“Networking sicuro con GNU/Linux”

Marco Balduzzi <embyte@bglug.it>

Di cosa parliamo?

- Introduzione al networking in ambiente GNU/Linux
- Configurazione di una interfaccia di rete
- Accesso ad internet mediante modem (dial-up)
- Condivisione di una connessione Internet
- Connessione wireless e problematiche connesse

- Introduzione alla sicurezza
- Analisi e gestione dei servizi e degli accessi di rete
- Utilizzo del firewall iptables
- Accenno alla crittografia di rete
- Accenno al concetto di Intrusion Detection System
- L'importanza dei log

Che cosa sono le interfacce di rete?

- Dispositivo virtuale (***device***) fornito dal kernel che permette all'utente di accedere al canale di comunicazione.

- **Alcune categorie importanti**
  - Ethernet (eth): principalmente reti wired ti tipo Intranet
  - Wireless (wlan): interfaccia 802.11
  - Internet (ppp): acronimo di Point-To-Point-Protocol: gestisce l'incapsulamento e la trasmissione dei dati su link seriali.
  - Loopback (lo): interfaccia per la comunicazione tcp/ip locale
  - Tunnel (vtun, ipsec, pptp): interfacce di incapsulamento quali VPN, PPP over IP (modem ADSL)

Che cosa sono le interfacce di rete?

- **Configurazione del kernel con il supporto del driver corretto**
  - Schede di rete: *Device Drivers -> Network device support -> Ethernet 10/100 -> "Scheda"*
  - Wireless: [CONFIG_NET_WIRELESS]
  - Internet: [CONFIG_PPP]

- Caricamento modulo e verifica
  - # insmod MODULO (modprobe)
  - # lsmod
- Elenco delle interfacce conosciute dal kernel
  - # ifconfig -a

