

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 **Inetd**
 - ii. Este súper demonio se instala con la orden **sudo apt install openbsd-inetd**
 - iii. Después se instala el demonio servidor ftp con la orden **sudo apt install ftpd**
- b. Arrancar el servidor ftp (que en realidad es arrancar el súper demonio de red) con la orden **sudo /etc/init.d/openbsd-inetd restart**
- c. ¿Cómo puedo saber si está arrancado o no?
 - i. Mirando los procesos que están ejecutándose en el sistema mediante la orden **ps aux | grep vsftpd**
 - ii. Mediante nmap

```
gonefdez@gonefdez:~$ nmap 192.168.1.39

Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-30 16:50 CET
Nmap scan report for gonefdez (192.168.1.39)
Host is up (0.000064s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

- iii. Mediante un telnet al puerto del servidor ftp mediante la orden **telnet "ip" 21**
- d. ¿Qué puerto utiliza este servidor? **21**

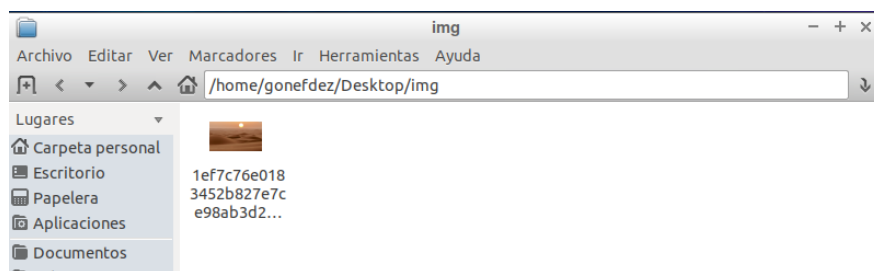
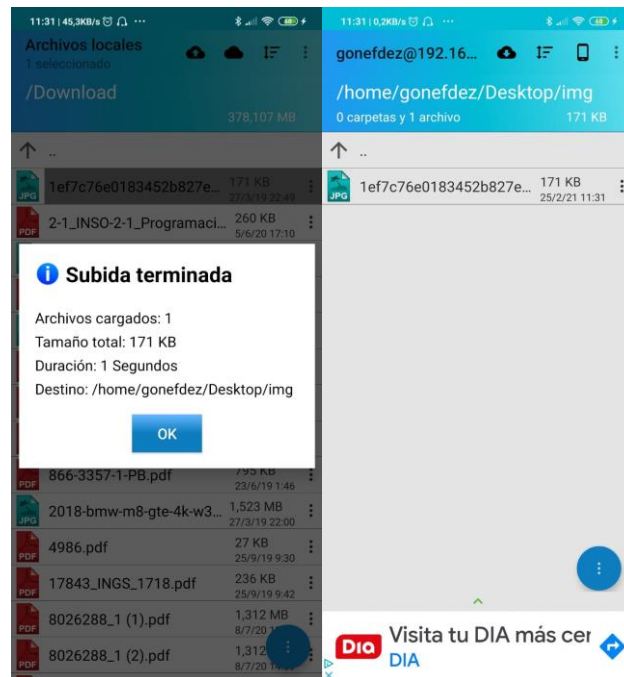
2. Instalar un cliente ftp en el móvil (ojo que no sea SFTP, que sea FTP).

Enviar una foto desde el móvil al servidor FTP.

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

'archivo o ruta del archivo' 'ruta de destino'

b.



3. Monitorización con un sniffer

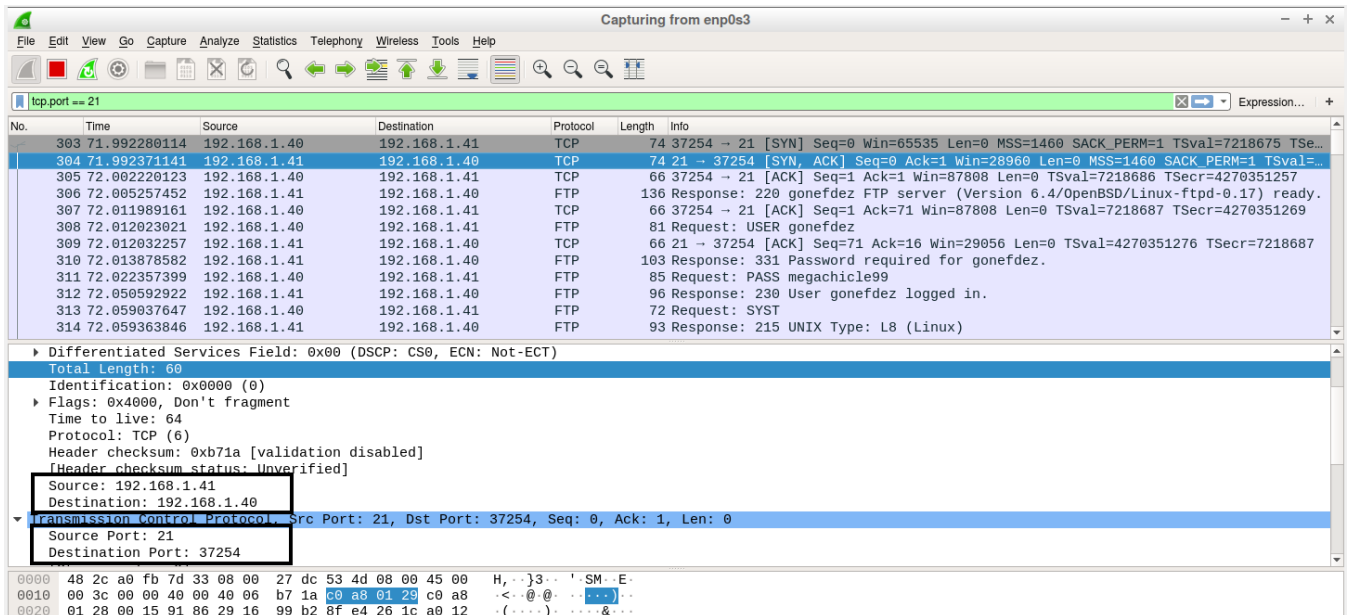
a. Una vez que se ha logrado la conexión cliente-servidor, capturar mediante el wireshark los siguientes paquetes:

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

Capturing from enp0s3

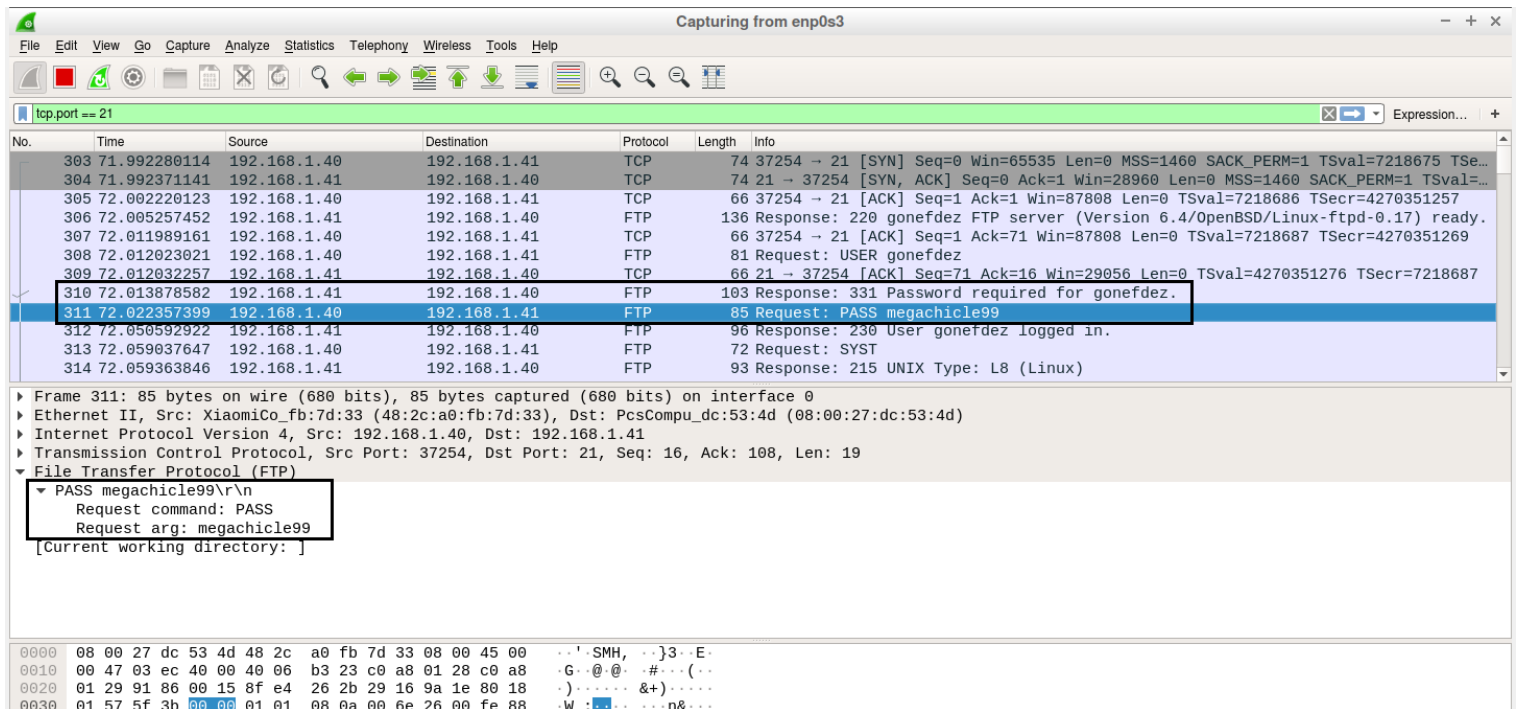
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|--------------|--------------|----------|--------|---|
