

Actividad 8: Seguridad en redes

Seguridad Informática

13/11/2014

Brais López Yáñez

Índice

Objetivos de la práctica.....	3
Pasos Iniciales.....	3
Configuración de las máquinas	3
Ejercicio 1	4
TELNET.....	4
CONEXIÓN WEB.....	6
SSH.....	7
Conclusión	8
Ejercicio 2	8
NMAP	8
NMAP escaneo silencioso	11
Interfaz gráfico NMAP	11
Conclusión	12

Objetivos de la práctica

En esta sesión realizaremos dos actividades:

- Una sesión de interceptación de mensajes utilizando el sniffer/analizador de redes WIRESHARK, para comprobar la vulnerabilidad de los servicios que no usan cifrado.
- Una sesión de recopilación de información empleando el escáner de puertos NMAP.

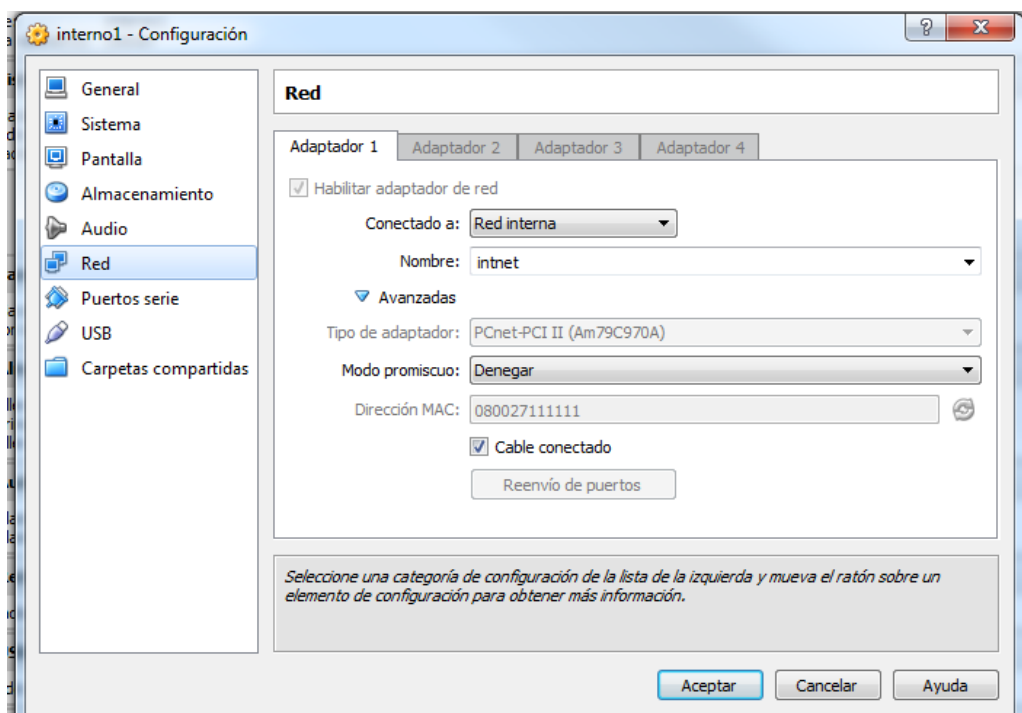
Pasos Iniciales

Creación de las tres máquinas virtuales con virtual box. Las máquinas virtuales interno1 e interno2 utilizaremos la imagen texto.vdi. Para la otra, observador usaremos la imagen grafico.vdi, que tiene entorno gráfico instalado.

Configuración de las máquinas

	Interno1	Interno1	Observador
Almacenamiento	Controlador IDE: texto.vdi	Controlador IDE: texto.vdi	Controlador IDE: grafico.vdi
Tipo de red	Red interna	Red interna	Red interna
MAC	080027111111	080027222222	080027333333
Modo tarjeta	-	-	Modo promiscuo
IP	192.168.100.11	192.168.100.22	192.168.100.33

