

## Tema 8 - Exercicis

(Recordeu fer servir captures de pantalla a les respostes per demostrar el funcionament dels script/comandes que feu servir i donar suport a les vostres afirmacions. Feu servir referències també quan calgui.)

1. Quines són les diferències entre inetd i xinetd? Explica també els seus fitxers de configuració, incloent-hi els camps que tenen.

Per una banda, ens trobem amb el Inetd (Internet Daemon), és un dimoni conegut també com a Súper Servidord'Internet, ja que s'encarrega de controlar i gestiona la connexió de molts dimonis (controla dimonis com **Daemon comsat**,**Daemon ftpd**,**Daemon fingerd** ...), concretament controla els ports de xarxa, perquè aquest el que fa és en segon pla va escoltant tots els ports de xarxa que n'hi ha al SO i quan detecta que a un d'aquells ports li ha arribat una petició d'internet, crida el dimoni corresponent perquè s'encarregui d'aquella petició i després tornar al procés de continuar escoltant. Aquest dimoni és molt útil, ja que redueix la càrrega de treball del sistema operatiu cridant als dimonis corresponent únicament quan és necessari.

Aquest dimoni llegeix tota la seva informació de configuració de l'arxiu **/etc/inetd.conf** i les entrades de l'arxiu **/etc/inetd.conf** té la següent informació

**Nom del servei:** Especifica el nom del servei d'Internet

**Tipus de socket :** Especifica i marca el tipus de socket d'Internet utilitzar per al servei d'Internet prèviament especificat

**Protocol:** Especifica el Protocol fet servir pel servei d'Internet, pot ser protocol com TCP,TCP6,UDP,UDP6

**Espera o Ara (Wait/NoWait) :** Per una banda, està el mode wait, un mode que es fa servir per serveis d'un únic fil (single-threaded), on el dimoni encarregat d'aquell servei no deixa d'escoltar el port fins que el servei terminal. En canvi, no wait és per serveis multi-thread, permetent múltiples connexions simultànies

**Usuari:** Especifica el nom de l'usuari que inetd ha de fer servir per iniciar el subservidor

**Via:** Específica per on ha d'accendir el dimoni inetd per proporcionar i efectuar el servei, és per dir-ho així el Path per on ha de passar.

**Mandat:** Especifica el nom del servei que començarà i els paràmetres que ha de tenir.

```
GNU nano 6.2                                /etc/inetd.conf *
2025 stream tcp nowait root /bin/date date
```

### **Fotografia 1: Exemple fet per mi de la configuració de inetd**

Per una altra banda, comptem amb el Xinetd (Extended Internet Daemon), que igual que el Inetd, és un dimoni que s'encarrega d'escoltar els ports i cridar als corresponents dimonis, per complir la petició corresponent, però millora en molts aspectes a l'anterior dimoni, sobretot en l'aspecte de seguretat, ja que proporciona més control i flexibilitat sobre diversos paràmetres entre les principals diferències destacaríem que

- Ofereix protecció contra atacs Dos(Denial of Service)
- Pots fer controls basats en intervals de temps
- Pots fer controls per serveis TCP,UDP i RCP
- Pot treballar com un proxy manejant connexions cap certes xarxes
- Ja no té únicament un fitxer de configuració sinó que ara té un fitxer global a `/etc/xinetd.conf` i després té un directori amb arxius per cada servei individual `/etc/xinetd.d`

Aquest sistema a diferència de inetd, no és un conjunt de línies llargues, on cada una de les línies llargues representa la configuració per cada servei, sinó que aquí almenys de manera visual es veu com un bloc amb claus (fa que sigui més fàcil de llegir), aquest dimoni conté tot els camps mencionats anteriorment al inetd, però també compte amb altres camps com

- **only\_From**: Permet especificar quines adreces vols que es pugui connectar a aquell servei en específic
- **banner\_fail** : És un camp on es permet especificar un arxiu de text que es mostrarà quan la host remota denegui la connexió
- **log\_on\_failure** : Un atribut que indica la informació que s'escriu en el registre quan falla una connexió.
- **acces\_time** : Hores a les quals pot funcionar el servei.

```
GNU nano 6.2                                /etc/xinetd.d/ejemplo1 *

service ejemplo1
{
    type          = UNLISTED
    port          = 2025
    socket_type   = stream
    protocol      = tcp
    wait          = no
    user          = root
    server        = /bin/date
}
```

*Fotografia 2: Exemple fet per mi de la configuració de xinetd*

## **2. Com es pot configurar el servei SSH amb inetd i xinetd? Descriu el procés que hauries de seguir per fer-ho amb cada un.**

Primer explicaré el procés per fer-lo amb inetd, i posteriorment explicaré pas a pas com fer el de xinetd.

Primer de tot, cal destacar que n'hi ha un pas que he fet pels dos, perquè funcioni el dimoni de SSH amb inetd i xinetd, primer he de parar el servei original SSH, perquè podem adreçar-lo al servei xinetd o inetd corresponent. És per això que el primer pas serà el següent

- **Systemctl stop ssh**, per parar el servei original i així poder adreçar-lo amb inetd o xinetd
- **Systemctl disable ssh** , ja que tal com diu al PowerPoint un servei pot estar en 3 executions levels i jo ara mateix vull que l'original estigui en disabled.

```
javier@javier-virtual-machine:/ $ sudo systemctl stop ssh
javier@javier-virtual-machine:/ $ sudo systemctl disable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable ssh
Removed /etc/systemd/system/sshd.service.
Removed /etc/systemd/system/multi-user.target.wants/sshd.service.
javier@javier-virtual-machine:/ $
```

*Fotografia 3: Parar el servei original SSH*

Cal aclarir que també ens hem de descarregar els paquets corresponents, de inetd i de xinetd, cosa que jo ja he fet per l'exercici 1, per veure l'interior dels seus .conf. Cal dir que aquests dos paquets són incompatibles, només pot tenir un dels dos

```
javier@javier-virtual-machine:~$ sudo apt update
sudo apt install openbsd-inetd
Obj:1 http://es.ports.ubuntu.com/ubuntu-ports jammy InRelease
Obj:2 http://es.ports.ubuntu.com/ubuntu-ports jammy-updates InRelease
Obj:3 http://ports.ubuntu.com/ubuntu-ports jammy-security InRelease
Obj:4 http://es.ports.ubuntu.com/ubuntu-ports jammy-backports InRelease
Des:5 http://ports.ubuntu.com/ubuntu-ports jammy-proposed InRelease [279 kB]
Descargados 279 kB en 1s (309 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 152 paquetes. Ejecute «apt list --upgradable» para verlos.
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  tcpd
Se instalarán los siguientes paquetes NUEVOS:
  openbsd-inetd tcpd
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 152 no actualizados.
Se necesita descargar 50,6 kB de archivos.
Se utilizarán 177 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://es.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 tcpd arm64 7.6.q-31build2 [25,4 kB]
Des:2 http://es.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 openbsd-inetd arm64 0.20160825-5 [25,1 kB]
Descargados 50,6 kB en 1s (76,6 kB/s)
Seleccionando el paquete tcpd previamente no seleccionado.
(Leyendo la base de datos ... 220825 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../tcpd_7.6.q-31build2_arm64.deb ...
Desempaquetando tcpd (7.6.q-31build2) ...
Seleccionando el paquete openbsd-inetd previamente no seleccionado.
Preparando para desempaquetar .../openbsd-inetd_0.20160825-5_arm64.deb ...
Desempaquetando openbsd-inetd (0.20160825-5) ...
Configurando tcpd (7.6.q-31build2) ...
Configurando openbsd-inetd (0.20160825-5) ...
Created symlink /etc/systemd/system/multi-user.target.wants/inetd.service → /lib/systemd/system/inetd.service.
Procesando disparadores para man-db (2.10.2-1) ...
javier@javier-virtual-machine:~$
```