| 303 | 71.992280114 | 192.168.1.40 | 192.168.1.41 | TCP | 74 | 37254 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=7218675 TSecr=... |
| 304 | 71.992371141 | 192.168.1.41 | 192.168.1.40 | TCP | 74 | 21 → 37254 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=... |
| 305 | 72.002220123 | 192.168.1.40 | 192.168.1.41 | TCP | 66 | 37254 → 21 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=7218686 TSecr=4270351257 |
| 306 | 72.005257452 | 192.168.1.41 | 192.168.1.40 | FTP | 136 | Response: 220 gonefdez FTP server (Version 6.4/0nenBSD/Linux-ftpd-0.17) ready... |

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



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|--------------|--------------|----------|--------|--|
| 303 | 71.992280114 | 192.168.1.40 | 192.168.1.41 | TCP | 74 | 37254 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=7218675 TSe... |
| 304 | 71.992371141 | 192.168.1.41 | 192.168.1.40 | TCP | 74 | 21 → 37254 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=... |
| 305 | 72.002220123 | 192.168.1.40 | 192.168.1.41 | TCP | 66 | 37254 → 21 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=7218686 TSecr=4270351257 |
| 306 | 72.005257452 | 192.168.1.41 | 192.168.1.40 | FTP | 136 | Response: 220 gonefdez FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready. |
| 307 | 72.011989161 | 192.168.1.40 | 192.168.1.41 | TCP | 66 | 37254 → 21 [ACK] Seq=1 Ack=71 Win=87808 Len=0 TSval=7218687 TSecr=4270351269 |
| 308 | 72.012023021 | 192.168.1.40 | 192.168.1.41 | FTP | 81 | Request: USER gonefdez |
| 309 | 72.012032257 | 192.168.1.41 | 192.168.1.40 | TCP | 66 | 21 → 37254 [ACK] Seq=71 Ack=16 Win=29056 Len=0 TSval=4270351276 TSecr=7218687 |
