in collaborazione con

l'Università degli studi di Bergamo

Facoltà d'Ingegneria

presenta:

Sicurezza nei sistemi Linux

Marco Balduzzi <embyte@bglug.it>

Di che parliamo?

Accenno al TCP/IP *(prerequisito!)*

Analisi e gestione dei servizi

I firewall: Iptables

L'importanza dei log: Sysklogd (syslogd + klogd)

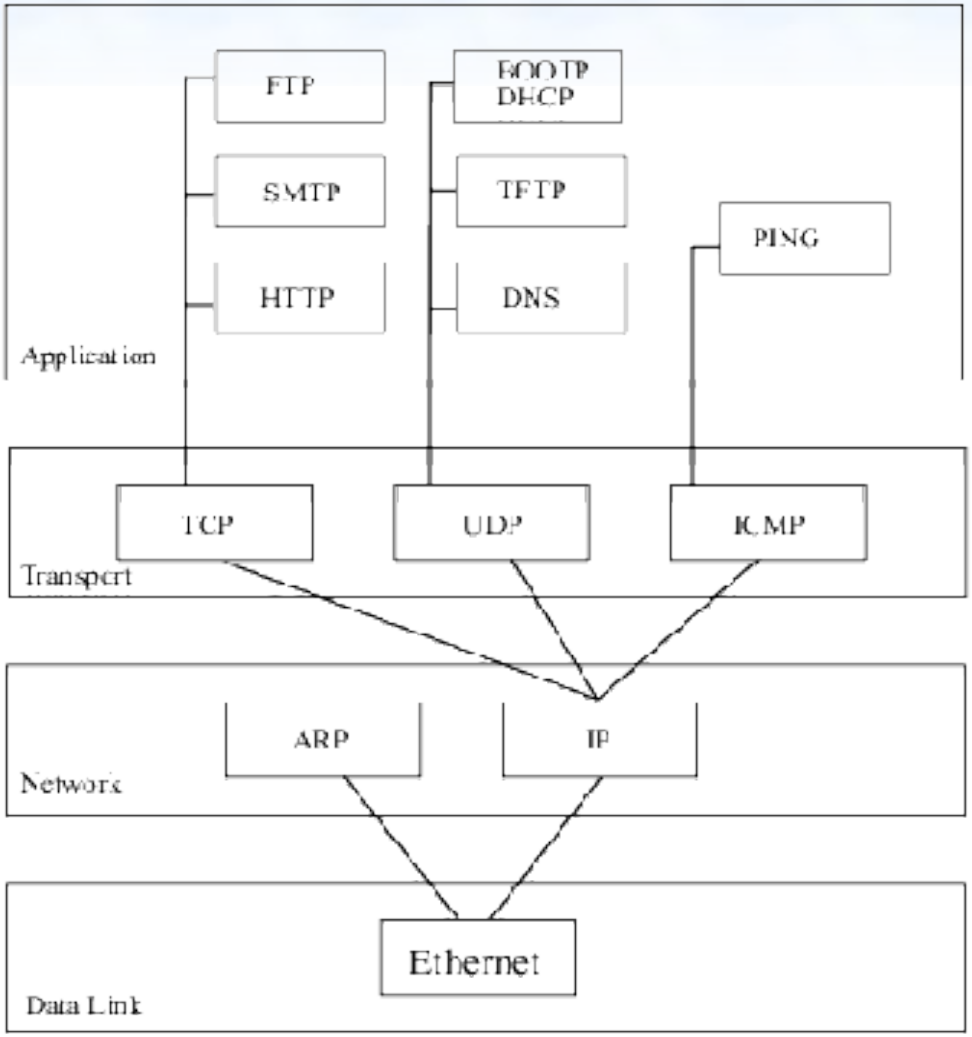
Accenno al TCP/IP

- Ethernet Protocol (RFC 894):
indirizzo a 48 bit
x:x:x:x:x:x | 0 < x < 0xFF

- IP Internet Protocol (RFC 791):
indirizzo a 32 bit
x.x.x.x | 0 < x < 2^8-1 (255)

- TCP e UDP (RFC 793/768):
porta a 16 bit
p | 0 < p < 2^{16}-1 (65535)

- ICMP (RFC 792)
tipo e codice
es: 8;0 -> echo request (ping)



Analisi e gestione servizi (1)

- ***Definizione di una politica***
  - E' un client?
  - E' un server?
  - Di che genere di server si tratta (web, mail, dns)?
  - Quali servizi vogliamo offire? A chi?