Ejemplo de modificación de interno1



Ejercicio 1

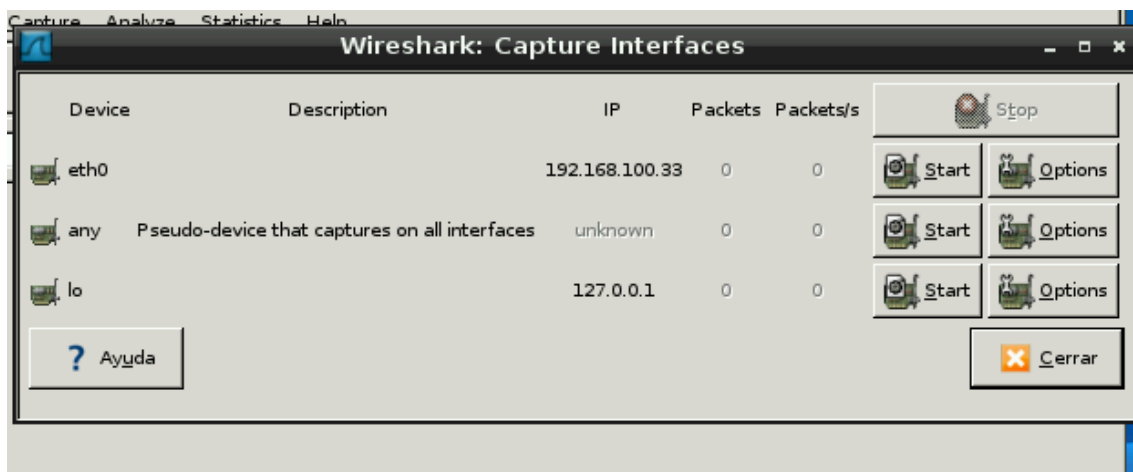
El primer ejercicio consistirá en el uso de la herramienta *WIRESHARK* desde el equipo observador para interceptar el tráfico *TELNET*, *HTTP* y *SSH* entre los equipos interno1 e interno2.

WIRESHARK es un sniffer y analizador de protocolos que recopila los paquetes que fluyen por la red, los analiza, extrae el contenido de los campos de diferentes protocolos y los presenta al usuario.

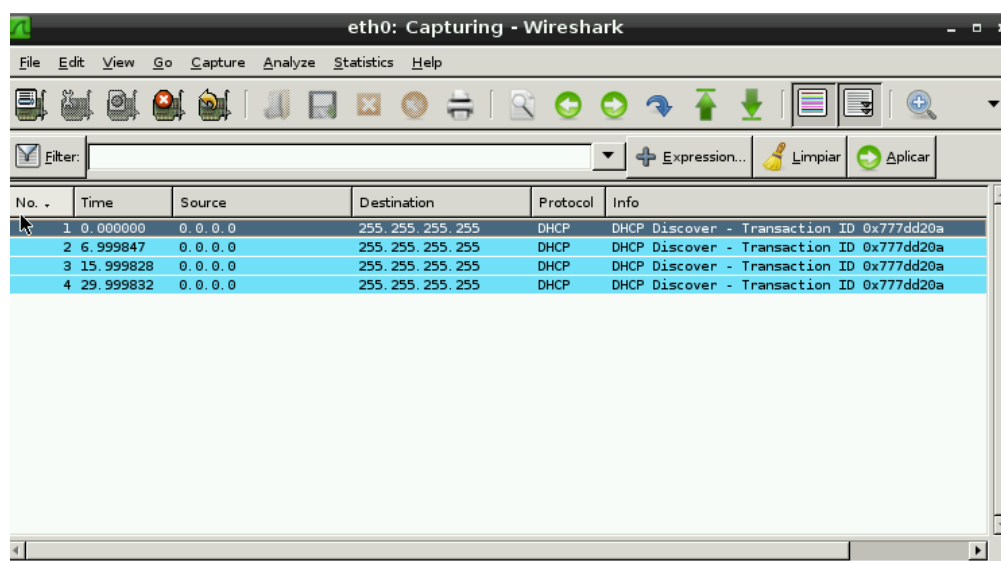
TELNET

1. En la máquina observador arrancamos en modo gráfico, con el comando `startx`, una vez en modo gráfico iniciamos el *WIRESHARK*. Accedemos al botón interfaces y seleccionamos `eth0` para comenzar la escucha.

Ventana para iniciar la escucha



Ventana de la escucha



2. El siguiente paso que hacemos es hacer algún movimiento entre las dos máquinas para que quede registrado, y pueda captarlo el observador. Esto se realizará a través del comando TELNET, con el cual en interno2 nos conectamos a interno1:

Comando: telnet usuario1 192.168.100.11

```

individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
interno2:~# telnet 192.168.100.11
Trying 192.168.100.11...
Connected to 192.168.100.11.
Escape character is '^J'.

Linux 2.6.26-1-686 (::ffff:192.168.100.22) (pts/0)

interno1 nombre: usuario1
usuario1
Contraseña:usuario1

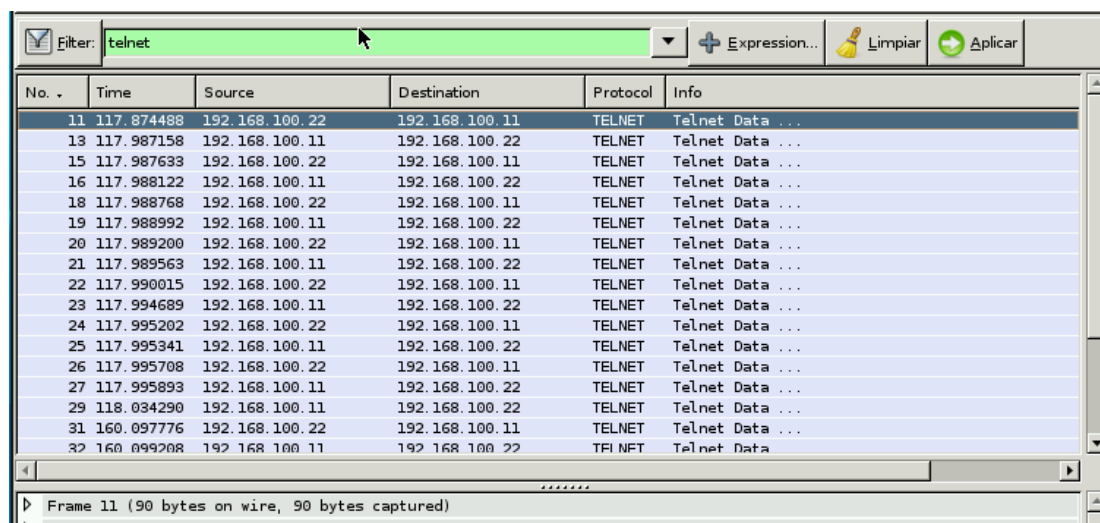
Último inicio de sesión:jue abr 23 20:50:47 CEST 2009de localhosten pts/0
Linux ligero 2.6.26-1-686 #1 SMP Sat Jan 10 18:29:31 UTC 2009 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
usuario1@interno1:~$ _
  
```

Después de realizar algunas acciones (ls, cd, ...) en interno2, paramos la escucha e rastreamos los datos obtenidos:

No. -	Time	Source	Destination	Protocol	Info
28	118.034014	192.168.100.22	192.168.100.11	TCP	52017 > telnet [ACK] Seq=154 Ack=151 Win=5888
29	118.034290	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
30	118.034637	192.168.100.22	192.168.100.11	TCP	52017 > telnet [ACK] Seq=154 Ack=170 Win=5888
31	160.097776	192.168.100.22	192.168.100.11	TELNET	Telnet Data ...
32	160.099208	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
33	160.100610	192.168.100.22	192.168.100.11	TCP	52017 > telnet [ACK] Seq=163 Ack=181 Win=5888
34	160.452869	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
35	160.453605	192.168.100.22	192.168.100.11	TCP	52017 > telnet [ACK] Seq=163 Ack=182 Win=5888
36	160.453616	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
37	160.453618	192.168.100.22	192.168.100.11	TCP	52017 > telnet [ACK] Seq=163 Ack=195 Win=5888
38	163.232590	192.168.100.22	192.168.100.11	TELNET	Telnet Data ...
39	163.234657	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
40	163.234838	192.168.100.22	192.168.100.11	TCP	52017 > telnet [ACK] Seq=172 Ack=198 Win=5888
41	163.555499	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
42	163.555747	192.168.100.22	192.168.100.11	TCP	52017 > telnet [ACK] Seq=172 Ack=637 Win=6912
43	163.587903	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
44	163.588847	192.168.100.22	192.168.100.11	TCP	52017 > telnet [ACK] Seq=172 Ack=659 Win=6912

Filtrado con la palabra telnet


No.	Time	Source	Destination	Protocol	Info
11	117.874488	192.168.100.22	192.168.100.11	TELNET	Telnet Data ...
13	117.987158	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
15	117.987633	192.168.100.22	192.168.100.11	TELNET	Telnet Data ...
16	117.988122	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
18	117.988768	192.168.100.22	192.168.100.11	TELNET	Telnet Data ...
19	117.988992	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
20	117.989200	192.168.100.22	192.168.100.11	TELNET	Telnet Data ...
21	117.989563	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
22	117.990015	192.168.100.22	192.168.100.11	TELNET	Telnet Data ...
23	117.994689	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
24	117.995202	192.168.100.22	192.168.100.11	TELNET	Telnet Data ...
25	117.995341	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
26	117.995708	192.168.100.22	192.168.100.11	TELNET	Telnet Data ...
27	117.995893	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
29	118.034290	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...
31	160.097776	192.168.100.22	192.168.100.11	TELNET	Telnet Data ...
32	160.099208	192.168.100.11	192.168.100.22	TELNET	Telnet Data ...

Los campos obtenidos son: el tiempo, la IP que manda el paquete, la IP que recibe el paquete, y el protocolo usado.

Al hacer clickar en una fila tenemos más información, como:

Frame: muestra el tiempo empleado en cada operación.