Che cosa sono le interfacce di rete

- Il comando ***ifconfig*** elenca le interfacce di rete

```
eth0      Link encap:Ethernet  HWaddr 00:40:D0:1E:26:F4
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6668 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5545480 (5.2 Mb)  TX bytes:771305 (753.2 Kb)
          Interrupt:11 Base address:0x1800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

Networking di base

- **Impostare l'indizzo internet dell'interfaccia manualmente**
  - *ifconfig interface address up*

    # ifconfig eth0 192.168.1.50 netmask 255.255.255.0 up
- **Tramite un server di indirizzamento DHCP**
  - usare un client DHCP come *dhcpcd* o *dhclient*

    # dhcpcd -d eth0

- Configurare i **DNS** per la risoluzione dei nomi
  - editare /etc/resolv.conf, sintassi è “nameserver DNS_SERVER”

    # cat /etc/resolv.conf

    nameserver 213.205.32.70

    nameserver 213.205.36.70

Networking di base

- Anche in GNU/Linux esiste un file mappatura statica degli host

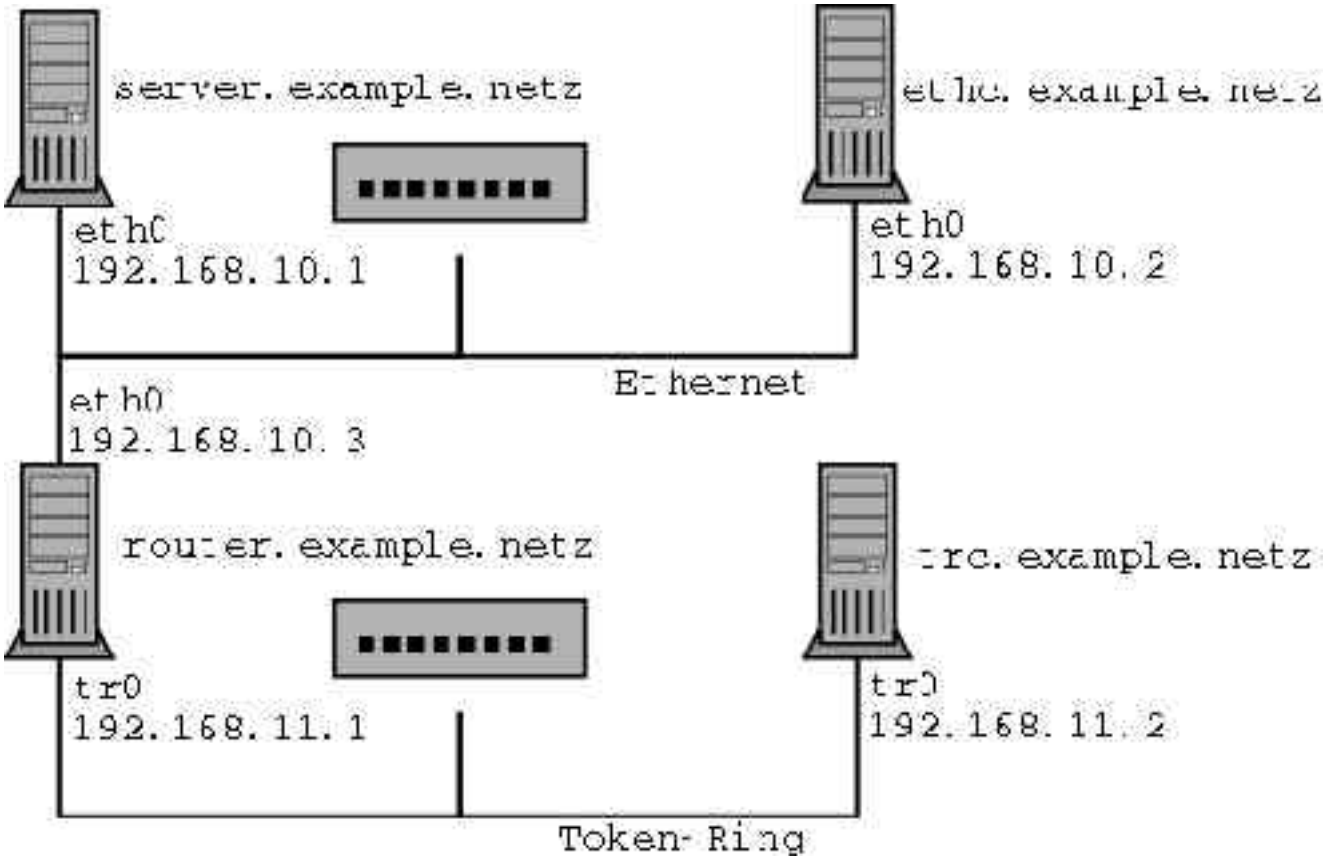
```
# cat /etc/hosts
# For loopbacking.
127.0.0.1               localhost
192.168.1.10            sunlight.too.fun   sunlight
192.168.1.254           router.too.fun     router
```

- E uno con la priorità di risoluzione dei nomi

