Instrumentación y Telemetría

Autora: Ingrid K.

Fecha: noviembre 2025.

Clasificación: Confidencial – Uso interno.

Alcance: Entorno de laboratorio aislado.

Máquinas involucradas:

Kali Linux (10.0.2.10).

Wazuh (10.0.2.20).

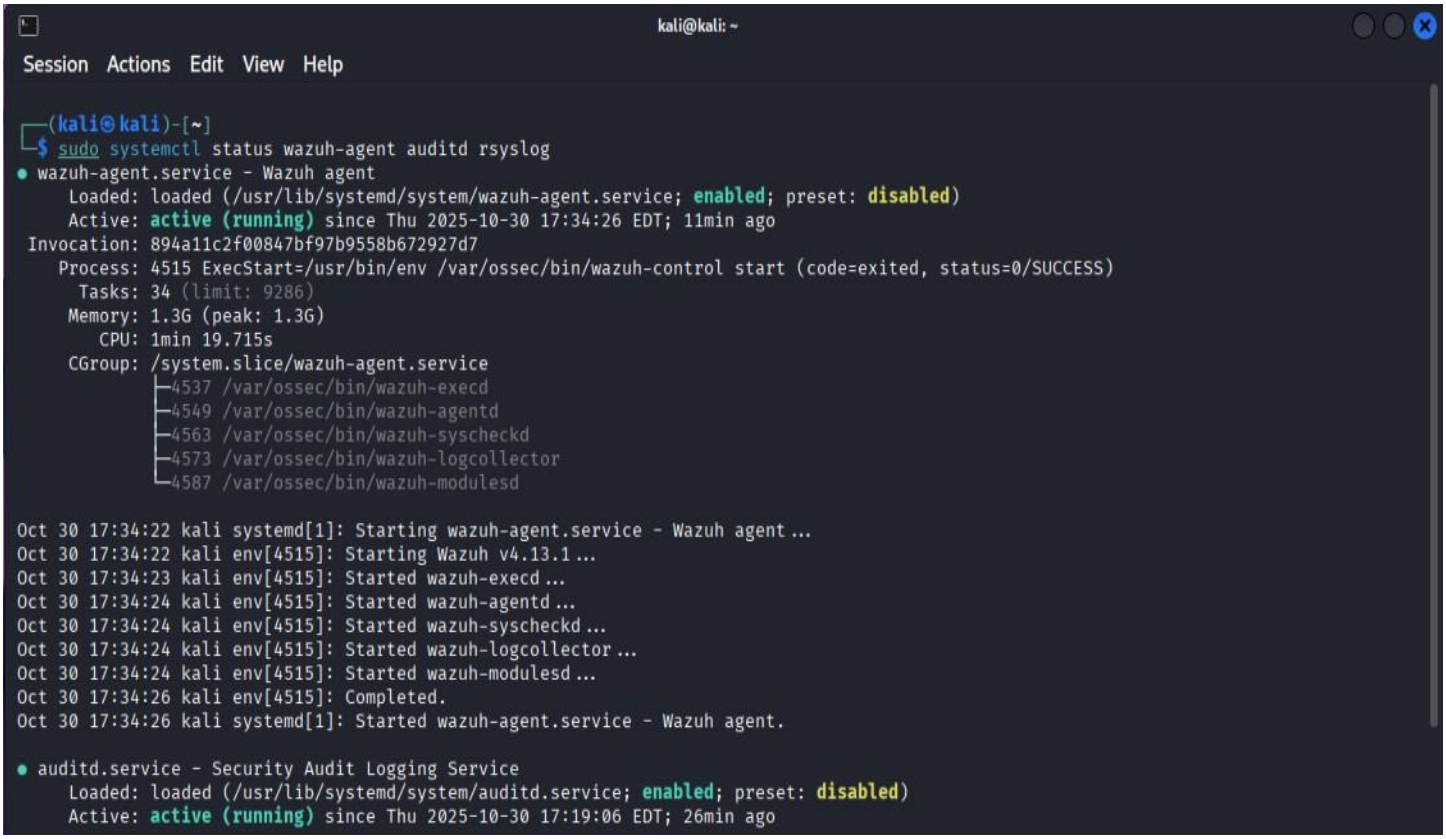
Objetivo

Implementar un sistema completo de telemetría y monitoreo de seguridad que incluya:

- Linux: Activación de auditd y reglas de auditoría, habilitación de logs de auth/sudo/kernel.
- Sensor de red: Despliegue de Suricata para generación de alertas IDS/NSM.
- Centralización: Envío de logs a Wazuh SIEM con timestamps sincronizados vía NTP.

La telemetría es la técnica que permite recopilar, medir y transmitir datos de forma remota y automática a una ubicación central para su análisis.

Evidencia 1: El agente de Wazuh funcionando correctamente.



Evidencia 2: Configuración de localfile para la monitorización proactiva.

```
(kali㉿kali)-[~]
$ sudo cat /var/ossec/etc/ossec.conf | grep -A 3 -B 1 "localfile"
  <!-- Log analysis -->
  <localfile>
    <log_format>command</log_format>
    <command>df -P</command>
    <frequency>360</frequency>
  </localfile>

  <localfile>
    <log_format>full_command</log_format>
    <command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).
\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 == \3 == \4 \5/' | sort -k 4 -g | sed 's/ == \(.*\) ==/:\1/' | sed 1,2d</command>
    <alias>netstat listening ports</alias>
    <frequency>360</frequency>
  </localfile>

  <localfile>
    <log_format>full_command</log_format>
    <command>last -n 20</command>
    <frequency>360</frequency>
  </localfile>

  <!-- Active response -->
  <active-response>
--
```

Evidencia 3: Configuración de localfile para la monitorización proactiva.

```
  <localfile>
    <log_format>journald</log_format>
    <location>journald</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/nginx/access.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/nginx/error.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/error.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
```

Evidencia 4: Archivos de log críticos del sistema para auditoría de seguridad.

```
┌──(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)-[~]
└─$
```

Evidencia 5: Simulación de actividades para auditoría.

```
┌──(kali㉿kali)-[~]
└─$ echo "== INICIO PRUEBAS AUTH ==" | sudo tee -a /var/log/auth.log
== INICIO PRUEBAS AUTH ==

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

┌──(kali㉿kali)-[~]
└─$ sudo su - kali
┌──(kali㉿kali)-[~]
└─$ sudo ls /root
[sudo] password for kali:
wazuh-certs

┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/auth.log
2025-10-30T17:51:36.265535-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2025-10-30T17:51:44.797231-04:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/su - kali
2025-10-30T17:51:44.797827-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-10-30T17:51:44.835235-04:00 kali su[7150]: (to kali) root on pts/1
2025-10-30T17:51:44.881367-04:00 kali su[7150]: pam_unix(su-l:session): session opened for user kali(uid=1000) by kali(uid=0)
2025-10-30T17:51:55.297626-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/ls /root
2025-10-30T17:51:55.298214-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-10-30T17:51:55.299781-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2025-10-30T17:52:06.187775-04:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-10-30T17:52:06.188613-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
```

Evidencia 6: Prueba de monitorización, generación de eventos en auth.log.

```
┌──(kali㉿kali)-[~]
└─$ echo "═══ INICIO PRUEBAS AUDIT ═══" | sudo logger -p auth.info

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

┌──(kali㉿kali)-[~]
└─$ sudo chmod 777 /tmp/archivo_prueba_audit.txt

┌──(kali㉿kali)-[~]
└─$ echo "dato de prueba" | sudo tee /tmp/archivo_prueba_audit.txt
dato de prueba

┌──(kali㉿kali)-[~]
└─$ sudo rm /tmp/archivo_prueba_audit.txt
```

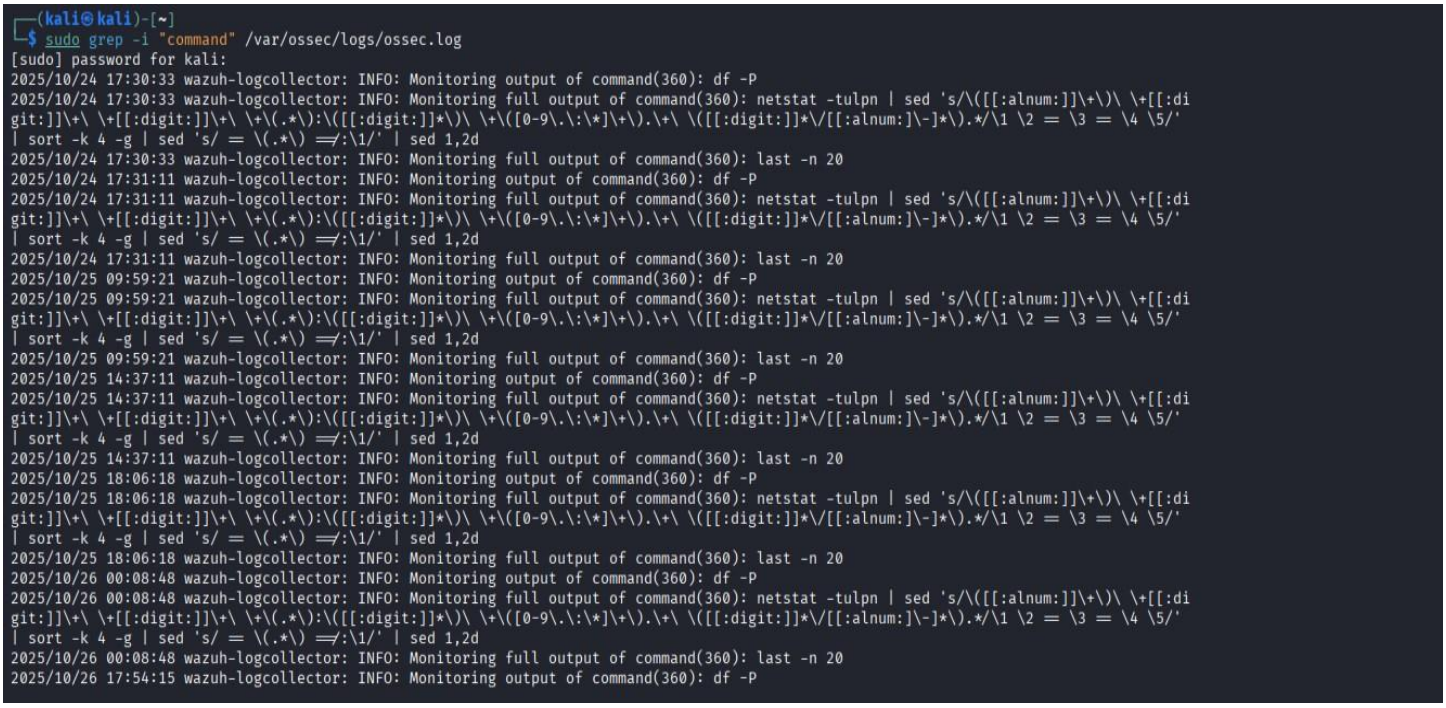
Evidencia 7: Salida de ausearch mostrando eventos de auditoría del sistema.

```
┌──(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=73797374656D63746C2073746174757320776174A75682
D6167656E74206175646974642072737973 6C6F67 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'
```

