

Introducción a las redes

PRÁCTICA I (PARTE I)

Los objetivos de esta práctica son los siguientes:

I. DEMONIOS EN LINUX

1. Estudiar los servicios (demonios) en Linux y el proceso de conexión cliente-servidor.
2. Instalar, arrancar y administrar dos tipos de demonios en Linux:
 - a. Los demonios dependientes y gestionados por el súper demonio de red o súper servidor. Es este súper demonio el que escucha y arranca los demonios al llegar una petición al puerto correspondiente.
 - b. Se elegirán en este caso los demonios ftpd y telnetd, que deberán arrancarse mediante el súper demonio de red Inetd.
 - c. Los demonios *standalone*, llamados así porque funcionan de forma independiente del súper demonio de red.

Para ello instalaremos tres servicios: FTP/Telnet (ambos deberán arrancarse mediante el súper demonio de red Inetd) y SSH, (Open SSH)

II. USO DEL WIRESHARK COMO SNIFFER

1. Uso de un sniffer como el Wireshark para:
 - a. Identificar los paquetes del Three-way handshake
 - b. Identificar las características más importantes de los paquetes enviados: direcciones IP origen y destino, flags, número de secuencia y número ack (Leer artículo de la revista Hackxcrack “1-port_scanning_hxc.pdf”, pags. 59-61).

2. Capturar los paquetes con el nombre de usuario y contraseña en una sesión ftp y telnet (no cifrada) y en una sesión ssh y sftp (cifrada) para ver sus datos, en este caso los usuarios y contraseñas:
 - a. En texto claro en telnet y en ftp
 - b. Cifradas mediante claves pública y privada en SSH (ya explicaremos este método de cifrado en el curso más adelante)

III. USO DE NMAP PARA ESCANEAR PUERTOS

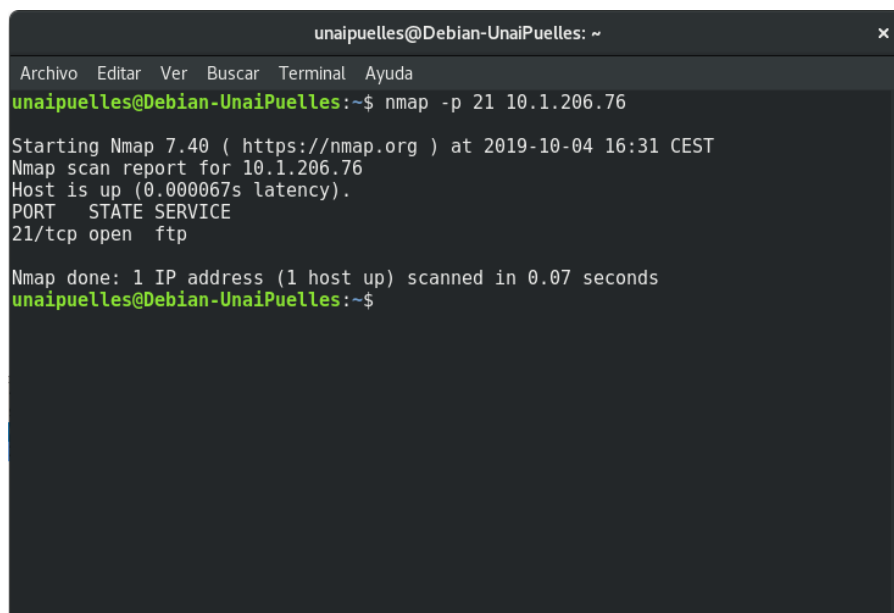
1. Aprender a usar nmap para escanear puertos
2. Entender los diferentes tipos de escaneo que hay y el uso de los distintos flags en los paquetes TCP/IP

