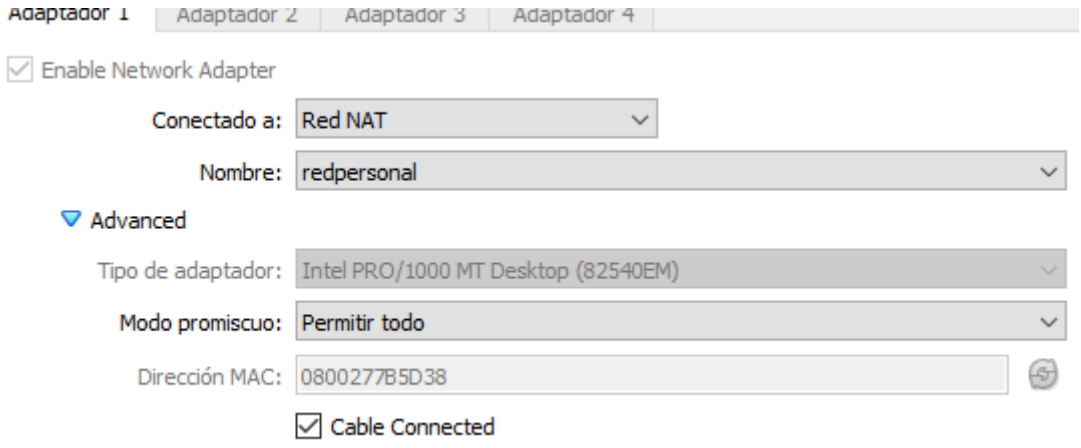
EJERCICIOS ESCÁNER DE RED NMAP

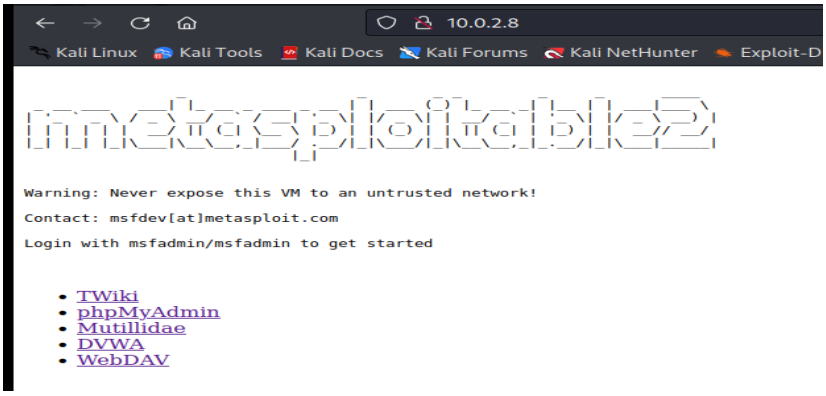
Prerrequisitos

- Kali Linux
- Metasploitable2

Creación del laboratorio

- Descarga la imagen de máquina virtual de Metasploitable2:
  - https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- Sigue esta guía de instalación para crear la máquina virtual Metasploitable2:
  - https://www.hacking-tutorial.com/tips-and-trick/install-metasploitable-on-virtual-box/
- Utiliza la siguiente configuración para las máquinas virtuales Metasploitable2 y Kali
  - Linux: Configuración > Red > Adaptador 1 > Red NAT > NatNetwork > Aceptar





- Enciende las máquinas virtuales, Metasploitable2 y Kali Linux, y comprueba:
  - Dirección IP de Kali Linux

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe4b:1f9f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:4b:1f:9f  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 650 (650.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 2822 (2.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Direccion IP de Metasploitable

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:7b:5d:38
          inet addr:10.0.2.8  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7b:5d38/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5250 (5.1 KB)  TX bytes:7298 (7.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

