

Serveis en Xarxa

René Serral-Gracià Xavier Martorell-Bofill¹

¹Universitat Politècnica de Catalunya (UPC)

November 19, 2014

Temari

- 1 Introducció a l'Administració de Sistemes
- 2 Instal·lació del Sistema Operatiu
- 3 Gestió d'usuaris
- 4 Gestió d'aplicacions
- 5 Monitorització del sistema
- 6 Manteniment del sistema de fitxers
- 7 Serveis locals
- 8 **Serveis de xarxa**
- 9 Protecció i seguretat
- 10 Virtualització

Outline

- 1 Introducció
- 2 Servidors
- 3 Serveis
- 4 Sistemes de fitxers
- 5 Monitoratge
- 6 Exercici

Outline

- 1 Introducció
 - Objectius
 - Consideracions prèvies
 - Network Address Translation
 - Firewalls

2 Servidores

3 Serveis

4 Sistemes de fitxers

5 Monitoratge

6 Exercici

Objectius

Coneixements

- Principals serveis i protocols de xarxa
 - Superservidor, portmapper, DNS, FTP, WWW, e-mail

Habilitats

- Dimensionat dels servidors
- Ubicació dels serveis de xarxa
- Localització de Firewalls

- Relaciona els serveis amb el corresponent número de port
 - ho consulten diversos programes (`netstat`, ...)

nomservei	port/protocol	llista alias
-----------	---------------	--------------

```

echo          7/tcp
echo          7/udp
systat        11/tcp          users
systat        11/udp          users
ftp-data      20/tcp
ftp-data      20/udp
# 21 is registered to ftp, but also used by fsp
ftp           21/tcp
ftp           21/udp          fsp fspd
ssh           22/tcp
ssh           22/udp
telnet        23/tcp
telnet        23/udp
# 24 - private mail system
smtp          25/tcp          mail
smtp          25/udp          mail
domain        53/tcp
domain        53/udp
http          80/tcp          www www-http
http          80/udp          www www-http

```


Network Address Translation – NAT

- El router tradueix adreces internes per una de pròpia
 - Permet usar una IP reservada i mantenir la connectivitat amb l'exterior
- El router recorda les connexions de sortida per reconèixer les connexions de tornada
 - Connexió de sortida:
 - 192.168.1.25 (port 1085) → 212.106.192.142 (11086)
 - Connexió de tornada:
 - 212.106.192.142 (11086) → 192.168.1.25 (1085)

Eines: `iptables` (SNAT), `dnsmasq`

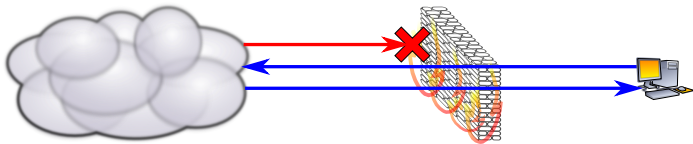
Efectes colaterals del NAT

- Les adreces internes no són visibles des de l'exterior
 - Només el router pot ser víctima d'atacs – excepte en connexions funcionant
- La seguretat de la xarxa depèn de la seguretat del router
- Les màquines internes no poden oferir serveis a l'exterior
 - Excepte si usem Port Address Translation (PAT)
- Impacte important sobre el rendiment de la xarxa
 - Totes les connexions exteriors passen per un sol router
 - Cada paquet requereix un cert càlcul de CPU
- Alguns serveis no es poden usar amb NAT
 - Aquells que fan connexions cap a dins
 - FTP, IRC, Netmeeting, ...

Firewalls

Servidor que determina quines comunicacions poden ser establertes entre dues xarxes

- Treballa típicament a nivell de xarxa i de transport
 - En general no coneix detalls de l'aplicació
- Pot mantenir estat (Connection Tracking)
 - Permetre connexions relacionades: “de tornada”



Firewall == Seguretat?