ACTIVIDADES

PARTE 1

1. Instalar un servidor ftp en Linux.

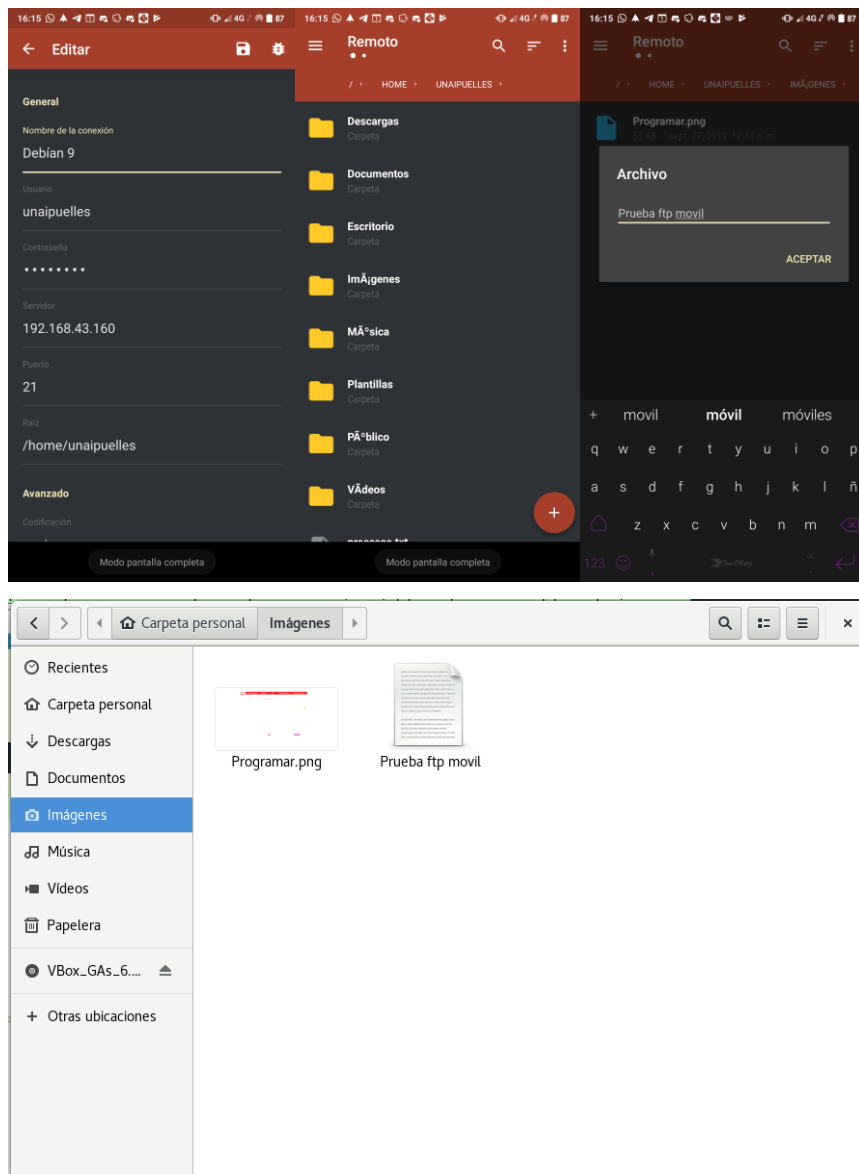
- a. ¿Cómo funciona y cómo se instala?
 - i. Lo lanza el súper demonio de red llamado `openbsd-inetd`. Este súper demonio se instala con la orden `sudo apt-get install openbsd-inetd`
 - ii. Después se instala el demonio servidor ftp con la orden `sudo apt-get install ftpd`
- b. Arrancar el servidor ftp (que en realidad es arrancar el súper demonio de red) con la orden `sudo service openbsd-inetd start` o `sudo /etc/init.d/openbsd-inetd start`
- c. ¿Cómo puedo saber si está arrancado o no?
 - i. Mirando los procesos que están ejecutándose en el sistema mediante la orden `ps-ef | grep ftpd`
 - ii. Mediante nmap



```
unaipuelles@Debian-UnaiPuelles: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
unaipuelles@Debian-UnaiPuelles:~$ nmap -p 21 10.1.206.76  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2019-10-04 16:31 CEST  
Nmap scan report for 10.1.206.76  
Host is up (0.000067s latency).  
PORT      STATE SERVICE  
21/tcp    open  ftp  
  
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds  
unaipuelles@Debian-UnaiPuelles:~$
```

- iii. Mediante un telnet al puerto del servidor ftp mediante la orden `open ip puerto, en mi caso: open 192.168.1.55 21`
- d. ¿Qué puerto utiliza este servidor? Utiliza el puerto 21

2. Instalar un cliente ftp en el móvil (ojo que no sea SFTP, que sea FTP). Enviar una foto desde el móvil al servidor FTP.



