

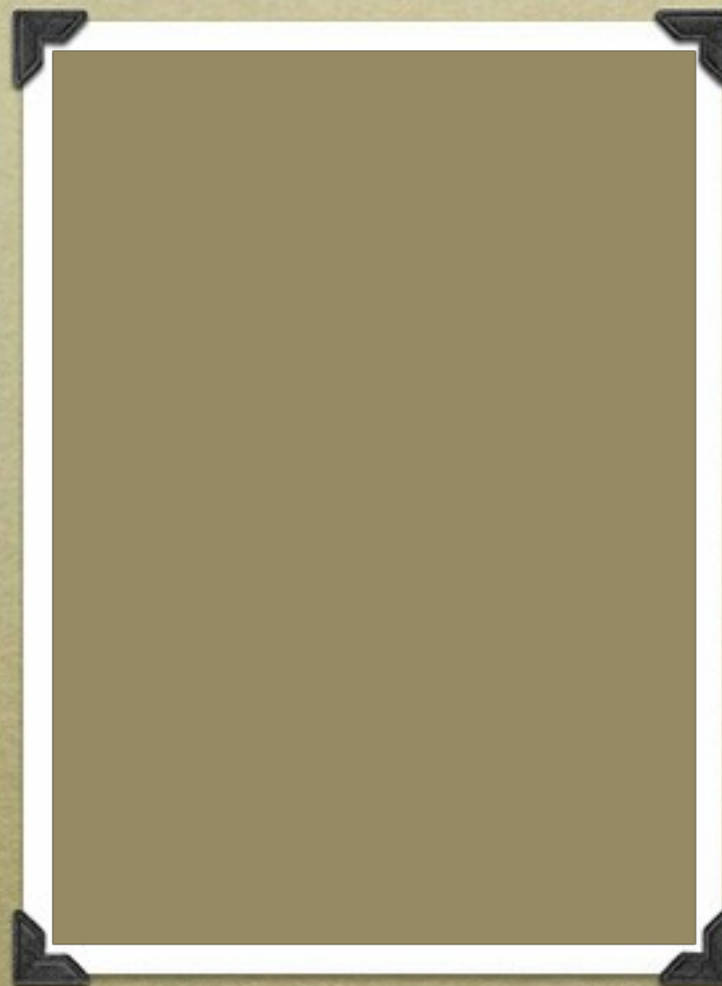
# Corso Avanzato GNU/Linux

---

Op<sup>e</sup>n consulting

Docente:

Gianluca Granero



# Di cosa ci occuperemo

---

- Configurazione e Diagnosi
  - Pacchetti
  - Rete
  - Filesystem
  - Demoni

# Di cosa ci occuperemo (2)

---

- Networking e Servizi di Base
  - Accesso Remoto
  - Condivisione di Risorse
  - Routing
  - Firewalling
  - Intrusion Detection System

# Sistemi di pacchettizzazione

---

*RedHat Package Management*  
*Debian Package*

# Configurazione e Diagnosi

---

- Sistemi di pacchettizzazione
  - DPKG
    - *Debian Package*
  - RPM
    - *RedHat Package Management*

# RPM - fondamenti

---

- **Aggiornabilità**

Usando RPM potete aggiornare singoli componenti del sistema senza reinstallarli completamente. Quando installate una nuova versione di un sistema operativo basato su RPM (come Red Hat Linux), non dovete reinstallare tutto il sistema

# RPM - fondamentali (2)

- Opzioni di interrogazione

RPM fornisce potenti opzioni di interrogazione del sistema. Nel vostro database potete effettuare ricerche di pacchetti o di semplici file, nonché sapere a quale pacchetto appartiene un certo file e risalire alle origini del pacchetto. I file contenuti in un pacchetto RPM sono in un archivio compresso, con un header binario personalizzato che racchiude informazioni utili sul pacchetto e sul suo contenuto.

# RPM - fondamentali (3)

- Verifica del sistema

Un'altra funzione molto utile è la capacità di verificare pacchetti. Se avete cancellato un file importante per alcuni pacchetti, verificate il pacchetto stesso. Durante la verifica vi viene indicata qualsiasi anomalia. A questo punto, potete reinstallare il pacchetto, se necessario. Tutti i file di configurazione che avete modificato vengono conservati durante la reinstallazione.

# RPM - fondamenti (4)

---

- Sorgenti inalterate

Uno degli obiettivi principali era quello di permettere l'utilizzo delle sorgenti inalterate del software, come distribuite dall'autore stesso. In RPM sono contenuti i sorgenti originali e tutte le modifiche che sono state apportate, nonché tutte le istruzioni per la ricompilazione.

# RPM - fondamentali (5)

---

- Il formato standard dei pacchetti
  - foo-1.0-1.i386.rpm
    - *nome del pacchetto ( foo )*
    - *versione ( 1.0 )*
    - *release ( 1 )*
    - *architettura ( i386 )*

# RPM - utilizzo

- **QUERYING PACKAGES...**

- `rpm {-q | --query} [select-options] [query-options]`
  - *rpm -qa -> visualizza tutti i pacchetti installati*
  - *rpm -qai -> visualizza le info su tutti i pacchetti installati*
  - *rpm -qail -> visualizza le info + files su tutti i pacchetti installati*

# RPM - utilizzo (2)

- Opzioni di selezione...
  - `-a` interroga tutti i pacchetti installati
  - `-f <file>` interroga il pacchetto contenente il `<file>`
    - *Quando specificate un file, dovete indicare il percorso del file (per esempio, `/usr/bin/lis` )*
  - `-p <filepacchetto>` interroga il pacchetto `<filepacchetto>`

# RPM - utilizzo (3)

- Opzioni di selezione...
  - `-g <gruppo>`
    - *gruppo -> Development/Tools*
    - *gruppo -> System\Environment/Kernel*

# RPM - utilizzo (4)

- Opzioni di interrogazione...
  - **-i** mostra informazioni sul pacchetto
  - **-l** mostra l'elenco dei file contenuti nel pacchetto
  - **-S** mostra lo stato di tutti i file nel pacchetto
  - **-d** mostra un elenco dei file di documentazione
  - **-C** mostra un elenco dei file di configurazione

# RPM - utilizzo (5)

---

- Opzioni di interrogazione...
  - -v per trasformare la visualizzazione degli elenchi in modalità simile a quella del comando *ls -l*

# RPM - utilizzo (6)

- AND VERIFYING...

