# Lab nmap-ssh



**Présentation**

Cet exercice Labtainer utilise **nmap** et les compétences exercées dans les précédents laboratoires de labtainer pour identifier et exploiter une faiblesse dans un système.

Vous effectuez des tests de sécurité ad hoc 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 et de divulguer le contenu d'un fichier particulier.

**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 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.

Clients <===> [Routeur]<===> serveurs

## Tâches

Vous savez que l'adresse IP du serveur SSH cible est 172.25.0.2 et que 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 accéder en SSH depuis "MyComputer" sur le serveur SSH avec le compte « ubuntu » (le mot de passe ne vous est pas connu) 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 par qui ?

**Démarche**

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

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

*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>".*

## 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

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