Fotografía 4: Instal·lació paquete inetd

```
javier@javier-virtual-machine:~$ sudo apt install xinetd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  tcpd
Utilice «sudo apt autoremove» para eliminarlo.
Los siguientes paquetes se ELIMINARÁN:
  openbsd-inetd
Se instalarán los siguientes paquetes NUEVOS:
  xinetd
0 actualizados, 1 nuevos se instalarán, 1 para eliminar y 152 no actualizados.
Se necesita descargar 97,1 kB de archivos.
Se utilizarán 213 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://es.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 xinetd arm64 1:2.3.15.3-1 [97,1 kB]
Descargados 97,1 kB en 1s (112 kB/s)
(Leyendo la base de datos ... 220845 ficheros o directorios instalados actualmente.)
Desinstalando openbsd-inetd (0.20160825-5) ...
Seleccionando el paquete xinetd previamente no seleccionado.
(Leyendo la base de datos ... 220837 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../xinetd_1%3a2.3.15.3-1_arm64.deb ...
Desempaquetando xinetd (1:2.3.15.3-1) ...
Configurando xinetd (1:2.3.15.3-1) ...
Procesando disparadores para man-db (2.10.2-1) ...
javier@javier-virtual-machine:~$
```

Fotografía 5: Instal·lació paquete xinetd

Ara ja tenim això començarem amb la configuració de l'inetd

- Primer hem d'obrir el fitxer /etc/inetd.conf amb nano per afegir una línia
- Ara hem d'afegir una línia sabent que cada línia de inetd necessita el següent per configurar el servei
  - **Nom del servei:** Aquí posarem SSH, ja que és el nom del servei, que estem configurant
  - **Tipus de socket :** Aquí tenim l'opció o bé de stream o bé dgram, es recomana l'opció de stream perquè és important que la informació arribi de manera ordenada i que no es perdi la informació (de l'altre mode també arriba la informació, però no passa res si la informació es perd o arriba de manera ordenada).l
  - **Protocol:** El protocol normalment de la SSH és TCP, ja que és el protocol recomanat per serveis com ssh.
  - **Espera o Ara (Wait/NoWait) :** Per SSH, es sol utilitzar No wait, ja que es vol permetre que molta gent entri a la vega (és a dir permetre la concorrència).
  - **Usuari:** Aquí posarem com l'usuari el root perquè tingui els permisos corresponents per executar la comanda
  - **Via:** Aquí posarem el path, que ha de fer servir, en aquest cas pel SSH és /usr/sbin/sshd
  - **Mandat:** Per últim, tenim l'acció que ha de fer que és sshd i li posem un -i, aquest flag -i indica al servei sshd que no s'executi com un dimoni independent sinó que esperi a rebre connexió a través de inetd.
- Per tant, la comanda ens quedaria la següent : **ssh stream tcp nowait root /usr/sbin/sshd sshd -i**
- Finalment, quan ja hem afegit aquesta línia hem de guardar el fitxer i reiniciar inetd perquè capti els canvis que hem fet (**sudo systemctl restart inetd**)

Per demostrar que va el que he fet és connectar-me des de la meva pròpia màquina virtual a través de SSH i com podem veure al principi sí que em deixa connectar a través de ssh, però en el moment en què faig el stop del servei inetd, ja no em deixa connectar

```
GNU nano 6.2                                     /etc/inetd.conf *
```

```
ssh stream tcp nowait root /usr/sbin/sshd sshd -i
```

*Fotografía 6: Configuració del servei ssh*

```
javier@javier-virtual-machine:~$ sudo systemctl stop ssh
javier@javier-virtual-machine:~$ sudo systemctl restart openbsd-inetd
javier@javier-virtual-machine:~$ ssh javier@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:rbU/5E0w/fCpMxDrq0wGMXqWVdWhBogiAcoAd8X18WU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
javier@localhost's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.8.0-88-generic aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 165 actualizaciones de forma inmediata.
1 de estas es una actualización de seguridad estándar.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

1 actualización de seguridad adicional se puede aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps at https://ubuntu.com/esm

Last login: Mon Dec  1 11:44:31 2025 from 172.16.114.1
javier@javier-virtual-machine:~$
```

*Fotografía 7: Prova del seu correcte funcionament*

```
javier@javier-virtual-machine:~$ ssh javier@localhost
javier@localhost's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.8.0-88-generic aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

El mantenimiento de seguridad expandido para Applications está desactivado
[...]
Se pueden aplicar 165 actualizaciones de forma inmediata.
1 de estas es una actualización de seguridad estándar.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

1 actualización de seguridad adicional se puede aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps at https://ubuntu.com/esm

New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Dec 14 17:04:49 2025 from 127.0.0.1
javier@javier-virtual-machine:~$ exit
cerrar sesión
Connection to localhost closed.
javier@javier-virtual-machine:~$ sudo systemctl stop openbsd-inetd
javier@javier-virtual-machine:~$ ssh javier@localhost
ssh: connect to host localhost port 22: Connection refused
javier@javier-virtual-machine:~$
```

*Fotografía 8: Prueba de que funciona a partir de inetd*

Per una altra banda, per la configuració del xinetd no és tan diferent, els passos que s'han de fer són els següents

- Hem de crear un fitxer amb el següent path **/etc/xinetd.d/{service\_name}**, en el meu cas i posaré com nom SSH
- Posteriorment de crear-lo l'obrim i hem d'afegir el següent bloc d'informació entre claudetes
  - **Nom del servei:** SSH
  - **Tipus de socket :** Stream (Explicitat anteriorment perquè)
  - **Protocol:** TCP (Explicitat anteriorment perquè)
  - **Espera o Ara (Wait/NoWait) :** no (Explicitat anteriorment perquè)
  - **Usuari:** Root (Explicitat anteriorment perquè)
  - **Via:** Aquí posarem el path, que ha de fer servir, en aquest cas pel SSH és /usr/sbin/sshd
  - **Server\_args = -i**, per indicar-li que és el Inetd el que està escoltant el port (Inetd Mode)
  - **log\_on\_success=** HOST PID, amb això estem fent que quan el succès funcioni s'escrigui la IP de qui s'ha connectat i l'ID del procés que s'ha guardat
  - **log\_on\_failure =HOST USERID**, per si alguna persona intentar entrar i falla.es guarda la seva IP i l'usuari que va intentar usar
- Finalment, igual que abans hem de guarda el document i reiniciar el xinetd perquè agafi els canvis **sudo systemctl restart xinetd**