- Un firewall és un suplement a la seguretat del sistema
- El seu ús pot oferir una falsa idea de seguretat
- No es poden relaxar altres aspectes de la seguretat
 - Configuració correcta de les aplicacions
 - Actualitzar el software que té forats de seguretat
 - Limitar l'accès concurrent
- Altres eines de seguretat a la xarxa interna i als servidors continuen sent necessàries

Outline

- 1 Introducció
- 2 Servidors
 - Tipus de serveis
 - Tipus de servidors
- 3 Serveis
- 4 Sistemes de fitxers
- 5 Monitoratge
- 6 Exercici

Tipus de serveis

- Orientats a connexió
 - El servidor manté l'estat de la sessió
 - Incrementa el rendiment
 - Redueix la tolerància a fallades
- No orientats a connexió
 - No es guarda cap estat sobre els clients
 - No hi ha sessions
 - Les peticions han de ser autocontingudes
 - La petició del client ha de contenir tota la informació
 - Incrementa la tolerància a fallades

Tipus de servidors – Segons Autoritat

● Primaris

- Mantenen la còpia principal de la informació
- En cas de divergència es confia en el servidor primari
- N'hi ha un per servei

● Secundaris

- Mantenen còpies de la informació
- Actualitzacions periòdiques des del servidor primari
- Pot haver-n'hi més d'un per servei
- Balanceig de la càrrega
- Actuen com a backup si cau el servidor principal

● Cache (i/o proxies)

- Mantenen còpies –parcials– de la informació més usada
- Pot haver-n'hi més d'un per servei
 - Augment del rendiment
- S'hi poden afegir funcions de seguretat, filtratge, log, ...

Outline

1 Introducció

2 Servidors

3 Serveis

- Superservidor
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Simple Mail Transfer Protocol (SMTP)
- Recepció de correu electrònic
- Secure Shell (SSH)
- Virtual Private Networks (VPN)

Superservidor

- Un servei consumeix recursos encara que no es faci servir
 - Molts serveis es demanen de forma esporàdica: `telnet`, `ftp`, `ssh`, ...
- El superservidor escolta tots els ports i activa el servei només quan és necessari
 - Detecta la petició
 - Inicia el servidor
 - Passa el missatge
- Limitacions
 - No es pot guardar a memòria informació entre connexions
 - Overhead de creació de processos

Implementacions: `inetd`, `xinetd`

/etc/xinetd.conf, /etc/xinetd.d

Especifica els serveis atesos pel superservidor

Servei, Protocol,Usuari/grup, Servidor, Arguments

```
$ cat /etc/xined.conf
includedir /etc/xinetd.d
```

```
$ cat /etc/xined.d/ftp
service ftp
{
    socket_type          = stream
    wait                 = no
    user                  = root
    server                = /usr/sbin/vsftpd
    log_on_success        += HOST DURATION
    log_on_failure        += HOST
    disable               = no
}
```

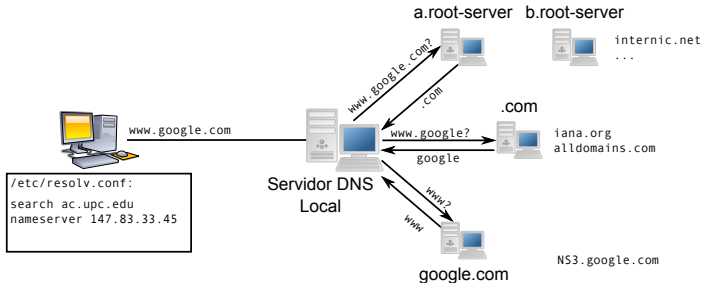
Domain Name System (DNS)

- Servei de traducció de noms
 - Hostname → adreça IP
 - Adreça IP → hostname
- Dificultats
 - Gran quantitat de màquines
 - Gran número de canvis
- Solució
 - Distribució jeràrquica de la informació (dominis)
 - Delegació de l'autoritat

Funcionament del DNS

Delegació de l'autoritat

- Cada domini administra el seu propi servidor
- Tothom coneix els servidors principals (root)
- Tothom coneix al servidor del seu domini
- Resolució de noms iterativa



Eficiència del servei

És convenient l'ús de "caches"

- Alta localitat temporal
 - Evitar repetir la mateixa cerca
- Alta localitat espacial
 - Evitar visitar continuament el servidor arrel
 - Evitar passos d'una cerca iterativa

DNS es pot usar per fer balanceig de càrrega

- Afegir varies adreces IP per un mateix nom
 - Cada resposta ofereix una IP diferent: Round Robin o bé Criteris "geogràfics"

```
$ nslookup www.google.com
Name:    www.google.com
Address: 212.106.221.23
Name:    www.google.com
Address: 212.106.221.27
Name:    www.google.com
Address: 212.106.221.25
...
```

