

# Servidor Semi Hackeado

## Introducción

¿Qué quiere decir semi hackeado? Quiere decir que el servidor no debe ser reinstalado, porque el hacker no ha podido conectarse en root a la máquina.

Podemos suponer con cierta seguridad que si no ha podido conectarse en root tampoco ha podido modificar el sistema.

## Cómo verlo

Lo que hay que remarcar son los procesos que se ejecutan en **nobody**. Es decir, el usuario utilizado por apache.

```
# ps auxw
nobody 23199 0.0 0.3 1436 392 ? S 18:15 0:00 smtp
nobody 23200 0.0 0.9 2148 1144 ttyp8 S 18:15 0:00 sh -i
nobody 23406 0.0 0.3 1432 416 ? S 18:15 0:00 ./bind
nobody 23408 0.0 0.9 2148 1164 ttyp9 S 18:15 0:00 sh -i
nobody 24225 0.0 0.2 1384 308 ttyp9 S 18:15 0:00 ./sshscan-211 213.186.35
nobody 24332 22.8 0.4 1444 560 ttyp9 S 18:15 0:55 ./sshscan-211 213.186
nobody 24768 0.0 0.3 1432 416 ? S 18:16 0:00 ./bind
nobody 24769 0.0 0.9 2148 1144 ttyta S 18:16 0:00 sh -i
nobody 25142 0.0 0.3 1352 436 ttyp5 S 18:16 0:00 ./vuln 217.157.smb
217.157.smb.out 20
nobody 25219 0.0 0.4 1360 520 ttyp8 S 18:16 0:00 ./samba -b 0 -v
213.186.242.231
nobody 26849 0.5 0.3 1344 428 ttyp7 S 18:17 0:00 ./vuln 64.180.smb
64.180.smb.out 20
nobody 2218 0.0 1.2 9648 1532 ? S 18:19 0:00 /usr/local/apache/bin/httpd
-DSSL
nobody 2240 0.0 0.3 1436 388 ? S 18:19 0:00 smtp
nobody 2242 0.0 0.9 2148 1144 ttypb S 18:19 0:00 sh -i
nobody 2316 0.0 1.2 9648 1532 ? S 18:19 0:00 /usr/local/apache/bin/httpd
-DSSL
nobody 2317 0.0 1.2 9648 1532 ? S 18:19 0:00 /usr/local/apache/bin/httpd
-DSSL
nobody 2317 0.0 1.2 9648 1532 ? S 18:19 0:00 /usr/local/apache/bin/httpd
-DSSL
nobody 3183 0.0 0.3 1336 432 ttyp4 S 18:19 0:00 ./o0o 64.218.smb.out
nobody 5439 0.0 0.3 1372 496 ttypb S 18:19 0:00 ./l -h 213.186.242.231
nobody 5440 0.0 0.2 1340 304 ttypb T 18:19 0:00 ./l -h 213.186.242.231
nobody 5447 0.0 0.0 0 0 ttypb Z 18:19 0:00 [l ]
nobody 10027 0.0 0.3 1336 432 ttyp6 S 18:19 0:00 ./o0o 144.89.smb.out
nobody 13037 0.0 0.3 1344 448 ttyp7 S 18:19 0:00 ./vuln 64.180.smb
64.180.smb.out 20
nobody 13146 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13160 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
```

## OVH

```
nobody 13163 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13165 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13179 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13183 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13187 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13201 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13205 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13210 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13231 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13232 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13233 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshscan-211213.186
nobody 13244 0.0 0.4 1444 568 ttyp9 S 18:19 0:00 ./sshsc
```

¿Qué es lo que vemos? Vemos procesos lanzados que aparentemente escanean la red. Podemos pensar que escanean la red para encontrar ssh.

Podemos pensar que el hacker a explotado un fallo a nivel de apache o que simplemente ha encontrado un script php a través del cual ha podido lanzar los comandos.

En cualquier caso, nada se ejecuta en root.

Hay que matar, por tanto, todos los procesos en nobody.

```
# ps auxw | grep nobody | awk {'print $2'} | xargs kill
```

A continuación hay que comprobar si se puede hackear apache.

