

## Méthode générale

Lorsqu'une machine plante et qu'il faut la rebooter, le problème est qu'on ne sait pas par où chercher l'origine du problème. Voici une méthode qui vous donnera quelques pistes :

- Le client nous dit : ça plante depuis 1 semaine. Je dois rebooter plusieurs fois par jour.

```
machine : 2298
release : 1.36
ip : 213.186.41.xx
hostname : nsxxx.ovh.net
#
```

Avant toute chose, il faut mettre la machine à jour au niveau de la release. On va donc éviter tous les problèmes de sécurité connus (à moins que la machine ne soit déjà hackée, auquel cas il est trop tard).

Un coup d'oeil avant de commencer sur le mrtg :

Bon, maintenant que la machine est à jour au niveau de la release :

```
# w
12:27pm up 1:21, 2 users, load average: 2.38, 2.57, 2.36
```

Effectivement la machine a un uptime d'1h21. La charge est déjà importante.

```
# free
total used free shared buffers cached
Mem: 514544 263096 251448 0 42388 80128
-/+ buffers/cache: 140580 373964
Swap: 522104 0 522104
```

140Mo de RAM utilisé. Ça ne swap pas. Visiblement on ne va pas chercher de ce côté-là.

```
# cat /proc/cpuinfo
processor : 0
vendor_id : 'GenuineIntel'
cpu family : 15
model : 1
model name : Intel(R) Celeron(R) CPU 1.80GHz
stepping : 3
cpu MHz : 1800.334
cache size : 20 KB
fdiv_bug : no
```

## OVH

```
hlt_bug : no
f00f_bug : no
coma_bug : no
fpu : yes
fpu_exception : yes
cpuid level : 2
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr
sse sse2 ss ht tm
bogomips : 3591.37
```

Un celeron 1.8GHz. C'est bon de le savoir pour avoir une idée de ce que la machine est capable de faire.

```
# dmesg
Linux version 2.4.19 (root@install.ovh.net) (gcc version 2.96 20000731 (Red Hat Linux 7.1 2.96-81)) #2
SMP mer nov 20 17:40:06 CET 2002
[...]
Freeing unused kernel memory: 256k freed
Adding Swap: 522104k swap-space (priority -1)
EXT3 FS 2.4-0.9.17, 10 Jan 2002 on ide0(3,1), internal journal
kjournald starting. Commit interval 5 seconds
EXT3 FS 2.4-0.9.17, 10 Jan 2002 on ide0(3,2), internal journal
EXT3-fs: mounted filesystem with ordered data mode.
eth0: Setting 100mbps full-duplex based on auto-negotiated partner ability 41e1.
```

Il n'y a rien d'extraordinaire dans le dmesg. Le noyau n'est pas à jour. C'est tout.

```
# ps auxw
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
[...]
markus 13410 0.0 0.1 1932 860 ? S 12:38 0:00 /bin/sh -c $HOME/bin/rrd_update.pl 6 >/dev/null 2>&1
markus 13411 0.0 0.2 2588 1316 ? S 12:38 0:00 /usr/bin/perl -w /home/markus/bin/rrd_update.pl 6
[...]
```

La sortie standard. On remarque un rrd\_update qui tourne par ici ou par là. Rien de grave.

```
# netstat -tanpu
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat PID/Program name
[...]
tcp 0 0 213.186.41.43:80 80.13.42.22:2569 SYN_RECV -
tcp 0 0 213.186.41.43:80 81.248.123.241:3932 SYN_RECV -
tcp 0 0 213.186.41.43:80 81.50.163.43:4156 SYN_RECV -
tcp 0 0 213.186.41.43:80 213.36.11.55:1328 SYN_RECV -
tcp 0 0 213.186.41.43:80 217.128.9.248:34257 SYN_RECV -
tcp 0 0 213.186.41.43:80 81.240.118.126:3747 SYN_RECV -
tcp 0 0 213.186.41.43:80 213.228.52.184:3749 SYN_RECV -
tcp 0 0 213.186.41.43:80 81.240.118.126:3743 SYN_RECV -
```

## OVH

```
tcp 0 0 213.186.41.43:80 81.248.123.241:3931 SYN_RECV –  
tcp 0 0 213.186.41.43:80 81.50.163.43:4191 SYN_RECV –  
tcp 0 0 213.186.41.43:80 213.36.11.55:1327 SYN_RECV –  
[...]
```

Il y a pas mal des SYN\_RECV. Comme l'IP est différente à chaque fois, on peut penser que le serveur web a pas mal de connexions. Actuellement, il y a 11 connexions qui sont encore ouvertes.