    - Haz ping para comprobar la conectividad entre ellas

CONECTIVIDAD COMPROBADA

```
└─# ping 10.0.2.8
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data.
64 bytes from 10.0.2.8: icmp_seq=1 ttl=64 time=0.518 ms
64 bytes from 10.0.2.8: icmp_seq=2 ttl=64 time=1.78 ms
64 bytes from 10.0.2.8: icmp_seq=3 ttl=64 time=2.02 ms
64 bytes from 10.0.2.8: icmp_seq=4 ttl=64 time=1.78 ms
64 bytes from 10.0.2.8: icmp_seq=5 ttl=64 time=1.06 ms
64 bytes from 10.0.2.8: icmp_seq=6 ttl=64 time=1.74 ms
64 bytes from 10.0.2.8: icmp_seq=7 ttl=64 time=2.09 ms
64 bytes from 10.0.2.8: icmp_seq=8 ttl=64 time=1.38 ms
64 bytes from 10.0.2.8: icmp_seq=9 ttl=64 time=2.05 ms
64 bytes from 10.0.2.8: icmp_seq=10 ttl=64 time=0.452 ms
64 bytes from 10.0.2.8: icmp_seq=11 ttl=64 time=1.91 ms
64 bytes from 10.0.2.8: icmp_seq=12 ttl=64 time=1.81 ms
64 bytes from 10.0.2.8: icmp_seq=13 ttl=64 time=1.86 ms
64 bytes from 10.0.2.8: icmp_seq=14 ttl=64 time=0.384 ms
64 bytes from 10.0.2.8: icmp_seq=15 ttl=64 time=1.39 ms
64 bytes from 10.0.2.8: icmp_seq=16 ttl=64 time=0.582 ms
64 bytes from 10.0.2.8: icmp_seq=17 ttl=64 time=0.778 ms
64 bytes from 10.0.2.8: icmp_seq=18 ttl=64 time=0.419 ms
64 bytes from 10.0.2.8: icmp_seq=19 ttl=64 time=1.52 ms
64 bytes from 10.0.2.8: icmp_seq=20 ttl=64 time=1.38 ms
64 bytes from 10.0.2.8: icmp_seq=21 ttl=64 time=1.66 ms
64 bytes from 10.0.2.8: icmp_seq=22 ttl=64 time=0.632 ms
64 bytes from 10.0.2.8: icmp_seq=23 ttl=64 time=1.46 ms
64 bytes from 10.0.2.8: icmp_seq=24 ttl=64 time=0.712 ms
```

```
── 10.0.2.8 ping statistics ──
185 packets transmitted, 185 received, 0% packet loss, time 186255ms
rtt min/avg/max/mdev = 0.199/1.210/2.123/0.572 ms
```

- En caso de obtener resultado negativo, revisa todos los pasos comenzando de nuevo desde el principio.
  En caso de obtener resultado positivo, realiza los siguientes ejercicios

Ejercicio 1 - Nmap

- Descubre los equipos conectados a la Red NAT 10.0.2.X/255.255.255.0 o /24

```
┌──(root㉿kali)-[~]
└─# nmap -sn 10.0.2.0-255
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 21:47 CET
Nmap scan report for 10.0.2.1
Host is up (0.00038s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00036s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00035s latency).
MAC Address: 08:00:27:AF:65:A1 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.8
Host is up (0.00098s latency).
MAC Address: 08:00:27:7B:5D:38 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.12 seconds
```

- Comprueba que la IP de la máquina Metasploitable2 aparece

La máquina metasploit aparece entre las escanedas.

```
Nmap scan report for 10.0.2.8
Host is up (0.00098s latency).
MAC Address: 08:00:27:7B:5D:38 (Oracle VirtualBox virtual NIC)
```

Ejercicio 2 – Nmap

- Escanea los puertos de la máquina Metasploitable2

```
┌──(root㉿kali)-[~]
└─# nmap -p- 10.0.2.8-255 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 21:50 CET
Nmap scan report for 10.0.2.8
Host is up (0.000077s 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
36501/tcp open  unknown
44235/tcp open  unknown
53693/tcp open  unknown
60883/tcp open  unknown
MAC Address: 08:00:27:7B:5D:38 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 248 IP addresses (2 hosts up) scanned in 12.10 seconds
```

Ejercicio 3 - Nmap

Realiza un esquema de la siguiente forma:

- PUERTO - ESTADO - SERVICIO - QUE HACE ESTE SERVICIO para todos los puertos del equipo

En este punto realice el escaneo de los 65535 puertos TCP, y este fue el resultado, no obstante quise escanear los puertos UDP pero el tiempo de espera era sumamente largo (puede que sea mi maquina), por otro lado dejo dos resultados teniendo en cuenta el esquema solicitado, utilice el comando -vv para poder hallar REASON y detectar que hace el servicio (no se si es correcto).

```
┌──(root㉿kali)-[~]
└─# nmap -p- -sS 10.0.2.8-255 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 22:26 CET
Nmap scan report for 10.0.2.8
Host is up (0.000056s 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
36501/tcp open  unknown
44235/tcp open  unknown
53693/tcp open  unknown
60883/tcp open  unknown
MAC Address: 08:00:27:7B:5D:38 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 248 IP addresses (2 hosts up) scanned in 9.60 seconds
```

```
Nmap scan report for 10.0.2.8
Host is up, received arp-response (0.000048s latency).
Scanned at 2022-12-14 03:23:25 CET for 1s
Not shown: 65505 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
3632/tcp  open  distccd      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
6697/tcp  open  ircs-u       syn-ack ttl 64
8009/tcp  open  ajp13        syn-ack ttl 64
8180/tcp  open  unknown      syn-ack ttl 64
8787/tcp  open  msgsrvr      syn-ack ttl 64
38616/tcp open  unknown      syn-ack ttl 64
38955/tcp open  unknown      syn-ack ttl 64
45838/tcp open  unknown      syn-ack ttl 64
53845/tcp open  unknown      syn-ack ttl 64
MAC Address: 08:00:27:7B:5D:38 (Oracle VirtualBox virtual NIC)
```

- Busca información de los puertos y servicios según el resultado de Nmap en Google

Según el primer screen del primer escaneo los puertos abiertos son:

- 21-ftp: es un protocolo de Internet que permite a las computadoras dentro de la red intercambiar archivos de forma masiva.

- 22-ssh: sirve para acceder a máquinas remotas a través de una red y manejar por completo el sistema mediante un intérprete de comandos.

- 23-telnet: Telnet, sirve para establecer conexión remotamente con otro equipo por la línea de comandos y controlarlo. Es un protocolo no seguro ya que la autenticación y todo el tráfico de datos se envía sin cifrar.

- 25-smtp: es el puerto, o la conexión, de la computadora por el que deben pasar los correos electrónicos salientes. El bloqueo del Puerto 25 evita que los piratas informáticos envíen correos electrónicos basura no autorizados de forma masiva.

- 53-domain: Es usado por el servicio de DNS, Domain Name System.

- 80-http: Este puerto es el que se usa para la navegación web de forma no segura HTTP.

- 111-rpcbing: garantiza la entrega de paquetes de datos en la misma orden, en que fueron mandados. La comunicación garantizada por el puerto TCP 111 es la diferencia mayor entre TCP y UDP

- 139-netbios ssn: es un puerto TCP que funciona cuando se accede a un archivo compartido o a una impresora compartida en su LAN a través de la red.

- 445-microsoft-ds: El puerto TCP 445 se utiliza para el acceso directo a redes TCP / IP MS que no requiere el uso de una capa NetBIOS.

- 512-exec: es un Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión, necesita el apretón de manos para determinar comunicaciones de principio a fin.

- 513-login: garantiza la entrega de paquetes de datos en la misma orden, en que fueron mandados. La comunicación garantizada por el puerto

- 514-Shell: Es usado por Syslog, el log del sistema operativo

- 1099-rmiregistry: garantiza la entrega de paquetes de datos en la misma orden, en que fueron mandados

- 1524-ingreslock: garantiza la entrega de paquetes de datos en la misma orden, en que fueron mandados

- 2049-nfs: es utilizado para que cualquier aplicación acceda a los sistemas de archivos "NFS" (en inglés: Network File System).