¿Cómo ver si es hackeable o no? Existe un fallo muy fácil de explotar en apache cuando funciona con una versión antigua de openssl y en ssl.

Hace falta que el puerto 443 esté abierto.

```
# netstat -tanpu | grep ":443"
#
```

Podemos también buscar las cadenas de caracteres en los logs de apache, pero esto puede no funcionar si el método que ha sido utilizado para enviar las informaciones es POST. Sólo obtendremos la información con GET.

Otro ejemplo

```
apache 25307 0.0 0.2 2232 652 ? S Nov13 0:01 [mingetty]
apache 32761 0.0 0.1 1452 300 ? S Nov13 0:00 sh -i
```

## OVH

```
apache 8577 0.0 0.1 1452 332 ? S Nov13 0:00 ./named
apache 9772 0.0 0.0 1352 212 ? T Nov13 0:00 ./vuln x
apache 9773 0.0 0.0 0 0 ? Z Nov13 0:00 [vuln ]
apache 11041 0.0 0.1 1356 320 ? S Nov13 0:00 1444
apache 20146 0.0 0.1 2096 356 ? T Nov14 0:00 ./lols
apache 20148 0.0 0.0 0 0 ? Z Nov14 0:00 [lols ]
apache 6432 0.0 0.1 1356 328 ? S Nov14 0:00 bash
apache 13721 0.0 0.1 2164 356 ? T Nov14 0:00 ./openssl-too -a 0x15
65.94.189.25
apache 13722 0.0 0.0 0 0 ? Z Nov14 0:00 [openssl-too ]
apache 969 0.0 0.0 1376 228 ? S Nov14
0:00 ./scan 202.56.21
apache 1809 0.0 0.1 1452 320 ? S Nov14 0:00 mingetty
apache 2749 0.0 0.3 2016 992 ? S Nov14 0:01 ./crond
apache 2753 0.0 0.3 2016 928 ? S Nov14 0:01 ./crond
apache 3747 0.0 0.1 1356 336 ? S Nov14 0:00 1122
apache 4239 0.0 0.1 1452 320 ? S Nov14 0:00 ./zbind
apache 5542 0.0 0.1 1356 332 ? S Nov14 0:00 1444
apache 13997 0.0 0.2 1576 596 ? S Nov14 0:00 ./mech
apache 14000 0.0 0.2 1576 592 ? S Nov14 0:00 ./mech
apache 20144 49.4 0.1 1348 260 ? R Nov14 536:37 ./p
apache 20256 49.5 0.1 1348 260 ? R Nov14 536:18 ./p
apache 25694 0.0 2.0 45304 5180 ? S 04:03 0:00 /usr/sbin/httpd
-DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_ACTIONS -DHAVE_ALIAS
-DHAVE_ASIS
apache 25695 0.0 1.8 45208 4748 ? S 04:03 0:00 /usr/sbin/httpd
-DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_ACTIONS -DHAVE_ALIAS
-DHAVE_ASIS
apache 25696 0.0 2.0 45304 5180 ? S 04:03 0:00 /usr/sbin/httpd
-DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_ACTIONS -DHAVE_ALIAS
-DHAVE_ASIS
apache 25697 0.0 2.0 45304 5180 ? S 04:03 0:00 /usr/sbin/httpd
-DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_ACTIONS -DHAVE_ALIAS
-DHAVE_ASIS
```

### Otro ejemplo

Algo interesante: aquí el puerto 443 está abierto y la versión de openssl tiene un bug de seguridad.

```
nobody 24929 0.0 0.6 1812 804 ? S Nov12 0:05 [httpd]
nobody 24933 0.0 0.2 1432 324 ? S Nov12 0:00 crond
nobody 27778 0.0 0.8 3436 1044 ? S Nov12 1:50 sendmail: accepting
connections
nobody 27877 0.0 0.4 2216 508 ? S Nov12 0:01 [mingetty]
nobody 15181 0.0 0.2 1432 312 ? S Nov12 0:00 ./cgi
nobody 20211 0.0 0.3 2296 460 ? S Nov13 0:00 ./up2date
nobody 23121 0.0 0.2 1432 312 ? S Nov13 0:00 ./zbind
```