Ethernet: indica las direcciones de red implicadas en el envío del paquete.

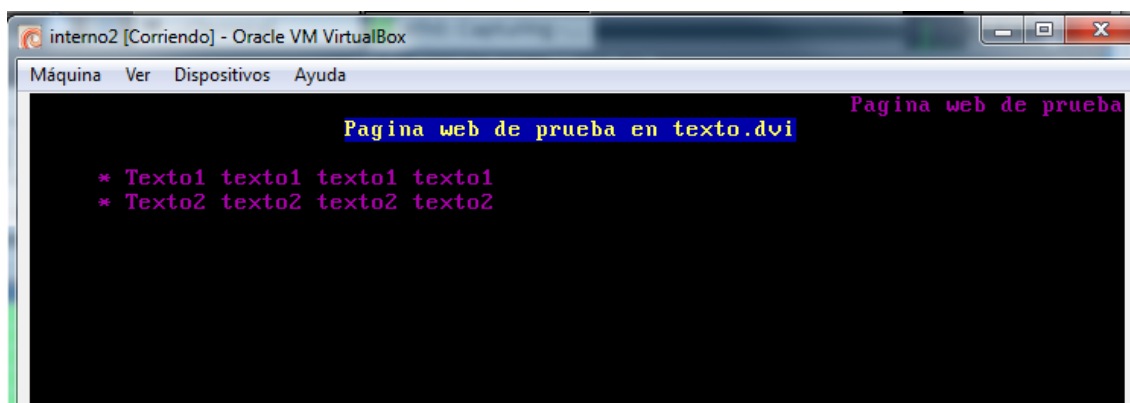
Internet Protocol: Nos da más información sobre el protocolo de Internet utilizado en ambos casos, longitud de los paquetes, tiempo de vida, etc.

Transmission protocol control: muestra la transmisión del protocolo con datos específicos del puerto.

CONEXIÓN WEB

En este apartado, al igual que hiciéramos con TELNET, volveremos a hacer los mismos pasos dejando el observador con el Wireshark en modo escucha, y esta vez nos conectaremos a interno1 con interno2 con el siguiente comando:

interno2:~# lynx 192.168.100.11



Una vez procedida la ejecución revisamos los datos escuchados con Wireshark, y podemos acceder a los mismos datos sin problemas, solo que esta vez el tipo de protocolo cambia.

SSH

En esta parte de la práctica volvemos a repetir los pasos anteriores y nos conectamos a interno2, mediante ssh, volvemos a realizar varias acciones:

interno2:~# ssh usuario1@192.168.100.11

```

interno2:~# ssh usuario1@192.168.100.11
usuario1@192.168.100.11's password:
Linux ligero 2.6.26-1-686 #1 SMP Sat Jan 10 18:29:31 UTC 2009 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov 6 18:52:34 2014 from 192.168.100.22
usuario1@interno1:~$ ls -la
total 24
drwxr-xr-x 2 usuario1 usuario1 4096 abr 23  2009 .
drwxr-xr-x 3 root      root      4096 abr 10  2009 ..
-rw-r--r-- 1 usuario1 usuario1  57 nov  6 18:52 .bash_history
-rw-r--r-- 1 usuario1 usuario1 220 abr 10  2009 .bash_logout
-rw-r--r-- 1 usuario1 usuario1 3116 abr 10  2009 .bashrc
-rw-r--r-- 1 usuario1 usuario1  675 abr 10  2009 .profile
usuario1@interno1:~$ ls
usuario1@interno1:~$ cd ..
usuario1@interno1:/home$ ls
usuario1
usuario1@interno1:/home$ _

