实验 - 在 Wireshark 中检查 Telnet 和 SSH

目标

第 1 部分：通过 Wireshark 检查 Telnet 会话

第 2 部分：通过 Wireshark 检查 SSH 会话

背景/场景

在本实验中，同学们将使用 Wireshark 捕获和查看 Telnet 和 SSH 会话。本练习将演示 SSH 中加密的重要性。

所需资源

- CyberOps Workstation VM

第 1 部分： 通过 Wireshark 检查 Telnet 会话

同学们将使用 Wireshark 来捕获和查看 Telnet 会话传输的数据。

第 1 步： 捕获数据

a. 启动 CyberOps Workstation 虚拟机，并使用用户名 **analyst** 和密码 **cyberops** 登录。

b. 打开一个终端窗口并启动 Wireshark。阅读警告消息后，按**确定**继续。

```
[analyst@secOps analyst]$ sudo wireshark-gtk
[sudo] password for analyst: cyberops

** (wireshark-gtk:950): WARNING **: Couldn't connect to accessibility bus: Failed
to connect to socket /tmp/dbus-REDRWOHelr: Connection refused
Gtk-Message: GtkDialog mapped without a transient parent.This is discouraged.
```

c. 在 **Loopback: lo** 接口上开始 Wireshark 捕获。

d. 打开另一个终端窗口。发起到本地主机的 Telnet 会话。系统提示时，输入用户名 **analyst** 和密码 **cyberops**。

