
SMIX M07

UF4: TELNET y SSH

MARTA MORENO

1. SERVIDOR TELNET

- ❖ Telnet viene de **TE**LEcommunication **NE**Twork.
- ❖ Es el nombre de un protocolo de red y del programa informático que implementa el cliente
- ❖ Un servidor telnet permite a los usuarios acceder a un ordenador huésped para realizar tareas como si estuviera trabajando directamente en ese ordenador.
- ❖ Pertenece a la familia de protocolos de Internet.
- ❖ Sigue un modelo cliente/servidor
- ❖ El puerto TCP que utiliza el protocolo telnet es el 23.

Aplicación	Telnet
Transporte	TCP
Red	IP

Telnet es un protocolo del nivel aplicación y va sobre TCP/IP

1. USOS SERVIDOR TELNET

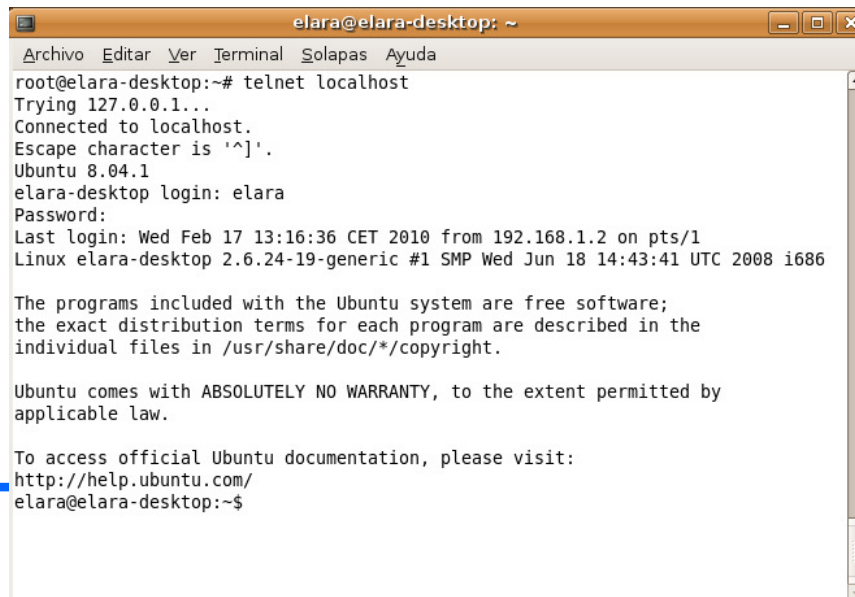
- ❖ **Telnet** sólo sirve para acceder remotamente en modo terminal, es decir, sin gráficos.
 - ❖ Útil para:
 - Arreglar fallos a distancia, de forma remota
 - Consultar datos a distancia.
 - ❖ Telnet ha tenido y tiene un fuerte uso en sistemas UNIX-LINUX y en equipos de comunicaciones (configuración de routers)
 - ❖ Permite abrir una sesión con una máquina UNIX, de modo que múltiples usuarios con cuenta en la máquina, se conectan, abren sesión y pueden trabajar utilizando esa máquina.
-

1. MANEJO BÁSICO DE TELNET

- ❖ Para iniciar una sesión con un intérprete de comandos de otro ordenador, teclear el comando telnet seguido del nombre o la dirección IP de la máquina en la que desea trabajar:

telnet servidor.upc.edu

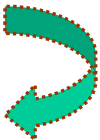
telnet 192.200.30.40



```
elara@elara-desktop: ~  
Archivo Editar Ver Terminal Solapas Ayuda  
root@elara-desktop:~# telnet localhost  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
Ubuntu 8.04.1  
elara-desktop login: elara  
Password:  
Last login: Wed Feb 17 13:16:36 CET 2010 from 192.168.1.2 on pts/1  
Linux elara-desktop 2.6.24-19-generic #1 SMP Wed Jun 18 14:43:41 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
elara@elara-desktop:~$
```

Una vez conectado, podrá ingresar el nombre de usuario y contraseña remoto para iniciar una sesión en modo texto a modo de consola virtual

1. PROBLEMAS SERVIDOR TELNET

- ❑ Mayor problema: la seguridad
 - ❑ Telnet, por defecto, no cifra ninguno de los datos enviados sobre la conexión (contraseñas inclusive). Todo viaja por la red como *texto plano* sin cifrar.
 - ❑ Cualquiera que espíe el tráfico de la red mediante un sniffer, puede obtener los nombres de usuario y contraseñas, y así acceder él también a las máquinas.
 - ❑ No se recomienda su uso. 
 - ❑ SOLUCIÓN: Protocolo **SSH** (versión cifrada de **Telnet**)
Permite cifrar toda la comunicación del protocolo entre el cliente y el servidor, durante el establecimiento de sesión
-

