run secure || die()

Guido Bolognesi
guido@kill-9.it
http://www.kill-9.it/guido

Presentazione

- Relatore
- Partecipanti
- Prerequisiti
- Minisondaggio
- Perché questo talk?
- host security?

Security break-in

Fanno sorgere problemi diversi:

- integrità dei propri dati
  - Defacement
  - code di posta
  - spool degli articoli
- traffico generato dalla macchina (testa di ponte)

Come succede?

- installazioni di default
- configurazioni di default
- errori di configurazione
- bug applicativi (phpnuke anyone?)

quindi

- remote exploit
- local escalation

Perché succede?

- Per curiosità (sfida)
- Per divertimento
- Per fare danni (personali o vandalismo)
- Per caso (mass rooter, mass defacement)

Quindi...

Quindi a me non succede!

Ahaahahah!

Come riduco il rischio?

Utilizzando piattaforme “intelligenti”

- SPARCv8/9 (Solaris, *BSD, Linux, OpenSTEP, ...)
- Alpha (Tru64, *BSD, Linux, WinNT :D)
- HP-PA (HP-ux, Linux, *BSD)
- IA64 (?) / AMD64 (tutto)

(controllo dell'esecuzione per pagina di memoria, ad esempio)

Come riduco il rischio? (2)

NON utilizzando piattaforme “stupide”

- i386
- MIPS (Sgi)
- PowerPC (Rs/6000, Mac)
- ARM...

Come riduco il rischio? (3)

Sistema operativo “esotico”

+

Piattaforma insolita

=

MOLTI meno binary exploit

(e shellcode diverso)

QUINDI molti meno kiddies (80%)

Come riduco il rischio? (4)

La diversità é vita!

Linux

solaris

*BSD

MacOsX

Attacchi comuni

Verso i servizi esposti ad Internet

- web: apache, php, sql, upload file, proxy
- posta: spam & co.
- ssh
- ftp
- nntp

Attacchi comuni, esempi

Web:

- GET /scripts/nsiislog.dll
- GET /scripts/..%255c%255c..

/winnt/system32/cmd.exe?/c+dir (e fratelli)

- GET /_vti_bin/.%252e.....
- POST http://<ip>:25/ HTTP/1.1
- SEARCH /\x90\x02\xb1\x02\xb1\x02\xb1\x02....

Upload di script per shell, ...

Attacchi comuni, esempi (2)

Posta:

- name=“message.scr”
- application/x-msdownload; name=“Q234711.exe”
- audio/x-wav; name="bqwzq.com"

Ftp:

a parte gli exploit binari (wu-ftpd?)

Command.txt

SITE EXEC echo s | format c:\ /u

Cosa ci posso fare?

Cercare di limitare i danni:

hardening del sistema operativo, più:

- chroot()
- jail()
- UML
- Partizioni di sistema (S/390, Solaris)
- vmware

Hardening dell'OS

userspace

- rimozione servizi/utenti inutili/non sicuri
- suid, log, fdescriptor, fs in ro
- controllo versioni/bug sw installato

kernel space

- eventuali patch (grsec, angel, ...)
- sysctl / securelevel

chroot

Limita la visibilità del filesystem host da parte dell'applicativo in chroot

```
int chroot(const char *dirname);
```

- Più difficile entrarci (poco sw)
- Difficile, ma non impossibile, uscirci (compilatore/interprete, suid)
- Non é POSIX

chroot, a cosa serve?

- Protegge in misura maggiore dai bug applicativi e binary exploit (se non esistesse /bin/sh?)
- Limita la visibilità del filesystem fisico della macchina
- Relativamente semplice da creare

E` il caso di non far girare applicativi da root (local privilege)

chroot, accorgimenti

- Va tenuta aggiornata insieme al sistema che la ospita
- Per installare il software si possono creare dei link simbolici in /
- Per poter fare il bind ad una porta, utilizzarne una >1024 e ridirigere a livello kernel

chroot, ambienti

Essendo solamente una syscall é piuttosto diffusa:

- [open, net, free]BSD
- linux
- Solaris, Irix, Tru64 ...

jail()

Disponibile per FreeBSD (e per linux)

- riproduce un ambiente completo, con tutti i vantaggi (e gli svantaggi - log)
- ha bisogno di un ip address
- permette di delegare root (dentro la jail)

jail() (2)

Dentro una jail

- No spoofing
- No binding a IN_ADDRANY
- No mknod
- No mount/unmount
- Niente accesso al kernel

UML (user mode Linux)

- Un kernel (o un programma?) per linux modificato, con utility in user-space per comunicare
- Rootfs completamente separato (via loop device)
- A tutti gli effetti una macchina virtuale completa dove sperimentare

UML (user mode Linux)

Pro:

- anche spazio processi separato
- facile backup/restore
- binari girano in modo nativo
- kernel recente (2.4 e 2.6)

Contro:

- solo per i386, SPARC

Partizioni di sistema: VM

Linux può essere fatto girare su piattaforma IBM zSeries (S/390), come host di z/VM o VM/ESA

La distro più diffusa è ThinkBlue/64.

