Am I paranoid enough?

Sicurezza,
illusione o gestione del rischio?

Guido Bolognesi
guido@kill-9.it

© guido@kill-9.it

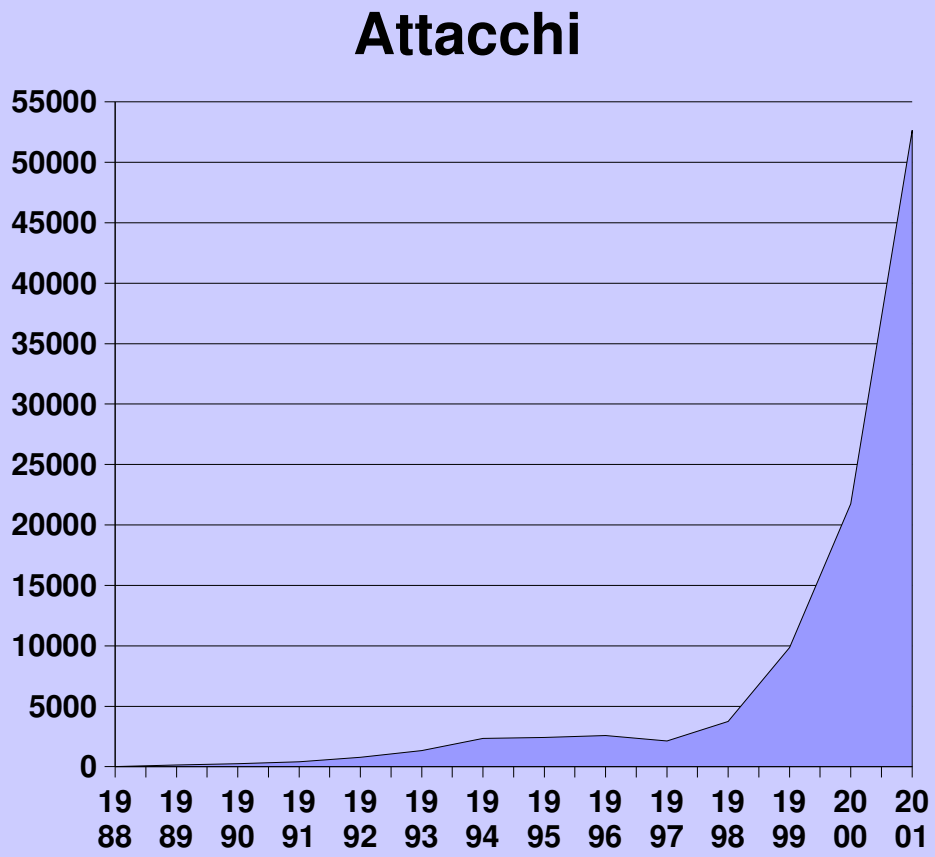
Prima Parte

La sicurezza in astratto

© guido@kill-9.it

Incidenti rilevati

- Problemi di sicurezza, ci sono davvero?
- In media viene denunciato il 37% degli eventi



Fonte: CERT

© guido@kill-9.it

La security e' un processo

...non uno one-shot!

```
If [ $SECURITY = “one-shot” ]
then
SYSADM=”one-kill”
fi
```


© guido@kill-9.it

La security e' un processo

Read bugtraq every day.
New vulnerability.
Rush to plug it up.

© guido@kill-9.it

Bilancia

Security
vs.
Usability

© guido@kill-9.it

Dominio di controllo

- Dati locali
- Dati in rete locale
- Email
- Transazioni web

© guido@kill-9.it

Cosa proteggere?

- Informazioni (Privacy)
- Integrita'
- Usabilita'

© guido@kill-9.it

Sicurezza fisica?

- Della rete (tubo blindato)
- Degli apparati (controllo accessi)
- Dei locali (*wardriving*)
- Dei dati "rimossi" (*dumpster diving*)
- ...degli operatori

© guido@kill-9.it

Stabilire procedure

Buffer overflow
vacationing sysadmin
computer is mine

© guido@kill-9.it

Seconda Parte

La sicurezza in pratica

© guido@kill-9.it

Tecniche

- Sniffing
- Session Hijacking
- Configurazioni
- Buffer overflow
- Problemi applicativi
- Broken standards
- Social engineering
- (D)DOS

© guido@kill-9.it

Sniffing

- Shared (*)
- Switched (**)
- Switched tunneled+ (***)
- Wireless (**)

© guido@kill-9.it

Session Hijacking

Mitnick,
Shimomura
&&
Toad.com

© guido@kill-9.it

Cattive configurazioni

- Ftp anonimo in scrittura
- C$ in share
- Sendmail execution
- / come httproot
- Oracle oracle
- QSECOFR?

© guido@kill-9.it

Buffer Overflow

- Wu-ftpd, il buco con il server intorno
- Sshd – crc32 compensation
- Microsoft UPnP
- Telnetd
- Snmp
- Quelli locali?

© guido@kill-9.it

Problemi applicativi

- /scripts/root.exe?/c+dir
- /..%c0%af../
- Phpnuke
- filename.cgi%00
- ' or 1=1
- Dns poisoning
- SNMP

© guido@kill-9.it

Broken Standards

e-mail attachment
installs computer virus
scripting can be fun

© guido@kill-9.it

Social Engineering

Root password mumbled
aloud in a crowded lab
how fast can I type?

© guido@kill-9.it

(D)DOS

Packets on a wire
consuming all my bandwidth
d-o-s victim

© guido@kill-9.it

Q & A

Security Haikus:

http://pubweb.nfr.net/~mjr/usenix/haiku.html

gr33tz to

n41f, k0b4, N4g4, v3cn4

thx to koan :)

© guido@kill-9.it