On va regarder les paramètres d'apache :

```
#pico /httpd.conf
```

Tiens, pas de paramètre concernant apache !? On va lui ajouter quelques paramètres de base pour bien commencer :

```
'MinSpareServers' 20  
'MaxSpareServers' 100  
'StartServers' 30  
'MaxClients' 60  
'MaxRequestsPerChild' 60
```

et on redemarre apache :

```
# /root/apare  
/usr/local/apache/bin/apachectl stop: httpd stopped  
/usr/local/apache/bin/apachectl start: httpd started  
# w  
12:46pm up 1:39, 1 user, load average: 2.54, 1.84, 2.04  
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT  
root pts/0 213.244.20.43 11:52am 0.00s 0.14s 0.01s w  
# netstat -tanpu  
[...]  
# top
```

Bon on va voir ce que ça donne en temps réel :

```
12:48pm up 1:41, 1 user, load average: 1,79, 1,81, 2,01  
116 processes: 114 sleeping, 2 running, 0 zombie, 0 stopped  
CPU states: 27,7% user, 14,8% system, 0,0% nice, 57,3% idle  
Mem: 514544K av, 286228K used, 228316K free, 0K shrd, 43616K buff  
Swap: 522104K av, 0K used, 522104K free 82676K cached
```

```
PID USER PRI NI SIZE RSS SHARE STAT %CPU %MEM TIME COMMAND  
14461 nobody 18 0 6936 6936 4132 S 12,1 1,3 0:01 httpd  
14516 nobody 9 0 6308 6308 4168 S 3,5 1,2 0:00 httpd  
14465 nobody 9 0 6860 6860 4156 S 2,9 1,3 0:00 httpd  
14625 nobody 9 0 6924 6924 4152 S 0,7 1,3 0:01 httpd
```

## OVH

```
111 root 9 0 0 0 0 SW 0,5 0,0 0:41 kjournald
14646 root 12 0 1092 1092 828 R 0,5 0,2 0:00 top
14759 root 9 0 716 716 640 S 0,3 0,1 0:00 crond
14765 markus 8 0 1316 1316 1112 S 0,3 0,2 0:00 rrd_update.pl
8 root 9 0 0 0 0 SW 0,1 0,0 0:47 kjournald
440 root 9 0 592 592 488 S 0,1 0,1 0:00 syslogd
803 root 9 -3 1284 1284 1216 S < 0,1 0,2 0:00 ncftpd
6763 root 9 0 2076 2076 1708 R 0,1 0,4 0:00 sshd
14484 nobody 9 0 6932 6932 4172 S 0,1 1,3 0:00 httpd
14535 nobody 9 0 6836 6836 4164 S 0,1 1,3 0:00 httpd
14540 nobody 9 0 6508 6508 4164 S 0,1 1,2 0:00 httpd
1 root 8 0 524 524 456 S 0,0 0,1 0:09 init
```

On remarque qu'il y a 57.3% de CPU libre. La RAM va bien. Il y a quelques process httpd qui prennent pas mal des CPU. kjournald ce qui donne l'information qu'il y a pas mal d'accès sur le disque dur. Rien de grave.

On laisse tourner top et on regarde ce qu'il se passe.