Evidencia 8: Monitoreo de audit.log con tail -f, mostrando eventos de auditoría detallados.

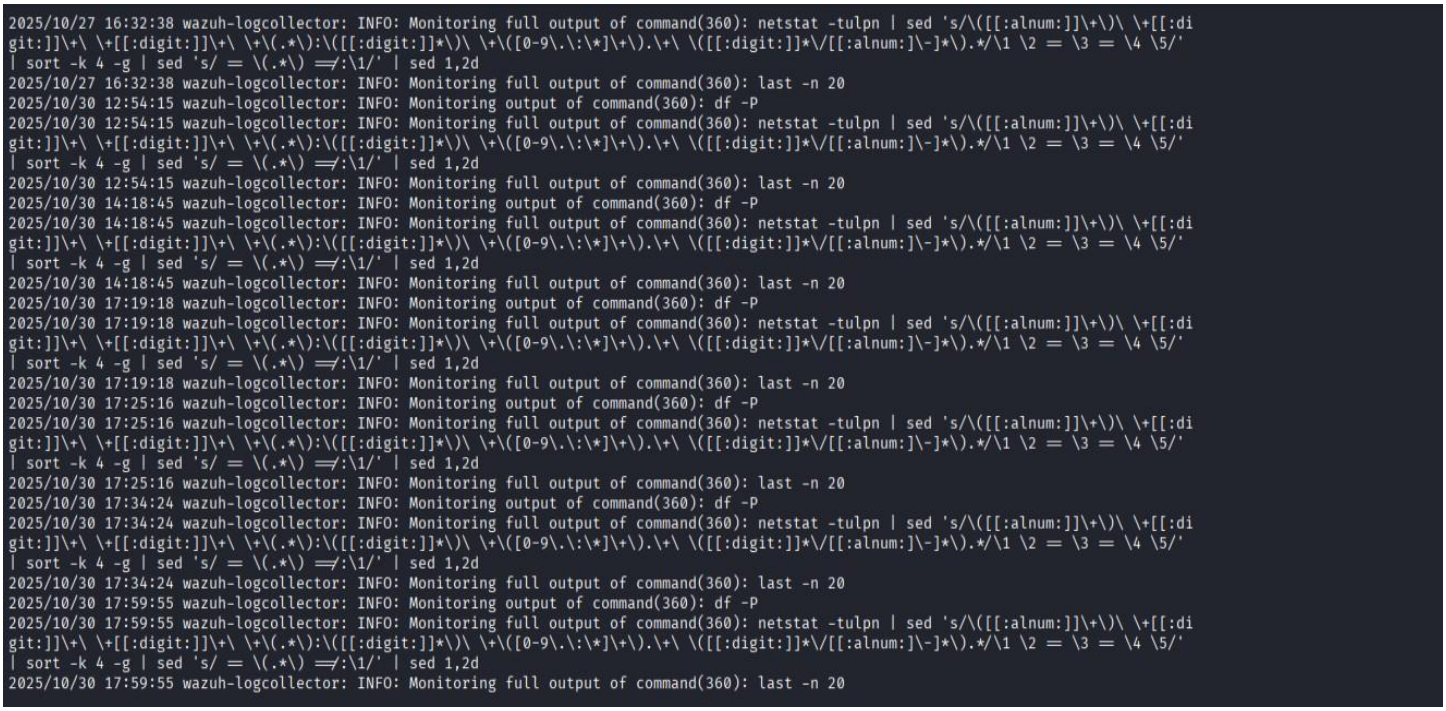
```
┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/audit/audit.log
type=USER_ACCT msg=audit(1761861316.449:372): pid=7252 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:accounting grantors=pam_permit,pam_localuser acct="kali" e
xe="/usr/bin/sudo" hostname=kali addr=? terminal=/dev/pts/1 res=success'UID="kali" AUID="kali"
type=USER_CMD msg=audit(1761861316.449:373): pid=7252 uid=1000 auid=1000 ses=2 subj=unconfined msg='cwd="/home/kali" cmd=617573656172636820 2D6D20616C6C202D74732072656
3656E74 exe="/usr/bin/sudo" terminal=pts/1 res=success'UID="kali" AUID="kali"
type=CRED_REFR msg=audit(1761861316.449:374): pid=7252 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/1 res=success'UID="kali" AUID="kali"
type=USER_START msg=audit(1761861316.449:375): pid=7252 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/1 res=success'UID="kali" AUID="kali"
type=USER_END msg=audit(1761861316.453:376): pid=7252 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/1 res=success'UID="kali" AUID="kali"
type=CRED_DISP msg=audit(1761861316.453:377): pid=7252 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/1 res=success'UID="kali" AUID="kali"
type=USER_ACCT msg=audit(1761861434.040:378): pid=7266 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/1 res=success'UID="kali" AUID="kali"
type=USER_CMD msg=audit(1761861434.040:379): pid=7266 uid=1000 auid=1000 ses=2 subj=unconfined msg='cwd="/home/kali" cmd=7461696C202D66202F7661722F6C6F672F61756469742
F61756469742E6C6F67 exe="/usr/bin/sudo" terminal=pts/1 res=success'UID="kali" AUID="kali"
type=CRED_REFR msg=audit(1761861434.040:380): pid=7266 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/1 res=success'UID="kali" AUID="kali"
type=USER_START msg=audit(1761861434.040:381): pid=7266 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/1 res=success'UID="kali" AUID="kali"
```

Evidencia 9: Wazuh está ejecutando comandos automáticamente cada 6 minutos.



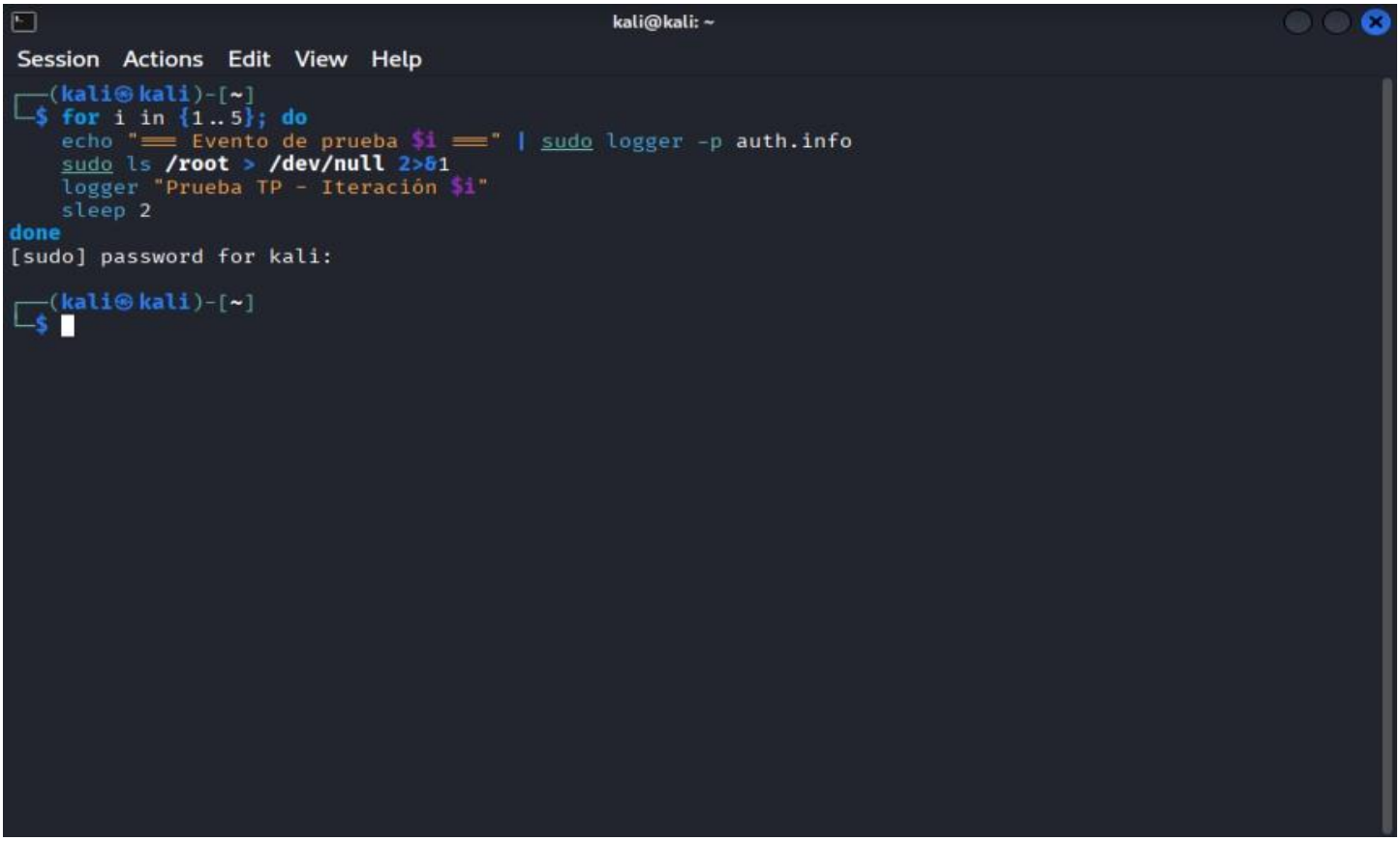
```
┌──(kali㉿kali)-[~]
└─$ sudo grep -i "command" /var/ossec/logs/ossec.log
[sudo] password for kali:
2025/10/24 17:30:33 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/24 17:30:33 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/24 17:30:33 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/24 17:31:11 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/24 17:31:11 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/24 17:31:11 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/25 09:59:21 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/25 09:59:21 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/25 09:59:21 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/25 14:37:11 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/25 14:37:11 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/25 14:37:11 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/25 18:06:18 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/25 18:06:18 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/25 18:06:18 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/26 00:08:48 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/26 00:08:48 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/26 00:08:48 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/26 17:54:15 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
```