## OVH

```
root 993 0.0 0.6 2172 792 ? S< Nov13 0:00 /usr/local/etc/ncftpd/ncftpd -q
/usr/local/etc/ncftpd/general.cf /usr/local/etc/ncftpd/domain.cf
nobody 31185 0.0 2.3 8860 3020 ? S 04:02 0:00 /usr/local/apache/bin/httpd
-DHAVE_MMAP_STATIC -DHAVE_VHOST_ALIAS -DHAVE_ENV -DHAVE_LOG_CONFIG -DHAV
nobody 31186 0.0 2.2 8548 2868 ? S 04:02 0:02 /usr/local/apache/bin/httpd
-DHAVE_MMAP_STATIC -DHAVE_VHOST_ALIAS -DHAVE_ENV -DHAVE_LOG_CONFIG -DHAV
```

Un segundo basta para echar mano a la máquina y hacer lo que queramos con ella (siendo nobody).

```
# netstat -tanpu
Conexiones Internet activas (servidores y estaciones)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat PID/Program name
tcp 0 0 0.0.0.0:4000 0.0.0.0:* LISTEN 23121/zbind
tcp 0 0 0.0.0.0:56100 0.0.0.0:* LISTEN 24929/[httpd]
tcp 0 0 0.0.0.0:6667 0.0.0.0:* LISTEN 27877/[mingetty]
tcp 0 0 0.0.0.0:44464 0.0.0.0:* LISTEN 15181/cgi
tcp 0 0 0.0.0.0:1234 0.0.0.0:* LISTEN 20211/up2date
tcp 0 0 0.0.0.0:8888 0.0.0.0:* LISTEN 27778/sendmail: acc
tcp 0 0 0.0.0.0:12121 0.0.0.0:* LISTEN 628/perl

# openssl version

OpenSSL 0.9.6 24 Sep 2000
```

El hacker simplemente ha iniciado un bot-irc que se conecta a un servidor IRC.  
Utiliza los nombres estándar de los programas para disimular (sendmail, bind, httpd ...)

```
# netstat -tanpu
Conexiones Internet activas (servidores y estaciones)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat PID/Program name
tcp 0 0 0.0.0.0:4000 0.0.0.0:* LISTEN 23121/zbind
tcp 0 0 0.0.0.0:56100 0.0.0.0:* LISTEN 24929/[httpd]
tcp 0 0 0.0.0.0:873 0.0.0.0:* LISTEN 439/xinetd
tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN 602/mysqld
tcp 0 0 0.0.0.0:6667 0.0.0.0:* LISTEN 27877/[mingetty]
tcp 0 0 0.0.0.0:12589 0.0.0.0:* LISTEN 24933/crond
tcp 0 0 0.0.0.0:110 0.0.0.0:* LISTEN 655/tcpserver
tcp 0 0 0.0.0.0:143 0.0.0.0:* LISTEN 503/couriertcpd
tcp 0 0 0.0.0.0:44464 0.0.0.0:* LISTEN 15181/cgi
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 455/httpd
tcp 0 0 0.0.0.0:1234 0.0.0.0:* LISTEN 20211/up2date
tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN 639/ncftpd
tcp 0 0 213.186.35.181:53 0.0.0.0:* LISTEN 379/named
```

