Prérequis Iptables

Prérequis concernant l'atelier iptables

Dans la grande majorité des cas, il n'est pas nécessaire d'installer **iptables**, c'est installé par défaut notamment sur les distributions récentes. Il faut quand même le vérifier sur les distributions moins grand public ou moins standards. Si ce n'est pas le cas, il faut **l'installer.** Pour savoir si **iptables** est installé, faire **sudo iptables –L** (les règles par défaut s'affichent si iptables est installé).

Attention, la commande iptables fonctionne en mode administrateur.

Il est indispensable d'installer **certains outils réseau** dont on aura besoin pour les tests. On utilisera principalement **nmap** et éventuellement **Wireshark**.

Il n'est pas nécessaire de **charger les modules ni d'activer le mode routeur et certains paquets** pour l'instant, on le fera selon nos besoins avec les exercices pratiques.

Pour résumer, il faut que les commandes de la partie 1 ou 2 soient fonctionnelles (notamment les quatre premières lignes), le reste est optionnel et sera abordé lors d'exercices pratiques.

1) L'installation sur Debian/Ubuntu (.deb)

sudo apt-get update

sudo apt-get install iptables

sudo apt-get install nmap

sudo apt-get install wireshark

sudo apt-get install tcpdump

sudo apt-get install traceroute

sudo apt-get install lsof

sudo apt-get install fuser

2) L'installation sur CentOS (.rpm)

yum install iptables

yum install nmap

yum install wireshark

yum install wireshark-gnome

yum install tcpdump

yum install traceroute

yum install lsof

yum install psmisc

3) Le chargement des modules si nécessaire

/sbin/modprobe

 # modprobe ip_tables

 # modprobe iptable_filter

 # modprobe iptable_nat

 # modprobe ip_nat_ftp

 # modprobe ip_nat_irc

 # modprobe iptable_mangle

 # modprobe ip_conntrack

 # modprobe ip_conntrack_ftp

 # modprobe ip_conntrack_irc

 # modprobe ipt_LOG

 # modprobe ipt_limit

 # modprobe ipt_tos

 # modprobe ipt_ttl

 # modprobe ipt_length

 # modprobe ipt_TCPMSS

 # modprobe ipt_state

 # modprobe ipt_owner

 # modprobe ipt_REJECT

 # modprobe ipt_MASQUERADE

 # modprobe ipt_recent

 # modprobe ipt_multiport

 # modprobe xt_connlimit

4) L'activation du mode routeur (prise en compte du NAT).
echo 1 > /proc/sys/net/ipv4/ip_forward

5) L'activation ou la désactivation de certains types de paquets.
echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_all
echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo 0 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

#echo "1" > /proc/sys/net/ipv4/conf/all/rp_filter
#echo "1" > /proc/sys/net/ipv4/conf/all/proxy_arp
#echo "1" > /proc/sys/net/ipv4/ip_dynaddr
 # echo 1 > /proc/sys/net/ipv4/ip_forward