Configuració del client de DNS

- `/etc/host.conf`
 - On es busca un nom i l'ordre de cerca
- `/etc/hosts`
 - Màquines traduïdes localment
- `/etc/resolv.conf`
 - Dominis on buscar automàticament
 - Adreces IP dels servidors de noms

Configuració del servidor de DNS

- `/etc/bind/named.conf`
 - Què administrem?
 - Dominis de DNS
 - Rangs d'adreces IP
 - Indica si som primari, secundari o de cache
- Fitxers de traducció directa
 - Nom.domini → adreça IP
 - 1 fitxer per cada domini que administrem
- Fitxers de traducció inversa
 - Adreça IP → nom.domini
 - 1 fitxer per rang d'adreces que administrem

Tipus de registres DNS

- SOA (Start of Authority)
 - Nombre de sèrie
 - Temps de refresc i retry
 - Temps d'expiració
 - TTL mínim
- A - traducció directa
 - Nom → adreça IP

```
romeu IN A 147.83.32.4
```

- CNAME - sinònims
 - Nom → nom

```
romeu IN CNAME lp_romeu
```

Tipus de registres DNS

- PTR - traducció inversa
 - Adreça IP → nom DNS

```
4 IN PTR romeu.ac.upc.edu.
```

- NS - delegació de dominis
 - Domini DNS → servidor

```
ac IN NS 147.83.32.3
```

- MX - mail exchanger
 - Domini DNS → servidor

```
ac IN MX 147.83.33.10
```

- I altres...
 - HINFO, WKS, ...

Exemple de configuració de DNS

Zona "cluster.craax.upc.edu", com a primari.

```
$ cat /etc/bind/named.conf
options {
    directory "/var/cache/bind";
    forwarders {
        147.83.159.217;
    };
    auth-nxdomain no;      # conform to RFC1035
    listen-on-v6 { any; };
};
zone "cluster.craax.upc.edu" {
    type master;
    file "/etc/bind/cluster.zone";
};
zone "1.1.10.in-addr.arpa" {
    type master;
    file "/etc/bind/cluster.rev";
};
```

Exemple de configuració de DNS

```
$ cat /etc/bind/cluster.zone
$TTL      604800
@          IN      SOA      cluster. cluster.craax.upc.edu. (
                        20101220      ; Serial
                        604800      ; Refresh
                        86400      ; Retry
                        2419200      ; Expire
                        604800 )      ; Negative Cache TTL
;
@          IN      NS       gandalf
$ORIGIN    cluster.craax.upc.edu.
gandalf    IN      A        10.1.1.1
boromir-1  IN      A        10.1.1.2
```

```
$ cat /etc/bind/cluster.rev
$TTL      604800
@          IN      SOA      cluster. cluster.craax.upc.edu. (
                        20101220      ; Serial
                        604800      ; Refresh
                        86400      ; Retry
                        2419200      ; Expire
                        604800 )      ; Negative Cache TTL
;
@          IN      NS       gandalf
$ORIGIN    cluster.craax.upc.edu.
1          IN      PTR      gandalf.cluster.craax.upc.edu.
2          IN      PTR      boromir-1.cluster.craax.upc.edu.
```

Activitat

- Tenim 3 servidors (server1, server2 i server3) amb aquests registres

```
server1 IN A 123.123.123.1  
server2 IN A 123.123.123.2  
server3 IN A 123.123.123.3
```

- Volem afegir resolució de noms per als serveis
 - **www** a server1
 - **ftp** a server1 i server2
 - **correu entrant/sortint** a server3

Quins registres afegireu?

Eines relacionades amb el DNS

- `whois domini`
 - Proporciona informació de contacte per un domini
- `dig [@server] petició`
 - Fa una petició de DNS
 - Possibilitat de controlar diversos paràmetres
 - Servidor, tipus de registre, resolució iterativa/recursiva, ...
 - Retorna els registres associats a la nostra petició
 - Se li pot demanar debugging

Dynamic Host Configuration Protocol (DHCP)

- Proporciona de forma automàtica la configuració de la xarxa a un equip
 - Assignació d'IP, Gateway i DNS
- La màquina no té perquè ser coneguda!
 - Per defecte assumeix que si algú es pot connectar és un usuari legítim
 - Possibilitat de proporcionar control d'accés a nivell MAC
- Les adreces IP s'obtenen de conjunts definits per l'administrador