| 310 | 72.013878582 | 192.168.1.41 | 192.168.1.40 | FTP | 103 | Response: 331 Password required for gonefdez. |
| 311 | 72.022357399 | 192.168.1.40 | 192.168.1.41 | FTP | 85 | Request: PASS megachicle99 |
| 312 | 72.050592922 | 192.168.1.41 | 192.168.1.40 | FTP | 96 | Response: 230 User gonefdez logged in. |
| 313 | 72.059037647 | 192.168.1.40 | 192.168.1.41 | FTP | 72 | Request: SYST |
| 314 | 72.059363846 | 192.168.1.41 | 192.168.1.40 | FTP | 93 | Response: 215 UNIX Type: L8 (Linux) |

- iii. **USUARIO Y CONTRASEÑA - INSERTAR PANTALLAZO EN LOS QUE SE VEAN LOS DOS PAQUETES**



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|--------------|--------------|----------|--------|--|
| 303 | 71.992280114 | 192.168.1.40 | 192.168.1.41 | TCP | 74 | 37254 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=7218675 TSe... |
| 304 | 71.992371141 | 192.168.1.41 | 192.168.1.40 | TCP | 74 | 21 → 37254 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=... |
| 305 | 72.002220123 | 192.168.1.40 | 192.168.1.41 | TCP | 66 | 37254 → 21 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=7218686 TSecr=4270351257 |
| 306 | 72.005257452 | 192.168.1.41 | 192.168.1.40 | FTP | 136 | Response: 220 gonefdez FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready. |
| 307 | 72.011989161 | 192.168.1.40 | 192.168.1.41 | TCP | 66 | 37254 → 21 [ACK] Seq=1 Ack=71 Win=87808 Len=0 TSval=7218687 TSecr=4270351269 |
| 308 | 72.012023021 | 192.168.1.40 | 192.168.1.41 | FTP | 81 | Request: USER gonefdez |
| 309 | 72.012032257 | 192.168.1.41 | 192.168.1.40 | TCP | 66 | 21 → 37254 [ACK] Seq=71 Ack=16 Win=29056 Len=0 TSval=4270351276 TSecr=7218687 |