- la verifica confronta le dimensioni, MD5, i permessi, il tipo, il proprietario e il gruppo di ogni file
- `rpm -V foo` verifica che tutti i file nel pacchetto `foo` siano identici a quelli installati originariamente
- `rpm -Vf /bin/vi` verifica il pacchetto che contiene il file `/bin/vi`

# RPM - utilizzo (7)

- Tag di verifica:
  - 5 - *MD5 checksum*
    - S - dimensioni del file
    - L - link simbolico
    - T - ora di modifica del file
    - D - dispositivo
    - U - utente
    - G - gruppo
  - M - *modalità (include permessi e tipo di file)*
    - ? - file non leggibile

# RPM - installazione

---

- Opzioni:
  - -i : installa
  - -U : aggiorna / installa
  - -h : stampa una progress bar
  - -v : aumenta il tasso d'informazione

# RPM - installazione (2)

- Utilizzo tipico
  - rpm -Uvh foo-1.0-1.i386.rpm
- Risposta in caso di successo

*Preparing...*

```
##### [100%]
```

*1:foo*

```
##### [100%]
```

# RPM - installazione (3)

- La firma di un pacchetto viene verificata durante l'installazione o l'aggiornamento di un pacchetto
- Se la verifica della firma non riesce, verrà visualizzato un messaggio di errore come il seguente:

```
error: V3 DSA signature: BAD,key ID  
0352860f
```

# RPM - rimozione

- Rimozione di un pacchetto foo-1.1-1
  - rpm -e foo
- Attenzione ai problemi di DIPENDENZA

*error: removing these packages break dependencies:  
foo is needed by bar-2.0.20-3.i386.rpm*

# RPM - Refresh

- Installa nuove versioni di pacchetti già presenti nel sistema
  - `rpm -Fvh *.rpm`
    - *vengono aggiornati solo i pacchetti già presenti nel sistema*

# RPM - problemi

---

- Pacchetti già installati
  - *Package foo-1.0-1 is already installed*
  - opzione `--replacepkgs`
    - *installa i file di configurazione originali*

# RPM - problemi (2)

- File in conflitto
  - file */usr/bin/foo* from install of *foo-1.0-1* conflicts with file from package *bar-2.0.20*
  - opzione *--replacefiles*

# RPM - problemi (3)

- Dipendenze non risolte
  - error: Failed dependencies:  
bar.so.2 is needed by foo-1.0-1  
Suggested resolutions:  
bar-2.0.20-3.i386.rpm
  - `rpm -q --redhatprovides bar.so.2`
  - sito [www.rpmfind.net](http://www.rpmfind.net)

# RPM - problemi (4)

---

- Dipendenze non risolte (2)
  - opzione `--nodep`

# RPM - problemi (4)

---

- Aggiornamento
  - incompatibilità in avanti
    - *file originali rinominati .rpmsaved*
  - installazione di versioni precedenti
    - *rpm -Uvh --oldpackage foo-1.0-1.i386.rpm*

# RPM - il database

---

- Ricostruire il DB dei pacchetti
  - `rpm --initdb | --rebuilddb`
- Trovare i file di RPM
  - `/var/lib/rpm/`

# RPM - ricompilazione

---

- RPMS - pacchetto sorgente
  - `rpmbuild --clean --target=i386 foo.rpms`
- Serve per ottimizzare un pacchetto

# RPM - documentazione

---

- `man rpm`
- `rpm --help`
- <http://www.rpm.org/>
- Package Management Tool
- <http://rhn.redhat.com/>

# DPKG - fondamenti

---

- Sistema di pacchettizzazione per distribuzione *DEBIAN*
- Molto simile ad RPM
- Esiste '*alien*' per trasformare RPM in DEB
- `nome_pacchetto_versione-revisione.deb`

# DPKG - debian pkg

---

- Il pacchetto:
  - è in formato *ar*
  - contiene
    - *data.tar.gz*
    - *control.tar.gz*

# DPKG - fondamenti (2)

- utilizzo di alien
  - alien --to-deb  
[opzioni] file\_da\_convertire
  - alien --to-rpm  
[opzioni] file\_da\_convertire
  - alien --to-tgz  
[opzioni] file\_da\_convertire
  - alien --to-slp  
[opzioni] file\_da\_convertire

# DPKG - utilizzo

---

- `dpkg -c zsh_3.1.2-10.deb`
  - Mostra l'elenco dei file che compongono il pacchetto `zsh`, contenuti nell'archivio indicato, esclusi i file che vengono creati dagli script del pacchetto stesso

# DPKG - utilizzo (2)

---

- `dpkg -I zsh_3.1.2-10.deb`
  - Mostra tutte le informazioni disponibili sull'archivio indicato

# DPKG - utilizzo (3)

---

- `dpkg -i zsh_3.1.2-10.deb`
  - Installa, o aggiorna, il pacchetto contenuto nell'archivio indicato, ammesso che ciò sia possibile in relazione alle dipendenze di questo

# DPKG - utilizzo (4)

---

- `dpkg -r zsh`
  - Rimuove il pacchetto indicato, senza eliminare i file di configurazione

# DPKG - utilizzo (5)

---

- `pkg --purge zsh`
  - Elimina completamente il pacchetto indicato, compresi i file di configurazione

# DPKG - utilizzo (6)

---

- `dpkg -l`
  - Elenca lo stato di tutti i pacchetti installati, o dei quali rimangono i file di configurazione

# DPKG - utilizzo (7)

---

- `dpkg -l z\*`
  - Elenca lo stato di tutti i pacchetti conosciuti che iniziano con la lettera «Z»

# DPKG - utilizzo (8)

---

- `dpkg -s zsh`
  - Mostra le informazioni sullo stato del pacchetto indicato, in modo più dettagliato

# Stato di un pacchetto

---

- TAG
  - installed
    - *unpacked and configured OK*
  - half installed
    - *not completely installed*
  - not-installed

# Stato di un pacchetto (2)

---

- TAG
  - unpacked
    - *unpackaged but not configured*
  - half-configured
    - *not completely configured*

