Aller au contenu

uho

Iptables pour privdb1 et privdb2 :

```
iptables -F #suppression des tables
iptables -t nat -F  #suppression de la tables nat
iptables -P INPUT DROP  #accepte les connexions entrantes
iptables -P FORWARD DROP
iptables -P OUTPUT DROP #accepter les connexions sortantes


iptables -A INPUT -p tcp --dport 22 -j ACCEPT #autorise ssh entrant
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT #autorise ssh sortant

iptables -A INPUT -p icmp -j ACCEPT #autorise ping
iptables -A OUTPUT -p icmp -j ACCEPT #autorise ping

iptables -A INPUT -p tcp -s 10.31.240.80 --dport 3306 -j ACCEPT #autorise db pour webpriv
iptables -A OUTPUT -p tcp -s 10.31.240.80 --sport 3306 -j ACCEPT #autorise db pour webpri

iptables -A INPUT -p tcp -s 10.31.248.80 --dport 3306 -j ACCEPT #autorise db pour webpub
iptables -A OUTPUT -p tcp -s 10.31.248.80 --sport 3306 -j ACCEPT #autorise db pour webpub

iptables -A INPUT -p tcp -s 10.31.248.25 --dport 3306 -j ACCEPT #autorise db pour mailpub
iptables -A OUTPUT -p tcp -s 10.31.248.25 --sport 3306 -j ACCEPT #autorise db pour mailpu
```

Puis crée **nano /etc/systemd/system/rc-local.service**
Et y écrire pour lancer rc.local :

```
[Unit]
Description=/etc/rc.local
ConditionPathExists=/etc/rc.local

[Service]
Type=forking
ExecStart=/etc/rc.local start
TimeoutSec=0
StandardOutput=tty
RemainAfterExit=yes
SysVStartPriority=99

[Install]
WantedBy=multi-user.target
```

Puis dans rc.local on lance le script reglesON :

```
#!/bin/bash
./home/reglesON.sh
```

Regles pour webpriv :

```
iptables -F

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

```

```

iptables -A INPUT -p tcp --dport 22 -j ACCEPT #ssh
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT #ssh

iptables -A INPUT -p tcp -s 10.31.240.82 -j ACCEPT #zabbix
iptables -A OUTPUT -p tcp -s 10.31.240.82 -j ACCEPT #zabbix

iptables -A INPUT -p tcp -s 10.31.240.33 --dport 3306 -j ACCEPT #db1
iptables -A OUTPUT -p tcp -s 10.31.240.33 --sport 3306 -j ACCEPT #db1

iptables -A INPUT -p tcp -s 10.31.240.34 --dport 3306 -j ACCEPT #db2
iptables -A OUTPUT -p tcp -s 10.31.240.34 -j --sport 3306 ACCEPT #db2

iptables -A INPUT -p tcp -s 10.31.240.67 --dport 67 -j ACCEPT #dhcp
iptables -A OUTPUT -p tcp -s 10.31.240.67 --sport 67 -j ACCEPT #dhcp
```

Zabbix

```
iptables -F #suppression des tables
iptables -t nat -F  #suppression de la tables nat
iptables -P INPUT DROP  #accepte les connexions entrantes
iptables -P FORWARD DROP
iptables -P OUTPUT DROP #accepter les connexions sortantes


iptables -A INPUT -p tcp --dport 22 -j ACCEPT #autorise ssh entrant
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT #autorise ssh sortant


iptables -A INPUT -p tcp -s 10.31.240.80 --dport 10051 -j ACCEPT #autorise db pour webpri
iptables -A OUTPUT -p tcp -s 10.31.240.80 --sport 10051 -j ACCEPT #autorise db pour webpr

iptables -A INPUT -p tcp -s 10.31.248.80 --dport 10051 -j ACCEPT #autorise db pour webpri
iptables -A OUTPUT -p tcp -s 10.31.248.80 --sport 10051 -j ACCEPT #autorise db pour webpr

iptables -A INPUT -p tcp -s 10.31.240.33 --dport 10051 -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.31.240.33 --sport 10051 -j ACCEPT

iptables -A INPUT -p tcp -s 10.31.240.34 --dport 10051 -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.31.240.34 --sport 10051 -j ACCEPT


iptables -A INPUT -p tcp -s 10.31.240.67 --dport 10051 -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.31.240.67 --sport 10051 -j ACCEPT


iptables -A INPUT -p tcp -s 10.31.240.68 --dport 10051 -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.31.240.68 --sport 10051 -j ACCEPT

iptables -A INPUT -p tcp -s 10.31.240.54 --dport 10051 -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.31.240.54 --sport 10051 -j ACCEPT


iptables -A INPUT -p tcp -s 10.31.240.82 --dport 10051 -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.31.240.82 --sport 10051 -j ACCEPT
```