a. Otra opción sería desde cualquier shell mediante la orden:

i. Primero abrimos conexión al servidor: *ftp ip*

1. Introducimos el usuario y la contraseña como nos indica.

ii. Nos colocamos en la ruta donde tenemos el fichero que queremos enviar: *lcd ruta*

iii. Enviamos el fichero: *put fichero.ext*

```
Símbolo del sistema - ftp 10.1.205.155

C:\Users\unai->open 10.1.205.155
"open" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\unai->ftp 10.1.205.155
Conectado a 10.1.205.155.
220 Debian-UnaiPuelles.debian FTP server (Version 6.4/OpenBSD/Linux-ftp-0.17) ready.
500 'OPTS UTF8 ON': command not understood.
Usuario (10.1.205.155:(none)): unaipuelles
331 Password required for unaipuelles.
Contraseña:
230-
230- The programs included with the Debian GNU/Linux system are free software;
230- the exact distribution terms for each program are described in the
230- individual files in /usr/share/doc/*/copyright.
230-
230- Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
230- permitted by applicable law.
230 User unaipuelles logged in.
ftp> lcd C:\Users\unai\Desktop
Directorio local ahora C:\Users\unai\Desktop.
ftp> put Programar.png
200 PORT command successful.
150 Opening ASCII mode data connection for 'Programar.png'.
226- WARNING! 92 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
ftp: 53883 bytes enviados en 0.00segundos 26941.50a KB/s.
ftp>
```

3. Monitorización con un sniffer

a. Una vez que se ha logrado la conexión cliente-servidor, capturar mediante el wireshark los siguientes paquetes:

i. Three-way handshake – Tres paquetes con los que se establece la conexión cliente-servidor –

Wireshark packet capture showing a three-way TCP handshake between 10.1.205.146 and 10.1.205.155. The interface is eth0.

No.	Time	Source	Destination	Protocol	Length	Info
85	4.623900000	10.1.205.146	10.1.205.155	TCP	60	60 59546 → 21 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
86	4.623954500	10.1.205.155	10.1.205.146	TCP	60	21 → 59546 [SYN, ACK] Seq=0 Ack=1 Win=29312 Len=0 MSS=1460 SACK_PERM=1 WS=128
87	4.624162721	10.1.205.146	10.1.205.155	TCP	60	60 59546 → 21 [ACK] Seq=1 Ack=1 Win=525568 Len=0

Source Port: 59546
Destination Port: 21
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1000 ... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
window size value: 64240
[Calculated window size: 64240]
Checksum: 0x74e3 [Unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

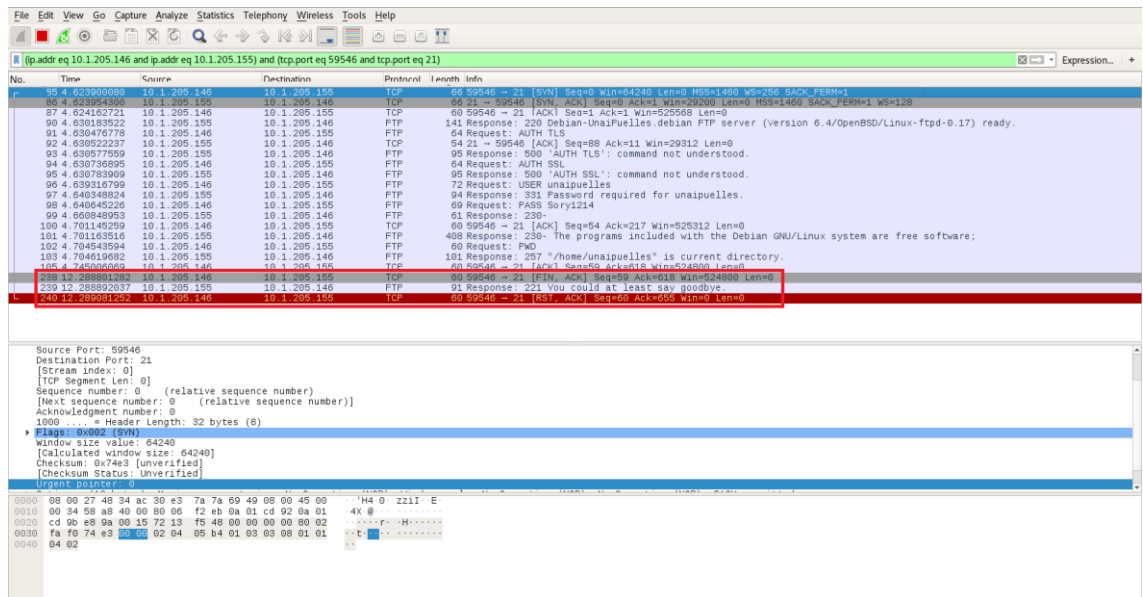
ii. INSERTAR PANTALLAZO donde aparezcan los puertos del cliente y el servidor, junto con sus direcciones IP.