Dynamic Host Configuration Protocol (DHCP)

Suport de boot remot mitjançant BOOTP i PXE

- Preboot Execution Environment (PXE)
- La targeta de xarxa obté informació de la xarxa directament per la BIOS
- Permet indicar una imatge del kernel
 - Descarregada per TFTP
 - Amb possibilitat de muntar un directori arrel remot

Dynamic Host Configuration Protocol (DHCP)

Per /etc/resolv.conf

Per PXE

Per ifconfig

Per route

```
ddns-update-style none;
option domain-name-servers 192.168.1.1;

allow booting;
allow bootp;
default-lease-time 600;
max-lease-time 7200;
authoritative;

subnet 192.168.1.0 netmask 255.255.255.0 {
    range dynamic-bootp 192.168.1.172 192.168.1.254;
    range 192.168.1.2 192.168.1.171;
    filename "pxelinux.0";

    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.1.255;
    option routers 192.168.1.1;
}
```

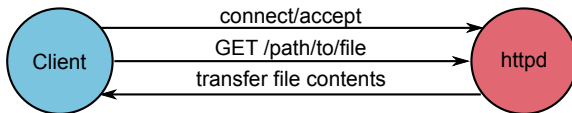
Activitat

Discutir en grup

- Quin problema pot haver-hi si es cau el servidor de DHCP?
- Com es podria implementar per evitar-lo?

Hypertext Transfer Protocol (HTTP)

- Servei de transferència de dades
- No orientat a connexió
 - No es recorda l'estat d'un client
 - Cada petició és autocontinguda
- No obstant això, usa TCP!



Apache Web Server

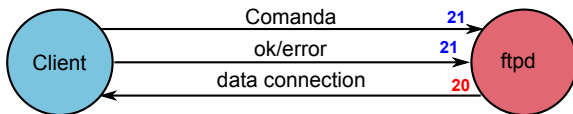
- Implementa suport per HTTP
- `/etc/apache/httpd.conf`

Principals funcionalitats

- Execució com a usuari no privilegiat
- Atenció de peticions per processos/fluxos independents
 - Model de compartició de memòria configurable
 - Número màxim de processos configurable
- Opcions de configuració per cada directori
- Configuració per dominis virtuals
 - Separació per adreça IP
 - Separació per nom del DNS

File Transfer Protocol (FTP)

- Servei de transferència de dades
- Orientat a connexió
- Connexió de control
 - Manté estat d'una petició a l'altra: `cwd`
- Connexió de dades
 - activa: no suporta NAT
 - passiva: suport per NAT
 - Nova connexió de dades per cada transferència



Configuració del FTP

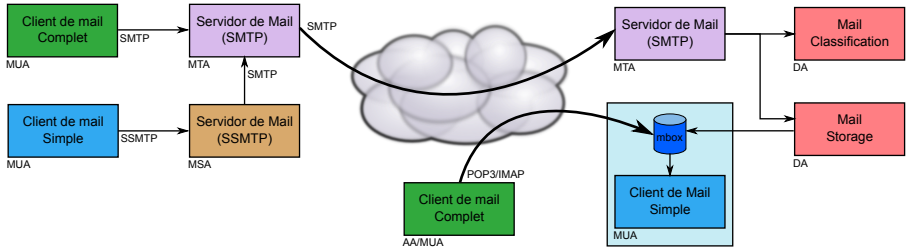
- Hi ha molts servidors
 - `wu-ftp`, `proftpd`, `vsftpd`, ...
- Control d'accés a nivell d'usuari: `/etc/ftpusers`
 - Llistat d'usuaris que **NO** poden accedir per FTP
- Utilitzar `chroot` per seguretat amb FTP anònim
 - Canvia l'arrel del sistema
 - Requereix configuració extra
 - Instal·lar comandes bàsiques i fitxers de configuració
 - `/etc/passwd`, `/etc/shadow`
 - `/bin/ls`, `/lib/libc.so`, ...
 - Inclús per usuaris regulars

Simple Mail Transfer Protocol (SMTP)