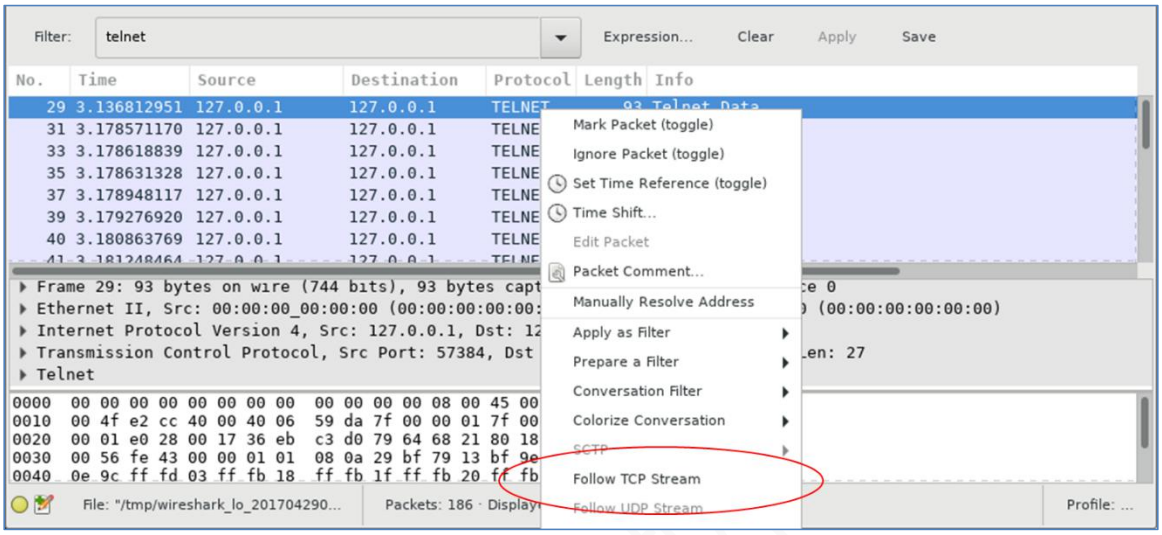
```
[analyst@secOps ~]$ telnet localhost
Trying ::1...
Connected to localhost.
Escape character is '^]'.

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. 在同学们提供用户凭证后停止 Wireshark 捕获。

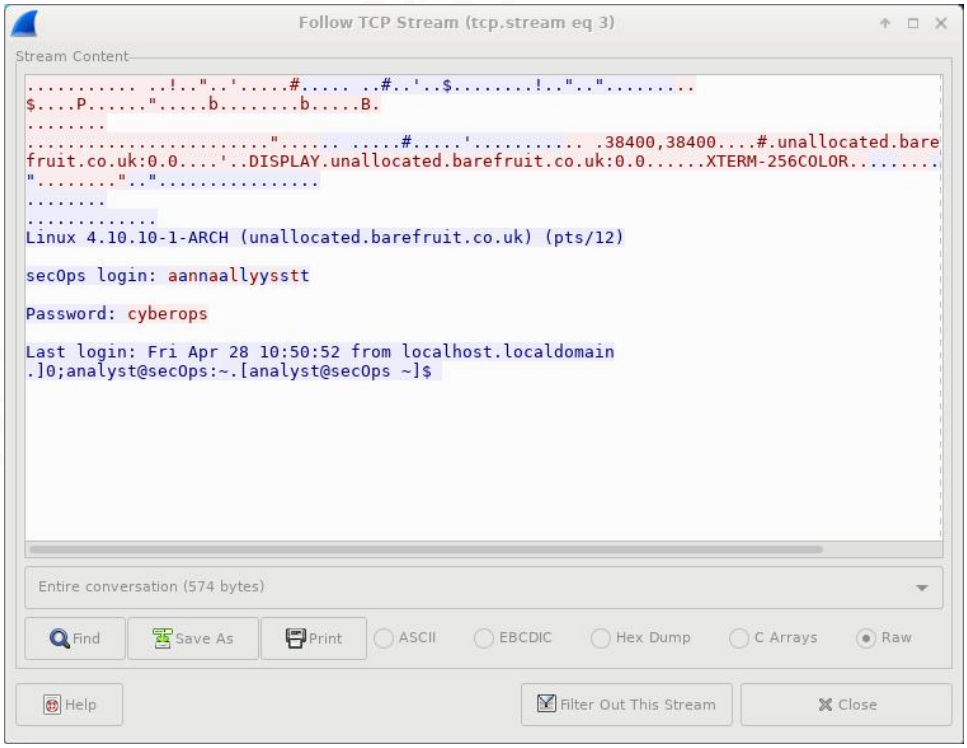
第 2 步： 检查 Telnet 会话。

a. 应用只显示与 Telnet 相关的流量的过滤器。在过滤器字段中输入 **Telnet**。

b. 在 Wireshark 的 Packet list（数据包列表）部分，右键点击一个 Telnet 线路，然后在下拉列表中，选择 Follow TCP Stream（跟踪 TCP 数据流）。



c. “跟踪 TCP 数据流”窗口显示 CyberOps Workstation 虚拟机中 Telnet 会话的数据。整个会话以明文显示，包括密码。请注意，同学们输入的用户名显示为重复字符。这是由 Telnet 中响应设置（允许同学们查看屏幕上输入的字符）造成的。



d. 在 Follow TCP Stream（跟踪 TCP 数据流）窗口中检查完同学们的 Telnet 会话后，请点击 Close（关闭）。

e. 在终端中键入 **exit** 以退出 **Telnet** 会话。

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

第 2 部分： 通过 Wireshark 检查 SSH 会话

在第 2 部分中，同学们将与本地主机建立 SSH 会话。我们将使用 Wireshark 来捕获和查看此 SSH 会话的数据。