```
# cat /etc/host.conf
order hosts, bind
multi on
```

Networking di base

- **Routing:** procedura che consente l'interconnessione e la distribuzione coerente dei pacchetti tcp/ip tra reti diverse



Networking di base

- Il processo di routing fa affidamente alla “tabella di routing”, che può essere **configurata manualmente o dinamicamente** attraverso i protocolli di routing quali RIP, OSPF, BGP.

- Configurazione manuale e statica
  - comando: *route add [-net|-host] target*

    # route add -net 192.168.1.0 netmask 255.255.255.0 dev eth0

    # route add -net 192.57.66.0 netmask 255.255.255.0 gw GATEWAY1

    # route add default gw GATEWAY2

- Nota: solitamente la rotta corrispondente alla rete di una interfaccia è inserita automaticamente da ifconfig. Grazie!

Condivisione connessione Internet

- Situazione: una serie di host della Intranet accedono a Internet **per mezzo di un router hardware o di un PC (GNU/Linux)** che condivide la propria connessione.

- In entrambi i casi le macchine della Intranet sono configurate allo stesso modo:
  - impostare l'indirizzo IP correttamente
  - impostare il router come default gateway
  - impostare i DNS del provider/i_propri o l'ip del router se configurato come DNS server/forwarding
  - DHCP permette di configurare il gateway e i DNS automagicamente :)

Configurazione Gateway GNU/Linux con Iptables

- La configurazione di un Gateway GNU/Linux richiede l'utilizzo di *iptables* per la funzione di Network Addess Translation.

- ***Firewall***: strumento che permette di applicare regole di filtering, logging, N[PAT] sul sul traffico di rete e molto altro!
- ***Netfilter***: firewall framework per kernel Linux 2.4 e 2.6

- ***Iptables***: implementazione userland del firewall Linux Netfilter (Linux 2.4 e 2.6). Costituisce la normale evoluzione di Ipchains (Linux 2.2) e Ipfwadm (Linux 2.0)

Installazione Netfilter e Iptables

- Installare il pacchetto iptables e abilitare nel kernel
  - TCP/IP networking [CONFIG_INET]
  - Network packet filtering (replaces ipchains) [CONFIG-NETFILTER]
  - IP tables support (required for filtering/masq/NAT) [CONFIG_IP_NF_IPTABLES]
  - Connection tracking (required for masq/NAT) [CONFIG_IP_NF_CONNTRACK] e relative sotto-opzioni

- Opzioni di filtering e logging (ne parlo più avanti..)
  - Packet filtering [CONFIG_IP_NF_FILTER]
  - 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]

Configurazione Gateway GNU/Linux con Iptables

IN -> PREROUTING -> ROUTING -> POSTROUTING -> OUT

(NAT destinazione) (NAT sorgente)

- Abilitare l'IP Forwarding via sysctl()

  # echo "1" > /proc/sys/net/ipv4/ip_forward

- ***Mascheramento IP***

  # iptables -t nat -A POSTROUTING -o ethX -j MASQUERADE

- ***Modifica dell'indirizzo di destinazione (IP-Forwarding)***

  # iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 -j DNAT --to-destination 192.168.7.7

- ***Modifica porta destinazione***

  # iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth1 -j DNAT --to-destination 192.168.1.1:8080

Dial-up verso Internet con un modem

- L'utility ***pppd*** permette di accedere a Internet con un modem

- Il file */etc/ppp/options* contiene le opzioni di configurazione:

```
lock
debug
defaultroute
noipdefault #no ip fisso
modem #usa il modem
/dev/ttyS1 #collegato alla porta COM2
115200 #con velocita' massima di 115.200 bps
crtscts # controllo di flusso hardware
asyncmap 0
name "nomeutente" #nome utente internet.
```

- Esiste un template d'esempio per il file delle opzioni: *options.tpl*

Dial-up verso Internet con un modem

- Configurazione delle credenziali di accesso

  in */etc/ppp/pap-secrets:*

  ```
  utente      *      password (ricordarsi dei tab)
  ```

- Il pacchetto pppd fornisce gli script per inzializzare il collegamento ad internet (*ppp-on)* e per terminarlo (*ppp-off)*

- Verifica con *ifconfig ppp0*

