.0.2.10","src_port":50767,"d
est_ip":"10.0.2.20","dest_port":1514,"ip_v":4,"proto":"TCP","flow":{"pkts_to
server":1,"pkts_toclient":1,"bytes_toserver":74,"bytes_toclient":60,"start":
"2025-10-31T18:34:15.747761-0400","end":"2025-10-31T18:34:15.748972-0400","a
ge":0,"state":"closed","reason":"timeout","alerted":false},"tcp":{"tcp_flags
":"16","tcp_flags_ts":"02","tcp_flags_tc":"14","syn":true,"rst":true,"ack":t
rue,"state":"closed","ts_max_regions":1,"tc_max_regions":1}}
^[[A{"timestamp":"2025-10-31T18:35:23.420960-0400","flow_id":963584556374298
,"in_iface":"eth0","event_type":"dns","src_ip":"10.0.2.10","src_port":38683,
"dest_ip":"8.8.8.8","dest_port":53,"proto":"UDP","ip_v":4,"pkt_src":"wire/pc
ap","dns":{"version":3,"type":"request","tx_id":0,"id":56159,"flags":"100","
rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"20.2.0.10.in-add
r.arpa","rrtype":"PTR"}]}}
{"timestamp":"2025-10-31T18:35:23.433252-0400","flow_id":963584556374298,"in
_iface":"eth0","event_type":"dns","src_ip":"8.8.8.8","src_port":53,"dest_ip"
:"10.0.2.10","dest_port":38683,"proto":"UDP","ip_v":4,"pkt_src":"wire/pcap",
"dns":{"version":3,"type":"response","tx_id":1,"id":56159,"flags":"8183","qr
":true,"rd":true,"ra":true,"opcode":0,"rcode":"NXDOMAIN","queries":[{"rrname
":"20.2.0.10.in-addr.arpa","rrtype":"PTR"}]}}
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 10.0.2.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 18:33 EDT
Nmap scan report for 10.0.2.20
Host is up (0.00051s latency).
All 1000 scanned ports on 10.0.2.20 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:73:36:BC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 18:35 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS 10.0.2.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 18:35 EDT
Nmap scan report for 10.0.2.20
Host is up (0.0012s latency).
All 1000 scanned ports on 10.0.2.20 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:73:36:BC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Sincronización NTP

