Formation Iptables : Correction TP

Table des matières

Email : ssales@alio.fr

1. Opérations sur une seule chaîne et sur la table filter:

Créer les règles suivantes : (vous noterez sur cette feuille chacune des règles demandées, ainsi que le test de la règle, à savoir un copié/collé du term, et/ou du résultat d'un sniff(ethereal,ngrep etc)

- interdire tout paquet entrant
- effacer la règle

iptables -A INPUT -j DROP
iptables -D INPUT 1

✔ paramètre protocole

- interdire le protocole icmp entrant
- effacer la règle

iptables -A INPUT -p icmp -j DROP

✔ paramètre source

- interdire le protocole icmp provenant de localhost
- effacer la règle

iptables -A INPUT -p icmp -s localhost -j DROP

✔ chaîne OUTPUT paramètre destination

- interdire tout paquet à destination de localhost
- effacer la règle

iptables -A OUTPUT -d localhost -j DROP

✔ paramètre inversion

- interdire un paquet s'il ne provient pas de localhost
- effacer la règle

iptables -A INPUT -s ! localhost -j DROP

✔ paramètre interface d'entrée

- interdire tout paquet entrant par *eth0*
- effacer la règle

iptables -A INPUT -i eth0 -j DROP

- interdire un paquet s'il provient de *lo* (à ne surtout jamais faire sur une machine si l'on ne sait pas EXACTEMENT ce que l'on fait)

Email : ssales@alio.fr

- effacer la règle

iptables -A INPUT -i lo -j DROP

✔ paramètre interface de sortie

- interdire tout paquet sortant par eth0
- effacer la règle

iptables -A OUTPUT -o eth0 -j DROP

✔ paramètre destination port

- interdire tout paquet à destination du port ftp
- effacer la règle

iptables -A INPUT -p tcp --dport 21 -j DROP

✔ paramètre source port

- interdire tout paquet sortant par eth0 dont le numéro de port source est inférieur à 1025

iptables -A OUTPUT -o eth0 -p tcp --sport :1024 -j DROP
iptables -A OUTPUT -o eth0 -p udp --sport :1024 -j DROP

- tester une connexion ftp
- effacer la règle et retester une connexion ftp

✔ paramètre flag TCP

- interdire toute tentative d'initialisation de connexion TCP provenant de eth0
- effacer la règle

iptables -A INPUT -i eth0 -p tcp --syn -j DROP

✔ paramètre flag icmp

- interdire tout paquet entrant correspondant à un ping
- effacer la règle

iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

- interdire toute réponse à un ping
- effacer la règle

iptables -A OUTPUT -p icmp --icmp-type echo-reply -j DROP

✔ paramètre extension:

- extension mac

Email : ssales@alio.fr

- interdire tout paquet entrant par eth0 dont l'adresse mac n'est pas celle du voisin
- effacer la règle

iptables -A INPUT -i eth0 -m mac --mac-source ! 00:50:FC:23:2D:D7 -j DROP

- extension limit
- positionner la police par défaut à *DROP* pour la chaîne *INPUT*

iptables -P INPUT DROP

- écrire une règle qui laisse passer 5 tentatives de connexion TCP puis qui n'en laisse passer plus que 2 par minute

iptables -A INPUT -p tcp --syn -m limit --limit 2/minute --limit-burst 5 -j ACCEPT

- faire de même avec les pings

iptables -A INPUT -p icmp --icmp-type ping -m limit --limit 2/minute --limit-burst 5 -j ACCEPT

- combien de temps(sans tentative de connexion ou d'echo-request)faudra t'il pour qu'on puisse à nouveau avoir 5 des ces paquets qui puissent passer à la suite ?