Elements que componen el sistema de correu

- MUA - Mail User Agent
 - Aplicació d'usuari per llegir i escriure correu - mail
- MSA - Mail Submission Agent
 - Aplicació que transmet el correu del client a l'MTA
 - Fa totes les comprovacions d'error prèvies
- MTA - Mail Transport Agent
 - Aplicació que dirigeix el correu entre màquines
- Delivery Agent
 - Aplicació que guarda el correu al mailbox de l'usuari
 - De vegades una base de dades en lloc d'un fitxer
- Access Agent
 - Aplicació que permet a l'usuari accedir al seu mailbox - mail

Components del sistema de correu



Anatomia d'un correu electrònic

- Sobre (envelope)
 - Destinatari del missatge
 - Origen
 - Invisible per als usuaris – visible per als servidors
- Capçaleres
 - Conjunt de propietats del missatge
 - Data d'enviament
 - Remitent i destinatari (mostrat pels clients de mail)
 - Llista d'equips pels que ha passat el missatge
- Cos del missatge
 - Amb format ASCII de 7 bits
 - Fitxers adjunts amb Base-64

Configuració del client de correu

Recepció de correu

- Accés a Mailbox local
 - Interpret del format mailbox/maildir
- Accés a un Mailbox remot
 - POP3
 - IMAP

Enviament de correu

- A través del servidor SMTP

Consideracions de seguretat

Autenticació d'usuaris

- Per defecte el servidor de correu no demana credencials
 - Es pot afegir SASL
- Es pot falsificar el sobre de correu — SPAM ...
- Relay de correu electrònic
 - El servidor sempre intenta entregar el correu al destinatari
 - Fins i tot si el sobre no té res a veure amb ell (Open Relays)

Consideracions de seguretat

Privacitat del correu

- El correu s'envia sense encriptar
 - Us de TLS (SSL) només entre MUA i MTA
- PGP - Pretty Good Privacy
 - Encriptació i signatura de missatges
 - Basat en clau pública
- S/MIME

Instal·lació de Filtres

- Anti-spam
 - Spamassassin, gray lists, black lists, ...
- Anti-virus
 - Clam AV, Amavis, f-prot,...

Recepció de correu electrònic

Post Office Protocol (POP)

- Permet els usuaris accedir al seu mailbox
- Porta els missatges cap a la màquina local
- Autenticació d'usuari sense encriptació
 - `pop3s` funciona sobre SSL

Internet Message Access (IMAP)

- Permet els usuaris manipular al seu mailbox
- Realitza les manipulacions remotament
- Autenticació d'usuari
 - Permet encriptació
- `imaps` treballa sobre SSL

Activitat – En grup

Hem posat un filtre per detectar el spam

- Quan es detecta un correu d'aquestes característiques, quina acció programaríeu?
- I si el filtre és d'anti-virus?

Secure Shell

- Substitueix els serveis de rsh/rlogin i telnet
- Afegeix seguretat
 - Realitza autenticació basada en RSA, DSA, ECDSA
 - El client signa l'identificador de sessió amb la clau privada
 - El servidor usa la clau pública (`.ssh/authorized_keys`) per comprovar si la signatura és correcta
 - Tams bé es pot usar autenticació basada en password
 - Encripta la informació que s'envia per la connexió
 - Confidencialitat: 3DES, Blowfish, ...
 - Integritat: `hmac-md5`, ...
- El servidor executa la comanda donada o l'interpret de comandes de l'usuari
- Sessió transparent
 - Quan no es demana usar un pseudo-terminal
 - Es pot fer servir per transferir dades en format binari
- Sessió de login
 - També pot fer forwarding de TCP i X11

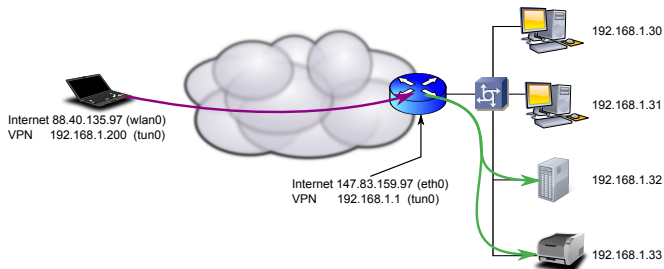
Activitat – En grup

Accions amb Secure Shell

- Com implementaríeu secure copy i secure file transfer sobre `ssh`?