| 310 | 72.013878582 | 192.168.1.41 | 192.168.1.40 | FTP | 103 | Response: 331 Password required for gonefdez. |
| 311 | 72.022357399 | 192.168.1.40 | 192.168.1.41 | FTP | 85 | Request: PASS megachicle99 |
| 312 | 72.050592922 | 192.168.1.41 | 192.168.1.40 | FTP | 96 | Response: 230 User gonefdez logged in. |
| 313 | 72.059037647 | 192.168.1.40 | 192.168.1.41 | FTP | 72 | Request: SYST |
| 314 | 72.059363846 | 192.168.1.41 | 192.168.1.40 | FTP | 93 | Response: 215 UNIX Type: L8 (Linux) |

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

| | | | | |
|------------------|--------------|--------------|-----|--|
| 188 41.087433270 | 192.168.1.41 | 91.189.91.39 | TCP | 66 58078 → 80 [FIN, ACK] Seq=150 Ack=39974 Win=109312 Len=0 TSval=2925958817 TSec... |
| 189 41.185578871 | 91.189.91.39 | 192.168.1.41 | TCP | 66 80 → 58078 [FIN, ACK] Seq=39974 Ack=151 Win=64768 Len=0 TSval=3595477875 TSec... |

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.

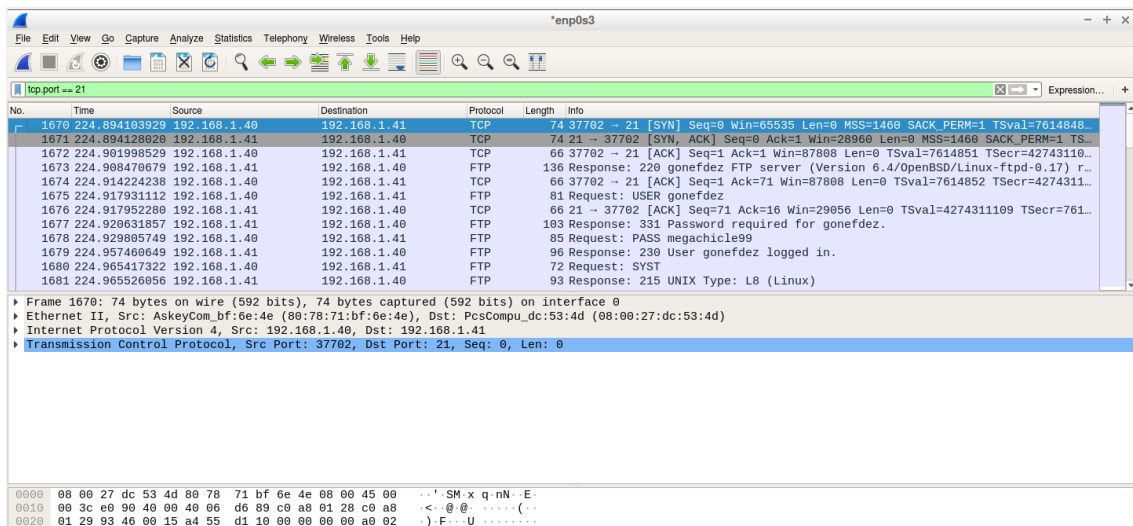
4. Escaneo de los puertos mediante nmap

- a. Hacer un escaneo **FULL SCAN** al servidor ftp mediante nmap

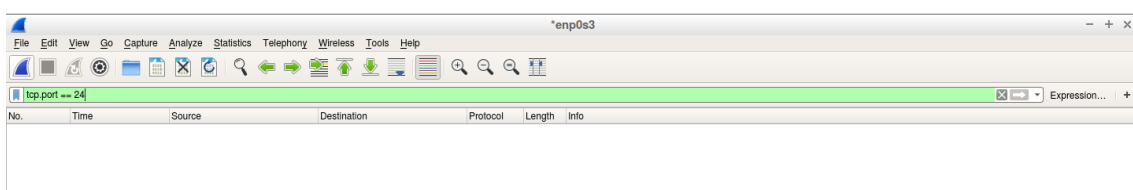
nmap -sT 192.168.1.41

- b. Identificar mediante wireshark y los filtros necesarios los paquetes mandados en ese escaneo a ese puerto en concreto. Para ello, debe aparecer:

- i. Un escaneo filtrado con éxito (a un puerto abierto)



- ii. 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 **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 /etc/init.d/openbsd-inetd restart**
- c. ¿Cómo puedo saber si está arrancado o no?
 - i. Mirando los procesos que están ejecutándose en el sistema mediante la orden **ps aux | grep telnet**
 - ii. Mediante nmap

