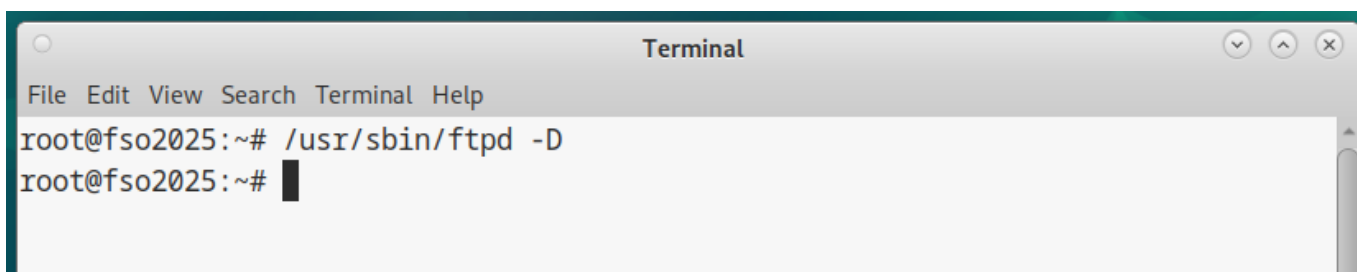


[FORT] Práctica 5: Control de Acceso a nivel de aplicación

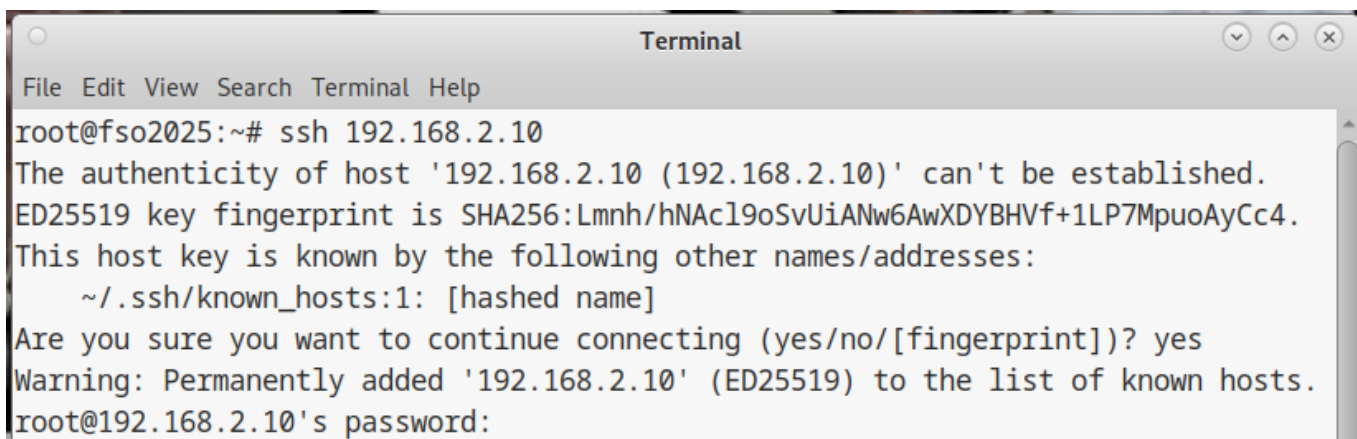
1. Habilita los servicios FTP en MAQUINA1 ejecutando `/usr/sbin/ftp -D`



```
Terminal
File Edit View Search Terminal Help
root@fso2025:~# /usr/sbin/ftpd -D
root@fso2025:~#
```

