Incidenti di sicurezza

Roberto Cecchini
INFN Firenze

III Incontro di GARR-B
Firenze 24-25 Gennaio 2001

Tipi di attacchi

- Vulnerabilità del software installato:
  - buffer overflow, backdoor, ...
- Vulnerabilità dei protocoli di rete (IPv4 non è stata progettata pensando alla sicurezza, con IPv6 le cose dovrebbero andare meglio...):
  - spoofing, session hijacking, man-in-the-middle, sniffing, analisi del traffico;
  - denial of service (DoS):
    - mail bombing, SYN flood, ping flood, ecc..
- *Social Engineering*.

Protezioni e controlli

- Host
  - strumenti di intrusion detection e controllo
    - **COPS**, **Tiger**, **aide**, **wots**, ...
  - "personal" firewall
    - **ipf**, **ipchains**, ...
  - scanner (port e vulnerability)
    - **nmap**, **sara**, **nessus**, ...
- Reti locali
  - firewall;
  - sistemi di network intrusion detection:
    - **snort**, **shadow**, **argus**, **arpwatch**, ...
- Protocolli di comunicazione
  - IPSec, SSH, SSL/TLS, PGP, S/MIME, ...

Metodi più comuni di accesso

- Vulnerabilità più di moda (al momento):
  - ftpd;
  - telnetd;
  - rpc;
  - LPRng;
  - mountd;
  - bind;
  - imap/pop;
  - ftp anonimo (*warez*).
- Password “rubate”:
  - una volta ottenuto l’accesso, anche non privilegiato, è **molto** facile diventare **root** (e non solo su Linux!);
  - ben più della metà delle compromissioni segnalate hanno seguito questa strada.

Modus operandi (1/2)

- Compromissione:
  - da remoto:
    - utilizzo di un exploit su un servizio (ad es. **ftp**) con ottenimento shell di root;
  - da locale:
    - login come utente legittimo;
    - scarico via rete programma di exploit (ad es. da ftp.technotronix.com);
    - compilazione, esecuzione e ottenimento shell di root.
- Compilazione e installazione *rootkit.*
- Installazione altre *backdoor*
  - shell suid in directory utente
  - attivazione di servizi di rete
  - creazione di nuovi utenti
  - ...

Modus operandi (2/2)

- Cancellazione tracce:
  - ripulitura file di log;
  - shell history in */dev/null*
- Attività preferite:
  - sniffer:
    - interfaccia generalmente in modo promiscuo (ma non necessariamente);
  - bot IRC:
    - elevato traffico tcp;
    - attività apparentemente da nodi che non esistono (*mirkforces*);
  - scansioni;
  - DoS:
    - elevato traffico icmp (ma non necessariamente);
  - ponte per attacchi ad altri nodi (in special modo sulla stessa LAN).

Ci sono ospiti?

- Ho ricevuto segnalazioni di attività sospette proveniente dalla mia macchina:
  - scansioni;
  - traffico ICMP;
  - ecc., ecc..
- La macchina si comporta in modo strano:
  - molto lenta, ma con **ps** (o **top**) non si vede nulla di particolare;
  - uno o più filesystem sono pieni, ma non riesco a scoprire perché;
  - i file di log sembrano incompleti o sono addirittura scomparsi;
  - il traffico in rete è molto elevato;
  - login ad ore strane e/o da nodi sconosciuti;
  - ecc. ecc.

Alla ricerca dell'intruso e delle *backdoor*

- Alcune utility di sistema potrebbero essere state "addomesticate" (*rootkit*):
  - un *rootkit* è un package con versioni modificate di tutte le principali utility: scaricato, compilato e installato dall'intruso.
    - **chsh, passwd**, **login**: permettono di diventare **root;**
    - **du**, **find**, **ls**: nascondono alcuni file e directory;
    - **ifconfig**: non mostra il flag di modo promiscuo;
    - **netstat**: nasconde particolari connessioni;
    - **ps**, **top**: nascondono certi processi;
    - **syslogd**: non scrive su syslog certe stringhe;
    - shared library di sistema;
    - programmi per modificare i log di sistema;
    - i file di controllo spesso in */dev* con nomi "strani", ad es. " ", ".. ", "...", ecc.;
  - per scoprirlo:
    - file integrity checker (ad es. **aide**), **attenzione alle shared library**;
    - **chkrootkit**;
    - confronto con un sistema identico;
    - CD Rom di emergenza (ad es. home made, **rip** o **tomsrtbt**).

