Linux: sicurezza dei sistemi

A cura di
Francesco Tomasoni
Linux User Group Brescia
ftomas@lugbs.linux.it

Punti critici di accesso

- accesso fisico al sistema
- sicurezza locale
  - installazione SO Linux
  - accesso locale (user access)
  - analisi e verifica sistema
    - Kernel e system files
    - Filesystem
    - administration tools
    - software management
- sicurezza di rete
  - sicurezza dei protocolli
  - funzioni dominio (routing, gatway,…)
  - sicurezza dei servizi di rete
  - condivisione delle risorse
  - firewalling
- strumenti di *attacks preamption* in Linux

Accesso fisico

- accesso al sistema
- configurazione del BIOS
  - C: (hda) come sola unità di boot
  - disabilitazione drive (A:, CDROM,…)
  - porte comunicazione (seriali, parallele, USB)
  - interrups (IRQ)
- configurazione di *lilo.conf*
  - delay time = 0 (spec. C2 security)
  - singola immagine di boot
  - specifica **`restricted`**
  - specifica **`password`**
- accesso limitato a *lilo.conf*

Sicurezza locale

- Accesso locale:
  - sicurezza tty
  - sicurezza pasword
    - /etc/passwd
    - /etc/shadow e gshadow
    - PAM (Plaggable Authentication Modules)

      (**`www.sun.com/…/pam`**)
      - RedHat (5.x e 6.0)
      - Debian (2.1, …)
      - Caldera (1.3, 2.2)
    - cracker pessword:

      Crack, Saltine, VCU, JtR,…

- **Configurazione e verifica del sistema**
  - versione : 2.2.x (luglio 1999)
    (**`ftp.kernel.org`**)
  - compilazione del kernel
    - opzioni da abilitare:
      - **`CONFIG_FIREWALL`**
      - **`CONFIG_IP_FORWARD`**
        (routing on IPvX)
      - **`CONFIG_IP_ALWAYS_DEFRAG`**
  - FileSystem:
    - partizionamento (/tmp, /home, …)
    - permission setting:
      - root priv. runtime tools (ls, df, du, stat,..)
    - eliminazione sicura (es: *wipe* tool)
    - ACL (Access Control List)
      (**`www.braysystems.com`**)

- Tools di amministrazione
  - Telnet SSL / SSH (LSH GNU)
  - NSH (commerciale disp. RPM (30 gg.))
  - sudo & Super
- Software management
  - dpkg
  - RPM
  - tarballs

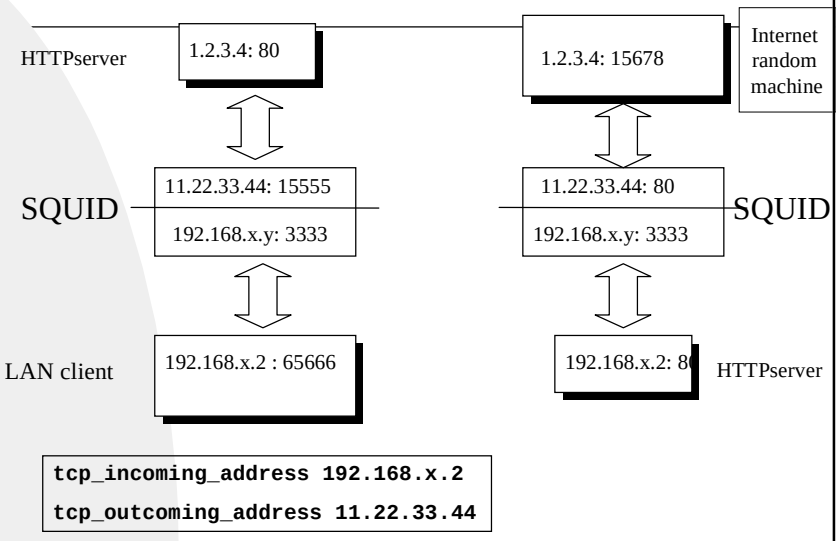
Sicurezza di rete

- protocolli:
  - TCP/IP
    - IP: IPv6, IPSec, VPN
      - analisi *inbound e outbound*
      - *HUNT (TCP/IP connections)* (**www.cri.cz**)
      - UserIPAcct (monitoraggio user bandwidth) (**zaheer.grid9.net**)
    - PPP
      - CHAP (Challenge Handshake Auth. Protocol) MD5
- Routing & Gatway functioms
  - routed (distr.)
  - gated (distr.)
  - zebra (www.zebra.org/)

- sicurezza nei servizi di rete
  - servizi:
    - FTP (proFTPd GPL lic.)
    - TELNET (Telnetd)
    - HTTP & HTTPS (APACHEs)
      - Apache with SSL (USA comm.)
      - Roxen (crypto syst.) (**www.roxen.com**)
    - Object Caching (SQUID)
  - firewalling dei servizi
    - firewalling: ipchains, ipfwadm
    - TCP_WRAPPERS: /etc/host.xxxxx

Esempio: Linux caching & firewalling on W-NT IIS

SQUID server




```
tcp_incoming_address 192.168.x.2
tcp_outcoming_address 11.22.33.44
```

Documentazione on line

- Linux security home page
  www.thei.net/aek
- Kernel security
  www.linuxhq.com
- security HOWTO
  ftp://metalab.unc.edu/pub/linux/docs
- VPN (Virtual Protected Network) on Linux
  hal2000.hal.vein.hu/ ~mag/linux-security/VPN-HOWTO-2.html
- IT-SEC spec.
  www.itsec.gov.uk
- Linux Security Applications
  www.freshmeat.net
- Appunti Linux (current : 12sett.99 - tomo 12)