2. Revisa las conexiones ftp y ssh de MAQUINA2 a MAQUINA1 usando las direcciones de red locales

Comprobación de SSH:



```
Terminal
File Edit View Search Terminal Help
root@fso2025:~# ssh 192.168.2.10
The authenticity of host '192.168.2.10 (192.168.2.10)' can't be established.
ED25519 key fingerprint is SHA256:Lmnh/hNAcl9oSvUiANw6AwXDYBHVf+1LP7MpuoAyCc4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.10' (ED25519) to the list of known hosts.
root@192.168.2.10's password:
```

```
Terminal
File Edit View Search Terminal Help
root@fso2025:~# ssh 192.168.3.10
The authenticity of host '192.168.3.10 (192.168.3.10)' can't be established.
ED25519 key fingerprint is SHA256:Lmnh/hNAcl9oSvUiANw6AwXDYBHVf+1LP7MpuoAyCc4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.3.10' (ED25519) to the list of known hosts.
root@192.168.3.10's password:

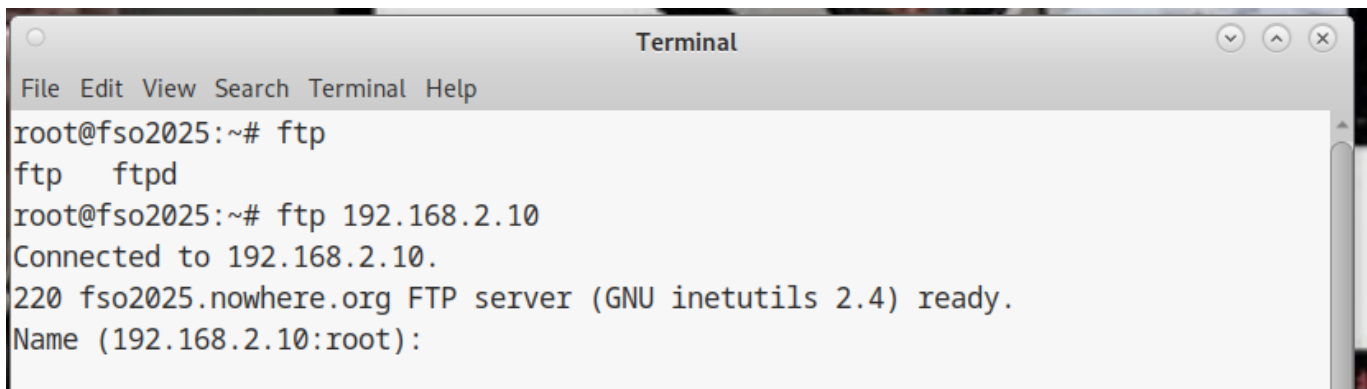
root@fso2025:~# ssh 192.168.4.10
The authenticity of host '192.168.4.10 (192.168.4.10)' can't be established.
ED25519 key fingerprint is SHA256:Lmnh/hNAcl9oSvUiANw6AwXDYBHVf+1LP7MpuoAyCc4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
  ~/.ssh/known_hosts:5: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.4.10' (ED25519) to the list of known hosts.
root@192.168.4.10's password:

root@fso2025:~# ssh 192.168.12.10
The authenticity of host '192.168.12.10 (192.168.12.10)' can't be established.
ED25519 key fingerprint is SHA256:Lmnh/hNAcl9oSvUiANw6AwXDYBHVf+1LP7MpuoAyCc4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
  ~/.ssh/known_hosts:5: [hashed name]
  ~/.ssh/known_hosts:6: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.12.10' (ED25519) to the list of known hosts.
root@192.168.12.10's password:

root@fso2025:~# ssh 192.168.13.10
The authenticity of host '192.168.13.10 (192.168.13.10)' can't be established.
ED25519 key fingerprint is SHA256:Lmnh/hNAcl9oSvUiANw6AwXDYBHVf+1LP7MpuoAyCc4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
  ~/.ssh/known_hosts:5: [hashed name]
  ~/.ssh/known_hosts:6: [hashed name]
  ~/.ssh/known_hosts:7: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.13.10' (ED25519) to the list of known hosts.
root@192.168.13.10's password: █
```

