Telnet Lab

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.

**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.



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:

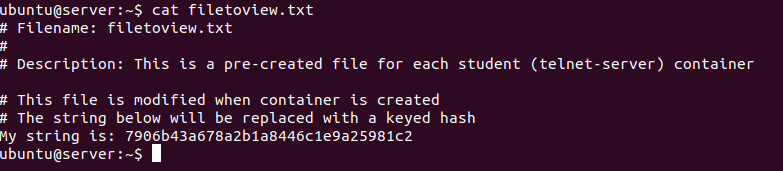
telnet <IP>

Vous serez invité à entrer un nom d'utilisateur, puis un mot de passe. Les deux sont “ubuntu”

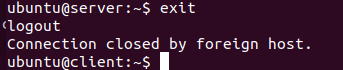
Il y a un fichier pré-créé sur le serveur nommé “filetoview.txt”.

* Vérifiez la présence de ce fichier en tapant la commande ls
* Afficher le contenu du fichier en tapant:

cat filetoview.txt



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



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.

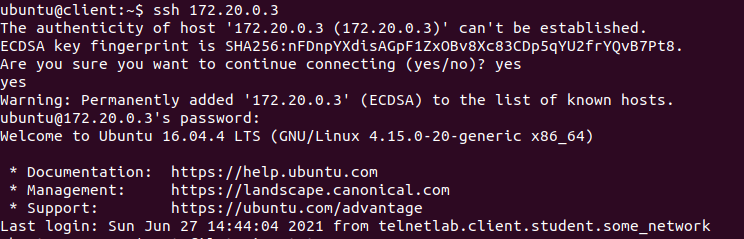
**Utiliser SSH pour protéger les communications avec le serveur**

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



* 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.