Evidencia 10: Wazuh está ejecutando comandos automáticamente cada 6 minutos.

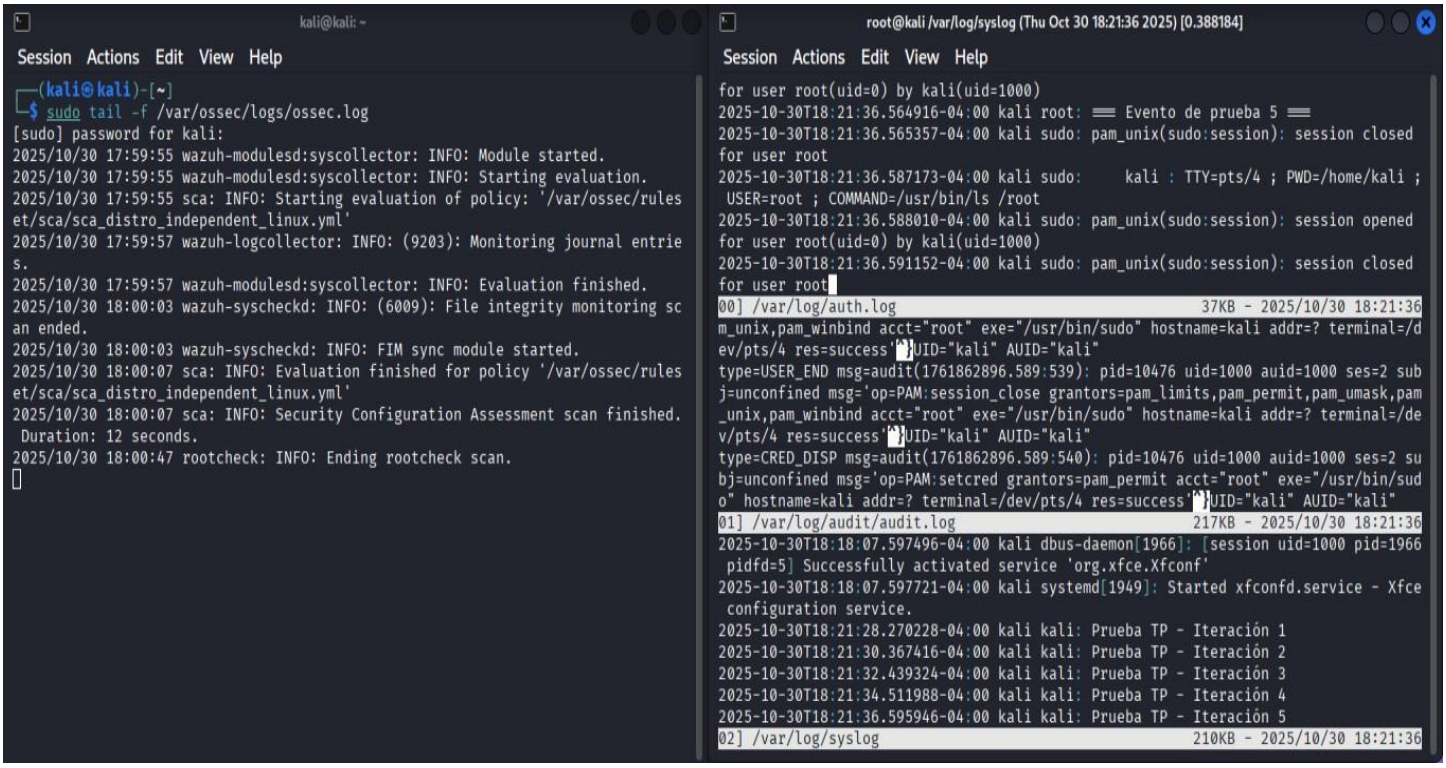


```
2025/10/27 16:32:38 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/27 16:32:38 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/30 12:54:15 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/30 12:54:15 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/30 12:54:15 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/30 14:18:45 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/30 14:18:45 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/30 14:18:45 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/30 17:19:18 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/30 17:19:18 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/30 17:19:18 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/30 17:25:16 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/30 17:25:16 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/30 17:25:16 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/30 17:34:24 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/30 17:34:24 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/30 17:34:24 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2025/10/30 17:59:55 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2025/10/30 17:59:55 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:di
git:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 = \3 = \4 \5/'
| sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d
2025/10/30 17:59:55 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
```

Evidencia 11: Script de generación de eventos de prueba, logger en auth.info.



Evidencia 12: Wazuh detectando eventos de prueba, sesiones sudo, comandos logger, etc.



Evidencia 13: Sesiones sudo para administración de servicios Wazuh y auditoría.

```
┌──(kali㉿kali)-[~]
└─$ echo "══ EVENTOS AUTH.LOG ══"
══ EVENTOS AUTH.LOG ══

┌──(kali㉿kali)-[~]
└─$ sudo tail -10 /var/log/auth.log
2025-10-30T21:30:21.334221-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-10-30T21:30:21.335382-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2025-10-30T21:30:54.343491-04:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/systemctl status wazuh-agent --no-pager -l
2025-10-30T21:30:54.344140-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-10-30T21:30:54.389801-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2025-10-30T21:31:08.763087-04:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/systemctl status auditd --no-pager -l
2025-10-30T21:31:08.763659-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-10-30T21:31:08.778732-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2025-10-30T21:32:47.026310-04:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/tail -10 /var/log/auth.log
2025-10-30T21:32:47.027050-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
```

Evidencia 14: Eventos detallados de audit.log mostrando autenticación y ejecución.

```
┌──(kali㉿kali)-[~]
└─$ echo "══ EVENTOS AUDIT.LOG ══"
══ EVENTOS AUDIT.LOG ══

┌──(kali㉿kali)-[~]
└─$ sudo tail -10 /var/log/audit/audit.log
type=USER_ACCT msg=audit(1761874367.020:87): pid=2654 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:accounting grantors=pam_permit,pam_localuser acct="kali" exe="/usr/bin/sudo" hostname=kali addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=USER_CMD msg=audit(1761874367.020:88): pid=2654 uid=1000 auid=1000 ses=2 subj=unconfined msg='cwd="/home/kali" cmd=7461696C202D3130202F7661722F6C6F672F617574682E6C6F67 exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="kali" AUID="kali"
type=CRED_REFR msg=audit(1761874367.020:89): pid=2654 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'UID="kali" AUID="kali"
type=USER_START msg=audit(1761874367.020:90): pid=2654 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=USER_END msg=audit(1761874367.052:91): pid=2654 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(1761874367.052:92): pid=2654 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'UID="kali" AUID="kali"
type=USER_ACCT msg=audit(1761874397.764:93): pid=2665 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:accounting grantors=pam_permit,pam_localuser acct="kali" exe="/usr/bin/sudo" hostname=kali addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=USER_CMD msg=audit(1761874397.764:94): pid=2665 uid=1000 auid=1000 ses=2 subj=unconfined msg='cwd="/home/kali" cmd=7461696C202D3130202F7661722F6C6F672F6175646974 2F617564469742E6C6F67 exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="kali" AUID="kali"
type=CRED_REFR msg=audit(1761874397.764:95): pid=2665 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'UID="kali" AUID="kali"
type=USER_START msg=audit(1761874397.764:96): pid=2665 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"
```