Per demostrar que va he fet la mateixa prova que abans, és a dir m'he connectat a través de la meva màquina virtual a través de ssh i posteriorment he fet un stop del servei.

```
GNU nano 6.2                                         /etc/xinetd.d/SSH *
service ssh
{
    socket_type      = stream
    protocol         = tcp
    wait             = no
    user             = root
    server           = /usr/sbin/sshd
    server_args      = -i
    log_on_success   += HOST PID
    log_on_failure   += HOST USERID
    disable          = no
}
```

*Fotografia 9: Configuració SSH amb xinetd.d*

```
javier@javier-virtual-machine:~$ sudo systemctl restart xinetd
javier@javier-virtual-machine:~$ ssh javier@localhost
javier@localhost's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.8.0-88-generic aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 165 actualizaciones de forma inmediata.
1 de estas es una actualización de seguridad estándar.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

1 actualización de seguridad adicional se puede aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps at https://ubuntu.com/esm

New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Dec 14 17:23:23 2025 from 127.0.0.1
javier@javier-virtual-machine:~$ sudo systemctl stop xinetd
[sudo] contraseña para javier:
javier@javier-virtual-machine:~$ exit
cerrar sesión
Connection to localhost closed.
javier@javier-virtual-machine:~$ ssh javier@localhost
ssh: connect to host localhost port 22: Connection refused
javier@javier-virtual-machine:~$
```

**Fotografia 10:** Prova que funciona i que només funciona a través de xinetd

**3. Crea un servei nou que escolti les connexions entrants a través de netcat i desí l'input en un fitxer de la teva elecció. El servei ha de complir amb les següents restriccions:**

**a. Només pot acceptar connexions entre les 8:00h i les 18:00h.**

**b. Només ha de permetre una única connexió simultània.**

**Explica com ho has fet.**

Per porta a cap aquest exercici, faré ús de l'eina xinetd, ja que a diferència de inetd aquesta quan fas la configuració del servei un paràmetre bastant interessant, la qual és accés time que és una que et permet definir les hores en les quals es pot accedir al servei (primer requisit) i després també es pot configurar si es vol que n'hi hagi una única connexió activant el Wait,(això també es pot fer a inetd).

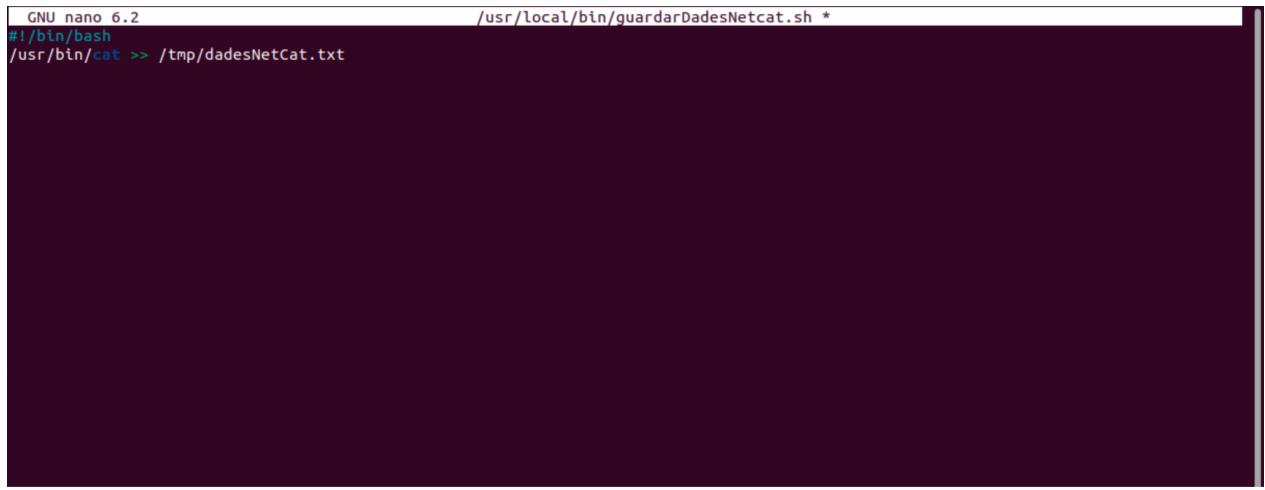
Llavor els passos per crear aquest nou servei són els següents

- Primer creem el fitxer txt on volem que es guardi totes les dades, jo en el meu cas l'he anomenat dadesNetCat.txt

The screenshot shows a terminal window with the title 'tmp/dadesNetCat.txt'. The status bar at the top left says 'GNU nano 6.2'. The main area of the terminal is completely blank, showing only the dark background of the text editor.

**Fotografia 11: Fitxer on es guardarà la informació**

- Després d'haver creat aquell TXT, crem un script que el que faci sigui que qualsevol informació que arribi de stdin (l'entrada normal) s'escrigui al fitxer que hem creat anteriorment, això el farem redirigint amb **cat >> /tmp/dadesNetCat.txt**. Posteriorment, li donem els permisos necessaris al script amb chmod +x



```
GNU nano 6.2                               /usr/local/bin/guardarDadesNetcat.sh *
#!/bin/bash
/usr/bin/cat >> /tmp/dadesNetCat.txt
```

*Fotografia 11: Script que executarà el servei*

- Posteriorment, hem de crear un fitxer amb el següent path **/etc/xinetd.d/{service\_name}**, en el meu cas , posaré com guardarDadesNetcat per començar la configuració del que se'ns demana

- Quan ja el tinc creat l'obro iafegeixo el següent bloc d'informació entre claudetes
  - **Type** : UNLISTED, perquè és la manera d'indicar que el servei que configurarem no és un dels típics, a diferència del SSH que he fet anteriorment ,es a dir indiquem que no esta al fitxer /etc/services
  - **Tipus de socket** : Stream, perquè m'interessa que tota la informació arribi correctament
  - **Protocol**: TCP
  - **Port**: Hem de definir el port pel qual escoltarem aquesta acció, com del port 0 al 1023 estan ocupats, jo faré ús del port 1024.
  - **Espera o Ara (Wait/NoWait)** : yes, això el posem amb yes perquè és la manera d'indicar que només es permet una connexió simultània (requisit que ens ha posat)
  - **Usuari**: Root (Explicitat anteriorment perquè)
  - **Server** : Aquí posarem el path, que ha de fer servir, en aquest cas posaré l'script que he creat que l'he anomenat guardarDadesNetcat.sh i el seu path seria /usr/local/bin/guardarDadesNetcat.sh
  - **acess\_times = 8:00-18:00**

```
GNU nano 6.2                               /etc/xinetd.d/guardarDades *
service guardarDades
{
    disable     = no
    type        = UNLISTED
    port        = 1024
    socket_type = stream
    protocol   = tcp
    wait        = yes
    user        = root
    server      = /usr/local/bin/guardarDadesNetcat.sh
    access_times = 8:00 - 18:00
}
```