Wireshark packet capture showing an FTP session. The packet list shows a SYN packet from 10.1.205.146 to 10.1.205.155. The packet details show the source port as 59546 and the destination port as 21. The packet bytes show the raw data of the SYN packet.

iii. USUARIO Y CONTRASEÑA

Wireshark packet capture showing an FTP session. The packet list shows a packet from 10.1.205.146 to 10.1.205.155. The packet details show the source port as 59546 and the destination port as 21. The packet bytes show the raw data of the packet.

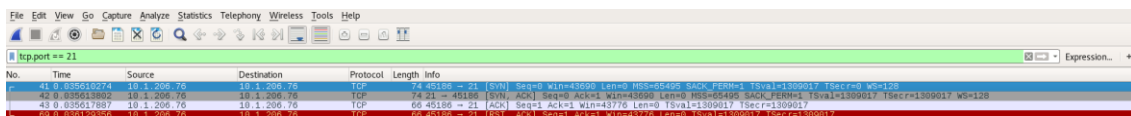
iv. Capturar los paquetes con los que se cierra la conexión -



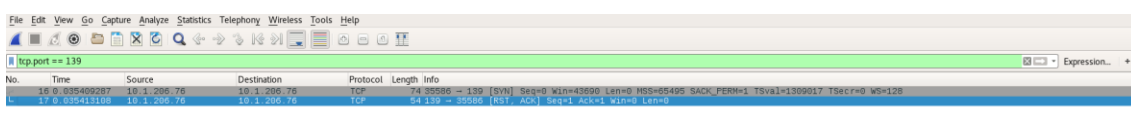
NOTA: No serán válidas capturas que no estén bien filtradas de forma que se puedan encontrar de forma más o menos sencilla esos paquetes. Destacar esos paquetes con un trazo rojo ayuda, pero eso no es un filtro de Wireshark.

4. Escaneo de los puertos mediante nmap

- Hacer un escaneo **FULL SCAN** al servidor ftp mediante nmap
- Identificar mediante wireshark y los filtros necesarios los paquetes mandados en ese escaneo a ese puerto en concreto. Para ello, debe aparecer:
 - Un escaneo filtrado con éxito (a un puerto abierto)



- Un escaneo filtrado a un puerto cerrado

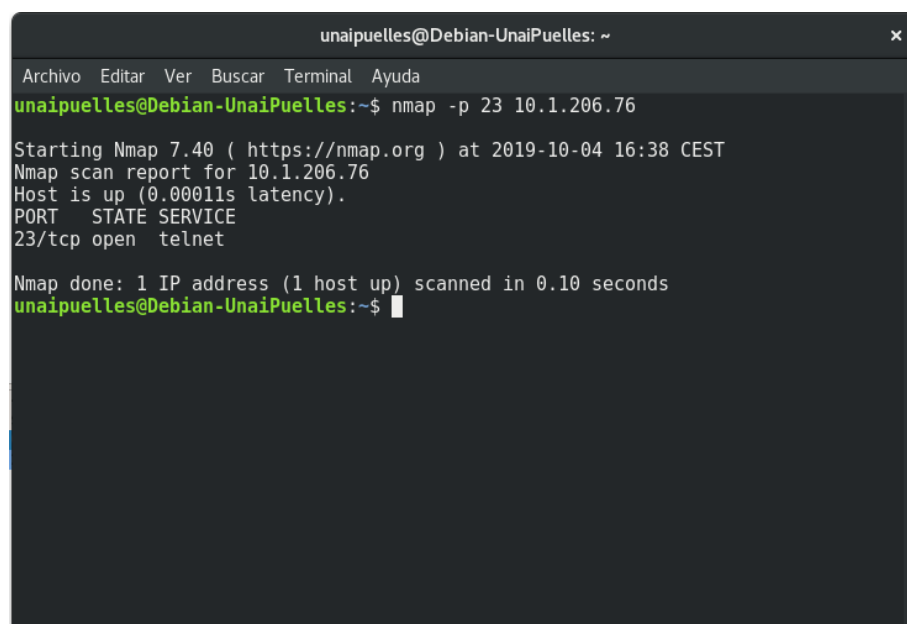


NOTA: El resultado de estos pantallazos deben reflejar las diapositivas que hay en la teoría donde se explica este tipo de escaneo.