- Tiempos unificados para evitar desajustes en alertas

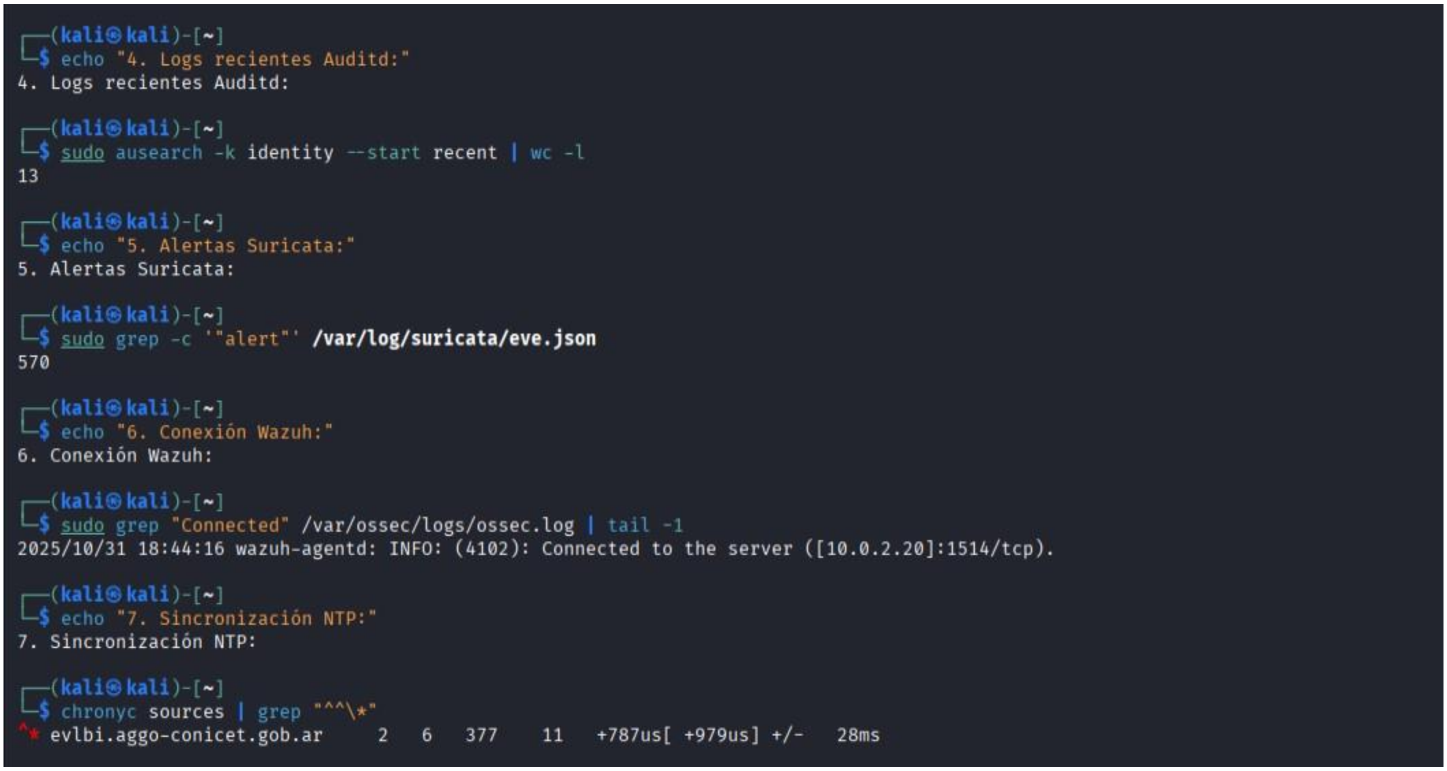
3. Resultados principales

El laboratorio validó la telemetría end-to-end del endpoint hacia el SIEM, demostrando detección efectiva de:

- Cambios en archivos críticos
- Comandos privilegiados (sudo)
- Ejecución de binarios
- Intentos de autenticación
- Tráfico sospechoso detectado por Suricata

Métricas finales:

- 13 eventos de auditoría recientes
- 570 alertas de Suricata
- Agente Wazuh totalmente operativo



```
┌──(kali㉿kali)-[~]
└─$ echo "4. Logs recientes Auditd:"
4. Logs recientes Auditd:

┌──(kali㉿kali)-[~]
└─$ sudo ausearch -k identity --start recent | wc -l
13

┌──(kali㉿kali)-[~]
└─$ echo "5. Alertas Suricata:"
5. Alertas Suricata:

┌──(kali㉿kali)-[~]
└─$ sudo grep -c '"alert"' /var/log/suricata/eve.json
570

┌──(kali㉿kali)-[~]
└─$ echo "6. Conexión Wazuh:"
6. Conexión Wazuh:

┌──(kali㉿kali)-[~]
└─$ sudo grep "Connected" /var/ossec/logs/ossec.log | tail -1
2025/10/31 18:44:16 wazuh-agentd: INFO: (4102): Connected to the server ([10.0.2.20]:1514/tcp).

┌──(kali㉿kali)-[~]
└─$ echo "7. Sincronización NTP:"
7. Sincronización NTP:

┌──(kali㉿kali)-[~]
└─$ chronyc sources | grep "^^\*"
^* evlbi.aggo-conicet.gob.ar     2   6   377    11   +787us[ +979us] +/-   28ms
```

4. Resumen final

Se logró la correcta integración entre auditoría del sistema, telemetría de red y correlación SIEM. Se reforzaron conceptos clave como:

- Recolección avanzada de logs
- Auditoría con reglas específicas en Linux
- Integración IDS + SIEM
- Validación de seguridad basada en eventos reales