Práctica de laboratorio: Examinar Telnet y SSH en Wireshark Objetivos

Parte 1: Examinar una sesión de Telnet con Wireshark

Parte 2: Examinar una sesión de SSH con Wireshark

Aspectos Básicos / Escenario

En esta actividad de laboratorio configurarán un router para que acepte conectividad de SSH y use Wireshark para capturar y ver sesiones de Telnet y SSH. Esto demostrará la importancia del cifrado con SSH.

Recursos Necesarios

- Máquina virtual "CyberOps Workstation"

Instrucciones

Parte 1: Examinar una Sesión de Telnet con Wireshark

Utilizar Wireshark para capturar y ver los datos transmitidos de una sesión de Telnet.

Paso 1: Capturar datos

a. Iniciar la Máquina Virtual CyberOps Workstation VM e iniciar sesión con **analyst** como usuario y **cyberops** como contraseña.

b. Abrir una ventana del terminal e iniciar Wireshark.

```
[analyst@secOps ~]$ wireshark &
```

c. Iniciar una captura de Wireshark en la interfaz **Loopback: lo**.

d. Abrir otra ventana del terminal. Iniciar una sesión de Telnet al host local. Introducir el nombre de usuario **analyst** y la contraseña **cyberops** cuando el sistema se los solicite. Tener en cuenta que puede tardar varios minutos para que aparezcan los indicadores "conectado al host local" e inicio de sesión.

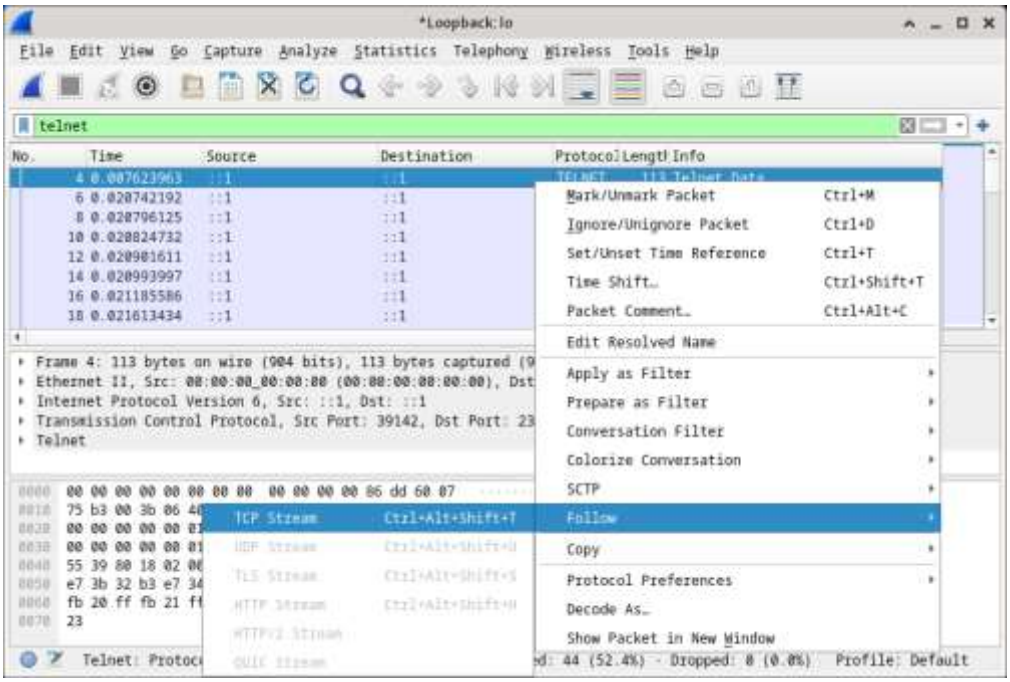
```
[analyst@secOps ~]$ telnet localhost
Trying ::1...
Connected to localhost.
Escape character is '^]'.

Linux 4.10.10-1-ARCH (unallocated.barefruit.co.uk) (pts/12)

secOps login: analyst
Password:
Last login: Fri Apr 28 10:50:52 from localhost.localdomain
[analyst@secOps ~]$
```

e. Detener la captura de Wireshark después de haber ingresado las credenciales de usuario.

Paso 2: Examinar la sesión de Telnet

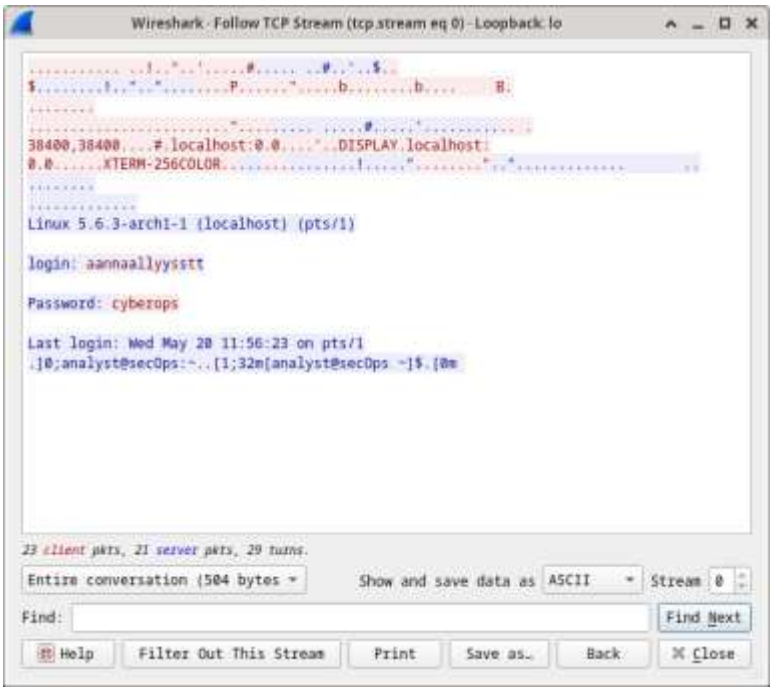
a. Aplicar un filtro que solo muestre tráfico relacionado con Telnet. Ingresar **telnet** en el campo de filtro y hacer clic en **Apply**.