PARTE 2

5. Instalar un servidor telnet en Linux.

- a. ¿Cómo funciona y cómo se instala?
 - i. Lo lanza el súper demonio de red llamado `openbsd-inetd`.
 - ii. Este súper demonio se instala con la orden `sudo apt-get install openbsd-inetd`.
 - iii. Después se instala el demonio servidor telnet con la orden `sudo apt-get install telnetd`
- b. Arrancar el servidor telnet (que en realidad es arrancar el súper demonio de red) con la orden `sudo service openbsd-inetd start` o `sudo /etc/init.d/openbsd-inetd start`
- c. ¿Cómo puedo saber si está arrancado o no?
 - i. Mirando los procesos que están ejecutándose en el sistema mediante la orden `ps -ef | grep telnetd`
 - ii. Mediante nmap



```
unaipuelles@Debian-UnaiPuelles: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
unaipuelles@Debian-UnaiPuelles:~$ nmap -p 23 10.1.206.76  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2019-10-04 16:38 CEST  
Nmap scan report for 10.1.206.76  
Host is up (0.00011s latency).  
PORT      STATE SERVICE  
23/tcp    open  telnet  
  
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds  
unaipuelles@Debian-UnaiPuelles:~$
```

- iii. Mediante un telnet a nuestro propio equipo mediante la orden `open 192.168.1.55 23`
- d. ¿Qué puerto utiliza este servidor? Utiliza el puerto 23

6. Acceder desde un cliente telnet en Windows. Una vez dentro del servidor borrar la imagen enviada en el punto anterior (la que enviamos con el FTP)

```
Telnet 10.1.206.76
Debian GNU/Linux 9
Debian-UnaiPuelles login: unaipuelles
Password:
Last login: Fri Oct  4 15:14:59 CEST 2019 from 10.1.204.181 on pts/1
Linux Debian-UnaiPuelles 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u1 (2019-09-20) x86_64

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.
unaipuelles@Debian-UnaiPuelles:~$ ls
Descargas Documentos Escritorio Imágenes Música Plantillas procesos.txt Programar.png Público Vídeos
unaipuelles@Debian-UnaiPuelles:~$ cd Imágenes/
unaipuelles@Debian-UnaiPuelles:~/Imágenes$ ls
Programar.png Screenshot_2019-09-27-16-15-544_turbo.client.png Screenshot_2019-09-27-16-15-40-182_turbo.client.png
Screenshot_2019-09-27-16-15-24-056_turbo.client.png Screenshot_2019-09-27-16-15-48-591_turbo.client.png
unaipuelles@Debian-UnaiPuelles:~/Imágenes$ rm Programar.png
unaipuelles@Debian-UnaiPuelles:~/Imágenes$ ls
Screenshot_2019-09-27-16-15-544_turbo.client.png Screenshot_2019-09-27-16-15-40-182_turbo.client.png
Screenshot_2019-09-27-16-15-24-056_turbo.client.png Screenshot_2019-09-27-16-15-48-591_turbo.client.png
unaipuelles@Debian-UnaiPuelles:~/Imágenes$
```

7. Monitorización con un sniffer

- a. Una vez que se ha logrado la conexión cliente-servidor, capturar mediante el wireshark los siguientes paquetes:
 - i. Three-way handshake – Tres paquetes con los que se establece la conexión cliente-servidor –

The image shows a Wireshark packet capture of a Telnet session. The first three packets are highlighted in red, representing the three-way handshake:

- Packet 222: SYN, Seq=6550706, Win=0, Len=0, MSS=1460, SACK_PERM=1
- Packet 223: SYN-ACK, Seq=6550706, Win=29312, Len=0, MSS=1460, SACK_PERM=1, WS=128
- Packet 224: ACK, Seq=6550706, Win=0, Len=0, MSS=1460, SACK_PERM=1, WS=128

