RECONOCIMIENTO ACTIVO Y ESCANEO DE VULNERABILIDADES

Adrián Alonso Ridao

2º ASIR

1º EVALUACIÍON

CIBERSEGURIDAD

Contenido

PRÁCTICA - MÓDULO 3: RECONOCIMIENTO ACTIVO Y ESCANEO DE VULNERABILIDADES

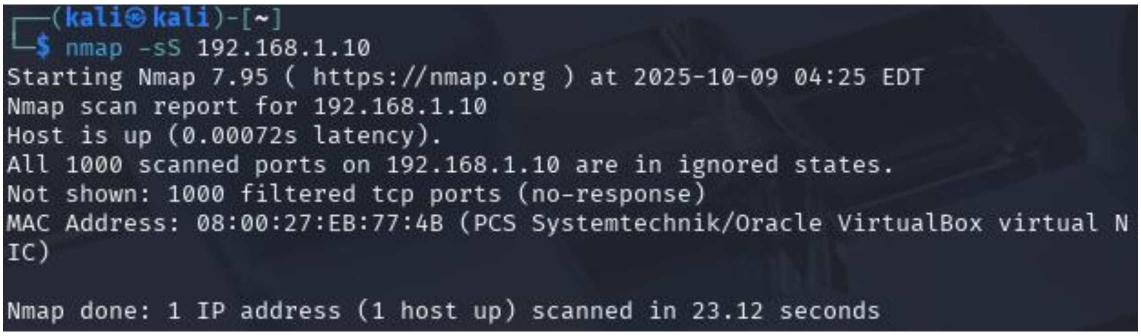
Objetivo: Aplicar técnicas de reconocimiento activo usando Nmap, enumeración de servicios y escaneo básico de vulnerabilidades.

Parte 1: Escaneo de Puertos con Nmap

Objetivo: Aprender a realizar diferentes tipos de escaneo de puertos para enumerar servicios.

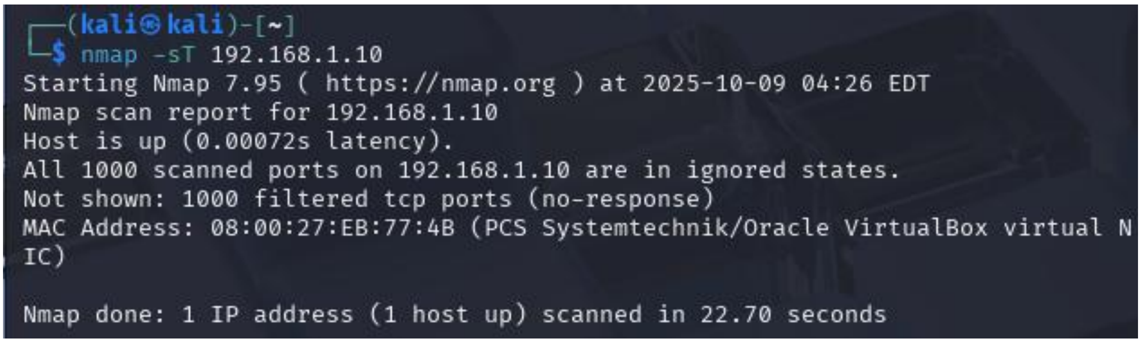
Tareas:

1. **Realiza un escaneo SYN básico al objetivo**



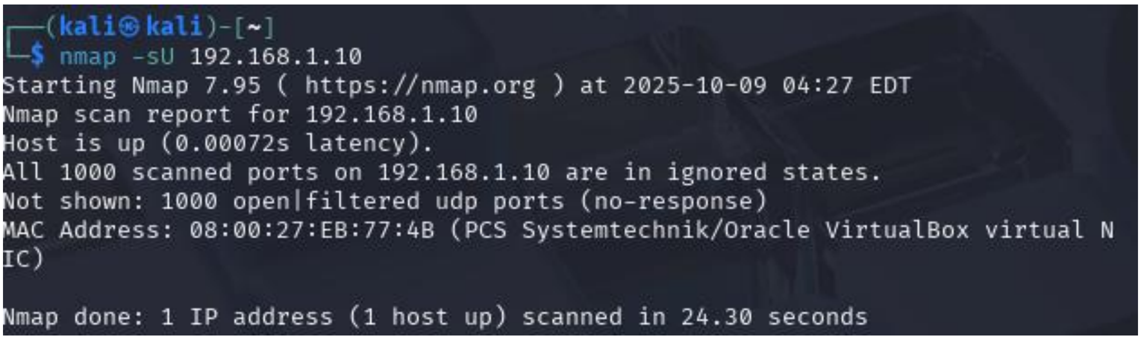
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 04:25 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00072s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 23.12 seconds
```

2. **Ejecuta un escaneo de conexión TCP completa**



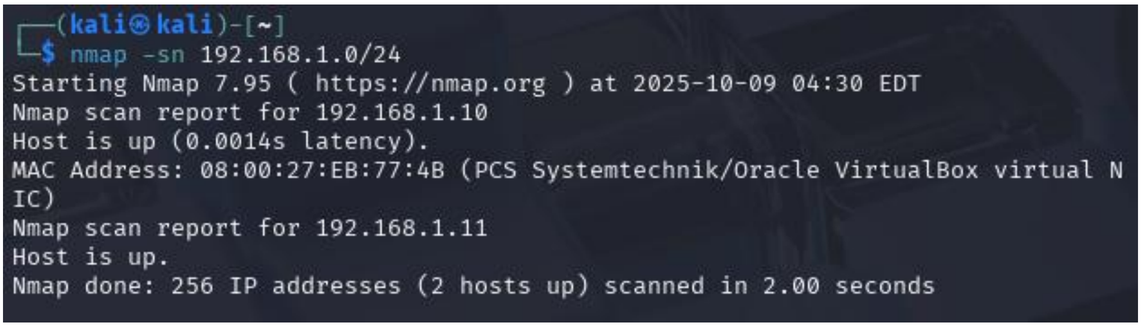
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 04:26 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00072s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 22.70 seconds
```

3. **Realiza un escaneo UDP en puertos comunes**



```
┌──(kali㉿kali)-[~]
└─$ nmap -sU 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 04:27 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00072s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 24.30 seconds
```

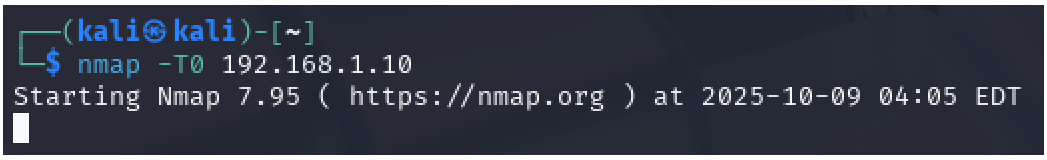
4. **Utiliza el escaneo de detección de hosts (-sn)**



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 04:30 EDT
Nmap scan report for 192.168.1.10
Host is up (0.0014s latency).
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.1.11
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.00 seconds
```

5. **Prueba diferentes plantillas de tiempo (-T0, -T4)**

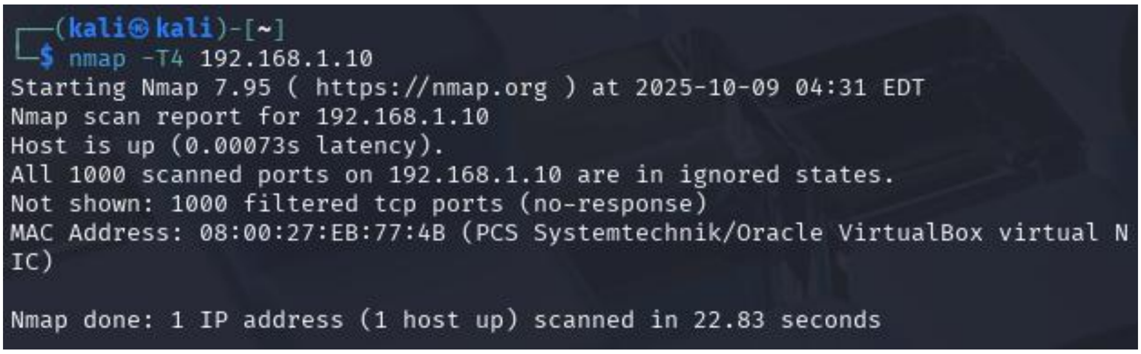
Paranoico:



```
┌──(kali㉿kali)-[~]
└─$ nmap -T0 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 04:05 EDT
```

No responde

Agresivo:



