

Aller au contenu

uho

Iptables pour privdb1 et privdb2 :

```

1 iptables -F #suppression des tables
2 iptables -t nat -F #suppression de la tables nat
3 iptables -P INPUT DROP #accepte les connexions entrantes
4 iptables -P FORWARD DROP
5 iptables -P OUTPUT DROP #accepter les connexions sortantes
6
7
8 iptables -A INPUT -p tcp --dport 22 -j ACCEPT #autorise ssh entrant
9 iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT #autorise ssh sortant
10
11 iptables -A INPUT -p icmp -j ACCEPT #autorise ping
12 iptables -A OUTPUT -p icmp -j ACCEPT #autorise ping
13
14 iptables -A INPUT -p tcp -s 10.31.240.80 --dport 3306 -j ACCEPT #autorise db pour webpriv
15 iptables -A OUTPUT -p tcp -s 10.31.240.80 --sport 3306 -j ACCEPT #autorise db pour webpri
16
17 iptables -A INPUT -p tcp -s 10.31.248.80 --dport 3306 -j ACCEPT #autorise db pour webpub
18 iptables -A OUTPUT -p tcp -s 10.31.248.80 --sport 3306 -j ACCEPT #autorise db pour webput
19
20 iptables -A INPUT -p tcp -s 10.31.248.25 --dport 3306 -j ACCEPT #autorise db pour mailput
21 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 :

```

1 [Unit]
2 Description=/etc/rc.local
3 ConditionPathExists=/etc/rc.local
4
5 [Service]
6 Type=forking
7 ExecStart=/etc/rc.local start
8 TimeoutSec=0
9 StandardOutput=tty
10 RemainAfterExit=yes
11 SysVStartPriority=99
12
13 [Install]
14 WantedBy=multi-user.target

```

Puis dans rc.local on lance le script reglesON :

```

1 #!/bin/bash
2 ./home/reglesON.sh

```

Regles pour webpriv :

```

1 iptables -F
2
3 iptables -P INPUT DROP
4 iptables -P OUTPUT DROP
5 iptables -P FORWARD DROP
6

```

```

7
8 iptables -A INPUT -p tcp --dport 22 -j ACCEPT #ssh
9 iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT #ssh
10
11 iptables -A INPUT -p tcp -s 10.31.240.82 -j ACCEPT #zabbix
12 iptables -A OUTPUT -p tcp -s 10.31.240.82 -j ACCEPT #zabbix
13
14 iptables -A INPUT -p tcp -s 10.31.240.33 --dport 3306 -j ACCEPT #db1
15 iptables -A OUTPUT -p tcp -s 10.31.240.33 --sport 3306 -j ACCEPT #db1
16
17 iptables -A INPUT -p tcp -s 10.31.240.34 --dport 3306 -j ACCEPT #db2
18 iptables -A OUTPUT -p tcp -s 10.31.240.34 -j --sport 3306 ACCEPT #db2
19
20 iptables -A INPUT -p tcp -s 10.31.240.67 --dport 67 -j ACCEPT #dhcp
21 iptables -A OUTPUT -p tcp -s 10.31.240.67 --sport 67 -j ACCEPT #dhcp

```

Zabbix

```

1 iptables -F #suppression des tables
2 iptables -t nat -F #suppression de la tables nat
3 iptables -P INPUT DROP #accepte les connexions entrantes
4 iptables -P FORWARD DROP
5 iptables -P OUTPUT DROP #accepter les connexions sortantes
6
7
8 iptables -A INPUT -p tcp --dport 22 -j ACCEPT #autorise ssh entrant
9 iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT #autorise ssh sortant
10
11
12 iptables -A INPUT -p tcp -s 10.31.240.80 --dport 10051 -j ACCEPT #autorise db pour webpri
13 iptables -A OUTPUT -p tcp -s 10.31.240.80 --sport 10051 -j ACCEPT #autorise db pour webpr
14
15 iptables -A INPUT -p tcp -s 10.31.248.80 --dport 10051 -j ACCEPT #autorise db pour webpri
16 iptables -A OUTPUT -p tcp -s 10.31.248.80 --sport 10051 -j ACCEPT #autorise db pour webpr
17
18 iptables -A INPUT -p tcp -s 10.31.240.33 --dport 10051 -j ACCEPT
19 iptables -A OUTPUT -p tcp -s 10.31.240.33 --sport 10051 -j ACCEPT
20
21 iptables -A INPUT -p tcp -s 10.31.240.34 --dport 10051 -j ACCEPT
22 iptables -A OUTPUT -p tcp -s 10.31.240.34 --sport 10051 -j ACCEPT
23
24
25 iptables -A INPUT -p tcp -s 10.31.240.67 --dport 10051 -j ACCEPT
26 iptables -A OUTPUT -p tcp -s 10.31.240.67 --sport 10051 -j ACCEPT
27
28
29 iptables -A INPUT -p tcp -s 10.31.240.68 --dport 10051 -j ACCEPT
30 iptables -A OUTPUT -p tcp -s 10.31.240.68 --sport 10051 -j ACCEPT
31
32 iptables -A INPUT -p tcp -s 10.31.240.54 --dport 10051 -j ACCEPT
33 iptables -A OUTPUT -p tcp -s 10.31.240.54 --sport 10051 -j ACCEPT
34
35
36 iptables -A INPUT -p tcp -s 10.31.240.82 --dport 10051 -j ACCEPT
37 iptables -A OUTPUT -p tcp -s 10.31.240.82 --sport 10051 -j ACCEPT

```

sisr2-afrique/mission_15_netfilter_hadj.txt · Dernière modification: 2022/01/11 14:40 de h-benzahaf