```
ppp0      Link encap:Point-Point Protocol
          inet addr:10.144.153.104  P-t-P:10.144.153.51 Mask:255.255.255.0
          UP POINTOPOINT RUNNING  MTU:552  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
          TX packets:0 errors:0 dropped:0 overruns:0
```

Connessioni Wireless 802.11

- GNU/Linux supporta vari tipi di **connessioni Wireless** tra cui 802.11, Bluetooth e IRDA
- La configurazione di una interfaccia Wireless 802.11 differisce in base al chipset della scheda utilizzata
- E' possibile utilizzare i driver forniti con il kernel Linux (device drivers -> network device support ->Wireless LAN) o reperiti da progetti esterni (ex. www.linux-wlan.org)

- **Esempio** installazione dei driver linux-wlan-ng per pcmcia prism2
  - compilazione del supporto PCMCIA e Wireless LAN nel kernel
  - download del pacchetto linux-wlan-ng
  - ./Configure e make all && make install
  - configurazione dei parametri di rete (ESSID, canale, WEP, ...)

Connessioni Wireless 802.11

- I moduli vengono caricati automaticamente all'inserimento della scheda Wireless 802.11b (demone hotplug)

- Verifica con ***iwconfig***

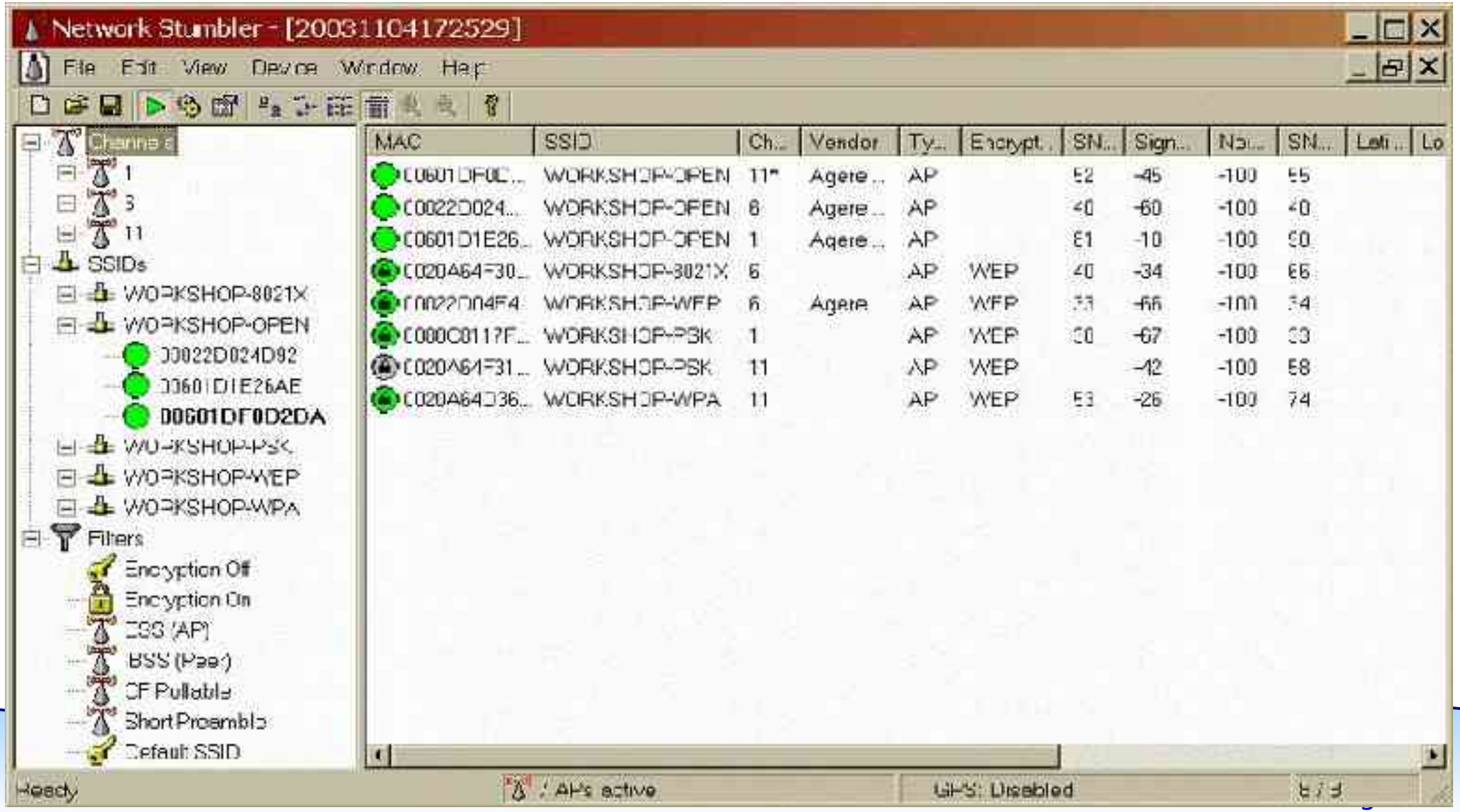
```
wlan0  IEEE 802.11-DS  ESSID:"3Com"  Nickname:"3Com"
       Mode:Auto  Frequency:2.467 GHz  Access Point: 3C:20:1B:43:22:01
       Bit Rate:11 Mb/s   Tx-Power:18 dBm
       Retry min limit:8   RTS thr:off   Fragment thr:off
       Encryption key: XXXX-XXXX-AHAS-SDFF   Security mode:restricted
       Link Quality:0  Signal level:0  Noise level:0
       Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
       Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Sicurezza Wireless 802.11

