Hardening di un sistema GNU/Linux

Gianluca “P|pex” Minnella

- Linux_Var -

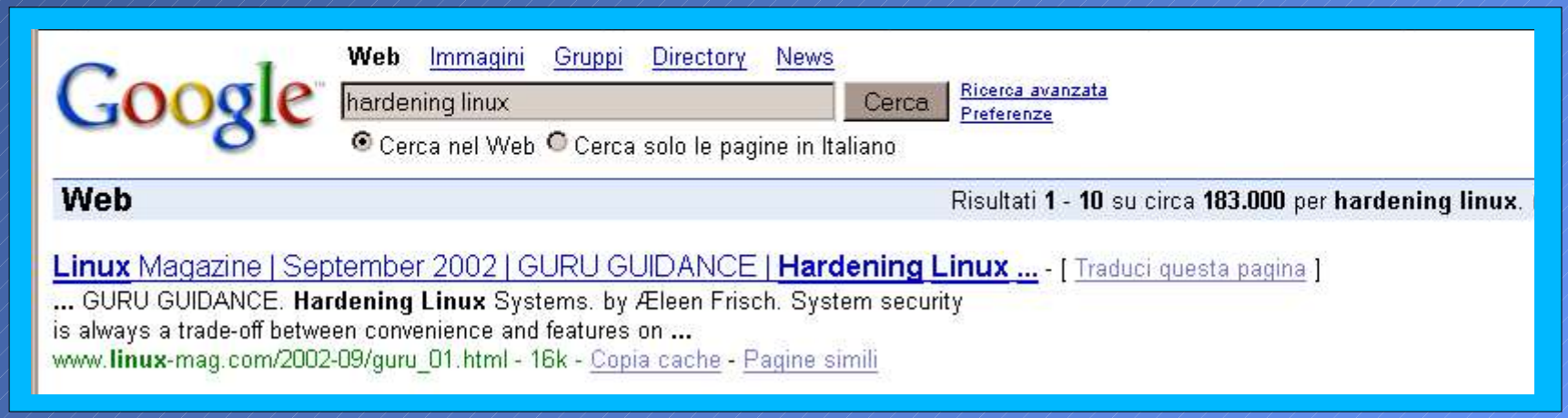
gianm@despammed.com

Hardening GNU/Linux Systems

- Hardening: è un aspetto della sicurezza informatica
- GNU/Linux OS - client e server
- Systems: il nostro PC