Virtual Private Networks (VPN)

- Servidor i client negocien una connexió segura
- Es disposa d'una @IP interna
 - És té accés a tots els serveis de la Intranet

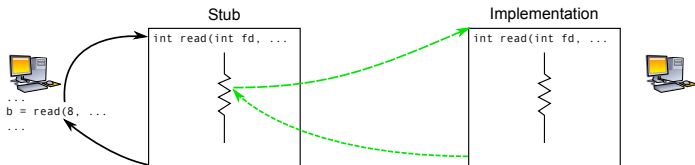


Outline

- 1 Introducció
- 2 Servidors
- 3 Serveis
- 4 Sistemes de fitxers**
 - Remote Procedure Calls (RPC)
 - Network File System (NFS)
 - Samba (SMB)
- 5 Monitoratge
- 6 Exercici

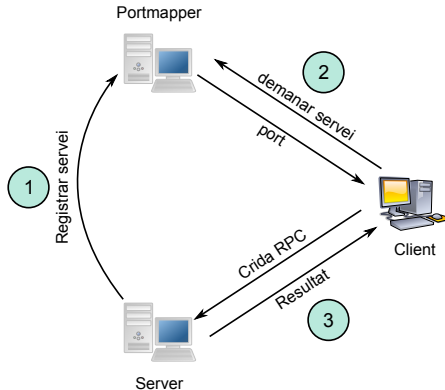
Remote Procedure Calls (RPC)

- Execució remota de subrutines
 - Identificades amb un número de servei
- Servidors de RPC
 - Implementen un conjunt de subrutines remotes
 - Escolten en un port no fixat
- Portmapper
- Registra els servidors d'RPC
 - Associa el port amb les subrutines
- Necessari per altres serveis
 - NFS, ...



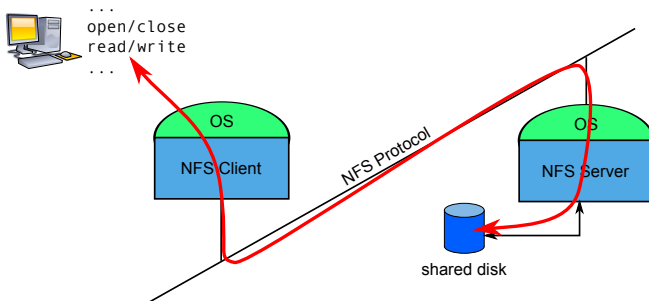
Portmapper

- Tot l'estat es guarda en memòria
 - Si falla el procés, no n'hi ha prou amb reiniciar-lo
 - S'han de reiniciar tots els servidors d'RPC
- Cal enregistrar tots els servidors al inici del portmapper



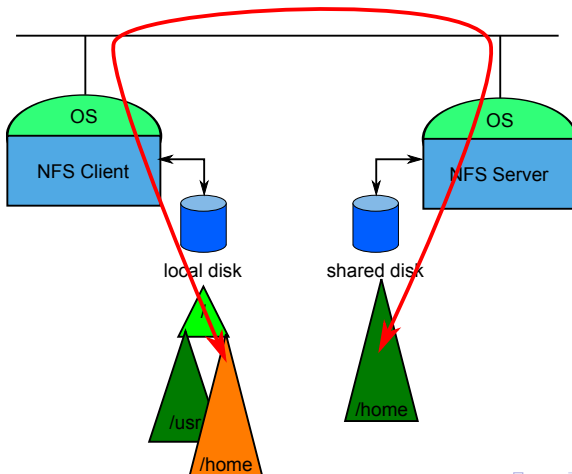
Network File System (NFS)

- Accés a fitxers guardats en un disc remot
 - Mantenint la semàntica del sistema de fitxers local
- Actua de forma transparent a l'usuari
 - Implementat usant RPC's



Mount Remot per NFS

El directori muntat es veu com si fos local



Permisos d'accés

- Els UIDs a la màquina remota i a la màquina local han de ser els mateixos
 - El sistema de fitxers guarda UIDs, no usernames
 - Possibilitat de mapejar usuaris amb `idmapd`
- Traducció automàtica de UID's (`idmapd`)
 - `root`, `nobody`
- Opcions
 - `no_root_squash`, `root` pot fer su a qualsevol usuari!
 - `all_squash`, es pot fer que tots els usuaris siguin `nobody`
 - Es pot definir qui serà `nobody`

```
anonuid=UID,anongid=GID
```