- Wardriving: attività di hacking praticata in *macchina o a piedi* (con un laptop), il cui intento è l'accesso non autorizzato a reti Wi-Fi.
- **Il wardriving è molto diffuso per la sua semplicità, sicurezza e per il divertimento suscitato nell'essere praticato.**
- Il wardriver può essere interessato a sfruttare la connettività internet di un normale utente per navigare gratis o per nascondere la propria identità.
- Il wardriver più skillato sfrutta la rete Wi-Fi come punto di accesso alla intranet dell'azienda.

Sicurezza Wireless 802.11

- Strumenti del wardriver: laptop con Wi-Fi, alimentatore per auto, antenne direzionali/omnidirezionali, GPS, software di scansione



Sicurezza Wireless 802.11

- Gli AP di default *NON* usano la crittografia e regalano l'accesso immediato all'attaccante (basta una semplice configurazione!)

- Soluzioni **security-oriented** offerte dallo standard 802.11
  - WEP (64 e 128bit): chiave statica di cifratura RC-4 condivisa
    - NOTA: il WEP è stato dimostrato essere ***vulnerabile*** ad attacchi diretti all'algoritmo
  - WPA (128 bit + 48 bit inizializzazione): chiave dinamica, CRC migliorato
  - WPA2 (128, 192 e 256bit): algoritmo crittografico AES
  - Supporto certificazione RADIUS
  - Filtro MAC sulle associazioni
  - Disattivazione annunci dell'ESSID
  - VPN

Cosa è la sicurezza (in poche parole..)

- **Il paradigma C.I.D.** descrive gli obiettivi della Sicurezza Informatica
  - *Confidenzialità:* offrire i servizi solamente a chi ne ha l'autorità
  - *Integrità*: garantire la modifica ai dati e l'accesso alle risorse in modo consistente
  - *Disponilbità*: garantire sempre un accesso assicurato e tempestivo

- **Sicurezza software:** bug di sicurezza, worm/virus/crack, attacco diretto alle password (brute-force), intercettazione dell'attività utente, trojan e backdoor, social engineering
- **Sicurezza di rete:** Denial of Service (DoS), occultamento identità (spoofing), avvelenamento delle informazioni di rete (poisoning), intercettamento di informazioni riservate dalla rete (sniffing), etc...

Ci occupiamo solo di Sicurezza di rete!

Ho una connessione di rete? E ora?

NON ESISTE SICUREZZA ASSOLUTA!

OGNI SISTEMA INFORMATICO CHE PUO' ESSERE COMPROMESSO PRIMA O POI LO SARA'

- Appena un PC è raggiungibile attraverso una connessione di rete diventa vulnerabile.
- E' necessario aver implementato soluzioni security-oriented.
- **Non è vero** che un attaccante non sia interessato a voi normali utenti, ma solo a grosse società!