- ***Identificazione dei servizi abiltiati e relative porte (primitva di bind)***

```
# netstat -pan --inet
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address    State       PID/Program name
tcp        0      0 0.0.0.0:32768      0.0.0.0:*          LISTEN      820/licq
tcp        0      0 0.0.0.0:587        0.0.0.0:*          LISTEN      675/sendmail: accept
tcp        0      0 0.0.0.0:6000       0.0.0.0:*          LISTEN      738/X
tcp        0      0 0.0.0.0:22         0.0.0.0:*          LISTEN      489/sshd
tcp        0      0 0.0.0.0:631        0.0.0.0:*          LISTEN      506/cupsd
tcp        0      0 0.0.0.0:25         0.0.0.0:*          LISTEN      675/sendmail: accept
udp        0      0 0.0.0.0:631        0.0.0.0:*                      506/cupsd
```

Analisi e gestione servizi (2) - Controllo

- ***Controllo d'esecuzione dei servizi (al boot)***

Dipende della distribuzione:

- RedHat: redhat-config-services (da X), ntsysv (Console)
- Mandrake: /etc/rc.d/rc0-6.d/, drakeServices
- Slackware: /etc/rc.d/rc.inet2, pkgtool (sottomenu)
- Gentoo: rc-update
- Debian: update-rc.d

Precisazione: alcuni servizi usano i wrapper inetd e xinetd.

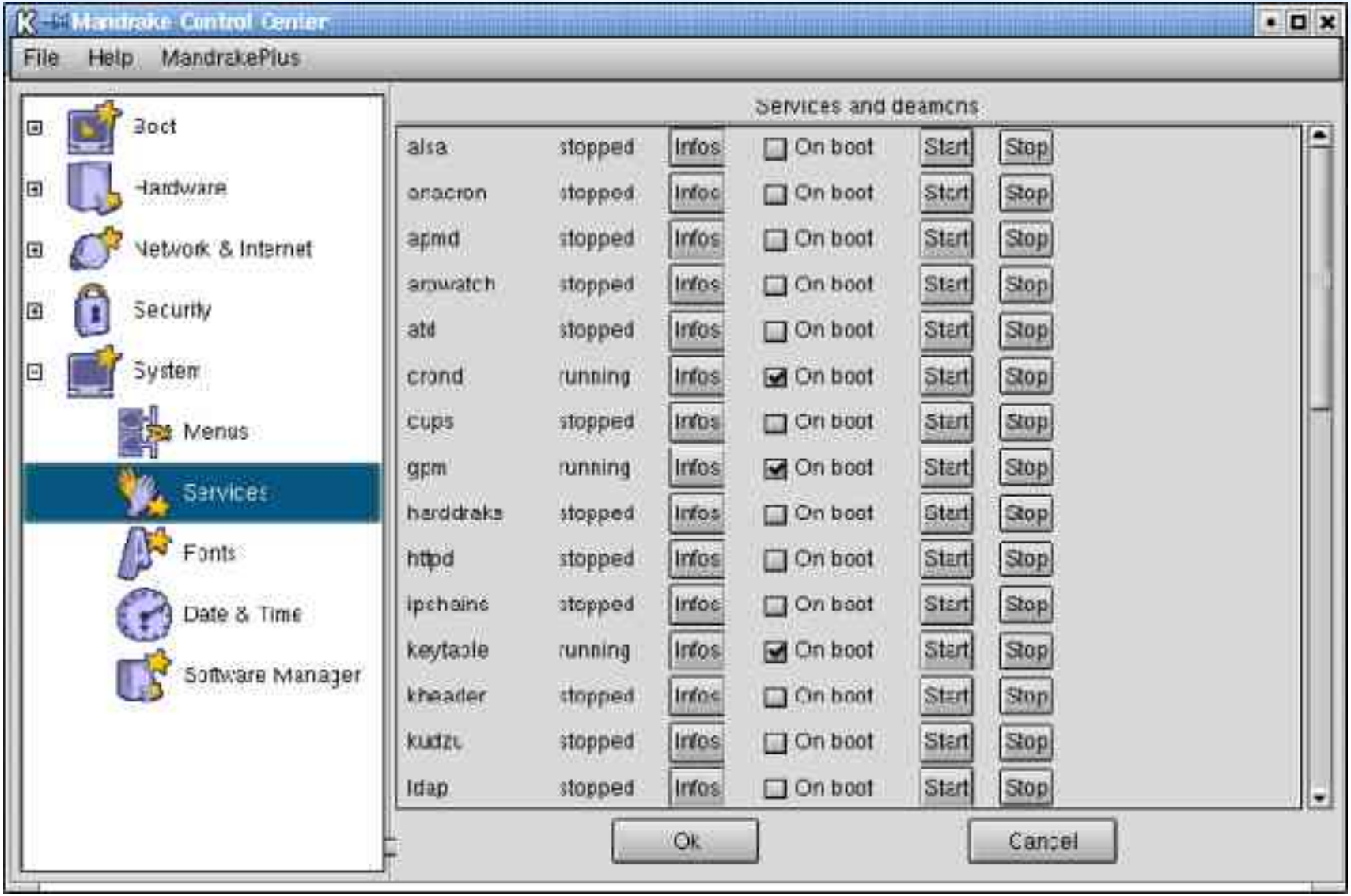
$ cat /etc/inetd.conf

```
# File Transfer Protocol (FTP) server:
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd  proftpd
# Telnet server:
telnet stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
```