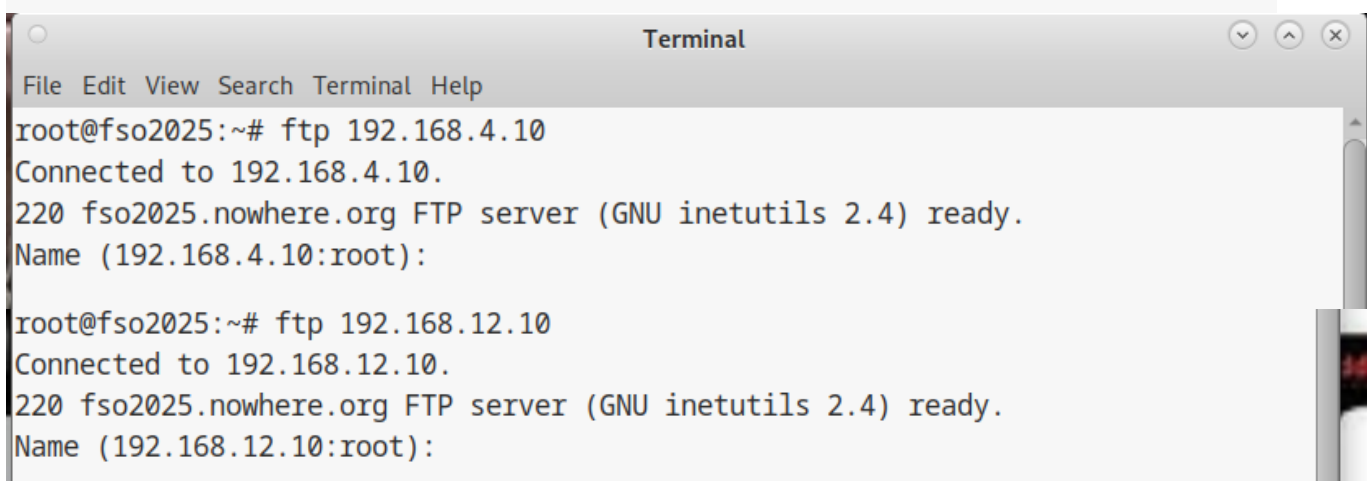
```
root@fso2025:~# ssh 192.168.14.10
The authenticity of host '192.168.14.10 (192.168.14.10)' can't be established.
ED25519 key fingerprint is SHA256:Lmnh/hNAcl9oSvUiANw6AwXDYBHVf+1LP7MpAoAyCc4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
  ~/.ssh/known_hosts:5: [hashed name]
  ~/.ssh/known_hosts:6: [hashed name]
  ~/.ssh/known_hosts:7: [hashed name]
  ~/.ssh/known_hosts:8: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.14.10' (ED25519) to the list of known hosts.
root@192.168.14.10's password: █
```

Comprobación ftp



```
Terminal
File Edit View Search Terminal Help
root@fso2025:~# ftp
ftp ftpd
root@fso2025:~# ftp 192.168.2.10
Connected to 192.168.2.10.
220 fso2025.nowhere.org FTP server (GNU inetutils 2.4) ready.
Name (192.168.2.10:root):
```

```
root@fso2025:~# ftp 192.168.3.10
Connected to 192.168.3.10.
220 fso2025.nowhere.org FTP server (GNU inetutils 2.4) ready.
Name (192.168.3.10:root):
```



```
Terminal
File Edit View Search Terminal Help
root@fso2025:~# ftp 192.168.4.10
Connected to 192.168.4.10.
220 fso2025.nowhere.org FTP server (GNU inetutils 2.4) ready.
Name (192.168.4.10:root):

root@fso2025:~# ftp 192.168.12.10
Connected to 192.168.12.10.
220 fso2025.nowhere.org FTP server (GNU inetutils 2.4) ready.
Name (192.168.12.10:root):
```

```
root@fso2025:~# ftp 192.168.13.10
Connected to 192.168.13.10.
220 fso2025.nowhere.org FTP server (GNU inetutils 2.4) ready.
Name (192.168.13.10:root):

root@fso2025:~# ftp 192.168.14.10
Connected to 192.168.14.10.
220 fso2025.nowhere.org FTP server (GNU inetutils 2.4) ready.
Name (192.168.14.10:root):
```