*Fotografia 12: Configuració que compleix el requeriments*

- Finalment, igual que abans hem de guarda el document i reiniciar el xinetd perquè agafi els canvis **sudo systemctl restart xinetd**

```
javier@javier-virtual-machine:~$ nc localhost 1024
hola como estas
hola
hola ^C
javier@javier-virtual-machine:~$
```

**Fotografia 14:** Prova de com va la configuració quan estem entre les 8:00 -16:00

```
GNU nano 6.2
hola como estas
hola
```

```
dadesNetCat.txt *
```

**Fotografia 15:** Contingut del fitxer .txt

```
javier@javier-virtual-machine:~$ date
dom 14 dic 2025 18:47:34 CET
javier@javier-virtual-machine:~$ nc localhost 1024
javier@javier-virtual-machine:~$
```

**Fotografia 16:** Prova de com no va si esta fora de l'horari

The image shows two terminal windows side-by-side. The left terminal window has a white background and contains the following text:

```
javier@javier-virtual-machine: ~
javier@javier-virtual-machine: $ sudo service xinetd restart
javier@javier-virtual-machine: $ nc localhost 1024
javier@javier-virtual-machine: $
```

The right terminal window has a dark background and contains the following text:

```
javier@javier-virtual-machine: ~
```

*Fotografia 17: Prova de com no va si n'hi ha una persona connectada (aquesta és la segona terminal, que intenta connectar-se)*

#### 4. Com hem de modificar els fitxers de configuració de sendmail per assignar @aso.com a domini de correu per defecte?

Primer de tot, m'agradaria explicar que és Sendmail, Sendmail és un agent de transferència de correu en servidors com Linux, el qual s'utilitza per enviar emails a destinataris específics, és com una espècie d'intermediari que rebeix correus electrònics de diferents llocs i els dirigeix als seus destins corresponents, per aconseguir fer això fa ús del protocol SMTP (Simple Mail Transfer Protocol).

Ara bé, per aconseguir el que se'ns està demanant a l'exercici, hem de seguir els següents passos

- Primer de tots ens hem de descarregar el paquet corresponent amb **sudo apt install sendmail sendmail-bin m4**

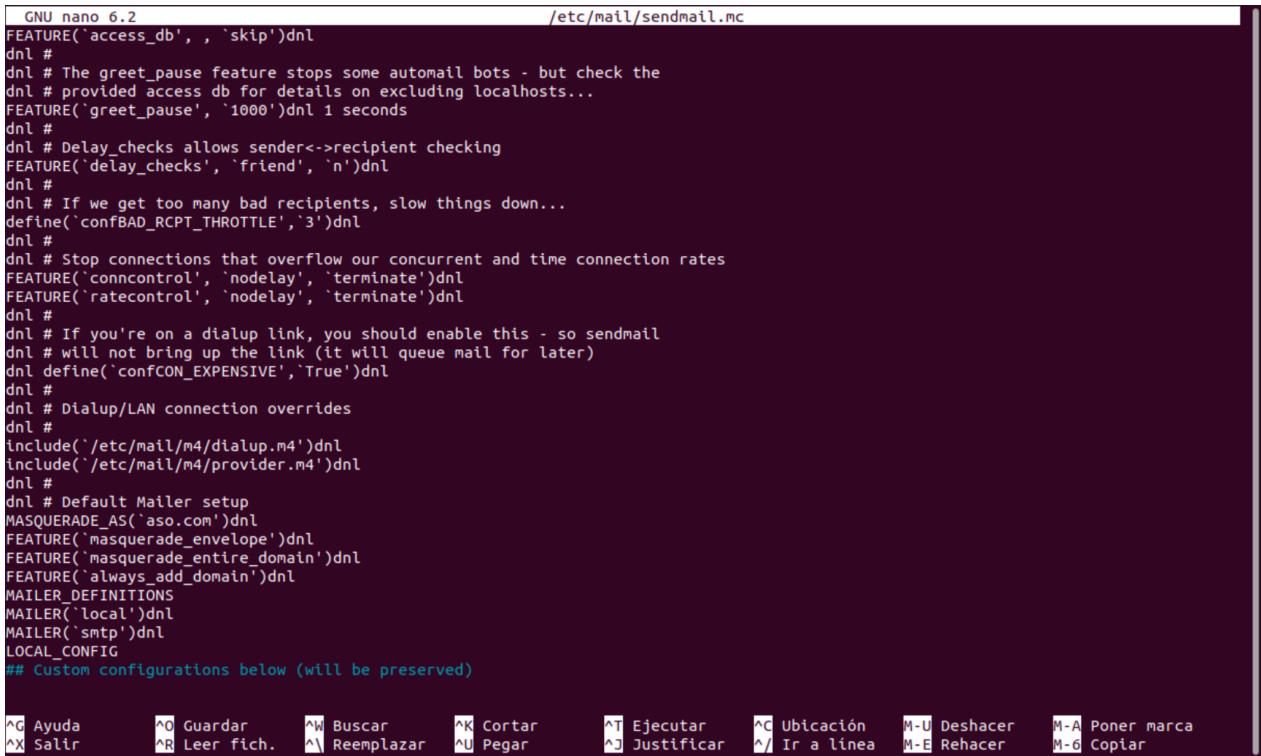
```
javier@javier-virtual-machine: $ sudo apt install sendmail
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  tcpd
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes adicionales:
  libblockfile-bin libblockfile1 libsigsegv2 lockfile-progs m4 make procmail sendmail-base sendmail-bin sendmail-cf sensible-md
Paquetes sugeridos:
  m4-doc make-doc sendmail-doc rmail logcheck resolvconf sasl2-bin
Se instalarán los siguientes paquetes NUEVOS:
  libblockfile-bin libblockfile1 libsigsegv2 lockfile-progs m4 make procmail sendmail sendmail-base sendmail-bin sendmail-cf
  sensible-md
0 actualizados, 12 nuevos se instalarán, 0 para eliminar y 152 no actualizados.
Se necesita descargar 1.316 kB de archivos.
Se utilizarán 5.172 kB de espacio de disco adicional después de esta operación.
Desea continuar? [S/n] S
Des:1 http://es.ports.ubuntu.com/ubuntu-ports jammy/main arm64 libsigsegv2 arm64 2.13-1ubuntu3 [14,5 kB]
Des:2 http://es.ports.ubuntu.com/ubuntu-ports jammy/main arm64 m4 arm64 1.4.18-Subuntu2 [196 kB]
Des:3 http://es.ports.ubuntu.com/ubuntu-ports jammy/main arm64 make arm64 4.3-4.1build1 [177 kB]
Des:4 http://es.ports.ubuntu.com/ubuntu-ports jammy/main arm64 libblockfile-bin arm64 1.17-1build2 [11,6 kB]
Des:5 http://es.ports.ubuntu.com/ubuntu-ports jammy/main arm64 libblockfile1 arm64 1.17-1build2 [6.948 B]
Des:6 http://es.ports.ubuntu.com/ubuntu-ports jammy/main arm64 lockfile-progs arm64 0.1.19build1 [9.784 B]
Des:7 http://es.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 sendmail-base all 8.15.2-22ubuntu3 [139 kB]
Des:8 http://es.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 sendmail-cf all 8.15.2-22ubuntu3 [85,9 kB]
Des:9 http://es.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 sendmail-bin arm64 8.15.2-22ubuntu3 [514 kB]
Des:10 http://es.ports.ubuntu.com/ubuntu-ports jammy/main arm64 procmail arm64 3.22-26build2 [147 kB]
Des:11 http://es.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 sensible-md arm64 8.15.2-22ubuntu3 [8.696 B]
Des:12 http://es.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 sendmail all 8.15.2-22ubuntu3 [6.456 B]
Descargados 1.316 kB en 3s (504 kB/s)
Seleccionando el paquete libsigsegv2:arm64 previamente no seleccionado.
(Leyendo la base de datos... 220875 ficheros o directorios instalados actualmente.)
```