b. Presionar clic en una de las líneas de **Telnet** en la sección de **Packet list** de Wireshark, y en la lista desplegable, seleccionar, **Follow** > **TCP Stream**.



c. En la ventana Follow TCP Stream se muestran los datos para su sesión de Telnet con la Máquina Virtual CyberOps Workstation VM. Toda la sesión se muestra como texto plano, incluida la contraseña.

Observar que el nombre de usuario que introdujeron aparece con caracteres duplicados. Esto se debe al ajuste de echo en Telnet para permitirle ver los caracteres que escribe en la pantalla.



d. Cuando termine de revisar la sesión de Telnet en la ventana **Follow TCP Stream**(Seguir stream de TCP), hacer clic en **Close** (Cerrar).

e. Escribir **exit** en el terminal para salir de la sesión de **Telnet**.

```
[analyst@secOps ~]$ exit
```

Parte 2: Examinar una sesión de SSH con Wireshark

En la Parte 2 establecerán una sesión de SSH con el host local. Se usará Wireshark para capturar y ver los datos de esta sesión de SSH.

a. Iniciar una captura de Wireshark en la interfaz **Loopback: lo**

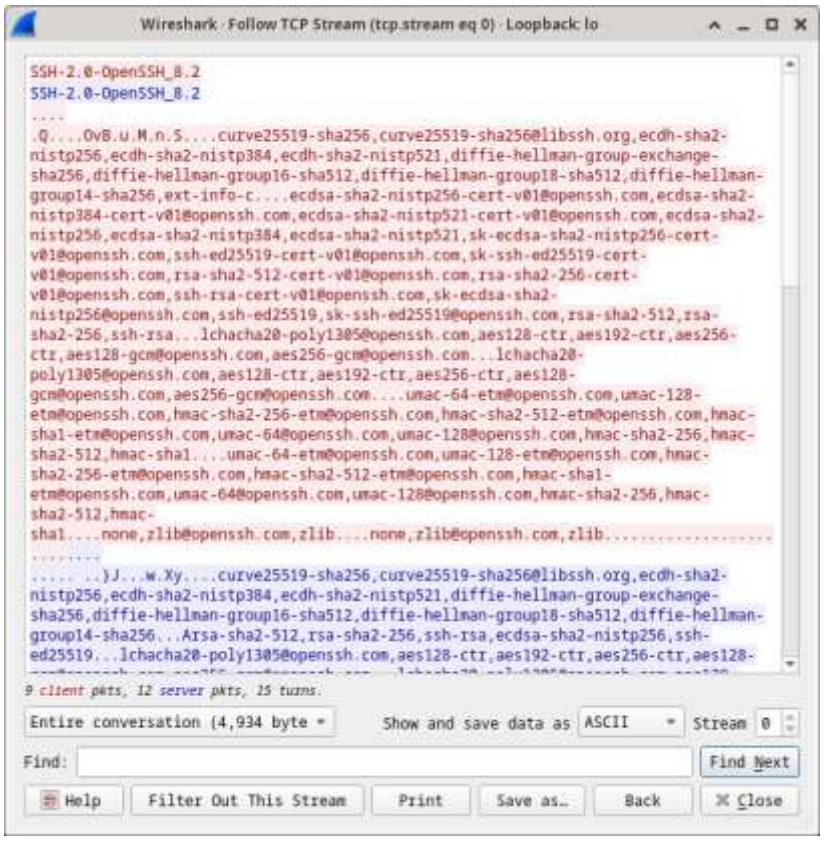
b. Establecerán una sesión de SSH con el host local. En el prompt del terminal, introducir **ssh localhost**. Ingresar **yes** (sí) para seguir con la conexión. Introducir **cyberops** cuando el sistema se los solicite.

```
[analyst@secOps ~]$ ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:1xZuV8NMeVsNQPRrzVf9nXHzdUP+EtgVouZVbWH80XA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
analyst@localhost's password:
Last login: Sat May 23 10:18:47 2020Stop the Wireshark capture.
```

c. Aplicar un filtro de SSH a los datos de la captura de Wireshark. Introducir **ssh** en el campo de filtro y haga clic en **Aplicar**.

d. Presionar click en una de las líneas de **Telnet** en la sección de **Packet list** de Wireshark, y en la lista desplegable, seleccionar, **Follow** > TCP Stream.

e. Examinar la ventana **Follow TCP Stream** en la sesión de SSH. Los datos se cifraron y son ilegibles. Comparar los datos de la sesión de SSH con los datos de la sesión de Telnet.



f. Luego de haber examinado su sesión SSH, hacer clic en **Close** (Cerrar).

g. Cerrar Wireshark.

Pregunta de reflexión

¿Por qué se prefiere SSH en lugar de Telnet para conexiones remotas?