Configuració d'NFS

- Determinar quins recursos s'exporten
- Màquines a qui exportar-los
- Flags de configuració

/etc/exports

```
/          master(rw) trusty(rw,no_root_squash)
/projects  proj*.local.domain(rw)
/usr       *.local.domain(ro) @trustedgroup(rw)
/home/joe  pc001(rw,all_squash,anonuid=150,anongid=100)
/pub       (ro,insecure,all_squash)
```


SMB — Samba

- Permet exportar fitxers i impressores
- Control d'accés a nivell d'usuari
 - Autenticació amb usuari i password
 - Basat en username, no en UID
 - Transmissió de passwords de forma encriptada o no
 - Restricció d'accés també a nivell de màquina
 - No permet distingir flags segons la màquina que estigui accedint
 - Usar noms de recurs diferents

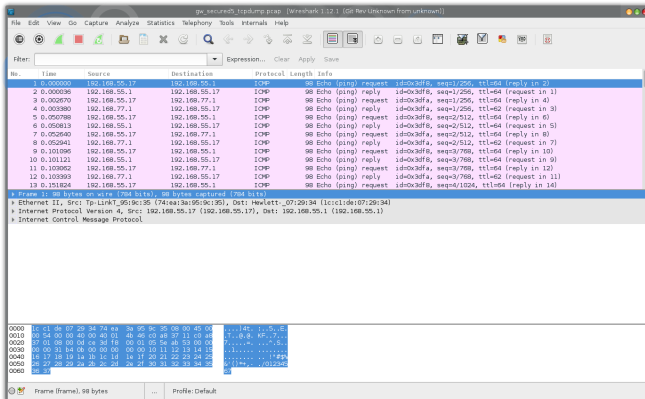
Outline

- 1 Introducció
- 2 Servidors
- 3 Serveis
- 4 Sistemes de fitxers
- 5 Monitoratge**
- 6 Exercici

Packet Sniffing — tcpdump

```
00:40:53.818471 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto ICMP (1), length 84)
 192.168.55.17 > 192.168.55.1: ICMP echo request, id 15864, seq 1, length 64
    0x0000: 4500 0054 0000 4000 4001 4b46 c0a8 3711
    0x0010: c0a8 3701 0000 0dce 3df8 0001 055e ab53
    0x0020: 0000 0000 31b4 0b00 0000 0000 1011 1213
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
    0x0050: 3435 3637
00:40:53.818507 IP (tos 0x0, ttl 64, id 3655, offset 0, flags [none], proto ICMP (1), length 84)
 192.168.55.1 > 192.168.55.17: ICMP echo reply, id 15864, seq 1, length 64
    0x0000: 4500 0054 0e47 0000 4001 7cff c0a8 3701
    0x0010: c0a8 3711 0000 15ce 3df8 0001 055e ab53
    0x0020: 0000 0000 31b4 0b00 0000 0000 1011 1213
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
    0x0050: 3435 3637
00:40:53.821141 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto ICMP (1), length 84)
 192.168.55.17 > 192.168.77.1: ICMP echo request, id 15866, seq 1, length 64
    0x0000: 4500 0054 0000 4000 4001 3546 c0a8 3711
    0x0010: c0a8 4d01 0000 b0c1 3dfa 0001 055e ab53
    0x0020: 0000 0000 80be 0b00 0000 0000 1011 1213
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
    0x0050: 3435 3637
00:40:53.821851 IP (tos 0x0, ttl 62, id 4565, offset 0, flags [none], proto ICMP (1), length 84)
:
```

Packet Sniffing — wireshark



Detecció de serveis—netstat

Syntax

- `netstat [options]`
- `-a` - Show all socket
- `-p` - Show program using the socket

```
aso@localhost:~$ netstat -anp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:17500	0.0.0.0:*	LISTEN	22643/dropbox
tcp	0	0	0.0.0.0:9020	0.0.0.0:*	LISTEN	22096/skype
tcp	0	0	192.168.1.7:55741	192.168.78.189:443	ESTABLISHED	22122/iceweasel