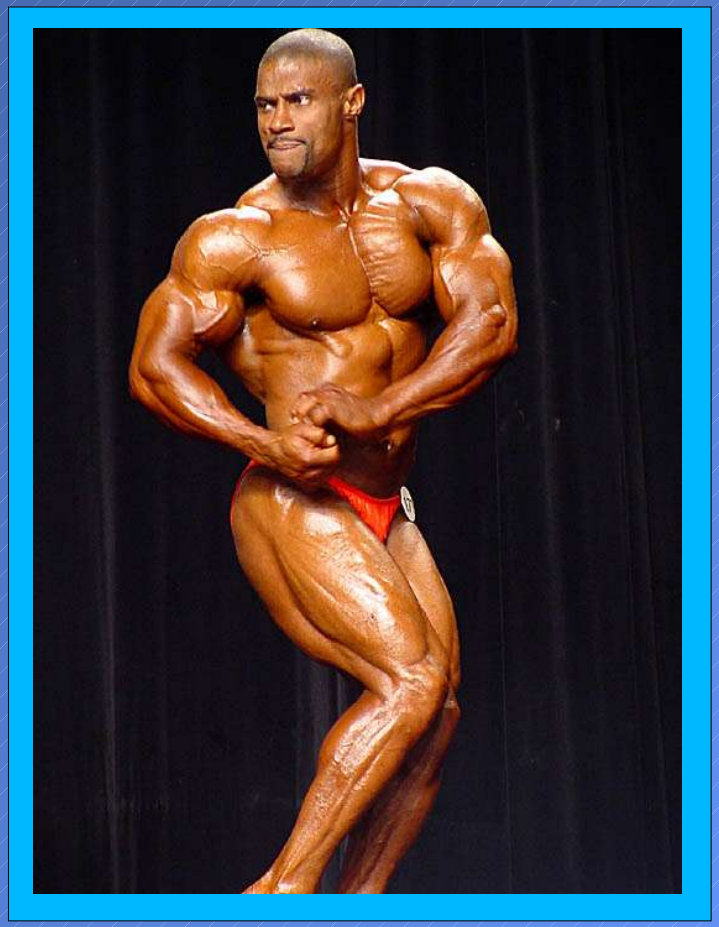
Hardening GNU/Linux

- Rendere *più sicura* una linux box
- Google.com: 183.000 hits
-

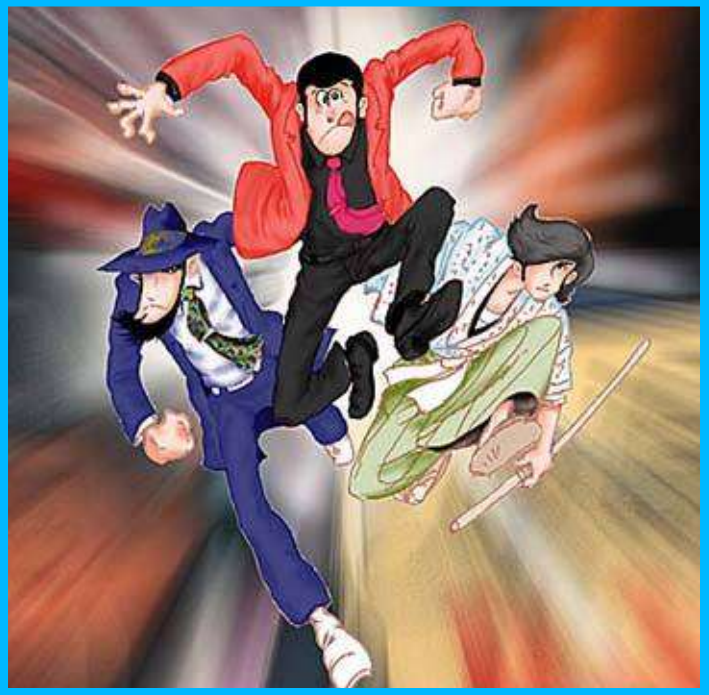


Hardening GNU/Linux

- Forte è Sicuro?
  - Livello fisico, hardware
  - Livello applicativo
    - Kernel e OS
    - Applicazioni (demoni e programmi)
  - Livello networking



Hardening hardware



- Accesso al PC (fisso o portatile)

  I boot manager (lilo o grub)

  - Basta premere CTRL+ALT+CANC **TODO** disabilitare modificando `/etc/inittab`
  - Senza essere utente del pc che stiamo usando, basta fare il reboot (magari staccando la spina!) e passare i parametri al boot manager per eseguire una shell
    TODO inserire password nel boot manager:
    `/etc/lilo.conf` : togliere prompt e mettere password
    `/boot/grub/menu.lst`: password
    Chiedere la pass di root in “single user mode”: `/etc/inittab` inserire `sp:S:respawn:/sbin/sulogin`

Hardening hardware

- Accesso alle periferiche (floppy, cdrom, usb-key, boot-on-lan) al boot
  - Con un CD-Live siamo “fregati”. **TODO**: modifica Bios
- Accensione della macchina (pass bios)
  - Se si tratta di un server remoto _è_un_problema_ nel caso si volesse fare il reboot per installare un nuovo kernel
  - Se si tratta del portatile _è_obbligatori_ averla... Basta lasciarlo in giro
  - Se è il PC di casa? Basta portarlo al LinuxDay 2005....
  - o a casa di “amici”
  - **TODO**: modifica Bios, fingerprint, smartcard

OS hardening

– Un OS Linux appena installato _non_ è sicuro

Sono necessarie una serie di attività di configurazione

- Installare il servizi necessari
- Installare le patch di sicurezza: kernel e appl
- Verificare i permessi del filesystem e i binari S*ID
- Migliorare la sicurezza del login e degli utenti
- Impostare/verificare la sicurezza fisica ed del boot
- Rafforzare il controllo dell'accesso ai "demoni" attraverso la rete
- Aumentare le informazioni dei log e dell'audit
- Configurare i software che forniscono "sicurezza" (IDS, host firewall)