```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 04:31 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00073s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 22.83 seconds
```

6. **Documenta las diferencias entre cada tipo de escaneo**
   a. **SYN (-sS)**: detecta puertos open/filtered enviando SYN; menos ruidoso. Documenta: puertos open (SYN-ACK), filtered (sin respuesta/ICMP), timestamps y TTL.

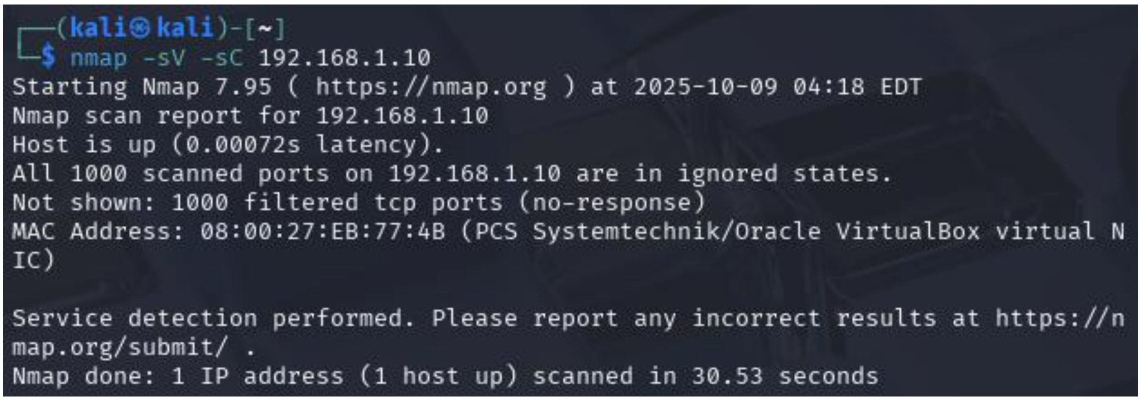
b. **TCP connect (-sT)**: completa handshake; más ruidoso pero confirma servicios y banners. Documenta: puertos open con banner, resets, y logs observados.
c. **UDP (-sU)**: frecuentemente open|filtered (silencio = ambiguo). Documenta: ICMP type/code recibidos y puertos inconclusos para retesting.
d. **Host discovery (-sn)**: confirma si el host está up. Documenta el método usado y latencia; anota falsos negativos.
e. **Timing (-T0 vs -T4)**: -T0 = muy lento, menos detección; -T4 = rápido, más probabilidad de rate-limit/filtered. Documenta duración total, diferencias en puertos reportados y señales de rate-limiting.

Parte 2: Enumeración de Servicios

Objetivo: Obtener información detallada de los servicios detectados.

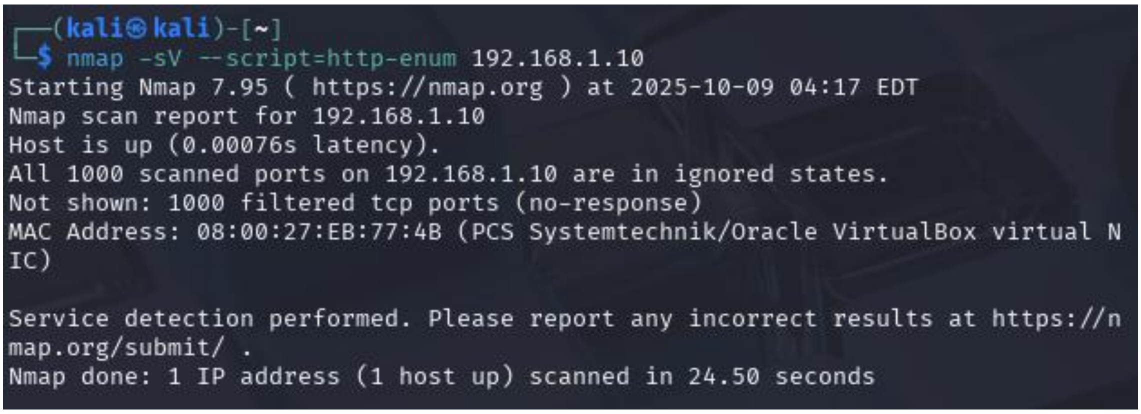
Tareas:

1. **Utiliza Nmap con detección de versión (-sV)**



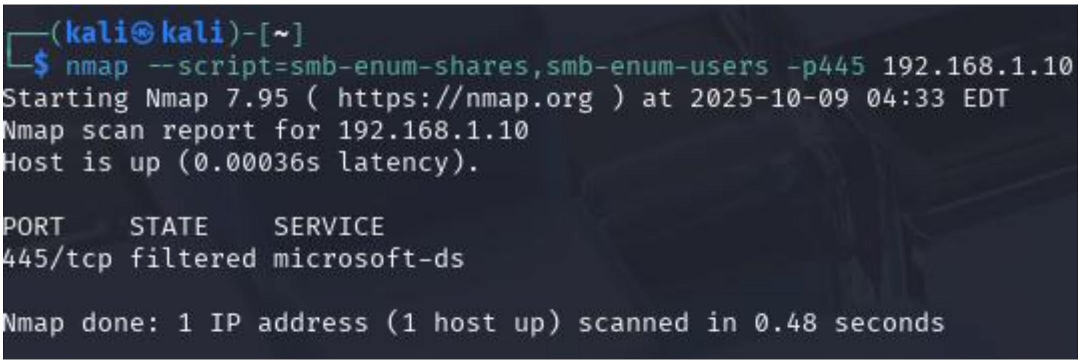
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 04:18 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00072s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.53 seconds
```

2. **Ejecuta scripts NSE para enumeración básica**



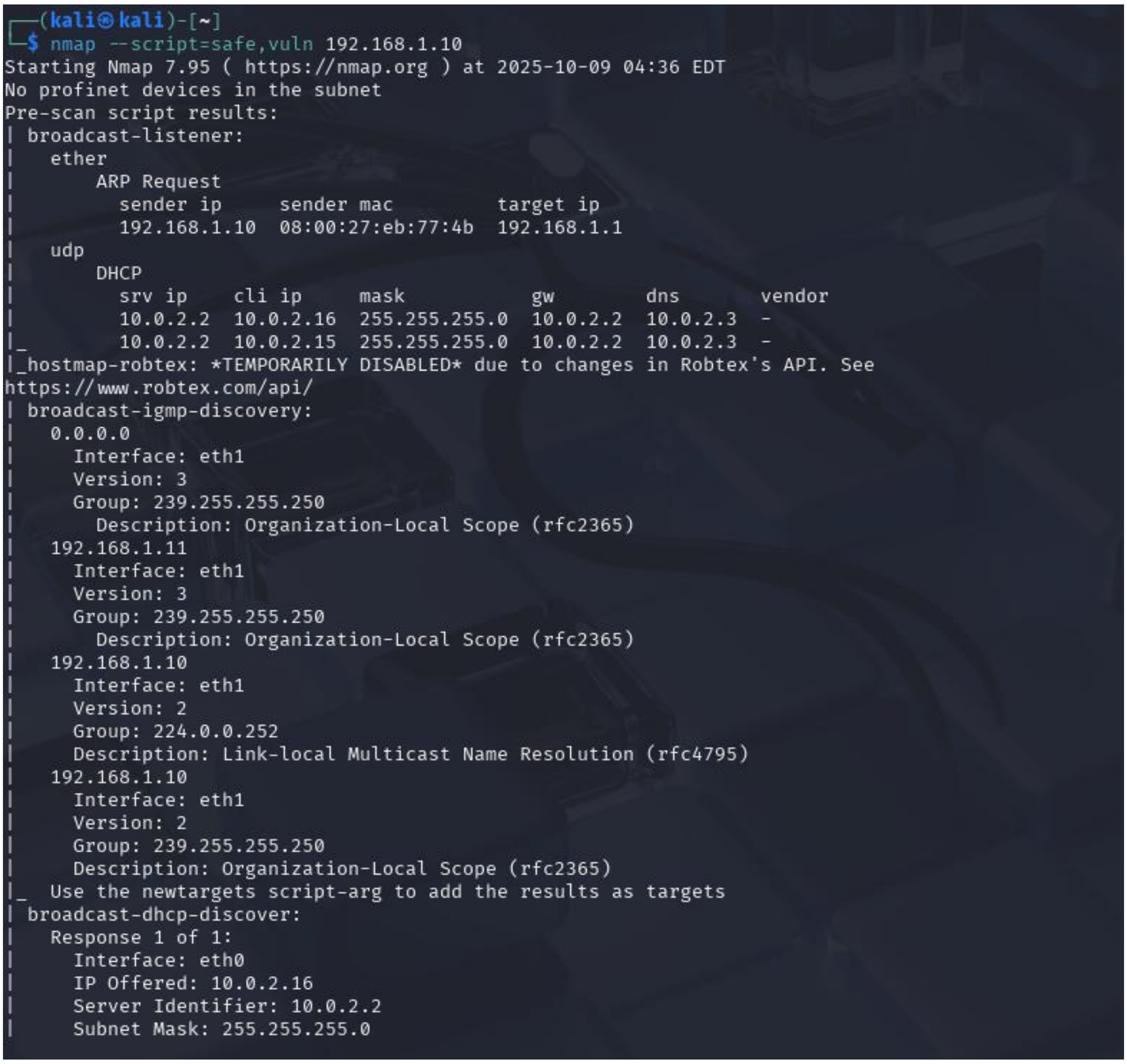
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=http-enum 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 04:17 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00076s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.50 seconds
```

3. **Realiza enumeración de servidores web con http-enum**



```
┌──(kali㉿kali)-[~]
└─$ nmap --script=smb-enum-shares,smb-enum-users -p445 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 04:33 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00036s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

4. **Prueba la enumeración SMB si hay puerto 445 abierto**



```
┌──(kali㉿kali)-[~]
└─$ nmap --script=safe,vuln 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 04:36 EDT
No profinet devices in the subnet
Pre-scan script results:
| broadcast-listener:
|   ether
|       ARP Request
|         sender ip     sender mac         target ip
|         192.168.1.10  08:00:27:eb:77:4b  192.168.1.1
|   udp
|       DHCP
|         srv ip    cli ip     mask           gw        dns       vendor
|         10.0.2.2  10.0.2.16  255.255.255.0  10.0.2.2  10.0.2.3  -
|_        10.0.2.2  10.0.2.15  255.255.255.0  10.0.2.2  10.0.2.3  -
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
| broadcast-igmp-discovery:
|   0.0.0.0
|     Interface: eth1
|     Version: 3
|     Group: 239.255.255.250
|       Description: Organization-Local Scope (rfc2365)
|   192.168.1.11
|     Interface: eth1
|     Version: 3
|     Group: 239.255.255.250
|       Description: Organization-Local Scope (rfc2365)
|   192.168.1.10
|     Interface: eth1
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name Resolution (rfc4795)
|   192.168.1.10
|     Interface: eth1
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as targets
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: eth0
|     IP Offered: 10.0.2.16
|     Server Identifier: 10.0.2.2
|     Subnet Mask: 255.255.255.0
```