Evidencia 15: Activación de servicios desktop y supervisión de procesos por rtkit.

```
┌──(kali㉿kali)-[~]
└─$ echo "══ EVENTOS SYSLOG ══"
══ EVENTOS SYSLOG ══

┌──(kali㉿kali)-[~]
└─$ sudo tail -10 /var/log/syslog
2025-10-30T21:29:48.806298-04:00 kali systemd[1996]: Started xdg-desktop-portal-gtk.service - Portal service (GTK/GNOME implementation).
2025-10-30T21:29:48.923397-04:00 kali rtkit-daemon[1182]: Supervising 6 threads of 3 processes of 1 users.
2025-10-30T21:29:48.923645-04:00 kali rtkit-daemon[1182]: Supervising 6 threads of 3 processes of 1 users.
2025-10-30T21:29:48.924501-04:00 kali rtkit-daemon[1182]: Supervising 6 threads of 3 processes of 1 users.
2025-10-30T21:29:48.961470-04:00 kali rtkit-daemon[1182]: Supervising 6 threads of 3 processes of 1 users.
2025-10-30T21:29:48.962103-04:00 kali rtkit-daemon[1182]: Supervising 6 threads of 3 processes of 1 users.
2025-10-30T21:29:48.962864-04:00 kali rtkit-daemon[1182]: Supervising 6 threads of 3 processes of 1 users.
2025-10-30T21:29:48.971005-04:00 kali dbus-daemon[2014]: [session uid=1000 pid=2014 pidfd=5] Successfully activated service 'org.freedesktop.portal.Desktop'
2025-10-30T21:29:48.971885-04:00 kali systemd[1996]: Started xdg-desktop-portal.service - Portal service.
2025-10-30T21:29:58.533412-04:00 kali systemd[1]: pcscd.service: Deactivated successfully.
```

Evidencia 16: Kern.log, eventos de virtualización VirtualBox y estado de conectividad de red.

```
┌──(kali㉿kali)-[~]
└─$ echo "══ EVENTOS KERN.LOG ══"
══ EVENTOS KERN.LOG ══

┌──(kali㉿kali)-[~]
└─$ sudo tail -10 /var/log/kern.log
2025-10-30T21:28:04.902039-04:00 kali kernel: 01:28:04.777829 main     OS Product: Linux
2025-10-30T21:28:04.902040-04:00 kali kernel: 01:28:04.777876 main     OS Release: 6.16.8+kali-amd64
2025-10-30T21:28:04.902045-04:00 kali kernel: 01:28:04.777942 main     OS Version: #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24)
2025-10-30T21:28:04.902052-04:00 kali kernel: 01:28:04.777986 main     Executable: /opt/VBoxGuestAdditions-7.2.0/sbin/VBoxService
2025-10-30T21:28:04.902053-04:00 kali kernel: 01:28:04.777987 main     Process ID: 703
2025-10-30T21:28:04.902054-04:00 kali kernel: 01:28:04.777988 main     Package type: LINUX_64BITS_GENERIC
2025-10-30T21:28:04.902055-04:00 kali kernel: 01:28:04.795697 main     7.2.0 r170228 started. Verbose level = 0
2025-10-30T21:28:04.902056-04:00 kali kernel: 01:28:04.796901 main     vbglR3GuestCtrlDetectPeekGetCancelSupport: Supported (#1)
2025-10-30T21:28:05.872227-04:00 kali kernel: e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
2025-10-30T21:28:08.919829-04:00 kali kernel: NET: Registered PF_QIPCRTR protocol family
```

Evidencia 17: Eventos de Wazuh.

```
┌──(kali㉿kali)-[~]
└─$ sudo tail -20 /var/ossec/logs/ossec.log
2025/10/30 21:34:52 wazuh-agentd: INFO: Trying to connect to server ([10.0.2.20]:1514/tcp).
2025/10/30 21:34:52 wazuh-agentd: ERROR: (1216): Unable to connect to '[10.0.2.20]:1514/tcp': 'Transport endpoint is not connected'.
2025/10/30 21:35:02 wazuh-agentd: INFO: Trying to connect to server ([10.0.2.20]:1514/tcp).
2025/10/30 21:35:02 wazuh-agentd: ERROR: (1216): Unable to connect to '[10.0.2.20]:1514/tcp': 'Transport endpoint is not connected'.
2025/10/30 21:35:12 wazuh-agentd: INFO: Trying to connect to server ([10.0.2.20]:1514/tcp).
2025/10/30 21:35:12 wazuh-agentd: ERROR: (1216): Unable to connect to '[10.0.2.20]:1514/tcp': 'Transport endpoint is not connected'.
2025/10/30 21:35:22 wazuh-agentd: INFO: Trying to connect to server ([10.0.2.20]:1514/tcp).
2025/10/30 21:35:22 wazuh-agentd: ERROR: (1216): Unable to connect to '[10.0.2.20]:1514/tcp': 'Transport endpoint is not connected'.
2025/10/30 21:35:32 wazuh-agentd: INFO: Trying to connect to server ([10.0.2.20]:1514/tcp).
2025/10/30 21:35:32 wazuh-agentd: ERROR: (1216): Unable to connect to '[10.0.2.20]:1514/tcp': 'Transport endpoint is not connected'.
2025/10/30 21:35:32 wazuh-agentd: INFO: Requesting a key from server: 10.0.2.20
2025/10/30 21:35:32 wazuh-agentd: ERROR: (1208): Unable to connect to enrollment service at '[10.0.2.20]:1515'
2025/10/30 21:35:42 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.
2025/10/30 21:35:42 wazuh-agentd: WARNING: Unable to connect to any server.
2025/10/30 21:35:42 wazuh-agentd: INFO: Trying to connect to server ([10.0.2.20]:1514/tcp).
2025/10/30 21:35:42 wazuh-agentd: INFO: (4102): Connected to the server ([10.0.2.20]:1514/tcp).
2025/10/30 21:35:42 sca: INFO: Evaluation finished for policy '/var/ossec/ruleset/sca/sca_distro_independent_linux.yml'
2025/10/30 21:35:42 sca: INFO: Security Configuration Assessment scan finished. Duration: 449 seconds.
2025/10/30 21:35:43 rootcheck: INFO: Starting rootcheck scan.
2025/10/30 21:35:45 wazuh-modulesd: INFO: Agent is now online. Process unlocked, continuing...
```

Evidencia 18: Estado de auditd, con logging de seguridad y rotación de archivos de auditoría.

```
Session  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status auditd
[sudo] password for kali:
● auditd.service - Security Audit Logging Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-10-31 17:53:28 EDT; 14min ago
 Invocation: f4617f4fb4874ec9aed0666622a2ce74
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
    Process: 437 ExecStart=/usr/sbin/auditd (code=exited, status=0/SUCCESS)
   Main PID: 443 (auditd)
      Tasks: 2 (limit: 9286)
     Memory: 5.1M (peak: 5.5M)
        CPU: 325ms
     CGroup: /system.slice/auditd.service
             └─443 /usr/sbin/auditd

Oct 31 17:53:27 kali systemd[1]: Starting auditd.service - Security Audit Logging Service...
Oct 31 17:53:27 kali auditd[443]: No plugins found, not dispatching events
Oct 31 17:53:28 kali auditd[443]: Init complete, auditd 4.1.2 listening for events (startup state enable)
Oct 31 17:53:28 kali systemd[1]: Started auditd.service - Security Audit Logging Service.
Oct 31 17:53:44 kali auditd[443]: Audit daemon rotating log files
```

Evidencia 19: Agente Wazuh v4.13.1 operativo.

```
┌──(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.
```

