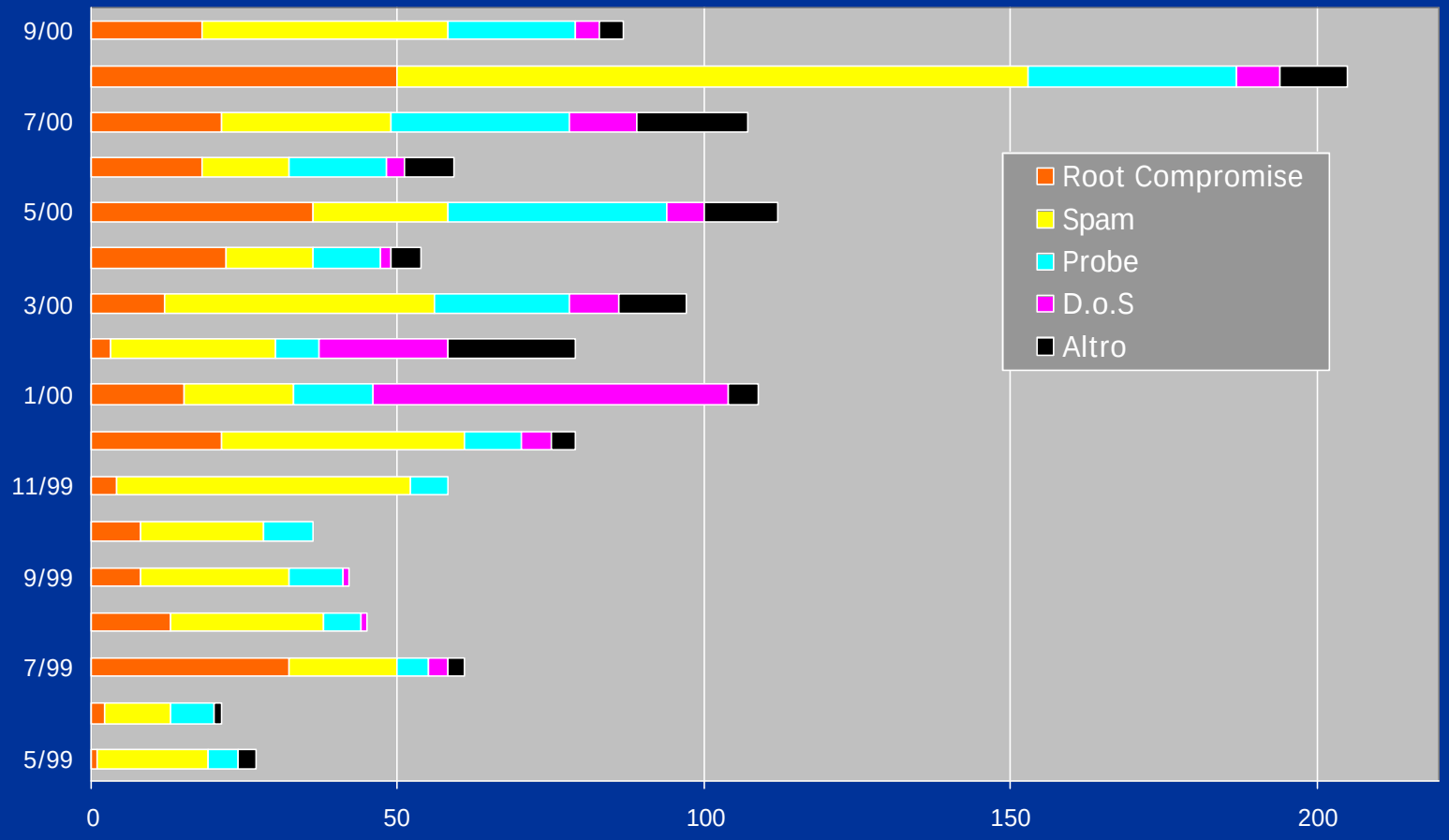
Gestione incidenti di sicurezza

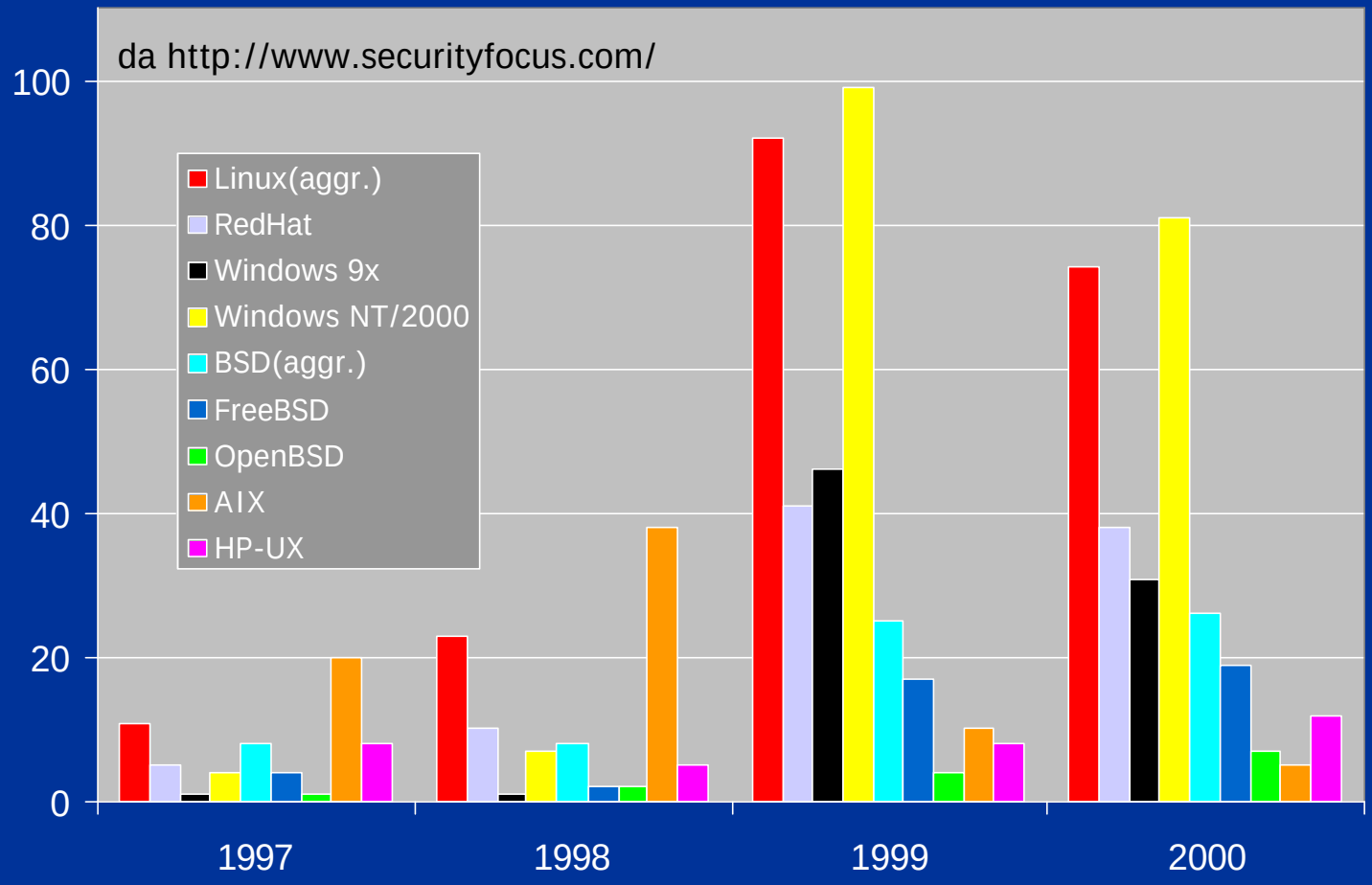
Roberto Cecchini
INFN, Sezione di Firenze

I INFN Security Workshop
Firenze 19-20 Settembre 2000

Incidenti segnalati a GARR-CERT



Vulnerabilità scoperte (da Bugtraq)



Mi hanno compromesso?

- Ho ricevuto segnalazioni di attività sospette proveniente dalla mia macchina
- La macchina si comporta in modo strano
  - molto lenta, ma **top** non segnala nulla di particolare
  - uno o più fs 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
  - ecc. ecc.