5. **Documenta versiones de software y información obtenido**
6. **Prioriza vulnerabilidades según CVSS**

PRÁCTICA DE LABORATORIO

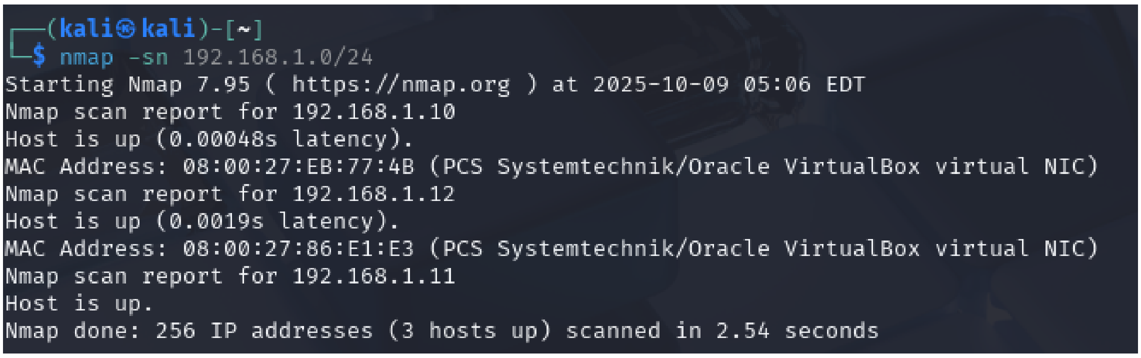
PARTE 1: ESCANEO BÁSICO DE RED

Ejercicio 1.1 - Descubrimiento de Hosts

# Identificar todos los hosts activos en la red del laboratorio

Tareas:

- Descubrir hosts activos usando escaneo ping
- Identificar las IPs asignadas a cada máquina del laboratorio
- Documentar los resultados en una tabla



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:06 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00048s latency).
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.12
Host is up (0.0019s latency).
MAC Address: 08:00:27:86:E1:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.11
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.54 seconds
```

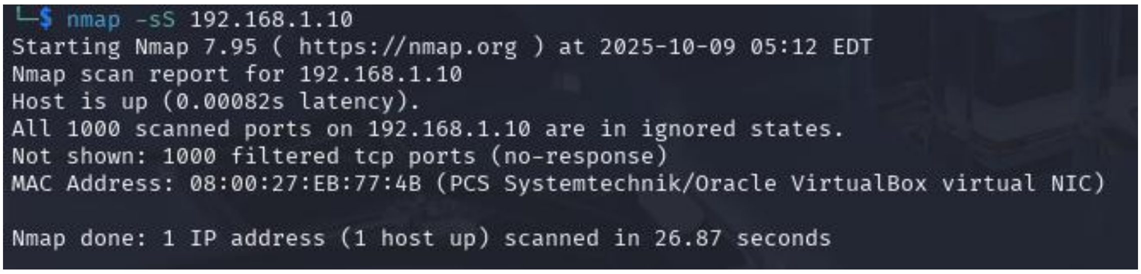
	Kali	**Windows**	**Metasploitable**
IPs	192.168.1.11	192.168.1.10	192.168.1.12

Ejercicio 1.2 - Escaneo de Puertos por Defecto

Tareas:

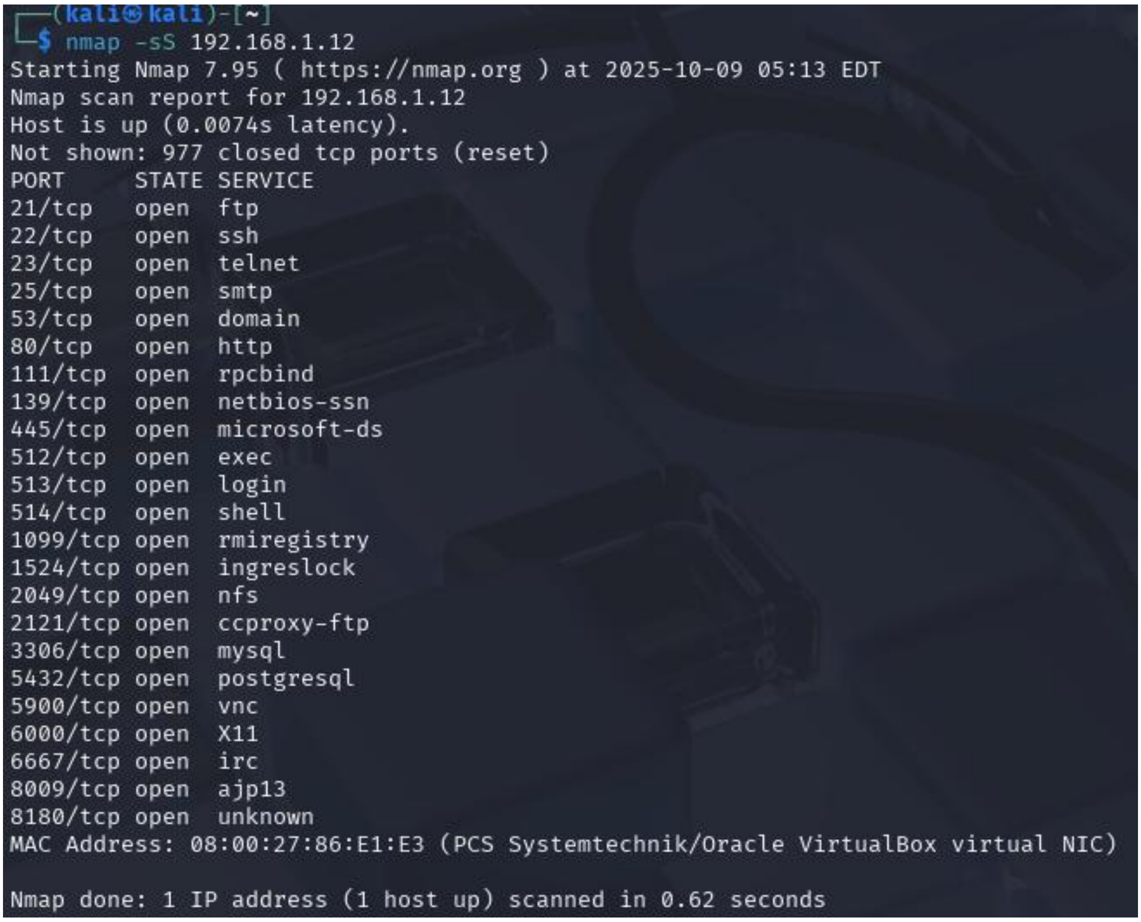
- Ejecutar escaneo SYN a los 1000 puertos más comunes
- Identificar puertos abiertos en Metasploitable2
- Comparar con escaneo a Windows 10

Windows:



```
└─$ nmap -sS 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:12 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00082s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 26.87 seconds
```

Metasploitable:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:13 EDT
Nmap scan report for 192.168.1.12
Host is up (0.0074s 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: 08:00:27:86:E1:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

La máquina de Windows no te da ninguna información sobre los puertos y la Metasploitable si al ser una máquina muy vulnerable.

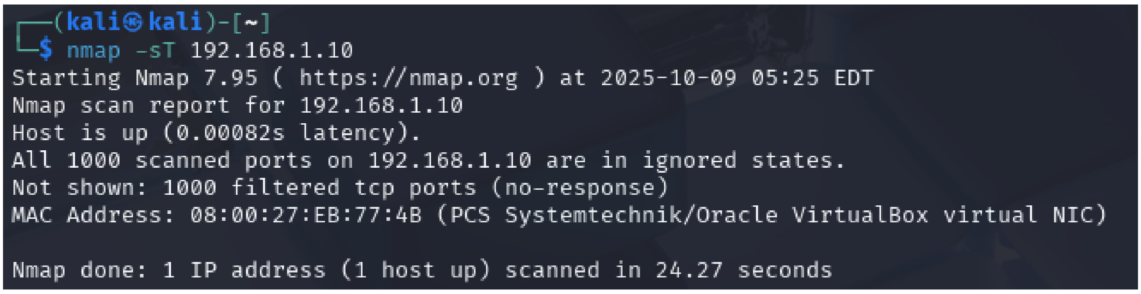
PARTE 2: TÉCNICAS AVANZADAS DE ESCANEO

Ejercicio 2.1 - Escaneo Completo de Puertos

Tareas:

- Realizar escaneo completo de puertos TCP (1-65535)
- Medir el tiempo requerido para el escaneo completo
- Identificar servicios inusuales en puertos altos

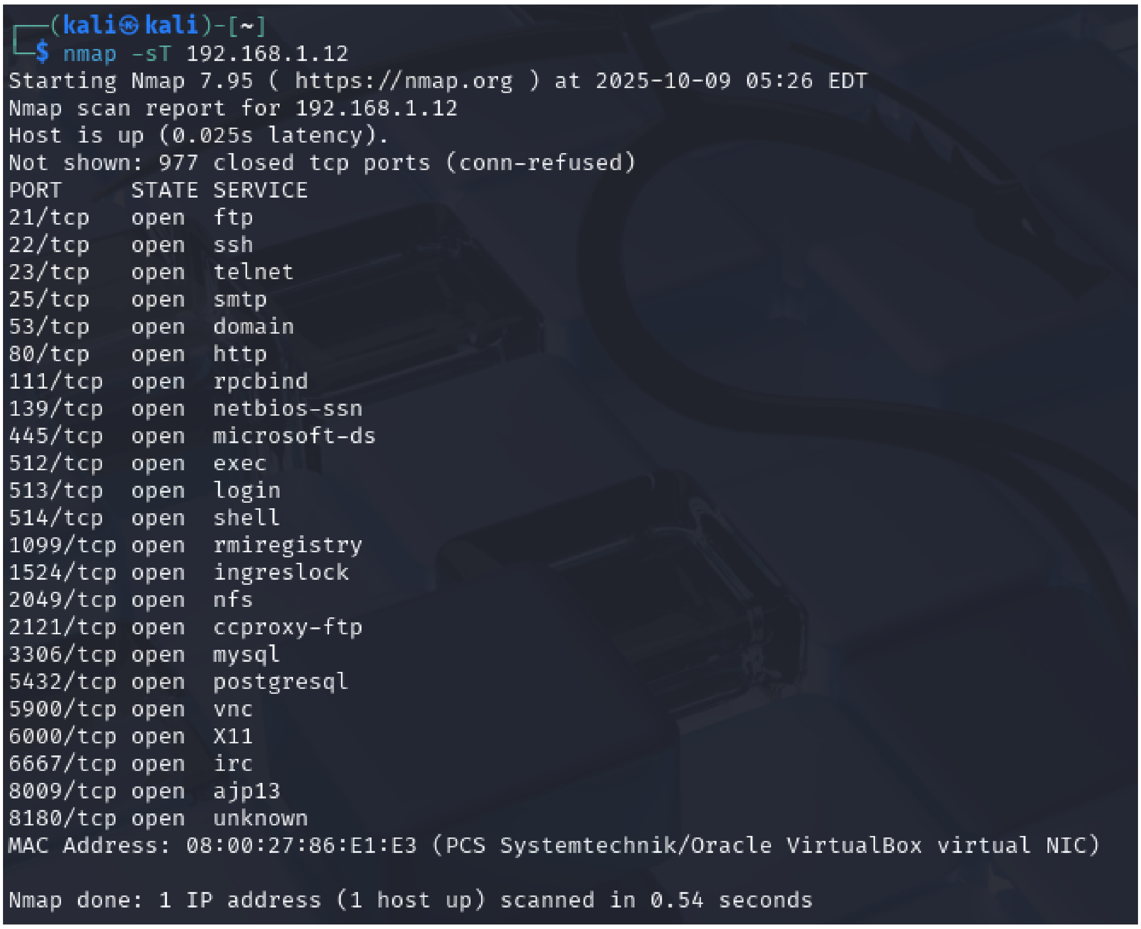
Windows:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:25 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00082s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 24.27 seconds
```