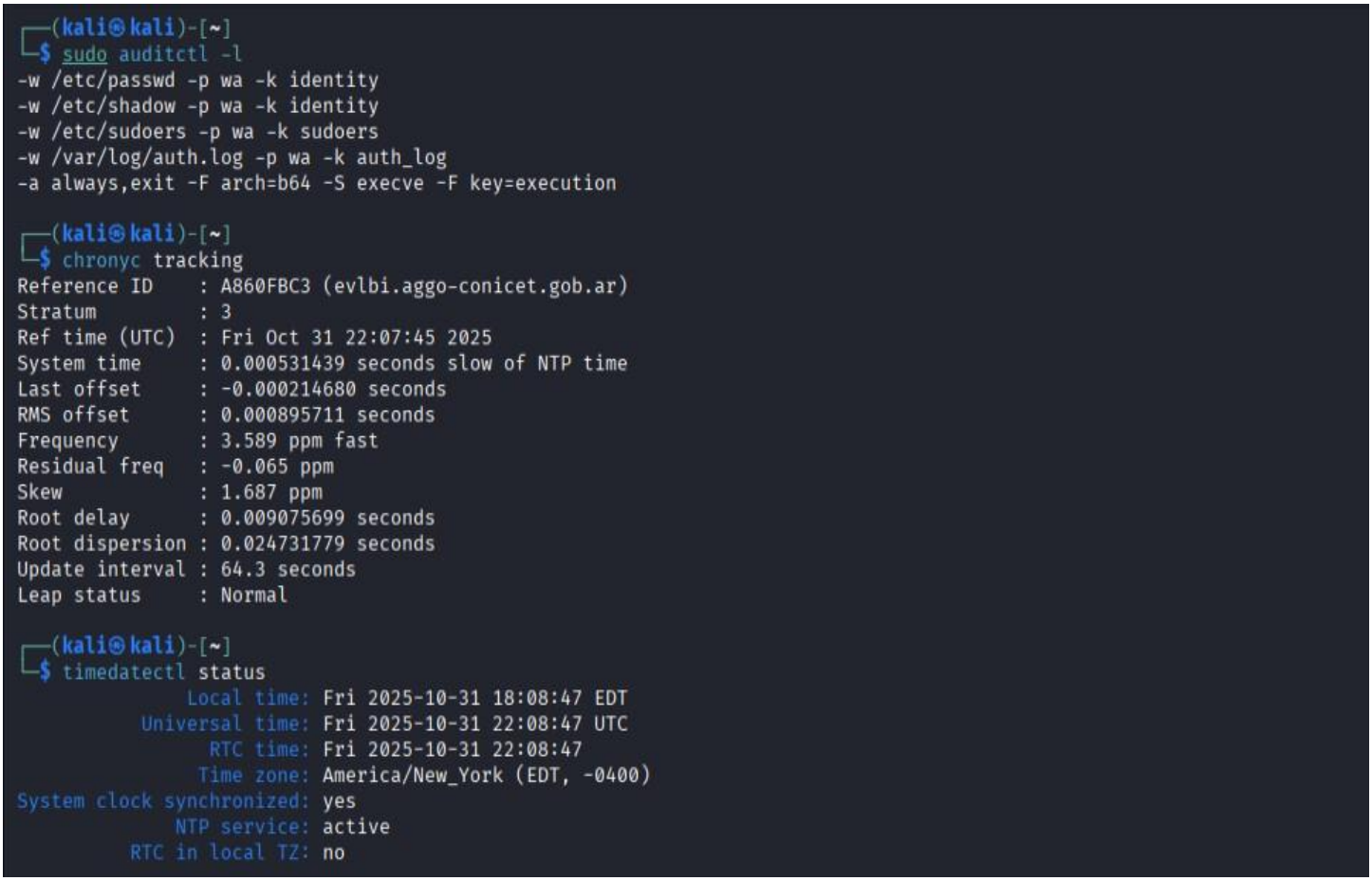
Evidencia 20: Servicio Suricata IDS/IPS activo, analizando tráfico de red.

```
┌──(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.
```

Evidencia 21: Sincronización de reloj del sistema con servidores pool.ntp.org.

```
┌──(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)
```

Evidencia 22: Verificación de configuraciones de seguridad.



Evidencia 23: Operaciones de gestión de usuarios y archivos.

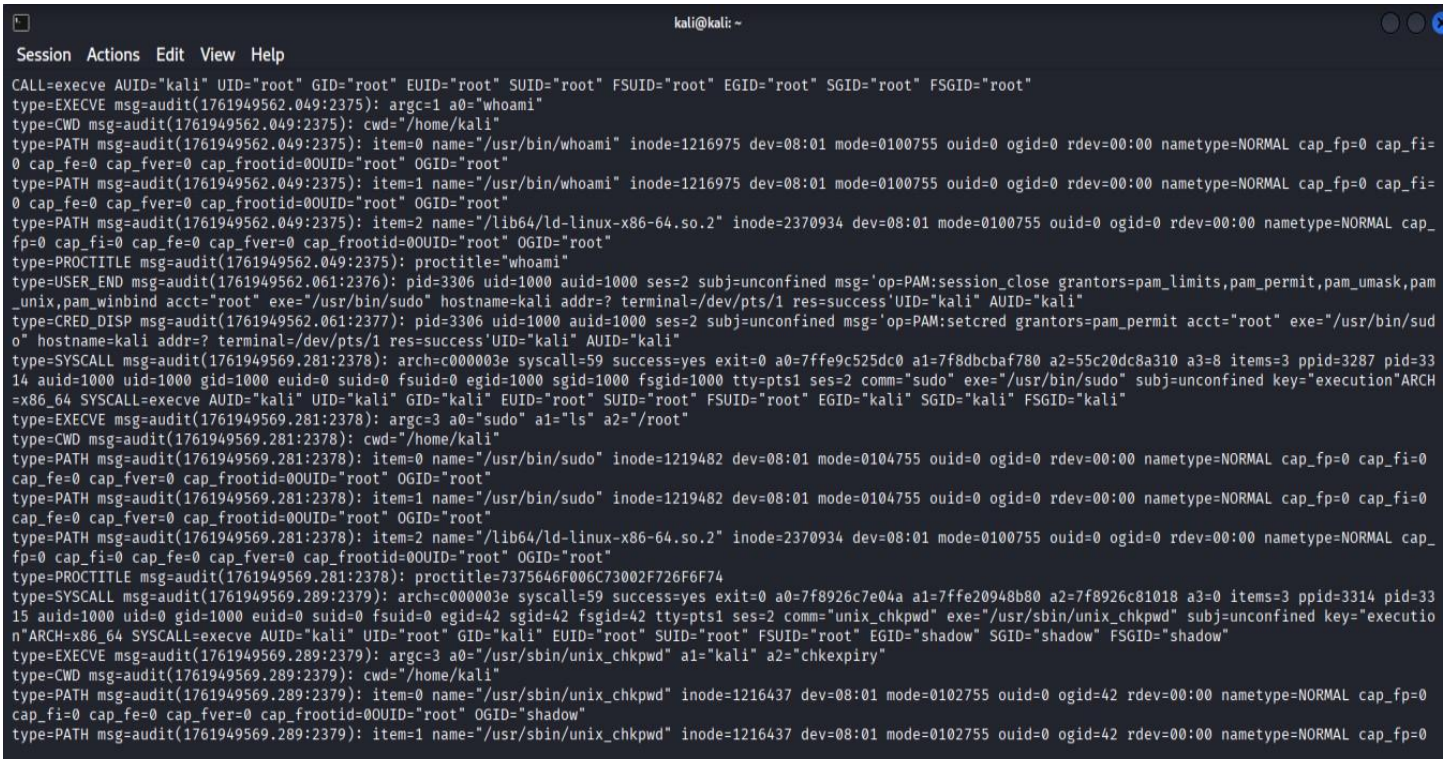
Evidencia 24: Eventos detallados de auditd mostrando la ejecución de “rm /etc/test-passwd”.

```
Session  Actions  Edit  View  Help
 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
```

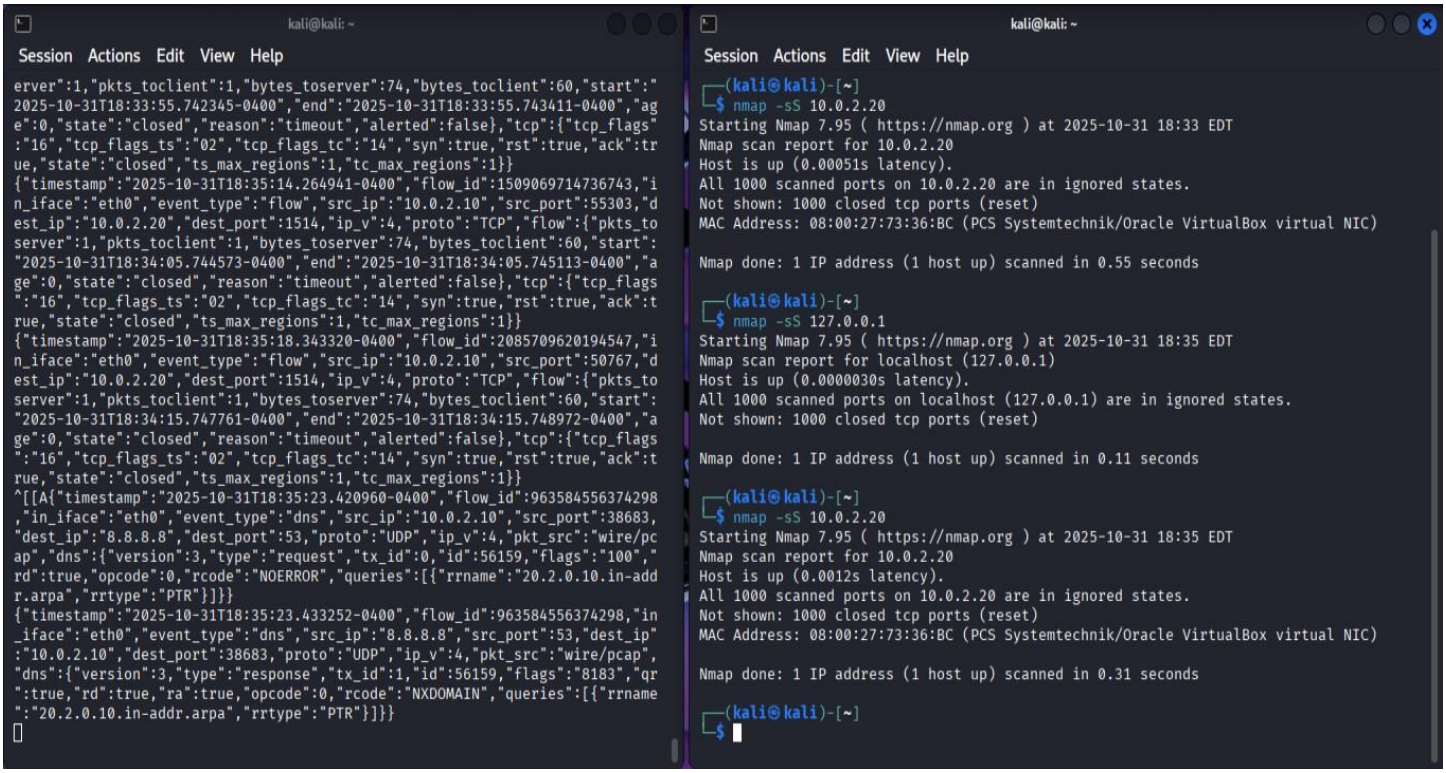
Evidencia 25: Búsqueda de eventos de auditoría con clave “identity”.

```
┌──(kali㉿kali)-[~]
└─$ sudo whoami
[sudo] password for kali:
root

┌──(kali㉿kali)-[~]
└─$ sudo ls /root
wazuh-certs

┌──(kali㉿kali)-[~]
└─$ sudo ausearch -k identity | tail -10
----
time→Fri Oct 31 18:22:27 2025
type=PROCTITLE msg=audit(1761949347.929:2286): proctitle=7573657264656C007465737475736572
type=PATH msg=audit(1761949347.929:2286): item=4 name="/etc/shadow" inode=4197684 dev=08:01 mode=01006
40 ouid=0 ogid=42 rdev=00:00 nametype=CREATE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1761949347.929:2286): item=3 name="/etc/shadow" inode=4197675 dev=08:01 mode=01006
40 ouid=0 ogid=42 rdev=00:00 nametype=DELETE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1761949347.929:2286): item=2 name="/etc/shadow+" inode=4197684 dev=08:01 mode=0100
640 ouid=0 ogid=42 rdev=00:00 nametype=DELETE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1761949347.929:2286): item=1 name="/etc/" inode=4194305 dev=08:01 mode=040755 ouid
=0 ogid=0 rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1761949347.929:2286): item=0 name="/etc/" inode=4194305 dev=08:01 mode=040755 ouid
=0 ogid=0 rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1761949347.929:2286): cwd="/home/kali"
type=SYSCALL msg=audit(1761949347.929:2286): arch=c000003e syscall=82 success=yes exit=0 a0=7ffc5c6851
70 a1=5598d06df500 a2=7ffc5c6850e0 a3=100 items=5 ppid=3192 pid=3193 auid=1000 uid=0 gid=0 euid=0 suid
=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=2 comm="userdel" exe="/usr/sbin/userdel" subj=unconfined
 key="identity"
```