Alla ricerca dell'intruso e delle backdoor

- Alcune utility di sistema potrebbero essere 'addomesticate'
  - un *rootkit* è un package con versioni modificate di tutte le principali utility, viene scaricato e installato dall'intruso. Ad esempio:
    - **chsh, passwd**: permettono di diventare **root**
    - **du**, **find**, **ls**: nascondono alcuni file e directory
    - **ifconfig**: non mostra il flag di modo promiscuo
    - **login**: permette login come **root**
    - **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
  - per scoprirlo il modo più sicuro è con un file integrity checker (ad es. **tripwire**) o confrontandole con quelle di un sistema identico

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”?
- *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**
    - http://security.fi.infn.it/tools/ifstatus/
  - filesystem in rapida crescita
- Processi attivi
  - spesso con nomi innocenti: ad es. ps o addirittura “ “

Controllo connessioni di rete (1/3)

- Connessioni da/a nodi insoliti?
  - controllate i logfile locali e del NIDS (ad es. **argus**)
- Connessioni di rete sospette?
  - **netstat** & **lsof**

```
# netstat -a
Active Internet connections (including servers)
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 fa.it:ssh          pcc.es:906        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
```

- Traffico in rete elevato?
  - controllate con **ntop**

Controllo connessioni di rete (2/3)

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

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

Port	State	Service (RPC)
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-fileserver

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

Port	State	Service (RPC)
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
845/udp	open	unknown
855/udp	open	unknown
1357/udp	open	pegboard
2049/udp	open	nfs
2121/udp	open	unknown
2345/udp	open	unknown
2687/udp	open	unknown
2865/udp	open	unknown

Controllo connessioni di rete (3/3)

- **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
program vers proto   port
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!

- Staccate la macchina dalla rete e lavorate in single user
  - potrebbe essere meglio staccare la corrente!
    - esistono programmi che cancellano il sistema se cade la connessione di rete
- Provate a seguire le tracce dell'intruso (non fatevi troppe illusioni, ma qualche volta l'hacker è distratto...):
  - *messages, xferlog, wtmp, maillog, ecc.*
    - **molto** consigliabile che il file di log venga salvato anche su un'altra macchina perchè di solito viene ripulito
  - shell history file
- Fate un backup il più completo possibile (anche a fini legali)

Mi hanno compromesso!

- 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 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 http://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
- Valutate l'ipotesi di una denuncia alla Polizia Postale
- Se preferite il fai-da-te contattate direttamente i responsabili dei siti da cui è venuto l'attacco (trovati con **whois**)

Migliorare la sicurezza: account

- Eseguite **crack** periodicamente sui vostri file di password: di solito trova almeno 1/3 delle password!
- Controllate periodicamente che gli account vengano usati e disabilitateli in caso contrario, o, meglio, createli con una data di scadenza.
- Valutate la possibilità di usare le *shadow password*.
- verificate che il PATH non contenga **.**
- Account speciali (ad es. **bin**):
  - disabilitateli mettendo `/bin/false` come shell in */etc/passwd*.
- Account di **root**:
  - disabilitate il login tranne che da console *(/etc/ttys* o */etc/ttytab*): usate **ssh** e **su**;
  - controllate che tutti i file eseguiti durante il login e da **cron** siano di root e non siano scrivibili dal mondo.
- Disabilitate l'accesso ftp a tutti gli account di sistema (*/etc/ftpusers*).

Migliorare la sicurezza: **Yellow Pages**

- **Fatene a meno se possibile!**
  - valutare l'opportunità di sostituirlo con una serie di script (ad es. usando **rsync** e **ssh**)
- Usate nomi di dominio non facilmente indovinabili
- Accertatevi che la riga che comincia con **+** in */etc/passwd* sia solo sulle macchine client

Migliorare la sicurezza: macchine "fidate"

- **Meglio non averne nessuna!**
- Se proprio non potete farne a meno
  - usate **ssh**
  - cercate di ridurre al minimo le macchine da cui si accettano login senza autorizzazione, in ogni caso **mai** esterne alla LAN
  - Utilizzate */etc/hosts.equiv* e proibite l'uso di *~/.rhosts* (anche per **root**!)
    - *hosts.equiv* deve essere di root e con permesso 600
    - non esistono caratteri di commento in questi fle!
- Non usate *.netrc*

Migliorare la sicurezza: **server web**

- Lasciare in *cgi-bin* solo gli script che servono effettivamente: **preferibilmente nessuno!**:
  - esistono script distribuiti con vecchie versioni dei server con ben note vulnerabilità, ad es. **phf**, **cgi-count**, **test**, ecc.
  - filtrate i caratteri in input passati agli script CGI
- Non fate girare il server come **root,** ma come un utente non privilegiato.
- Permettete solo a **root** l'accesso alle directory di configurazione e di log
- Non abilitate gli *upload* via ftp anonimo sul server web, o, alla peggio, non consentite a **www** l'accesso alla directory di upload.
- Analizzate periodicamente i file di log
- Per saperne di più: **http://security.fi.infn.it/documenti/**