```
gonefdez@gonefdez:~$ nmap 192.168.1.41

Starting Nmap 7.60 ( https://nmap.org ) at 2021-02-25 12:39 CET
Nmap scan report for gonefdez (192.168.1.41)
Host is up (0.000054s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

iii. Mediante un telnet a nuestro propio equipo mediante la orden

telnet 'ip' 23

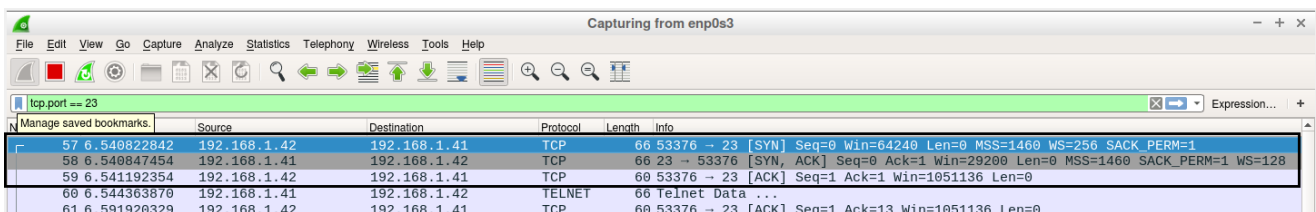
d. ¿Qué puerto utiliza este servidor? **23**

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)