Analisi e gestione dei servizi

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

- Identificazione dei **servizi attivi** e relative porte (primitiva bind())

```
# netstat -pan --inet
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address  Foreign Addr. 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 dei servizi

- **Controllo d'esecuzione dei servizi (al boot)** (dipende dalla distro)
  - Slackware: /etc/rc.d/rc.inet2, pkgtool (sottomenu)
  - Gentoo: rc-update
  - Debian: update-rc.d

- 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

- Controllo accessi attraverso hosts.allow e hosts.deny
  - sintassi: daemon_list : ... user_pattern@host_pattern ...

    (hosts.allow) in.telnetd: LOCAL, .my.domain

    (hosts.deny) ALL: ALL

Analisi e gestione dei servizi

- **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
```

Nota: Nmap senza flags controlla solo le porte in */usr/share/nmap/nmap-services*; usare -p

Analisi e gestione dei servizi

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

- Esempio: scansione automatizzata del banner dei demoni di uno o più host alla ricerca di vulnerabilità note (sfruttabili da 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

Funzionalità filtering di Iptables

- **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 soddisfatta dal pacchetto applicata l'azione (target) specificata con -j
  - Se il pacchetto passa indenne fino al fondo della catena 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

Firewall – Iptables - Esempio 1

Filtering della porta 21 (ftp) ad uno specifico host (zeus.too.fun)

zeus:~# nmap -p 21 -P0 portatile

[...]

PORT STATE SERVICE

21/tcp open ftp

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

Firewall – Iptables - 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 --rejectwith tcp-reset

zeus:~# nmap -p 21 -P0 portatile

[...]

PORT STATE SERVICE

21/tcp open ftp

puzzle:~# nmap -p 21 -P0 portatile

[...]

PORT STATE SERVICE

21/tcp closed 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)

Firewall – Iptables - Esempio 3

Filtering 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)

Crittografia di rete

- **E' molto semplice catturare il traffico di rete (sniffing) intercettando dati sensibili quali username e password**

Attaccante

 # ./nast -x

Vittima

[~]$ ncftp -u hacker www.unibg.it

```
---[ TCP Hex-Ascii Data ]----------------------------------------
0x0000    3232 3020 4654 5020 7365 7276 6572 2072    220.FTP.server.r
0x0010    6561 6479 2e0d 0a                         eady...
---[ TCP Hex-Ascii Data ]----------------------------------------
0x0000    5553 4552 2068 6163 6b65 720d 0a          USER.hacker..
```

```
Password requested by X.X.X.X for user "hacker".
Please specify the password.

Password: ***************
Login incorrect.
```

```
---[ TCP Hex-Ascii Data ]----------------------------------------
0x0000    5041 5353 206c 615f 6d69 615f 7061 7373    PASS.la_mia_pass
0x0010    776f 7264 0d0a                            word..
```