# Stato di un pacchetto (3)

---

- TAG
  - config-files
    - *only configuration files exist*

# DPKG - utilizzo (9)

---

- `dpkg -L zsh`
  - Elenca i file che appartengono al pacchetto `zsh`

# DPKG - utilizzo (10)

---

- `dpkg -S /bin/cat`
  - Cerca di scoprire a chi appartiene il file `/bin/cat`

# DPKG - albero della distribuzione

---

- Distribuzioni
  - stable, testing, unstable
- Gruppi
  - main, contrib, non-free, non-US, local

# APT

advanced package tool

- Utility di gestione delle sorgenti di pacchetto
  - Programma fondamentale *apt-get*
  - File di configurazione */etc/apt/source.list*
- *deb file:/dir/ stable main contrib non-free non-US*
- *deb file:/dir/ stable main contrib non-free*
- *deb http://sito/debian stable main contrib non-free*
- *deb http://sito/debian-non-US stable non-US*

# APT - utilizzo

---

- Aggiornamento della lista dei pacchetti
  - `apt-get update`
- Aggiornamento dei pacchetti
  - `apt-get upgrade`
- Installazione di un pacchetto (+ dipendenze)
  - `apt-get install zsh`

# APT - utilizzo (2)

---

- Upgrade della distribuzione (*opzionale*)
  - `apt-get -f dist-upgrade`
- Configurazione dei pacchetti aggiornati
  - `dpkg --configure --pending`

# dselect

---

- Tool di configurazione visuale
- Shell-mode, molto leggero
- Si utilizzano i tasti +, -, \_
  - risolve direttamente le dipendenze

# La rete

*Configurazione e Diagnosi*

# La Rete

---

- Viene mutuata da BSD
- Supporta IPv4 e IPv6
- Disponibili demoni routing
  - gated, routed e Zebra
- Supporta IPsec
  - freeSwan o USAGI

# La Rete (2)

---

- Comandi di configurazione
  - ifconfig
  - route
  - arp

# ifconfig

- ifconfig interface [aftype] options | address
  - interface -> eth0, en0, ...
    - *ifconfig -a mostra tutte le interfacce*
  - **address family type** -> inet (TCP/IP), inet6 (IPv6), ax25 (AMPR Packet Radio), ddp (Appletalk Phase 2), ipx (Novell IPX) e netrom (AMPR Packet radio)

# ifconfig (2)

- ifconfig interface [aftype] options | address
  - options
    - *up, down, [-]arp, [-]promisc, [-]allmulti, metric [n], mtu [n], dstaddr, pointopoint*
    - *add addr/prefixlen (IPv6 address)*
    - *del addr/prefixlen (IPv6 address)*
    - *tunnel aa.bb.cc.dd (IPv6-in-IPv4)*

# ifconfig - utilizzo

---

- ifconfig eth0 193.205.140.245/24 up
  - attiva la eth0
    - *indirizzo IPv4* 193.205.140.245
    - *netmask* 255.255.255.0
    - *network* 193.205.140.0

# Linux- IPv6

---

- Check List per IPv6
  - kernel ready?
    - */proc/net/if\_inet6*
      - *modprobe -a ipv6*
  - net tools ready?
    - *route -?*
    - *ifconfig -?*
      - *family inet6*

# ifconfig - IPv6

---

- Attivare l'interfaccia IPv4
  - `ifconfig eth0 193.205.140.243 /24 up`
- Attivare il supporto IPv6
  - `ifconfig eth0 inet6 add 3ffe:ffff:0:f101::1 /64`

# ifconfig - MAC address

---

- E' possibile variare il MAC address
  - `ifconfig eth0 hw ether aa:bb:cc:dd:ee:ff`
    - *non si è cambiato definitivamente*
    - *alla successiva accensione viene ripristinato*
    - *attenzione al MAC-Spoofing*

# route

---

- Tool di manipolazione della routing table
  - mantenimento di rotte statiche
    - *add*
    - *del*
  - visualizzazione della tabella

# route - add

- `route [-v] [-A family] add [-net | -host] target [netmask Nm] [gw Gw] [[dev] If]`
  - `-v` Verbose
  - `-A` `inet` | `inet6` | ...
  - `-net` il *target* è una rete (netmask)
  - `-host` il *target* è un host
  - `gw` indirizzo del gateway per il *target*

# route del

- route [-v] [-A family] del [-net|-host] target [gw Gw] [netmask Nm] [[dev] If]
  - attenzione al matching di rete e netmask
    - *route del 10.0.0.0 cancella solo se esiste una sola rotta 10.0.0.0*
      - *10.0.0.0/24 e 10.0.1.0/24 sono fuorvianti*

# route - utilizzo

---

- Inserimento di una rotta
  - ifconfig inserisce per noi
    - *route add -net 10.0.0.0 eth0*
      - *la netmask ??*
- Inserimento della rotta di default
  - descrive chi è il default gw
    - *route add default gw 10.0.0.1 eth0*

# route - utilizzo

---

- Cancellazione di una rotta
  - route del -net 10.0.0.0/24 eth0

# route - utilizzo

---

- Visualizzazione della routing table
  - route
    - *risolve i nomi*
  - route -C
    - *visualizza la cache del kernel*
  - route -A inet6
    - *visualizza solo le rotte IPv6*

# Letture della routing table

- Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
193.204.161.0	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	exomi-gw.unirom	0.0.0.0	UG	0	0	0	eth0

# I Flags

• 193.204.161.0 \* 255.255.255.0 *U* 0 0 0 eth0

- U (route is up)  
H (target is a host)  
G (use gateway)
- R (reinstate route for dynamic routing)  
D (dynamically installed by daemon or redirect)  
M (modified from routing daemon or redirect)  
A (installed by addrconf)
- C (cache entry)  
! (reject route)

# La metrica

---

- Numero di hop che ci vogliono per raggiungere quella net | host
  - non utilizzata dal Kernel
  - utilizzata dai demoni di routing
  - impostabile con il parametro *metric*

# arp

---

- Ogni macchina ha una sua cache ARP
  - si compila automaticamente
  - possono essere aggiunte delle entry
  - possono essere cancellate delle entry

# arp - utilizzo

- `arp [-vn] [<HW>] [-i <if>] [-a] [<hostname>]`
  - visualizza
- `arp [-v] [-i <if>] -d <hostname> [pub]  
[nopub]`
  - cancella
- `arp [-vnD] [<HW>] [-i <if>] -f [<filename>]`
  - inserisce da file