Per xinetd vedere il corrispettivo /etc/xinetd.conf e /etc/xinetd.d/

Snapshot (Slackware 9.1)

Snapshot (Mandrake 8.0)



Analisi e gestione servizi (3) - Testing

- ***Testing:*** netstat, nmap, hping, ps, fuser, lsof

```
# nmap localhost

Starting nmap 3.45 ( http://www.insecure.org/nmap/ ) at 2003-11-17 13:36 CET
Interesting ports on localhost (127.0.0.1):
(The 1652 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
587/tcp  open  submission
631/tcp  open  ipp
6000/tcp open  X11

Nmap run completed -- 1 IP address (1 host up) scanned in 2.358 seconds
```

NB: Nmap senza flags controlla solo le porte in /usr/share/nmap/nmap-services, usare -p

Analisi e gestione servizi (4) - Banner

- ***Strumenti "avanzati" di un attaccante:*** troppi...

Esempio: scansione automatizzata del banner dei demoni di uno o più host alla ricerca di vulnerabilià note (sfruttate dagli exploit)

```
# ./exscan -qv router.too.fun
Scanning Host: router.too.fun [192.168.1.254]
Port   21 Open: File Transfer Protocol Service Running.
Data Returned:
220 Inactivity timer = 120 seconds. Use 'site idle <secs>' to change.
Port   23 Open: Telnet Service Running.
Data Returned:
Port   80 Open: Hypertext Transfer Protocol Service Running.
Data Returned:
HTTP/1.0 401 Authorization Required
WWW-Authenticate: Basic realm="SpeedTouch (00-12-E2-92-BB-C2)"
```

Mascherare i banner di default – procedura diversa per demone:

- Proftpd: /etc/proftpd.conf -> ServerName, ServerIdent
- SSH: /ect/ssh/sshd_config -> banner

I firewall: Iptables (1)

- ***Firewall***: strumento che permette di applicare regole di filtraggio sul traffico passante per le interfacce di rete (e non solo!).

***Iptables*:** implementazione userland del firewall Linux Netfilter (Kernel 2.4/2.6) ed evoluzione di Ipchains (Linux 2.2) e Ipfwadm (Linux 2.0)

Installare il *pacchetto iptables* e abilitare nel *kernel* (opzioni necessarie):
- TCP/IP networking [CONFIG_INET]
- Network packet filtering (replaces ipchains) [CONFIG-NETFILTER]
- IP tables support (required for filtering/masq/NAT) [CONFIG_IP_NF_IPTABLES]
- Packet filtering [CONFIG_IP_NF_FILTER]

consigliate:
- Connection tracking (required for masq/NAT) [CONFIG_IP_NF_CONNTRACK] e relative sotto-opzioni
- REJECT target support [CONFIG_IP_NF_TARGET_REJECT]
- Packet mangling [CONFIG_IP_NF_MANGLE]
- LOG target support [CONFIG_IP_NF_TARGET_LOG]
- ULOG target support [CONFIG_IP_NF_TARGET_ULOG]

I firewall: Iptables (2)

- ***Filtering***
  - La Tabella filter possiede tre catene predefinite:
    - INPUT: pacchetti in ingresso
    - OUTPUT: pacchetti in uscita
    - FORWARD: pacchetti che attraversano l'host