7. Monitorización con un sniffer

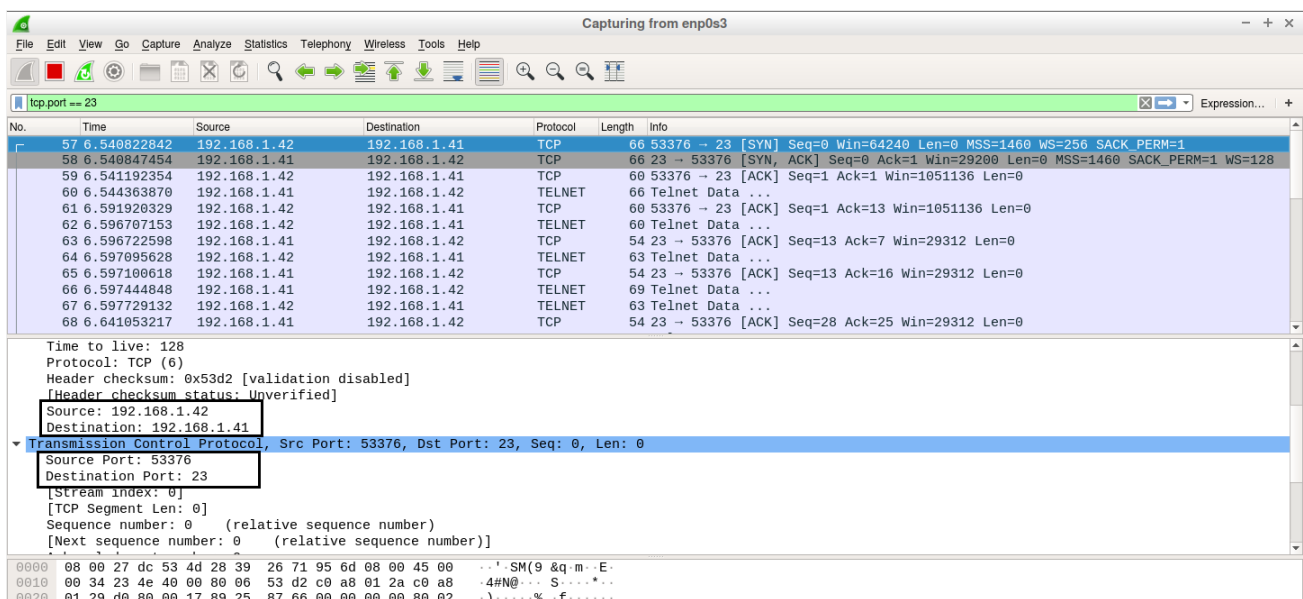
a. Una vez que se ha logrado la conexión cliente-servidor, capturar mediante el wireshark los siguientes paquetes:

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



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|--------------|--------------|----------|--------|---|
| 57 | 6.540822842 | 192.168.1.42 | 192.168.1.41 | TCP | 66 | 53376 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 58 | 6.540847454 | 192.168.1.41 | 192.168.1.42 | TCP | 66 | 23 → 53376 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 59 | 6.541192354 | 192.168.1.42 | 192.168.1.41 | TCP | 60 | 53376 → 23 [ACK] Seq=1 Ack=1 Win=1051136 Len=0 |

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



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|--------------|--------------|----------|--------|---|
| 57 | 6.540822842 | 192.168.1.42 | 192.168.1.41 | TCP | 66 | 53376 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 58 | 6.540847454 | 192.168.1.41 | 192.168.1.42 | TCP | 66 | 23 → 53376 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 59 | 6.541192354 | 192.168.1.42 | 192.168.1.41 | TCP | 60 | 53376 → 23 [ACK] Seq=1 Ack=1 Win=1051136 Len=0 |
| 60 | 6.544363870 | 192.168.1.41 | 192.168.1.42 | TELNET | 66 | Telnet Data ... |
| 61 | 6.591920329 | 192.168.1.42 | 192.168.1.41 | TCP | 60 | 53376 → 23 [ACK] Seq=1 Ack=13 Win=1051136 Len=0 |
| 62 | 6.596707153 | 192.168.1.42 | 192.168.1.41 | TELNET | 60 | Telnet Data ... |
| 63 | 6.596722598 | 192.168.1.41 | 192.168.1.42 | TCP | 54 | 23 → 53376 [ACK] Seq=13 Ack=7 Win=29312 Len=0 |
| 64 | 6.597095628 | 192.168.1.42 | 192.168.1.41 | TELNET | 63 | Telnet Data ... |
| 65 | 6.597100618 | 192.168.1.41 | 192.168.1.42 | TCP | 54 | 23 → 53376 [ACK] Seq=13 Ack=16 Win=29312 Len=0 |
| 66 | 6.597444848 | 192.168.1.42 | 192.168.1.41 | TELNET | 69 | Telnet Data ... |
| 67 | 6.597729132 | 192.168.1.42 | 192.168.1.41 | TELNET | 63 | Telnet Data ... |
| 68 | 6.641053217 | 192.168.1.41 | 192.168.1.42 | TCP | 54 | 23 → 53376 [ACK] Seq=28 Ack=25 Win=29312 Len=0 |

