MISE EN PLACE D'UN FIREWALL

Le but de ce travail est de mettre en place un firewall en utilisant la commande `iptables`. L'ensemble du travail devra être effectué avec les droits de l'administrateur système.

1. Configuration par défaut

Attribuez l'adresse IP `192.168.1.1` à la machine `fedora-1` et `192.168.1.2` à la machine `fedora-2`. Sur la machine `fedora-1` développez un premier script qui vide entièrement le contenu des tables `filter`, `nat` et `mangle`. Puis placez-y une politique par défaut rejetant tous les paquets de type `INPUT`, `OUTPUT` ou `FORWARD`.

2. Configuration de l'interface loopback

Exécutez `ping 127.0.0.1`. Que se passe-t-il ?

Complétez votre script de façon à ce que toute connexion sur l'interface locale (et uniquement elle) fonctionne. **Attention !** : toute adresse de la forme `127.0.0.0/8` est attachée à l'interface locale.

Exécutez `ping` *votre adresse ip*. Que se passe-t-il ?

Modifiez votre script de façon à ce que toute connexion sur votre adresse IP initiée par votre machine soit acceptée (un ping extérieur vers votre machine ne doit pas fonctionner,vérifiez-le à partir de la machine `fedora-2`).

3. Filtrage du ping

Ecrire un ensemble de règles de façon à ce que votre machine refuse uniquement de répondre aux requêtes extéreures de type ping. Toute autre requête doit être acceptée, par exemple une requête Ssh. Testez ceci à partir de la machine `fedora-2`.

4. Un premier problème

Pour les questions suivantes vous devez désactiver le firewall par défaut de `fedora-2`. Pour celà, exécutez :
`/etc/rc.d/init.d/iptables stop`
Repartez sur `fedora-1` de la configuration où seules les connexions locales sont acceptées. Lancez un serveur Web sur `fedora-2` (`/etc/rc.d/init.d/httpd start`) et configurez le firewall `fedora-1` afin qu'elle puisse uniquement se connecter sur le serveur Web de `fedora-2`.

Lancez un serveur Web sur `fedora-1`. Sur `fedora-2` lancez `nmap` *adresse ip de A*. Que constatez-vous ?

Arrêtez le serveur web de `fedora-2`. Relancez sur `fedora-2` `nmap` avec l'option `-g 80` (cf. man de `nmap`). Que constatez-vous ? Explication ?

Malgré le firewall en place sur `fedora-1`, vous avez pu découvrir l'ensemble des ports en écoute sur cette machine. Pour vous connecter sur le serveur Web de `fedora-1`, vous pouvez utiliser `nc` (netcat) qui est l'équivalent de la commande `cat` pour le réseau. La commande `cat` recopie sur la sortie standard ce que l'on tape sur l'entrée standard. La commande `nc` envoie sur le réseau ce que vous tapez sur l'entrée standard. Utilisez `nc` sur la machine `fedora-2` pour afficher le code HTML de la page de garde du serveur Web de `fedora-1`.

5. Firewall stateless vs Firewall statefull

Utilisez judicieusement l'option `--syn` de `iptables` pour que `fedora-1` refuse en entrée tout paquet initiant une connexion vers le port 80 (par rapport à l'état de votre firewall, vous n'avez aucune règle à rajouter). Vérifiez alors que `nc` ne vous permet plus de récupérer la page Web de `fedora-1` et que `nmap` ne vous renvoie pas les ports ouverts de `fedora-1`.
Pour finir de vérifier votre configuration relancer le serveur Web sur `fedora-2` et assurez-vous que vous pouvez toujours vous y connecter à partir de `fedora-1`.

Date: Janvier 2010.

La machine `fedora-1` est-elle définitivement protégée ? Malheureusement non. Lancez `ethereal` sur `fedora-2` puis exécutez le programme `ack2` qui se trouve dans le répertoire `/root`. Ce programme prend en paramètre une adresse IP source, une adresse IP destination et un numéro de port. Il construit alors une trame tcp de type `ACK` avec ces données et l'envoie. Utilisez le pour envoyer une trame de `fedora2` vers `fedora1` en utilisant pour numéro de port 80 puis 33. Qu'observez-vous ? Déduisez-en une attaque permettant d'éventuellement déterminer les ports ouverts sur `fedora-1` malgré le firewall.

Le firewall que vous avez développé est un firewall stateless, c'est à dire qu'il accepte des paquets tcp hors contexte (paquet tcp n'appartenant à aucune vraie connexion tcp initiée par le three way handshake).

Utilisez le module `state` de `iptables` de façon à ce que votre firewall n'accepte en entrée à destination du port 80 que des trames appartenant à une connexion déjà existante. Vérifiez alors que votre programme qui génère une trame ack ne vous permet plus d'obtenir des informations sur les ports ouverts de `fedora-1`.

6. Prerouting et Postrouting

Configurez une deuxième interface réseau sur `fedora2` avec pour adresse IP `10.1.1.1`. Lancez sur `fedora2` un serveur Web en écoute uniquement sur l'interface `10.1.1.1`. Modifiez pour cela le fichier `/etc/httpd/conf/httpd.conf` et exécutez `/etc/rc.d/init.d/httpd start`.

Désactivez sur `fedora1` votre firewall. Sur `fedora2`, mettez en place un firewall qui refuse toute connexion par défaut et qui utilise la fonction `PREROUTING` de la table `nat` pour rediriger tout paquet issu de `fedora1` à destination du port 8080 de `192.168.1.2` vers le port `80` de `10.1.1.1`. Ajoutez alors les deux règles manquantes qui vous permettront, en émettant une requête vers `@192.168.1.2:8080` à partir de `fedora1`, de vous connecter sur le serveur Web en écoute sur la deuxième interface de `fedora2` .