## OVH

```
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN 379/named
tcp 0 0 0.0.0.0:8888 0.0.0.0:* LISTEN 27778/sendmail: acc
tcp 0 0 0.0.0.0:25 0.0.0.0:* LISTEN 653/tcpserver
tcp 0 0 0.0.0.0:12121 0.0.0.0:* LISTEN 628/perl
tcp 0 0 0.0.0.0:443 0.0.0.0:* LISTEN 455/httpd
tcp 0 0 0.0.0.0:11230 0.0.0.0:* LISTEN 349/sshd
tcp 0 0 213.186.35.181:4228 202.134.0.13:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:4382 202.158.3.23:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:4223 202.134.0.13:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:1763 202.158.3.23:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:3761 208.37.46.246:6667 ESTABLISHED
27778/sendmail: acc
tcp 0 0 213.186.35.181:3497 195.47.220.2:6667 ESTABLISHED 20211/up2date
tcp 0 0 213.186.35.181:3349 62.93.214.24:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 240 213.186.35.181:11230 80.14.166.64:52198 ESTABLISHED 22035/sshd
tcp 0 0 213.186.35.181:1784 66.40.25.214:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:1529 202.158.3.23:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:3105 62.93.214.24:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:2789 202.158.3.23:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:4222 62.93.214.24:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:3556 202.134.0.13:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:3555 202.134.0.13:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:3562 202.134.0.13:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:3563 202.134.0.13:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:3568 202.134.0.13:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:4608 195.54.102.4:6667 ESTABLISHED
27877/[mingetty]
tcp 0 0 213.186.35.181:3550 202.134.0.13:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:3545 202.134.0.13:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:3547 202.134.0.13:6667 ESTABLISHED 27778/sendmail:
acc
tcp 0 0 213.186.35.181:3117 66.40.25.214:7000 ESTABLISHED 27778/sendmail:
acc
```

## Desconfie

El hacker puede haber dejado en crond el reinicio automático del shell que le permite el acceso al servidor. Hay que comprobarlo.

```
[root@nsXXXX /root]# cd /var/spool/cron/
[root@nsXXXX cron]# ls -l
total 20
[....]
-rw- 1 root nobody 225 nov 6 18:22 nobody
[...]
```

```
[root@ns3054 cron]# cat nobody
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (cron.d installed on Thu Nov 6 18:22:35 2003)
# (Cron version $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
* * * * * /tmp/.../y2kupdate >/dev/null 2>&1
```

```
[root@ns3054 cron]# rm nobody
rm: remove `nobody'? y
```

```
[root@ns3054 cron]# cd /tmp/...
```

```
[root@ns3054 ...]# ls -l
total 1436
-rw- 1 nobody nobody 18782 nov 17 10:23 c-leet
-rw- 1 nobody nobody 18389 nov 17 10:23 c-leet.old
drwxr-xr-x 2 nobody nobody 4096 nov 6 18:22 help
drwxr-xr-x 2 nobody nobody 4096 nov 17 10:26 log
drwxr-xr-x 2 nobody nobody 4096 nov 17 09:23 motd
-rwxr-xr-x 1 nobody nobody 14306 oct 2 2002 proc
-rw- 1 nobody nobody 7 nov 17 01:20 psybnc.pid
-rwxr-xr-x 1 nobody nobody 61 oct 2 2002 run
drwxr-xr-x 2 nobody nobody 4096 nov 6 18:22 scripts
-rw- 1 nobody nobody 5096 nov 17 01:23 USER10.LOG
-rw- 1 nobody nobody 4517 nov 11 15:15 USER10.LOG.old
-rw- 1 nobody nobody 15569 nov 11 16:44 USER11.LOG
-rw- 1 nobody nobody 6826 nov 11 09:55 USER12.LOG
-rw- 1 nobody nobody 4413 nov 11 09:55 USER13.LOG
-rw- 1 nobody nobody 4913 nov 11 09:55 USER14.LOG
-rw- 1 nobody nobody 6329 nov 11 09:55 USER15.LOG
-rw- 1 nobody nobody 4853 nov 11 09:55 USER16.LOG
-rw- 1 nobody nobody 5555 nov 11 09:55 USER17.LOG
-rw- 1 nobody nobody 5547 nov 11 09:55 USER18.LOG
-rw- 1 nobody nobody 6348 nov 11 09:55 USER19.LOG
-rw- 1 nobody nobody 217 nov 17 07:46 USER1.LOG
-rw- 1 nobody nobody 7465 nov 11 09:55 USER20.LOG
```