# arp - utilizzo (2)

- `arp [-v] [<HW>] [-i <if>] -s <hostname>  
<hwaddr> [temp][noper]`
  - inserisce l'entry relativa a <hostname>
- `arp [-v] [<HW>] [-i <if>] -s <hostname>  
<hwaddr> [netmask<nm>] pub`
  - inserisce e propaga l'entry (proxy arp)

# arp - utilizzo (3)

- `arp [-v] [<HW>] [-i <if>] -Ds <hostname> <if> [netmask <nm>] pub`
  - inserisce e propaga l'entry
  - ricava <HW> dall'interfaccia <if>

ip

---

- OBSOLETO iproute

# La Rete (3)

---

- Comandi di diagnosi
  - ping, ping6
  - traceroute, traceroute6
  - netstat
  - tcpdump

# netstat

---

- Visualizza
  - connessioni di rete
  - tabelle di routing
  - statistiche d'interfaccia
  - connessioni mascherate
  - gruppi multicast

# ping

---

- Manda un messaggio ICMP (echo request)
- Aspetta una risposta ICMP (echo reply)
- Parametri:
  - `-c <count>`
  - `-f` (flooding)
  - `-s <packet size>`

# traceroute

- Visualizza la rotta seguita da un pacchetto IP
  - -m <TTL>
  - -p <port>
  - -s <src-addr>
- Permette LSR - loose source routing
  - -g <host>

# netstat - utilizzo

- senza alcun parametro visualizza
  - connessioni di rete aperte
    - *protocollo di livello 4*
    - *byte in uscita*
    - *byte in ingresso*
    - *indirizzi (locale e remoto)*
    - *stato della connessione*

```
tcp  0  0  tocai.dia.uniroma3.:ssh 193.204.161.67:1317 ESTABLISHED
```

# netstat - server

- netstat -l
  - mostra le porte in stato LISTEN

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	*:mysql	*:*	LISTEN
tcp	0	0	*:http	*:*	LISTEN
tcp	0	0	*:ftp	*:*	LISTEN
tcp	0	0	*:ssh	*:*	LISTEN

# netstat - statistiche

- netstat -s
  - mostra le statistiche divise per protocollo

## **Icmp:**

**712 ICMP messages received**  
**2 input ICMP message failed.**  
**ICMP input histogram:**  
**destination unreachable: 8**  
**echo requests: 695**  
**echo replies: 7**  
**856 ICMP messages sent**

## **Ip:**

**266096303 total packets received**  
**0 forwarded**  
**0 incoming packets discarded**  
**265662628 incoming packets delivered**  
**263532112 requests sent out**

# tcpdump

- Tool per il dump del traffico di rete
  - tcpdump [ -adeflnNOpqRStuvxX ] [ -c count ] [ -C file\_size ] [ -F file ] [ -i interface ] [ -m module ] [ -r file ] [ -s snaplen ] [ -T type ] [ -U user ] [ -w file ] [ -E algo:secret ] [ expression ]
- Può salvare e leggere da file
- Usa espressioni booleane come filtro
- Abilita il *promiscuous mode* (default)
- Risolve i nomi

# tcpdump - utilizzo

- `tcpdump -n not port 80 and host 193.204.161.11`
- `tcpdump -n arp or \( \(port 80 and port 23\) or host pippo.plu.to \)`
- `tcpdump -i lo`
- `tcpdump -r file-scrittura.dump`
- `tcpdump -w file-lettura.dump`
- `tcpdump -vvv`
- Protocolli supportati
  - ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp and udp

# La Rete (4)

---

- Demoni di Routing
  - gated
  - Zebra

# gated

---

- Prodotto commerciale di nexthop
  - rilasciato con licenza GPL usi accademici
  - gestisce Rip v1, OSPF, Rip v2
  - file di configurazione */etc/gated.conf*

# gated (2)

- File di configurazione

- rip yes  
  {  
    interface all ripin ripout version 2;  
  }
- import proto rip  
  {  
    all ;  
    default restrict ;  
  }

# gated (3)

- File di configurazione:
  - export proto rip
    - {
      - proto direct ;
      - proto static metric 1;
    - }

# Zebra

- Prodotto Open Source (GPL)
- Multi demone (uno per ogni protocollo)
  - **bgpd**  
Manages BGP-4 and BGP-4+ protocol
  - **ripd**  
Manages RIPv1, v2 protocol
  - **ripngd**  
Manages RIPng protocol
  - **ospfd**  
Manages OSPFv2 protocol
  - **ospf6d**  
Manages OSPFv3 protocol

# Zebra (2)

---

- File di configurazione
  - */etc/zebra*
  - *<protocollo>.conf*
  - *zebra.conf*
    - per lo scambio di informazioni fra i protocolli

# Zebra (3)

- router bgp 7675
  - ! bgp router-id 10.0.0.1
  - ! network 10.0.0.0/8
  - ! neighbor 10.0.0.2 remote-as 7675
  - ! neighbor 10.0.0.2 route-map set-next-hop out
  - ! neighbor 10.0.0.2 ebgp-multihop
  - ! neighbor 10.0.0.2 next-hop-self
  - !
  - ! access-list all permit any
  - !
  - ! route-map set-next-hop permit 10
  - ! match ip address all
  - ! set ip next-hop 10.0.0.1

# La Rete (5)

- I servizi
  - inetd, telnet, ftp, ssh
  - lpd, cups
  - nfs, smb
  - sendmail, postfix
  - MySql, PostgreSQL
  - Apache, Squid

# inetd

---

- Il ‘super-server’ internet
  - gestisce le connessioni con i servizi
  - serve per ridurre il carico applicativo
  - può prendere decisioni

# inetd (2)

---

- File di configurazione
  - /etc/inetd.conf
  - /etc/hosts.allow
  - /etc/hosts.deny

# inetd - inetd.conf

---

- Ogni riga contiene:
  - service name
  - socket type
  - protocol
  - wait/nowait[.max]
  - user[.group]
  - server program
  - server program arguments

# inetd.conf

---

- ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/proftpd
  - servizio ftp su TCP multithreaded dell'utente root gestito dai tcp-wrappers che passano il controllo a proftpd
- daytime dgram udp wait root internal
  - servizio di sincronizzazione temporale udp, con gestione del datagramma (max 40 server serializzabili) dell'utente root gestito dal demone inetd stesso

