Utiliser nmap pour la découverte du réseau

Présentation

Cet exercice Labtainer explore l'utilisation de l'utilitaire nmap pour découvrir des ordinateurs et des services sur les réseaux.

Démarrage

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

```
labtainer nmap-discovery
```

Le terminal virtuel résultant comprend un shell bash connecté à un ordinateur **client**.
L'utilitaire **nmap** est préinstallé sur l'ordinateur **client**.

Taches

Votre responsable Randall veut que vous prépariez une réunion sur un projet sur lequel vous n'avez pas travaillé depuis des mois. Vous avez un fichier récapitulatif sur le serveur « friedshrimp » auquel vous avez précédemment accédé via ssh; cependant, vous ne vous souvenez pas de l'adresse IP de « friedshrimp », et vous avez également oublié quel port a été affecté au service ssh sur ce serveur. Vous savez que c'est entre 2000 et 3000.

La seule chose que vous savez avec certitude est que votre nom d'utilisateur et votre mot de passe sont tous deux « ubuntu ». Il ne vous reste qu'une seule option : utiliser la commande **nmap** pour trouver l'adresse IP et le numéro de port utilisés par le service ssh. Après avoir trouvé cette information, examinez le contenu du fichier « friedshrimp.txt » 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 que vous souhaitez arrêter de travailler, 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.