## OVH

```
-rw- 1 nobody nobody 79916 nov 17 01:23 USER21.LOG
-rw- 1 nobody nobody 12454 nov 17 06:15 USER22.LOG
-rw- 1 nobody nobody 7383 nov 17 01:24 USER23.LOG
-rw- 1 nobody nobody 7440 nov 17 01:24 USER24.LOG
-rw- 1 nobody nobody 8482 nov 17 01:24 USER25.LOG
-rw- 1 nobody nobody 14006 nov 17 01:25 USER26.LOG
-rw- 1 nobody nobody 6877 nov 13 08:39 USER27.LOG
-rw- 1 nobody nobody 5868 nov 17 09:52 USER28.LOG
-rw- 1 nobody nobody 1138 nov 12 08:53 USER29.LOG
-rw- 1 nobody nobody 145857 nov 17 01:20 USER2.LOG
-rw- 1 nobody nobody 11362 nov 11 07:14 USER2.LOG.old
-rw- 1 nobody nobody 7319 nov 17 05:31 USER30.LOG
-rw- 1 nobody nobody 1221 nov 9 19:43 USER31.LOG.old
-rw- 1 nobody nobody 1029 nov 8 18:14 USER32.LOG
-rw- 1 nobody nobody 10805 nov 17 09:42 USER33.LOG
-rw- 1 nobody nobody 2728 nov 10 17:16 USER34.LOG
-rw- 1 nobody nobody 714 nov 8 06:08 USER35.LOG
-rw- 1 nobody nobody 2523 nov 8 11:19 USER36.LOG
-rw- 1 nobody nobody 11573 nov 11 10:20 USER37.LOG
-rw- 1 nobody nobody 2997 nov 17 01:26 USER38.LOG.old
-rw- 1 nobody nobody 1933 nov 12 17:19 USER39.LOG
-rw- 1 nobody nobody 8091 nov 11 17:31 USER39.LOG.old
-rw- 1 nobody nobody 4444 nov 17 01:49 USER3.LOG
-rw- 1 nobody nobody 5966 nov 7 18:24 USER3.LOG.old
-rw- 1 nobody nobody 2107 nov 17 09:19 USER4.LOG
-rw- 1 nobody nobody 3488 nov 13 07:43 USER4.LOG.old
-rw- 1 nobody nobody 19687 nov 17 01:49 USER6.LOG
-rw- 1 nobody nobody 156789 nov 17 07:03 USER7.LOG
-rw- 1 nobody nobody 27105 nov 17 07:17 USER8.LOG
-rw- 1 nobody nobody 1475 nov 17 04:08 USER9.LOG
-rw- 1 nobody nobody 1265 nov 13 05:25 USER9.LOG.old
-rwxr-xr-x 1 nobody nobody 593336 oct 2 2002 vi
-rwxr-r- 1 nobody nobody 164 nov 6 18:22 y2kupdate
```

```
[root@ns3054 ...]# cd ..
```

```
[root@ns3054 /tmp]# tar cvfz hack.tar.gz ...
```

```
.../
.../vi
.../log/
.../log/psybnc.log
.../log/psybnc.log.old
.../run
.../help/
.../help/SWITCHNET.TXT
.../help/JUMP.TXT
.../help/ADDNETWORK.TXT
.../help/DELSERVER.TXT
.../help/PASSWORD.TXT
.../help/ADDSERVER.TXT
.../help/LISTSERVERS.TXT
```

```
.../help/DELNETWORK.TXT
.../help/SOCKSTAT.TXT
.../help/BCONNECT.TXT
.../motd/
.../motd/USER10.MOTD.old
.../motd/USER3.MOTD
.../motd/USER4.MOTD.old
.../motd/USER3.MOTD.old
.../motd/USER4.MOTD
.../motd/USER7.MOTD
.../motd/USER6.MOTD.old
.../motd/USER2.MOTD.old
.../motd/USER2.MOTD
.../motd/USER1.MOTD
.../motd/USER14.MOTD.old
.../motd/USER18.MOTD.old
.../motd/USER9.MOTD.old
.../motd/USER32.MOTD.old
.../motd/USER11.MOTD.old
.../motd/USER5.MOTD
.../motd/USER9.MOTD
.../motd/USER16.MOTD.old
.../motd/USER5.MOTD.old
.../motd/USER12.MOTD.old
.../motd/USER34.MOTD.old
.../motd/USER20.MOTD.old
