Práctica de laboratorio: Examinación de Telnet y SSH en Wireshark

Topología



Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	N/D
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: configurar los dispositivos para el acceso por SSH

Parte 2: examinar una sesión de Telnet con Wireshark

Parte 3: examinar una sesión de SSH con Wireshark

Aspectos básicos/situación

En esta actividad de laboratorio, deberá configurar un router para que acepte la conectividad de SSH y usará Wireshark para capturar y ver las sesiones de Telnet y SSH. Esto demostrará la importancia del cifrado con SSH.

Nota: Los routers que se utilizan en las actividades prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces de router al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS versión 15.2(4)M3, imagen universal o similar)
- 1 PC (Windows 7, 8 o 10 con un programa de emulación de terminal, como Tera Term, y Wireshark instalado)
- Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 1: Configurar los dispositivos para el acceso por SSH

En la parte 1, establecerá la topología de la red y configurará los ajustes básicos, como las direcciones IP de la interfaz, el acceso al dispositivo y las contraseñas del router.

Paso 1: Realizar el cableado de red tal como se muestra en la topología

Paso 2: Iniciar y Volver a cargar el router

Paso 3: Configurar los ajustes básicos en el router

- a. Acceda al router mediante el puerto de la consola e ingrese al modo EXEC privilegiado.
- b. Entre al modo de configuración.
- c. Configure el nombre del dispositivo como se indica en la tabla de direccionamiento.
- d. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- e. Asigne class como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne cisco como la contraseña de consola y permita el inicio de sesión.
- g. Asigne cisco como la contraseña de VTY y habilite el inicio de sesión.
- h. Encripte las contraseñas de texto no cifrado.
- i. Cree un banner que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- j. Configure y active la interfaz G0/1 utilizando la información de la tabla de direccionamiento.

Paso 4: Configurar R1 para el acceso por SSH

a. Configure el dominio para el dispositivo.

R1(config) # ip domain-name ccna-lab.com

b. Configure el método de cifrado de clave.

R1(config) # crypto key generate rsa modulus 1024

c. Configure un nombre de usuario de la base de datos local.

R1(config)# username admin privilege 15 secret adminpass

d. Habilite Telnet y SSH en las líneas VTY.

R1(config)# line vty 0 4

R1(config-line) # transport input telnet ssh

- e. Cambie el método de inicio de sesión para utilizar la base de datos local para la verificación del usuario.
 - R1(config-line)# login local

R1(config-line)# end

Paso 5: Guardar la configuración en ejecución en el archivo de configuración de inicio

Paso 6: Configurar PC-A

- a. Configure PC-A con una dirección IP y una máscara de subred.
- b. Configure una puerta de enlace predeterminada para PC-A.

Paso 7: Verificar la conectividad de la red

Haga ping a R1 desde PC-A. Si el ping falla, resuelva los problemas de la conexión.

Parte 2: Examinar una sesión de Telnet con Wireshark

En la parte 2, deberá usar Wireshark para capturar y ver los datos transmitidos de una sesión de Telnet en el router. Utilizará Tera Term para acceder a R1 mediante Telnet, se registrará y luego emitirá el comando **show run** en el router.

Nota: Si no tiene un paquete de software de cliente Telnet/SSH instalado en la PC, deberá instalarlo antes de continuar. Dos paquetes populares de software gratuito de Telnet/SSH son Tera Term (<u>http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html</u>) y PuTTY (<u>www.putty.org</u>).

Nota: Telnet no está disponible desde el símbolo del sistema enWindows 7, de manera predeterminada. Para habilitar Telnet para usarlo en la ventana de símbolo del sistema, haga clic en **Start** (Comenzar) > **Control Panel** (Panel de control) > **Programs** (Programas) > **Programs and Features** (Programas y funciones) > **Turn Windows features on or off** (Activar o desactivar las funciones de Windows). Haga clic en la casilla de verificación **Telnet Client** (Cliente Telnet) y luego haga clic en **OK** (Aceptar).

Paso 1: Capturar los datos

- a. Abra Wireshark.
- b. Comience a capturar los datos en la interfaz de LAN.

Nota: Si no puede comenzar la captura en la interfaz LAN, deberá abrir Wireshark con la opción **Run as Administrator** (Ejecutar como administrador).

Paso 2: Iniciar una sesión de Telnet en el router

a. Abra Tera Term y seleccione el botón de opción **Telnet** del campo Service (Servicio) y, en el campo Host, ingrese **192.168.1.1**.