Controllo filesystem (1/2)

- File **setuid** o **setgid** in directory utente

```
find / -type f -a \( -perm -4000 -o -perm -2000 \) \
   -exec ls -lg {} \;
```

- File regolari in */dev*
  - alcuni rootkit hanno i file di configurazione in ***/dev/pty****
  - spesso i **bot irc** si trovano in ***/dev/...*** (o varianti)
- *.rhosts*, *hosts.equiv, .shosts, ecc.*
  - attenzione ai **+** e ai **#** (non esistono caratteri di commento!)
- *.login*, *.logout*, *.profile*, *.cshrc, .forward*
  - comandi “strani”?
- */etc/passwd*
  - nuovi account;
  - account di sistema non disabilitati (come dovrebbero essere);
  - account con uid/gid errati e/o 0;
  - account vecchi con nuove password.

Controllo filesystem (2/2)

- *inetd.conf*
  - servizi non richiesti, anche apparentemente innocui;
- **crontabs** e **at-jobs**
- file di startup (*rc.local*, *sh.login*, ecc.)
  - è stato cambiato il PATH? (ad esempio aggiungendo “.”)
- file modificati di recente
  - ad es. i file modificati da non meno di 1 giorno, ma non più di 2:
    ```
    find / -ctime -2 -ctime + 1 -exec ls -lg {} \;
    ```
- ftp anonimo
  - è stato abilitato?
  - sono stati modificati i permessi delle directory?

Controllo processi

- Presenza di sniffer
  - **ifconfig** (se non modificato) lo dovrebbe segnalare

```
# ifconfig eth0
eth0   Link encap:Ethernet  HWaddr 00:60:08:92:CF:79
 inet addr:132.83.135.18  Bcast:132.83.135.255 Mask:255.255.255.0
 UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
 RX packets:157127188 errors:20787 dropped:20787 overruns:26633
 TX packets:4960510 errors:0 dropped:0 overruns:0
 Interrupt:11 Base address:0x6400
```

  - **ifstatus**
  - filesystem in rapida crescita;
  - antisniffer? [**security.fi.infn.it/conferenze/fi00/**]
- Processi attivi
  - spesso con nomi innocenti: ad es. **ps** o addirittura “ “

Controllo connessioni di rete (1/5)

- Connessioni da/verso nodi insoliti?
  - controllate i logfile locali e dell'eventuale Network Intrusion Detection System
    - ad esempio **argus**

```
ra -r argus.out -c host VITTIMA
```

```
08/11 20:49:36 *  tcp  RETEVISION.1031   ->      VITTIMA.23    1550  1505   56659   41352   CLO
08/11 20:50:51    tcp     VITTIMA.1067   -> TECHNOTRONIC.21    26    19     141     1332    CLO
08/11 20:51:12    tcp     VITTIMA.1068  <-  TECHNOTRONIC.20    4     5      0       2451    CLO
08/11 21:14:59    tcp     VITTIMA.1071   ->       BAROLO.21    20    16     109     410     CLO
08/11 21:15:10    tcp     VITTIMA.1072  <-        BAROLO.20    6     9      0       8145    CLO
08/11 21:26:25 *  tcp RETEVISION2.1028   ->      VITTIMA.23    2405  2362   1658    146227  CLO
08/11 21:29:47    tcp     VITTIMA.1080   ->      TITANIA.23    283   239    161     13700   CLO
08/11 21:29:47    tcp     TITANIA.26862  ->      VITTIMA.113   5     5      9       36      CLO
08/11 22:40:11 *  tcp RETEVISION2.1053   ->      VITTIMA.23    4938  5342   458935  90861   CLO
08/11 23:07:27 s  tcp     VITTIMA.1143   o>         IRC1.6667  2     0      0       0       TIM
08/11 23:10:22    tcp     VITTIMA.1147  <|          IRC2.6667  1     1      0       0       RST
08/11 23:10:56 d  tcp     VITTIMA.1152   ->         IRC3.6667  169   179    1367    14136   CLO
08/11 23:10:57    tcp        IRC3.22133  ->      VITTIMA.113   5     5      13      39      CLO
08/11 23:24:23 *  tcp     VITTIMA.1168   |>         IRC4.6667  143   125    884     11665   RST
08/11 23:24:24    tcp        IRC4.4531   ->      VITTIMA.113   7     6      169     38      CLO
```

Controllo connessioni di rete (2/5)

- Connessioni di rete sospette? **netstat** & **lsof**
  - che connessioni sono attive?

```
# netstat -a
Proto Recv-Q Send-Q  Local Address  Foreign Address     State
tcp        0      0     *:sunrpc          *:*           LISTEN
tcp        0      0     *:auth            *:*           LISTEN
tcp        0      0     *:ssh             *:*           LISTEN
tcp        0     20  host:ssh       pcc.es:4325   ESTABLISHED
udp        0      0     *:syslog          *:*
udp        0      0     *:sunrpc          *:*
udp        0      0     *:2345            *:*
# lsof -i | grep 2345
nc   12112 root    3u  inet 0x01437018     0t0  UDP *:2345
```

  - quale processo ha aperto una connessione con **host2**?