Quelques minutes plus tard :

```
12:51pm up 1:44, 1 user, load average: 4,68, 2,75, 2,30
138 processes: 125 sleeping, 12 running, 1 zombie, 0 stopped
CPU states: 66,5% user, 33,2% system, 0,0% nice, 0,0% idle
Mem: 514544K av, 437532K used, 77012K free, 0K shrd, 44040K buff
Swap: 522104K av, 0K used, 522104K free 83288K cached
```

```
PID USER PRI NI SIZE RSS SHARE STAT %CPU %MEM TIME COMMAND
15172 mysql 15 0 5048 5048 1188 R 7,7 0,9 0:00 mysqld
14475 nobody 14 0 15460 15M 4152 R 7,3 3,0 0:05 httpd
15175 mysql 15 0 5048 5048 1188 R 7,3 0,9 0:00 mysqld
14623 nobody 14 0 16004 15M 4160 S 6,1 3,1 0:01 httpd
15155 mysql 11 0 5048 5048 1188 S 6,1 0,9 0:00 mysqld
14468 nobody 14 0 16988 16M 4160 S 5,7 3,3 0:02 httpd
15168 mysql 10 0 5048 5048 1188 S 5,5 0,9 0:00 mysqld
15173 mysql 15 0 5048 5048 1188 R 5,3 0,9 0:00 mysqld
14533 nobody 9 0 7064 7064 4164 S 3,9 1,3 0:01 httpd
14549 nobody 10 0 17384 16M 4144 S 3,9 3,3 0:02 httpd
14551 nobody 10 0 17492 17M 4144 S 3,9 3,3 0:00 httpd
15158 mysql 9 0 5048 5048 1188 S 3,5 0,9 0:00 mysqld
14467 nobody 9 0 18168 17M 4192 S 3,3 3,5 0:02 httpd
14481 nobody 9 0 18056 17M 4128 S 3,1 3,5 0:01 httpd
15159 mysql 9 0 5048 5048 1188 S 3,1 0,9 0:00 mysqld
14459 nobody 9 0 18028 17M 4148 S 2,7 3,5 0:02 httpd
14625 nobody 9 0 17924 17M 4152 S 2,5 3,4 0:03 httpd
15157 mysql 9 0 5048 5048 1188 S 2,3 0,9 0:00 mysqld
14469 nobody 9 0 17908 17M 4172 S 1,9 3,4 0:03 httpd
14550 nobody 9 0 17772 17M 4168 S 1,9 3,4 0:04 httpd
15153 mysql 9 0 5048 5048 1188 S 1,7 0,9 0:00 mysqld
14485 nobody 11 0 6816 6816 4168 S 1,5 1,3 0:01 httpd
15160 mysql 9 0 5048 5048 1188 S 1,5 0,9 0:00 mysqld
```

## OVH

```
14463 nobody 15 0 7112 7112 4160 R 1,1 1,3 0:04 httpd
15156 mysql 9 0 5048 5048 1188 S 1,1 0,9 0:00 mysqld
15176 mysql 9 0 5048 5048 1188 S 1,1 0,9 0:00 mysqld
14646 root 12 0 1092 1092 828 R 0,7 0,2 0:01 top
```

Plus de CPU, la RAM prise devient de plus en plus importante, la charge monte.  
Il y a de plus en plus des process httpd et mysql qui prennent toutes les ressources.

On laisse tourner top.

4 heures plus tard :

```
4:47pm up 5:41, 2 users, load average: 47,83, 23,91, 12,70
185 processes: 138 sleeping, 47 running, 0 zombie, 0 stopped
CPU states: 21,0% user, 73,4% system, 0,0% nice, 5,5% idle
Mem: 514544K av, 511596K used, 2948K free, 0K shrd, 1168K buff
Swap: 522104K av, 272488K used, 249616K free 25696K cached
```

```
PID USER PRI NI SIZE RSS SHARE STAT %CPU %MEM TIME COMMAND
10072 nobody 15 0 14368 13M 5992 R 1,9 2,7 0:15 httpd
9500 nobody 9 0 17416 8376 7352 D 1,6 1,6 0:18 httpd
9872 nobody 10 0 17372 8796 7476 R 1,4 1,7 0:11 httpd
13684 nobody 14 0 14588 5896 2744 R 1,4 1,1 0:01 httpd
13618 nobody 11 0 14292 5416 2736 S 1,1 1,0 0:01 httpd
13363 nobody 15 0 14028 6124 2820 S 1,0 1,1 0:02 httpd
12584 nobody 13 0 14120 13M 2812 S 0,9 2,6 0:06 httpd
13461 nobody 16 0 14436 5008 2824 S 0,9 0,9 0:02 httpd
13534 mysql 14 0 14692 10M 2452 R 0,9 1,9 0:01 mysqld
10683 nobody 13 0 13148 12M 5616 S 0,8 2,4 0:08 httpd
13479 nobody 19 0 14344 5948 2820 R 0,8 1,1 0:02 httpd
13653 mysql 12 0 14692 10M 2452 S 0,8 1,9 0:00 mysqld
13690 mysql 15 0 14692 10M 2452 R 0,8 1,9 0:01 mysqld
9497 nobody 9 0 17384 8932 6876 R 0,7 1,7 0:14 httpd
10685 nobody 15 0 13324 12M 5616 R 0,7 2,4 0:12 httpd
13037 nobody 9 0 14848 14M 2792 R 0,7 2,7 0:03 httpd
13521 mysql 18 0 14692 10M 2452 R 0,7 1,9 0:00 mysqld
13539 mysql 14 0 14692 10M 2452 R 0,7 1,9 0:01 mysqld
13612 mysql 14 0 14692 10M 2452 S 0,7 1,9 0:00 mysqld
13650 nobody 14 0 15276 5888 2752 R 0,7 1,1 0:02 httpd
13652 mysql 10 0 14692 10M 2452 S 0,7 1,9 0:00 mysqld
8469 nobody 9 0 14100 13M 2728 D 0,6 2,6 0:15 httpd
8603 nobody 9 0 13004 12M 2648 R 0,6 2,4 0:23 httpd
8636 nobody 9 0 12256 11M 2644 D 0,6 2,2 0:18 httpd
```