Fotografia 18: Instal·lació del paquet Sendmail

```
javier@javier-virtual-machine:~$ sudo apt install sendmail-bin m4
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
m4 ya está en su versión más reciente (1.4.18-5ubuntu2).
Fijado m4 como instalado manualmente.
sendmail-bin ya está en su versión más reciente (8.15.2-22ubuntu3).
Fijado sendmail-bin como instalado manualmente.
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  tcpd
Utilice «sudo apt autoremove» para eliminarlo.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 152 no actualizados.
javier@javier-virtual-machine:~$
```

**Fotografia 19: Instalació del paquet Sendmail 2**

- Posteriorment, hem d'anar al fitxer **/etc/mail/sendmail.mc** que és on es troba la configuració per posar com default el domini [@aso.com](mailto:@aso.com).



```

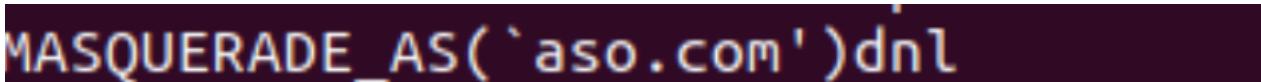
GNU nano 6.2                               /etc/mail/sendmail.mc
FEATURE(`access_db', , `skip')dnl
dnl #
dnl # The greet_pause feature stops some automail bots - but check the
dnl # provided access db for details on excluding localhosts...
FEATURE(`greet_pause', `1000')dnl 1 seconds
dnl #
dnl # Delay_checks allows sender<->recipient checking
FEATURE(`delay_checks', `friend', `n')dnl
dnl #
dnl # If we get too many bad recipients, slow things down...
define(`confBAD_RCPT_THROTTLE', `3')dnl
dnl #
dnl # Stop connections that overflow our concurrent and time connection rates
FEATURE(`connccontrol', `nodelay', `terminate')dnl
FEATURE(`ratecontrol', `nodelay', `terminate')dnl
dnl #
dnl # If you're on a dialup link, you should enable this - so sendmail
dnl # will not bring up the link (it will queue mail for later)
dnl define(`confCON_EXPENSIVE', `True')dnl
dnl #
dnl # Dialup/LAN connection overrides
dnl #
include('/etc/mail/m4/dialup.m4')dnl
include('/etc/mail/m4/provider.m4')dnl
dnl #
dnl # Default Mailer setup
MASQUERADE_AS(`aso.com')dnl
FEATURE(`masquerade_envelope')dnl
FEATURE(`masquerade_entire_domain')dnl
FEATURE(`always_add_domain')dnl
MAILER_DEFINITIONS
MAILER(`local')dnl
MAILER(`smtp')dnl
LOCAL_CONFIG
## Custom configurations below (will be preserved)

^G Ayuda      ^O Guardar      ^N Buscar      ^K Cortar      ^T Ejecutar      ^C Ubicación      M-U Deshacer      M-A Poner marca
^X Salir      ^R Leer fich.   ^Y Reemplazar   ^U Pegar       ^J Justificar    ^I Ir a línea    M-E Rehacer      M-B Copiar

```

**Fotografia 20: Fitxer sendmail.c**

- Quan ja estem allí ens n'hem d'anar a una línia que té la següent estructura **MASQUERADE\_AS('host.domain')**, aquesta és la línia per determinar el domini de correu per defecte, això si únicament modifica el domini de manera visible , així que en la part on posa host.domain hem de posar [@aso.com](mailto:@aso.com)



**MASQUERADE\_AS(`aso.com')dnl**

**Fotografia 21: Configuració domini**

- També hem de modificar una línia que posa FEATURE (**masquerade\_envelope**) que és la adreça que utilitza Sendmail per fer el procés de SMTP i que si no coincideix amb el **masquerade\_as** dona problemes (és el que m'ha passat a mi).

```
PIPE " /usr/bin/ls -l & cat < /dev/null "
MASQUERADE_AS('aso.com')dnl
FEATURE('masquerade_envelope')dnl
FEATURE('masquerade_entire_domain')dnl
FEATURE('always_add_domain')dnl
MAILER DEFINITIONS
```

### Fotografia 22: Configuració domini 2

- Finalment, hem de crear el fitxer de configuració que Sendmail farà servir per fer tot aquest procés. Aquest fitxer el farem a partir del paquet m4 que ens hem descarregat anteriorment. Però com a mi no m'anava molt bé el que jo vaig fer va ser utilitzar la comanda sendmailconfig que em configura allò ja manualment.

```
javier@javier-virtual-machine: $ sudo sendmailconfig
Configure sendmail with the existing /etc/mail/sendmail.conf? [Y] Y
Reading configuration from /etc/mail/sendmail.conf.
Validating configuration.
Writing configuration to /etc/mail/sendmail.conf.
Writing /etc/cron.d/sendmail.
Configure sendmail with the existing /etc/mail/sendmail.mc? [Y] Y
Updating sendmail environment ...
Reading configuration from /etc/mail/sendmail.conf.
Validating configuration.
Writing configuration to /etc/mail/sendmail.conf.
Writing /etc/cron.d/sendmail.
Reading configuration from /etc/mail/sendmail.conf.
Validating configuration.
Writing configuration to /etc/mail/sendmail.conf.
Writing /etc/cron.d/sendmail.
Could not open /etc/mail/databases(No such file or directory), creating it.
Reading configuration from /etc/mail/sendmail.conf.
Validating configuration.
Creating /etc/mail/databases...
Checking filesystem, this may take some time - it will not hang!
... Done.

Checking for installed MDAs...
```

### Fotografía 23: Ús de la comanda sendmailconfig

- Quan ja hem fet tot això hem de fer un **systemctl restart sendmail** perquè el paquet Sendmail agafi la nova configuració que hem fet

Per demostrar que tota la configuració està bé el que vaig fer és enviar-me un mail al meu mail de la universitat per veure amb quin email m'arribava, cal dir que per enviar-me l'email m'he hagut de descarregar un altre paquet, anomenat mail.

Com podem veure a la fotografia on faig l'email, l'email s'envia perfectament, però per culpa dels filtres que tenen plataformes com Gmail, en cap minut m'ha arribat l'email. Per tant, tampoc puc acabar de provar que això funciona, però tot el procés està correcte.

És per això que un altre dia vaig decidir enviar-me l'email al meu propi usuari per posteriorment fer un `cat /var/mail/javier`, per veure com si es feia bé el domini [@aso.com](mailto:@aso.com) i com podem veure a l'última imatge sí que es fa bé

```
javier@javier-virtual-machine:~$ echo "Prova per fer comprobar el domini ." | mail -s "Prova Domini correcte " javier.fv@students.salle.url.edu
No se ha encontrado la orden «mail», pero se puede instalar con:
sudo apt install mailutils
javier@javier-virtual-machine:~$ sudo apt install mailutils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
tcpd
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes adicionales:
  gsasl-common guile-3.0-libs libgsasl7 libmailutils8 libmysqlclient21 libntlm0 libpq5 mailutils-common mysql-common
Paquetes sugeridos:
  mailutils-mh mailutils-doc
Se instalarán los siguientes paquetes NUEVOS:
  gsasl-common guile-3.0-libs libgsasl7 libmailutils8 libmysqlclient21 libntlm0 libpq5 mailutils mailutils-common mysql-common
0 actualizados, 10 nuevos se instalarán, 0 para eliminar y 152 no actualizados.
Se necesita descargar 10,2 MB de archivos.
Se utilizarán 66,0 KB de espacio de disco adicional después de esta operación.
```

**Fotografia 23: Prova cap a un Gmail personal**

```
javier@javier-virtual-machine:~$ echo " Test Intern" | mail -s "Test Intern" javier
javier@javier-virtual-machine:~$ sudo cat /var/mail/javier
From JAVIER javier@aso.com Fri Dec 19 01:20:17 2025
```

**Fotografia 24: Prova interna**

```
Prova per fer comprobar el domini .

From javier@aso.com Fri Dec 19 01:20:17 2025
Return-Path: <javier@aso.com>
Received: from javier-virtual-machine (localhost [127.0.0.1])
    by javier-virtual-machine (8.15.2/8.15.2/Debian-22ubuntu3) with ESMTP id 5BJ0KHvr084473
    for <javier@javier-virtual-machine>; Fri, 19 Dec 2025 01:20:17 +0100
Received: (from javier@localhost)
    by javier-virtual-machine (8.15.2/8.15.2/submit) id 5BJ0KHak084438;
    Fri, 19 Dec 2025 01:20:17 +0100
From: JAVIER <javier@aso.com>
Message-ID: <202512190020.5BJ0KHak084438@javier-virtual-machine>
Subject: Test Intern
To: javier@javier-virtual-machine
User-Agent: mail (GNU Mailutils 3.14)
Date: Fri, 19 Dec 2025 01:19:17 +0100

    Test Intern

javier@javier-virtual-machine:~$
```

**Fotografia 25: Comprovació de la prova interna**

## 5. Com a departament, hem d'organitzar els següents usuaris segons la seva àrea:

- a. IT: Matt, Joan i Paco
- b. HR: Pepe, Toni i Anna

Com hem de configurar el sistema de correu electrònic perquè, quan envoieix un correu a [@aso.com](mailto:@aso.com) només arribi als quals pertanyen a aquella àrea? Descriu el procés que has de seguir.

Per poder fer això hem de fer ús de les àlies, és a dir hem de definir unes àlies per cada

usuari. Per aconseguir fer això el que farem serà anar al fitxer **/etc/mail/aliases** i agrega una entrada per cada client de correu. L'estructura que hem de seguir per cada línia que definim ha de ser la següent:**alias:expanded-alien**

Com per aquests exercicis ens demanen dos àlies, n'haurem d'afegir dues, línies per cada una dels àlies corresponents. Un serà la línia IT: matt, joan, paco i l'altre serà HR: pepe, toni, anna. Cal dir que els usuaris que estic posant són usuaris que posteriorment jo crearé amb un adduser per fer la prova.

Quan ja hagim fet això executaré la comanda **sudo newaliases** (també podria fer la comanda **sudo sendmail -bi**), aquesta comanda serveix per actualitzar i traduir a Sendmail, les dades que he posat al fitxer **/etc/mail/aliases**. Posteriorment a això per si de cas el que faré serà fer un restart a Sendmail perquè agafi tota la informació amb un **sudo systemctl restart sendmail**

```
[Es correcta la información? [S/n] S
javier@javier-virtual-machine:$ sudo adduser paco
Añadiendo el usuario 'paco' ...
Añadiendo el nuevo grupo 'paco' (1007) ...
Añadiendo el nuevo usuario 'paco' (1006) con grupo 'paco' ...
Creando el directorio personal '/home/paco' ...
Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para paco
Introduzca el nuevo valor, o presione INTRO para el predeterminado
  Nombre completo []: paco
  Número de habitación []:
  Teléfono del trabajo []:
  Teléfono de casa []:
  Otro []:
¿Es correcta la información? [S/n] S
javier@javier-virtual-machine:$ sudo adduser pepe
Añadiendo el usuario 'pepe' ...
Añadiendo el nuevo grupo 'pepe' (1008) ...
Añadiendo el nuevo usuario 'pepe' (1007) con grupo 'pepe' ...
Creando el directorio personal '/home/pepe' ...
Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para pepe
Introduzca el nuevo valor, o presione INTRO para el predeterminado
  Nombre completo []: pepe
  Número de habitación []:
  Teléfono del trabajo []:
  Teléfono de casa []:
  Otro []:
¿Es correcta la información? [S/n] S
```

### Fotografia 26: Afegir usuaris

```
javier@javier-virtual-machine:$ sudo adduser toni
Añadiendo el usuario 'toni' ...
Añadiendo el nuevo grupo 'toni' (1009) ...
Añadiendo el nuevo usuario 'toni' (1008) con grupo 'toni' ...
Creando el directorio personal '/home/toni' ...
Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para toni
Introduzca el nuevo valor, o presione INTRO para el predeterminado
  Nombre completo []:
  Número de habitación []:
  Teléfono del trabajo []:
  Teléfono de casa []:
  Otro []:
¿Es correcta la información? [S/n] S
javier@javier-virtual-machine:$ sudo adduser anna
Añadiendo el usuario 'anna' ...
Añadiendo el nuevo grupo 'anna' (1010) ...
Añadiendo el nuevo usuario 'anna' (1009) con grupo 'anna' ...
Creando el directorio personal '/home/anna' ...
Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para anna
Introduzca el nuevo valor, o presione INTRO para el predeterminado
  Nombre completo []: anna
  Número de habitación []:
  Teléfono del trabajo []:
  Teléfono de casa []:
  Otro []:
¿Es correcta la información? [S/n] S
javier@javier-virtual-machine:$
```