| | |
|--|------------------------------|
| Time to live: 128 | |
| Protocol: TCP (6) | |
| Header checksum: 0x53d2 [validation disabled] | |
| [Header checksum status: Unverified] | |
| Source: | 192.168.1.42 |
| Destination: | 192.168.1.41 |
| Transmission Control Protocol, Src Port: 53376, Dst Port: 23, Seq: 0, Len: 0 | |
| Source Port: | 53376 |
| Destination Port: | 23 |
| [Stream index: 0] | |
| [TCP Segment Len: 0] | |
| Sequence number: | 0 (relative sequence number) |
| Next sequence number: | 0 (relative sequence number) |

iii. USUARIO Y CONTRASEÑA –

```
...#...'.....#..'.'.....h.  
2...'.....ANSI.....!.....!.....Ubuntu 18.04 LTS  
...gonefdez login: ggoonneeffddeezz  
  
Password: megachicle99  
  
Last login: Thu Feb 25 12:48:28 CET 2021 from 192.168.1.42 on pts/2  
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic i686)  
  
* Documentation: https://help.ubuntu.com  
* Management:   https://landscape.canonical.com  
* Support:      https://ubuntu.com/advantage  
  
Pueden actualizarse 555 paquetes.  
359 actualizaciones son de seguridad.  
  
Est.. disponible la nueva versi..n ..20.04.2 LTS..  
Ejecute ..do-release-upgrade.. para actualizarse a ella.  
  
gonefdez@gonefdez:~$
```

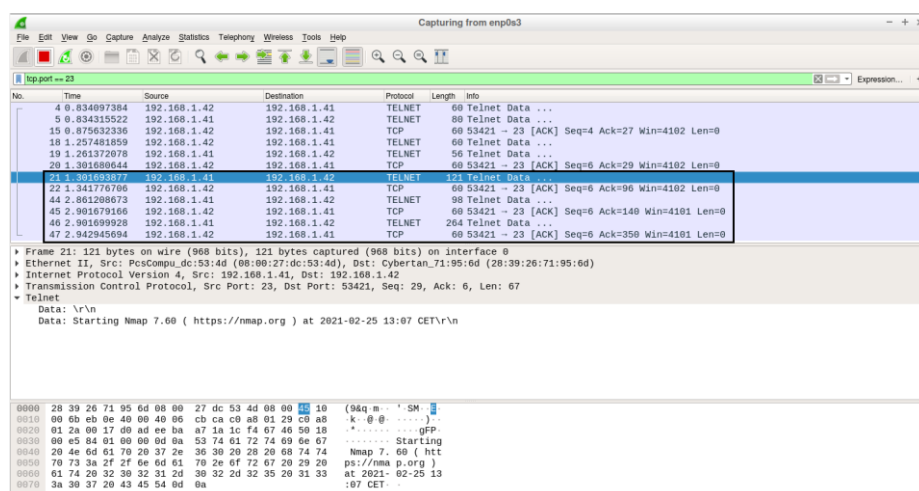
iv. Capturar los paquetes con los que se cierra la conexión –

| | | | | | | | | | | | |
|------|---------------|--------------|--------------|-----|----|------------|------------|----------|----------|-------------|-------|
| 4776 | 672.703647864 | 192.168.1.41 | 192.168.1.42 | TCP | 54 | 23 → 53385 | [FIN, ACK] | Seq=1207 | Ack=102 | Win=29312 | Len=0 |
| 4777 | 672.703603138 | 192.168.1.42 | 192.168.1.41 | TCP | 60 | 53385 → 23 | [ACK] | Seq=102 | Ack=1208 | Win=1049856 | Len=0 |
| 4778 | 672.703611758 | 192.168.1.42 | 192.168.1.41 | TCP | 60 | 53385 → 23 | [FIN, ACK] | Seq=102 | Ack=1208 | Win=1049856 | Len=0 |