La machine est presque plantée. La charge est très importante. Il n'y a plus de CPU libre, plus de RAM disponible.

On essaie de récupérer la machine avant qu'elle ne plante. 15 minutes pour taper la commande...

```
# killall -9 httpd
```

C'est bon on l'a recuperé. Allez vite vite vite pour voir s'il reste des choses intéressantes :

```
# w
4:56pm up 5:50, 2 users, load average: 45.38, 44.91, 29.18
# netstat -tanpu
[...]
```

Rien d'exceptionnel. On regarde les logs :

```
# cd /usr/local/apache/logs/
# tail -n 100 *_log
```

Résultat : visiblement le serveur plante parce que des choses très lourdes tournent sur la machine. Il faut jouer avec status-server pour récupérer les informations sur les requêtes faites sur la machines, de la même manière qu'on récupérerait les informations via top.

Un peu de lecture et configuration ConfigurerEtUtiliserServerStatus

```
# pico /httpd.conf
# /root/apare
/usr/local/apache/bin/apachectl stop: httpd (pid 14458?) not running
/usr/local/apache/bin/apachectl start: httpd started
# telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /ovh-status HTTP/1.0

HTTP/1.1 200 OK
Date: Sun, 09 Nov 2003 16:03:54 GMT
Server: Apache/1.3.28 (Unix) mod_gzip/1.3.19.1a PHP/4.3.3 mod_ssl/2.8.15 OpenSSL/0.9.6i
Connection: close
Content-Type: text/html
```

```
Server Version: Apache/1.3.28 (Unix) mod_gzip/1.3.19.1a PHP/4.3.3 mod_ssl/2.8.15 OpenSSL/0.9.6i
Server Built: Sep 10 2003 21:34:14
Current Time: Sunday, 09-Nov-2003 17:03:55 CET
```

```
Restart Time: Sunday, 09-Nov-2003 17:03:49 CET
```

```
Parent Server Generation: 0
```

```
Server uptime: 6 seconds
```

```
Total accesses: 52 - Total Traffic: 4 kB
```

## OVH

CPU Usage: u1.19 s.81 cu0 cs0 – 33.3% CPU load

8.67 requests/sec – 682 B/second – 78 B/request

8 requests currently being processed, 22 idle servers

\_KKKKKWKK

[...]

Voilà. Maintenant nous avons la possibilité de suivre les requêtes qui sont en cours d'exécution sur la machine.