The packet details for the first packet (222) are shown below:

```

Frame 222: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct  3, 2019 17:44:05.839461442 CEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1570117445.839461442 seconds
    [Time delta from previous captured frame: 0.000170148 seconds]
    [Time delta from previous displayed frame: 0.000170148 seconds]
    [Time since reference or first frame: 0.547709117 seconds]
    Frame Number: 224
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    ...
    0000  08 00 27 4b 34 ac 30 e3 7a 7a 69 49 00 00 45 00  ...H4 0 zll E
    0010  00 28 a3 2a 40 00 00 00 a8 79 0a 01 cc dd 0a 01  ...  Y
    0020  c8 4c c5 12 00 17 c8 00 42 be 4a 2f 21 40 50 10  ...  B 3/8P
    0030  08 05 b9 c5 00 00 00 00 00 00 00 00 00 00 00 00
  
```

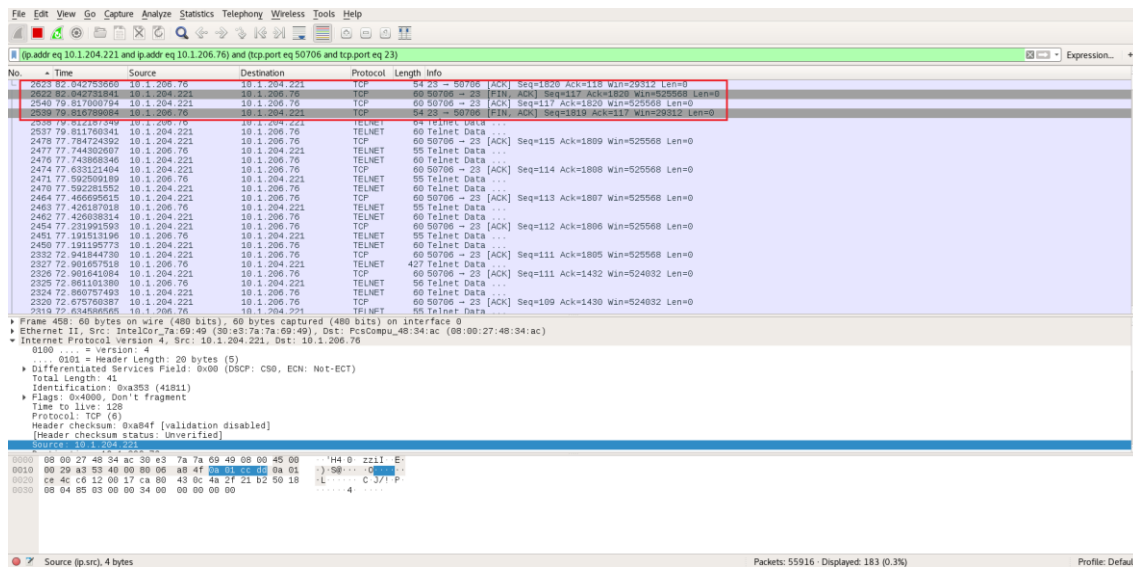
- ii. **INSERTAR PANTALLAZO** donde aparezcan los puertos del cliente y el servidor, junto con sus direcciones IP.