```

No. °	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.100.22	192.168.100.11	TCP	47672 > ssh [SYN] Seq=0 Win=5840 Len=0 MSS=146
2	0.000013	192.168.100.11	192.168.100.22	TCP	ssh > 47672 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
3	0.000267	192.168.100.22	192.168.100.11	TCP	47672 > ssh [ACK] Seq=1 Ack=1 Win=5888 Len=0
4	0.009802	192.168.100.11	192.168.100.22	SSH	Server Protocol: SSH-2.0-OpenSSH_5.1p1 Debian-!
5	0.010143	192.168.100.22	192.168.100.11	TCP	47672 > ssh [ACK] Seq=1 Ack=33 Win=5888 Len=0
6	0.010563	192.168.100.22	192.168.100.11	SSH	Client Protocol: SSH-2.0-OpenSSH_5.1p1 Debian-!
7	0.010573	192.168.100.11	192.168.100.22	TCP	ssh > 47672 [ACK] Seq=33 Ack=33 Win=5824 Len=0
8	0.011061	192.168.100.22	192.168.100.11	SSHv2	Client: Key Exchange Init
9	0.011072	192.168.100.11	192.168.100.22	TCP	ssh > 47672 [ACK] Seq=33 Ack=825 Win=7424 Len=0
10	0.011862	192.168.100.11	192.168.100.22	SSHv2	Server: Key Exchange Init
11	0.012292	192.168.100.22	192.168.100.11	SSHv2	Client: Diffie-Hellman GEX Request
12	0.015199	192.168.100.11	192.168.100.22	SSHv2	Server: Diffie-Hellman Key Exchange Reply
13	0.018337	192.168.100.22	192.168.100.11	SSHv2	Client: Diffie-Hellman GEX Init
14	0.042260	192.168.100.11	192.168.100.22	SSHv2	Server: Diffie-Hellman GEX Reply
15	0.046228	192.168.100.22	192.168.100.11	SSHv2	Client: New Keys
16	0.084967	192.168.100.11	192.168.100.22	TCP	ssh > 47672 [ACK] Seq=1689 Ack=1009 Win=8960 Len=0
17	0.085211	192.168.100.22	192.168.100.11	SSHv2	Encrypted request packet len=48

Con SSH la cosa ya cambia, este encripta los paquetes. Cuando intentamos acceder a la escucha y ver el contenido de esta, ya no somos capaces de acceder al contenido en texto plano del paquete.

Conclusión

Del programa usado, *WIRESHARK*, para que funcione correctamente necesitamos ejecutarlo como superusuario. Pero esto, podría causar un fallo en el sistema, si en la escucha o al analizar los datos, se produjese un error.

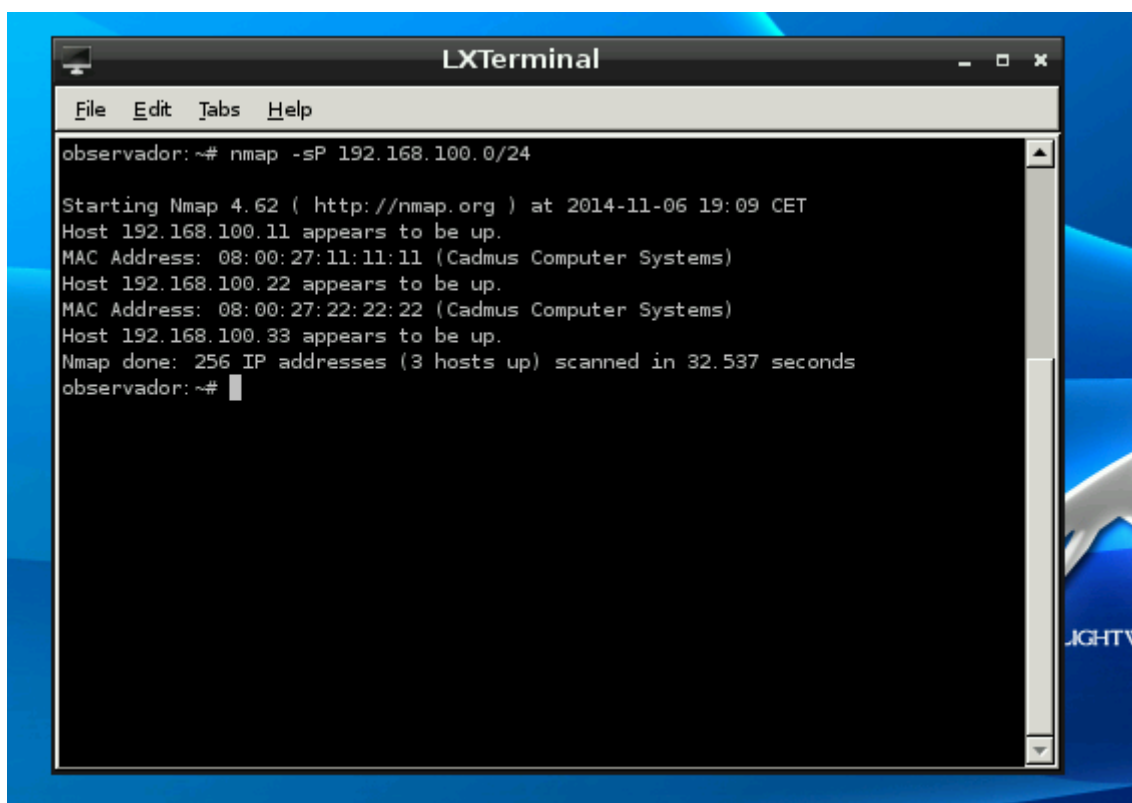
Podemos acabar esta primera parte de la actividad, concluyendo que la conexión *SSH* es la más segura de todas estas, ya que esta encripta los datos de los paquetes y dificulta su escucha. Por el contrario *HTTP* y *TELNET*, no transmiten los paquetes cifrados, por lo que tienen menor seguridad que *SSH*.

