COMANDOS UNIX

- ps : muestra los procesos activos
- cat *file* : muestra por pantalla el fichero *file*
- cp src_file (-r) dst_file : copia archivo / dir (-r) contenido dir
- mv " " : mueve archivo / dir " "
- rm (-r) file : borra archivo / dir " "
- ls -la : lista el directorio actual
- chmod nnn file : cambia permisos

user	group	world
rwx	rwx	rwx
4 2 1	4 2 1	4 2 1

- cd path : cambia el dir actual
- mkdir directory : crea dir
- rm dir directory : borra dir
- man comando : da ayuda del comando.
- echo string : muestra string por pantalla
- programa > fichero_salida : redirecciona la salida del prog al fichero
- " >> " : IDEM pero lo añade al fichero.

FICHEROS IMPORTANTES (COMUNICACIONES)

/etc/hosts ⇒ Resolución de nombres (DNS)
/etc/protocols ⇒ Lista el número asociado a cada protocolo (IP, TCP, ...)
/etc/services ⇒ Relaciona cada servicio de red con el puesto y protocolo que utiliza (ftp, telnet, ...)
/etc/inetd.conf ⇒ Especifica los servicios de red que se ejecutaran al arrancar.
/etc/resolv.conf ⇒ DNS que se consultan para resolver direcciones.
/proc/sys/net/ipv4/ip_forward ⇒ Si contiene un "1" podemos hacer de router.

COMANDOS USUALES

= Consultas DNS

host [nombe | dir_IP] : Resuelve nombre a IP y viceversa.
nslookup [nombre | IP] : IDEM indicando el serv. DNS usado.
whois IP : Da info sobre la org propietaria de la dir IP.

- Gestión de las comunicaciones

netstat : Info sobre estado de las com. en el host local
(conexiones, servicios activos, dispositivos, tablas enrutamiento)

ifconfig : configura interfaces de red.
ifconfig eth0 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255

ping : envia una petición de ping
ping -c 15 192.168.0.2

route : Administra la tabla de rutas
route -n : muestra la tabla de rutas.
route del '' -net 192.168.0.0 netmask 255.255.255.0
route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.0.1 dev eth0

ethereal : sniffer de red
Config ⇒ Filter : host 192.168.0.1 solo lista datagramas de o hacia IP
'Habilitar : Cap. Pack in promisc. mode ; Updt list real time ; Autom. scrolling
Deshabilitar : Enable MAC name res ; Enable network ... ; Enable transport ...
Filtrar un protocolo Filter : ip proto #num_proto

source routing

ping -S <src_ip> < router 1>... < router n> < dst_ip >

JOSE Mª HERRERO C.

LA HERRAMIENTA IPTABLES

Operaciones más comunes sobre las reglas:

- A : Añade una nueva regla
- D : Borra una regla. Deben usarse las mismas opciones que se usaron para añadirla.

* Uso de iptables para filtrado de paquetes.

Las reglas de filtrado se introducen en tres cadenas:

INPUT : para los paquetes destinados a la máquina.
OUTPUT : " que salen por un interfaz.
FORWARD : " que entran por un interfaz y salen por otro (o por el mismo)

Sintaxis:

```
iptables -A INPUT [-f] -s <dir> -p <proto> -j <acción> -i <interfaz>
iptables -A OUTPUT [-f] -d <dir> -p <proto> -j <acción> -o <interfaz>
```

- -f : procesar fragmentos
- -s <dir>, -d <dir> : dirección origen o destino, puede ser el nombre de un host o estar expresado en notación decimal con puntos o como IP/bits red o IP/mascara de red.
- -p <proto> : protocolos a procesar ICMP, UDP o TCP.
- -j <acción> : puede ser DROP (tirar) o ACCEPT.

Mediante "!" se puede invertir el argumento de una opción

Condiciones de filtrado específicas para TCP

```
--source-port <puerto>          } también para UPP
--destination-port <puerto>     }
--tcp-option <option>
--tcp-flags <flags>             ALL, SYN, ACK, FIN, RST, URG, PSH
```

Condiciones de filtrado específicas para ICMP

```
--icmp-type <código ICMP>
            echo-request , echo-reply
```

* Uso de iptables para traducción de direcciones

Para especificar las reglas NAT se utiliza la opción "-t nat"
Las reglas de NAT se introducen en tres cadenas:

DNAT
- PREROUTING: Cambio de destino de los paquetes que llegan por los diferentes interfaces del router.
- OUTPUT: Cambio de destino de los paquetes generados en la propia máquina.

SNAT
- POSTROUTING: Cambio de origen.

- Cambio de origen (SNAT)

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to <IP:port>
```

- Cambio de destino (DNAT)

```
iptables -t nat -A PREROUTING -i eth1 -j DNAT -s <dir> --to <IP:port>
iptables -t nat -A OUTPUT -d <dir> -j DNAT --to <dir>
```

<IP:port> puede ser una sola IP, un rango 1.2.3.4-1.2.3.6 o si se ha usado la opción "-p TCP" un puerto o rango de puertos.

Cmd útiles

```
iptables -t nat -L
```

Ejemplos

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 -jDNAT --to IP:port
iptables -A FORWARD -d 192.168.2.0/24 -p tcp -j DROP
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth0 -j SNAT --to IP
```