No.	Time	Source	Destination	Protocol	Length	Info
222	4.547617917	10.1.204.221	10.1.206.76	TCP	60	50706 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
223	4.547638990	10.1.206.76	10.1.204.221	TCP	60	23 → 50706 [SYN, ACK] Seq=0 Ack=1 Win=29312 Len=0 MSS=1460 SACK_PERM=1 WS=128
224	4.547709117	10.1.204.221	10.1.206.76	TCP	60	50706 → 23 [ACK] Seq=1 Ack=1 Win=525568 Len=0
225	4.555825690	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
226	4.559870326	10.1.206.76	10.1.204.221	TCP	54	23 → 50706 [ACK] Seq=13 Ack=7 Win=29312 Len=0
227	4.559911476	10.1.206.76	10.1.204.221	TELNET	60	Telnet Data ...
228	4.560024753	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
229	4.560090964	10.1.204.221	10.1.206.76	TCP	60	50706 → 23 [ACK] Seq=16 Ack=16 Win=525568 Len=0
230	4.560051450	10.1.206.76	10.1.204.221	TELNET	60	Telnet Data ...
231	4.560720656	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
232	4.561803515	10.1.206.76	10.1.204.221	TCP	54	23 → 50706 [ACK] Seq=28 Ack=25 Win=29312 Len=0
233	4.562052997	10.1.204.221	10.1.206.76	TELNET	70	Telnet Data ...
234	4.562088034	10.1.206.76	10.1.204.221	TCP	54	23 → 50706 [ACK] Seq=28 Ack=41 Win=29312 Len=0
235	4.562269088	10.1.206.76	10.1.204.221	TELNET	60	Telnet Data ...
236	4.562626603	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
237	4.562766557	10.1.206.76	10.1.204.221	TCP	54	23 → 50706 [ACK] Seq=40 Ack=44 Win=29312 Len=0
238	4.562852078	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
239	4.562999595	10.1.206.76	10.1.204.221	TCP	54	23 → 50706 [ACK] Seq=40 Ack=53 Win=29312 Len=0
240	4.563077469	10.1.206.76	10.1.204.221	TELNET	60	Telnet Data ...
241	4.563081553	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
242	4.563087705	10.1.206.76	10.1.204.221	TELNET	180	Telnet Data ...
243	4.563085402	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
244	4.563087494	10.1.206.76	10.1.204.221	TCP	54	23 → 50706 [ACK] Seq=92 Ack=59 Win=29312 Len=0
245	4.563086633	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...

- iii. **USUARIO Y CONTRASEÑA** Una vez analizados los datos podemos ver que la contraseña y usuario se envían cada letra en un paquete obteniendo como respuesta del servidor la misma letra que es la que se muestra en el cliente. En el caso de la contraseña el servidor no muestra nada para que la contraseña no se imprima por pantalla.

No.	Time	Source	Destination	Protocol	Length	Info
349	7.826348221	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
350	7.826584120	10.1.206.76	10.1.204.221	TELNET	55	Telnet Data ...
352	7.940999990	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
353	7.940534375	10.1.206.76	10.1.204.221	TELNET	55	Telnet Data ...
356	8.050579220	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
357	8.050590774	10.1.206.76	10.1.204.221	TELNET	60	Telnet Data ...
358	8.190778950	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
359	8.190912621	10.1.206.76	10.1.204.221	TELNET	55	Telnet Data ...
372	8.263631935	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
373	8.263699457	10.1.206.76	10.1.204.221	TELNET	55	Telnet Data ...
377	8.427488206	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
378	8.427665913	10.1.206.76	10.1.204.221	TELNET	55	Telnet Data ...
384	8.579683109	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
385	8.580695793	10.1.206.76	10.1.204.221	TELNET	60	Telnet Data ...
419	9.716128546	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
419	9.847721000	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
421	10.017012746	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
428	10.189278707	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
437	10.383318093	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
444	10.505131605	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
450	10.601804711	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
458	10.515352063	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
464	11.005058876	10.1.204.221	10.1.206.76	TELNET	60	Telnet Data ...
465	11.101697621	10.1.206.76	10.1.204.221	TELNET	56	Telnet Data ...
468	11.142754478	10.1.206.76	10.1.204.221	TELNET	600	Telnet Data ...

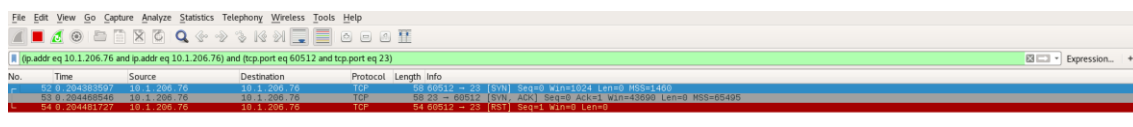
iv. Capturar los paquetes con los que se cierra la conexión



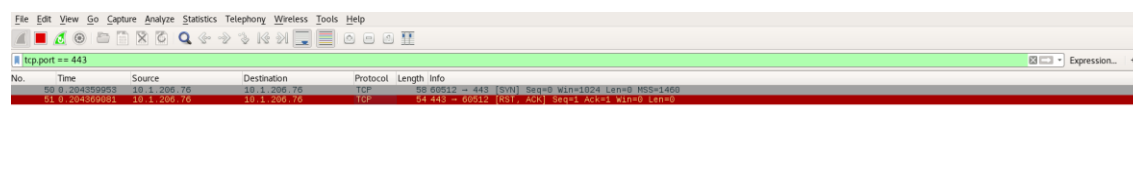
NOTA: No serán válidas capturas que no estén bien filtradas de forma que se puedan encontrar de forma más o menos sencilla esos paquetes. Destacar esos paquetes con un trazo rojo ayuda, pero eso no es un filtro de Wireshark.

