TP Netfilter

‡Corrigé‡

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.

1 Exercice 1 : ping

Le poste de travail ne peut que "pinguer" les machines du réseau. Il peut être "pingué" lui-même.

1. Effacez toutes les règles qui pourraient exister ‡
   iptables -F (n'efface que les règles des tables standard)‡
2. Définissez vos stratégies par défaut (vous les conserverez pendant tout le TP) ‡
   iptables -P INPUT DROP
   iptables -P OUTPUT DROP
   iptables -P FORWARD DROP‡
3. Écrivez les règles correspondantes ‡
   iptables -A INPUT -p icmp –icmp-type echo-request -j ACCEPT
   iptables -A OUTPUT -p icmp -j ACCEPT‡
4. Testez

2 Exercice 2 : surf

Le poste de travail peut seulement surfer sur le web, il ne peut pas pinguer ni être pingué

1. Effacez les règles précédentes ‡
   iptables -F
   conserver les stratégies à "DROP"‡
2. Écrivez les règles correspondantes ‡
   iptables -A OUTPUT -p tcp –dport 80 -m state –state NEW,ESTABLISHED -j ACCEPT
   iptables -A OUTPUT -p tcp –dport 443 -m state –state NEW,ESTABLISHED -j ACCEPT
   iptables -A OUTPUT -p udp –dport 53 -m state –state NEW -j ACCEPT
   iptables -A INPUT -m state –state ESTABLISHED -j ACCEPT‡
3. Testez

3 Exercice 3 : serveur

Maintenant le poste de travail devient serveur web exclusivement. Il ne peut rien faire d'autre.

1. Effacez les règles précédentes ‡
   iptables -F
   puis remettre les stratégies à "ACCEPT"‡
2. Vérifiez que l'on peut se connecter sur le poste de travail par ssh
3. Vérifiez que l'on peut se connecter sur le poste de travail sur un serveur web (au besoin installez-le)
4. Ecrivez les règles correspondantes ‡
   iptables -P INPUT DROP
   iptables -P OUTPUT DROP
   iptables -P FORWARD DROP
   iptables -A INPUT -p tcp –dport 80 -m state –state NEW,ESTABLISHED -j ACCEPT
   iptables -A INPUT -p tcp –dport 443 -m state –state NEW,ESTABLISHED -j ACCEPT
   iptables -A OUTPUT -m state –state ESTABLISHED -j ACCEPT‡

5. Testez

4 Exercice 4 : prévenir le "Deny of Service"

Le DoS est une attaque qui consiste à noyer une machine sous une avalanche de paquets dans le but de la mettre à genoux. Une parade est de limiter certains trafic. Essayez de limiter les "ping". ‡
iptables -F
puis remettre les stratégies à "ACCEPT"
iptables -A INPUT -p icmp –icmp-type echo-request -m hashlimit –hashlimit 3/m –hashlimit-mode dstport –hashlimit-name pings -j ACCEPT
iptables -A INPUT -p icmp –icmp-type echo-request -J DROP
Le fonctionnement surprend au début car 5 paquets sont acceptés (valeur par défaut de "–hashlimit-burst" puis un paquet est accepté chaque fois qu'on descend en dessous de "–hashlimit" soit 3 par minutes dans notre cas)‡

5 Exercice 5 : "logger"

Enregistrez dans le journal les pings reçus (le journal est dans /var/log/message, vous le visualisez facilement avec tail ou mieux tail -f). Vous pouvez limiter la fréquence. ‡
iptables -A INPUT -p icmp -m limit –limit 1/minute -j LOG –log-prefix "Bonjour les cocos"
Ici on utilise le module "limit" moins souple et plus ancien que "hashlimit"
le "–log-prefix" permet de trouver plus facilement les lignes dans le journal‡