3. Configura rcptwrappers (/etc/hosts.allow y /etc/hosts.deny) en MAQUINA1 para:

Aceptar todas las conexiones ftp excepto las que vienen de

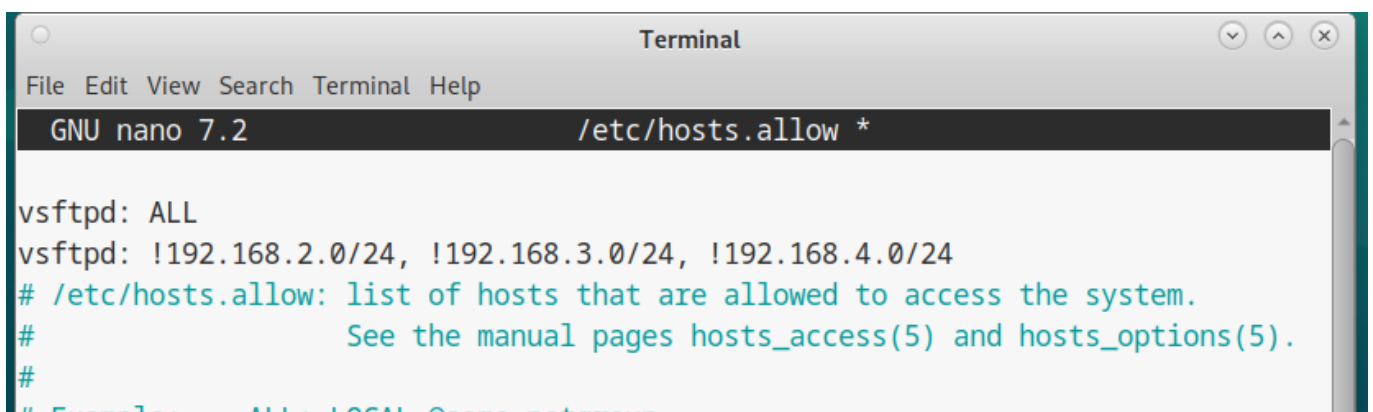
- 192.168.2.X
- 192.168.3.X
- 192.168.4.X

Rechazar todas las conexiones ssh que vienen de:

- 192.168.12.x
- 192.168.13.x
- 192.168.14.X

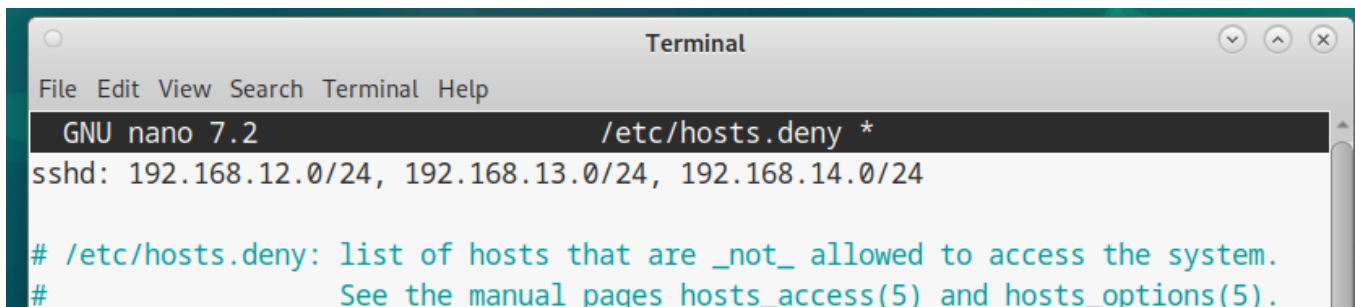
Comenzamos editando el archivo /etc/hosts.allow para aceptar todas las conexiones menos las indicadas con las siguientes líneas:

```
vsftpd: ALL #Se permite todo el tráfico FTP
vsftpd: !192.168.2.0/24, !192.168.3.0/24, !192.168.4.0/24 #Se bloquean los rangos indicados para conexiones FTP
```