# inted.conf - parametri

---

- The *service-name* entry is the name of a valid service in the *file/etc/services*
- The *socket-type* should be one of 'stream', 'dgram', 'raw', 'rdm', or 'seqpacket'
- The *protocol* must be a valid protocol as given in */etc/protocols*

# inted.conf - parametri

---

- The *wait/nowait* entry is applicable to datagram sockets only
  - gli altri devono avere *nowait*
- *nowait* fa diventare il server un 'multithreaded server' lasciando libero il canale *a priori* del processamento (no - timeout)

# inetd.conf - parametri

---

- The *server-program* entry should contain the pathname of the program
- The *server program arguments* should be just as arguments normally are, starting with *argv[0]*

# tcpwrappers

---

- Prima forma di firewalling host-based
- Componenti del controllo:
  - tcpd - access control facility
  - hosts\_access - host access control files
  - utilizzati in congiunzione con *inetd*

# hosts.allow e hosts.deny

---

- Commenti: iniziano per #
- Righe di specifica
  - daemon\_list:client\_list
    - *process names (argv[0] values)*
    - *host names, host addresses, patterns*
    - *daemon@host and user@host*

# hosts.allow e hosts.deny

(2)

- Pattern accettabili:
  - nomi che partono con ‘.’
    - *.lugroma3.org*
  - stringhe che finiscono con ‘.’
    - *193.205.*

# hosts.allow e hosts.deny

(3)

- Pattern accettabili:
  - `n.n.n.n/m.m.m.m'
  - `n.n.n.n/mm'
  - *ip + netmask*
- Wildcards:
  - ALL, LOCAL, PARANOID, EXCEPT

# tcpwrappers

---

- Peso delle regole nei files:
  - più pesanti le regole di *allow*
  - non c'è precedenza ordinale

# hosts.allow e hosts.deny

(4)

- /etc/hosts.deny:  
ALL: ALL
- /etc/hosts.allow:  
ALL:127.0.0.1  
ALL:10.0.0.0/255.0.0.0

in.telnetd:cecchetti@10.0.0.102

sshd:..lugroma3.org

proftpd:ALL

imapd:ALL

# telnet

---

- Controllato da inetd
  - in.telnetd
- esistono server avanzati con
  - kerberos 5
  - SSL

# ftp

---

- */etc/ftpusers*
  - definisce gli utenti a cui non è permesso il login
- */etc/ftpd.conf*
  - command class [arguments]

# ftp - sicurezza

---

- chroot
  - nella directory *chroot* devono trovarsi:
    - *librerie*
    - *eseguibili*
    - *tutto il necessario per l'esecuzione....*

# proFTPd

- Server FTP maggiormente utilizzato
  - */etc/proftpd.conf*
- *Direttive <Directory> come Apache*
  - *<Directory \*>*
    - <Limit WRITE>*
    - DenyAll*
    - </Limit>*
    - </Directory>*

# ssh

- Secure Shell Protocol v.1 (porta 22)
  - autenticazione host-based
    - */etc/hosts.equiv* o */etc/ssh/ssh\_known\_hosts*
    - *.rhosts* o *.shosts*
  - autenticazione combinata
    - *chiave RSA + rhost*
      - */etc/ssh/ssh\_known\_hosts*

# ssh

- Generazione delle chiavi

`ssh-keygen [-q] [-b bits] -t type [-N new_passphrase] [-C comment] [-f output_keyfile]`

- Agente di autenticazione

- ssh-agent padre delle applicazioni di login
- ssh-add aggiunge identità da gestire

# ssh

- RSA base authentication
  - algoritmo crittografia a chiave pubblica
    - *\$HOME/.ssh/authorized\_keys*
  - challenge con random number

# ssh2

- Secure Shell Protocol v.2 (porta 22)
  - RSA, DSA
- file /etc/ssh/sshd\_config  
/etc/ssh/ssh\_config
  - attenzione
    - *PermitRootLogin*
    - *X11Forwarding*

# ssh2

---

- Fasi di autenticazione
  - metodo hostbased
  - metodo public key
  - keyboard-interactive

# lpd

- line printer spooler daemon
  - */etc/hosts.equiv* o */etc/hosts.lpd*
  - */etc/printcap*
  - porta 515
  - directory di spooling */var/spool/lpd*

# lpd

---

- Visualizzazione della coda
  - lpq -P<nome\_coda>
- Rimozione del job
  - lprm <numero>
- Console di gestione
  - lpc

# lpd

---

- Tool di creazione della coda
  - printtool
- Filtri per le code
  - */usr/lib/printfilters*

# cups

---

- common unix printing system
  - sistema evoluto per la gestione delle code di stampa basato su IPP
  - compatibile con *lpd*
  - */etc/cups/cupsd.conf*
  - */etc/cups/printers.conf*

# cups

- Sistema di gestione web-based
  - `http://localhost:631`
- Attenzione alle richieste di discovery
  - `BrowseAddress x.y.z.255`
  - `BrowseAllow 127.0.0.1`  
`BrowseAllow @LOCAL`  
`BrowseDeny All`

# nfs

- Network FileSystem
  - nfsd.o
    - *kernel module part*
  - rpc.nfsd
    - *user level part*
  - rpc.mountd
    - *mount request daemon*

# nfs

- Controllo delle esportazioni
  - */etc/exports*
    - */home 10.0.0.3(rw,no\_root\_squash,sync)*
      - rw, ro
      - [no\_]root\_squash
      - [a]sync

# nfs

---

- Impostare le esportazioni
  - `exportfs -a`
- Controllare le esportazioni
  - `exportfs`

# nfs

- Montare una partizione NFS
  - `mount -t nfs <server>:/<rdir> <mdir>`
  - */etc/fstab*

seneca:/home /home nfs defaults, rsize=8192, wsize=8192 0 0

# samba

---

- SMB/CIFS services per client tipo:
  - MSCLIENT 3.0 for DOS
  - Windows for Workgroups
  - Windows 95/98/ME
  - Windows NT, Windows 2000
  - OS/2
  - DAVE for Macintosh

# samba

---

- **smbd**
  - demone SMB/CIFS
- **nmbd**
  - netbios nameserver (over IP)
- **smbclient**
  - SMB/CIPF resource client