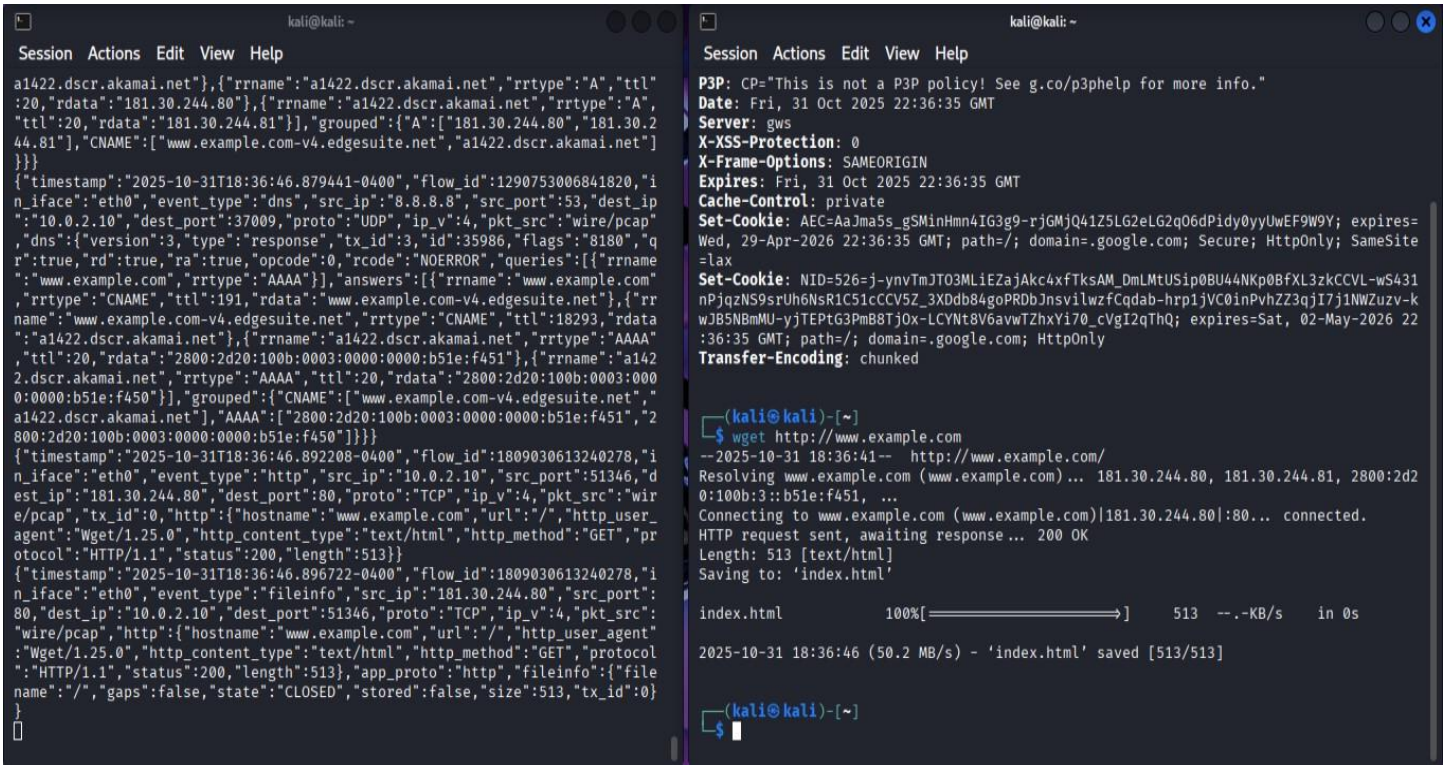
Evidencia 26: Resultado de alertas.



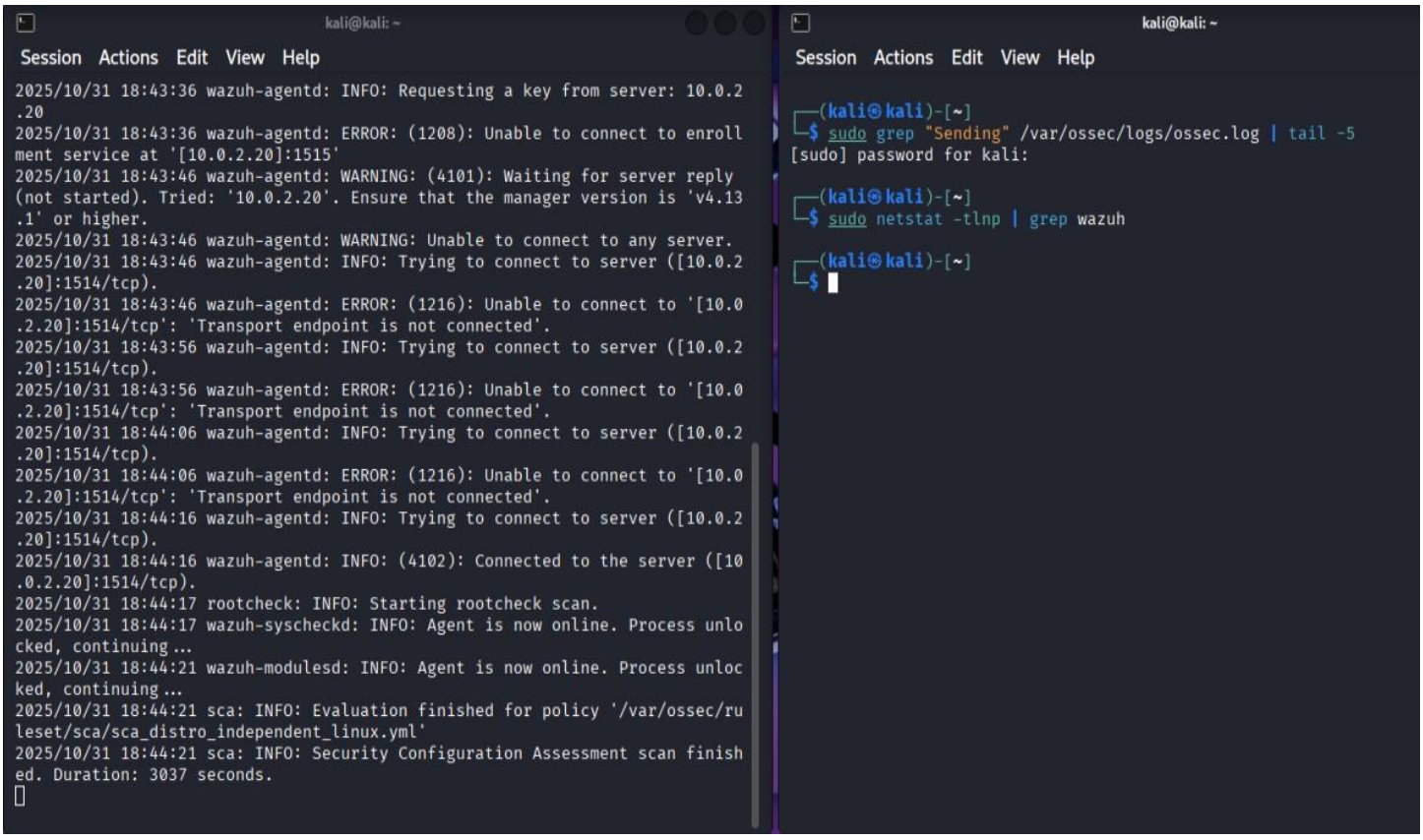
Evidencia 27: Detección de actividad de red, Suricata capturando flujos TCP/UDP.