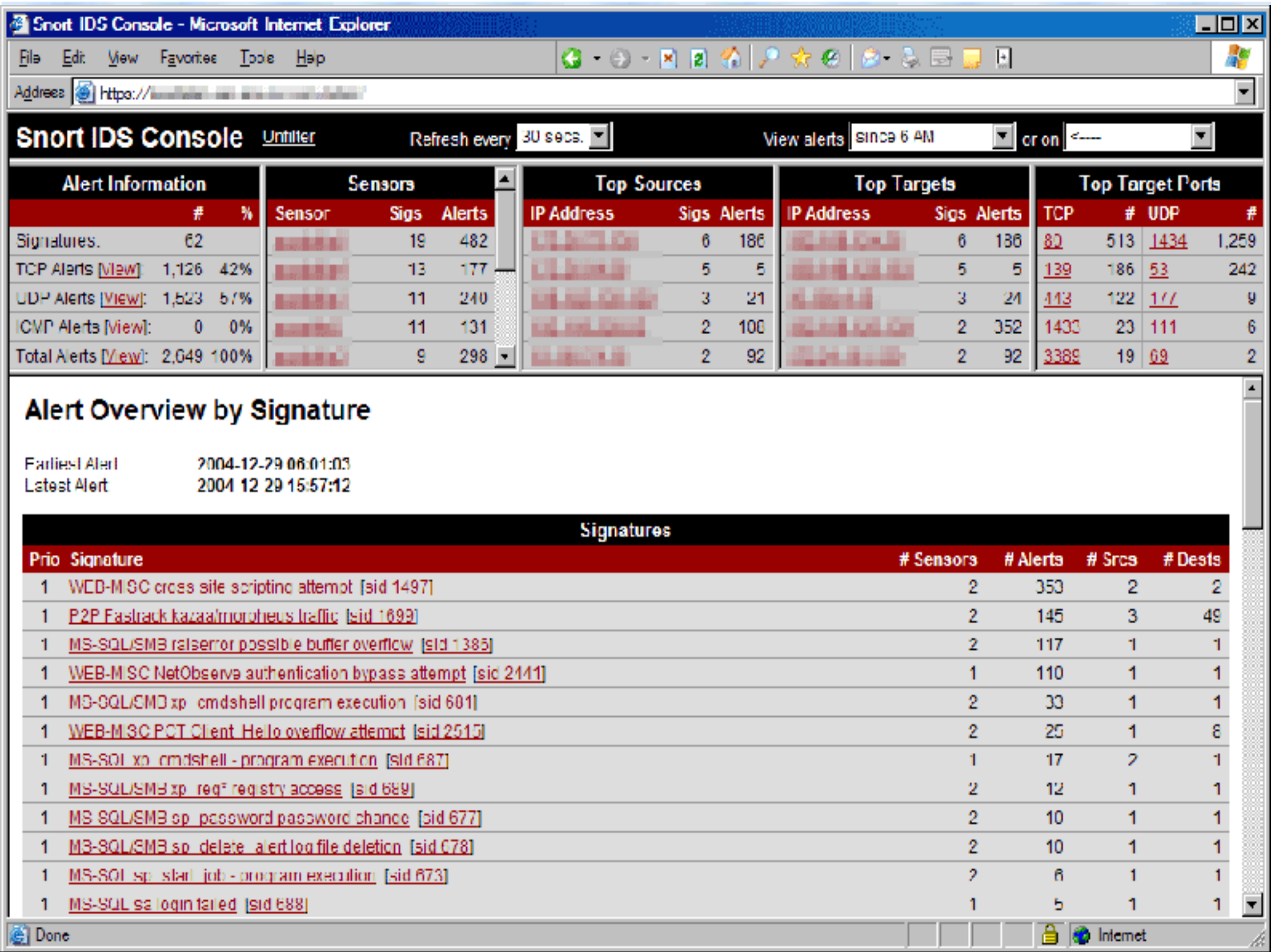
Crittografia di rete

- **Soluzione**
  - Usare i corrispondenti protocolli di rete che implementano un layer di crittografia
    - telnet -> ssh
    - ftp -> ftps
    - http -> https
    - pop3 -> pop3s o APOP (dipende dal server)
    - irc -> ircs
  - Creare canali di comunicazione crittografati (tunnel) quali
    - IPSEC (layer 3 e 4) – Openswan (http://www.openswan.org/)
    - VTUN (layer 4) – OpenVPN (http://openvpn.net/)
    - SSL – OpenSSL (http://www.openssl.org/)
  - Usare PGP per scambiarsi le mail
    - GNU Privacy Guard (http://www.gnupg.org)

Intrusion Detection System

- **Permettono di identificare attività anomale**
- Paragoniamo il firewall a una porta blindata, l'IDS all'antifurto

- Network-based IDS: catturano il traffico di rete e lo confrontano con un database di firme di attacchi noti.
  - Va installato o su una singola macchina (quella da monitorare) o su un punto di smistamento del traffico (gateway, porta di monitoring dello switch)
  - **snort**
- Host-based IDS: vanno installati sull'host da monitorare e ne controllano le attività
  - grsecurity: patch del kernel per l'identificazione di attacchi noti
  - logcheck: utility di analisi dei log