● TCP/ <u>I</u> P	Hos <u>t</u> :	192.168.1.1		•
	Service: (ℤ Hist <u>o</u> ry) Te <u>l</u> net	TCP port#: 2	3
	() <u>s</u> sh	SSH version: SSH	2 -
	0	Other	Proto <u>c</u> ol: UNSF	PEC 🔻
⊙ S <u>e</u> rial	Po <u>r</u> t: (-

¿Cuál es el puerto TCP predeterminado para las sesiones de Telnet?

 b. En la petición Username: (Nombre de usuario:), ingrese admin y en la petición Password: (Contraseña:), ingrese adminpass. Estas peticiones se generan porque configuró las líneas VTY para que utilicen la base de datos local con el comando login local.



c. Emita el comando show run.

R1# show run

d. Ingrese exit (Salir) para cerrar la sesión de Telnet y Tera Term.

R1# exit

Paso 3: Detener la captura Wireshark

Paso 4: Aplicar un filtro de Telnet a los datos de captura de Wireshark

telnet	×→	•	Expre

Paso 5: Utilizar la función Follow TCP Stream (Seguir stream de TCP) en Wireshark para ver la sesión de Telnet

a. Haga clic con el botón derecho en una de las líneas **Telnet** y en la sección **Packet list** (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream**.

File Edit View Go Cap	pture Analyze Statistics	Telephony Wirele	ss Tools Help	
🚄 🔳 🖉 💿 📙 🚠 🗙	🖸 🍳 🗢 🔿 😤 👔	👲 📃 📃 🔍 Q	e. 🎹	
📕 telnet				Expression
telnet No. Time 28 30.684843 29 30.686497 31 30.687898 32 30.688515 34 30.706429 35 30.707252 36 30.707716 38 30.707786 41 30.905737 Frame 28: 66 Ethernet II, Src: Cis Internet Protocol Ver Transmission Control Telnet	Source 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.3 192.168.1.3 192.168.1.3 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.3 n wire (528 bi protocol, Src Free Science Scienc	Destination ark/Unmark Packet nore/Unignore Packet t/Unset Time Reference me Shift lit Resolved Name oply as Filter epare a Filter onversation Filter olorize Conversation CTP	Protocol Leng Ctrl+M Ctrl+D ctrl+T Ctrl+Shift+T Ctrl+Alt+C	Expression th Info 6 Telnet Data 8 Telnet Data 9 Telnet Data
	Cr Pr Dr Sł	opy otocol Preferences ecode As Iow Packet in New Wind	e dow	UDP Stream SSL Stream HTTP Stream

b. En la ventana Follow TCP Stream (Seguir stream de TCP), se muestran los datos para su sesión de Telnet con el router. Toda la sesión y la contraseña se muestran como texto no cifrado. Observe que el nombre de usuario y el comando show run que ingresó aparecen con caracteres duplicados. Esto se debe al ajuste de eco en Telnet para permitirle ver los caracteres que escribe en la pantalla.

✓ Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_D4A31D
^
User Access Verification
Username:
Password: adminpass
R1#ssnb rruunn
Building configuration
Current configuration : 2039 bytes
version 12.4
39 dient pkts, 35 server pkts, 55 turns,
Entire conversation (3302 bytes) Show and save data as ASCII Stream
Find: Find Next
Filter Out This Stream Print Save as Back Close Help

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

Parte 3: Examinar una sesión de SSH con Wireshark

En la parte 4, deberá usar el software Tera Term para establecer una sesión de SSH con el router. Se usará Wireshark para capturar y ver los datos de esta sesión de SSH.

Paso 1: Abrir Wireshark y comenzar a capturar los datos en la interfaz LAN

Paso 2: Iniciar una sesión de SSH en el router

 Abra Tera Term e ingrese la dirección IP de la interfaz G0/1 de R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: Conexión nueva). Asegúrese de que el botón de opción SSH esté seleccionado y haga clic en OK (Aceptar) para conectarse al router.

Tera Term: New cor	nnection	×
● TCP <u>/I</u> P	Hos <u>t</u> : 192.168.1 V Hist <u>o</u> ry Service: O Te <u>l</u> net O <u>S</u> SH O Other	I.1 ▼ TCP port#: 22 SSH yersion: SSH2 ▼ Protocol: UNSPEC ▼
○ S <u>e</u> rial	Po <u>r</u> t: OK Cance	el <u>H</u> elp

¿Cuál es el puerto TCP predeterminado que se usa para las sesiones de SSH? ____

 La primera vez que establece una sesión de SSH con un dispositivo, se genera una SECURITY WARNING (Advertencia de seguridad) para comunicarle que no se conectó a ese dispositivo anteriormente. Este mensaje es parte del proceso de autenticación. Lea la advertencia de seguridad y luego haga clic en Continue (Continuar).

