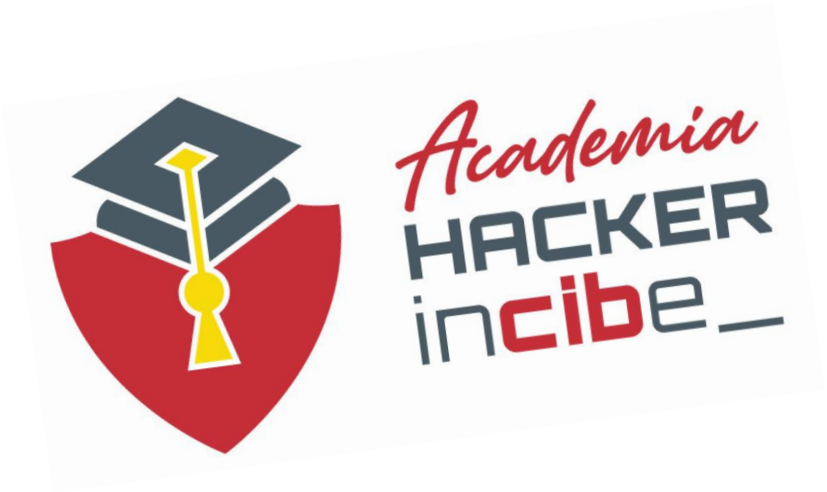
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL



Academia Hacker INCIBE

Tramas en la Red

Dificultad: **Media**

Categoría de Reto: **Forense**

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017 TU AYUDA EN CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

No se encuentran elementos de tabla de ilustraciones.

ÍNDICE DE TABLAS

No se encuentran elementos de tabla de ilustraciones.

1. CONTEXTO

Se entrega al participante una captura de tráfico donde se ha realizado una conexión remota de una máquina a otra a través de Telnet, sin solicitar ningún tipo de certificado. Se le solicita que extraiga de las tramas el usuario y la contraseña utilizados en el siguiente formato "usuario:contraseña".

Flag: **fake:user**

Datos proporcionados:

- Archivo .pcap

2. DESCRIPCIÓN PARA PARTICIPANTES

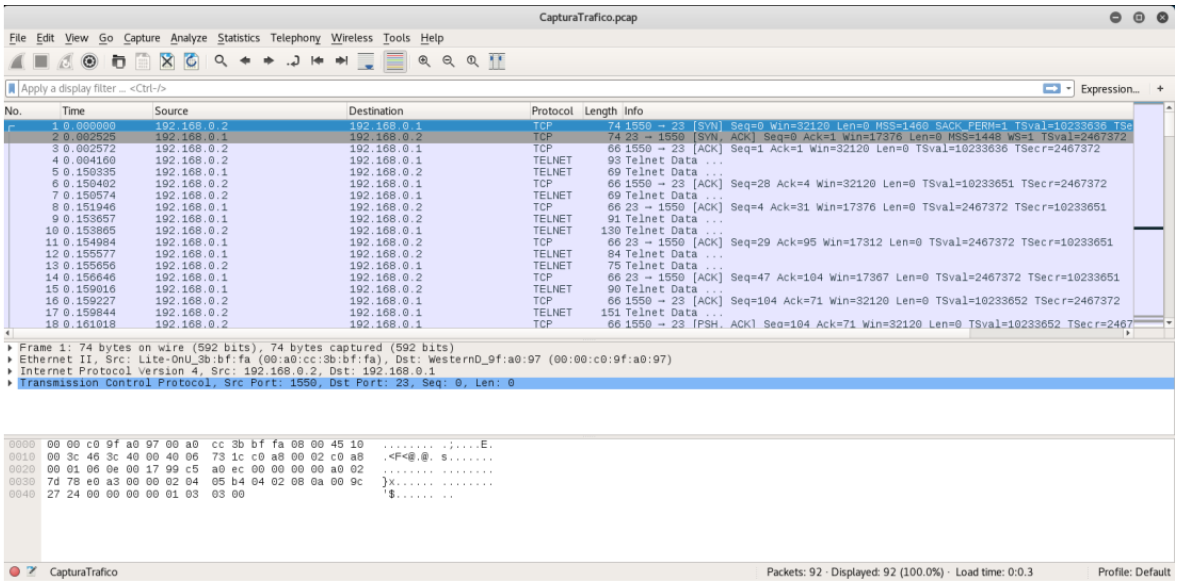
Se ha obtenido una la captura de tráfico donde se ha producido una conexión remota entre dos equipos. Encuentra las credenciales utilizadas en dicha conexión.

3. PISTAS

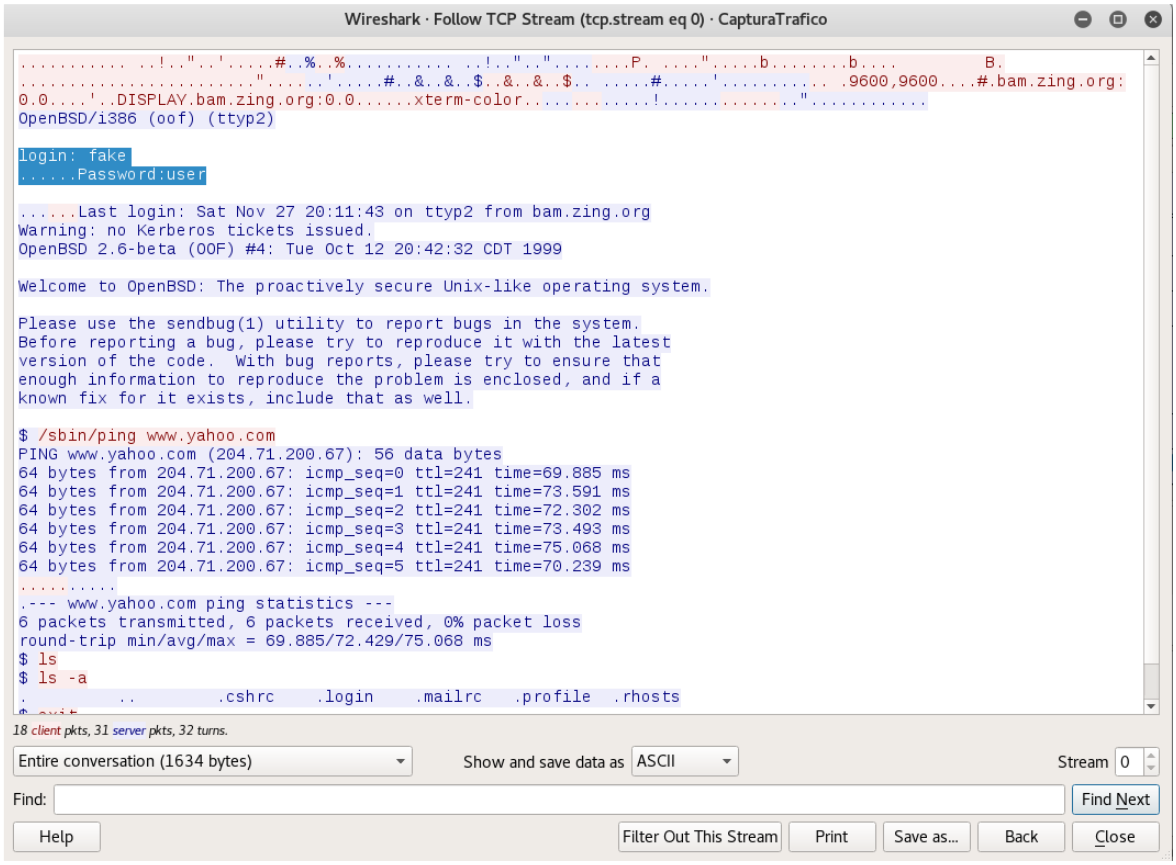
1. ¿Existe un protocolo conocido de conexión remota en la captura?
2. Intenta seguir la trama de dicha conexión.
3. La conexión utilizada es Telnet.

4. SOLUCIÓN

Se abre el archivo "Captura.pap" con Wireshark.



En este caso al ser pocos paquetes se puede detectar claramente que la conexión remota se ha realizado a través de Telnet. Para obtener usuario y contraseña se selecciona una de las tramas de Telnet y con el botón derecho: Follow >TCP Stream.



Aquí se puede obtener las credenciales utilizadas y los demás comandos utilizados durante la conexión.

Flag: **fake:user**