**Ejercicio 1**

**TELNET**

1. **¿Cuál es la dirección IP del cliente y cuál es la del servidor?**

Cliente: 192.168.12.1 Servidor: 192.168.12.2

1. **¿Qué credenciales se han utilizado para acceder al servidor? a. PISTA: En esta captura TELNET, el cliente TELNET envía un solo carácter por mensaje en la mayoría de las tramas.**

Por mayor comodidad, filtramos tramas: telnet

Se solicita una contraseña: *cisco*

NOTA: la contraseña en este caso se envía carácter a carácter dado que el cliente-servidor lo negociaron así previamente. Para saber cuando finaliza la solicitud de contraseña, buscamos latrama que envíe como datos \r\n (enter).

A screenshot of a computer

Description automatically generated

*Trama inicial de solicitud*

A screenshot of a computer

Description automatically generated

*Tramas de contraseña y enter*

1. **¿Qué tipo de sistema es el servidor?**

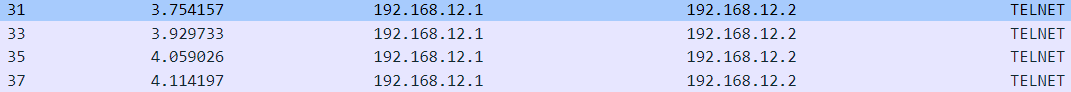
Podemos deducir el tipo de servidos por la respuesta prompt del servidor (R2) está basado en *Radare2* que originalmente estaría desarrollado para sistemas Unix, aunque hay una versión para Windows.

Dado esta captura especifica, no sabemos a ciencia cierta a que sistema podría pertenecer.

1. **¿Qué comando(s) ha ejecutado el cliente en el servidor?**

Por mayor comodidad, filtramos tramas: telnet && ip.src == 192.168.12.1

Comando: *exit*



*Trama de comando*

***FTP***

1. **¿Cuál es la dirección IP del cliente y cuál es la del servidor?**

Cliente: 192.168.1.182 Servidor: 192.168.1.231

1. **¿Qué credenciales se han utilizado para acceder al servidor?**

User: ftp Password: ftp

1. **¿Qué tipo de sistema es el servidor?**

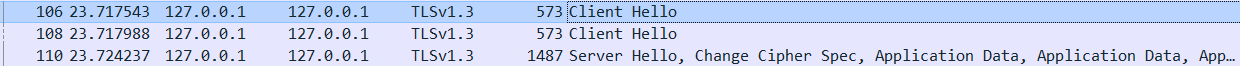
En este caso el cliente escribe el comando SYST para solicitar información al servidor sobre el tipo de sistema que es.



1. **¿Qué comando(s) ha ejecutado el cliente en el servidor?**

SYST, FEAT, PWD, EPSV, LIST, TYPE, SIZE, RETR, MDTM, CWD, STOR, MKD, SITE, QUIT

**Ejercicio 2.1**

****

1. **¿Cuándo (de qué trama a qué trama) se procede con el proceso de handshake (sesión SSL), tal y como se ha explicado en teoría?**

De la trama 106 a la 110

1. **En esta conexión se utiliza TLS1.3. ¿Dónde se negocia exactamente la versión de TLS que se utiliza?**

Se negocia en el intercambio de mensajes *Client Hello* y *Server Hello.*

- El cliente inicia la conexión enviando un mensaje “Client Hello” al servidor cuando quiere establecer una conexión segura. Envía las versiones que soporta de TLS, junto con otros elementos tales como extensiones que admite y las suites de cifrado preferidas o su clave pública o *nonce* para la posterior creación de la clave de sesión.

- El servidor selecciona la versión de TLS y responderá con un mensaje “Server Hello” confirmando la versión y puede aceptar o ajustar las preferencias del cliente en términos de suites de cifrado y otras configuraciones.

**NOTA**

**Es importante destacar que en TLS 1.3, la versión de TLS se especifica en el campo legacy\_version dentro de los mensajes ClientHello y ServerHello. Aunque el nombre del campo incluye la palabra "legacy", este es el campo utilizado para indicar la versión de TLS en esta versión del protocolo.**

**Por ejemplo, el campo legacy\_version contendrá 0x0304 para indicar TLS 1.3. El valor 0x03 indica TLS y 0x04 indica la versión específica, en este caso, TLS 1.3.**

1. **En la parte del cliente, ¿en qué trama se puede ver las suites de cifrado que soporta el cliente? ¿Cuáles son?**

A screenshot of a computer

Description automatically generatedEn la misma trama 108 por ejemplo.

1. A screenshot of a computer

   Description automatically generated**¿Qué suite de cifrado se acepta finalmente para el proceso de conexión?**
2. **En TLS1.3, no es posible ver la trama en la que se envía el certificado digital del servidor. ¿Por qué ocurre eso?**

Porque el servidor responde en “Server Hello” con un mensaje *Certificate* que contiene el certificado digital del servidor, pero cifrado con la clave pública del cliente.

**• Adicionalmente, de forma opcional: ¿Sería posible inferir cuál es la trama en la que el servidor envía al cliente su certificado?**

En TLS 1.3 el mensaje *Certificate* normalmente se envía después del mensaje *Server Hello* y antes del intercambio de claves *ChangeCipherSpec*.

**Ejercicio 2.2**

1. **¿Cuándo (de qué trama a qué trama) se procede con el proceso de handshake (sesión SSL), tal y como se ha explicado en teoría?**

Desde las tramas 70 hasta 138

**A screenshot of a computer

Description automatically generated**

1. **En esta conexión se utiliza TLS1.2. ¿Dónde se negocia exactamente la versión de TLS que se utiliza?**

Igual que en TLS1.3, en los mensajes *Client Hello* y *Server Hello.*

1. **En la parte del cliente, ¿en qué trama se puede ver las suites de cifrado que soporta el cliente? ¿Cuáles son?**

A screenshot of a computer

Description automatically generated

1. **¿Qué suite de cifrado se acepta finalmente para el proceso de conexión?**

A screenshot of a computer

Description automatically generated

1. **¿En qué trama se envía el certificado digital del servidor? En esa trama, ¿Dónde se encuentra vuestro nombre (el “common name” cuando creasteis el certificado)? ¿Cuál es la clave pública del servidor?**

A screenshot of a computer

Description automatically generated

A computer screen shot of a code

Description automatically generated

1. **¿El servidor se autentica al cliente? ¿Y el cliente al servidor?**

Nuestro servidor en todo momento envía su certificado para autentificarse. En el caso del cliente en ningún momento envía un certificado.