TP 5 Compte rendu Fabien Mauhourat

Inventaire des services :

Commandes :
ss -ntplu : tcp/udp/listen/port au format numérique

Debian :

Port	Protocole	Écoute	Destination
22	TCP	*	172.18.10.0/24
514	TCP et UDP	*	-
80	TCP	*	172.18.10.0/24
161	UDP	*	-
53	TCP (AXFR) et UDP	*	172.18.10.10, 172.18.10.12, 8.8.8.8
445 et 139	TCP	*	-

Centos :

Port	Protocole	Écoute	Destination
22	TCP	*	-
514	TCP et UDP	-	172.18.10.10
80	TCP	*	172.18.10.0/24
161	UDP	*	172.18.10.0/24
53	TCP (AXFR) et UDP	*	172.18.10.10, 172.18.10.12, 8.8.8.8
445 et 139	TCP	-	172.18.10.10

Alpine :

Port	Protocole	Écoute	Destination
22	TCP	*	-
514	TCP et UDP	-	172.18.10.10
80	TCP	*	172.18.10.0/24

161	UDP	*	-
53	TCP et UDP	-	172.18.10.10, 172.18.10.12
445 et 139	TCP	-	172.18.10.10

Sécurisation des machines :

Configuration Globale :

```
# Effacer les règles
iptables -F
iptables -X

# Politique du traffic
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD ACCEPT

# Loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# ICMP
iptables -A INPUT -p icmp -j ACCEPT
iptables -A OUTPUT -p icmp -j ACCEPT

# Connexion établie
iptables -t filter -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

# SSH sauf debian
iptables -A INPUT -p tcp -i eth0 -s 172.18.10.10 --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp -o eth0 -d 172.18.10.10 --sport 22 -j ACCEPT

# HTTP
iptables -A INPUT -p tcp -i eth0 -s 172.18.10.0/24 --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -o eth0 -d 172.18.10.0/24 --sport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -o eth0 -d 172.18.10.0/24 --dport 80 -j ACCEPT

# SNMP sauf centos
iptables -A INPUT -p udp -i eth0 -s 172.18.10.12 --dport 161 -j ACCEPT
iptables -A OUTPUT -p udp -o eth0 -d 172.18.10.12 --sport 161 -j ACCEPT
```

Samba sauf debian
iptables -A OUTPUT -p tcp -o eth0 -d 172.18.10.10 --dport 445 -j ACCEPT

RSYSLOG sauf debian
iptables -A OUTPUT -p tcp -o eth0 -d 172.18.10.10 --dport 514 -j ACCEPT

DNS
iptables -A OUTPUT -p udp -o eth0 -d 172.18.10.0/24 --dport 53 -j ACCEPT

Debian :

SSH
iptables -A OUTPUT -p tcp -o eth0 -d 172.18.10.0/24 --dport 22 -j ACCEPT

Samba
iptables -A INPUT -p tcp -i eth0 -s 172.18.10.0/24 --dport 445 -j ACCEPT
iptables -A OUTPUT -p tcp -o eth0 -d 172.18.10.0/24 --sport 445 -j ACCEPT

RSYSLOG
iptables -A INPUT -p tcp -i eth0 -s 172.18.10.0/24 --dport 514 -j ACCEPT

DNS
iptables -A INPUT -p udp -i eth0 --dport 53 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 --dport 53 -j ACCEPT
iptables -A OUTPUT -p udp -o eth0 --sport 53 -j ACCEPT
iptables -A OUTPUT -p tcp -o eth0 --sport 53 -j ACCEPT
iptables -A OUTPUT -p udp -o eth0 -d 8.8.8.8 --dport 53 -j ACCEPT

Centos :

SNMP
iptables -A OUTPUT -p udp -o eth0 -d 172.18.10.0/24 --dport 161 -j ACCEPT

DNS
iptables -A INPUT -p udp -i eth0 --dport 53 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 --dport 53 -j ACCEPT
iptables -A OUTPUT -p udp -o eth0 --sport 53 -j ACCEPT
iptables -A OUTPUT -p tcp -o eth0 --sport 53 -j ACCEPT
iptables -A OUTPUT -p udp -o eth0 -d 8.8.8.8 --dport 53 -j ACCEPT

Vérification des statistiques :
iptables -L -v -n

Iptables persistent :
apt install iptables-persistent
iptables-save > /etc/iptables/rules.v4

Forward de port :

Sur centos :
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 172.18.10.10:80
iptables -t nat -A POSTROUTING -p tcp -d 172.18.10.10 --dport 80 -j SNAT --to-source 172.18.10.12

Sur alpine :
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 172.18.10.10:80
iptables -t nat -A POSTROUTING -p tcp -d 172.18.10.10 --dport 80 -j SNAT --to-source 172.18.10.11

Vérification :
curl -I 172.18.10.12:80
HTTP/1.1 200 OK
Date: Wed, 06 Nov 2019 10:36:38 GMT
Server: Apache/2.4.38 (Debian)