TP3

Mise en réseau et analyses

partie II

Reprise du contexte du TP3 - partie I

Le rendu doit comporter des captures régulières de ton travail, ce que tu juges nécessaire à me montrer

A. Prérequis d'accès à ce laboratoire

- Un ordinateur
- Un accès à internet
- Un hyperviseur (*je conseil VirtualBox*)
- L'image Debian CLI (format .ova)
- MobaXterm (pour ceux sous Windows)
- Un client SSH (pour ceux sous Mac ou Linux)
- Wireshark

B. Mise en place du laboratoire

🌞 *Ce laboratoire est la continuité du TP3 - partie I*

1. Démarre Debian1 et Debian2 depuis VirtualBox
2. Vérifie que Debian1 puisse communiquer avec Debian2 depuis l'adaptateur Host-Only
3. Connecte toi en ssh sur chacune des Debian depuis MobaXterm (ou autre client ssh) avec l'utilisateur que tu as précédemment créé (ton prénom)

C. Transfert sécurisé avec scp

Utilisation de scp entre Debian1 et Debian2

scp (secure copy) est un protocole de transfert de fichier sécurisé en réseau.

Première manipulation : envoi d'un fichier de Debian1 vers Debian2

❖ **Depuis Debian1** (en ssh)

1. Affiche ton répertoire de travail avec **pwd** (l'endroit où tu te trouves)
2. Créer un fichier de 10Mo avec la commande suivante : *(!!) il y 7 zéro*

   dd if=/dev/zero of=MonFichier10Mo bs=1 count=10000000
3. Vérifier avec **ls -sh** que ton fichier pèse *presque* 10 Mo dans ton répertoire

❖ **Depuis Debian2** (en ssh)

4. Affiche ton répertoire de travail avec **pwd** et vérifie qu'il soit vide

❖ **Depuis Debian1** (en ssh)

5. Utilise **scp** pour envoyer MonFichier10Mo vers Debian2 dans le répertoire de travail de ton utilisateur (/home/<user>)

❖ **Depuis Debian2** (en ssh)

6. Vérifie la présence de MonFichier10Mo dans ton répertoire de travail, et son poids
7. Créer un nouveau fichier de 10Mo

   dd if=/dev/zero of=NouveauFichier10Mo bs=1 count=10000000

8. Vérifier que NouveauFichier10Mo pèse *presque* 10Mo et se trouve dans ton répertoire de travail

Seconde manipulation : récupération d'un fichier (Debian1 depuis Debian2)

Depuis Debian1 (en ssh)

9. Utilise **scp** pour récupérer **NouveauFichier10Mo** depuis Debian2
10. Vérifie la présence de **NouveauFichier10Mo**

Supprime les fichiers créés de Debian1 et Debian2 avec la commande **rm**

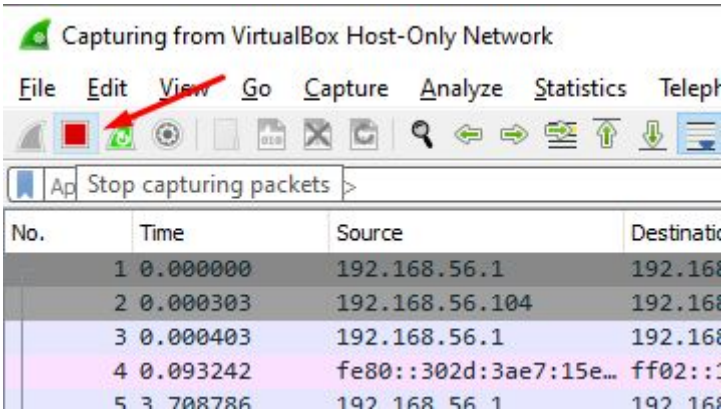
D. Analyse de la communication avec Netcat

Utilisation de Wireshark et tcpdump

Revenons à nos moutons et notre petit tchat local que nous avions créé dans le TP3 - partie I

1. Met Debian1 en écoute sur le port 1234
2. Ouvre Wireshark et démarre la capture sur la carte ***VirtualBox Host-Only Network*** en double cliquant dessus
3. Ouvre ton local terminal MobaXterm et établi la connexion **nc** sur Debian1
4. Tape : toto et ferme la connexion avec **ctrl+c**

5. Arrête la capture Wireshark en utilisant le bouton stop



6. Met en évidence le **3-way handshake** du protocol **TCP,** défini-le et commente par rapport à ta capture Wireshark
7. Met en évidence que le protocole Netcat n'est pas sécurisé en retrouvant le message que tu as envoyé (toto *normalement)*

   Astuce : il faut suivre le flux tcp sur Wireshark [sinon Google : follow TCP ...]

Faisons maintenant un tchat UDP parce que c'est tellement la grosse rigolade !

8. Renouvelle les manipulations à partir du D1, mais en .. **udp**, et met en évidence la différence avec le protocole **TCP**
9. Met en évidence que le protocole UDP n'est pas plus sécurisé que TCP