

Table des matières

SSH .....	3
Apache .....	3



## SSH

Ce script, une fois cronné selon les besoins, vérifie les connexions indésirables au serveur SSH. Si n connexions ont échouées dans l'heure courante alors l'IP est blacklistée au moyen d'iptables. Un mail d'info est également envoyé et un la commande de blacklist est renvoyée dans un fichier qu'il faudra exécuter au boot de la machine. Ci-dessous le script :

```
#!/bin/bash
EXCL="X.X.X.X" ''#on spécifie des adresses qui peuvent se planter''
C_HEURE="date +%H:"
LIST_IP="grep sshd /var/log/auth.log|egrep -v "$EXCL"|grep ${C_HEURE}|grep "Failed"|awk -F "from" '{print $2}'\
|awk '{print $1}'|sort -u"

for IP in `echo $LIST_IP`
do
NB=`grep sshd /var/log/auth.log|egrep -v "$EXCL"|grep $IP|grep ${C_HEURE}|grep "Failed"|awk -F "from" '{print $2}'|\
awk '{print $1}'|wc -l`

if [ $NB -ge 10 ]
then
if grep $IP /usr/bin/bl_SSHD;then
exit
else
echo "SSHD - Adresse blacklistée : $IP - `date +%d/%m/%Y_%HH%M` - $NB tentatives" |mailx -s "Blacklist SSHD" \
some.email@domain.com
echo "iptables -I INPUT -s $IP -p tcp --dport 22 -j DROP          #`date +%d/%m/%Y_%HH%M`" >> /usr/bin/bl_SSHD
/sbin/iptables -I INPUT -s $IP -p tcp --dport 22 -j DROP
fi
fi
done
```

Si on utilise MySecureShell : [des solutions ici](#).

## Apache

Le même mais pour Apache.

```
#!/bin/bash
for file in `find /var/log/apache2 -name "error_log"`
do
DATE="date +%b %d"
liste_ip="egrep -i "not found|mismatch|failure" $file|grep "$DATE"|awk '{print $8}'|sed "s/[/]/g"|sort -u"
for ip in `echo ${liste_ip}`
do
heure="date +%H:"
NB="egrep -i "not found|mismatch|failure" $file|grep $ip|grep "$DATE"|wc -l"
site="echo $file |awk -F "/" '{print $5}'"
echo "$site : $ip -> $NB tentatives"
if [ $NB -gt 10 ]
then
if ! grep $ip /usr/bin/bl_HTTP >/dev/null
then
vhost="echo $file|awk -F "/" '{print $5}'"
echo "HTTP - Adresse blacklistée : $ip - `date +%d/%m/%Y_%HH%M` - $NB tentatives sur $vhost"
|mailx -s "Blacklist HTTP" some.email@domain.com
echo "iptables -I INPUT -s $ip -p tcp --dport 80 -j DROP          #`date +%d/%m/%Y_%HH%M`" >> /usr/bin/bl_HTTP
/sbin/iptables -I INPUT -s $ip -p tcp --dport 80 -j DROP
fi
fi
done
done
```

From:  
<https://unix.ndlp.info/> - **Where there is a shell, there is a way**

Permanent link:  
[https://unix.ndlp.info/doku.php/informatique:nix:linux:linux\\_reseau:blacklister\\_les\\_indesirables\\_apache\\_ssh](https://unix.ndlp.info/doku.php/informatique:nix:linux:linux_reseau:blacklister_les_indesirables_apache_ssh)

Last update: **2009/06/29 21:04**