# samba

- /etc/smb.conf

- contiene le configurazioni dei servizi

- *directory*

[public]

path = /tmp

- *stampanti*

public = yes

- *autenticazione*

only guest = yes

writable = yes

printable = no

# samba

---

- Visualizzare le risorse disponibili
  - `smbclient -L <indirizzo>`
- Visualizzare le risorse di un gruppo
  - `smbclient -L <indirizzo> -W`

# samba - visualizzare

Sharename	Type	Comment
-----	----	-----
public	Disk	
IPC\$	IPC	IPC Service (Samba 2.2.3a (build 26))
ADMIN\$	Disk	IPC Service (Samba 2.2.3a (build 26))

Server	Comment
-----	-----
ORATIO	Samba 2.2.3a (build 26)

Workgroup	Master
-----	-----
LADISPOLI	GIANO
WORKGROUP	ORATIO

# sendmail

---

- mail transport agent
  - spedisce i messaggi a 1 o più caselle
  - veicola i messaggi di posta fra diverse reti
  - gestisce il forwarding
  - non è dotato di un MUA predefinito

# sendmail - i file

---

- /etc/mail
  - /sendmail.conf
    - *configurazione del server*
  - /sendmail.cf
    - *configurazione del servizio*

# sendmail - i file (2)

---

- Altri file di configurazione
  - */etc/mail/aliases*
    - *alias di posta nel formato alias:mail*
  - */var/spool/mqueue/\**
    - *message repository*

# sendmail - m4

---

- Il linguaggio di configurazione è complesso
- Si preferisce scrivere delle macro config
  - si passa la macro config al macro compiler
  - il Mcompiler produce il file di configurazione finale
    - *in questo modo si evitano anche problemi di configurazione su differenti versioni*

# sendmail -

---

- Alcuni famosi FLAGS
  - dominio per cui gestire la posta
    - *Cw*<*dominio*>
  - macchine locali al dominio
    - *Fw*<*file con nomi di host FQDN*>
  - macchine / domini per cui fare relay
    - *FR-o* <*file con nomi di dominio*>

# sendmail - log

- I log di sendmail sono gestiti da syslog
  - si trovano in */var/log/mail*
    - *danno info sugli accessi e sulle spedizioni*

**Jul 28 18:07:05 seneca sm-mta[11960]: h6SG75Rt011960:  
from=<clubtiscali@it.tiscali.com>, size=12960, class=0, nrcpts=1,  
msgid=<3F1E2054002E30E8@mail-8.tiscali.it> (added by  
postmaster@mail-8.tiscali.it), proto=ESMTP, daemon=MTA,  
relay=ricciardi@localhost [127.0.0.1]**

**Jul 28 18:07:05 seneca sm-mta[11970]: h6SG75Rt011960:  
to=<ricciardi@localhost>, delay=00:00:00, xdelay=00:00:00, mailer=local,  
pri=43164, dsn=2.0.0, stat=Sent**

# postfix

---

- mail transfer agent
  - sviluppato da IBM
  - rilasciato *OPENSOURCE*
  - compatibile con *sendmail*

# postfix - moduli

---

- postfix
  - modulo di controllo ed interfaccia
- master
  - demone SMTP

# postfix - i comandi

- Comand postfix
  - start
    - *inizializza il servizio - chk configurazione*
  - stop
    - *ferma il servizio in modo conservativo*
  - flush
    - *forza la spedizione dei messaggi*

# postfix - i comandi (2)

---

- I comandi
  - check
    - *Validazione della configurazione*
  - reload
    - *rilettura della configurazione*
  - abort
    - *stop immediato del processo*

# postfix - configurazione

- File di configurazione in */etc/postfix/*
  - main.cf
    - *configurazione del servizio*
  - master.cf
    - *configurazione del demone SMTP*
  - transport
    - *configurazione del delivery*

# MySQL

---

- RDBMS
  - supporta BLOB (64MB)
  - transazionale (bind esterno)
  - molto veloce
  - ODBC, JDBC, nativo php
  - esistono degli HOWTO

# mysql - fondamentali

---

- Server
  - mysqld
- Interfaccia shell
  - mysql
    - *-h <host> -u<user> -p<password>*

# mysql - accesso

---

- Permette la gestione degli utenti
  - permessi su singole tabelle
  - permessi immersi in *mysql.user*
  - attivazione con *mysqladmin flush-privileges*

# mysql - gestione

---

- interfaccia Web - oriented
  - phpMyAdmin
- dump e check
  - mysqldump, mysqlcheck
- database
  - /var/lib/mysql

# PostgreSQL

---

- (O) Relational DataBase Management Sys
  - Large Object (4GB) (BLOB)
  - Transazionale
  - Supporto per Store Procedures (PL/SQL)
  - ODBC, JDBC, nativo php e perl
  - non esistono HOWTO

# postgres

---

- Server
  - postmaster
- Interfaccia Shell
  - psql
    - *-U<utente> <database>*
    - *-h <host>*

# postgres - nuovo DB

---

- Connessione al template1
  - `psql -Upostgres template1`
    - *CREATE DATABASE <nome>*

# postgres - accesso

- /etc/postgresql

- pg\_hba.conf

- *client access config file*

- | # | TYPE  | DATABASE | IP_ADDRESS | MASK            | AUTH_TYPE |
|---|-------|----------|------------|-----------------|-----------|
|   | local | all      |            |                 | trust     |
|   | host  | all      | 10.0.0.110 | 255.255.255.255 |           |

  
sameuser

- pg\_ident.conf

- *client user map file*

# pgsql - configurazione

- /etc/postgresql
  - postgresql.conf
    - *#tcpip\_socket = false*
    - #ssl = false*
    - #max\_connections = 32*
    - #port = 5432*
    - #hostname\_lookup = false*
    - #show\_source\_port = false*
    - #unix\_socket\_directory = "*
    - #unix\_socket\_group = "*
    - #unix\_socket\_permissions = 0777*

# postgres - files

---

- /var/lib/postgres
  - data/base
    - *database repository*
  - global
    - *file di runtime*
  - pg\_clog pg\_xlog
    - *transaction logging*

# Apache

---

- Cosa dire?

