Nicolas Trugeon

TP Sécurité : Pare-feu

Objectifs

Être capable de configurer un pare-feu personnel et d'entreprise simple.

Comprendre les mécanismes de sécurité réseau.

Durée

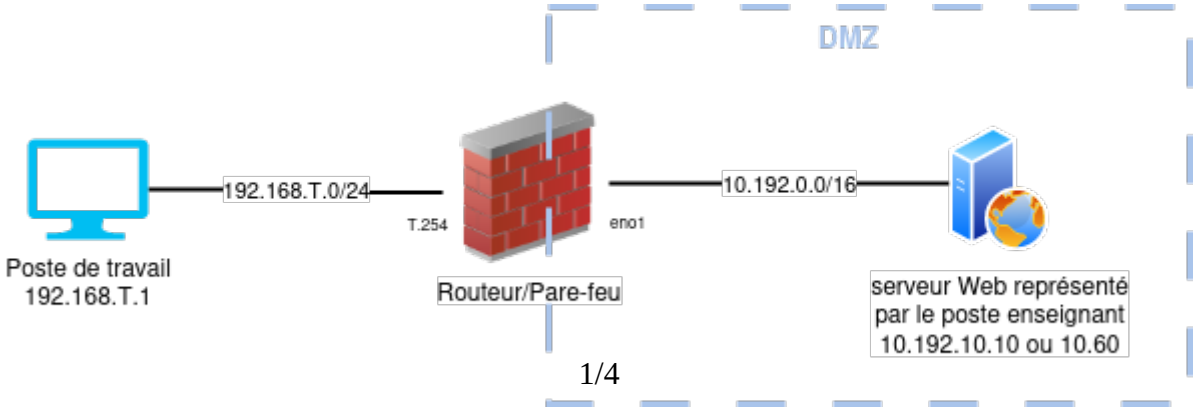
3h

Préambule

Enregistrez l'énoncé tant qu'il est encore temps. Lisez cet énoncé soigneusement et entièrement. Au cours de ce TP vous allez mettre en place un routeur statique et l'équiper d'un pare-feu.

- Vous capturerez les trames qui transitent par le routeur en lançant 2 instances de wireshark, une pour chaque interface.
- **Vous ne devez pas exécuter directement la commande iptables dans un terminal ! ! !**
- Vous commenterez vos scripts iptables. N'hésitez pas à utiliser iptables -S ou -L pour lister vos règles.
- Au cas où, la passerelle de la salle est 10.192.0.255 et vous pouvez retrouver une adresse ip facilement avec la commande sudo dhclient -v eno1
- L'enseignant vous attribut un numéro de table T par binôme.

Le plus important dans ce TP est de définir une procédure de tests pour chaque exercice. Des tests inappropriés ou insuffisants peuvent vous faire croire que vous avez obtenu le résultat attendu alors qu'il n'en est rien.



Configuration préalable

Vous êtes sous Ubuntu. Pour utiliser les commandes en tant qu'administrateur, vous devez préfixer vos commandes de sudo.

- Arrêtez NetworkManager par les commandes systemctl disable NetworkManager.service puis systemctl stop NetworkManager.service
- Arrêtez également docker par les commandes systemctl disable docker.service puis systemctl stop docker.service
- Supprimer l'interface docker0 par la commande ip link delete docker0

Interfaces

Configurez le routeur et le poste de travail comme sur le schéma. L'interface eno1 du routeur ne change pas d'adresse.

Petit rappel, pour modifier une adresse IP dans cette salle, vous devez d'abord vider la configuration puis adresser l'interface.

Par exemple :

```
ip address flush enp1s0
ifconfig enp1s0 192.168.20.4/24
```

Pensez à activer le routage sur le routeur :

```
sysctl -w net.ipv4.ip_forward=1
```

Et à définir votre routeur comme passerelle par défaut sur votre poste. (route add …)

Script de remise à zéro du pare-feu

Vous trouverez sur moodle, le script raz.sh permettant d'enlever toutes les règles du pare-feu et de mettre les politiques par défaut à ACCEPT. Exécutez ce script sur vos deux machines afin d'enlever tout blocage.

Vous pourrez exécuter à nouveau ce script pour retrouver une configuration propre.

Validation

Les commandes suivantes doivent maintenant fonctionner :

À partir du routeur :

ping -c 3 192.168.T .1 (ping vers le poste de travail)

ping -c 3 10.192.10.10 ou 10.60 (ping vers la DMZ : poste enseignant de la salle)

À partir du poste de travail :

ping -c 3 192.168.T .254 (ping vers le routeur)

Par contre le ping vers la DMZ ne fonctionne pas. Expliquez pourquoi et corrigez le problème.

Une fois le problème résolu, vérifiez que vous pouvez joindre la DMZ avec les protocoles icmp, ssh et http à partir de votre routeur et du poste de travail (pour http, il faudra ajouter une exception dans le navigateur dans la partie proxy en ajoutant le réseau 10.192.0.0/16)

ICMP

Nous voulons que le routeur accepte uniquement les trames du protocole icmp.

Vous devez créer un nouveau script appelé routeur.sh permettant de répondre à cette problématique.

1. Définissez les stratégies par défaut des chaînes INPUT, OUTPUT et FORWARD à DROP.
2. Vérifiez qu'aucun des protocoles déjà testés ne fonctionne.
3. Écrivez les règles qui autorisent le protocole icmp. Testez depuis le poste de travail et depuis la DMZ.

SSH

Nous voulons pouvoir administrer le routeur/pare-feu depuis le poste de travail uniquement. Complétez le script routeur.sh pour autoriser le protocole ssh sur le pare-feu.

1. Écrivez les règles de pare-feu permettant d'autoriser le protocole ssh.
2. Testez le bon fonctionnement de ssh depuis le poste de travail mais cela ne doit pas fonctionner depuis la DMZ.

Accès à la DMZ

Le poste de travail doit pouvoir accéder au serveur web de la DMZ. Le poste enseignant possède un serveur apache qui ne fonctionne qu'en http. Cependant le service https ouvrira bientôt... Pour cela, votre poste de travail émettra aussi des requêtes qui se font en protocole UDP sur le port 53 d'un serveur DNS.

1. Écrivez les règles adéquates en complétant le script routeur.sh.

2. Vérifiez que le poste de travail peut bien accéder au serveur web de la DMZ.

Administration de la DMZ

Le poste de travail doit pouvoir également modifier des fichiers sur le serveur web de la DMZ à l'aide du protocole ssh.

1. Écrivez les règles adéquates en complétant le script routeur.sh.
2. Vérifiez que le poste de travail peut bien accéder à la DMZ à travers le protocole ssh.

Optimisation

Afin d'éviter la surcharge de la DMZ, limitez à 5 le nombre de connexions sur le serveur web passant par le pare-feu en utilisant le module connlimit.

1. Ajoutez les règles adéquates dans le script
2. Testez en ouvrant plusieurs onglets

Journalisation

Nous voulons enregistrer dans les fichiers de log (/var/log) toutes les traces de connexions ssh faites sur le pare-feu.

1. Ajoutez ces règles dans le script
2. Vérifiez que les accès ssh sont bien visibles.

Accès à internet pour le poste de travail

Le poste de travail n'a pas accès à internet, car le réseau 192.168.T.0/24 n'est pas connu des équipements réseaux de l'université. La solution pour palier à ce problème est de « cacher » ce réseau grâce au NAT.

Ajoutez une règle au pare-feu pour donner accès au net à ce réseau : `iptables -t nat …`