OS hardening

– Politica di correzione Bug di sicurezza

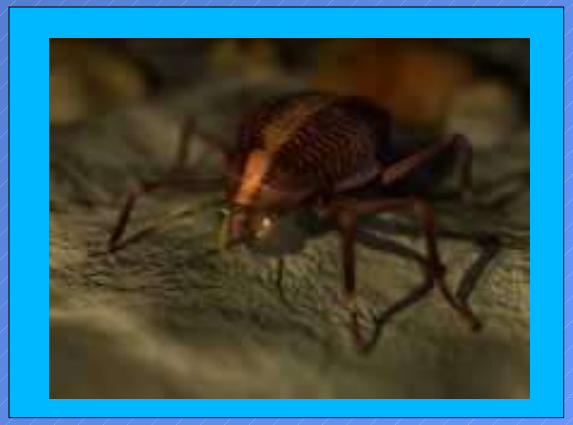
- Il caso debian

Vengono corretti i bug nei software del ramo stable e unstable

- Il caso Fedora – Redhat enterprise

Rilascio di nuove versioni del software con le correzioni

Rilascio a pagamento delle security patch



OS hardening

- Partizionamento
  - Tutto RO (?)
  - Fare partizioni separate per /boot, /usr, /var, /tmp, and /home
  - Montare le partizioni nel modo giusto
    - In /etc/fstab: `/dev/hda7 /tmp ext2 defaults,nosuid,noexec,nodev 0 2`
    - `mount -o remout,exec /tmp; apt-get install pack.deb;mount -o remount, nosuid,noexec,nodev /tmp`
    - Si può circuire con un semplice
      - `$/lib/ld-linux.so.2 /tmp/eseguibile`
- Kernel hardening

  OpenWall http://www.openwall.com/linux/

Software automatic hardening

– Bastille 

URL: http://www.bastille-linux.org/

Attivazione: iptables, aggiornamenti OS, disabilita SUID su alcuni programmi (ping, linuxconf), scadenze password, limitazione risorse, logging system e utenti, rafforzamento apache

Disattiva: servizi non sicuri r*, CTRL+ALT+CANC, banner /etc/motd, compilatore, lpr SUID, FTP

– Harden package (debian)

- harden-tools: strumenti che aumentano la sicurezza del sistema (controllo d'integrità, rilevamento delle intrusioni, patch al kernel...)
- harden-servers – harden-clients -harden-remoteflaws - harden-localflaws
- harden-remoteaudit: strumenti per un controllo remoto di un sistema.

System hardening

- Account
  - Strong password policy /etc/login.defs
    PASS_MIN_LEN, PASS_MAX_DAYS - chage
  - SSH users AllowUsers PermitRootLogin
  - Shell: rbash, history
  - /etc/security/limits.conf
- Log
  - Syslog: replicare i log, stamparli, remote logging
- Audit
  - Accounting, logcheck, watchlog
- Security by obscurity: /etc/issue e /etc/issue.net
  - Porte e banner dei demoni

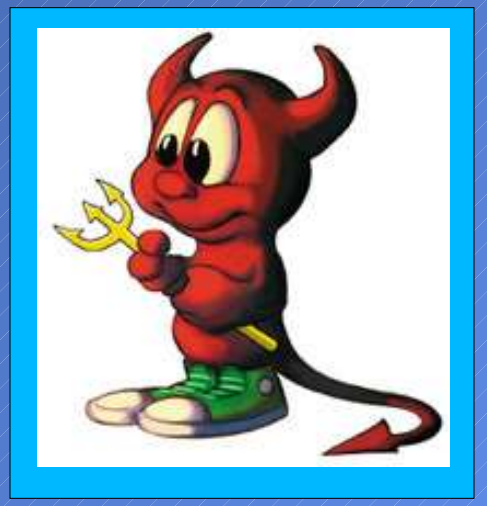
System hardening

- Utilizzare il _meno_ possibile root
  - SUDO: visudo
  - PAM per “su”: gruppo wheel

```
auth required /lib/security/pam_wheel.so use_uid
```

- IDS
  - Network: snort
  - System: tripwire, aide

System hardening



- daemon
  - preferire i servizi sicuri a quelli non sicuri
    - Telnet --> SSH
    - FTP --> sftp
    - POP3 --> POP3 SSL
    - SMTP --> SMTP SSL
  - limitare la visibilità dei servizi
- inetd / xinetd
  - `/etc/inetd.conf`: disabilitare il superfluo (discard,daytime,time)