2. PROTOCOLO SSH

- ❖ SSH (*Secure SHell*) es el nombre de un protocolo y del programa que lo implementa.
 - ❖ Cifra la información antes de transmitirla, autentica la máquina a la cual se conecta y puede emplear mecanismos de autenticación de usuarios más seguros.
 - ❖ SSH permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.
 - ❖ Se utiliza TCP en el puerto 22 y la versión 2 (la versión 1 presenta un grave problema de seguridad)
-

2. SEGURIDAD EN SSH

- ❖ SSH trabaja de forma similar a como se hace con telnet.
- ❖ La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión
- ❖ No obstante es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos *-man-in-the-middle*.

2. SECUENCIA CONEXIÓN SSH

- La siguiente serie de eventos lo ayudan a proteger la integridad de la comunicación SSH entre dos host:
 1. Se lleva a cabo un 'handshake' (apretón de manos) encriptado para que el cliente pueda verificar que se está comunicando con el servidor correcto.
 2. La capa de transporte de la conexión entre el cliente y la máquina remota es encriptada mediante un código simétrico.
 3. El cliente se autentica ante el servidor.
 4. El cliente remoto interactúa con la máquina remota sobre la conexión encriptada.
-

PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Paso 1. Arrancar un Linux Desktop o Server dentro del Vmware o Virtual Box.

Paso 2. Abrir un terminal e instala el servidor de TELNET de Linux:

sudo apt update (actualización herramienta descarga aplicaciones)
sudo apt install telnetd -y (instalación del servidor de telnet)

```
marta@marta-virtual-machine:~$ sudo apt install telnetd -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  openssh-client openssh-server openssh-sftp-server
Se instalarán los siguientes paquetes NUEVOS:
  openssh-client openssh-server openssh-sftp-server telnetd
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 89 no actualizados.
```

PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Paso 3. Una vez completada la instalación, puedes comprobar el estado del servicio Telnet con el siguiente comando:

sudo systemctl status inetd

```
marta@marta-virtual-machine:~$ sudo systemctl status inetd
● inetd.service - Internet superserver
   Loaded: loaded (/lib/systemd/system/inetd.service; enabled; vendor preset:
   Active: active (running) since Mon 2022-03-21 09:11:04 CET; 8min ago
     Docs: man:inetd(8)
   Main PID: 3301 (inetd)
    Tasks: 1 (limit: 2173)
   Memory: 764.0K
    CGroup: /system.slice/inetd.service
            └─3301 /usr/sbin/inetd

mar 21 09:11:04 marta-virtual-machine systemd[1]: Starting Internet superserve
mar 21 09:11:04 marta-virtual-machine systemd[1]: Started Internet superserver.
lines 1-12/12 (END)
```

Paso 4. Para el servicio, vuelve a comprobar su estado y reinícialo de nuevo

sudo systemctl stop inetd - sudo systemctl restart inetd

PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Paso 5. Visualiza el fichero de configuración del telnet
sudo nano /etc/inetd.conf

```
GNU nano 4.8 /etc/inetd.conf
## /etc/inetd.conf:  see inetd(8) for further informations.
#
# Internet superserver configuration database
#
# Lines starting with "[:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# If you want to disable an entry so it isn't touched during
# package updates just comment it out with a single '#' character.
#
# Packages should modify this file by using update-inetd(8)
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
#:INTERNAL: Internal services
#discard          stream  tcp      nowait  root    internal
#discard          dgram   udp      wait    root    internal
#daytime          stream  tcp      nowait  root    internal
#time             stream  tcp      nowait  root    internal
```

PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Paso 6. Comprobar el funcionamiento del servidor telnet, ejecutando desde un terminal **telnet localhost**. ¿Qué usuario pondrás?

```
marta@marta-virtual-machine:~$ telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 20.04.4 LTS
marta-virtual-machine login: marta
Password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-30-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage
```

Paso 7. Sal de la sesión mediante exit, y agrega un nuevo usuario al sistema (debe de ser un usuario relacionado con el nombre del alumno):

sudo adduser mmoreno

Paso 8. Prueba de conectarte con el nuevo usuario. ¿Que se observa de forma diferencial?

```
mmoreno@marta-virtual-machine:~$
```

PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Paso 9. Instala el servidor SSH:

sudo apt install openssh-server

```
marta@marta-virtual-machine:~$ sudo apt install openssh-server
[sudo] contraseña para marta:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  ncurses-term openssh-sftp-server ssh-import-id
Paquetes sugeridos:
  molly-guard monkeysphere ssh_askpass
Se instalarán los siguientes paquetes NUEVOS:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
```