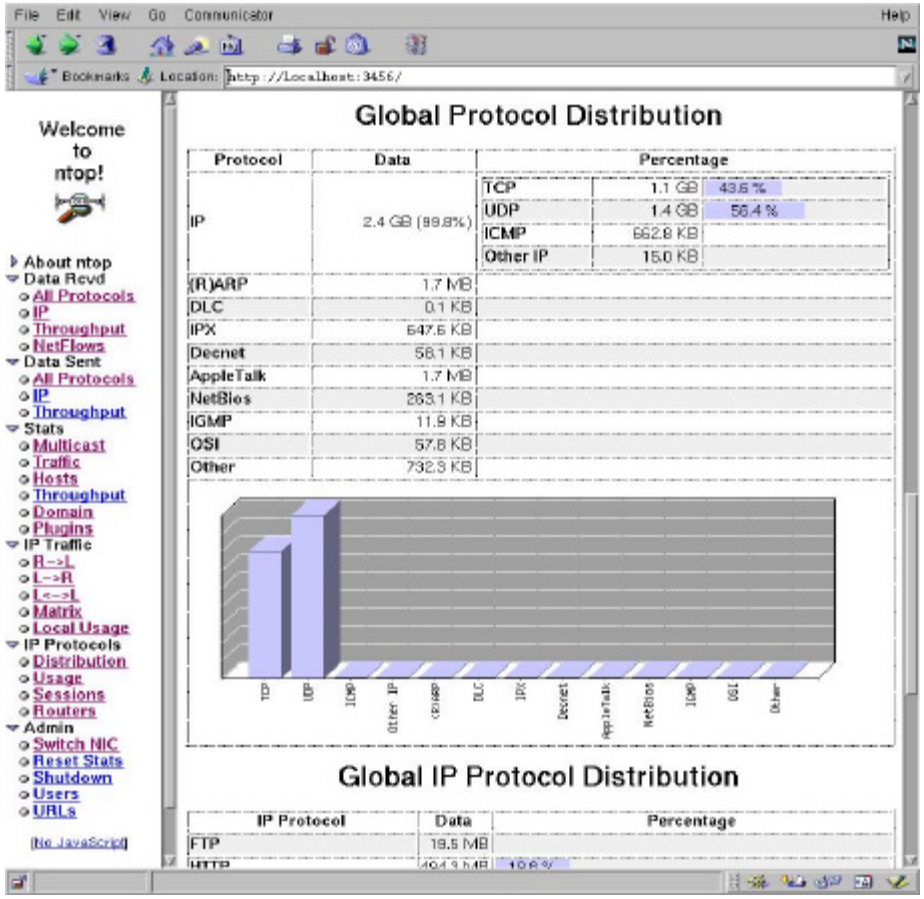
```
lsof -i | grep host2
ps  28637 root inet TCP host1:1768 -> host2:1456 (ESTABLISHED)
```

  - che file sta usando **ps**?

```
lsof | grep ps
ps  28637 root cwd  VDIR 31,0x5000  3072  10240 /dev/ttyq2
```

Controllo connessioni di rete (3/5)

- Traffico in rete elevato?
  - controllate con **ntop**
    - multipiattaforma
    - molti tipi di report
      - per host
        - » data sent/received
        - » traffic distribution ...
      - globali
        - » connessioni aperte
        - » traffic matrix ...
    - possibilità di generare allarmi e/o azioni
  - usate uno sniffer
    - **tcpdump**
    - **ethereal**



Controllo connessioni di rete (4/5)

- Su che porte sto ascoltando?
  - fate una scansione (da un altro nodo) con **nmap**

```
#nmap -sS -p1-64000 yy.yy.yy
```

Port	State	Service
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
111/tcp	open	sunrpc
139/tcp	open	netbios-ssn
515/tcp	open	printer
847/tcp	open	unknown
942/tcp	open	unknown
1036/tcp	open	unknown
1043/tcp	open	unknown
2121/tcp	open	unknown
2788/tcp	open	unknown
2819/tcp	open	unknown
5280/tcp	open	unknown
6010/tcp	open	unknown
6011/tcp	open	unknown
6018/tcp	open	unknown
6023/tcp	open	unknown
7000/tcp	open	afs3-fserver

```
#nmap -sUR -p1-64000 yy.yy.yy
```