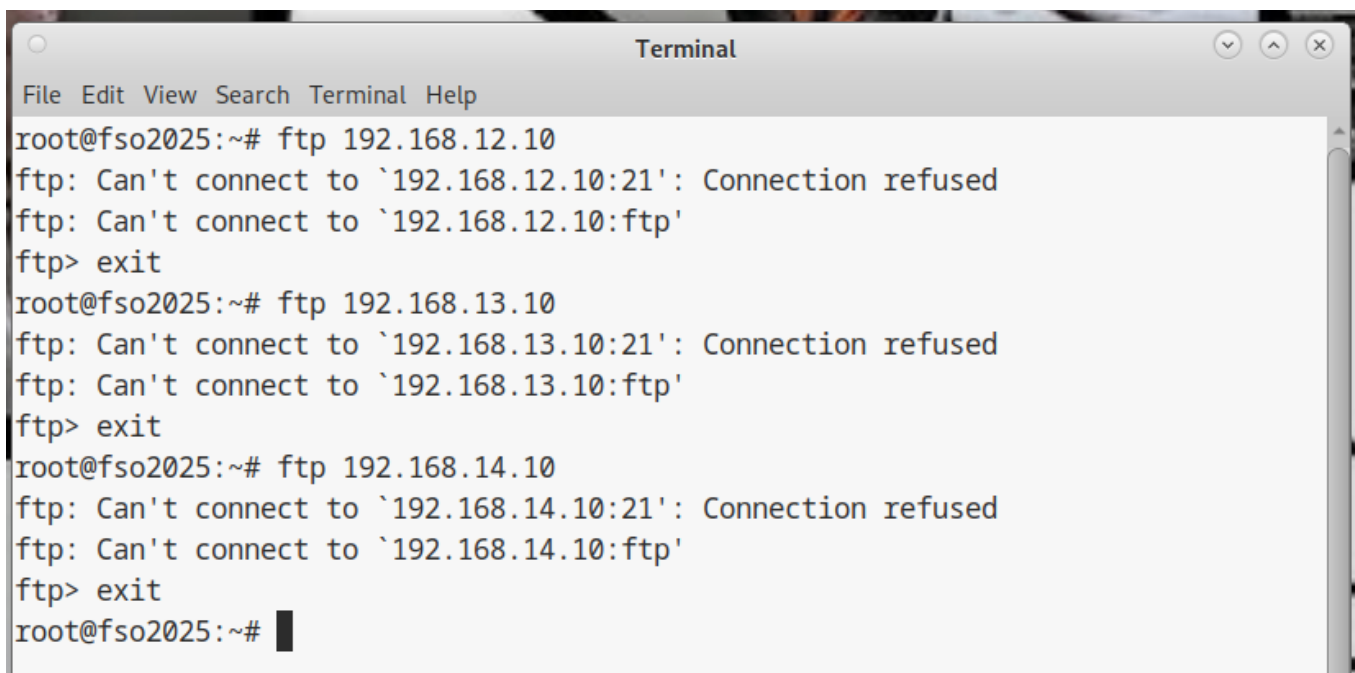
Tras eso procedemos a editar el archivo /etc/hosts.deny para bloquear las conexiones indicadas con las siguientes líneas:

sshd: 192.168.12.0/24, 192.168.13.0/24, 192.168.14.0/24 #Se bloquea el SSH para las direcciones indicadas



4. Revisa las conexiones ftp y ssh desde MAQUINA2 a MAQUINA1

Comenzamos revisando las conexiones FTP:




```
Terminal
File Edit View Search Terminal Help
root@fso2025:~# ftp 192.168.2.10
ftp: Can't connect to `192.168.2.10:21': Connection refused
ftp: Can't connect to `192.168.2.10:ftp'
ftp> exit
root@fso2025:~# ftp 192.168.3.10
ftp: Can't connect to `192.168.3.10:21': Connection refused
ftp: Can't connect to `192.168.3.10:ftp'
ftp>
ftp> exit
root@fso2025:~# ftp 192.168.4.10
ftp: Can't connect to `192.168.4.10:21': Connection refused
ftp: Can't connect to `192.168.4.10:ftp'
ftp> exit
```