Paso 10. Para el servicio, reinícialo de nuevo y comprueba su estado:

sudo systemctl stop ssh

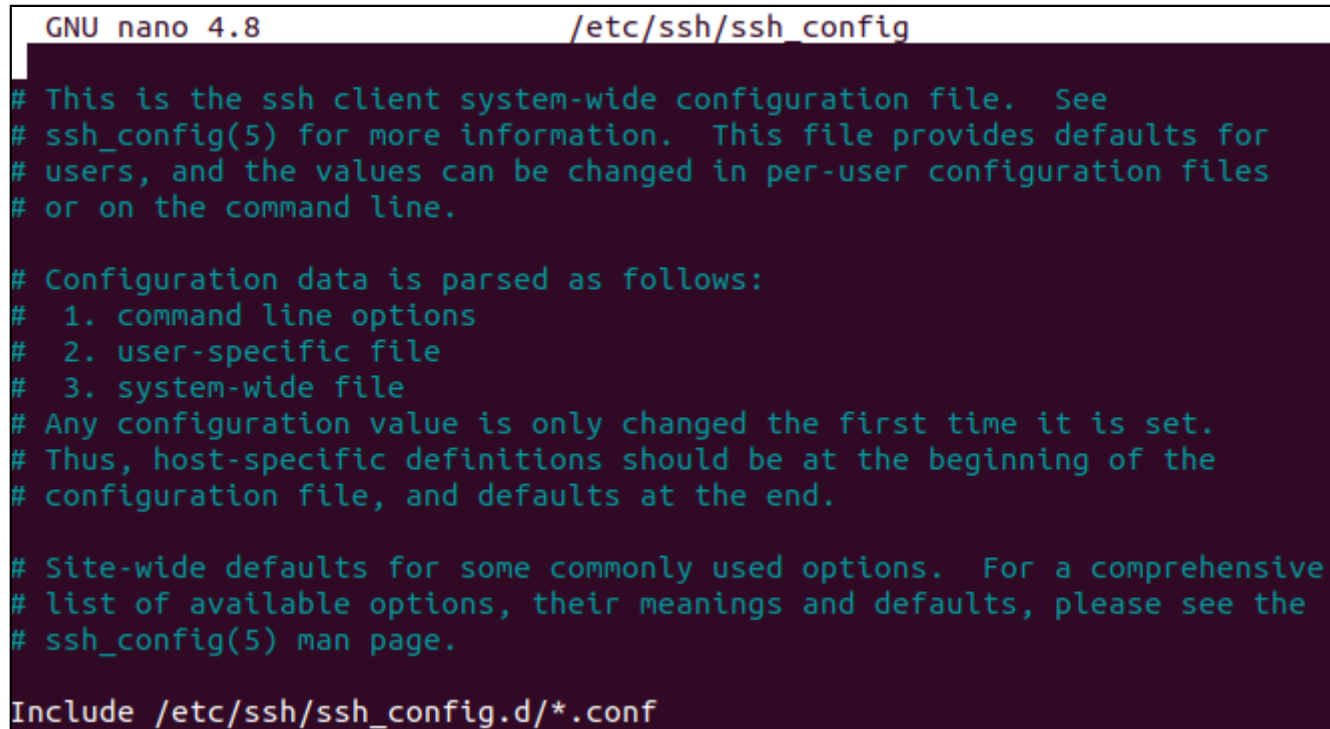
sudo systemctl restart ssh

sudo systemctl status ssh

PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Paso 11. El fichero de configuración de ssh es `/etc/ssh/sshd_config`. Captura una imagen de este fichero.

sudo nano /etc/ssh/ssh_config



```
GNU nano 4.8 /etc/ssh/ssh_config
# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
# 1. command line options
# 2. user-specific file
# 3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

Include /etc/ssh/ssh_config.d/*.conf
```

PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

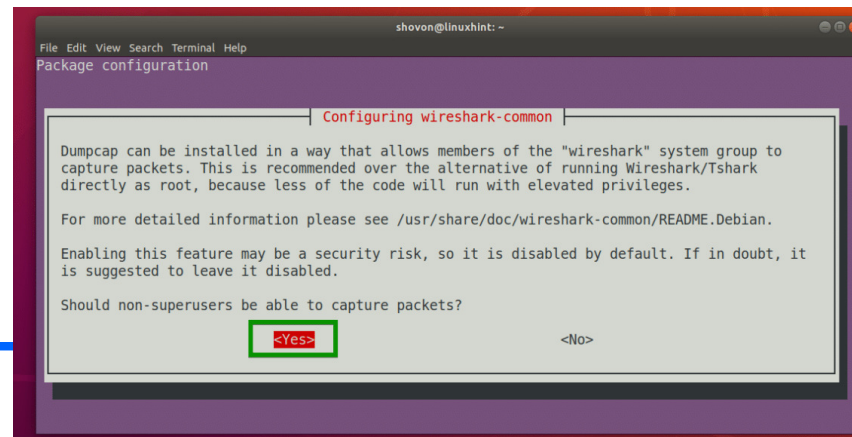
Paso 12. Instala el programa Putty para Linux

sudo apt install -y putty

```
marta@marta-virtual-machine:~$ sudo apt install -y putty
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  putty-tools
Paquetes sugeridos:
  putty-doc
Se instalarán los siguientes paquetes NUEVOS:
  putty putty-tools
```

Paso 13. Instala el programa wireshark.

sudo apt install wireshark



PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Comprobación en la seguridad de los protocolos

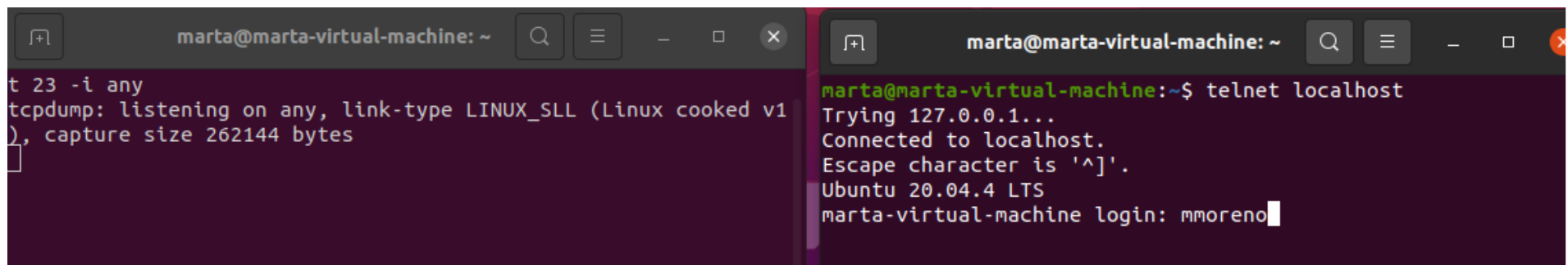
A continuación, vamos a comprobar cómo el protocolo Telnet envía los datos en claro por la red (incluyendo logins y passwords), y el protocolo SSH los envía encriptados.

Paso 14. Abriremos dos terminales. En uno ejecutaremos tcpdump que es un sniffer de paquetes de red (capturaremos los paquetes telnet)

sudo tcpdump -w password.bin port 23 -i any

```
marta@marta-virtual-machine:~$ sudo tcpdump -w password.bin port 23 -i any
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
```

Paso 15. En el otro ejecutaremos el telnet sobre el usuario del alumno creado en 7:



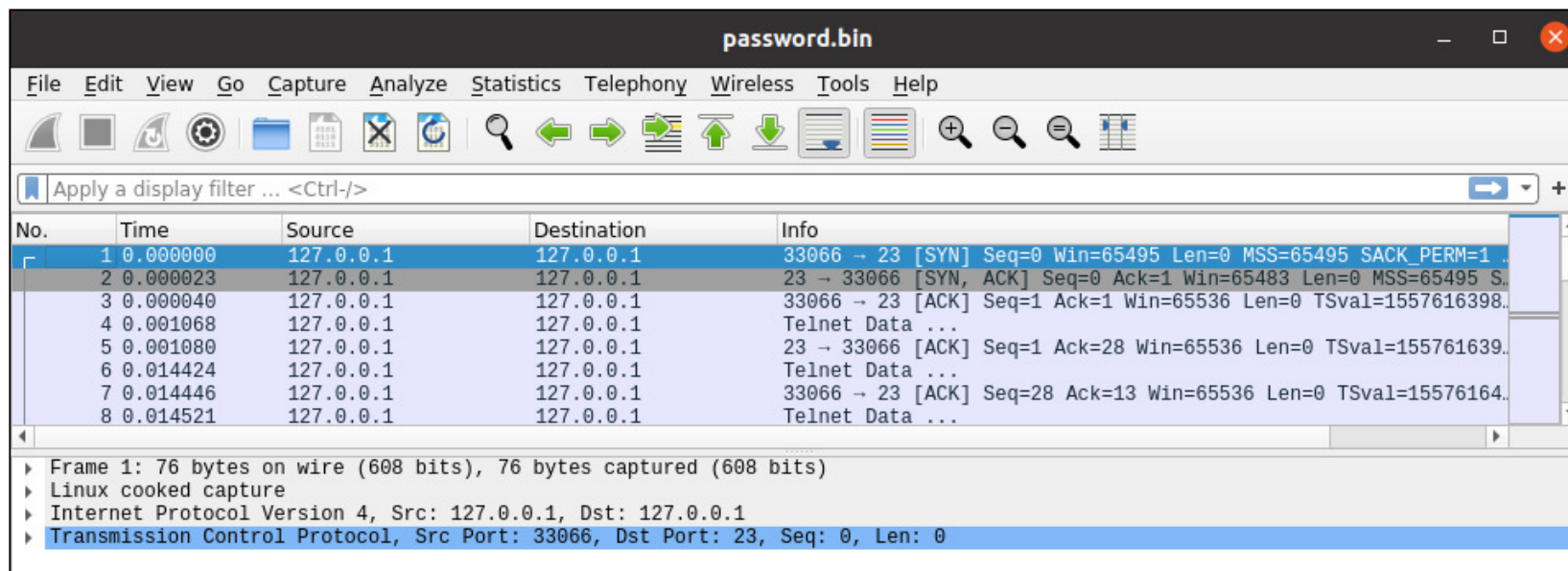
```
marta@marta-virtual-machine: ~
t 23 -i any
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes

marta@marta-virtual-machine:~$ telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 20.04.4 LTS
marta-virtual-machine login: mmoreno
```


PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

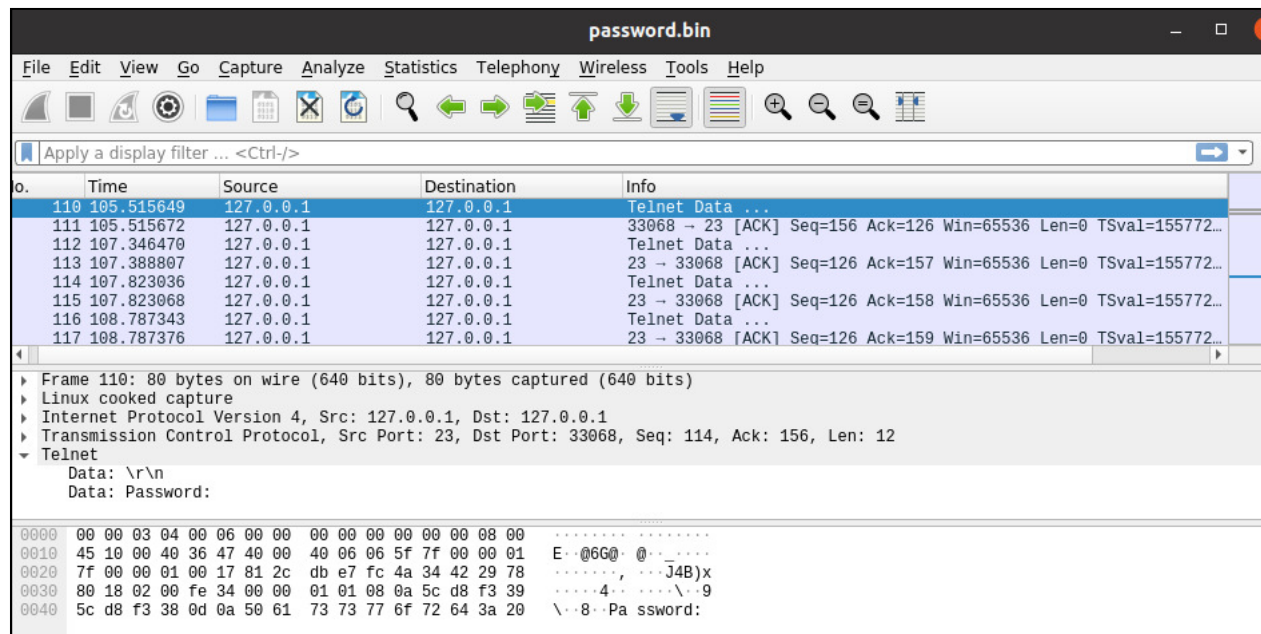
Paso 16. Una vez hemos entrado en la sesión telnet, cancelamos la captura de tramas con tcpdump (Ctrl+C) y visualizamos los datos con el wireshark: **sudo wireshark password.bin**

```
marta@marta-virtual-machine:~$ sudo tcpdump -w password.bin port 23 -i any
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
^C181 packets captured
362 packets received by filter
0 packets dropped by kernel
marta@marta-virtual-machine:~$ sudo wireshark password.bin
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```



PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Paso 17. Entre las tramas debemos buscar la palabra "Password". A continuación Telnet envía cada carácter de la cadena de password en un paquete, por lo tanto se enviará 'm', 'm', 'o', 'r', 'e', 'n', 'o' en un total de 7 mensajes, donde cada carácter está al final del mensaje.



A partir de aquí en los siguientes paquetes Telnet Data irán apareciendo las letras del password en texto plano

PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Paso 18. Realiza diferentes capturas donde se vaya viendo el password introducido en el telnet:

Paquete 110 Telnet Data "password"

Paquete 112 Telnet Data "m"

Paquete 114 Telnet Data "m"

Paquete 116 Telnet Data "o"

Paquete 118 Telnet Data "r"

Paquete 120 Telnet Data "e"

password.bin				
File	Edit	View	Go	Capture
Analyze	Statistics	Telephony	Wireless	Tools
Help				
Apply a display filter ... <Ctrl-/>				
No.	Time	Source	Destination	Info
110	105.515649	127.0.0.1	127.0.0.1	Telnet Data ...
