

Objectifs

Partie 1 : Analyse des services et ports ouverts sur un réseau

Partie 2 : Découvrir l'utilitaire tshark

Partie 3 : Exploiter une faiblesse dans un système.

Contexte/scénario

Vous effectuez des tests de sécurité pour un client qui pense que son serveur SSH interne est relativement sécurisé, mais vous souhaitez en confirmer la validité. Votre objectif est de tenter d'accéder à distance à ce serveur SSH dont vous ne connaissez que l'adresse IP sans avoir connaissance du login et du mot de passe et de divulguer le contenu d'un fichier se situant sur le serveur.

Ressources requises

- Poste de travail VM labtainer , Accès Internet
- Fiche Technique sur les outils de diagnostic nmap, tshark, tcpdump
- Pré-requis : labtainer **nmap-discovery**, pcapanalysis (recommandé)

NB : Si vous avez besoin d'aide sur plusieurs commandes, vous pouvez utiliser « man *commande* » pour afficher le manuel depuis un terminal de la VM Ubuntu qui contient les labtainers.

Instructions

AVERTISSEMENT : avant d'utiliser des outils de capture de trame ou de découverte de services sur un réseau, demandez l'autorisation des propriétaires du réseau. En particulier le scan d'un hôte distant n'est pas autorisé sauf s'il s'agit d'un « bac à sable », d'un « pot de miel » ou tout hôte pour lequel vous en avez l'autorisation.

Partie 1 : Analyse des services et ports ouverts sur un réseau

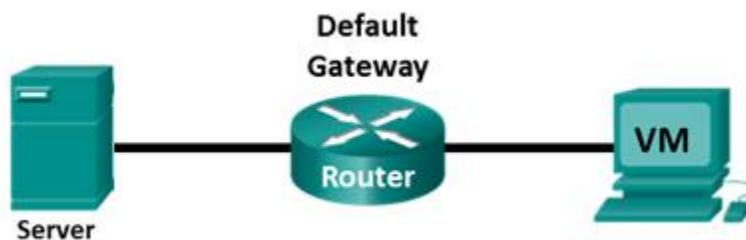
Étape 1: Tâche labtainer – lancement du lab

- Depuis le terminal de la VM labtainer, exécutez le **labtainer nmap-ssh** à l'aide la commande :

```
labtainer nmap-ssh
```

Les terminaux virtuels résultants comprennent : un terminal (shell bash) connecté à un ordinateur **client** "MyComputer" et un terminal (shell bash) connecté à un **routeur**. L'utilitaire nmap est pré-installé sur l'ordinateur **client**.

Le routeur se trouve entre les postes de travail clients de l'organisation et les serveurs.



Tâches à réaliser

En tant qu'analyste sécurité, on vous donne les informations suivantes : l'adresse IP du serveur SSH cible est 172.25.0.2 et le numéro de port SSH change fréquemment dans la plage de 2000 à 3000. Un compte vous a été attribué, « analyst » sur l'ordinateur client et sur le routeur.

Votre objectif est de réussir à découvrir un login et un mot de passe valide afin d'accéder en SSH depuis « MyComputer » sur le serveur SSH et d'accéder au contenu d'un fichier.

Astuces

- nmap est installé sur l'ordinateur « MyComputer »
- tshark et tcpdump sont installés sur le routeur
- Quels autres services réseau protégés par mot de passe sont utilisés sur le réseau ? Et pour quel utilisateur (on estime que le mot de passe sera identique pour le serveur SSH) ?

Démarche

- I. Utiliser la commande **ifconfig** pour découvrir les adresses réseau du client et du routeur
- II. Utiliser la commande **nmap** pour trouver le numéro de port utilisé par le service ssh et découvrir les autres services du réseau des serveurs.
- III. Utiliser la commande **tcpdump** pour trouver des informations sur les services réseau protégés par mot de passe utilisés sur le réseau
- IV. Utiliser la commande **tshark** pour trouver le mot de passe utilisé par un service non chiffré sur le réseau
- V. Après avoir trouvé ces informations, examinez le contenu des dossiers et ouvrez un des fichiers à partir d'une session ssh.

Notez que pour accéder en ssh à un hôte par l'intermédiaire d'un port autre que celui par défaut, il faut utiliser la commande "ssh -p <port> <host>".

Si vous avez besoin d'aide sur les commandes, vous pouvez utiliser « man nomcommande » pour afficher le manuel.