8. Escaneo de los puertos mediante nmap

- Hacer un escaneo **HALF SCAN** al servidor ftp mediante nmap
- Identificar mediante wireshark y los filtros necesarios los paquetes mandados en ese escaneo a ese puerto en concreto. Para ello, debe aparecer:
 - Un escaneo filtrado con éxito (a un puerto abierto)



- Un escaneo filtrado a un puerto cerrado



PRÁCTICA 3

9. Realizar el paso 3 (captura del Three-way handshake, fin de conexión y usuario y contraseña) para el servidor Open SSH, con sus correspondientes pantallazos. ¿Has podido ver la contraseña en Wireshark? ¿Qué paquetes son los que definen la autenticación? Señálalos en tu captura.

- Three-way handshake:

Wireshark capture showing the Three-way handshake for an SSH connection. The filter is '(ip.addr eq 10.1.204.221 and (ip.addr eq 10.1.206.76) and (tcp.port eq 51217 and tcp.port eq 22))'. The packet list shows the SYN exchange (60.51217 to 22, 60.22 to 51217) and the ACK (60.51217 to 22). The packet details for the ACK show 'SSH Client: Protocol (SSH-2.0-PuTTY_Release_0.71)'.

- Fin de conexión:

Wireshark capture showing the end of the SSH connection. The filter is '(ip.addr eq 10.1.206.76 and ip.addr eq 10.1.204.181) and (tcp.port eq 22 and tcp.port eq 50198)'. The packet list shows the FIN exchange (60.50198 to 22, 60.22 to 50198) and the ACK (60.50198 to 22). The packet details for the ACK show 'SSH Server: Encrypted packet (len=4)'.

- Usuario y contraseña: No podemos visualizar el usuario y la contraseña como hemos podido ver en los anteriores casos ya que previamente, antes de que se realice el intercambio de datos , se encripta toda la comunicación entre el cliente y el servidor y viceversa.

10. Explica en pocas líneas qué es el servicio SSH y para qué sirve, qué puerto utiliza, cómo es su autenticación y cómo viajan los datos que se intercambian entre el cliente y el servidor. ¿Hay un servicio análogo para el servicio ftp basado en SSH?

El ssh, cuyas palabras significan Secure Shell, es un protocolo de administración remota que permite al usuario la administración de un equipo a través de la red. Por defecto utiliza el puerto 22 y los datos se transfieren de forma encriptada desde el cliente al servidor. Cuando un cliente intenta conectarse, el servidor presenta los protocolos de encriptación y las respectivas versiones que soporta. Se llega a un acuerdo y la conexión comienza con el protocolo aceptado. Además, el servidor también utiliza una clave pública que el cliente utiliza para verificar la autenticación del host.

Una vez que se ha establecido la conexión, las dos partes utilizan la clave de algoritmo de intercambio que se llama “Diffie-Hellman” para crear una clave simétrica. Esta clave permite que el cliente y el servidor se pongan de acuerdo para realizar una transferencia de archivos encriptada.

IMPORTANTE: Si se detecta que este último punto está copiado la práctica será calificada con un 0.

INSTRUCCIONES

- Entrega:
 - Un archivo PDF a partir de este documento de Word modificado con las respuestas escritas (las que están señaladas en rojo) y los pantallazos pedidos.
- Los ejercicios **SÓLO** podrán realizarse en grupos de dos alumnos como máximo. Si hay un grupo de tres se debe escribir un correo al profesor para notificárselo. **No se permiten entregas de prácticas por grupos de tres o más alumnos que no hayan sido notificadas en fecha al profesor.**
- El nombre del fichero entregado serán los apellidos de los alumnos separados por guion.
- Se deberán usar al menos dos equipos diferentes (cliente y servidor) o realizarlo mediante máquinas virtuales.
- **La fecha límite de entrega será el viernes 11 de octubre a las 23 horas.**
- No se recogerán memorias entregadas fuera de fecha o por otro medio distinto de los indicados (como por ejemplo el mail). Debe entregarse en el apartado correspondiente en el campus virtual.