- 2121-ccproxy-ftp: es un protocolo orientado en la conexión, necesita el apretón de manos para determinar comunicaciones de principio a fin. Solo cuando la conexión es determinada, los datos del usuario pueden ser mandados de modo bidireccional por la conexión.

- 3306: mysql: es el puerto por defecto usado para el protocolo MySQL. Lo usarás para conectar con clientes de MySQL y utilidades como mysqldump.

- 3632 distccd: es el puerto para acceder a otro dispositivo.

- 5432-postgresql: Este es el puerto PostgreSQL por defecto.

- 5900-vnc: VNC es un software libre de escritorio remoto basado en la estructura cliente-servidor. Permite controlar el equipo servidor.

- 6000-x11: usa el Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión.

- 6667-irc: Es el puerto desde el cual una computadora envía y recibe comunicaciones y mensajes basados en clientes web desde un servidor web.

- 6697-ircs-u: en el cliente para conectarse a través de SSL

- 8009-ajp13: garantiza la entrega de paquetes de datos en la misma orden, en que fueron mandados. La comunicación garantizada por el puerto TCP 8009 es la diferencia mayor entre TCP y UDP.

- 8180-desconocido: El puerto TCP 8180 usa el Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión, necesita el apretón de manos para determinar comunicaciones de principio a fin

- 8787-msgsrvr: garantiza la entrega de paquetes de datos en la misma orden, en que fueron mandados.

- 36501-desconocido: l puerto TCP 36501 usa el Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión.

- 44235-desconocido: usa el Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión.

- 53693-desconocido: usa el Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión.

- 60883-desconocido: usa el Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión.

Ejercicio 4 - Nmap

¿Qué versión de sistema operativo utiliza?

```
┌──(root㉿kali)-[~]
└─# nmap -p- -O 10.0.2.8 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 22:15 CET
Nmap scan report for 10.0.2.8
Host is up (0.0012s 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
36501/tcp open  unknown
44235/tcp open  unknown
53693/tcp open  unknown
60883/tcp open  unknown
MAC Address: 08:00:27:7B:5D:38 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds
```

Ejercicio 5 - Nmap

Completa el esquema del ejercicio 3 con la versión de los servicios desplegados.

- PUERTO - ESTADO - SERVICIO - VERSION DEL SERVICIO

```
┌──(root㉿kali)-[~]
└─# nmap -p- -sSV 10.0.2.8-255 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 22:36 CET
Nmap scan report for 10.0.2.8
Host is up (0.000057s latency).
Not shown: 65505 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  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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
36501/tcp open  java-rmi    GNU Classpath grmiregistry
44235/tcp open  nlockmgr    1-4 (RPC #100021)
53693/tcp open  mountd      1-3 (RPC #100005)
60883/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:7B:5D:38 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 248 IP addresses (2 hosts up) scanned in 136.89 seconds
```

Ejercicio 6 - Nmap, Http, Netcat y Telnet

- Comprueba manualmente la versión de dos de los servicios levantados utilizando nc, telnet y navegador web

Abajo se divisa la versión y servicio obtenido con la herramienta netcat

```
┌──(root㉿kali)-[~]
└─#  nc 10.0.2.8 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

En cuanto al comando telnet, con esta herramienta podemos conectarnos a un dispositivo en red siempre que el puerto al que llamemos este abierto. El puerto 25 en este caso se encuentra abierto por lo que se produjo la conexión,

```
┌──(root㉿kali)-[/]
└─# telnet --ipv4 10.0.2.8 25
Trying 10.0.2.8 ...
Connected to 10.0.2.8.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

El puerto 443 no se encuentra abierto por ende rechaza la conexión.

```
┌──(root㉿kali)-[~]
└─# telnet --ipv4 10.0.2.8 443
Trying 10.0.2.8 ...
telnet: Unable to connect to remote host: Conexión rehusada
```

En cuanto al navegador web, he realizado la búsqueda y efectivamente se encuentra expuesta información sensible acerca del servidor de esta maquina.

Utilice http://10.0.0.8:80 para llegar a este resultado.

Index of /dav

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 10.0.2.8 Port 80