a. 开始另一次 Wireshark 捕获。

b. 同学们将与本地主机建立 SSH 会话。在终端提示符后，输入 **ssh localhost**。输入 **yes** 以继续连接。系统提示时，输入 **cyberops**。

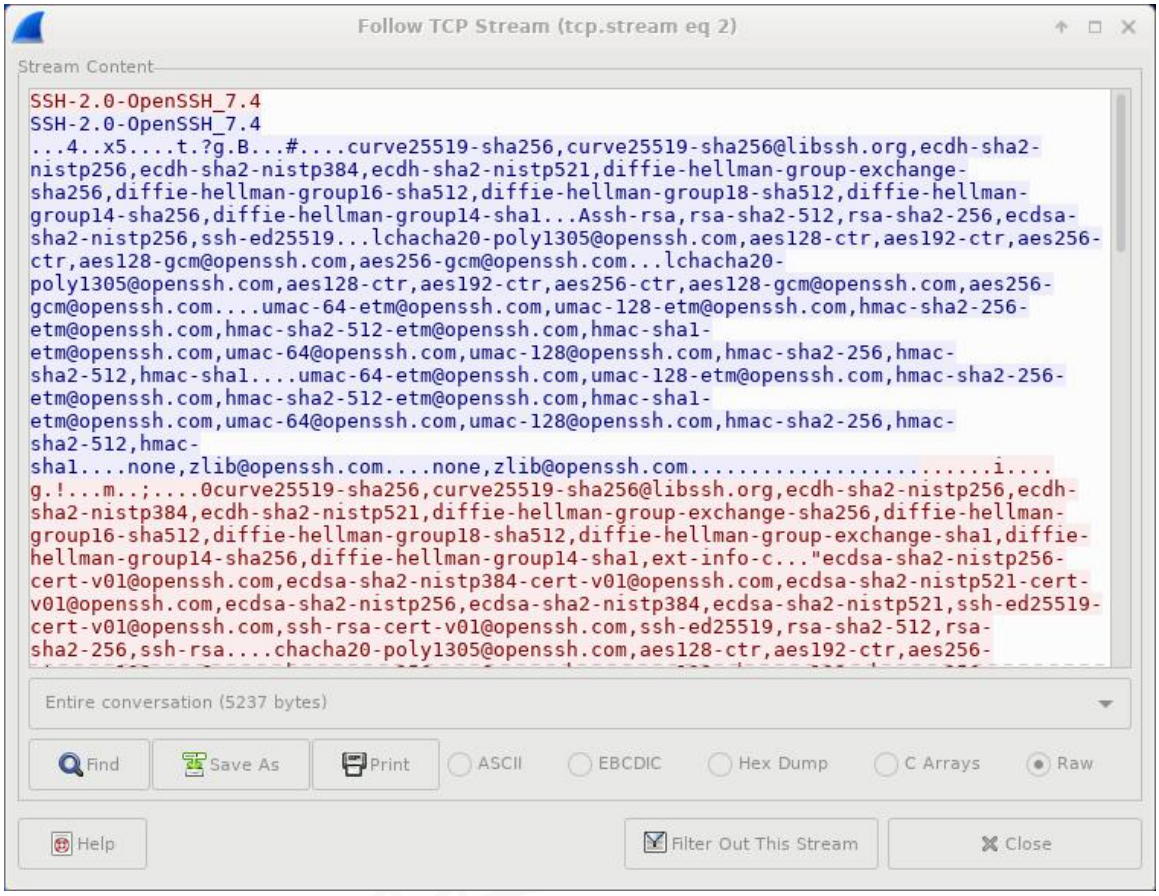
```
[analyst@secOps ~]$ ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:uLDhKZflmvsR8Et8jer1NuD91cGDS1mUl/p7VI3u6kI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
analyst@localhost's password:
Last login: Sat Apr 29 00:04:21 2017 from localhost.localdomain
```

c. 停止 Wireshark 捕获。

d. 对 Wireshark 捕获数据应用 SSH 过滤器。在过滤器字段中输入 **ssh**。

e. 在 Wireshark 的 Packet list（数据包列表）部分，右键点击一个 **SSHv2** 线路，然后在下拉列表中，选择 Follow TCP Stream（跟踪 TCP 数据流）选项。

f. 检查 SSH 会话的 Follow TCP Stream（跟踪 TCP 数据流）窗口。数据已加密，无法读取。将 SSH 会话中的数据与 Telnet 会话中的数据进行比较。



g. 检查同学们的 SSH 会话后，点击 Close（关闭）。

h. 关闭 Wireshark。

思考

进行远程连接时为什么首选 SSH，而不是 Telnet？

_____

_____

_____

_____

_____

_____