### Fotografia 27: Afegir usuaris 2

```
GNU nano 6.2                                         /etc/mail/aliases *
```

```
IT: matt, joan, paco  
HR: pepe, tont, anna
```

*Fotografia 28: Configuració Àlies*

```
javier@javier-virtual-machine:/$ sudo nano /etc/mail/aliases  
javier@javier-virtual-machine:/$ sudo newaliases  
WARNING: local host name (javier-virtual-machine) is not qualified; see cf/README  
E: WHO AM I?  
/etc/mail/aliases: 2 aliases, longest 16 bytes, 36 bytes total  
javier@javier-virtual-machine:/$
```

*Fotografia 29: Configuració Àlies 2*

```
javier@javier-virtual-machine:~$ echo " HR" | mail -s "Test HR" HR
javier@javier-virtual-machine:~$ sudo cat /var/mail/pepe
From javier@aso.com Fri Dec 19 01:02:26 2025
Return-Path: <javier@aso.com>
Received: from Javier-Virtual-Machine (localhost [127.0.0.1])
    by Javier-Virtual-Machine (8.15.2/8.15.2/Debian-22Ubuntu3) with ESMTP id 5B3020YB083610
    for <HR@javier-virtual-machine>; Fri, 19 Dec 2025 01:02:24 +0100
Received: (from Javier@localhost)
    by Javier-Virtual-Machine (8.15.2/8.15.2/Submit) id 5B3020Jh083602;
    Fri, 19 Dec 2025 01:02:24 +0100
From: JAVIER <javier@aso.com>
Message-ID: <>202512190002.5B3020Jh083602@javier-virtual-machine>
Subject: Test HR
To: HR@javier-virtual-machine
User-Agent: mail (GNU Mailutils 3.14)
Date: Fri, 19 Dec 2025 01:01:24 +0100

HR

javier@javier-virtual-machine:~$ sudo cat /var/mail/toni
From javier@aso.com Fri Dec 19 01:02:25 2025
Return-Path: <javier@aso.com>
Received: from Javier-Virtual-Machine (localhost [127.0.0.1])
    by Javier-Virtual-Machine (8.15.2/8.15.2/Debian-22Ubuntu3) with ESMTP id 5B3020YB083610
    for <HR@javier-virtual-machine>; Fri, 19 Dec 2025 01:02:24 +0100
Received: (from Javier@localhost)
    by Javier-Virtual-Machine (8.15.2/8.15.2/Submit) id 5B3020Jh083602;
    Fri, 19 Dec 2025 01:02:24 +0100
From: JAVIER <javier@aso.com>
Message-ID: <>202512190002.5B3020Jh083602@javier-virtual-machine>
Subject: Test HR
To: HR@javier-virtual-machine
User-Agent: mail (GNU Mailutils 3.14)
Date: Fri, 19 Dec 2025 01:01:24 +0100

HR

javier@javier-virtual-machine:~$ █
```

### *Fotografia 30 Prova del funcionament dels àlies*

## **6. Què passa quan hi ha regles contradictòries als fitxers /etc/hosts.deny i /etc/hosts.permit? Mostra també un exemple.**

Primer m'agradaria explicar que fa cada un dels dos fitxers i posteriorment explicaré que passa si n'hi ha informació contradictòria en aquests dos fitxers.

Per una banda, tenim host.deny, el qual és un arxiu de text per sistemes operatius com Linux, que bàsicament serveix per bloquejar unes IP o una llista d'adreses IP, de tal manera que l'ordinador no pugui accedir al seu ordinador, és a dir serveix per especificar quines adreces IP, hostnames o que dominis no poden connectar-se al servidor de l'ordinador. A aquest fitxer cada línia conté tres camps, un és l'adreça IP, l'altre és el nom de l'amfitrió i de manera opcional pot posar com tercer camp l'àlies que tens assignat per aquella host. Per exemple si vols bloquejar Google seria ficar una línia així **123.45.6.7 [www.google.com](http://www.google.com)**

Per una altra banda, ens trobem amb la host.permit o en alguns dispositius host.allow ,que tal com indica el seu nom és un fitxer que conté els noms, IP o dominis de host que tenen accés al nostre PC.

Aquests dos fitxers estan controlats i gestionat pel TCPD, per tant, quan passa això de què n'hi ha alguna contradicció TCPD li donarà prioritat i precedència ala host.allow respecte la host.deny perquè així està configurat, ja que quan troba una coincidència en .allow ja no busca a .deny. En conseqüència, si posem per exemple una prohibició cap al domini de Google en host.deny i després a host.permit posem que està permesa aquesta adreça, el sistema operatiu li deixarà a Google accedir al nostre ordinador.

Per demostrar això el que faré serà posar tant al meu fitxer host.deny que prohíbeix la connexió sshd de la IP de la meva màquina virtual (que en el meu cas és la 172.16.114.130) i, per una altra banda, posaré al fitxer host.allow que sí que accepti la connexió SSHD de la IP del meu ordinador. Com podem veure a l'última imatge ,sí que em deixa connectar fer la connexió SSH. Per tant, la host.allow té prioritat davant la host.deny

```
GNU nano 6.2                                     /etc/hosts.deny *
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#           See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
sshd: 172.16.114.130
```

█

**Fotografia 31: Configuració fitxer host.deny**

```
GNU nano 6.2                                     /etc/hosts.allow *
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#           See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
sshd: 172.16.114.130
```

█

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación M-U Deshacer M-A Poner marca  
^Y Salir ^O Guardar ficha ^W Buscar linea ^K Borrar ^T Ejecutar linea ^C Ubicación linea M-U Deshacer linea M-A Poner marca linea

**Fotografia 32: Configuració fitxer host.allow**

```
javier@javier-virtual-machine: $ sudo nano /etc/hosts.deny
javier@javier-virtual-machine: $ sudo nano /etc/hosts.allow
javier@javier-virtual-machine: $ ssh javier@172.16.114.130
The authenticity of host '172.16.114.130 (172.16.114.130)' can't be established.
ED25519 key fingerprint is SHA256:rbU/5E0W/fCpqXDrq0wGMXqWdWhBogiAcoAd8Xi8WU.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.114.130' (ED25519) to the list of known hosts.
javier@172.16.114.130's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.8.0-88-generic aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 154 actualizaciones de forma inmediata.
1 de estas es una actualización de seguridad estándar.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

3 actualizaciones de seguridad adicionales se pueden aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps at https://ubuntu.com/esm

New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
You have no mail.
Last login: Sun Dec 14 17:25:17 2025 from 127.0.0.1
javier@javier-virtual-machine: $
```

**Fotografia 33: Prova del seu funcionament**

**7. Volem implementar les següents polítiques pel que fa a l'accés extern als nostres serveis:**

- a. Denega totes les connexions que no provenen de la IP del sistema host.
- b. Denega tots els serveis excepte SSH i Telnet.
- c. Denega totes les connexions que provenen del port 80.

