El protocolo TELNET

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

La IP del cliente es 192.168.12.2 y del servidor 192.168.12.1, esto lo se debido a que en el protocolo TELNET siempre inicia la conexión el cliente.

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

En la trama 7 puedo observar que las credenciales son usuario y contraseña, la contraseña parece ser “cisco”

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. ¿Qué tipo de sistema es el servidor?

No se puede ver ya que no ha sido capturado

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

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

El protocolo FTP

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

La primera trama es la petición de conexión del cliente, que tiene como source la ip 192.168.1.182 (la del cliente), y la de destinación 192.168.1.231(la del servidor)

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

Se usa el usuario y el email del usuario como contraseña

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

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

Como es un proFTPD Anonymous server usará Unix o similares.

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

Esta es la lista de comandos que ha ejecutado el cliente

Texto

Descripción generada automáticamente con confianza media

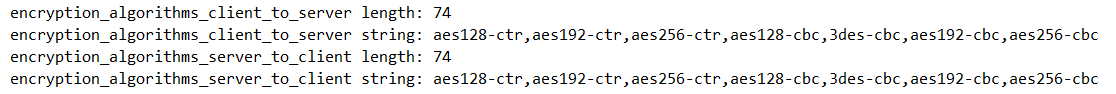
El protocolo SSH

1. **¿A partir de qué paquete comienzan a establecerse o negociarse las claves de sesión SSH? ¿De qué tipo son las claves de sesión?**

A partir de la 15 porque es un key Exchange init



Son de tipo aes ctr



1. **¿A partir de qué paquete comienza a cifrarse el tráfico de red?**

Se empieza a cifrar a partir de la trama 34 cuando ya se tienen todas las claves

****

1. **¿Qué tipo de criptosistemas se está aplicando para proteger los canales de comunicación? ¿Se aplica alguna medida de comprensión?**

Como usa el aes, el criptosistema será simétrico, no parece que se use ninguna medida de comprensión ya que no hay una entrada en el apartado ssh para ella

1. **¿Qué tipo de error se está produciendo durante la transferencia de paquetes SSH entre el cliente y el servidor?**

Esta ocurriendo un BoundErrorUnreassembled Packet

**5. ¿Es posible ver alguna información sobre las credenciales de seguridad como puede ser el usuario y la contraseña?**

No es posible debido a que el protocolo ssh usa un cifrado de extremo a extremo a diferencia de los dos vistos anteriormente.

El protocolo TLS

1. **¿Cuándo (de qué trama a qué trama) se procede con el handshake (sesión SSL) y la fase de conexión (Conexión SSL)?**

El handshake ocurre entre las tramas 74 y 77



1. **¿Qué versión de TLS se utiliza? ¿Dónde se indica? • NOTA: NO se indica en una columna del programa Wireshark, sino en el propio paquete TLS**

Se utiliza la versión 1.2, se indica en la capa tls



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

Se puede ver en la trama 74 correspondiente al client hello

Texto

Descripción generada automáticamente

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

Finalmente se acepta aes 256 gcm



1. **¿En qué trama se envía el certificado digital del servidor? En esa trama, ¿Cuál es la clave pública de meneame.net?**

No he encontrado ningún apartado correspondiente al certificado en el server hello o en cualquiera de las siguientes tramas. La clave publica de meneame.net es 32f7a4a8803905442edbbc41f7021da7d8e3c728181f7947572431d7d97a1f34

Interfaz de usuario gráfica, Texto, Word

Descripción generada automáticamente

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

Si, ambas se autentican en el hanshake