Ejercicio 2

El segundo ejercicio consistirá en el uso de la herramienta de escaneo de puertos *NMAP* para obtener información de los equipos y servicios de la red. *NMAP* implementa diversas técnicas para extraer información de los equipos que forman parte de una red y para identificar los puertos y servicios que están disponibles en distintas máquinas. Algunos de los métodos disponibles realizan el escaneo sin dejar rastro, mientras que otros dejarán un rastro en los ficheros de log de las máquinas analizadas.

NMAP

Desde el observador, arrancamos una terminal y lanzamos un escaneo Ping Sweeping para identificar las máquinas que forman parte de nuestra red. Al lanzar el comando `nmap -sP 192.168.100.0/24`, podemos ver las máquinas anteriormente configuradas.

A screenshot of an LXTerminal window titled "LXTerminal". The terminal shows the execution of the command "nmap -sP 192.168.100.0/24". The output indicates that three hosts (192.168.100.11, 192.168.100.22, and 192.168.100.33) are up, all identified as "Cadmus Computer Systems" with MAC address "08:00:27:11:11:11". The scan took 32.537 seconds to complete. The terminal interface includes a menu bar with "File", "Edit", "Tabs", and "Help".

```
observador:~# nmap -sP 192.168.100.0/24

Starting Nmap 4.62 ( http://nmap.org ) at 2014-11-06 19:09 CET
Host 192.168.100.11 appears to be up.
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)
Host 192.168.100.22 appears to be up.
MAC Address: 08:00:27:22:22:22 (Cadmus Computer Systems)
Host 192.168.100.33 appears to be up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 32.537 seconds
observador:~#
```


Con los siguientes comandos, comprobamos los puertos que están abiertos:

observador:~# nmap -sT -v 192.168.100.11

observador:~# nmap -sT -v 192.168.100.22

Interno1

```
observador:~# nmap -sT -v 192.168.100.11

Starting Nmap 4.62 ( http://nmap.org ) at 2014-11-06 19:12 CET
Initiating ARP Ping Scan at 19:12
Scanning 192.168.100.11 [1 port]
Completed ARP Ping Scan at 19:12, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:12
Completed Parallel DNS resolution of 1 host. at 19:12, 13.00s elapsed
Initiating Connect Scan at 19:12
Scanning 192.168.100.11 [1715 ports]
Discovered open port 23/tcp on 192.168.100.11
Discovered open port 80/tcp on 192.168.100.11
Discovered open port 22/tcp on 192.168.100.11
Completed Connect Scan at 19:12, 1.33s elapsed (1715 total ports)
Host 192.168.100.11 appears to be up ... good.
Interesting ports on 192.168.100.11:
Not shown: 1712 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.508 seconds
Raw packets sent: 1 (42B) | Rcvd: 1 (42B)
observador:~#
```

Interno2:

```
observador:~# nmap -sT -v 192.168.100.22

Starting Nmap 4.62 ( http://nmap.org ) at 2014-11-06 19:13 CET
Initiating ARP Ping Scan at 19:13
Scanning 192.168.100.22 [1 port]
Completed ARP Ping Scan at 19:13, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:13
Completed Parallel DNS resolution of 1 host. at 19:14, 13.00s elapsed
Initiating Connect Scan at 19:14
Scanning 192.168.100.22 [1715 ports]
Discovered open port 22/tcp on 192.168.100.22
Completed Connect Scan at 19:14, 1.35s elapsed (1715 total ports)
Host 192.168.100.22 appears to be up ... good.
Interesting ports on 192.168.100.22:
Not shown: 1714 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:22:22:22 (Cadmus Computer Systems)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.553 seconds
Raw packets sent: 1 (42B) | Rcvd: 1 (42B)
observador:~#
```

En el siguiente caso probamos el mismo comando en interno1, con la opción -O para que NAMP trate de identificar el sistema operativo y -sV para los servicios que tiene activados.

observador:~# nmap -sT -O -sV 192.168.100.11

```

observador:~# nmap -sT -O -sV 192.168.100.11

Starting Nmap 4.62 ( http://nmap.org ) at 2014-11-06 19:16 CET
Interesting ports on 192.168.100.11:
Not shown: 1712 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      (protocol 2.0)
23/tcp    open  telnet   BSD-derived telnetd
80/tcp    open  http     Apache httpd 2.2.9 ((Debian))
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servi
cefp-submit.cgi :
SF-Port22-TCP:V=4.62%I=7%D=11/6%Time=545BBB28%P=i686-pc-linux-gnu%r(NULL,2
SF:0,"SSH-2\0-OpenSSH_5\0.lpl\x20Debian-5\r\n");
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.24
Uptime: 0.050 days (since Thu Nov 6 18:05:49 2014)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .

```

Verificamos si ha quedado rastro de las conexiones realizadas por NMAP, accediendo al fichero `/var/log/syslog`.

Interno1

```

GNU nano 2.0.7 Fichero: /var/log/syslog

Nov 6 19:16:24 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:16:39 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:16:41 ligero dhclient: No DHCP OFFERS received.
Nov 6 19:16:41 ligero dhclient: No working leases in persistent database - sle
Nov 6 19:17:01 ligero /usr/sbin/cron[1999]: (root) CMD ( cd / && run-parts -s
Nov 6 19:17:31 ligero telnetd[2002]: getpeername: Transport endpoint is not co
Nov 6 19:17:33 ligero telnetd[2004]: tloop: peer died: Resource temporarily $
Nov 6 19:23:56 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:24:02 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:24:10 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:24:25 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:24:41 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:24:53 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:24:57 ligero dhclient: No DHCP OFFERS received.
Nov 6 19:24:57 ligero dhclient: No working leases in persistent database - sle
Nov 6 19:30:39 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:30:47 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:31:03 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:31:23 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68
Nov 6 19:31:33 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 68

```

Interno2

```

GNU nano 2.0.7 Fichero: /var/log/syslog

Nov 6 18:08:07 ligero /usr/sbin/cron[1696]: (CRON) INFO (pidfile fd = 3)
Nov 6 18:08:07 ligero /usr/sbin/cron[1697]: (CRON) STARTUP (fork ok)
Nov 6 18:08:07 ligero /usr/sbin/cron[1697]: (CRON) INFO (Running @reboot jobs)
Nov 6 18:08:46 ligero kernel: [ 50.748805] eth1: link up
Nov 6 18:08:56 ligero kernel: [ 60.562872] usb 1-1: USB disconnect, address 2
Nov 6 18:08:57 ligero kernel: [ 61.138028] usb 1-1: new full speed USB device
Nov 6 18:08:57 ligero kernel: [ 61.383566] usb 1-1: configuration #1 chosen $
Nov 6 18:08:57 ligero kernel: [ 61.396733] input: VirtualBox USB Tablet as /$
Nov 6 18:08:57 ligero kernel: [ 61.437589] input,hidraw0: USB HID v1.10 Mous$
Nov 6 18:08:57 ligero kernel: [ 61.437748] usb 1-1: New USB device found, id$
Nov 6 18:08:57 ligero kernel: [ 61.437766] usb 1-1: New USB device strings: $
Nov 6 18:08:57 ligero kernel: [ 61.437782] usb 1-1: Product: USB Tablet
Nov 6 18:08:57 ligero kernel: [ 61.437797] usb 1-1: Manufacturer: VirtualBox
Nov 6 18:08:57 ligero kernel: [ 61.557220] eth1: no IPv6 routers present
Nov 6 18:17:01 ligero /usr/sbin/cron[1804]: (root) CMD ( cd / && run-parts -s
Nov 6 19:17:01 ligero /usr/sbin/cron[1821]: (root) CMD ( cd / && run-parts -s
Nov 6 19:40:30 ligero telnetd[1844]: getpeername: Transport endpoint is not co

```

NMAP escaneo silencioso

Procedemos a hacer lo mismo pero con un escaneo silenciosos de tipo SYN scanning, con los comandos:

```
observador:~# nmap -sS 192.168.100.11
```

```
observador:~# nmap -sS 192.168.100.22
```

Ejemplo de interno1

```
observador:~# nmap -sS 192.168.100.11

Starting Nmap 4.62 ( http://nmap.org ) at 2014-11-06 19:54 CET
Interesting ports on 192.168.100.11:
Not shown: 1712 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 14.506 seconds
observador:~# nmap -sS 192.168.100.22

Starting Nmap 4.62 ( http://nmap.org ) at 2014-11-06 19:54 CET
Interesting ports on 192.168.100.22:
Not shown: 1713 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 08:00:27:22:22:22 (Cadmus Computer Systems)
```

```
interno1 [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
GNU nano 2.0.7 Fichero: /var/log/syslog

Nov 6 19:49:02 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:49:07 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:49:12 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:49:19 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:49:27 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:49:43 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:49:50 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:49:57 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:50:03 ligero dhclient: No DHCP OFFERS received.
Nov 6 19:50:03 ligero dhclient: No working leases in persistent database - sle$
Nov 6 19:55:08 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:55:16 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:55:26 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:55:41 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:55:55 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:56:07 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 6$
Nov 6 19:56:09 ligero dhclient: No DHCP OFFERS received.
Nov 6 19:56:09 ligero dhclient: No working leases in persistent database - sle$
```