Tras eso revisamos las conexiones ssh:

```
Terminal
File Edit View Search Terminal Help
root@fso2025:~# ssh 192.168.2.10
root@192.168.2.10's password:

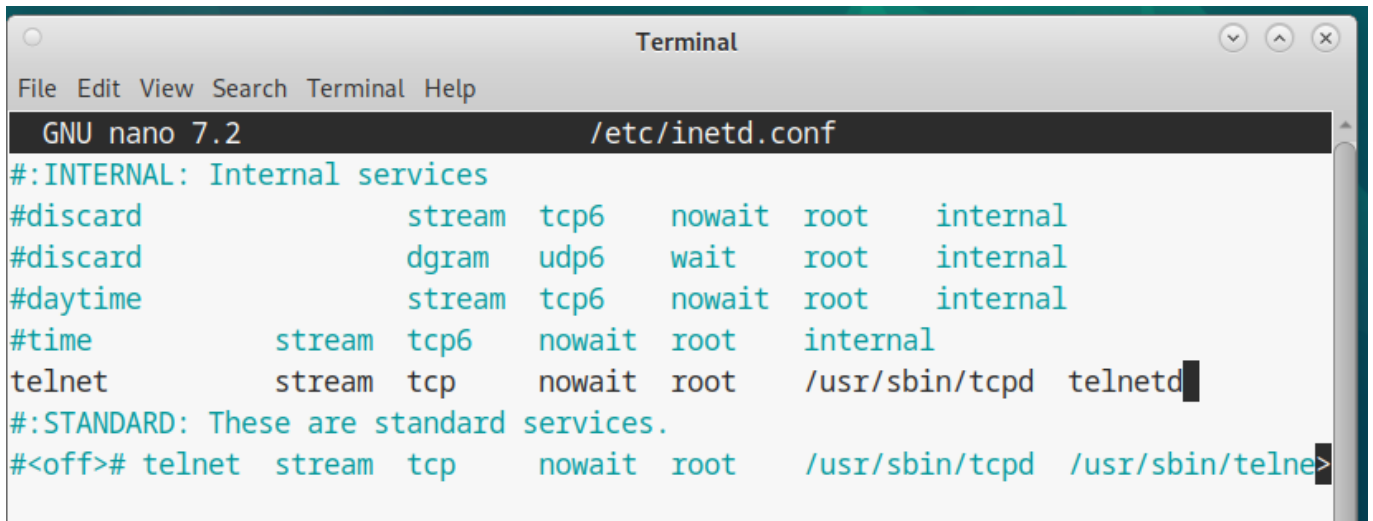
root@fso2025:~# ssh 192.168.3.10
root@192.168.3.10's password:

root@fso2025:~# ssh 192.168.4.10
root@192.168.4.10's password:

root@fso2025:~# ssh 192.168.12.10
kex_exchange_identification: read: Connection reset by peer
Connection reset by 192.168.12.10 port 22
root@fso2025:~# ssh 192.168.13.10
kex_exchange_identification: read: Connection reset by peer
Connection reset by 192.168.13.10 port 22
root@fso2025:~# ssh 192.168.14.10
kex_exchange_identification: read: Connection reset by peer
Connection reset by 192.168.14.10 port 22
root@fso2025:~# █
```

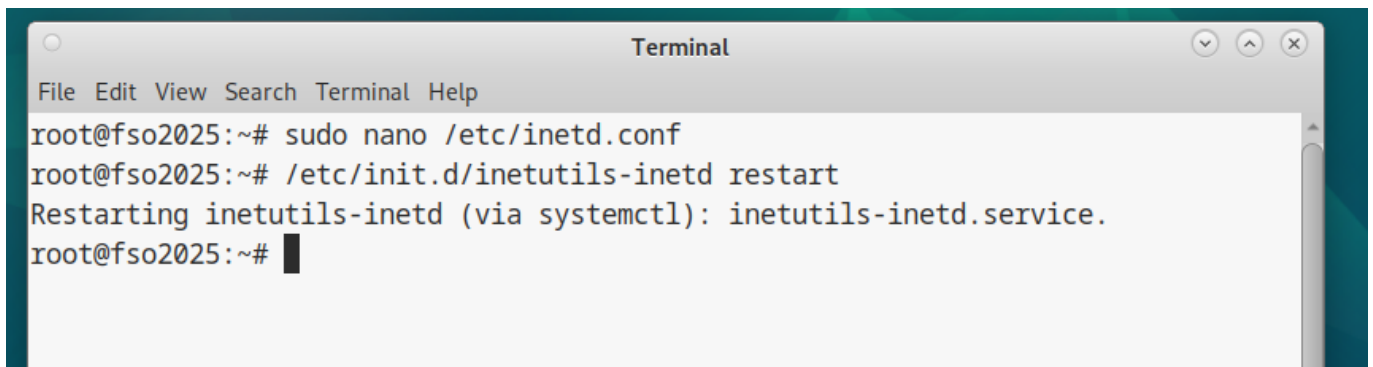
5. En MAQUINA1 habilita los servicios telnet añadiendo la siguiente línea a /etc/inetd.conf

```
telnet      stream    tcp nowait root /usr/sbin/tcpd  telnetd
```



```
Terminal
File Edit View Search Terminal Help
GNU nano 7.2 /etc/inetd.conf
#:INTERNAL: Internal services
#discard          stream  tcp6   nowait  root    internal
#discard          dgram  udp6   wait    root    internal
#daytime          stream  tcp6   nowait  root    internal
#time            stream  tcp6   nowait  root    internal
telnet           stream  tcp    nowait  root    /usr/sbin/tcpd  telnetd
#:STANDARD: These are standard services.
#<off># telnet    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/telne>
```

