Analyse de Telnet et de SSH dans Wireshark

Objectifs

Partie 1 : Analyser une session Telnet avec Wireshark

Partie 2 : Analyser une session SSH avec Wireshark

Contexte/scénario

Au cours de ces travaux pratiques, vous allez configurer un routeur pour qu'il accepte les connexions SSH, et vous utiliserez Wireshark pour capturer et afficher des sessions Telnet et SSH. Vous verrez ainsi l'importance du chiffrement avec SSH.

Ressources requises

- Poste de travail CSE_LABVM

Instructions

Partie 1 : Analyser une session Telnet avec Wireshark

Vous allez utiliser Wireshark pour capturer et afficher les données transmises d'une session Telnet.

Étape 1: Capturez des données.

a. Démarrez le poste de travail de la machine virtuelle CSE_LABVM

b. Ouvrez une fenêtre du terminal et démarrez Wireshark.

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

c. Démarrez une capture Wireshark sur l'interface **Loopback: lo**.

d. Ouvrez une autre fenêtre de terminal. Démarrez une session Telnet pour accéder à l'hôte local (localhost). À l'invite, saisissez le nom d'utilisateur **cisco** et le mot de passe **password**.

```
[cisco@labvm ~]$ telnet localhost
Trying ::1...
Connected to localhost.
Le caractère d'échappement est '^]'.

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

secOps login: cisco
```

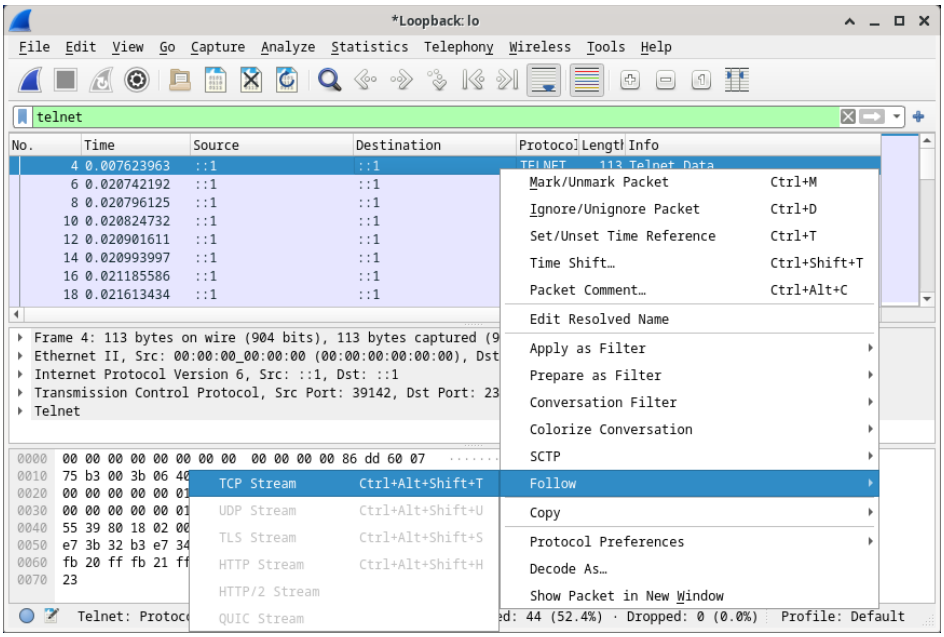
```
Mot de passe :
Last login: Fri Apr 28 10:50:52 from localhost.localdomain
[cisco@labvm ~]$
```

e. Arrêtez la capture Wireshark après avoir saisi les informations d'identification.