On va installer un petit outil de chez OVH, otop. Le code source est aussi simple qu'efficace : on se connecte sur apache pour récupérer server-status et on le trie.

```
# cat > otop.pl
# cat > otop
# chmod 755 otop.pl otop
# ./otop
ns30075.ovh.net GET /ovh-status HTTP/1.0 127.0.0.1 ns30075
www.tv-realite.net GET /images/button.gif HTTP/1.1 81.49.201.169 ns30075
www.tv-realite.net GET /images/button.gif HTTP/1.1 82.65.220.249 ns30075
www.tv-realite.net GET /images/icons/profile.gif HTTP/1.1 193.248.177.54 ns30075
www.tv-realite.net GET /images/smilies/icon_wink.gif HTTP/1.1 62.147.34.237 ns30075
www.tv-realite.net GET /images/subject/icon32.gif HTTP/1.1 62.147.216.161 ns30075
www.tv-realite.net GET /modules/dbcounter/cache/cpt.php HTTP/1.1 62.147.216.161 ns30075
www.tv-realite.net GET /modules/dbcounter/cache/cpt.php HTTP/1.1 62.39.220.121 ns30075
www.tv-realite.net GET /modules/dbcounter/cache/cpt.php HTTP/1.1 81.50.123.85 ns30075
www.tv-realite.net GET /modules/forum/ HTTP/1.1 81.249.117.200 ns30075
www.tv-realite.net GET /modules/Jeux/Jeux/Action/pacmanswf/pacman.swf HTTP/1.1 80.238.52.86
ns30075
www.tv-realite.net GET /modules/magalerie/galerie/Star%20Academy%20/Jeremy/jerem3 80.238.52.86
ns30075
www.tv-realite.net GET /modules/news/images/friend1.gif HTTP/1.1 81.50.47.133 ns30075
www.tv-realite.net GET /modules/news/images/print1.gif HTTP/1.1 81.48.39.152 ns30075
www.tv-realite.net GET /smilies/fouet.gif HTTP/1.1 62.147.210.205 ns30075
www.tv-realite.net GET /smilies/nixweiss.gif HTTP/1.1 62.147.210.205 ns30075
www.tv-realite.net GET /smilies/oops.gif HTTP/1.1 213.36.58.1 ns30075
www.tv-realite.net GET /smilies/oops.gif HTTP/1.1 81.50.123.85 ns30075
www.tv-realite.net GET /smilies/tesbete.gif HTTP/1.1 81.248.97.134 ns30075
www.tv-realite.net GET /themes/FD-Bluenet/images/bag2.gif HTTP/1.1 193.248.177.54 ns30075
www.tv-realite.net GET /themes/FD-Bluenet/images/bag2.gif HTTP/1.1 81.48.39.152 ns30075
www.tv-realite.net GET /themes/FD-Bluenet/images/bag2.gif HTTP/1.1 81.49.201.169 ns30075
www.tv-realite.net GET /themes/FD-Bluenet/images/bag2.gif HTTP/1.1 82.65.220.249 ns30075
www.tv-realite.net GET /themes/FD-Bluenet/images/top.gif HTTP/1.1 195.93.73.6 ns30075
```

On va donc maintenant le faire tourner toutes les 2 secondes pour trouver le problème :

```
# while true; do ./otop; sleep 2;done
```

Et dans une 2ème console, on se reconnecte pour faire tourner top.

Et on laisse tourner pendant quelques heures.