# Logging

*syslog ci aiuti...*

# Il logging

---

- Problema o Necessità ?
  - controllare un sistema vuol dire
    - *monitorare gli INPUT*
    - *monitorare l'OUTPUT*
    - *modificare la funzione di trasferimento per rendere minimo l'errore*

# input e output

---

- Azioni e Reazioni
  - le possiamo controllare con i LOG
    - *ogni applicazione dovrebbe averne uno*
    - *sarebbe ottimo poter scegliere il livello di dettaglio da visualizzare*

# funzione di trasferimento

---

- Si agisce sui file di configurazione dei
  - demoni applicativi
  - sistemi di firewalling
  - sistemi di routing

# syslogd

---

- demone che gestisce tutto il log
  - proveniente dalle applicazioni
  - proveniente dal kernel
  - legge messaggi da
    - */dev/log*
    - */dev/klog*

# syslog - configurazione

---

- /etc/syslog.conf
  - ogni linea contiene due parti
    - *selettore*
    - *azione*

# syslog - selettori

---

- Selettore diviso in
  - facility
    - *parte del sistema che ha generato il msg*
  - . (dot)
  - livello
    - *gravità del messaggio*

# syslog - produttore

---

- Facility
  - auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp
  - local0 ... local7

# syslog - livello

---

- Level
  - emerg, alert, crit, err, warning, notice, info e debug
  - none
    - *disabilita la facility*

# syslog - mix

- + produttori, stesso livello
  - prod1,prod2,prod3.livello azione
- 1 produttore, tutti i livelli
  - prod1.\* azione
- tutti i produttori, 1 livello
  - \*.emerg azione
- + produttori, stessa azione
  - prod1.lev1;prod2.lev2 azione

# syslog - esempio

- \*.err;kern.\*;authpriv,remoteauth.none;mail.crit

/dev/console

\*.notice;\*.info;authpriv,remoteauth

/var/log/system.log

kern.debug;mail.crit

/var/log/system.log

# The authpriv log file should be restricted access; these  
# messages shouldn't go to terminals or publically-readable  
# files.

authpriv.\*;remoteauth.crit

/var/log/secure.log

lpr.info

/var/log/lpr.log

mail.\*

/var/log/mail.log

ftp.\*

/var/log/ftp.log

netinfo.err

/var/log/netinfo.log

# logrotate

---

- Utility per la compressione e la rotazione dei file di LOG
  - permette una gestione parzializzata
  - molto più snella la ricerca
  - prevede azioni post-log

# logrotate.conf

---

- Direttive generiche

- # rotate log files weekly  
weekly

- # keep 4 weeks worth of backlogs  
rotate 4

- # create new (empty) log files after rotating old ones  
create

# logrotate.conf (2)

- Direttive specifiche
  - /var/log/messages {  
rotate 5  
weekly  
postrotate  
    /sbin/killall -HUP syslogd  
endscript  
}

# Gestione temporizzata

*cron, at et altri*

# Eseguire compiti

---

- Nei sistemi server è spesso necessario:
  - eseguire compiti ripetitivi
    - *a scadenze ed orari non 'umani'*
    - *senza attesa attiva da parte di processi*
  - sono disponibili demoni di 'schedulazione'

# schedulazione

- crond
  - esegue job in modo schedulato con differenti *granularità* (s,m,h,d,w,m,y)
- atd
  - esegue jobs ad un determinato orario
- anacron
  - attiva i lavori non eseguiti da *cron*

# cron

- */var/spool/cron/crontabs*
  - le entry vengono create e distrutte con *crontab*
    - *crontab -l (lista)*
    - *crontab -e (edit)*
    - *crontab -r (remove)*

# crontab

---

- /etc/crontab
  - file in cui specifichiamo anche chi è l'utente che sta eseguendo un comando
  - m h dom m dow user command

# crontab -l | -e

---

- il formato di una singola linea è:
  - environment VAR
    - *nome = valore (PATH=/usr/bin)*
  - info sulla temporizzazione
    - *m h d-of-m m d-of-w comando*

# crontab

---

- Caratteri speciali
  - \* (ogni occorrenza)
  - /<n> (con ripetizione ogni <n>)

# crontab - esempio

```
# m h dom mon dow user  command
42 6 * * * root    run-parts --report /etc/cron.daily
*/1 * * * 7 root    run-parts --report /etc/cron.weekly
52 1-6/2 * * * root    run-parts --report /etc/cron.monthly
```

@reboot Run once, at startup.  
@yearly Run once a year, "0 0 1 1 \*".  
@annually (same as @yearly)  
@monthly Run once a month, "0 0 1 \* \*".  
@weekly Run once a week, "0 0 \* \* 0".  
@daily Run once a day, "0 0 \* \* \*".  
@midnight (same as @daily)  
@hourly Run once an hour, "0 \* \* \* \*".

# at

---

- at esegue un comando 1 sola volta
  - at 4pm + 3 days
  - at 10am Jul 31
  - at 1am tomorrow
- specifica completa
  - /usr/share/doc/at/timespec

# at - suite

---

- at
  - inserimento di un job
- atq
  - coda di job in attesa
- atrm
  - rimozione dalla coda dei job

# at - inserimento

---

- at TIME
  - giano:~# at 4pm +3 days  
warning: commands will be  
executed using /bin/sh  
at> ls  
at> <EOT>  
job 4 at 2003-08-02 16:00

# at - interrogazione

---

- atq

- 4      2003-08-02 16:00 a root

# at - cancellazione

---

- atrm 4
  - <nulla>

# anacron

---

- Controlla se i jobs di cron sono stati eseguiti
  - se non sono stati eseguiti (SRVdown)
    - *li esegue*
  - altrimenti
    - *si rimette in attesa*

# Filesystem

*montare, duplicare, swappare*

# Lo swap

- Area di memoria virtuale su dispositivo di massa
  - ci vanno a finire i blocchi di memoria di job
    - *in attesa di input*
    - *in attesa di dati da dispositivi di I/O*
    - *in stato Suspended (CTRL + z)*
    - *in stato di processo non in esecuzione*

# mount

---

- Comando che permette di associare
  - dispositivo fisico / logico
  - punto di montaggio nell'albero del FS
- `mount -t <tipo> </dev/dispositivo> <dir>`

# fstab

---

- /etc/fstab
  - contiene informazioni su
    - *punto di mount predefinito*
    - *check del dispositivo*
    - *tipologia del filesystem*
    - *opzioni di mounting (ro,rw)*

# fsck

- Utility per la verifica del FS
  - ripara i *blocchi* e gli *inode* danneggiati oppure li marca in */lost+found*
  - utilizzato se il FS non è correttamente smontato
  - `fsck.ext2 /dev/hda3 -y`
    - *risponde automaticamente 'y' a tutte le domande di riparazione*