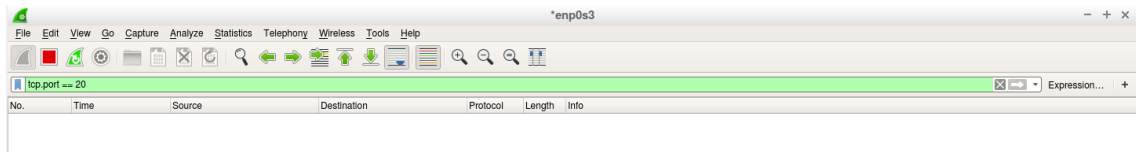
NOTA: No serán válidas capturas que no estén bien filtradas de forma que se puedan encontrar de forma más o menos sencilla esos paquetes. Destacar esos paquetes con un trazo rojo ayuda, pero eso no es un filtro de Wireshark.

8. Escaneo de los puertos mediante nmap

- a. Hacer un escaneo **HALF SCAN** al servidor ftp mediante nmap
sudo nmap -sS 192.168.1.41
- b. Identificar mediante wireshark y los filtros necesarios los paquetes mandados en ese escaneo a ese puerto en concreto. Para ello, debe aparecer:
 - i. Un escaneo filtrado con éxito (a un puerto abierto)



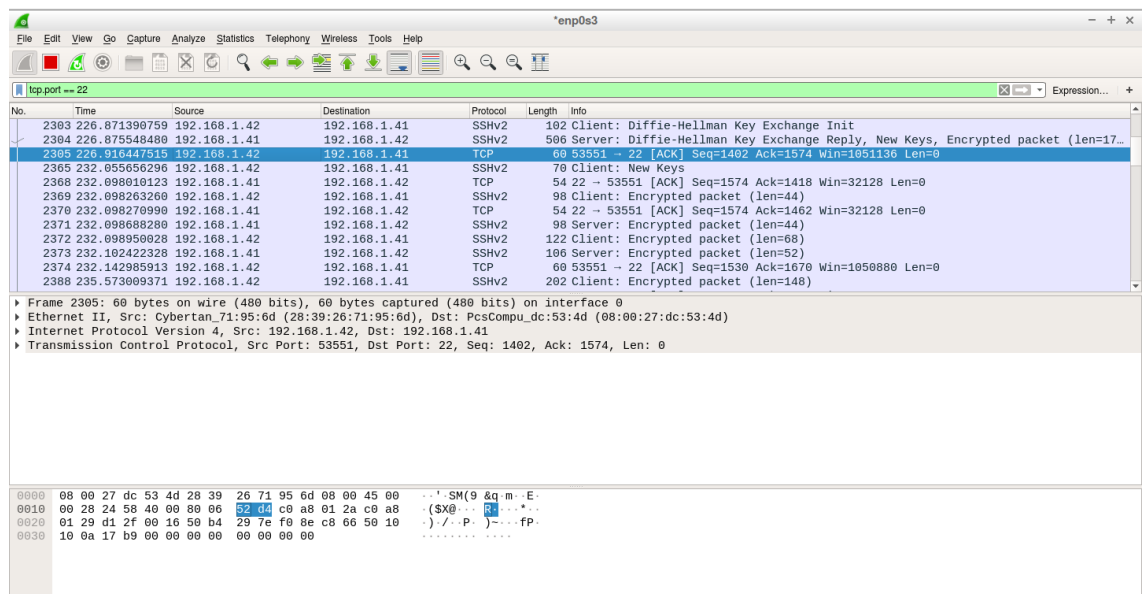
ii. Un escaneo filtrado a un puerto cerrado



NOTA: La única diferencia es que hay que hacer un escaneo HALF SCAN para el servidor telnet y ver los paquetes (en especial los flags que están activados) que se mandan en este caso.

PRÁCTICA 3

- 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.



El usuario y contraseña no se puede ver con wireshark, funciona de forma independiente al super demonio de red y está encriptado.

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?

Es un protocolo de administración remota que facilita las comunicaciones seguras entre dos sistemas(cliente/servidor). Los usuarios pueden conectarse a un host remotamente. Puerto TCP 22.

El mecanismo de autenticación usa técnicas que encriptan los datos de un lado a otro. Es decir, ssh, encripta la sesión de conexión, haciendo con lo que nadie puede obtener contraseñas no encriptadas.

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 16 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.