111	105.515672	127.0.0.1	127.0.0.1	33068 - 23 [ACK] Seq=156 Ack=126
112	107.346470	127.0.0.1	127.0.0.1	Telnet Data ...
113	107.388807	127.0.0.1	127.0.0.1	23 - 33068 [ACK] Seq=126 Ack=114
114	107.823036	127.0.0.1	127.0.0.1	Telnet Data ...
115	107.823068	127.0.0.1	127.0.0.1	23 - 33068 [ACK] Seq=126 Ack=114
116	108.787343	127.0.0.1	127.0.0.1	Telnet Data ...
117	108.787376	127.0.0.1	127.0.0.1	23 - 33068 [ACK] Seq=126 Ack=116
Frame 112: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)				
Linux cooked capture				
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1				
Transmission Control Protocol, Src Port: 33068, Dst Port: 23, Seq: 156, Ack: 126, Len: 1				
Telnet				
Data: m				
0000	00 00 03 04 00 06 00 00 00 00 00 00 00 00 00 00		
0010	45 10 00 35 47 2c 40 00 40 06 f5 85 7f 00 00 01	E..56+@.0.....		
0020	7f 00 00 01 81 2c 00 17 34 42 29 78 db e7 fc 564B)X..V		
0030	80 18 02 00 fe 29 00 00 01 01 08 0a 5c d8 fa 60).....\..		
0040	5c d8 f3 39 6d	\..9m		

password.bin				
File	Edit	View	Go	Capture
Analyze	Statistics	Telephony	Wireless	Tools
Help				
Apply a display filter ... <Ctrl-/>				
No.	Time	Source	Destination	Info
110	105.515649	127.0.0.1	127.0.0.1	Telnet Data ...
111	105.515672	127.0.0.1	127.0.0.1	33068 - 23 [ACK] Seq=156 Ack=126
112	107.346470	127.0.0.1	127.0.0.1	Telnet Data ...
113	107.388807	127.0.0.1	127.0.0.1	23 - 33068 [ACK] Seq=126 Ack=114
114	107.823036	127.0.0.1	127.0.0.1	Telnet Data ...
115	107.823068	127.0.0.1	127.0.0.1	23 - 33068 [ACK] Seq=126 Ack=114
116	108.787343	127.0.0.1	127.0.0.1	Telnet Data ...
117	108.787376	127.0.0.1	127.0.0.1	23 - 33068 [ACK] Seq=126 Ack=116
Frame 114: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)				