# mkfs

---

- Crea un filesystem di un certo tipo
  - `mkfs.ext2 /dev/hda1`
  - `mkfs.vfat`
  - `mkfs.<tipo>`

# dd

- Utility per copiare file
  - `dd if=<input-file> of=<output-file>`
  - *opzioni*
    - *bs=BYTES (at time)*
    - *count=BLOCCHI*
    - *skip=BLOCCHI (da start of input)*
    - *seek=BLOCCHI (da start of output)*

# df

- Ci da informazioni sullo spazio libero nei dispositivi attualmente montati
  - -i : inode
  - senza opzioni blocchi liberi
  - -k : in kilobyte
  - -h : human readable

# Firewalling

*iptables e dintorni...*

# iptables

---

- Tool user-space
- Rimpiazza ipchains
- Kernel 2.4
- Si appoggia a NETFILTER

# iptables (2)

---

- Punti di forza:
  - Connection tracking
    - *stateful packet inspection*
      - *ICMP, UDP, TCP*
      - *Smurf* amplification attack, a *Tribe Flood Network* communication between master and daemon, or a *Loki 2* back-door

# iptables (3)

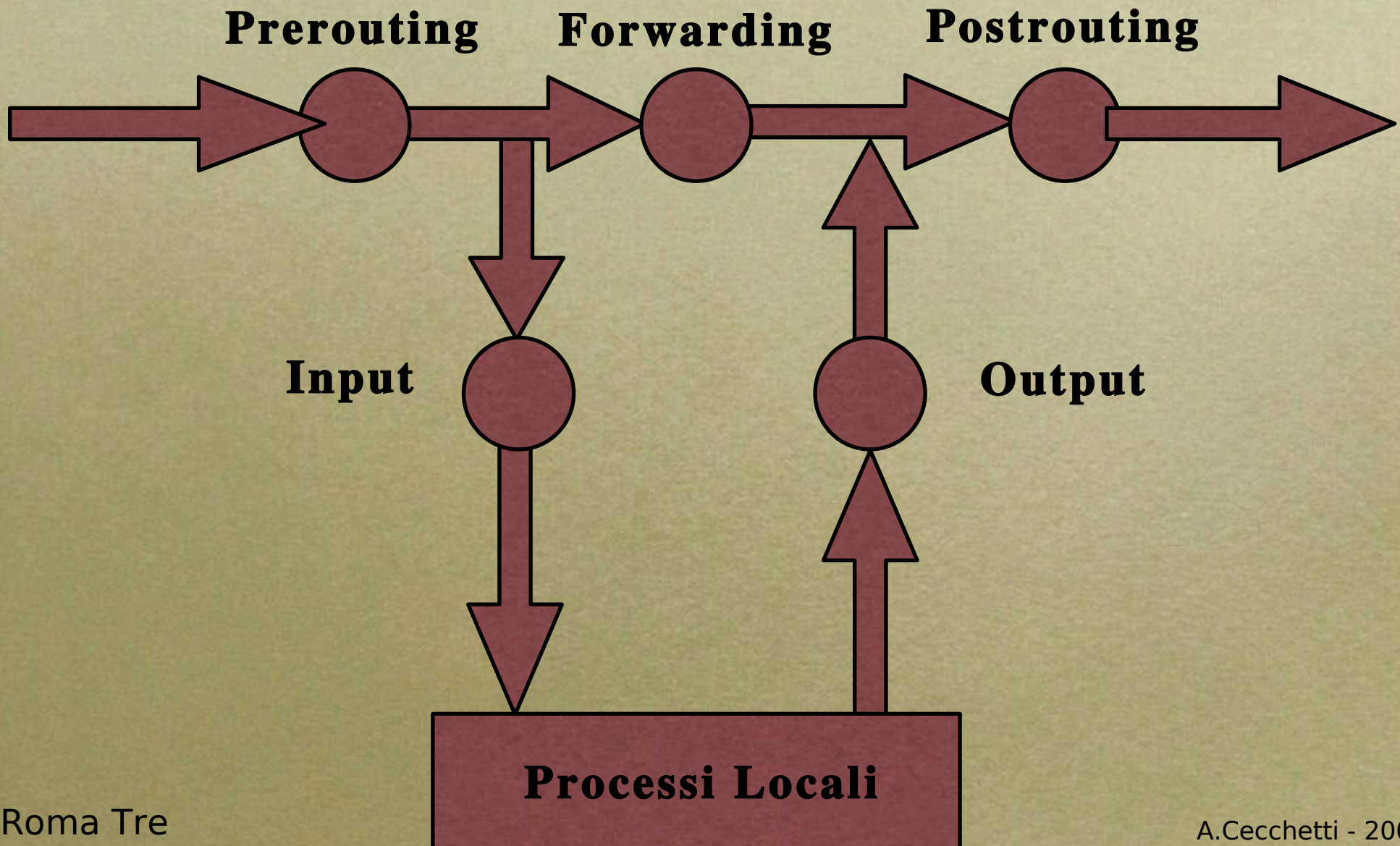
- Catene precostituite
  - INPUT, FORWARD, OUTPUT
    - *es. il routing fra interfacce di un host segue solo le regole della FORWARD*
- Separazione fra packet filtering e NAT
  - masquerading caso particolare di SNAT
  - redirection caso particolare di DNAT

# iptables (4)

---

- Limite di banda (Rate limit)
  - prevenzione di DDOS
- Capacità di Logging
  - prevenzione di DOS
- Filtering su opzioni e flag TCP
- Filtering rispetto al MAC address

# le catene (kernel space)



# IDS

---

- Tool che fanno un mappa del FS
  - hash dei file (MD5)
  - marcatura data di creazione e modifica
  - marcatura della testa/coda del file
- Tripwire
- slocate - checksecurity

# NIDS

---

- Tool che osservano il traffico di rete
  - utilizzano pattern di attacco predefiniti
  - utilizzano informazioni statistiche
  - sono dotati di reazioni di default

# Snort

---

- NIDS basato su pattern predefiniti
  - ha azioni predefinite di log
  - può essere utilizzato per comandare iptables

# Acid e Snort

---

- Acid è un tool web-based per
  - visualizzazione dei log di snort
  - caratterizzazione statistica attacchi