- ***Regole essenziali***
  - Ogni pacchetto percorre la relativa catena con una politica *top-down*
  - Se la regola è soddisfatta dal pacchetto è applicata l'azione (*target*) specificata con -j
  - Se il pacchetto passa indenne fino al fondo della catena è applicata la politica di default (opzione -P)

- ***Comandi, parametri e target base***
  - -A (append), -D (delete), -I (insert), -L (list), -F (flush), -X (erase), -P (policy)
  - -p (protocol), -s (source), -d (destination), -i (iface), -j (jump – set target)
  - *Target* impostati con -j: ACCEPT, REJECT (--reject-with), DROP, LOG

I firewall: Iptables (3) - Esempi

- Esempio 1: firewalling di una porta ad uno specifico host

```
zeus:~# nmap -p 21 -P0 portatile
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-19 22:09 CET
Interesting ports on portatile.too.fun (192.168.1.1):
PORT   STATE    SERVICE
21/tcp open     ftp
Nmap run completed -- 1 IP address (1 host up) scanned in 0.020 seconds

portatile:~# iptables -A INPUT -p tcp -s zeus.too.fun --dport ftp -j REJECT

zeus:~# nmap -p 21 -P0 portatile
[...]
PORT   STATE    SERVICE
21/tcp filtered ftp

portatile:~# tcpdump -ti eth0
zeus.too.fun.59392 > portatile.too.fun.ftp: S 3474004913:3474004913(0) win 2048
portatile.too.fun > zeus.too.fun: icmp: portatile.too.fun tcp port ftp unreachable
```

I firewall: Iptables (4)

- Esempio 2: firewalling “nascosto” di una porta a tutti eccetto uno specifico host

```
portatile:~# iptables -A INPUT -p tcp -s ! zeus.too.fun --dport ftp -j REJECT --reject-with tcp-reset

puzzle:~# nmap -p 21 -P0 portatile
[...]
PORT   STATE  SERVICE
21/tcp closed ftp

zeus:~# nmap -p 21 -P0 portatile
[...]
PORT   STATE    SERVICE
21/tcp open     ftp

portatile:~# tcpdump -ti eth0
zeus.too.fun.37177 > portatile.too.fun.ftp: S 2592154468:2592154468(0) win 4096
portatile.too.fun.ftp > zeus.too.fun.37177: R 0:0(0) ack 2592154469 win 0 (DF)
```

I firewall: Iptables (5)

- Esempio 3: firewalling degli icmp echo request (ping)

```
embyte@zeus:~$ ping -c 1 portatile
PING portatile.too.fun (192.168.1.1) 56(84) bytes of data.
64 bytes from portatile.too.fun (192.168.1.1): icmp_seq=1 ttl=64 time=0.122 ms
--- portatile.too.fun ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.122/0.122/0.122/0.000 ms

portatile:~# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

embyte@zeus:~$ ping -c 2 portatile
PING portatile.too.fun (192.168.1.1) 56(84) bytes of data.
--- portatile.too.fun ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 0ms

portatile:~# tcpdump -ti eth0 icmp
tcpdump: listening on eth0
zeus.too.fun > portatile.too.fun: icmp: echo request (DF)
portatile.too.fun > zeus.too.fun: icmp: echo reply
zeus.too.fun > portatile.too.fun: icmp: echo request (DF)
zeus.too.fun > portatile.too.fun: icmp: echo request (DF)
```

L'importanza dei log : Sysklogd

- ***Logging***: qualsiasi procedura con cui un sistema operativo o un'applicazione registra gli eventi e li preserva per un controllo successivo.