6. Reinicia inetd (/etc/init.d/inetutils-inetd restart, systemctl restart inetutils-inetd.service kill -HUP pid_de_inetd)



```
Terminal
File Edit View Search Terminal Help
root@fso2025:~# sudo nano /etc/inetd.conf
root@fso2025:~# /etc/init.d/inetutils-inetd restart
Restarting inetutils-inetd (via systemctl): inetutils-inetd.service.
root@fso2025:~#
```

7. Revisa la conexión telnet de MAQUINA2 a MAQUINA1

```
Terminal
File Edit View Search Terminal Help
root@fso2025:~# telnet 192.168.2.10
Trying 192.168.2.10...
Connected to 192.168.2.10.
Escape character is '^]'.

Linux 6.1.0-30-amd64 (fso2025.nowhere.org) (pts/1)

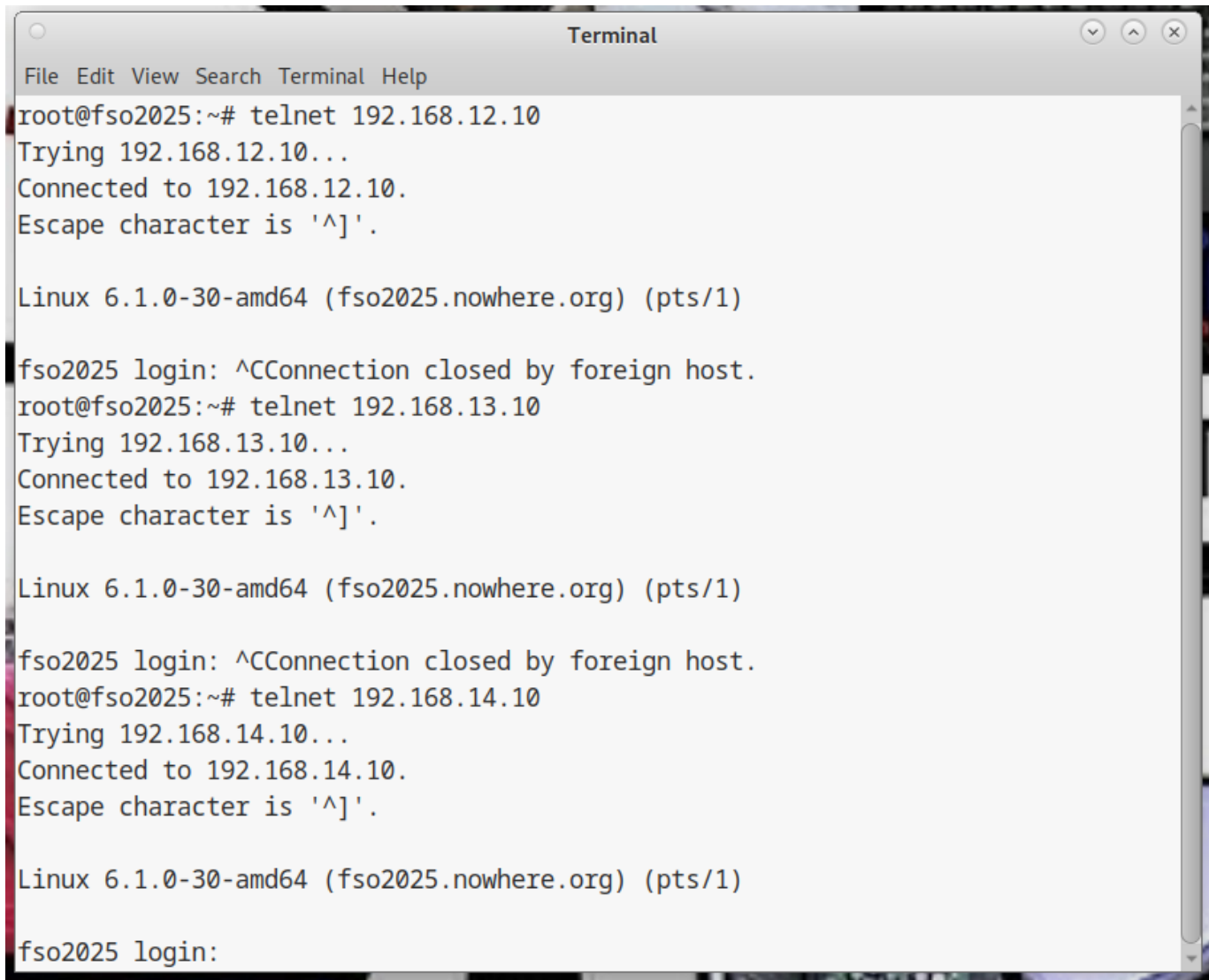
fso2025 login: ^CConnection closed by foreign host.
root@fso2025:~# telnet 192.168.3.10
Trying 192.168.3.10...
Connected to 192.168.3.10.
Escape character is '^]'.