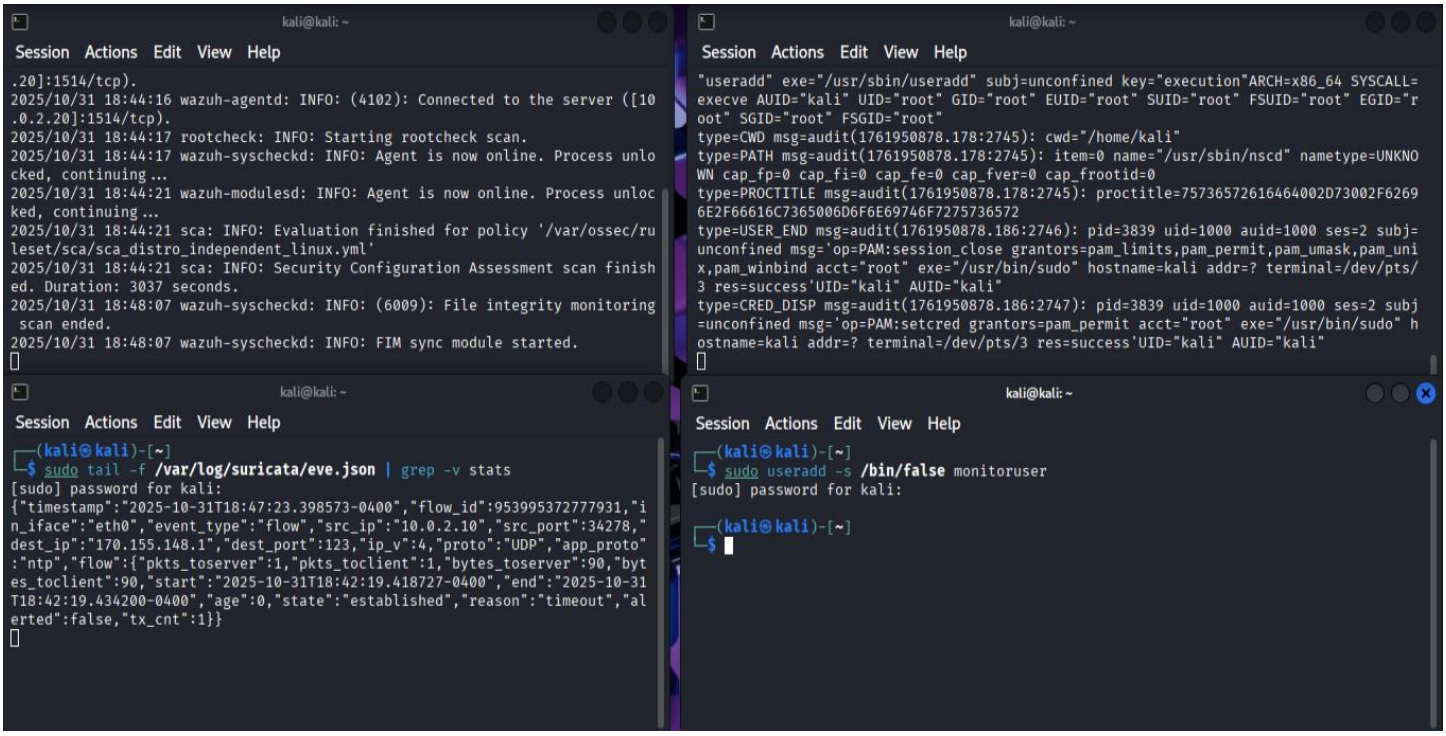
Evidencia 28: Alertas y trafico http/https en Suricata.



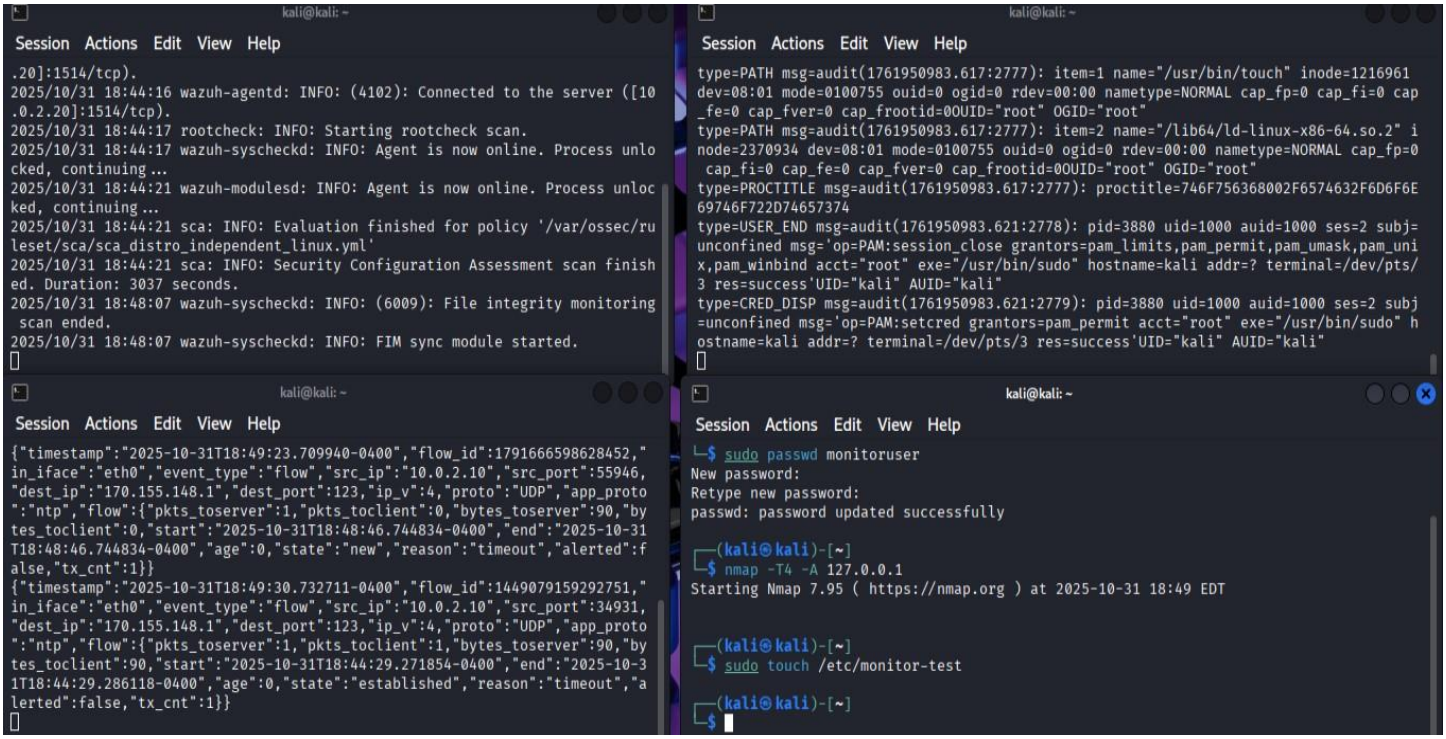
Evidencia 29: Wazuh recolectando y enviando logs al servidor.



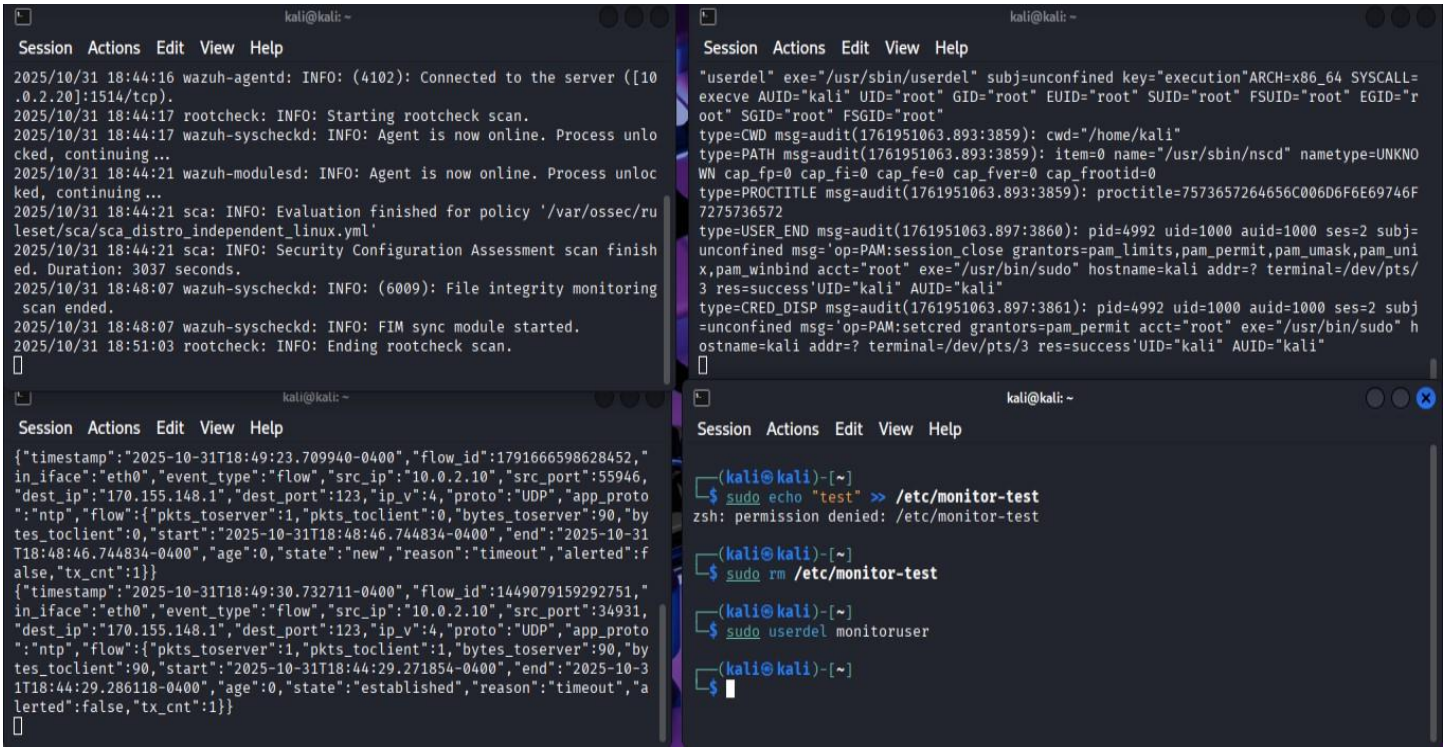
Evidencia 30: Integración de herramientas de seguridad, Wazuh, Suricata y auditd.



