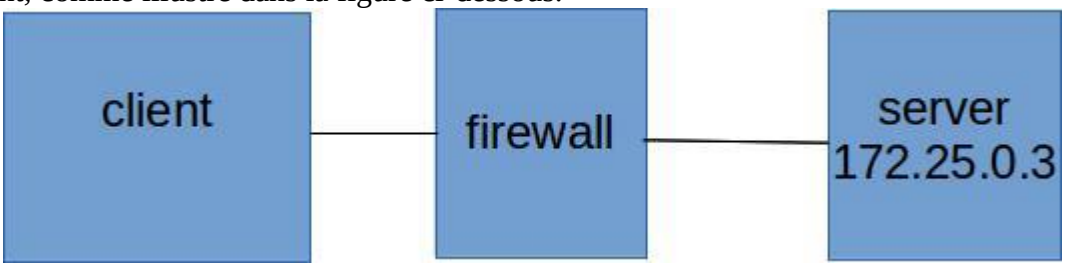
Lab Iptables

Présentation

Cet exercice Labtainer illustre l'utilisation d'iptables sur un pare-feu pour limiter l'accès réseau à un serveur à partir d'un client, comme illustré dans la figure ci-dessous.



Lorsqu'il est correctement configuré, le pare-feu n'autorisera que le trafic sélectionné du client vers le serveur.

La limitation des types de trafic réseau envoyés à un serveur peut contribuer à protéger le serveur contre les accès non autorisés.
Par exemple, si le serveur contient un service non sécurisé disponible par le biais de son interface réseau, l'exploitation de ce service est plus difficile si quelque chose bloque le trafic destiné à ce service.
Il existe une variété de techniques et de produits différents dans le but de limiter le trafic du réseau IP entre des ordinateurs.
Dans cet activité, vous limiterez le trafic IP grâce à l'utilisation d'iptables sous Linux.

Prérequis

L'étudiant est censé avoir appris séparément l'utilisation d'iptables pour bloquer sélectivement le trafic réseau. Le composant pare-feu inclut un exemple de script de configuration de pare-feu auquel vous pouvez vous référer.
La page de manuel d'iptables peut être consultée sur le terminal du pare-feu en utilisant :

```
man iptables
man iptables-extensions
```

Les étudiants doivent avoir une connaissance de base de la ligne de commande Linux ainsi que la capacité d'éditer des fichiers et d'exécuter des scripts shell simples. Une certaine expérience avec Wireshark est également présumée, par exemple à travers l'étude du laboratoire d'introduction à wireshark *wireshark-intro*.

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 iptables2
```

Les terminaux virtuels résultants comprennent : un terminal (shell bash) connecté à un ordinateur **client** "MyComputer" et un terminal (shell bash) connecté à un Firewall.

Client <===> [Firewall]<===> serveur (nom server, adresse IP 172.25.0.3)

Tâches

1 Exploration

L'utilitaire Wireshark est installé sur le pare-feu. Utilisez-le pour afficher le trafic réseau à travers le pare-feu et pour déboguez vos règles de pare-feu. Démarrez-le à partir du terminal du pare-feu :

```
wireshark &
```

Sélectionnez ensuite l'interface eth0.

Sur le terminal client, utilisez l'utilitaire nmap pour répertorier (certains des) ports ouverts sur le serveur :

```
nmap server
```
ou
```
nmap 172.25.0.3
```

Utilisez `wget` pour confirmer que le serveur répond aux requêtes HTTP , utilisez ctrl C pour quitter une fois que vous obtenez une réponse du serveur.

```
wget server &
```

Vérifiez qu'un service ssh est proposé sur le serveur - vous n'avez pas besoin de vous connecter lorsque vous y êtes invité, répondez « no » ou utilisez ctrl C pour quitter une fois que vous obtenez une réponse du serveur.

```
ssh server
```

Vérifiez qu'un service telnet est proposé sur le serveur - vous n'avez pas besoin de vous connecter lorsque vous y êtes invité, utilisez également ctrl C pour quitter une fois que vous obtenez une réponse du serveur.

```
telnet server
```

Observez le trafic dans wireshark, notez les adresses IP sources et les ports de destination utilisés par le client lors de la connexion au serveur.

2. Utiliser iptables pour limiter le trafic

L'utilitaire iptables est installé sur le composant « firewall ». Utilisez-le pour empêcher le pare-feu de transférer tout trafic vers le serveur autre que SSH et HTTP.

Vous pouvez vous référer à l'exemple de script de pare-feu qui se trouve sur le composant de pare-feu dans le répertoire *home* et l'expérimenter.

Consultez le contenu du script exemple `example_fw.sh` pour comprendre ce qu'il fait.

Notez que la dernière ligne du script `example fw.sh` demande à iptables d'enregistrer les paquets bloqués dans les logs d'iptables `/var/log/iptables.log`.

Pour exécuter le script `example_fw.sh`, utilisez :

```
sudo ./example_fw.sh
```

Vous pouvez visualiser les logs enregistrés à partir de l'un des onglets du terminal du pare-feu via :

```
tail -f /var/log/iptables.log
```

Après avoir modifié votre configuration iptables, utilisez les applications sur le client pour démontrer que le pare-feu n'autorise que le trafic souhaité. Surveillez le trafic dans wireshark pour voir que la négociation TCP échoue lorsque vous essayez de vous connecter aux ports filtrés. Utilisez nmap pour confirmer la bonne configuration :

```
nmap server
```

NB : Pensez à mettre vos commandes iptables dans un script, il est ainsi plus facile de tester et de reconfigurer iptables si vous redémarrez le laboratoire.

3. Ouvrir un nouveau service sur un port

L'ordinateur client comprend un programme `wizbang` que vous devez maintenant autoriser à envoyer du trafic vers le serveur. Exécutez le programme à partir du client et observez le port qu'il tente d'utiliser dans wireshark :

```
./wizbang
```

Ensuite, modifiez votre iptables pour autoriser ce service. Après avoir ajusté vos règles iptables, confirmez que vous pouvez exécuter le programme wizbang avec succès.
Utilisez à nouveau nmap pour confirmer la bonne configuration

```
nmap server
```

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.