Tiempo requerido: 24.27 segundos

Metasploitable:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:26 EDT
Nmap scan report for 192.168.1.12
Host is up (0.025s latency).
Not shown: 977 closed tcp ports (conn-refused)
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: 08:00:27:86:E1:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

Tiempo requerido: 0.54 segundos

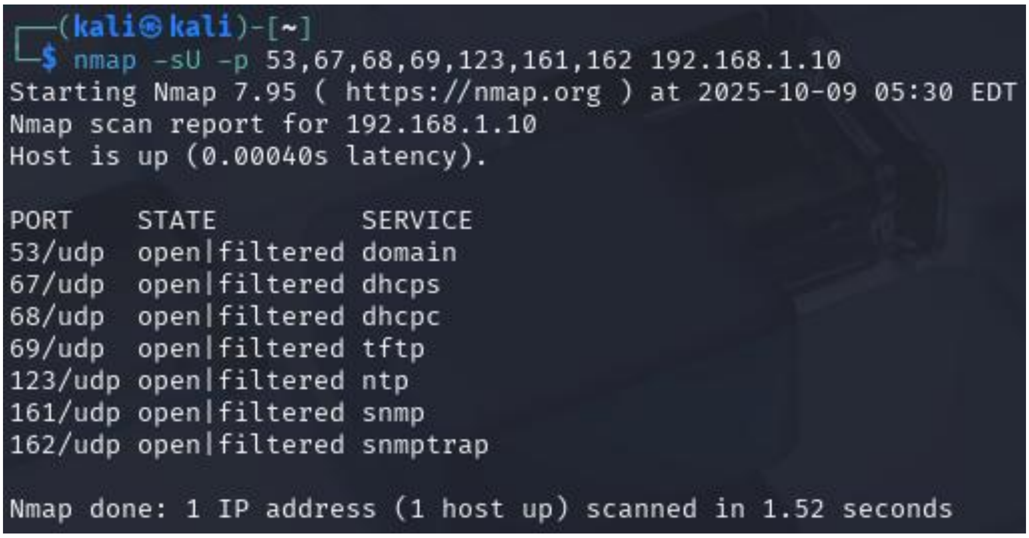
Servicio inusual en puerto 8180

Ejercicio 2.2 - Escaneo UDP

Tareas:

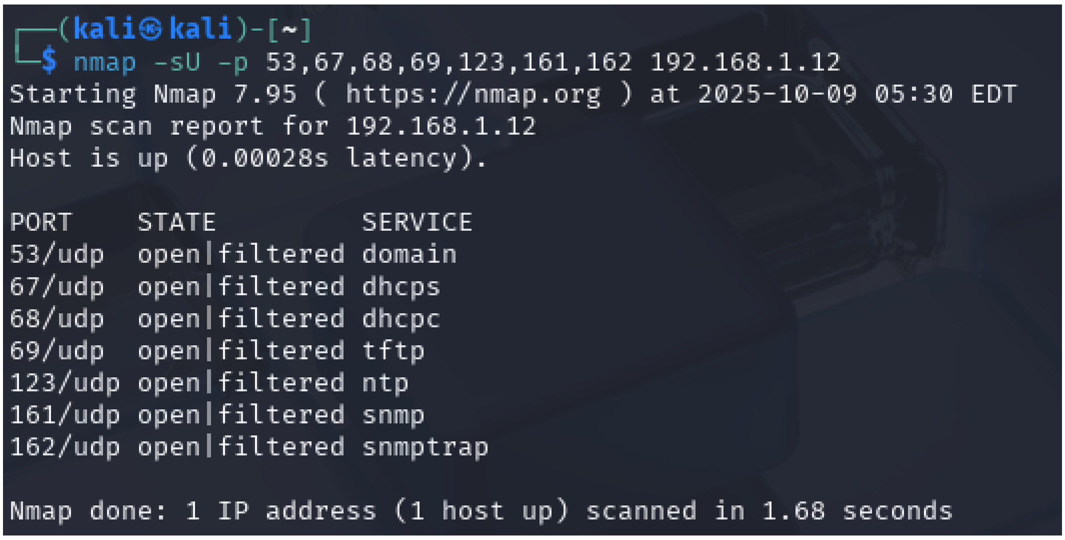
- Escanear puertos UDP 53, 67, 68, 69, 123, 161, 162
- Comparar resultados entre escaneo TCP y UDP
- Documentar servicios UDP encontrados

Windows:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sU -p 53,67,68,69,123,161,162 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:30 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00040s latency).

PORT    STATE         SERVICE
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
123/udp open|filtered ntp
161/udp open|filtered snmp
162/udp open|filtered snmptrap

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
```

Metasploitable:



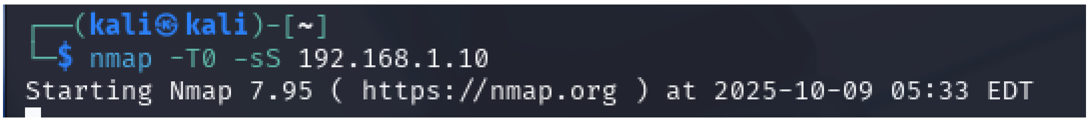
```
┌──(kali㉿kali)-[~]
└─$ nmap -sU -p 53,67,68,69,123,161,162 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:30 EDT
Nmap scan report for 192.168.1.12
Host is up (0.00028s latency).

PORT    STATE         SERVICE
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
123/udp open|filtered ntp
161/udp open|filtered snmp
162/udp open|filtered snmptrap

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
```

Ejercicio 2.3 - Técnicas de Evasión

Tareas:

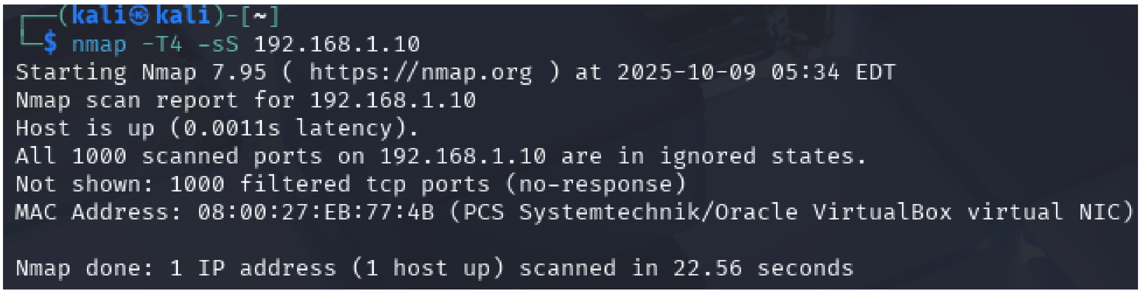
- Ejecutar escaneos con -T0 (paranoico) y -T4 (agresivo) –
- Comparar tiempos de ejecución y precisión
- Identificar ventajas/desventajas de cada técnica

Windows:



```
┌──(kali㉿kali)-[~]
└─$ nmap -T0 -sS 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:33 EDT
```

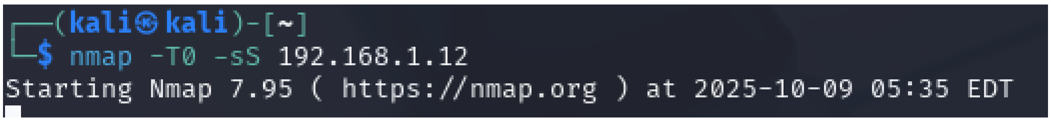
No recibimos respuesta con -T0



```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -sS 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:34 EDT
Nmap scan report for 192.168.1.10
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 22.56 seconds
```

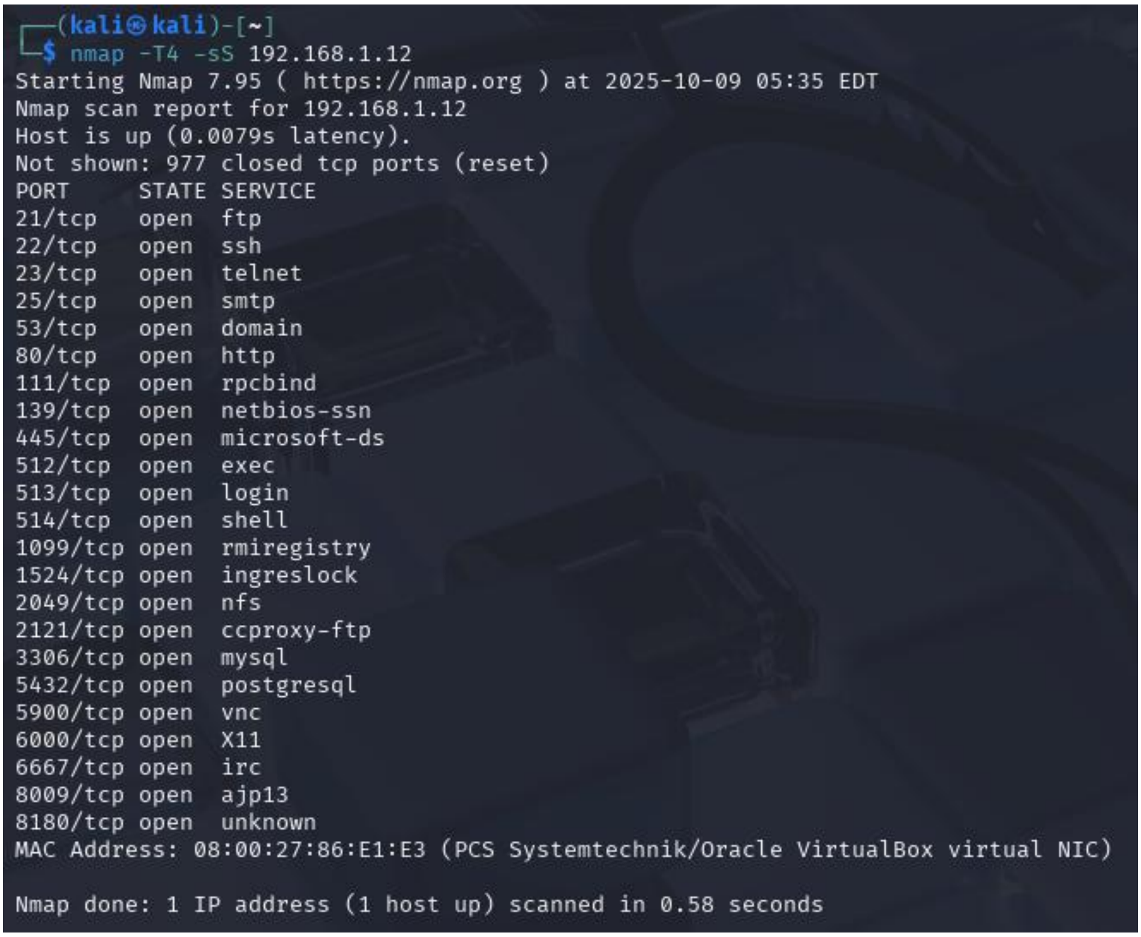
Tiempo ejecución: 22.56 segundos

Metasploitable:



```
┌──(kali㉿kali)-[~]
└─$ nmap -T0 -sS 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:35 EDT
```

Al igual que en Windows no recibimos respuesta



```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -sS 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:35 EDT
Nmap scan report for 192.168.1.12
Host is up (0.0079s 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: 08:00:27:86:E1:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

Tiempo ejecución 0.58 segundos.

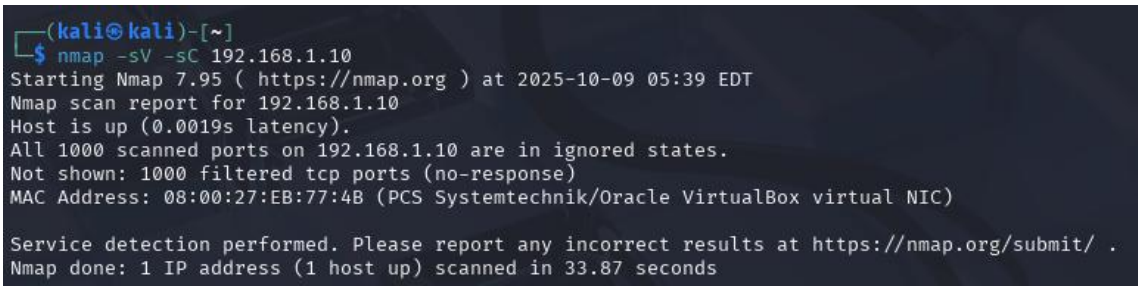
PARTE 3: ENUMERACIÓN DE SERVICIOS

Ejercicio 3.1 - Detección de Versiones

Tareas:

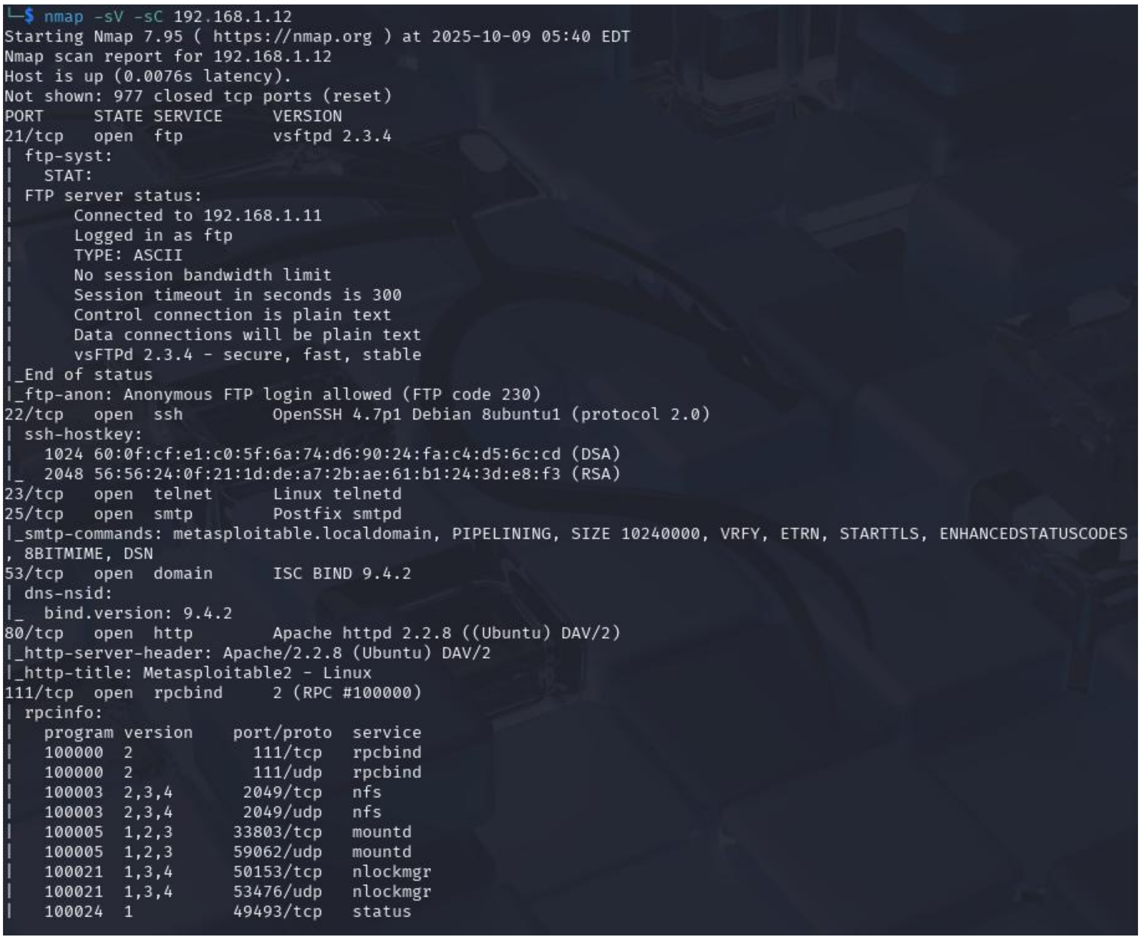
- Usar opción -sV para detección de versiones
- Ejecutar scripts básicos de enumeración (-sC)
- Documentar versiones vulnerables encontradas

