CISCO Academy

Answers: 16.3.12 Lab - Examining Telnet and SSH in Wireshark

Objectives

Part 1: Examine a Telnet Session with Wireshark

Part 2: Examine an SSH Session with Wireshark

Background / Scenario

In this lab, you will configure a router to accept SSH connectivity and use Wireshark to capture and view Telnet and SSH sessions. This will demonstrate the importance of encryption with SSH.

Required Resources

• Security Workstation virtual machine

Instructions

Part 1: Examining a Telnet Session with Wireshark

You will use Wireshark to capture and view the transmitted data of a Telnet session.

Step 1: Capture data.

- a. Start the Security Workstation VM and log in with username sec_admin and password net_secPW.
- b. Open a terminal window and start Wireshark.

[sec_admin@secOps ~]\$ wireshark &

- c. Start a Wireshark capture on the Loopback: lo interface.
- d. Open another terminal window. Start a Telnet session to the localhost. Enter username sec_admin and password net_secPW when prompted. Note that it may take several minutes for the "connected to localhost" and login prompt to appear.

```
[sec_admin@secOps ~]$ telnet localhost
Trying ::1...
Connected to localhost.
Escape character is '^]'.
Linux 5.10.14-arch1-1 (localhost) (pts/2)
login: sec_admin
Password:
Last login: Tue Feb 16 15:07:23 on pts/2
[sec_admin@secOps ~]$
```

e. Stop the Wireshark capture after you have provided the user credentials.

Step 2: Examine the Telnet session.

a. Apply a filter that only displays Telnet-related traffic. Enter telnet in the filter field and click Apply.

b. Right-click one of the **Telnet** lines in the **Packet list** section of Wireshark, and from the drop-down list, select **Follow** > **TCP Stream**.

		^ _	. o x					
<u>F</u> il	e <u>E</u> dit <u>V</u> iew <u>G</u> o	<u>C</u> apture <u>A</u> nalyze	<u>S</u> tatistics Telephon <u>y</u>	<u>W</u> ireless <u>T</u> ools <u>H</u> elp				
		I 🖹 🖹 🏹 🤇) @ @ % K %					
, t	elnet					•		
No.	Time	Source	Destination	Protocol Lengtł Info		^		
	4 0.007623963	::1	::1	TELNET 113 Telnet Data				
	6 0.020742192	::1	::1	<u>M</u> ark/Unmark Packet	Ctrl+M			
	8 0.020796125	::1	::1	Ignore/Unignore Packet	Ctrl+D			
	10 0.020824732	1	1	Set/Unset Time Reference	Ctrl+T			
	14 0.020993997	::1	::1	Time Shift	Ctrl+Shift+T			
	16 0.021185586	::1	::1	Parlat Grand	ct_lialtic			
	18 0.021613434	::1	::1	Packet Comment	Ctrl+Alt+C	-		
4				Edit Resolved Name				
► E	rame 4: 113 bytes (on wire (904 bits),	113 bytes captured (9	Apply as Filter	Þ			
	nternet Protocol V	ersion 6. Src: ::1.	Dst: ::1	Prepare as Filter	•			
► T.	Transmission Control Protocol, Src Port: 39142, Dst Port: 2			Conversation Filter				
► T	elnet		Conversation Filter					
				Colorize Conversation	+			
000	0 00 00 00 00 00 0	0 00 00 00 00 00 00	86 dd 60 07 · · · · · ·	SCTP	+			
001	75 b3 00 3b 06 4	TCP Stream	Ctrl+Alt+Shift+T	Follow	÷.			
002	000000000000000000000000000000000000000	1 UDP Stream	Ctrl+Alt+Shift+U	Copy	•			
0040	55 39 80 18 02 0	e TLS Stroom	C+rl (Alt) Chift (C					
005	e7 3b 32 b3 e7 3	4 ILS SLIEdill	CULL+AIU+SHILL+S	Protocol Preferences	•			
006	0 TD 20 TT TD 21 T	HTTP Stream	Ctrl+Alt+Shift+H	Decode As				
507	23	HTTP/2 Stream		Show Packet in New Window				
0	QUIC Stream							

c. The Follow TCP Stream window displays the data for your Telnet session with the Security Workstation VM. The entire session is displayed in plaintext, including your password. Notice that the username that you entered is displayed with duplicate characters. This is caused by the echo setting in Telnet to allow you to view the characters that you type on the screen.

A	Wireshark · Follow TC	P Stream (tcp.str	eam eq 0) · Loopbac	k: lo	<u>^ -</u>		×
\$P	!	#'\$ b	5 B.	#]
 20100 2010	·····".		· · · · · · · · · · · · · · · · · · ·				
50400,5040	U	INPL					
Linux 5.10	.14-arch1-1 (loc	alhost) (pts/	(2)				
" <mark>1</mark>	.ogin: sseeccaa	addmmiinn					
Password	net secPW						
10350010.	nec_seenw						
Last login	: Tue Feb 16 15:	07:23 on pts/	2				
.]0;sec_ad	lmin@secOps:~[?	2004h[sec_adm	nin@secOps ~]\$				
!5 <mark>client</mark> pkts, 24	server pkts, 31 turns.						
!5 <i>client pkts, 24</i> Entire convei	server pkts, 31 turns.	Show data a	s ASCII	▼ Si	ream	0]
?5 <i>client pkts, 24</i> Entire conver Find:	server pkts, 31 turns. rsation (456 byt. 💌	Show data as	s ASCII	✓ Si	ream Find <u>N</u>	0]

- d. After you have finished reviewing your Telnet session in the Follow TCP Stream window, click Close.
- e. Type exit at the terminal to exit the Telnet session.

[sec admin@secOps ~]\$ exit

Part 2: Examine an SSH Session with Wireshark

In Part 2, you will establish an SSH session with the localhost. Wireshark will be used to capture and view the data of this SSH session.

- a. Start another Wireshark capture using the **Loopback: lo** interface.
- b. You will establish an SSH session with the localhost. At the terminal prompt, enter **ssh localhost**. Enter **yes** to continue connecting. Enter the **net_secPW** when prompted.

```
[sec_admin@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.
sec_admin@localhost's password:
Last login: Sat May 23 10:18:47 2020
```

- c. Stop the Wireshark capture.
- d. Apply an SSH filter on the Wireshark capture data. Enter **ssh** in the filter field and click **Apply**.
- e. Right-click one of the SSHv2 lines in the Packet list section of Wireshark, and in the drop-down list, select the Follow > TCP Stream.

f. Examine the **Follow TCP Stream** window of your SSH session. The data has been encrypted and is unreadable. Compare the data in your SSH session to the data of your Telnet session.

🚄 🛛 Wireshark · Follow TCP Stream (tcp.stream eq 0) · Loopback: lo 💦 🔺 🗖 🗙
SSH-2.0-OpenSSH_8.4 SSH-2.0-OpenSSH_8.4
hellman-group14-sha1,diffie-hellman-group18-sha512,diffie-hellman- group14-sha256,ext-info-cecdsa-sha2-nistp256-cert-
v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2- nistp521-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert- v01@openssh.com_ssh-ed25519-cert-v01@openssh.com_sk-ssh-ed25519-cert-
v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert- v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-
sha2-nistp384,ecdsa-sha2-nistp521,sk-ecdsa-sha2-nistp256@openssh.com,ssh- ed25519,sk-ssh-ed25519@openssh.com,rsa-sha2-512,rsa-sha2-256,ssh- rsalchacha20-polv1305@openssh.com,aes128-ctr.aes192-ctr.aes256-
<pre>ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.comlchacha20- poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-</pre>
gcm@openssn.com,aes256-gcm@openssn.comumac-64- etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256- etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac- sha2-256,hmac-sha2-512,hmac-sha1umac-64-etm@openssh.com,umac-128- otm@opensch.com,bmac.sha2.556.otm@opensch.com,bmac.sha2.512
etm@openssh.com,hmac-shal- etm@openssh.com,hmac-shal- etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-
sha2-256, hmac - sha2-512, hmac - Packet 8. 9 client pkts, 13 server pkts, 15 turns. Click to select.
Entire conversation (6,890 by Show data as ASCII Stream 0
Image: Constraint of the stream Print Save as Back X Close

- g. After examining your SSH session, click Close.
- h. Close Wireshark.

Reflection Question

Why is SSH preferred over Telnet for remote connections?