**Mostra quines modificacions has hagut de fer i demostra que els teus canvis funcionen.**

Per porta a cap aquest exercici, el que vaig fer és jugar amb el fitxer **host.allow** i el fitxer **host.deny**. Ara explicaré pas a pas el que faig fer

1. Primer de tot vaig anar a editar el fitxer /etc/host.allow i vaig posar les següents línies per permetre els serveis SSH i Telnet sol des de la IP del sistema host.
  - a. **ssh:172.16.114.1**
  - b. **in.telnetd: 172.16.114.1**
2. Posteriorment, vaig anar al fitxer /etc/host.deny i vaig fer un **ALL:ALL**, d'aquesta manera el que estic fent és bloquejant tots els serveis ssh i telnet que no tinguin la IP de la meva host, a més del mateix temps bloquejant totes les connexions en general que no provenen de la IP del sistema host. Amb això estem complint les dues primeres condicions que se'ns ha marcat .
3. Per una altra banda, sabem que el port 80,és un port asignat normalment per un servei WEB/HTTP és per això que per aconseguir fer aquest objectiu el que he fet és afegir una altra línia a **host.deny** amb els noms **HTTP, www.in.httpd:ALL, pero** cal dir que com ja tinc un ALL: ALL al fitxer teòricament ja s'hauria d'estar bloquejant aquest servei.

Per provar que això que he fet va el que vaig fer és provar connectar-me a diferents serveis i des de diferents IPS a la meva màquina virtual. I com podem veure funciona perfectament. Cal dir que per la prova de telnet, com el meu ordinador no té el telnet instal·lat vaig fer ús de la comanda tcpmatch amb la IP de la meva host per prova si acceptava quan era la IP de la host o no i com podem veure sí que accepta la IP. Però cal dir que en el món real els servidors reals com Apache no fan ús de TCP Wrappers, per tant, hi hauria ocasions en què aquesta manera de bloquejar webs podria no funcionar,és per això que per aquesta condició seria millor utilitzar comandes com **UFW** o fer us d'eines com **iptables**

```
GNU nano 6.2                                         /etc/hosts.allow *
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#           See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:   ALL: LOCAL @some_netgroup
#           ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
#sshd:172.16.114.
#in.telnetd: 172.16.114.
```

*Fotografia 34: Configuració fitxer host.allow*

```
GNU nano 6.2                                         /etc/hosts.deny *
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#           See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:   ALL: some.host.name, .some.domain
#           ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
ALL:ALL
HTTP,www.in.hhtpd:ALL
```

*Fotografia 35: Configuració fitxer host.deny*

```
[javierfernandez@MacBook-Pro-de-Javier ~ % ssh javier@172.16.114.130
[javier@172.16.114.130's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.8.0-90-generic aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 155 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

3 actualizaciones de seguridad adicionales se pueden aplicar con ESM Apps.
Aprenda más sobre como activar el servicio ESM Apps at https://ubuntu.com/esm

New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

You have mail.
Last login: Fri Dec 19 16:24:24 2025 from 172.16.114.130
javier@javier-virtual-machine:~$ ]
```

*Fotografia 36: Prova ssh desde el meu host*

```
javier@javier-virtual-machine:~$ ssh javier@127.0.0.1
kex_exchange_identification: read: Connection reset by peer
Connection reset by 127.0.0.1 port 22
javier@javier-virtual-machine:~$ ]
```

*Fotografia 37: Prova ssh desde qualsevol IP*

```
javier@javier-virtual-machine:~$ tcpdump httpd 172.16.114.1
client: address 172.16.114.1
server: process httpd
access: denied
javier@javier-virtual-machine:~$ ]
```

*Fotografia 38: Prova port 80*

```
javier@javier-virtual-machine:~$ tcpdmatch in.telnetd 172.16.114.1
client: address 172.16.114.1
server: process in.telnetd
access: granted
javier@javier-virtual-machine:~$
```

*Fotografia 39: Prova telnet simulat amb tcpdmatch*

```
javier@javier-virtual-machine:~$ tcpdmatch in.telnetd 172.16.115.1
client: address 172.16.115.1
server: process in.telnetd
access: denied
javier@javier-virtual-machine:~$
```

*Fotografia 40: Prova telnet desde qualsevol ip*

## REFERENCIAS

<https://www.ochobitshacenunbyte.com/2017/01/18/servicios-de-internet-en-linux-con-xinetd/>

<https://es.wikipedia.org/wiki/Inetd>

<http://www.sudo.es/docnux/xinetd.html>

<https://debian-handbook.info/browse/es-ES/stable/sect.inetd.html>

<https://www.linuxquestions.org/questions/linux-security-4/xinetd-vs-inetd-176132/>

<https://www.linux.com/training-tutorials/weekend-project-replace-inetd-xinetd-better-network-administration/>

[https://docs.redhat.com/es/documentation/red\\_hat\\_enterprise\\_linux/6/html/security\\_guide/sect-security\\_guide-tcp\\_wrappers\\_and\\_xinetd-xinetd\\_configuration\\_files](https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-tcp_wrappers_and_xinetd-xinetd_configuration_files)

<https://es.scribd.com/document/168222676/2-Punto-Stream-y-Dgram>

<https://www.ibm.com/docs/es/i/7.5.0?topic=inetd-configuring-server>

<https://serverfault.com/questions/391383/ssh-with-xinetd>

<https://superuser.com/questions/695170/changing-default-from-e-mail-address-for-system-accounts-when-using-sendmail>

<https://man7.org/linux/man-pages/man8/sendmail.8.html>

<https://www.solarum.com/library/configuring-sendmail-on-linux/>

<https://askubuntu.com/questions/1363136/configuring-sendmail-on-ubuntu-20-04>

[https://docs.oracle.com/cd/E26502\\_01/html/E28999/mailadmin-43.html](https://docs.oracle.com/cd/E26502_01/html/E28999/mailadmin-43.html)

[https://www.reddit.com/r/linuxquestions/comments/qe0roc/is\\_hostsdeny\\_used\\_to\\_enhance\\_security\\_of\\_servers/?tl=es-es](https://www.reddit.com/r/linuxquestions/comments/qe0roc/is_hostsdeny_used_to_enhance_security_of_servers/?tl=es-es)

<https://labex.io/es/lesson/etc-hosts>

<https://www.merlos.org/linux/2002/02/hosts-access.html>

<https://www.merlos.org/linux/2002/02/hosts-access.html>

[https://docs.oracle.com/cd/E37929\\_01/html/E36533/mailadmin-52.html](https://docs.oracle.com/cd/E37929_01/html/E36533/mailadmin-52.html)