Linux cooked capture				
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1				
Transmission Control Protocol, Src Port: 33068, Dst Port: 23, Seq: 157, Ack: 126, Len: 1				
Telnet				
Data: m				
0000	00 00 03 04 00 06 00 00 00 00 00 00 00 00 00 00		
0010	45 10 00 35 47 2c 40 00 40 06 f5 84 7f 00 00 01	E..56+@.0.....		
0020	7f 00 00 01 81 2c 00 17 34 42 29 79 db e7 fc 564B)Y..V		
0030	80 18 02 00 fe 29 00 00 01 01 08 0a 5c d8 fc 3d).....\..=		
0040	5c d8 fc 3d 6d	\..m		

password.bin				
File	Edit	View	Go	Capture
Analyze	Statistics	Telephony	Wireless	Tools
Help				
Apply a display filter ... <Ctrl-/>				
No.	Time	Source	Destination	Info
110	105.515649	127.0.0.1	127.0.0.1	Telnet Data ...
111	105.515672	127.0.0.1	127.0.0.1	33068 - 23 [ACK] Seq=156 Ack=126
112	107.346470	127.0.0.1	127.0.0.1	Telnet Data ...
113	107.388807	127.0.0.1	127.0.0.1	23 - 33068 [ACK] Seq=126 Ack=114
114	107.823036	127.0.0.1	127.0.0.1	Telnet Data ...
115	107.823068	127.0.0.1	127.0.0.1	23 - 33068 [ACK] Seq=126 Ack=114
116	108.787343	127.0.0.1	127.0.0.1	Telnet Data ...
117	108.787376	127.0.0.1	127.0.0.1	23 - 33068 [ACK] Seq=126 Ack=116
Frame 116: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)				
Linux cooked capture				
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1				
Transmission Control Protocol, Src Port: 33068, Dst Port: 23, Seq: 158, Ack: 126, Len: 1				
Telnet				
Data: o				
0000	00 00 03 04 00 06 00 00 00 00 00 00 00 00 00 00h...		
0010	45 10 00 35 47 2d 40 00 40 06 f5 83 7f 00 00 01	E..56+@.0.....		
0020	7f 00 00 01 81 2c 00 17 34 42 29 7a db e7 fc 564B)z..V		