.../motd/USER19.MOTD.old
.../motd/USER26.MOTD
.../motd/USER28.MOTD.old
.../motd/USER31.MOTD.old
.../motd/USER27.MOTD.old
.../motd/USER7.MOTD.old
.../motd/USER29.MOTD.old
.../motd/USER6.MOTD
.../motd/USER30.MOTD.old
.../motd/USER36.MOTD.old
.../motd/USER21.MOTD
.../motd/USER38.MOTD.old
.../motd/USER39.MOTD.old
.../motd/USER26.MOTD.old
.../motd/USER13.MOTD.old
.../motd/USER1.MOTD.old
.../motd/USER8.MOTD.old
.../motd/USER17.MOTD.old
.../motd/USER21.MOTD.old
.../motd/USER37.MOTD.old
.../motd/USER35.MOTD.old
.../motd/USER23.MOTD.old
.../motd/USER22.MOTD.old
.../motd/USER24.MOTD.old
.../motd/USER33.MOTD.old
```

```
.../motd/USER22.MOTD
.../motd/USER23.MOTD
.../motd/USER24.MOTD
.../motd/USER25.MOTD.old
.../motd/USER25.MOTD
.../motd/USER28.MOTD
.../motd/USER30.MOTD
.../motd/USER33.MOTD
.../motd/USER38.MOTD
.../motd/USER8.MOTD
.../motd/USER10.MOTD
.../motd/USER11.MOTD
.../motd/USER12.MOTD
.../motd/USER13.MOTD
.../motd/USER14.MOTD
.../motd/USER15.MOTD
.../motd/USER16.MOTD
.../motd/USER17.MOTD
.../motd/USER18.MOTD
.../motd/USER19.MOTD
.../motd/USER20.MOTD
.../motd/USER27.MOTD
.../motd/USER29.MOTD
.../motd/USER31.MOTD
.../motd/USER15.MOTD.old
.../proc
.../USER1.LOG
.../c-leet
.../scripts/
.../scripts/DEFAULT.SCRIPT
.../y2kupdate
.../psybnc.pid
.../c-leet.old
.../USER39.LOG
.../USER4.LOG.old
.../USER2.LOG
.../USER6.LOG
.../USER21.LOG
.../USER25.LOG
.../USER15.LOG
.../USER4.LOG
.../USER34.LOG
.../USER36.LOG
.../USER10.LOG
.../USER3.LOG.old
.../USER38.LOG.old
.../USER26.LOG
.../USER16.LOG
.../USER7.LOG
.../USER8.LOG
.../USER13.LOG
```

```
.../USER9.LOG  
.../USER11.LOG  
.../USER12.LOG  
.../USER14.LOG  
.../USER17.LOG  
.../USER18.LOG  
.../USER19.LOG  
.../USER20.LOG  
.../USER23.LOG  
.../USER22.LOG  
.../USER24.LOG  
.../USER28.LOG  
.../USER29.LOG  
.../USER30.LOG  
.../USER27.LOG  
.../USER33.LOG  
.../USER32.LOG  
.../USER35.LOG  
.../USER37.LOG  
.../USER3.LOG  
.../USER2.LOG.old  
.../USER39.LOG.old  
.../USER31.LOG.old  
.../USER10.LOG.old  
.../USER9.LOG.old
```

```
[root@ns3054 /tmp]# rm -rf ...
```

```
[root@ns3054 /tmp]# ps auxw | grep send  
root 643 0.0 0.2 1332 304 ? S Oct24 0:00 supervise qmail-send  
qmails 652 0.0 0.3 1396 404 ? S Oct24 0:12 qmail-send  
nobody 24481 0.2 1.8 3704 2276 ? S 01:20 1:33 sendmail: accepting  
connections  
root 6196 0.0 0.5 1796 744 pts/3 R 10:27 0:00 grep send
```

```
[root@ns3054 /tmp]# kill -9 24481
```

### Mas información

: ServidorSemihackeado2 :: El ejemplo del 29/09/2004

: ServidorHackee :: Cuando el servidor sufre el ataque de un hacker.

: ServidorInfectado :: Cuando el servidor se contagia con un troyano o un virus.