Windows:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:39 EDT
Nmap scan report for 192.168.1.10
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.87 seconds
```

Metasploitable:



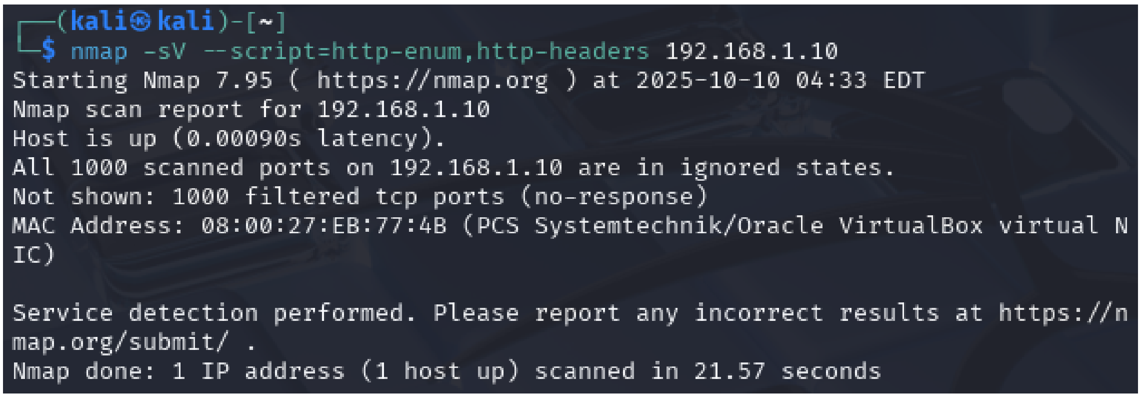
```
└─$ nmap -sV -sC 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:40 EDT
Nmap scan report for 192.168.1.12
Host is up (0.0076s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.11
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES
, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      33803/tcp   mountd
|   100005  1,2,3      59062/udp   mountd
|   100021  1,3,4      50153/tcp   nlockmgr
|   100021  1,3,4      53476/udp   nlockmgr
|   100024  1          49493/tcp   status
```

Ejercicio 3.2 - Enumeración Específica

Tareas:

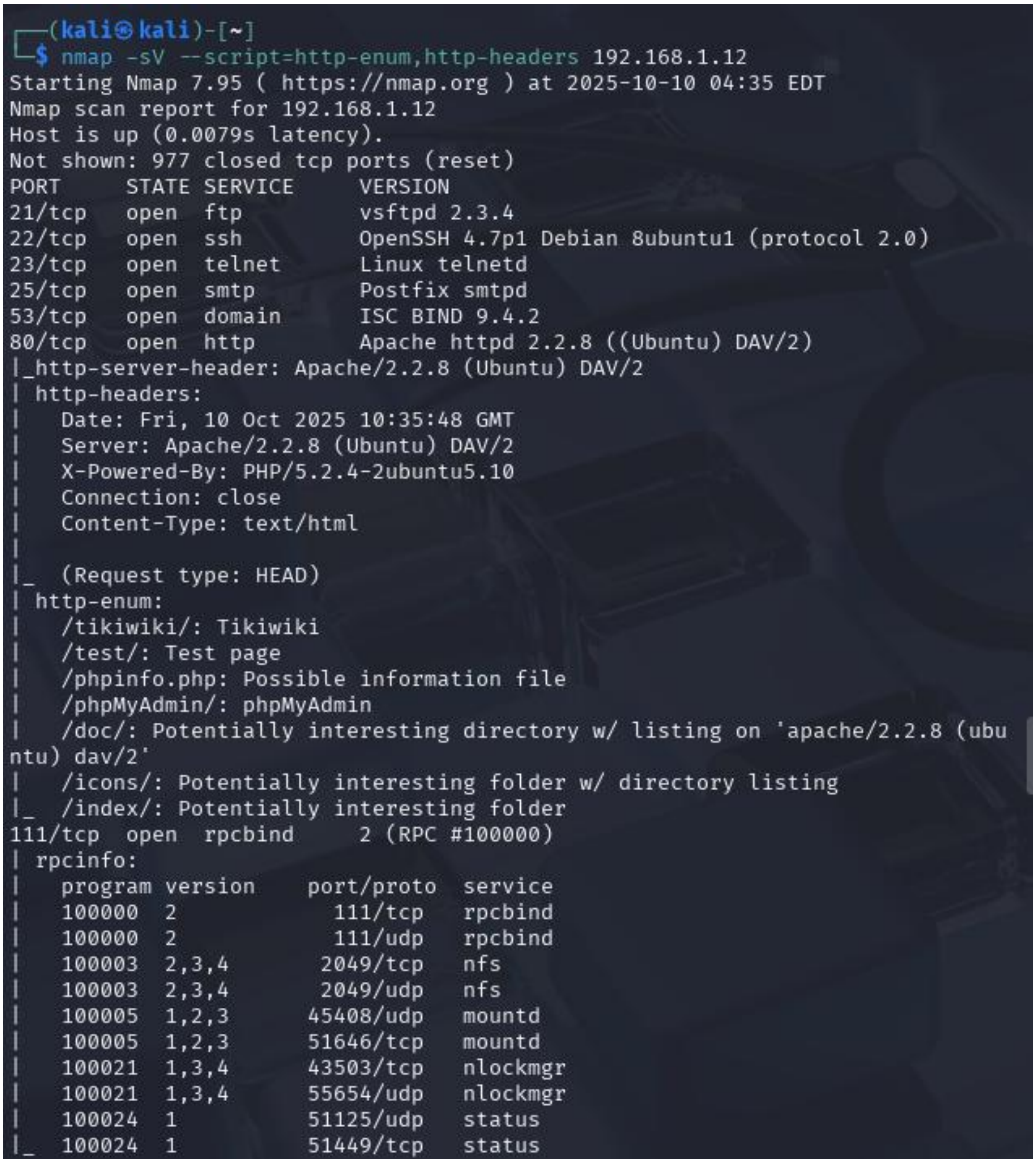
- Para servidor web (puerto 80): usar http-enum, http-headers-

  Windows:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=http-enum,http-headers 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:33 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00090s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.57 seconds
```

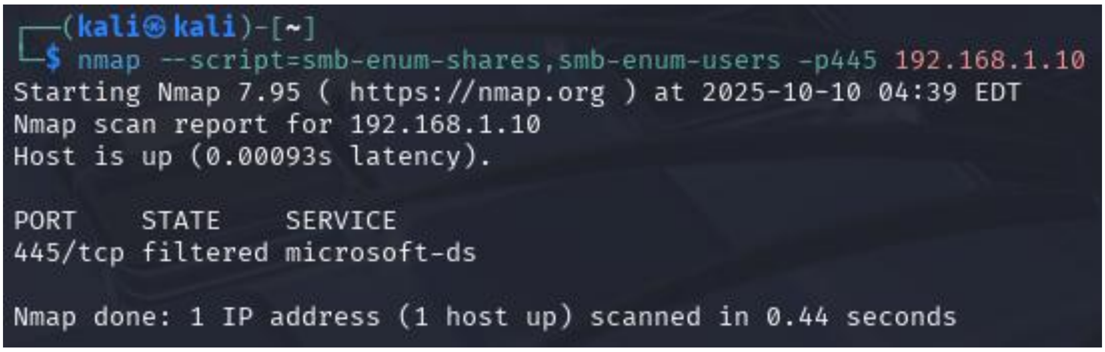
Metasploitable:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=http-enum,http-headers 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:35 EDT
Nmap scan report for 192.168.1.12
Host is up (0.0079s 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)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-headers:
|   Date: Fri, 10 Oct 2025 10:35:48 GMT
|   Server: Apache/2.2.8 (Ubuntu) DAV/2
|   X-Powered-By: PHP/5.2.4-2ubuntu5.10
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubu
ntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      45408/udp   mountd
|   100005  1,2,3      51646/tcp   mountd
|   100021  1,3,4      43503/tcp   nlockmgr
|   100021  1,3,4      55654/udp   nlockmgr
|   100024  1          51125/udp   status
|_  100024  1          51449/tcp   status
```

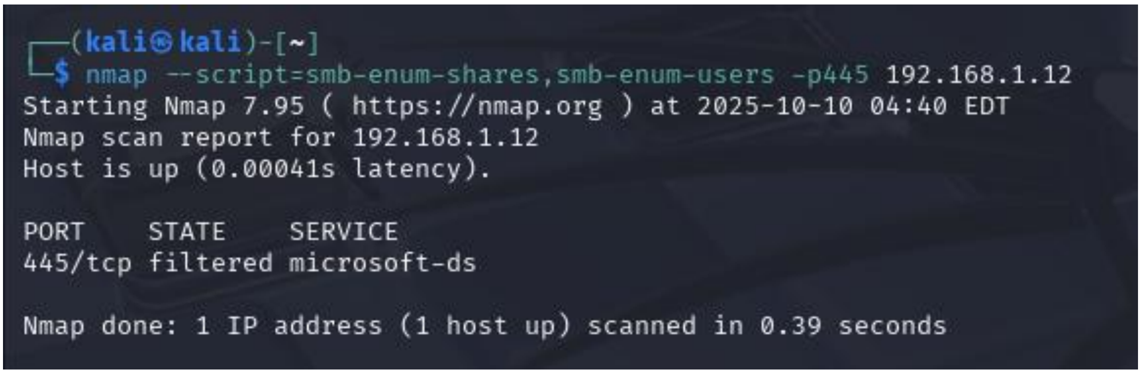
- Para SMB (puerto 445): usar smb-enum-shares, smb-os-discovery-

Windows:



```
┌──(kali㉿kali)-[~]
└─$ nmap --script=smb-enum-shares,smb-enum-users -p445 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:39 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00093s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