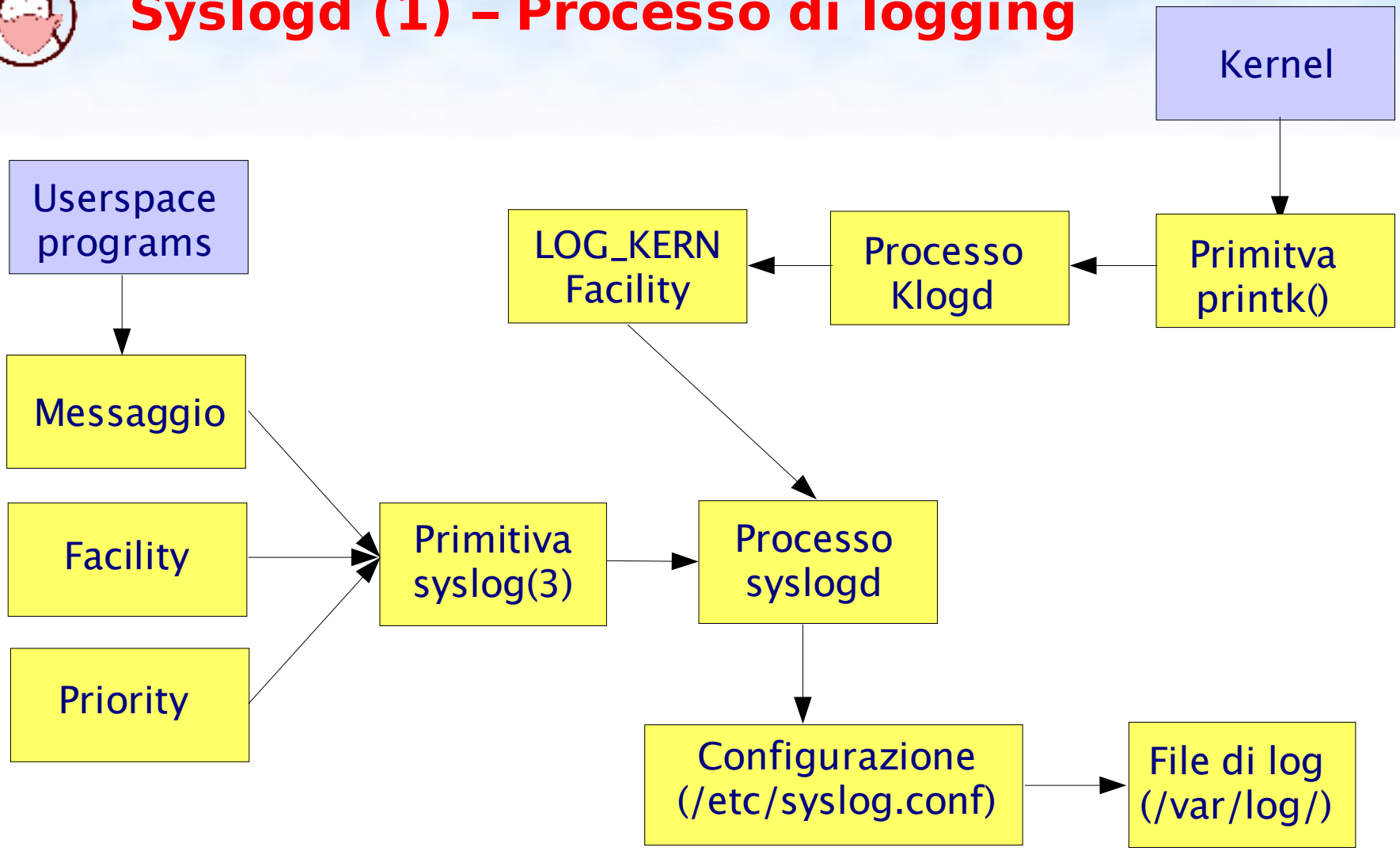
- I log sono una PROVA evidente di un attacco informatico.

- I log devono essere conservati in un LUOGO SICURO:
  non sulla macchina monitorata (esportati in remoto)
  meglio se crittografati (sia a livello di protocollo che di filesystem)

- I log devono possedere una struttura ORDINATA
  per facilitare l'auditing (analisi dei log)

- ***Sysklogd*** The Linux system logging utilities.
  - Syslogd: supporto al logging di systema
  - Klogd: logging dei messaggi del kernel

Syslogd (1) – Processo di logging



Syslogd (2) – Facility e Priority

- ***Facility***: argomento del messaggio
  - LOG_AUTHPRIV security/authorization messages
  - LOG_MAIL mail subsystem
  - LOG_CRON clock daemon (cron and at)
  - LOG_LOCAL0-7 reserved for local use

- ***Priority***: livello d'importanza del messaggio
  - LOG_DEBUG debug-level message
  - LOG_INFO informational message
  - LOG_NOTICE normal, but significant, condition
  - LOG_WARNING warning conditions
  - LOG_ERR error conditions
  - LOG_CRIT critical conditions
  - LOG_ALERT action must be taken immediately
  - LOG_EMERG system is unusable