```

Active UNIX domain sockets (servers and established)

```

Proto	RefCnt	Flags	Type	State	I-Node	PID/Program name	Path
unix	2	[ACC]	STREAM	LISTENING	2586	-	/tmp/.font-unix/fs7101
unix	2	[ACC]	STREAM	LISTENING	12043594	22643/dropbox	/home/rserral/.dropbox/command_socket
unix	2	[ACC]	STREAM	LISTENING	12043596	22643/dropbox	/home/rserral/.dropbox/iface_socket
unix	2	[ACC]	STREAM	LISTENING	12038213	-	/tmp/.X11-unix/X0

Detecció de serveis—nmap

Syntax

- `nmap [options] IP_list`

```
aso@localhost:~$ nmap 192.168.1.2
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2014-11-19 00:18 CET
```

```
Nmap scan report for 192.168.1.2
```

```
Host is up (0.057s latency).
```

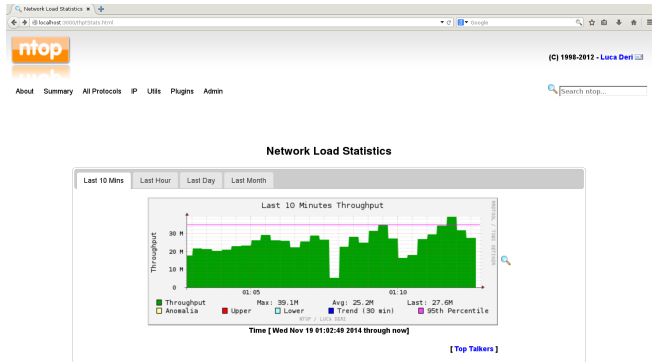
```
Not shown: 988 closed ports
```

PORT	STATE	SERVICE
22/tcp	open	ssh
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
143/tcp	open	imap
443/tcp	open	https
514/tcp	open	shell
993/tcp	open	imaps
2049/tcp	open	nfs
6566/tcp	open	sane-port
9101/tcp	open	jetdirect
9103/tcp	open	jetdirect

```
Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds
```

Altres aplicacions

- snort - Intrusion detection system
- logwatch - Log Watcher
- ntop - Network Top



Outline

- 1 Introducció
- 2 Servidors
- 3 Serveis
- 4 Sistemes de fitxers
- 5 Monitoratge
- 6 Exercici**

Activitat

Una empresa de màrketng ha muntat una xarxa amb les següents característiques:

- El departament de direcció consta de 15 PC.
- El departament d'administració té 10 PC.
- Sabem que disposem del rang d'adreces IP 180.45.23.0/28.
- Cada departament té els seus propis servidors
- La empresa requereix els següents serveis:
 - Web
 - Correu Electrònic
 - File Sharing (NFS)
 - VPN
 - SSH
 - FTP
 - DNS
 - Impressió
 - Intranet

Activitat

- Càrrega dels serveis

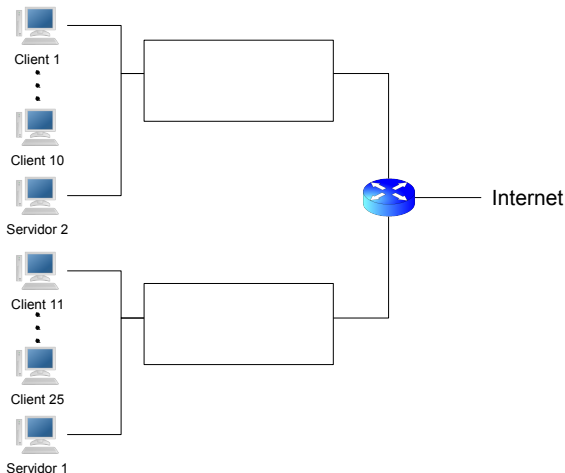
- Web **Molt alta**
- Correu Electrònic **Alta**
- File Sharing (NFS) **Molt alta**
- VPN **Molt baixa**
- SSH **Molt baixa**
- FTP **Baixa**
- DNS **Normal**
- Impressió **Molt Baixa**
- Intranet **Normal**

- De tots aquests serveis:

- El web està desdoblant amb tres parts una per cada departament
- La compartició de fitxers, la intranet, i la impressió són específiques a cada departament
- L'FTP, el Correu, l'SSH i el DNS són compartits a nivell de l'empresa

Activitat

Afegeix el hardware que consideris oportú i assigna adreces IP



Activitat

Preguntes

- Indica si compraries algun equip més a part dels equips de xarxa anteriors
- Distribueix els serveis entre tots els servidors
- Indica on instal·laries el (o els) firewall i quins criteris seguiries per configurar-los