Linux 6.1.0-30-amd64 (fso2025.nowhere.org) (pts/1)

fso2025 login: ^CConnection closed by foreign host.
root@fso2025:~# telnet 192.168.4.10
Trying 192.168.4.10...
Connected to 192.168.4.10.
Escape character is '^]'.

Linux 6.1.0-30-amd64 (fso2025.nowhere.org) (pts/1)

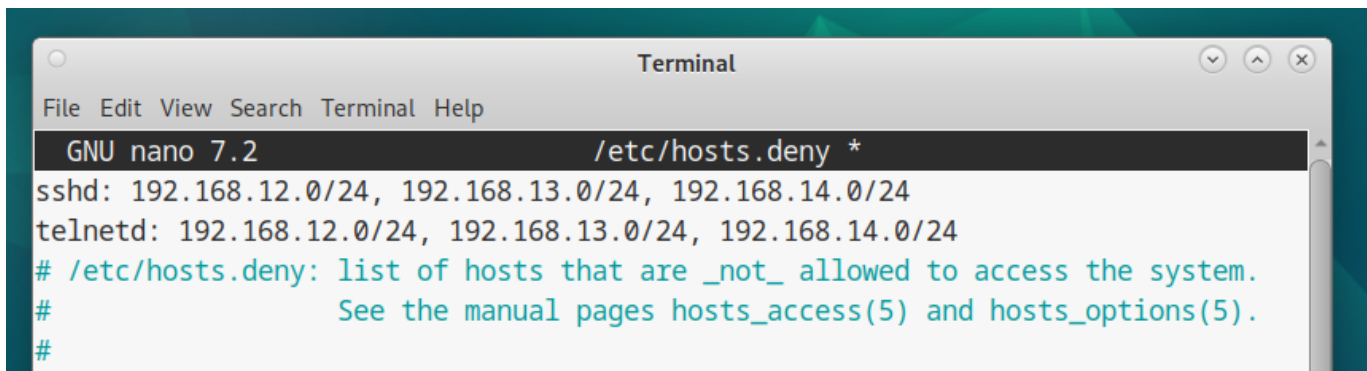
fso2025 login:
```

8. Configura tcpwrappers para rechazar todas las conexiones telnet desde 192.168.12.X, 192.168.13.X y 192.168.14.X

Configuramos /etc/hosts.deny con las siguientes líneas:

```
telnetd: 192.168.12.0/24, 192.168.12.0/24, 192.168.13.0/24
```



9. Revisa la comunicación telnet desde MAQUINA2 hasta MAQUINA1

From:

<https://knoppia.net/> - **Knoppia**

Permanent link:

https://knoppia.net/doku.php?id=master_cs:fortificacion:p5&rev=1741707049

Last update: **2025/03/11 15:30**