Étape 2: Analyser la session Telnet

a. Appliquez un filtre pour afficher uniquement le trafic lié à Telnet. Dans le champ Filter, saisissez **Telnet** , puis cliquez sur **Apply**.

b. Cliquez avec le bouton droit sur l'une des lignes **Telnet** dans la section **Packet list** (Liste des paquets) de Wireshark et, dans la liste déroulante, sélectionnez l'option **Follow** > **TCP Stream**(Suivre le flux TCP).



c. La fenêtre Follow TCP Stream affiche les données de votre session Telnet avec le poste de travail virtuel CyberOps. La session complète s'affiche en texte clair, y compris votre mot de passe. Notez que les caractères du nom d'utilisateur que vous avez saisi sont dupliqués. Cela provient du paramètre d'écho dans Telnet qui vous permet d'afficher les caractères que vous tapez à l'écran.

d. Une fois que vous avez fini de passer en revue votre session Telnet dans la fenêtre **Follow TCP Stream** (Suivre le flux TCP), cliquez sur **Close** (Fermer).

e. Saisissez **exit** à l'invite du terminal pour fermer la session **Telnet**.

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

Partie 2 : Analyser une session SSH avec Wireshark

Dans la partie 2, vous allez établir une session SSH avec l'hôte local. Wireshark permet de capturer et d'afficher les données de cette session SSH.

a. Démarrez une capture Wireshark en utilisant l'interface **Loopback: lo**.

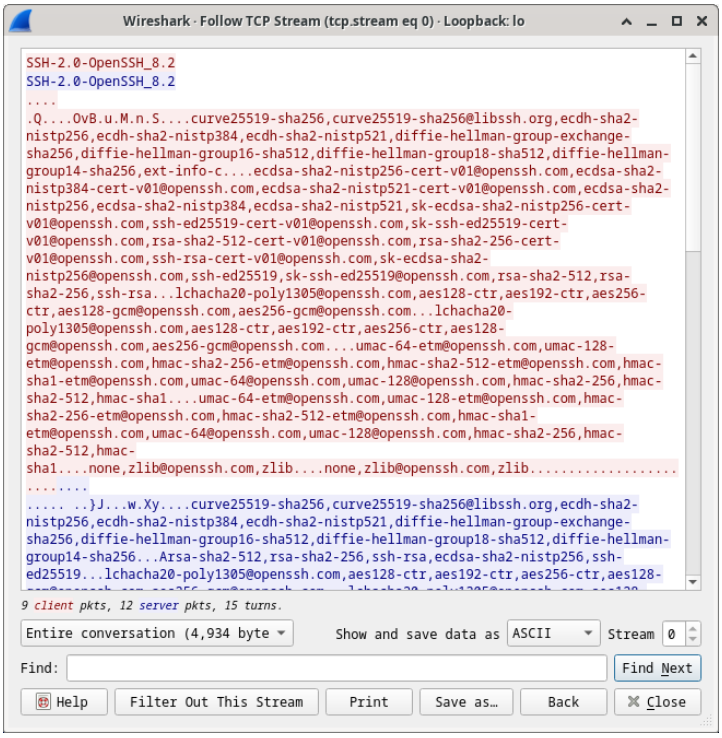
b. Vous allez établir une session SSH avec l'hôte local. À l'invite du terminal, saisissez **ssh localhost**. Saisissez **yes** pour poursuivre la connexion. À l'invite, saisissez le mot de passe **password**.

```
[cisco@labvm ~]$ 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. Appliquez un filtre SSH sur les données de capture Wireshark. Dans le champ Filter, saisissez **ssh**, puis cliquez sur **Apply**.

d. Cliquez avec le bouton droit sur l'une des lignes **SSHv2** dans la section **Packet list** (Liste des paquets) de Wireshark et, dans la liste déroulante, sélectionnez l'option **Follow >TCP Stream**(Suivre le flux TCP).

e. Examinez la fenêtre **Follow TCP Stream** (Suivre le flux TCP) de votre session SSH. Les données ont été chiffrées et sont illisibles. Comparez les données de votre session SSH aux données de votre session Telnet.



f. Après avoir examiné votre session SSH, cliquez sur **Close** (Fermer).

g. Fermez Wireshark.

Question de réflexion

Pourquoi SSH est-il préférable à Telnet pour les connexions distantes ?