5 minutes plus tard. La machine est out.

```

ns30075.ovh.net GET /ovh-status HTTP/1.0 127.0.0.1 ns30075
www.tv-realite.net GET / HTTP/1.1 172.190.55.200 ns30075
www.tv-realite.net GET / HTTP/1.1 193.248.171.49 ns30075
www.tv-realite.net GET / HTTP/1.1 195.93.66.12 ns30075
www.tv-realite.net GET / HTTP/1.1 202.123.0.150 ns30075
www.tv-realite.net GET / HTTP/1.1 217.128.35.49 ns30075
www.tv-realite.net GET / HTTP/1.1 80.201.114.225 ns30075
www.tv-realite.net GET / HTTP/1.1 81.249.82.249 ns30075
www.tv-realite.net GET / HTTP/1.1 81.64.6.73 ns30075
www.tv-realite.net GET / HTTP/1.1 81.64.6.73 ns30075
www.tv-realite.net GET /images/library/starac3-2/3nolwenn-2.jpg HTTP/1.1 213.228.55.146 ns30075
www.tv-realite.net GET /images/library/starac3-2/3nolwenn-4.jpg HTTP/1.1 213.228.55.146 ns30075
www.tv-realite.net GET /modules/forum/ HTTP/1.1 172.178.136.110 ns30075
www.tv-realite.net GET /modules/forum/ HTTP/1.1 213.44.198.73 ns30075
www.tv-realite.net GET /modules/forum/ HTTP/1.1 213.44.198.73 ns30075
www.tv-realite.net GET /modules/magalerie/galerie/Star%20Academy%20/cloclo_tf1_11 82.65.220.249
ns30075
www.tv-realite.net GET /modules/magalerie/images/rank3dbf8e9e7d88d.gif HTTP/1.1 82.65.220.249
ns30075
www.tv-realite.net GET /modules/mylinks/ratelink.php?lid=129 HTTP/1.1 82.64.102.4 ns30075
www.tv-realite.net GET /modules/mylinks/ratelink.php?lid=129 HTTP/1.1 82.64.102.4 ns30075
www.tv-realite.net GET /modules/newbb_plus/index.php HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/newbb_plus/viewforum.php?forum=1 HTTP/1.1 195.93.64.6 ns30075
www.tv-realite.net GET /modules/newbb_plus/viewforum.php?forum=1 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/newbb_plus/viewforum.php?forum=1 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/newbb_plus/viewforum.php?forum=1 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/newbb_plus/viewforum.php?forum=1 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/newbb_plus/viewforum.php?forum=1 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/newbb_plus/viewforum.php?forum=1 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/newbb_plus/viewforum.php?forum=3 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/news/article.php?item_id=2298 HTTP/1.1 193.248.177.54 ns30075
www.tv-realite.net GET /modules/news/article.php?storyid=2490 HTTP/1.1 81.49.201.169 ns30075
www.tv-realite.net GET /modules/news/article.php?storyid=2490 HTTP/1.1 81.49.201.169 ns30075
www.tv-realite.net GET /modules/news/article.php?storyid=2490 HTTP/1.1 81.49.201.169 ns30075
www.tv-realite.net GET /modules/news/article.php?storyid=2490 HTTP/1.1 81.49.201.169 ns30075
www.tv-realite.net GET /modules/news/article.php?storyid=2497 HTTP/1.1 81.49.201.169 ns30075
www.tv-realite.net GET /modules/news/article.php?storyid=2499 HTTP/1.1 213.36.11.162 ns30075
www.tv-realite.net GET /modules/news/article.php?storyid=2499 HTTP/1.1 213.36.11.162 ns30075
www.tv-realite.net GET /modules/news/article.php?storyid=2499 HTTP/1.1 213.36.11.162 ns30075
www.tv-realite.net GET /modules/news/article.php?storyid=2499 HTTP/1.1 213.36.11.162 ns30075
www.tv-realite.net GET /modules/news/article.php?storyid=2508 HTTP/1.1 62.147.34.237 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=22 HTTP/1.1 80.14.69.42 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075

```

## OVH

```
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/news/index.php?storytopic=27 HTTP/1.1 62.203.3.242 ns30075
www.tv-realite.net GET /modules/sections/index.php?op=viewarticle&artid=30 HTTP/1.1 217.128.35.49
ns30075
www.tv-realite.net GET /modules/xoopspoll/index.php HTTP/1.1 195.93.72.10 ns30075
www.tv-realite.net GET /modules/xoopspoll/index.php?poll_id=62 HTTP/1.1 193.252.57.189 ns30075
www.tv-realite.net GET /modules/xoopspoll/pollresults.php?poll_id=62 HTTP/1.1 172.178.136.110
ns30075
www.tv-realite.net GET /modules/xoopspoll/pollresults.php?poll_id=62 HTTP/1.1 172.188.48.244 ns30075
www.tv-realite.net GET /modules/xoopspoll/pollresults.php?poll_id=62 HTTP/1.1 172.188.48.244 ns30075
www.tv-realite.net GET /modules/xoopspoll/pollresults.php?poll_id=62 HTTP/1.1 62.147.34.237 ns30075
www.tv-realite.net GET /modules/xtremgquestbook/index.php?limite=40 HTTP/1.1 80.200.25.198 ns30075
www.tv-realite.net GET /themes/FD-Bluenet/images/top.gif HTTP/1.1 213.36.64.61 ns30075
www.tv-realite.net GET /user.php HTTP/1.1 193.250.7.174 ns30075
k
ill
all -9 httpd[root@ns30075 root]# killall -9 httpd
[root@ns30075 root]#
```