Port	State	Service
53/udp	open	domain
67/udp	open	bootps
69/udp	open	tftp
111/udp	open	sunrpc
123/udp	open	ntp
135/udp	open	loc-srv
137/udp	open	netbios-ns
138/udp	open	netbios-dgm
177/udp	open	xdmcp
514/udp	open	syslog
806/udp	open	unknown
855/udp	open	unknown
1357/udp	open	pegboard
2049/udp	open	nfs
2345/udp	open	unknown
2687/udp	open	unknown
2865/udp	open	unknown

Controllo connessioni di rete (5/5)

- **nfs:** esportate (e importate) solo il dovuto?

```
# showmount -e
export list for vittima:
/home/brz       whp.in.it,ftr.in.it
/usr            (everyone)
# showmount -a
hacker.org:     /usr
whp.in.it:      /home/brz
```

- **rpc**: sono stati aggiunti servizi?

```
# rpcinfo -p
100000    2   tcp    111  portmapper
100000    2   udp    111  portmapper
100024    1   udp    845  status
100024    1   tcp    847  status
100021    1   tcp    851  nlockmgr
100020    1   udp   1043  llockmgr
100020    1   tcp    860  llockmgr
100083    1   tcp   1036  ttdbserver
100005    1   udp    940  mountd
100005    1   tcp    942  mountd
100003    2   udp   2049  nfs
100068    2   udp   1046  cmsd
100068    2   tcp    853  cmsd
```

Mi hanno compromesso! (1/2)

- Staccate la macchina dalla rete e lavorate in single user
  - potrebbe essere meglio staccare la corrente!
- Provate a seguire le tracce dell'intruso:
  - *messages, xferlog, wtmp, maillog, secure, ecc.*
    - **molto** consigliabile che i file di log vengano salvati anche su un'altra macchina
  - shell history file.
- Fate un backup il più completo possibile (anche ai fini legali)
  - in alternativa smontate (e conservate) il disco;
  - *computer forensics* (ad es. **The Coroner's Toolkit**).

Mi hanno compromesso! (2/2)

- Cercate di scoprire come è entrato l'intruso
- Modificate **tutte** le password
- Se l'intruso è diventato **root** (cosa abbastanza probabile...)
  - reinstallate il sistema operativo (all'ultima versione e all'ultima patch!)
    - è **molto** difficile altrimenti essere sicuri che non siano rimaste backdoor
  - controllate l'esistenza di file **suid/gid** nelle directory utente
  - attenzione a riutilizzare i vecchi file di configurazione
- Quali altre macchine potrebbero essere state compromesse?
  - usavate *.rhost* (o simili)?
  - che accessi sulla rete locale sono stati fatti durante la compromissione?

Segnalate l'incidente

- Inviate un mail a **cert@garr.it** (o riempite il modulo online su **www.cert.garr.it**)
  - data e ora (con timezone e precisione del vostro clock)
  - descrizione dell'incidente
  - come essere contattati
  - estratti dai log e file lasciati dall'intruso
    - **se oltre 500k non li spedite, limitatevi a dire che li avete: verrete richiamati**
  - permesso (o diniego) di diffondere la vostra identità
- Riceverete un mail di conferma apertura incidente e verrete tenuti aggiornati sugli sviluppi fino alla chiusura
- Se preferite il fai-da-te contattate direttamente i responsabili dei siti da cui è venuto l'attacco

Bibliografia (1/2)

- Collezione di tools (free):
  - http://www.whitehats.com/
  - http://www.technotronics.com/
- **COPS**: ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/cops/
- **Tiger**: ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/tiger/
- **aide**: http://www.cs.tut.fi/~rammer/aide.html
- **chkrootkit:** http://www.chkrootkit.org/
- **rip**: http://www.tux.org/pub/people/kent-robotti/looplinux/rip/
- **tomsrtbt**: http://www.toms.net/rb/
- **argus**: ftp://ftp.sei.cmu.edu/pub/argus
- **snort:** http://www.snort.org/
- **arpwatch:** ftp://ftp.ee.lbl.gov/
- **lsof**: ftp://vic.cc.purdue.edu/pub/tools/unix/lsof
- **ifstatus:** ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/ifstatus/

Bibliografia (2/2)

- **ntop**: http://www.ntop.org/
- **tcpdump**: http://www.tcpdump.org/
- **ethereal**: http://www.ethereal.com/
- **nmap**: http://www.insecure.org
- The Coroner's Toolkit: http://www.porcupine.org/forensics/
- http://www.cert.org/security-improvement/
- http://www.cert.garr.it/documenti/
- http://security.fi.infn.it/documenti/