3 minutes

- effacer la règle

✔ le suivi de connexion(ip_conntrack)

- positionnez les règles par défaut à DROP pour les chaînes *INPUT*, *OUTPUT, FORWARD*

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

- autoriser tout paquet relatif à une connexion déjà établi ou en rapport avec une connexion déjà établi en entrée

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

- interdire tout paquet relatif à une connexion de type *INVALID*

iptables -A INPUT -m state --state INVALID -j DROP
iptables -A OUTPUT -m state --state INVALID -j DROP
iptables -A FORWARD -m state --state INVALID -j DROP

- autoriser tout paquet créant une nouvelle connexion en sortie à destination du port 80

iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT

- que faut il modifier ici pour que l'on puisse naviguer sur le net ?

iptables -A OUTPUT -p tcp --dport 53 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

Email : ssales@alio.fr

iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

- effacer la règle

2. Opérations sur plusieurs chaînes et sur la table filter:

- ✔ création d'une nouvelle chaîne
  - créer une nouvelle chaîne qui log les paquets entrants en ajoutant le préfixe [INPUT DROP] et qui le drop

iptables -N LOG_DROP
iptables -A LOG_DROP -j LOG --log-prefix «[INPUT DROP]»
iptables -A LOG_DROP -j DROP

- renvoyer sur cette nouvelle chaîne tout paquet engendrant une nouvelle connexion en entrée

iptables -A INPUT -m state –state NEW -j LOG_DROP

3. Opérations sur plusieurs chaires et sur plusieurs tables :

[Pour cette partie nous travaillerons sur des machines ayant au minimum 2 interfaces réseau]

- ✔ modification de champ *TCP*/IP ; table nat ; chaînes *PREROUTING*, *POSTROUTING* ; cibles *SNAT*, *DNAT*, *MASQUERADE*
  - positionnez les règles par défaut à DROP pour les chaînes *INPUT*, *OUTPUT, FORWARD*

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

- créer une règle qui modifie tout paquet qui arrive via l'interface eth1 à destination du port 2222 afin que ce paquet ai dans son champ *IP DST* l'adresse 192.168.0.1 et dans son champ *TCP DPORT* 22

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 2222 -j DNAT --to-destination 192.168.0.1:22

- que se passe t il si on tente une connexion sur eth1 sur le port 2222 ?

Rien car les paquets sont dropés dans la chaine FORWARD

- que faut il faire pour que la translation fonctionne effectivement ? (dans un sens comme dans l'autre)
- pour vous aider mettez ces règles dans un script se terminant par une règle qui log et drop tout et ensuite regarder attentivement les logs

Email : ssales@alio.fr

iptables -A FORWARD -s 192.168.0.1 -j ACCEPT
iptables -A FORWARD -d 192.168.0.1 -j ACCEPT

- effacer ces règles(sauf les polices par défaut)
- créer une règle qui altère le champ *IP SRC* de tout paquet sortant via l'interface eth1, en remplaçant la valeur de ce champ par l'adresse IP de cette interface(eth1)

iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to-source 62.212.36.222
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

- autoriser tout trafic provenant de eth0 à être forwardé par notre machine

iptables -A FORWARD -i eth0 -j ACCEPT

- autoriser tout trafic de statuts *ESTABLISHED,RELATED* à être forwardé par notre machine

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

4.SCRIPT

Le but sera ici de se placer dans un cas concret, et de répondre au mieux aux besoins de filtrage, d'accès aux services et de qualité de service .
Le cas concret :

4.1.partie 1

Nous considérerons qu' iptables est installé sur la machine servant de routeur/firewall et nous allons donc nous attacher à écrire le script pour cette machine.
Les machines, le routeur et le serveur placé dans la DMZ, doivent être protégées au mieux.
Le routeur a 3 interfaces réseau :

eth0(192.168.0.254) relié à la DMZ
eth1(192.168.1.254) relié au LAN
ppp0(62.212.36.222) relié à internet

La machine doit pouvoir être joignable via SSH depuis le LAN, et depuis Internet.
Les machines du LAN doivent pouvoir aller sur Internet(HTTP et FTP).
Les machines du LAN doivent pouvoir pinger une machine sur Internet.
Sur la DMZ, la machine 192.168.0.1 héberge le site web de l'entreprise, un relay mail et un serveur imap-ssl qui doivent être joignable, depuis le LAN, et depuis Internet. Cette machine doit aussi être joignable par SSH depuis le LAN et depuis Internet.
La machine est une debian et est maintenu à jour via apt, aussi la machine devra pour pouvoir aller télécharger via FTP et HTTP les mises à jours sur par exemple ftp.fr.debian.org.
(voir script)

Email : ssales@alio.fr

4.2.Partie 2

On veut mettre en place un proxy transparent sur un serveur dédié (192.168.0.2) situé dans la DMZ, que faudrait il changer dans notre script ?
(voir script)

Email : ssales@alio.fr