Migliorare la sicurezza: **nfs**

- Il servizio è intrinsecamente insicuro: basato sull'ID e GID dell'utente remoto.
- Mai esportare un filesystem al mondo!
  - attenzione ad ***/etc/exports***: nel caso seguente ***/usr*** è esportato al mondo:

```
/usr
/home/brz -access=whp.in.it,ftr.in.it
```

- Non consentite l'accesso remoto come **root**
  - keyword **`root=`** in ***/etc/exports***
- In */etc/exports* usate solo nomi completi e **mai** il server o **`localhost`**
- Usate **fsirand** periodicamente (prima di montare i filesystem)
- Attenzione a cosa **importate** (*/etc/fstab* o */etc/amd.conf*)
  - usate **`nosuid`** se potete
- Filtrate sul router le porte 111 e 2049 (tcp e udp).

Migliorare la sicurezza: **rpc**

- Servizi attivi (via **portmapper**):

```
# rpcinfo -p
   program vers proto   port
   100000    2   tcp    111  rpcbind
   100000    2   udp    111  rpcbind
   100024    1   udp    815  status
   100024    1   tcp    817  status
   100021    1   tcp    821  nlockmgr
   100020    1   udp   1048  llockmgr
   100068    5   udp   1051
   100005    1   udp    899  mountd
   100003    2   udp   2049  nfs
```

- Eliminate i servizi che non servono, in particolare:
  - **rexd** (**sempre!**)
    - *senza autenticazione* (o meglio l'autenticazione è dal lato **client**)
  - **statd** (o **status**) e **mountd** (se non usate NFS)

Migliorare la sicurezza: **ftp**

- Se possibile disabilitate la feature SITE EXEC
- Disabilitare l'accesso (*/etc/ftpusers*) agli account di sistema
- FTP anonimo:
  - per disabilitarlo eiminare la riga con ftp in */etc/passwd*
  - accertarsi che non ci siano interpreti di comandi (p.e. shell o perl) che possano essere eseguiti da SITE EXEC (in *~ftp/bin*, *~ftp/usr/bin*, *~ftp/sbin*, ecc.)
  - la shell dell'user ftp deve essere invalida:
    ```
    ftp:*:400:400:Anonymous FTP:/home/ftp:/bin/false
    ```
  - meglio non avere directory scrivibili, in caso devono essere di **root** con permesso **rwx-wx-wt**
  - altre regole su **http://www.cert.org/**

Migliorare la sicurezza: file system

- Script setuid: non ne esistono di sicuri, usate **super** o **sudo**
- Settate il bit **sticky** sulle directory pubbliche (**`chmod o+t`**)
  - gli utenti non possono cancellare e rinominare i file di altri utenti
  - in particolare ***/tmp*** deve essere di **root:system**.
- Settate il bit **setgid** sulle directory pubbliche (**`chmod g+s`**)
  - il gid dei nuovi file è quello della directory
- Controllate che i file con i bit **suid** o **sgid** siano legittimi.
- Controllate file e directory scrivibili dal gruppo e dal mondo

```
find / -type f \( -perm -2 -o -perm -20 \) - exec ls -lg {} \;
find / -type g \( -perm -2 -o -perm -20 \) - exec ls -lg {} \;
```

- Ccontrollate gli **umask**: quello di **root** deve essere almeno 0x22.
- Devices
  - ***/dev/mem*** e ***/dev/kmem*** non devono essere leggibili dal mondo
  - quasi tutti i device devono essere di **root** (eccezione i terminali)
  - attenzione ai file normali in /***dev***!
- Se possibile montate i file system **non-setuid** e read-only.

Migliorare la sicurezza: altri servizi

- **named**
  - vi serve proprio?
  - proibite gli *zone transfer* (tranne che verso i server secondari)
  - filtrate sul router la porta 53 (tcp e udp)
- **/etc/inetd.conf**
  - commentate tutte le righe tranne quelle indispensabili. In particolare:
    - **echo**, **chargen** (attacchi DoS)
    - **finger** (o al massimo sostituitelo con **safe-finger**), **who**, **systat**
    - **uucp**
- **snmp**
  - almeno non usate *public* come dominio
- **gated**
  - se le vostre route sono statiche, configuratele allo startup
- **syslogd**
  - se possibile mandate una copia dei messaggi su di un'altra macchina

```
*.info;mail.none;authpriv.none      /var/log/messages
*.info;mail.none;authpriv.none      @loghost
authpriv.*                          /var/log/secure
authpriv.*                          @loghost
mail.*                              /var/log/maillog
*.emerg                             *
*.emerg                             @loghost
```