0030	80 18 02 00 fe 29 00 00 01 01 08 0a 5c d9 00 01).....\..=		
0040	5c d8 fc 3d 6f	\..o		

PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

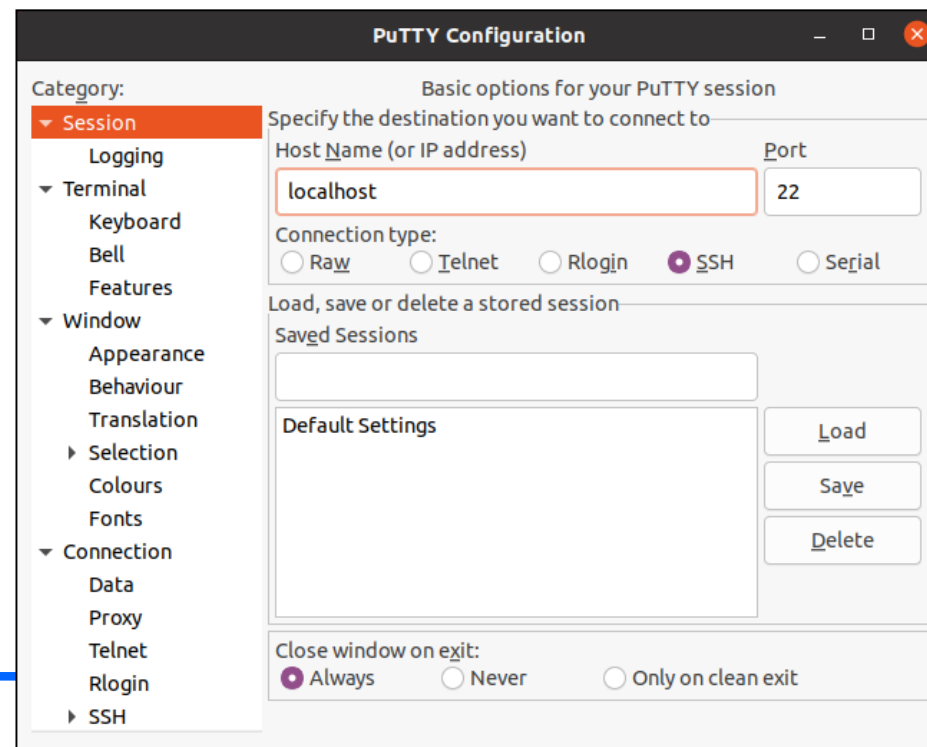
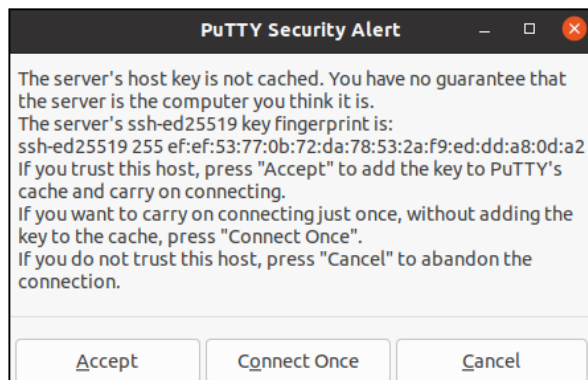
Paso 19. Realizaremos una conexión SSH (encriptada) con Putty. Volvemos a activar tcpdump y opcionalmente podemos parar el servidor telnet para ver que realmente se conecta al servidor SSH activo:

rm password.bin

sudo tcpdump -w password.bin port 22 -i any (ahora es 22)

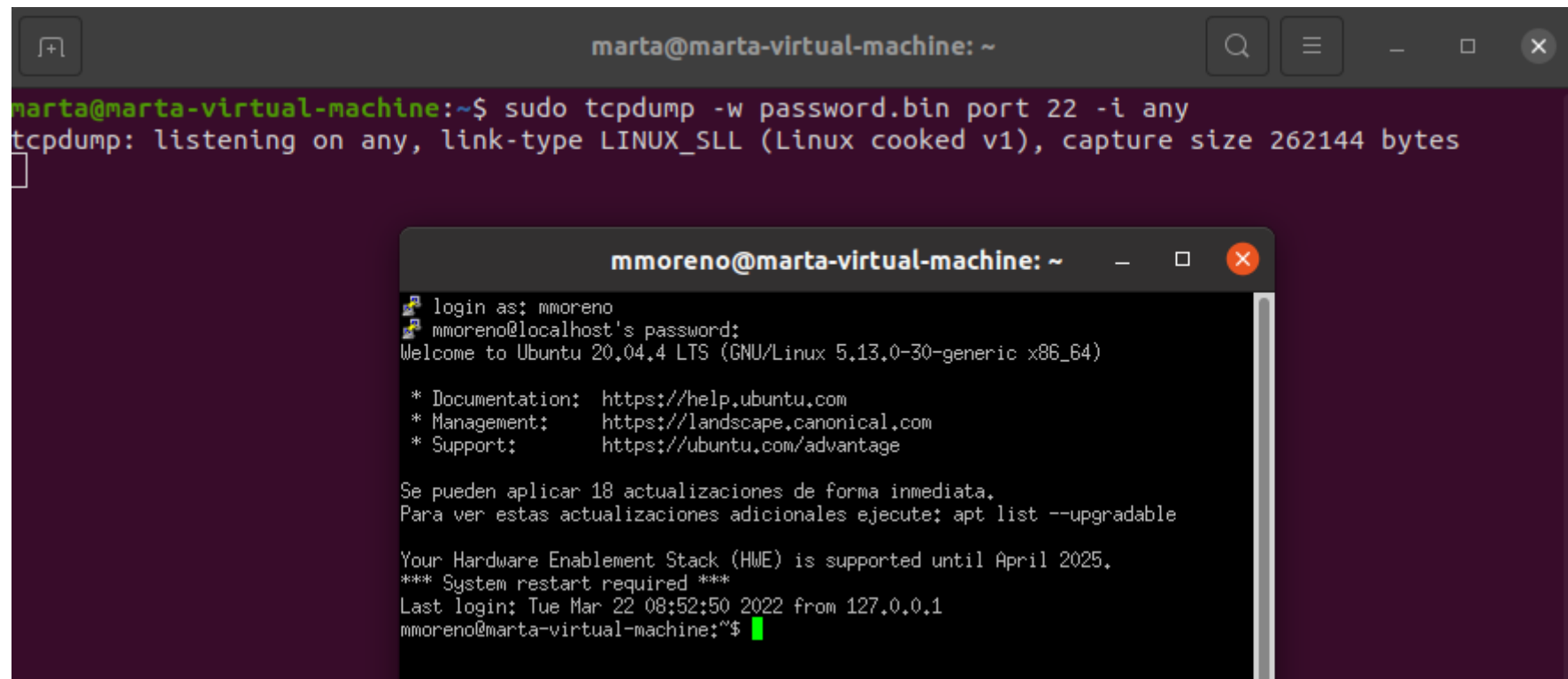
sudo systemctl stop inetd

sudo putty



PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Paso 20. Introducimos el login y password y nos conectamos al servidor:



```
marta@marta-virtual-machine: ~  
marta@marta-virtual-machine:~$ sudo tcpdump -w password.bin port 22 -i any  
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes  
  
mmoreno@marta-virtual-machine: ~  
login as: mmoreno  
mmoreno@localhost's password:  
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-30-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Se pueden aplicar 18 actualizaciones de forma inmediata.  
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable  
  
Your Hardware Enablement Stack (HWE) is supported until April 2025.  
*** System restart required ***  
Last login: Tue Mar 22 08:52:50 2022 from 127.0.0.1  
mmoreno@marta-virtual-machine:~$
```


PRACTICA 1. INSTALACIÓN SERVIDOR TELNET EN LINUX UBUNTU

Paso 21. Cerramos putty, finalizamos tcpdump y abrimos la traza con wireshark. La idea es que no se va a poder ver el password porque todos los paquetes están encriptados:

sudo wireshark password.bin