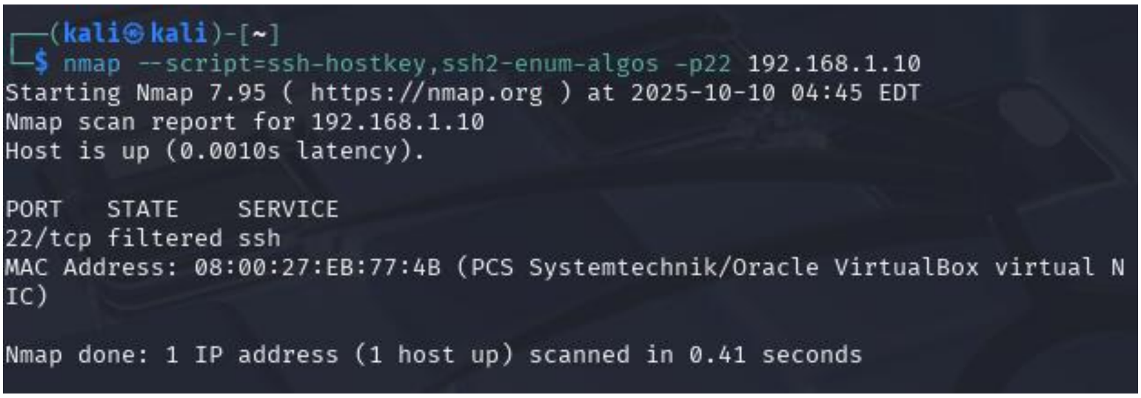
Metasploitable:



```
┌──(kali㉿kali)-[~]
└─$ nmap --script=smb-enum-shares,smb-enum-users -p445 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:40 EDT
Nmap scan report for 192.168.1.12
Host is up (0.00041s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

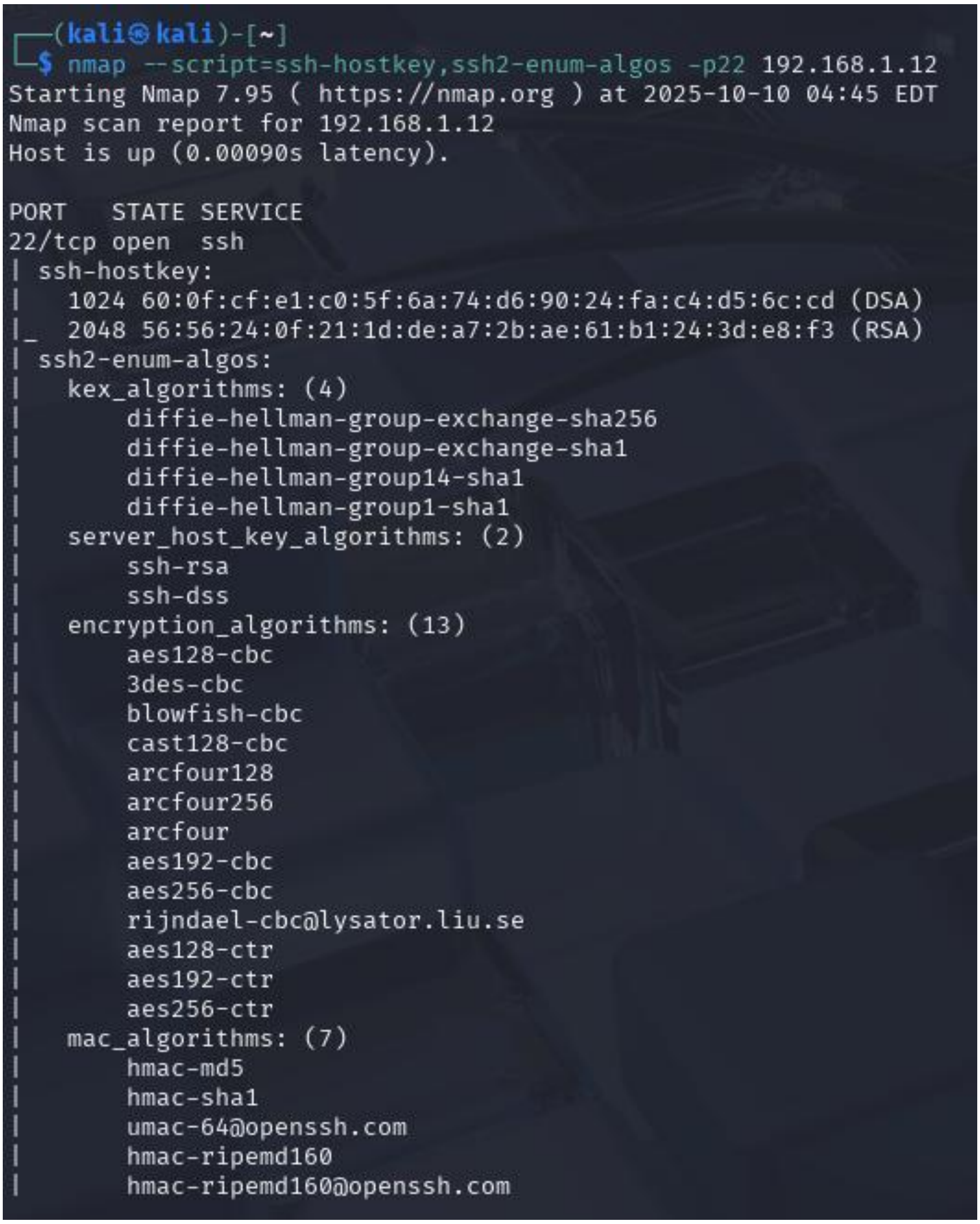
- Para SSH (puerto 22): usar ssh-hostkey, ssh2-enum-algos

Windows:



```
┌──(kali㉿kali)-[~]
└─$ nmap --script=ssh-hostkey,ssh2-enum-algos -p22 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:45 EDT
Nmap scan report for 192.168.1.10
Host is up (0.0010s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

Metasploitable:



```
┌──(kali㉿kali)-[~]
└─$ nmap --script=ssh-hostkey,ssh2-enum-algos -p22 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:45 EDT
Nmap scan report for 192.168.1.12
Host is up (0.00090s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
| ssh2-enum-algos:
|   kex_algorithms: (4)
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|       ssh-rsa
|       ssh-dss
|   encryption_algorithms: (13)
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       arcfour128
|       arcfour256
|       arcfour
|       aes192-cbc
|       aes256-cbc
|       rijndael-cbc@lysator.liu.se
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|   mac_algorithms: (7)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
```

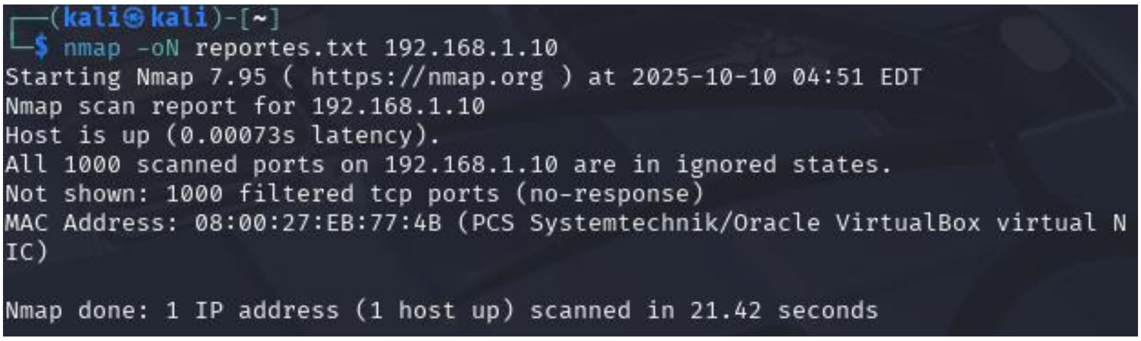
PARTE 4: ANÁLISIS Y REPORTING

Ejercicio 4.1 - Generación de Reportes

# Generar reportes en diferentes formatos

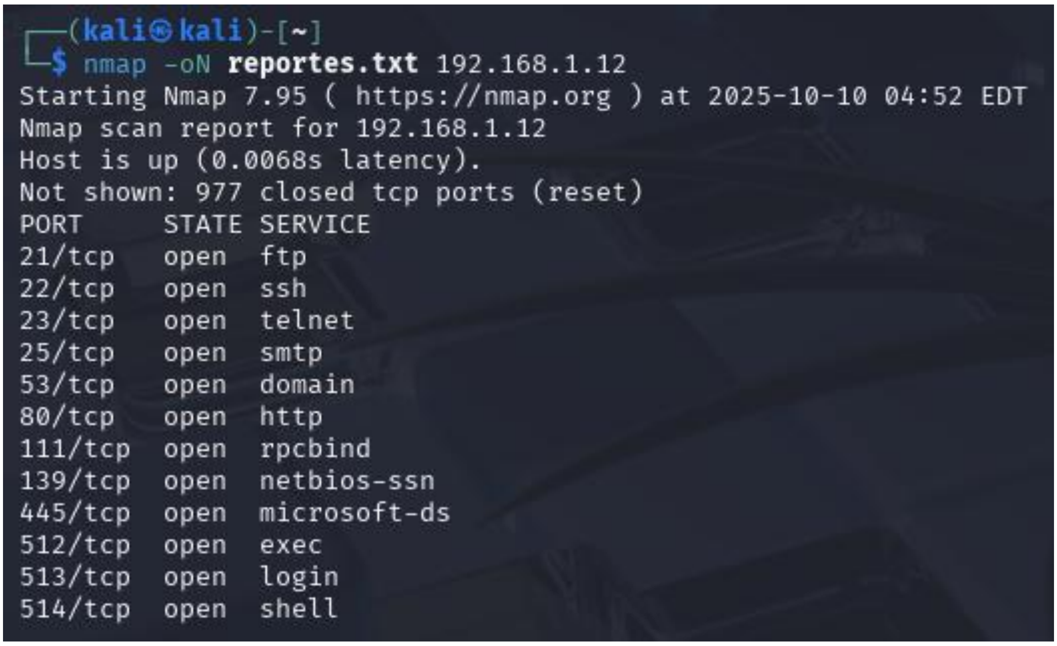
Tareas:

- Exportar resultados en formato normal (-oN)
  Windows:



```
┌──(kali㉿kali)-[~]
└─$ nmap -oN reportes.txt 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:51 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00073s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds
```

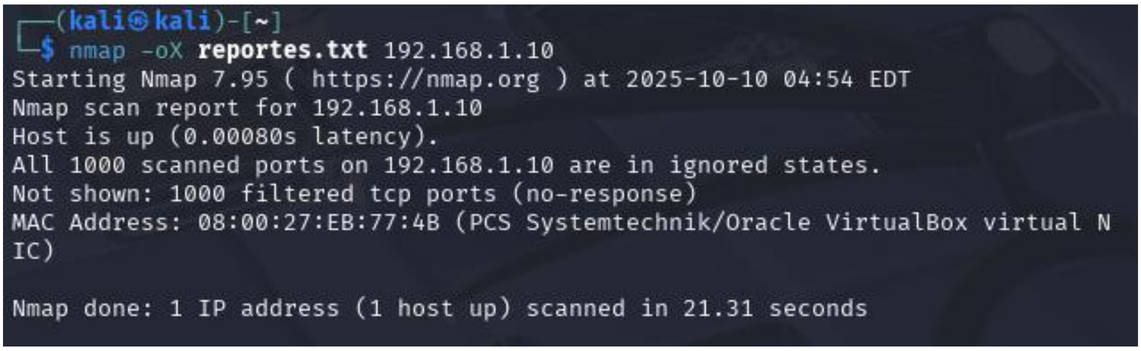
Metasploitable:



```
┌──(kali㉿kali)-[~]
└─$ nmap -oN reportes.txt 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:52 EDT
Nmap scan report for 192.168.1.12
Host is up (0.0068s 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
```

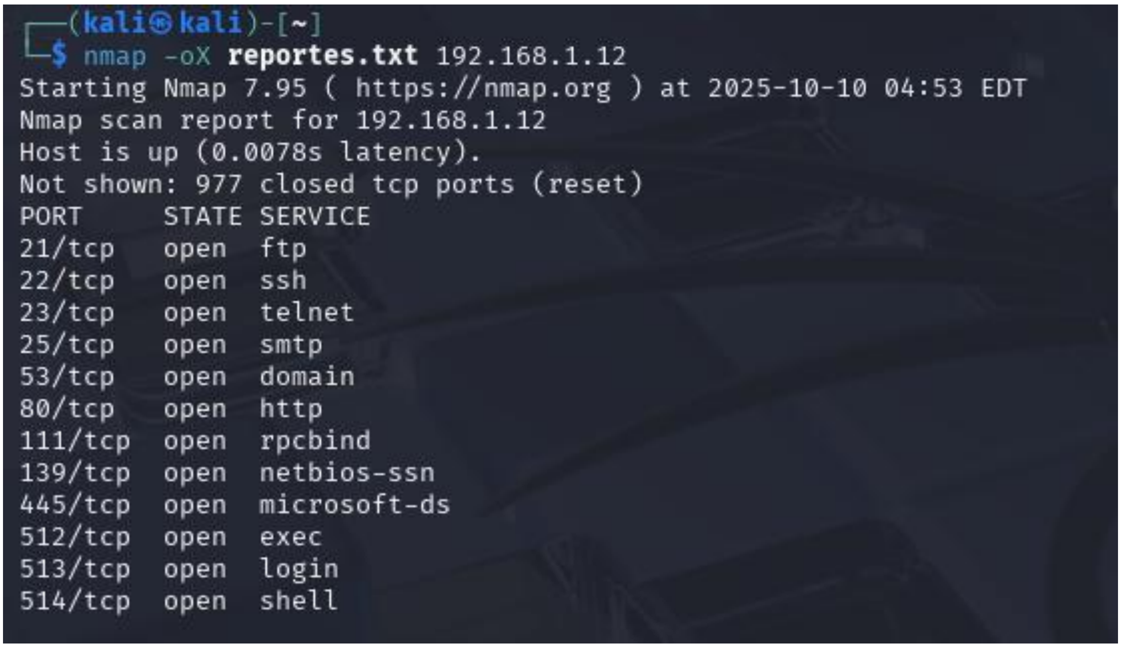
- Exportar en formato XML (-oX) para procesamiento automático

  Windows:



```
┌──(kali㉿kali)-[~]
└─$ nmap -oX reportes.txt 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:54 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00080s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 21.31 seconds
```

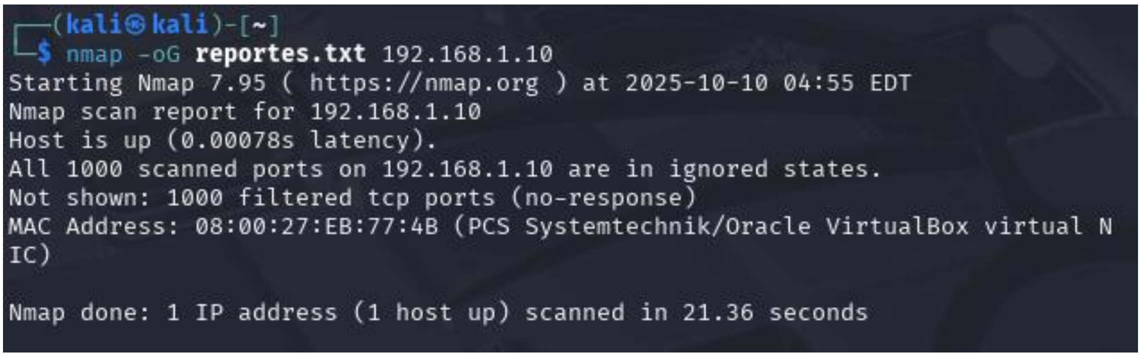
Metasploitable:



```
┌──(kali㉿kali)-[~]
└─$ nmap -oX reportes.txt 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:53 EDT
Nmap scan report for 192.168.1.12
Host is up (0.0078s 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
```

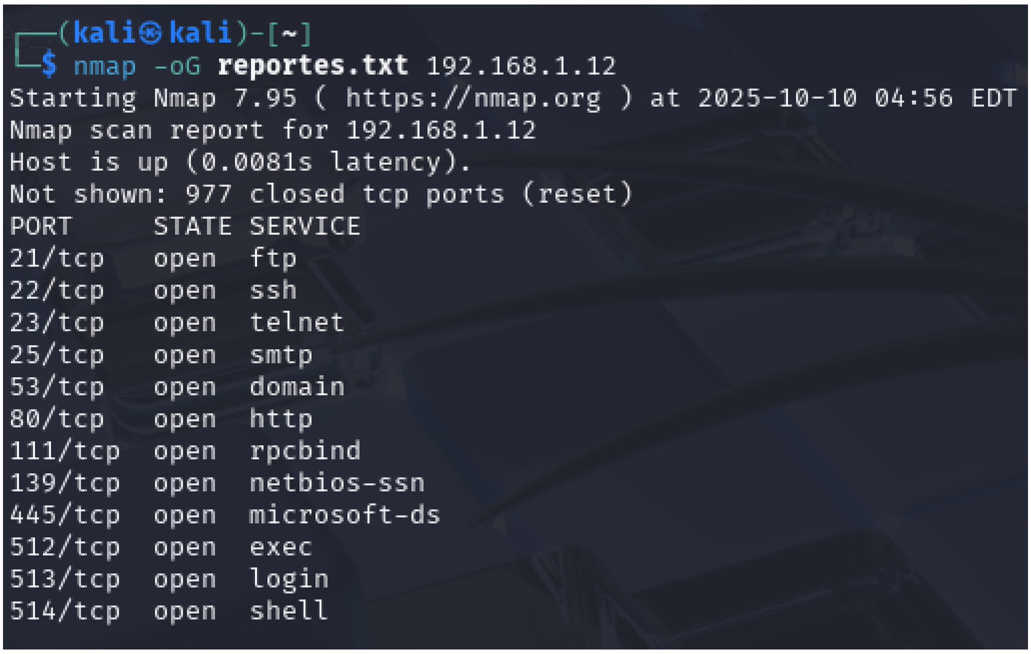
- Generar reporte legible (-oG)

  Windows:



```
┌──(kali㉿kali)-[~]
└─$ nmap -oG reportes.txt 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:55 EDT
Nmap scan report for 192.168.1.10
Host is up (0.00078s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:EB:77:4B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 21.36 seconds
```

Metasploitable:



```
┌──(kali㉿kali)-[~]
└─$ nmap -oG reportes.txt 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:56 EDT
Nmap scan report for 192.168.1.12
Host is up (0.0081s 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
```

Ejercicio 4.2 - Análisis de Resultados

# Analizar hallazgos de seguridad

Tareas:

- Identificar 3 servicios con versiones potencialmente vulnerables
- Priorizar riesgos según criticidad
- Proponer recomendaciones de seguridad
  - **vsftpd 2.3.4 (puerto 21/tcp) -** permite la ejecución remota de código mediante una puerta trasera oculta.
    Riesgo: Crítico
    Recomendación: Actualizar o deshabilitar el servicio FTP, y restringir acceso mediante firewall.
  - **Apache httpd 2.2.8 (puerto 80/tcp) -** vulnerabilidades de desbordamiento y ejecución remota.
    Riesgo: Alto
    Recomendación: Actualizar a una versión estable actual (2.4.x o superior) y habilitar HTTPS.
  - **Samba smbd 3.0.20 -** permite ejecución de código remoto.
    Riesgo: Alto
    Recomendación: Restringir el servicio SMB solo a redes internas seguras y actualizar a una versión más reciente.