Syslogd (3) - Configurazione

- Esempio di configurazione (*/etc/syslog.conf*)

```
# Log anything 'info' or higher, but lower than 'warn'.
# Exclude authpriv, cron, mail, and news.  These are logged elsewhere.
*.info;*.!warn;\
        authpriv.none;cron.none;mail.none;news.none     /var/log/messages

# Log anything 'warn' or higher.
# Exclude authpriv, cron, mail, and news.  These are logged elsewhere.
*.warn;\
        authpriv.none;cron.none;mail.none;news.none     /var/log/syslog

# Send critical messages to root
*.crit                                                  root

# Log anything to /dev/tty12 console
*.*                                                     /dev/tty12

# Send important log to remote host (run syslogd with -r flag)
*.err                                                   @host_remoto
```

Syslogd (4) – Esempio di log

```
Nov 24 19:36:39 portatile syslogd 1.4.1: restart.
Nov 24 19:36:40 portatile kernel: klogd 1.4.1, log source = /proc/kmsg started.
Nov 24 19:36:40 portatile kernel: Initializing CPU#0
Nov 24 19:36:40 portatile kernel: Memory: 370028k/376768k available (1453k
kernel code, 6352k reserved, 493k data, 104k init,0k highmem)
Oct 14 17:08:53 portatile kernel: hda: 39070080 sectors (20004 MB) w/2048KiB
Cache, CHS=2432/255/63, UDMA(100)
Oct 14 17:08:53 portatile kernel: hdc: ATAPI 24X DVD-ROM drive, 512kB Cache,
UDMA(33)

Oct 14 17:07:12 portatile useradd[669]: new user: name=embyte, uid=1000,
gid=100, home=/home/embyte, shell=/bin/bash
Oct 14 17:07:14 portatile chfn[670]: changed user `embyte' information
Oct 14 17:07:18 portatile passwd[671]: password for `embyte' changed by `root'

Nov 20 21:04:37 portatile login[692]: ROOT LOGIN  on `tty2'
Nov 20 21:36:46 portatile login[710]: invalid password for `root'  on `tty1'
Nov 20 21:37:05 portatile proftpd[730]: connect from 192.168.1.200
Nov 24 21:17:36 portatile su[1226]: + pts/3 embyte-root
Oct 18 01:19:18 portatile sudo:   embyte : TTY=pts/4 ; PWD=/home/embyte ;
USER=root ; COMMAND=/sbin/pkgtool
```

L'importanza dei log - Altre fonti d'informazioni

```
# lastlog
Username         Port     From             Latest
root             tty1                      gio nov 20 22:58:24 +0100 2003a
embyte           tty1                      lun nov 24 12:24:50 +0100 2003
sshd                                       **Never logged in**

# last | head
embyte   pts/1                      Mon Nov 24 12:25   still logged in
embyte   pts/0                      Mon Nov 24 12:25   still logged in
embyte   tty1                       Mon Nov 24 12:24   still logged in
reboot   system boot  2.4.22        Mon Nov 24 12:24          (00:13)
embyte   ftpd947      zeus.too.fun  Sat Nov 15 11:26 - 11:27  (00:00)

# w
12:39:02  up 15 min,  3 users,  load average: 1,09, 0,90, 0,44
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
embyte   tty1     -                12:24pm 14:11   0.14s  0.03s  /bin/sh
                                                                  /usr/X11R6/bin/startx
embyte   pts/0    -                12:25pm 13:47   0.00s  0.36s  kdeinit: kwrited
embyte   pts/1    -                12:25pm  7:20   0.04s  0.04s  links
```

Riferimenti

- The Protocols (TCP/IP Illustrated, Volume 1) by W. Richard Stevens (Author)
  http://www.amazon.com/gp/reader/0201633469/ref=sib_dp_pt/002-4626830-1224041#reader-link
- Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation
  http://www.amazon.com/gp/reader/0672316706/ref=sib_dp_pt/002-4626830-1224041#reader-link
- Linux Hack Proofing : A Guide to Open Source Security by James Stanger
  http://www.amazon.com/gp/reader/1928994342/ref=sib_dp_pt/002-4626830-1224041#reader-link
- Iptables/Netfilter *http://www.netfilter.org/documentation/index.html*
- Iptables tutorial *http://iptables-tutorial.frozentux.net/iptables-tutorial.html*
- Nmap portscanner *http://www.insecure.org/nmap/*
- Hping *http://www.hping.org/*
- Syslog-ng (next generation) *http://www.balabit.com/products/syslog_ng/*
- Security Focus *http://www.securityfocus.com/*
- Packetstorm Security *http://packetstormsecurity.nl/*
- S0ftpr0ject 2003 *http://s0ftpj.org/*
- S.P.I.N.E. Research Group *http://www.spine-group.org*