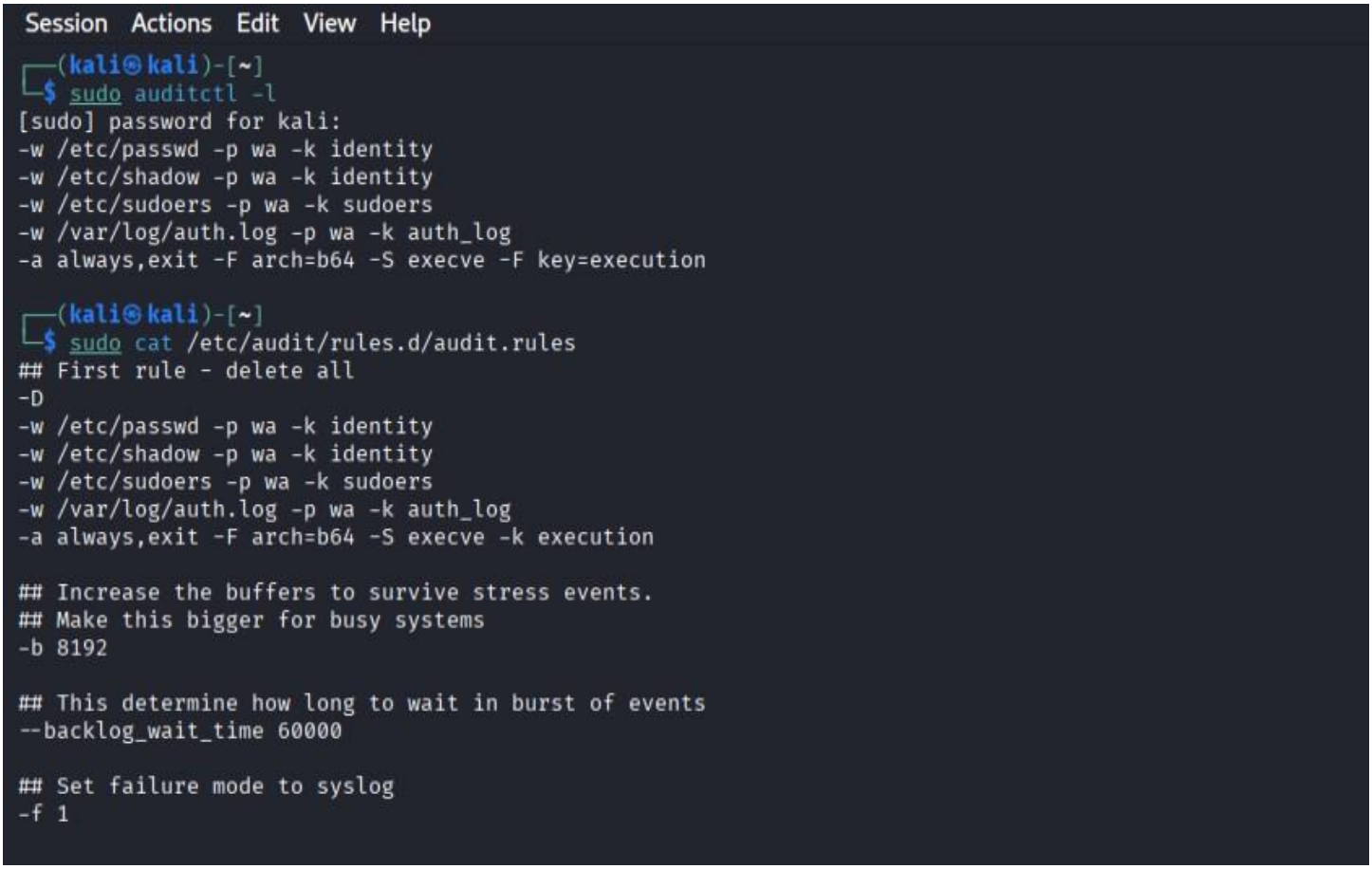
Evidencia 31: Integración de herramientas de seguridad, Wazuh, Suricata y auditd.



Evidencia 32: Integración de herramientas de seguridad, Wazuh, Suricata y auditd.



Evidencia 33: Configuración de auditd, monitorización de integridad en archivos críticos.



Evidencia 34: Interfaz eth0 en modo af-packet para captura de tráfico y log habilitado.

```
┌──(kali㉿kali)-[~]
└─$ sudo grep -A10 "af-packet" /etc/suricata/suricata.yaml
af-packet:
  - interface: eth0
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
    # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
    # This is only supported for Linux kernel > 3.1
    # possible value are:
    #  * cluster_flow: all packets of a given flow are sent to the same socket
    #  * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket

┌──(kali㉿kali)-[~]
└─$ sudo grep -A10 "eve-log" /etc/suricata/suricata.yaml
  - eve-log:
      enabled: yes
      filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
      filename: eve.json
      # Enable for multi-threaded eve.json output; output files are amended with
      # an identifier, e.g., eve.9.json
      #threaded: false
      # Specify the amount of buffering, in bytes, for
      # this output type. The default value 0 means "no
      # buffering".
      #buffer-size: 0
--
            # payload-buffer-size: 4 KiB  # max size of payload buffer to output in eve-log
            # payload-printable: yes   # enable dumping payload in printable (lossy) format
            # payload-length: yes      # enable dumping payload length, including the gaps
            # packet: yes              # enable dumping of packet (without stream segments)
            # metadata: no             # enable inclusion of app layer metadata with alert. Default yes
```

Evidencia 35: Configuración de Wazuh, recolección de logs locales de comandos del sistema.

```
┌──(kali㉿kali)-[~]
└─$ sudo grep -B2 -A5 "localfile" /var/ossec/etc/ossec.conf

  <!-- Log analysis -->
  <localfile>
    <log_format>command</log_format>
    <command>df -P</command>
    <frequency>360</frequency>
  </localfile>

  <localfile>
    <log_format>full_command</log_format>
    <command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:
]\-]*\).*/\1 \2 = \3 = \4 \5/' | sort -k 4 -g | sed 's/ = \(.*\) =/:\1/' | sed 1,2d</command>
    <alias>netstat listening ports</alias>
    <frequency>360</frequency>
  </localfile>

  <localfile>
    <log_format>full_command</log_format>
    <command>last -n 20</command>
    <frequency>360</frequency>
  </localfile>

  <!-- Active response -->
  <active-response>
    <disabled>no</disabled>
    <ca_store>etc/wpk_root.pem</ca_store>
--
  </logging>

  <localfile>
    <log_format>journald</log_format>
```

Evidencia 36: Estado de servicios, auditd, wazuh-agent, suricata y chrony activos.

```
┌──(kali㉿kali)-[~]
└─$ echo "══ RESUMEN FINAL ══"
══ RESUMEN FINAL ══

┌──(kali㉿kali)-[~]
└─$ echo "1. Servicios:"
1. Servicios:

┌──(kali㉿kali)-[~]
└─$ sudo systemctl is-active auditd wazuh-agent suricata chrony
active
active
active
active

┌──(kali㉿kali)-[~]
└─$ echo "2. Reglas Auditd:"
2. Reglas Auditd:

┌──(kali㉿kali)-[~]
└─$ sudo auditctl -l | wc -l
5
```

Evidencia 38: Métricas finales, 13 eventos de auditoría recientes, 570 alertas de Suricata, agente Wazuh conectado y sincronización NTP activa con servidor stratum 2.

```
┌──(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
```

Resumen Final

Se implementó y verificó exitosamente una infraestructura de seguridad integrada utilizando Wazuh para monitorización de endpoint, Auditd para auditoría del sistema y Suricata para detección de intrusiones en red.

Todos los servicios se encuentran operativos, con el agente Wazuh conectado al servidor, reglas de auditoría activas monitorizando archivos críticos y ejecución de procesos, y Suricata generando alertas de tráfico de red.

La configuración demostró capacidad efectiva para detectar actividades sospechosas, cambios en integridad de archivos y eventos de seguridad en tiempo real.

Herramientas

- Wazuh (OSSEC)
- Auditd
- Suricata
- Chrony
- Nmap
- Logger

Autora: Ingrid K.

Noviembre 2025.