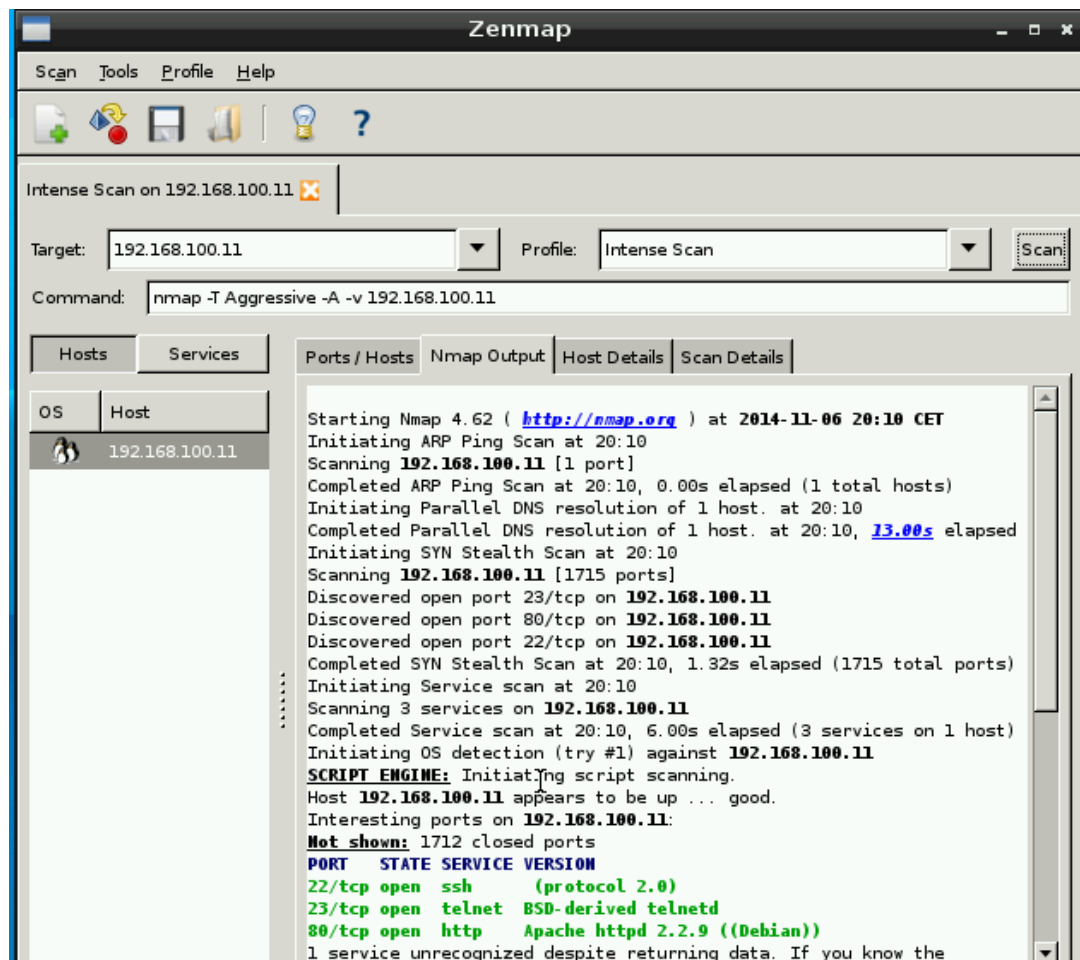
Omitimos la información de interno2, ya que llegamos a la misma conclusión que interno1. Esta sería, que al ejecutar el escaneo silencioso no quedan constancia de los datos de la conexión en el fichero syslog.

Interfaz gráfico NMAP

Para acabar con el ejercicio 2: existe un interfaz gráfico para NMAP que se puede arrancar desde el entorno gráfico de observador, para probar otras opciones de escáner.

Ejecutamos el siguiente comando (a pesar de tener la opción de poder seleccionarlo):

observador:~# zenmap &



Conclusión

NMAP como indicábamos en el principio del ejercicio 2, nos muestra la información de los equipos y red, esta información va a servir para evaluar la seguridad del sistema y usarla a nuestra favor.

Sin embargo, también se puede usar con fines mal intencionados ya que nos muestra los puertos que están abiertos, pero lo que no muestra NMAP es la información personal del usuario.

Para concluir con el ejercicio 2, NMAP presenta diversas opciones a la hora de realizar las escuchas, ya que estas pueden ser silenciosas y servir para evitar quedar registradas. Todo dependerá de la utilidad que quiera desempeñar el usuario que la use, como en todo, para fines contra la seguridad o a favor de esta.