Risorse condivise: memoria, potenza di CPU, storage e rete.

Partizioni di sistema: VM (2)

Pro:

- Un I/O da sogno
- Potenza di CPU (SMP a 10+ vie)
- Facilmente scalabile
- Separazione **totale**

Contro:

Forse un po' costoso (acquisto/gestione)

Partizioni di sistema: N1

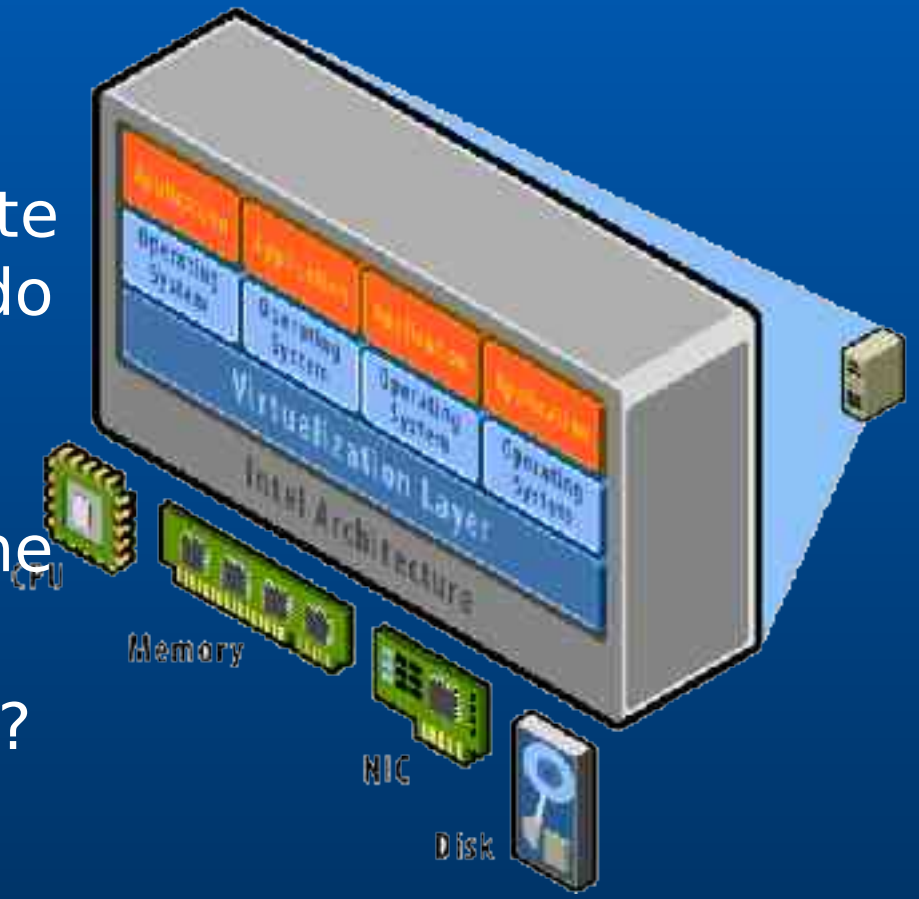
Solaris 10 introduce gli N1 (grid container)

- Root solamente dentro il container
- Process space separato
- Utilizzano un resource pool
- RBAC (role based access control)
- 4000+ N1GC per sistema*

* Fonte Sun Microsystems

Partizioni di sistema: vmware

- Tre flavour: workstation, server (GSX), ESX
- ESX si interfaccia direttamente con l'hardware, mantenendo le macchine virtuali
- Teoricamente non c'è condivisione tra le macchine
- Service console su linux (ma proprietaria): maintenance?



Quindi?

Quindi state attenti a

- cosa installate
- su che piattaforma
- cosa deve fare

configurandolo bene a privilegi minimi.

Quando tutto funziona, abbiamo appena cominciato! :)

Attenzione!

Quelli forniti finora sono solamente

suggerimenti

Non vi esimono ovviamente dall'uso degli accorgimenti che usereste:

- Utilizzare password sicure
- Esporre il minimo
- Fare i backup spesso!

Un setup di esempio?

- Una macchina UltraSparc
- Linux
- Apache in chroot per i servizi
- Mysql in chroot bindato su localhost
- Nessun servizio di management esposto (un altro chrootapache?)
- Demone Ipsec + sshd solo da localhost

Ma io ho Windows!

Peccato.

Ma io ho Windows!

In questo caso:

- Va fatto hardening (guida NSA)
- sicuramente mantenute aggiornate quotidianamente le macchine.
- mettere davanti dei proxy applicativi (postfix, squid, apache) o firewall che lo facciano (fw-1)

Prossimamente...

...su questi schermi (LAB):

Setup di

- apache + mod_security
- mysql
- Postfix

in chroot su Linux

...o altro che vi interessi

Domande?

Grazie a tutti.

Guido [Zen] Bolognesi - guido@kill-9.it