Snort IDS Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://
Snort IDS Console Unfilter
Refresh every 30 secs.
View alerts since 6 AM or on <----
Alert Information
%
Signatures. 62
TCP Alerts [View]: 1,126 42%
UDP Alerts [View]: 1,523 57%
ICMP Alerts [View]: 0 0%
Total Alerts [View]: 2,649 100%
Sensors
Sensor Sigs Alerts
19 482
13 177
11 240
11 131
9 298
Top Sources
IP Address Sigs Alerts
6 186
5 5
3 21
2 100
2 92
Top Targets
IP Address Sigs Alerts
6 186
5 5
3 21
2 352
2 92
Top Target Ports
TCP # UDP #
80 513 1434 1,259
139 186 53 242
113 122 177 9
1433 23 111 6
3389 19 69 2
Alert Overview by Signature
Earliest Alert 2004-12-29 06:01:03
Latest Alert 2004-12-29 15:57:12
Signatures
Prio Signature # Sensors # Alerts # Srcs # Dests
1 WEB-MISC cross site scripting attempt [sid 1497] 2 353 2 2
1 P2P Fasttrack kazaa/morpheus traffic [sid 1693] 2 145 3 49
1 MS-SQL/SMB raiserror possible buffer overflow [sid 1385] 2 117 1 1
1 WEB-MISC NetObserve authentication bypass attempt [sid 2111] 1 110 1 1
1 MS-SQL/SMB xp_cmdshell program execution [sid 601] 2 33 1 1
1 WEB-MISC PCT Client Hello overflow attempt [sid 2513] 2 25 1 6
1 MS-SQL xp_cmdshell - program execution [sid 687] 1 17 2 1
1 MS-SQL/SMB xp_regread registry access [sid 689] 2 12 1 1
1 MS-SQL/SMB sp_password password change [sid 677] 2 10 1 1
1 MS-SQL/SMB sp_delete_alert log file deletion [sid 678] 2 10 1 1
1 MS-SQL sp_start_job - program execution [sid 673] 2 8 1 1
1 MS-SQL sa login failed [sid 688] 1 5 1 1
Done
Internet

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 (syslog-ng)
  - 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 - Esempio di log

Nov 24 19:36:39 portatile syslogd 1.4.1: restart.

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

root@sunshine:/var/log# grep ssh messages | grep Failed |tail

Oct 18 16:12:51 sshd[3689]: **Failed password for embyte from 192.168.10.3 port 33639 ssh2**

sshd[2003]: Failed password for embyte from 127.0.0.1 port 32790 ssh2

sshd[2600]: **Failed none for invalid user raistlin from 192.168.100.2 port 33018 ssh2**

sshd[5041]: Failed password for guest from 129.241.132.214 port 32839 ssh2

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#reade

- 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

- Sicurezza Wi-Fi: http://www.spine-group.org/slides/satexpo04/satexpo2.pdf
- Rischi ed insicurezze dei sistemi informativi aziendali:

http://www.spine-group.org/slides/satexpo04/satexpo1_html/index.html

- Tecniche di prevenzione, protezione e identificazione degli attacchi informatici:

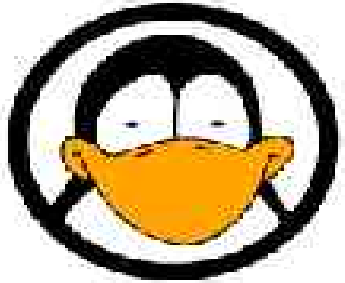
http://www.spine-group.org/slides/satexpo04/satexpo3_html/index.html

- IDS: stato dell'arte e ricerca:

http://www.spine-group.org/slides/ids04_html/ids_hkm04_html/img0.html

- Antenne Wi-Fi: dalla teoria alla pratica passando per le patatine:

http://www.spine-group.org/slides/wifi_moca.pdf



BGLug

BERGAMO - Linux User Group