La commande `checkwork` depuis le terminal labtainers de votre VM permet de vérifier où vous en êtes dans la résolution du lab

- I. Utiliser la commande **ifconfig** pour découvrir les adresses réseau du client et du routeur
 - Quelle est l'adresse IP du client ?
 - Quelle est l'adresse du réseau des clients ?
 - Quelles sont les adresses IP du routeur ?
 - Quelle est l'adresse du réseau des serveurs?
- II. Utiliser la commande **nmap** pour trouver le numéro de port utilisé par le service ssh et découvrir les autres services du réseau des serveurs.
Rappel : la commande **nmap -A -T4 network address/prefix** permet de découvrir les hôtes d'un réseau et les services ouverts.
 - Sur le réseau des serveurs, quelle(s) adresse(s) IP et quel(s) port(s) et service(s) sont ouverts ?
 - Sur quel port le service ssh est-il configuré ?
- III. Utiliser la commande **tcpdump** pour trouver des informations sur les services réseau protégés par mot de passe
 - A partir du terminal du **routeur**, saisissez `sudo tcpdump -i eth0 -X tcp -c 50`

- A quoi sert le commutateur -X, le commutateur -c ?
- Qu'est-ce que cette capture de paquets vous permet de visualiser comme échanges ?

Partie 2 : Découvrir tshark

Dans cette partie, vous allez utiliser les pages de manuel pour en savoir plus sur tshark.

La commande **man** [*program* | *utility* | *function*] affiche les pages de manuel associées aux arguments.

1. A partir du terminal du **routeur**, saisissez **tshark -h**

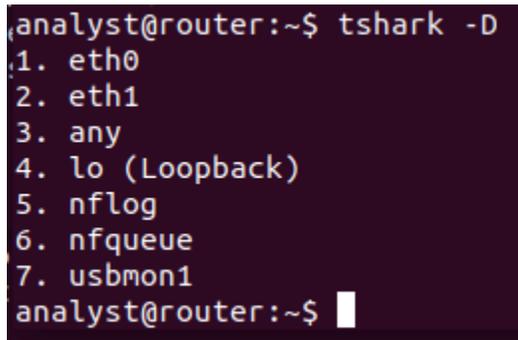
```
$ tshark -h
```

- Qu'est-ce que tshark ?
- À quoi tshark sert-il ?
- Faites défiler la page pour en savoir plus sur tshark. Saisissez « **q** » lorsque vous avez terminé.

Nous allons voir comment capturer les paquets réseaux avec tshark

2. Pour commencer on peut lister les interfaces dont tshark peut capturer le trafic avec la commande :

```
$ tshark -D
```



```
analyst@router:~$ tshark -D
1. eth0
2. eth1
3. any
4. lo (Loopback)
5. nflog
6. nfqueue
7. usbmon1
analyst@router:~$
```

On voit que le routeur peut capturer sur ses deux interfaces eth0 et eth1

- Sur quelle interface devez-vous capturer les échanges pour voir passer les trames à destination du réseau des clients ?
 - Sur quelle interface devez-vous capturer les échanges pour voir passer les trames à destination du réseau des serveurs ?
 - Dans notre cas cela a-t-il une importance si l'on veut capturer des informations de connexion entre le client et le serveur ?
3. Pour lancer la capture du trafic (limitée à 50 paquets) sur l'interface eth0 nous allons utiliser la commande :
\$ sudo tshark -i eth0 -c 50
- Qu'est-ce que cette capture vous permet de visualiser comme échanges ?

- IV. Utiliser la commande **tshark** pour trouver le mot de passe utilisé par un service non chiffré sur le réseau

```
$ sudo tshark -T fields -e telnet.data -i eth0 > capture.txt
```

Partie 3 : Exploiter une faiblesse dans un système

- V. Après avoir trouvé les informations précédentes, examinez le contenu des dossiers et ouvrez un des fichiers à partir d'une session ssh.
1. A partir des informations découvertes, terminez la mission et répondez aux questions suivantes
 - Quelle commande devez-vous utiliser pour accéder au serveur en ssh ?
 - Quelles commandes devez-vous utiliser pour examiner le contenu du dossier accessible via ssh ?
 - Quel est le nom du fichier auquel vous pouvez accéder ?
 - Quelle commande devez-vous utiliser pour examiner le contenu de ce fichier via ssh ?
 - Quelle information contient ce fichier ?
 2. Une fois terminé arrêtez le lab avec la commande `stoplab`

Crédits : d'après les laboratoires labtainer nmap-ssh