Telnet Lab

Présentation

Cet exercice Labtainer illustre l'utilisation d'un client telnet pour accéder aux ressources d'un serveur. Il s'agit d'un laboratoire simple destiné à illustrer la mise en réseau client-serveur de base et la transmission des mots de passe « en clair » par telnet sur un réseau.

Démarrer le laboratoire

Le laboratoire est lancé à partir du répertoire de travail labtainer sur votre hôte sur votre hôte ou votre machine virtuelle Linux. Exécutez la commande:

```
labtainer telnetlab
```

Les terminaux virtuels résultants comprennent : un terminal connecté à un ordinateur **client** et un terminal connecté à un **serveur**.

Tâches

1.

Déterminer l'adresse IP du serveur

- Dans le terminal du serveur, utilisez « ifconfig » pour afficher l'adresse IP du serveur.
  ```
  ifconfig
  ```

L'adresse IP du serveur suivra l'étiquette "inet adddr:" de votre interface réseau eth0.

```
ubuntu@server:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:14:00:03
          inet addr:           Bcast:              Mask:
```

Notez l'adresse du serveur :

2.

Utiliser Telnet pour accéder au serveur et afficher le contenu d'un fichier sur le serveur

- Sur le terminal client, utilisez la commande **telnet** pour accéder au serveur à l'aide de son adresse IP:
  ```
  telnet <IP>
  ```

Vous serez invité à entrer un nom d'utilisateur, puis un mot de passe. Les deux sont "ubuntu" Il y a un fichier pré-créé sur le serveur nommé "filetoview.txt".

- Vérifiez la présence de ce fichier en tapant la commande ls
- Afficher le contenu du fichier en tapant:
  ```
  cat filetoview.txt
  ```

```
ubuntu@server:~$ cat filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (telnet-server) container

# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: 7906b43a678a2b1a8446c1e9a25981c2
ubuntu@server:~$
```

- Quitter la session telnet sur le client par le biais de la commande de sortie : « exit »

```
ubuntu@server:~$ exit
logout
Connection closed by foreign host.
ubuntu@client:~$
```

3.

Afficher les mots de passe en clair.

- **Sur le serveur,** démarrez l'outil tcpdump pour afficher le trafic réseau TCP avec cette commande:
  `sudo tcpdump -i eth0 -X tcp`
- **Sur le client**, démarrez une session telnet, mais lorsque vous y êtes invité pour le mot de passe tapez : "ABC" (comme vous le savez ce mot de passe est incorrect). À mesure que vous tapez chaque lettre du mot de passe, observer les tcpdump du trafic.
- En gardant à l'esprit que chaque paquet est un "ack", voyez-vous le mot de passe ? Que remarquez-vous ?

- Sur le serveur tapez Ctrl+C pour arrêter la capture et `clear screen` pour effacer l'écran
- Recommencez la connexion telnet au serveur en tapant le bon mot de passe et affichez le fichier précédent avec la commande
  `cat filetoview.txt`
- Observez la sortie tcpdump et remarquez qu'elle est lisible en texte brut et que vous pouvez retrouver le contenu du fichier dans plusieurs paquets capturés après la saisie du mot de passe correct.

4.

Utiliser SSH pour protéger les communications avec le serveur

À partir de l'ordinateur client, utilisez la commande SSH pour accéder au serveur à l'aide de son adresse IP:

`ssh <IP>`

La première fois que vous établissez une connexion en SSH avec un serveur, SSH va vous avertir que "l'authenticité de l'hôte... ne peut pas être établie". La clé SHA256 du serveur est affichée, vous pouvez la vérifier pour être sûr qu'elle correspond bien au serveur que vous souhaitez atteindre

`ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1ZxOBv8Xc83CDp5qYU2frYQvB7Pt8`

```
ubuntu@client:~$ ssh 172.20.0.3
The authenticity of host '172.20.0.3 (172.20.0.3)' can't be established.
ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1ZxOBv8Xc83CDp5qYU2frYQvB7Pt8.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '172.20.0.3' (ECDSA) to the list of known hosts.
ubuntu@172.20.0.3's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Sun Jun 27 14:44:04 2021 from telnetlab.client.student.some_network
```

- Tapez "yes" à l'invite.
- Affichez le contenu du fichier en tapant:
  `cat filetoview.txt`
- Observez la sortie tcpdump et remarquez qu'elle n'est plus lisible en texte brut.

Arrêter le Labtainer

Lorsque le laboratoire est terminé, ou si vous souhaitez arrêter de travailler pendant un certain temps, dans le terminal qui vous a permis de le lancer, exécutez:

`stoplab telnetlab`

Vous pouvez toujours redémarrer le Labtainer et continuer votre travail. Lorsque le Labtainer est arrêté, un fichier zip est créé et copié dans un emplacement affiché par la commande « stoplab ». Results stored in directory: /home/student/labtainer_xfer/telnetlab

Une fois le laboratoire terminé, vous pouvez envoyer ce fichier zip au formateur pour correction éventuelle.