Bon. Des scripts php sont consultés avec une violence qui casse la machine. Est-ce que c'est une attaque ? On va bien voir en blacklistant les IP qui viennent : on redémarre apache puis le otop et dans la 2ème console on va blacklister.

```
[root@ns30075 root]# /root/apare
/usr/local/apache/bin/apachectl stop: httpd (pid 15167?) not running
/usr/local/apache/bin/apachectl start: httpd started
[root@ns30075 root]# while true; do ./otop; sleep 2;done
```

2ème console :

```
[root@ns30075 root]# cat > liste.sh
/usr/local/sbin/iptables -t mangle -A PREROUTING -i eth0 -s $1/32 -d 0.0.0.0/0 -j DROP
[root@ns30075 root]# chmod 755 liste.sh
[root@ns30075 root]# ./liste.sh 62.203.3.242
./liste.sh: /usr/local/sbin/iptables: No such file or directory
[root@ns30075 root]# /sbin/iptables
[root@ns30075 root]# pico liste.sh
[root@ns30075 root]# ./liste.sh 62.203.3.242
iptables: libiptc/libip4tc.c:384: do_check: Assertion `h->info.valid_hooks (1 << 0 | 1 << 3)' failed.
./liste.sh: line 1: 18721 Aborted /sbin/iptables -t mangle -A PREROUTING -i eth0 -s $1/32 -d 0.0.0.0/0 -j
DROP
[root@ns30075 root]#
```

Bon le kernel et iptables ne fonctionne pas bien ensemble. On va recompiler un iptables qui va bien :

```
[root@ns30075 root]#cd /temp
bash: cd: /temp: No such file or directory
[root@ns30075 root]# mkdir /temp
[root@ns30075 root]# cd /temp
[root@ns30075 temp]# wget http://www.iptables.org/files/iptables-1.2.9.tar.bz2
--17:25:19-- http://www.iptables.org/files/iptables-1.2.9.tar.bz2
=> `iptables-1.2.9.tar.bz2'
Connexion vers www.iptables.org:80...Connecté!
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 186,808 [application/x-tar]
```

```
0K ..... 27% @ 649.35 KB/s
50K ..... 54% @ 1.81 MB/s
100K ..... 82% @ 2.22 MB/s
150K ..... .. 100% @ 2.26 MB/s
```

```
17:25:19 (1.26 MB/s) - `iptables-1.2.9.tar.bz2' sauvegardé [186808/186808]
```

```
[root@ns30075 temp]# tar xjf iptables-1.2.9.tar.bz2
[root@ns30075 temp]# cd iptables-1.2.9
[root@ns30075 iptables-1.2.9]# make
```

On kill apache pendant la compilation

```
[root@ns30075 root]# killall -9 httpd
[root@ns30075 root]#
```

2ème console : ça compile bien

```
[...]
[root@ns30075 iptables-1.2.9]# rpm -e iptables
[root@ns30075 iptables-1.2.9]# make install
[...]
```

Un petit test à nouveau pour voir si ça marche mieux :

```
[root@ns30075 iptables-1.2.9]# cd
[root@ns30075 root]# pico liste.sh
[root@ns30075 root]### ./liste.sh 62.203.3.242
[root@ns30075 root]# /usr/local/sbin/iptables -t mangle -L PREROUTING -n
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
DROP all 62.203.3.242 0.0.0.0/0
```

Et donc on peut recommencer la chasse :

```
[root@ns30075 root]# /root/apare  
/usr/local/apache/bin/apachectl stop: httpd (pid 17618?) not running  
/usr/local/apache/bin/apachectl start: httpd started  
[root@ns30075 root]# while true; do ./otop; sleep 2;done
```

et dans la 2ème console on est prêt à taper l'IP à blacklister

```
[root@ns30075 root]# ./liste.sh
```

Et donc ? 30 minutes plus tard replantage avec le même problème, même en blacklistant les IP ça continue. Le problème ne vient peut-être ni de la machine ni d'une attaque mais tout simplement des scripts ?