SECURITY WARNING	\times
There is no entry for the server "192.168.1.1" in your list of known hosts. The machine you have contacted may be a hostile machine pretending to be the server.	
If you choose to add this machine to the known hosts list and continue, then you will not receive this warning again.	
The server's host key fingerprint is: Fingerprint hash algorithm: OMD5 SHA256 SHA256:2Y2C4RmPeO100D5cOQhsmE7+UYAIxEt7cCukjU/L+bo]
+[RSA 1024]+ 00 =0. = 0 = 00 * = =0 0 + 0 * 0000.* + . + =. *.S.B . = . 0.0 . E0 +[SHA256]+	
Add this machine and its key to the known hosts list	1

c. En la ventana SSH Authentication (Autenticación de SSH), ingrese admin en username (Nombre de usuario) y adminpass en passphrase (Frase de contraseña). Haga clic en OK (Aceptar) para registrarse en el router.

SSH Authentication		_	×
Logging in to 192.168	.1.1		
Authentication require	ed.		
User name:	admin		
Passphrase:	••••••		
	Remember password in memory		
	Forward agent		
Use plain passw	ord to log in		
O Use RSA/DSA/E	CDSA/ED25519 key to log in Private key file:		
O Use rhosts to lo	g in (SSH1) Local user name:		
	Host private key file:		
O Use challenge/re	esponse to log in(keyboard-interactive)		
O Use Pageant to	log in		
	OK Disconnect		

d. Estableció una sesión de SSH en el router. El software Tera Term parece muy similar a una ventana de comandos. En el símbolo del sistema, emita el comando **show run**.



e. Salga de la sesión de SSH emitiendo el comando exit.

R1# **exit**

Paso 3: Detener la captura Wireshark

Paso 4: Aplicar un filtro de SSH a los datos de captura de Wireshark



Paso 5: Utilizar la función Follow TCP Stream en Wireshark para ver la sesión de SSH

- a. Haga clic con el botón derecho en una de las líneas **SSHv2** en la sección Packet list (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream** (Seguir stream de TCP).
- b. Examine la ventana **Follow TCP Stream** (Seguir stream de TCP) en la sesión de SSH. Los datos se cifraron y son ilegibles. Compare los datos de la sesión de SSH con los datos de la sesión de Telnet.

✓ Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_D4A31D — 🛛	×					
SSH-2.0-Cisco-1.25	~					
SSH-2.0-TTSSH/2.83 Win32						
l4.c0=~QYdiffie-hellman-group-exchange-sha1,diffie-						
hellman-group14-sha1,diffie-hellman-group1-sha1ssh-rsaJaes128-						
ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-						
CDCJaes128-CTF, aes192-CTF, aes256-CTF, aes128-CDC, 30es-CDC, aes192- cbc_aes256-cbcbmac_sba1_bmac_sba1_96bmac_sba1_bmac_						
shal-96nonenonenone						
2L9>yFecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-						
nistp521,diffie-hellman-group18-sha512,diffie-hellman-group16-						
sha512,diffie-hellman-group14-sha256,diffie-hellman-group-exchange-						
sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-						
shal,diffie-hellman-groupl-shalWecdsa-sha2-nistp256,ecdsa-sha2-						
gcm@openssh.com.aes128-gcm@openssh.com.camellia256-ctr.aes256-						
<pre>ctr,camellia256-cbc,aes256-cbc,camellia192-ctr,aes192-ctr,camellia192-</pre>	v					
Backat 17, 22 client akts, 27 parties akts, 56 turns, Click to select						
Entire conversation (8777 bytes) Show and save data as ASCII	•					
Find: Find New	(t					
Filter Out This Stream Print Save as Back Close Help						

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

- c. Luego de haber examinado su sesión SSH, haga clic en Close (Cerrar).
- d. Cierre Wireshark.

Reflexión

¿Cómo brindaría acceso a un dispositivo de red a varios usuarios, cada uno con un nombre de usuario diferente?

Resumen de interfaces de router						
Modelo de router	Interfaz Ethernet 1	Interfaz Ethernet 2	Interfaz serial 1	Interfaz serial 2		
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)		
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)		
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)		
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)		
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)		

Tabla de resumen de interfaces de router

Nota: Para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de hacer una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz.