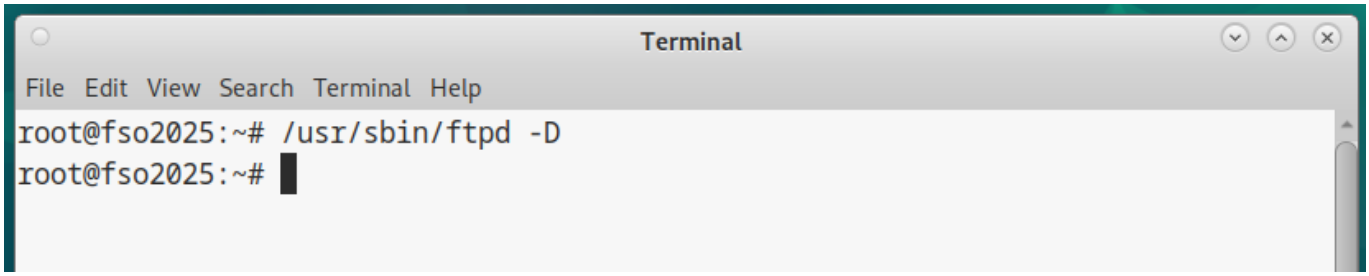
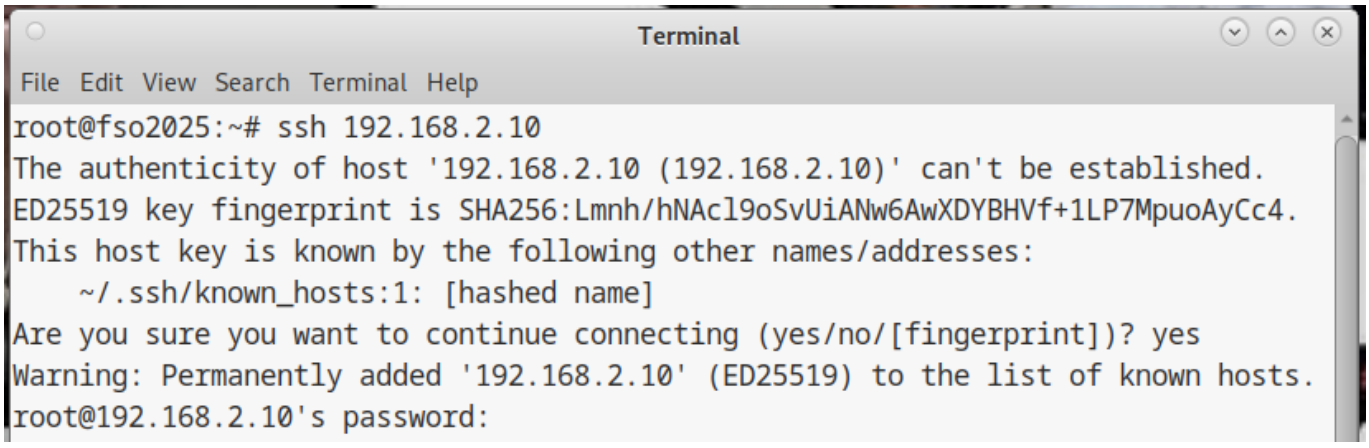
[FORT] Práctica 5: Control de Acceso a nivel de aplicación

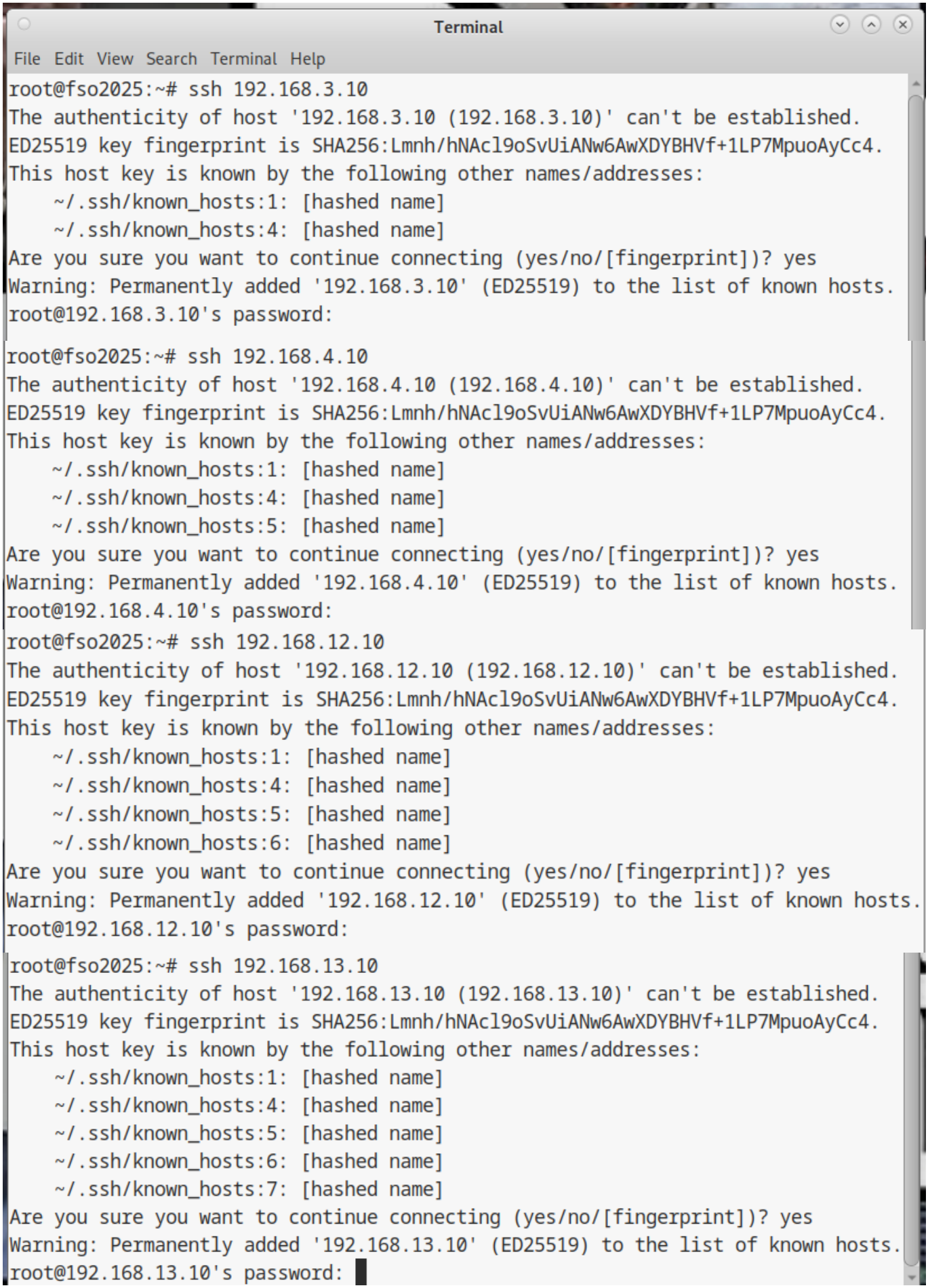
1. Habilita los servicios FTP en MAQUINA1 ejecutando /usr/sbin/ftp -D



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 192.168.3.10
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+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]
    ~/.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 rcpwrappers (/etc/hosts.allow y /etc/hosts.deny) en MAQUINA1 para:

Aceptar todas las conexiones ftp excepto las que vienen de

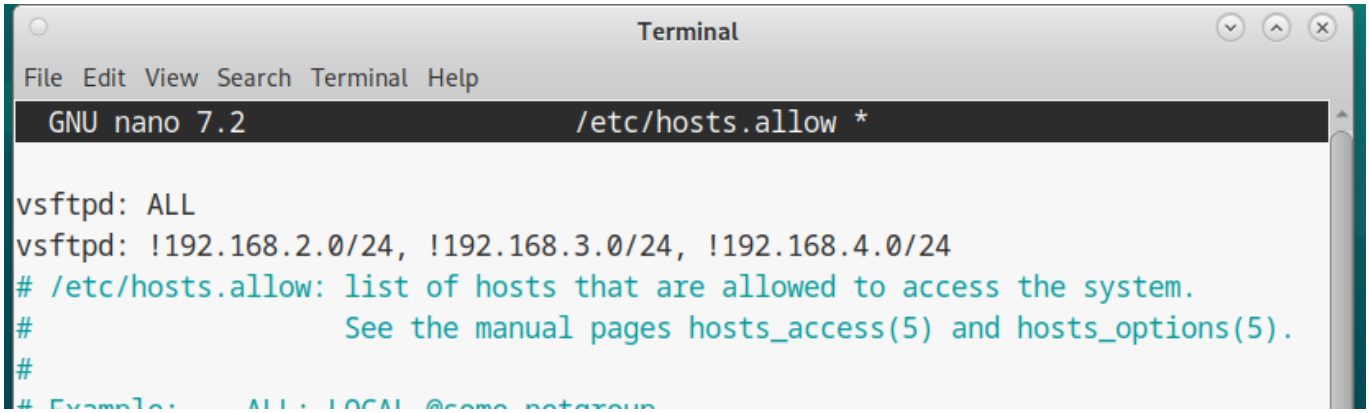
- 192.168.2.X
- 192.168.3.X
- 192.168.4.X

Rechazar todas las conexiones ssh que vienen de:

- 192.168.12.x
- 192,168.13.x
- 192.168.14.X

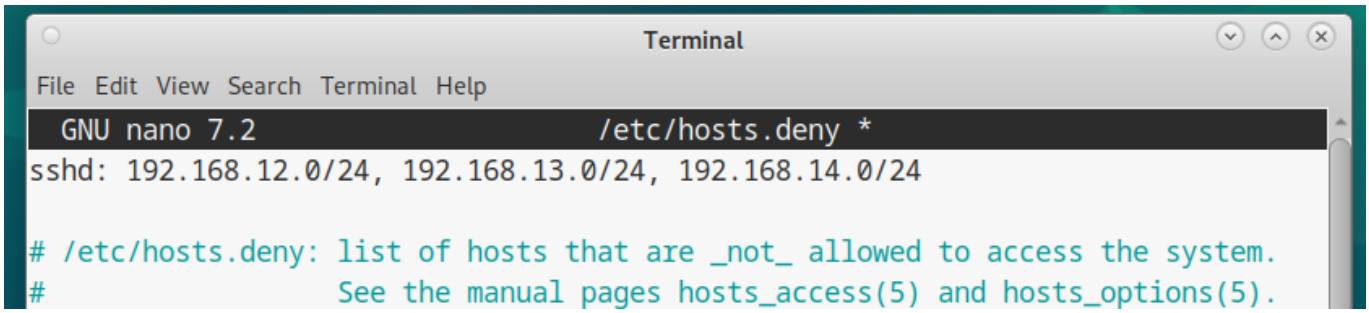
Comenzamos editando el archivo /etc/hosts.allow para aceptar todas las conexiones menos las indicadas con las siguientes líneas:

```
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
```



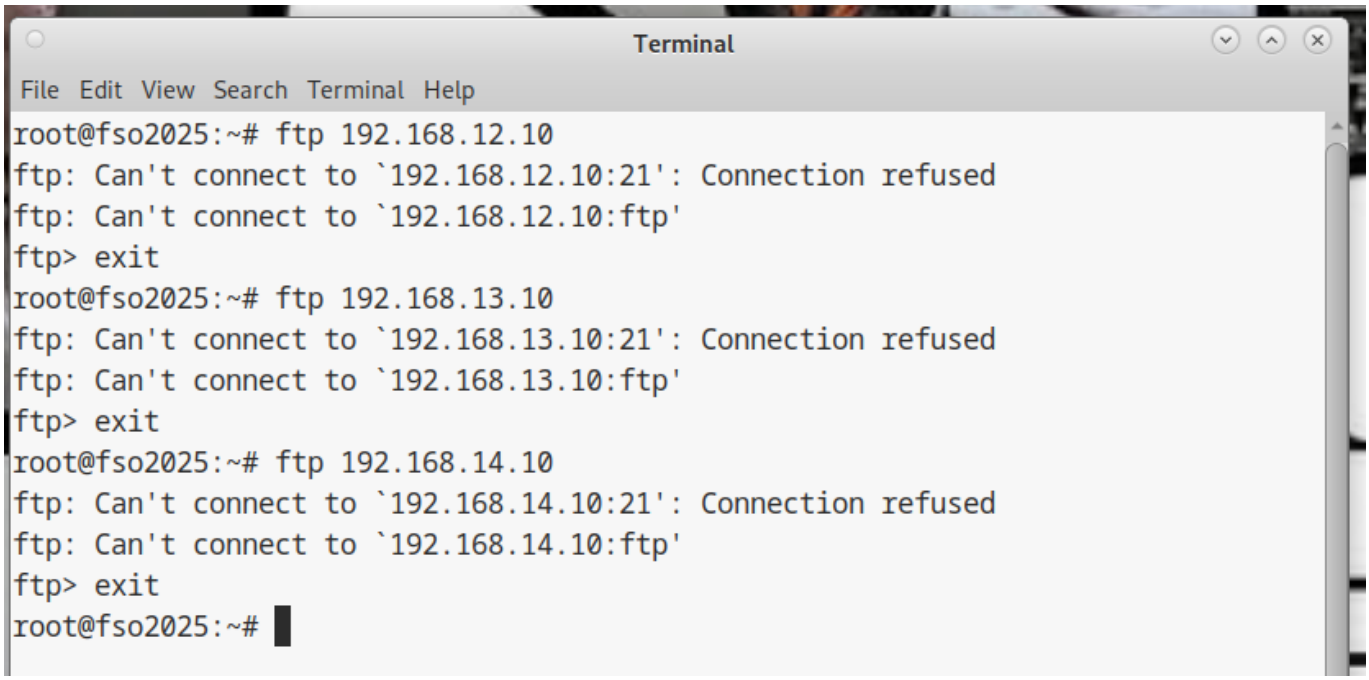
Tras eso procedemos a editar el archivo /etc/hosts.deny para bloquear las conexiones indicadas con las siguientes líneas:

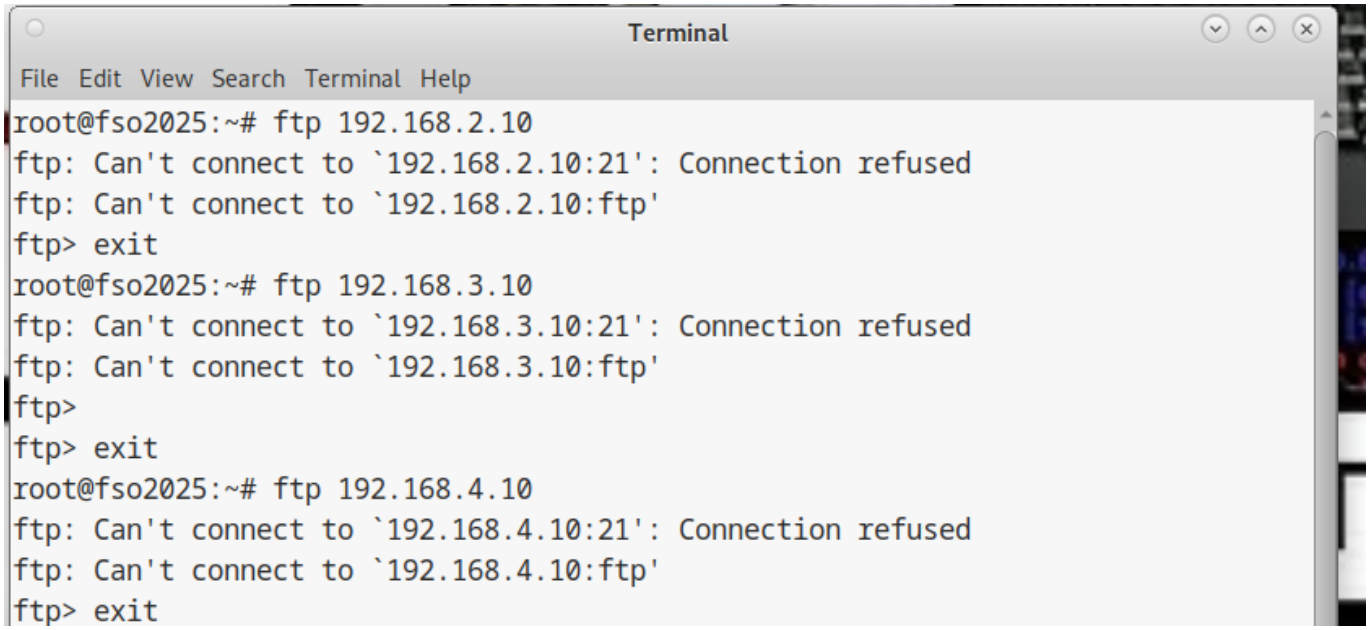
```
sshd: 192.168.12.0/24, 192.168.13.0/24, 192.168.14.0/24 #Se bloquea el SSH para las direcciones indicadas
```



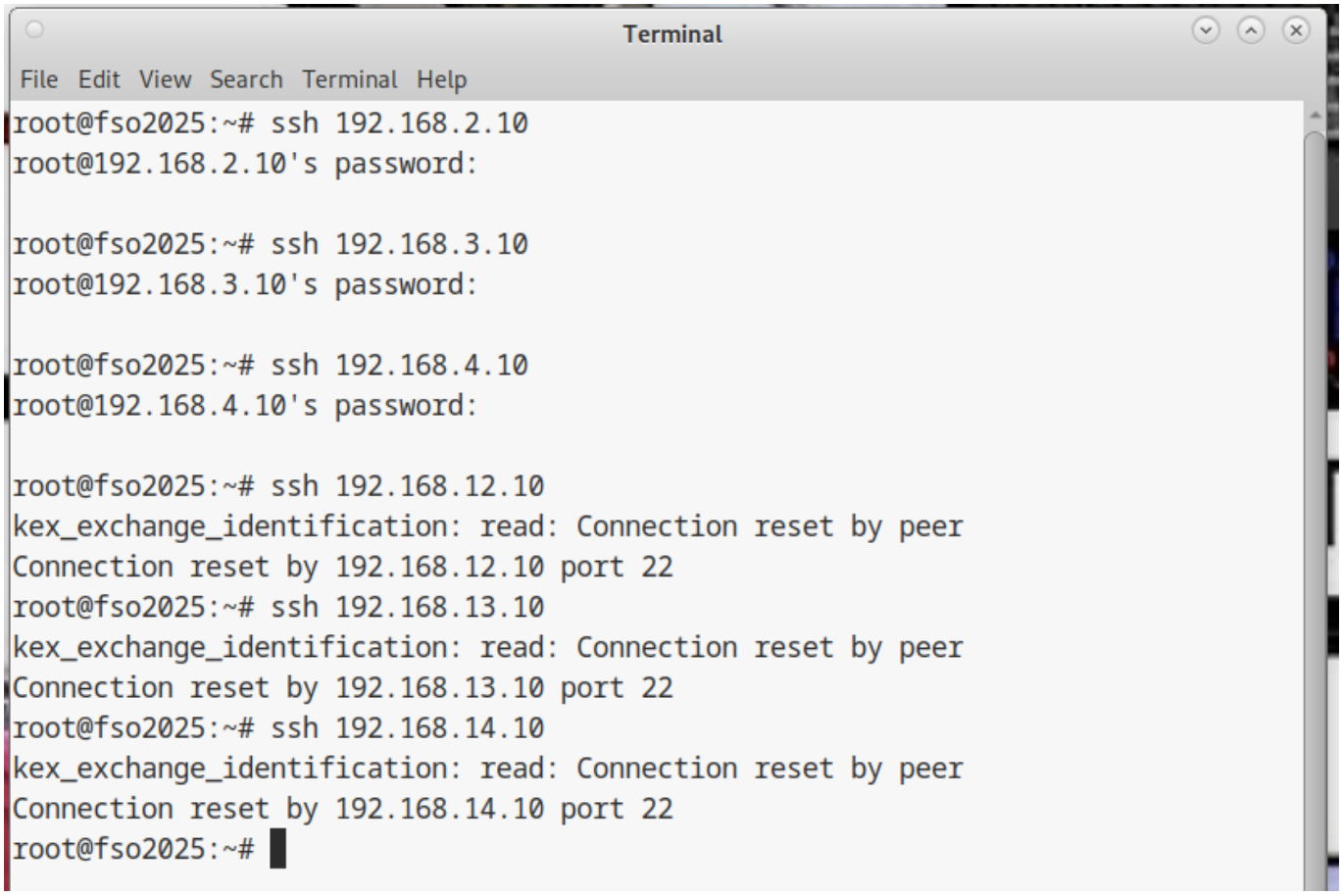
4. Revisa las conexiones ftp y ssh desde MAQUINA2 a MAQUINA1

Comenzamos revisando las conexiones FTP:



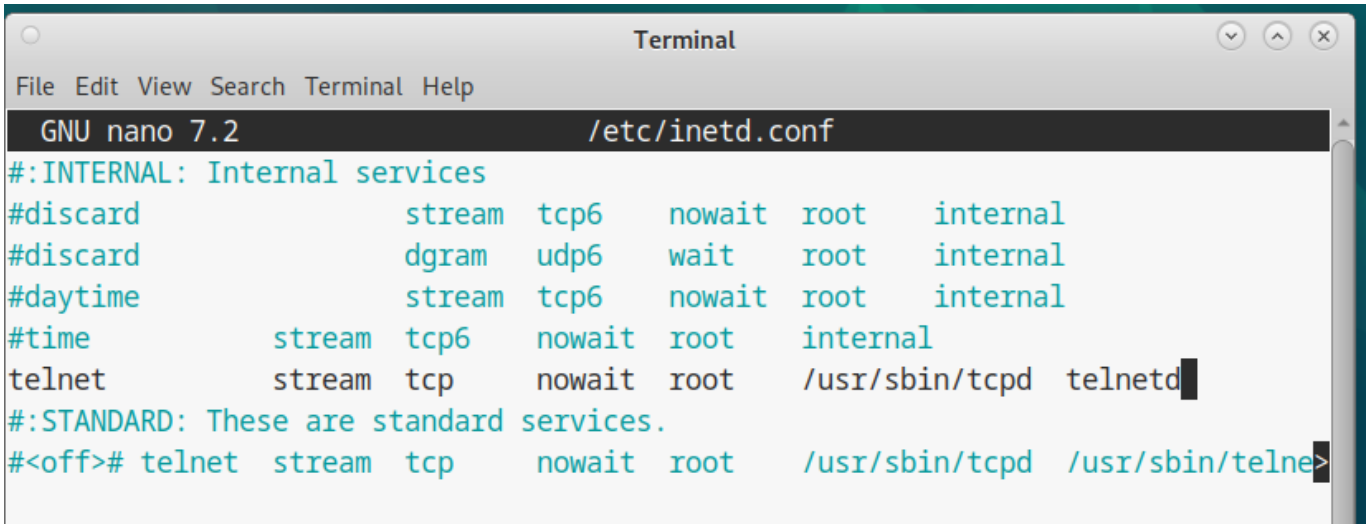


Tras eso revisamos las conexiones ssh:

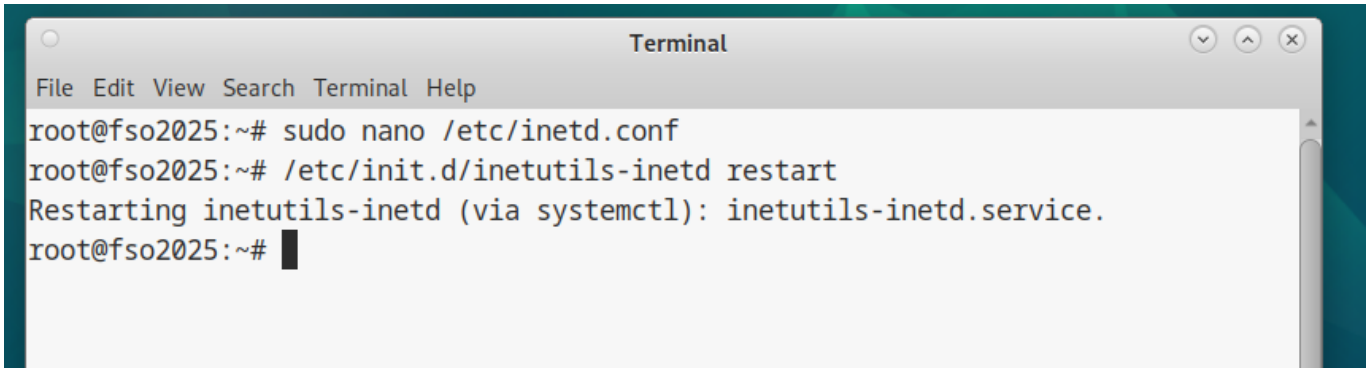


5. En MAQUINA1 habilita los servicios telnet añadiendo la siguiente línea a /etc/inetd.conf

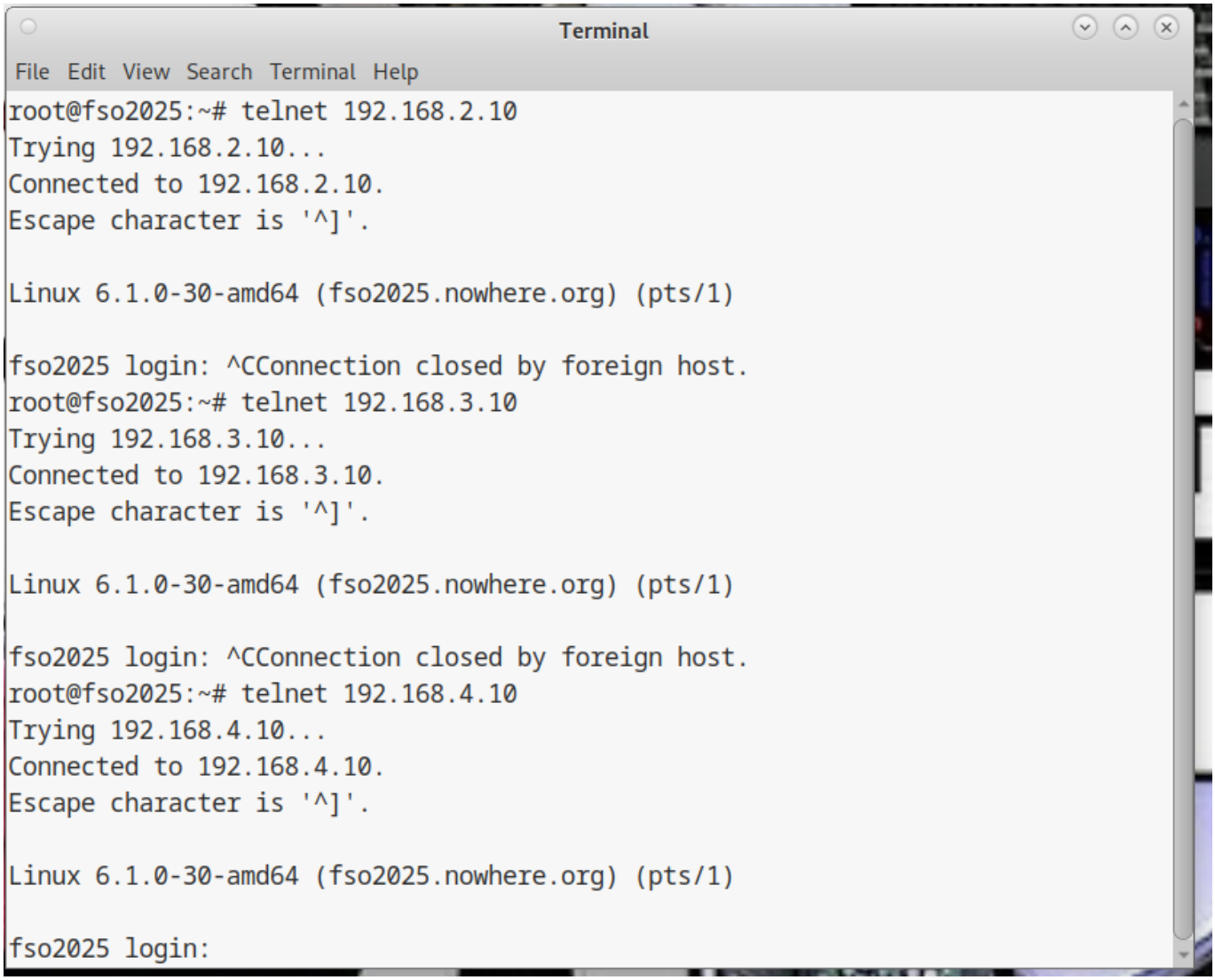
```
telnet      stream     tcp nowait root /usr/sbin/tcpd    telnetd
```

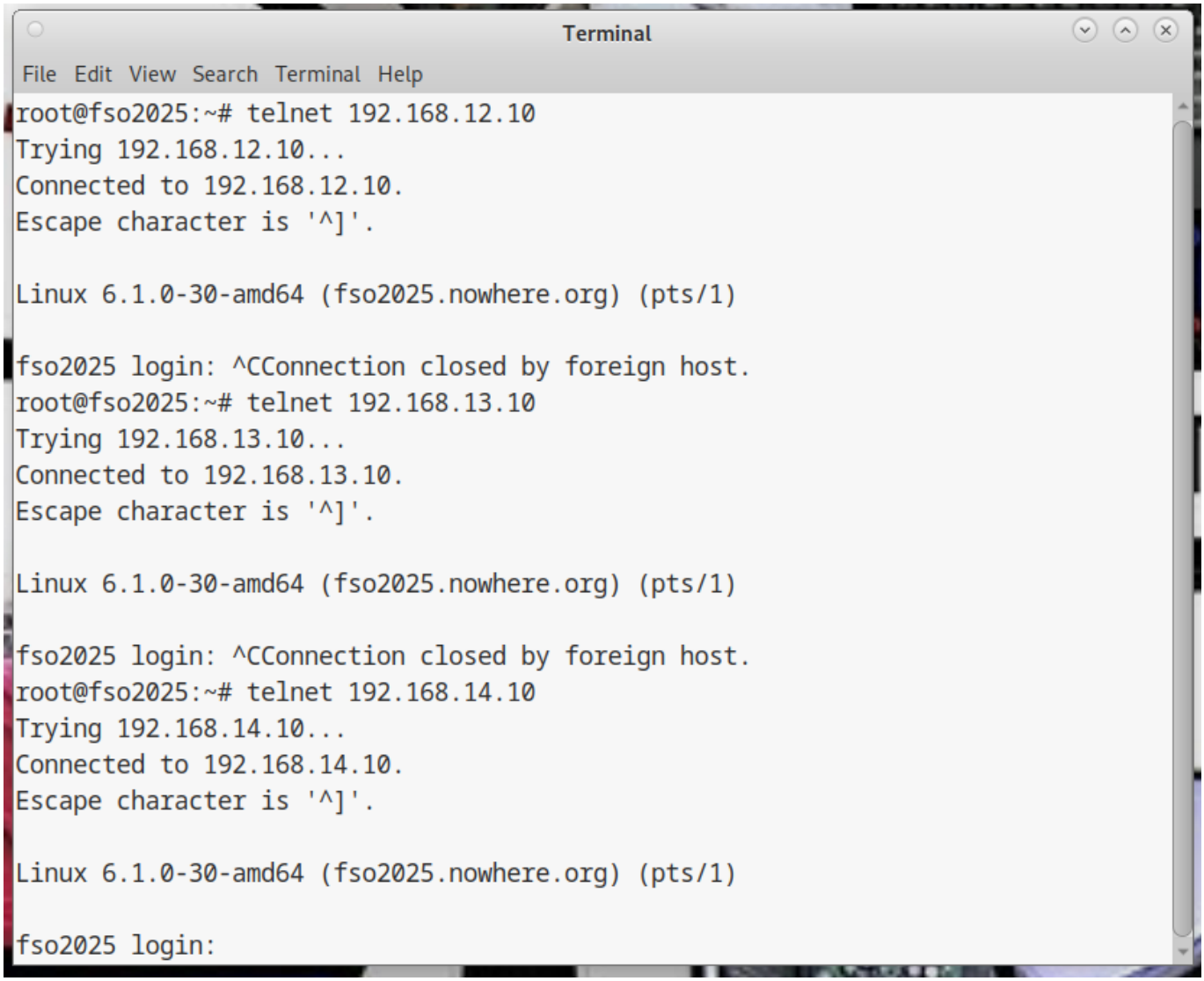


6. Reinicia inetd (/etc/init.d/inetutils-inetd restart, systemctl restart inetutils-inetd.service kill -HUP pid_de_inetd)



7. Revisa la conexión telnet de MAQUINA2 a MAQUINA1

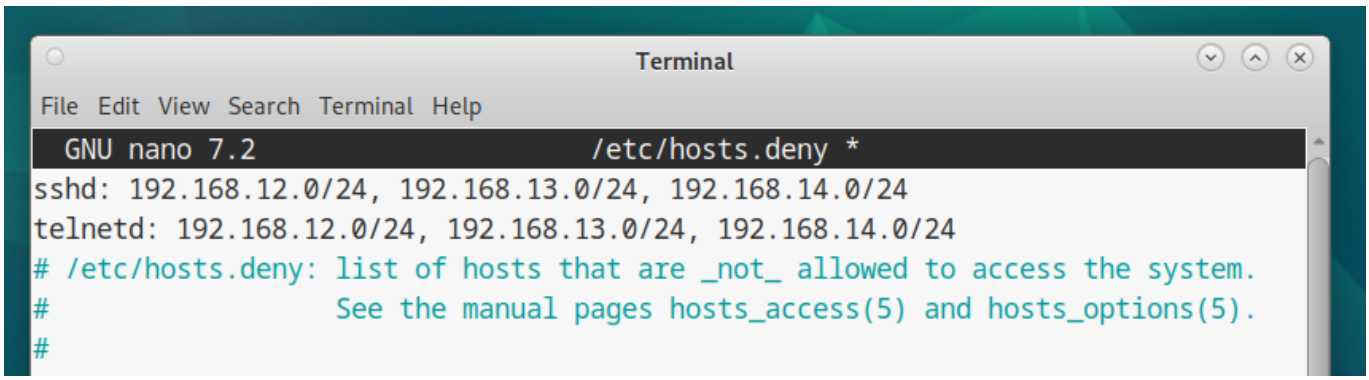

Terminal
File Edit View Search Terminal Help
root@fso2025:~# telnet 192.168.2.10
Trying 192.168.2.10...
Connected to 192.168.2.10.
Escape character is '^]'.
Linux 6.1.0-30-amd64 (fso2025.nowhere.org) (pts/1)
fso2025 login: ^CConnection closed by foreign host.
root@fso2025:~# telnet 192.168.3.10
Trying 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:



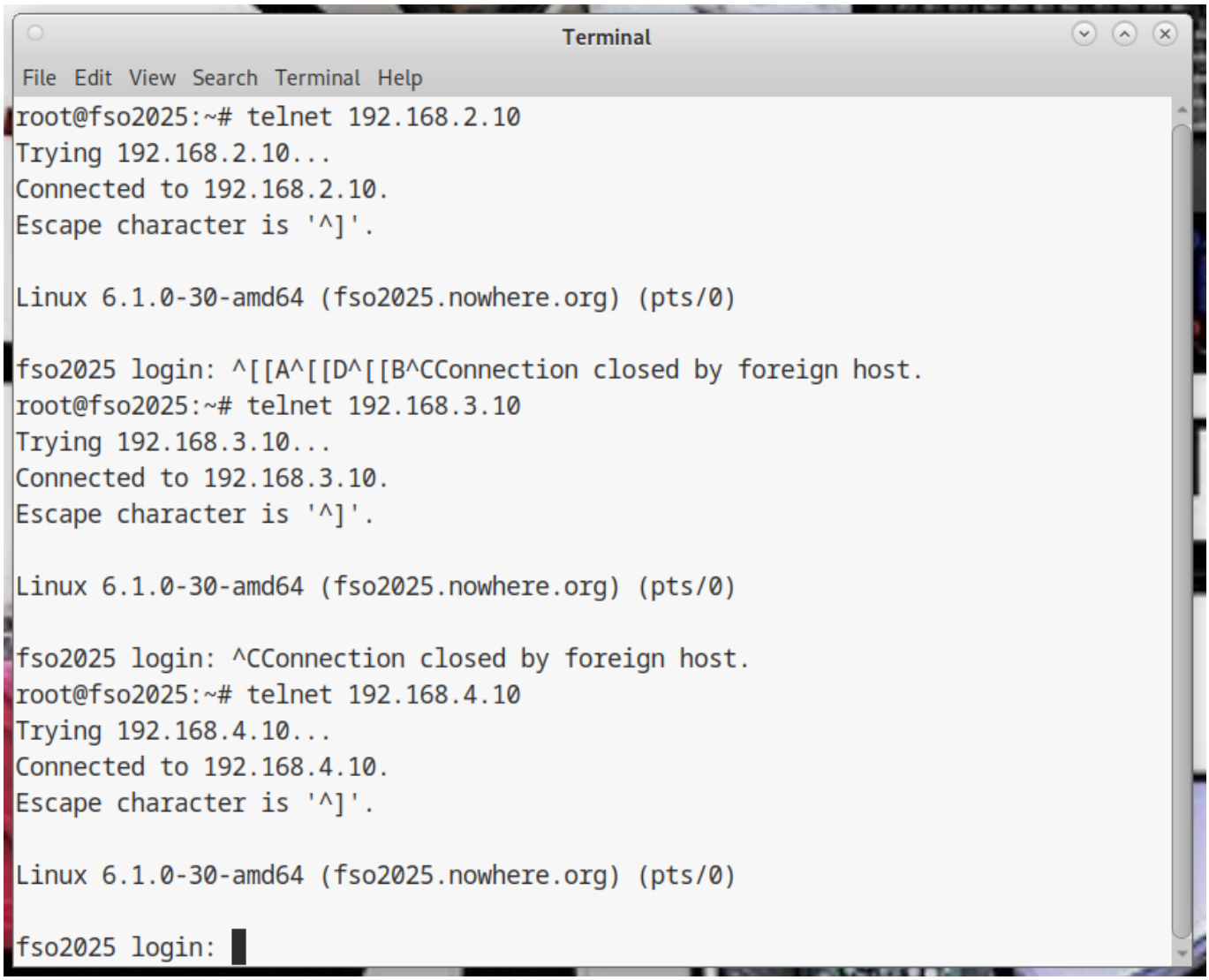
8. Configura tcpwrappers para rechazar todas las conexiones telnet desde 192.168.12.X, 192.168.13.X y 192.168.14.X

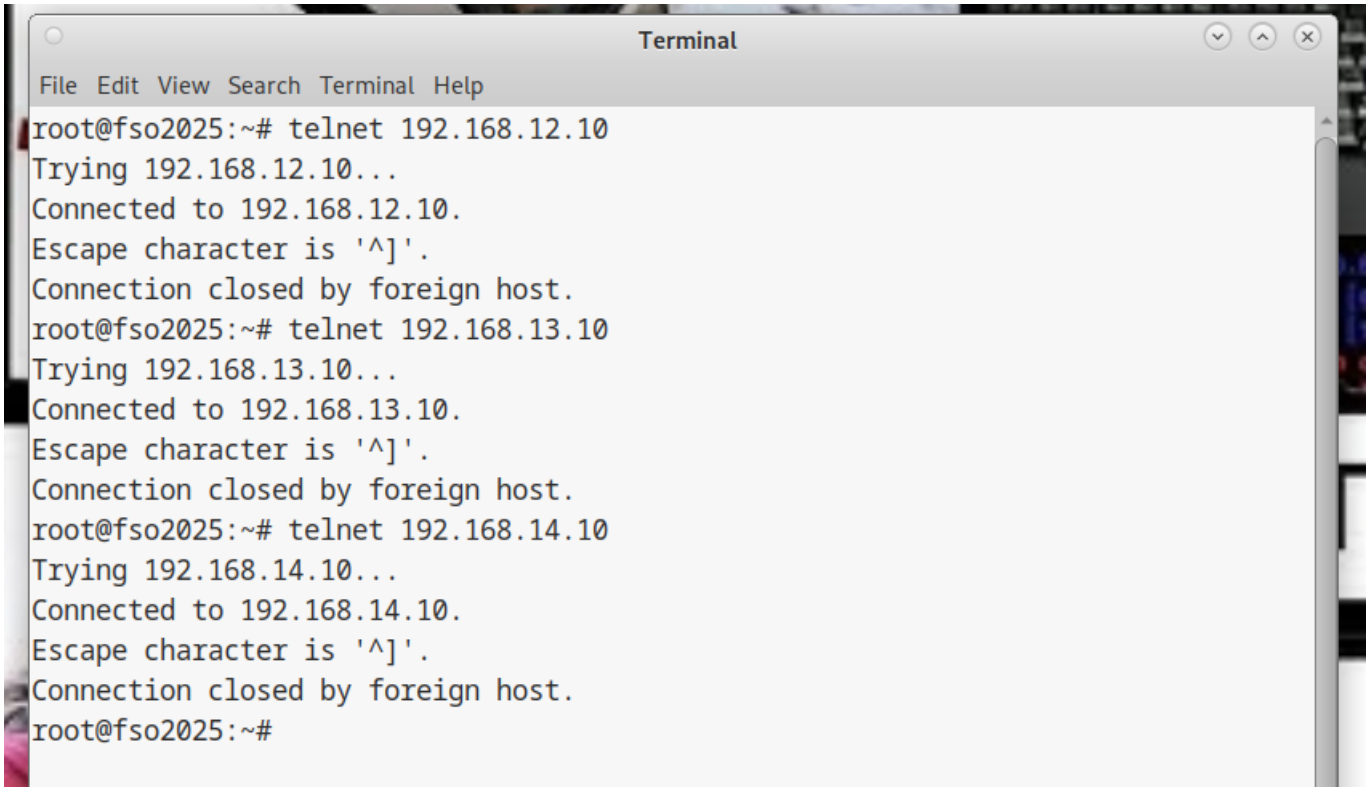
Configuramos /etc/hosts.deny con las siguientes líneas:

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



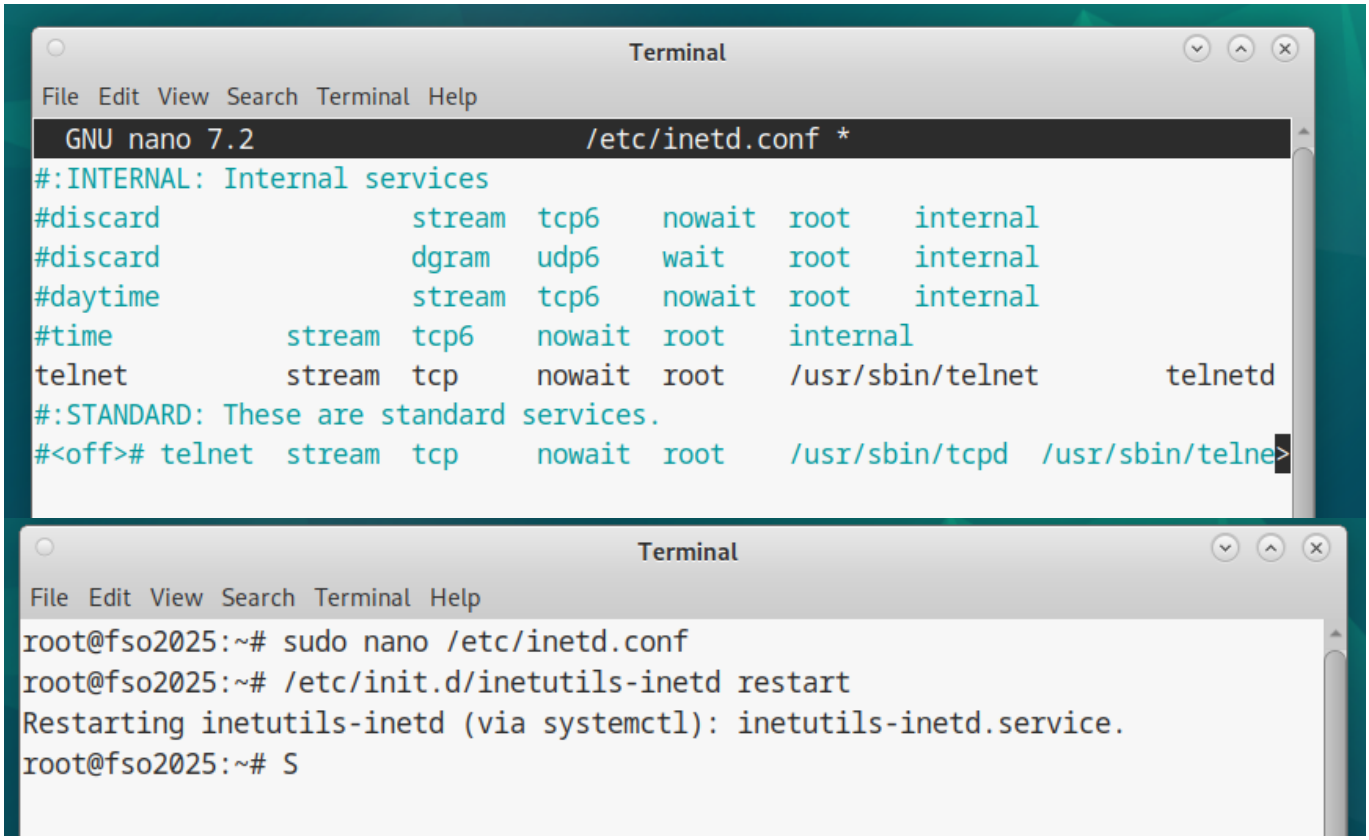
9. Revisa la comunicación telnet desde MAQUINA2 hasta MAQUINA1



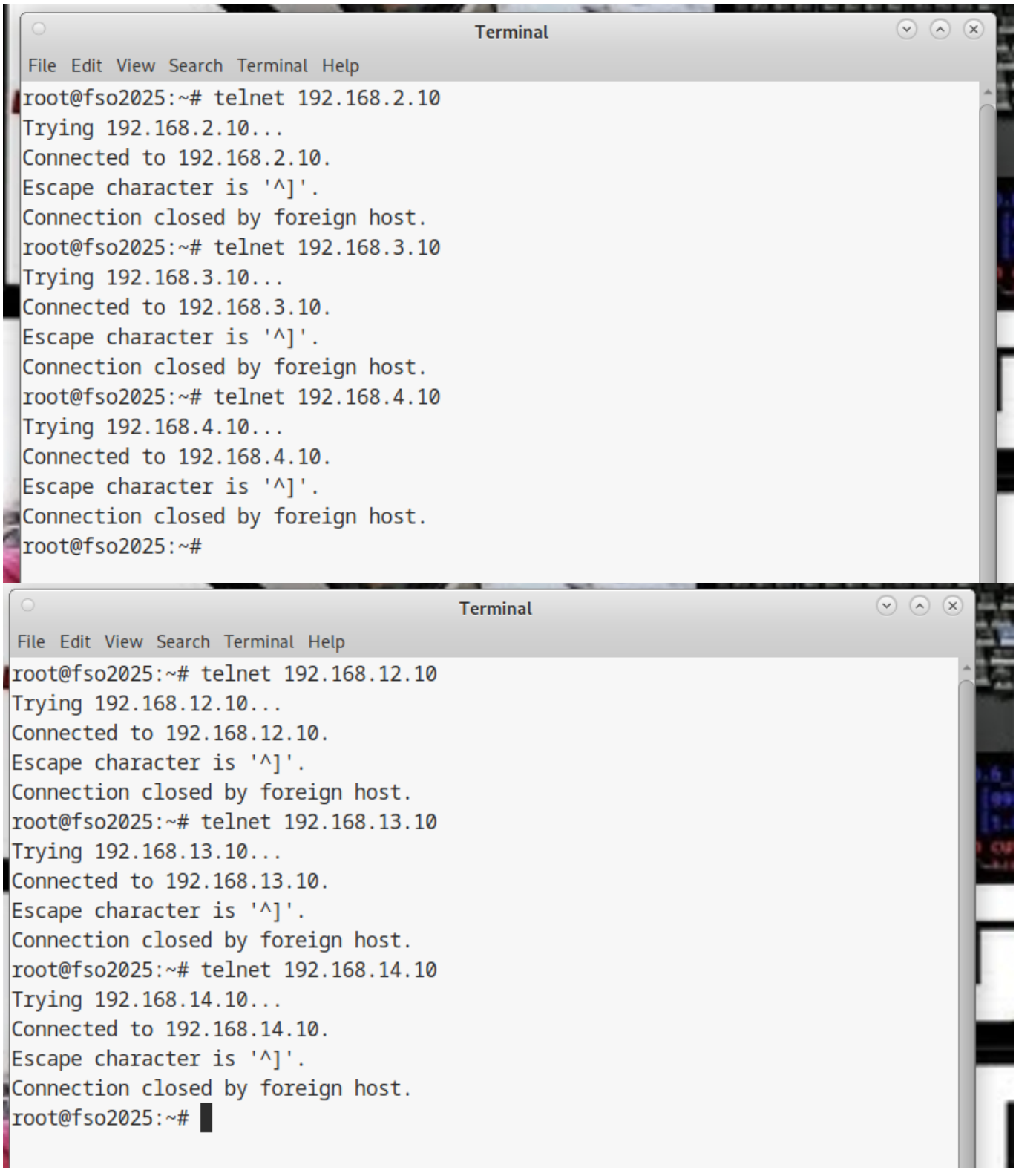


10. Sustituye la línea previa en /etc/inetd.conf con la siguiente y reinicia inetd

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



11. Revisa la conexión telnet de MAQUINA2 a MAQUINA1



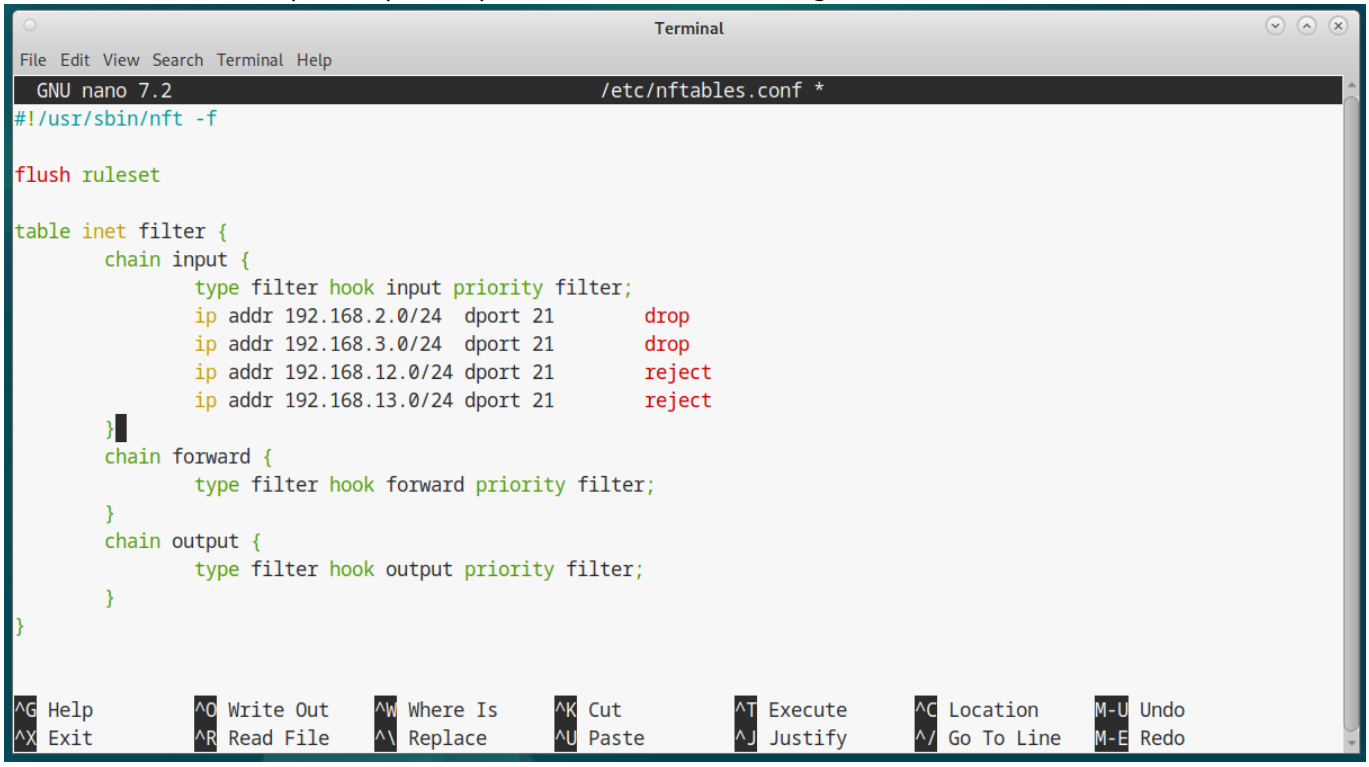
12. Mira que librerías usan sshd, ftpd, inetd, tcpd y telnetd

```
root@fso2025:~# ldd /bin/ssh
        linux-vdso.so.1 (0x00007ffe007ee000)
        libselinux.so.1 => /lib/x86_64-linux-gnu/libselinux.so.1 (0x00007f308e949000)
        libgssapi_krb5.so.2 => /lib/x86_64-linux-gnu/libgssapi_krb5.so.2 (0x00007f308e8f6000)
        libcrypto.so.3 => /lib/x86_64-linux-gnu/libcrypto.so.3 (0x00007f308e400000)
        libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007f308e8d7000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f308e21f000)
        libpcre2-8.so.0 => /lib/x86_64-linux-gnu/libpcre2-8.so.0 (0x00007f308e185000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f308eaa0000)
        libkrb5.so.3 => /lib/x86_64-linux-gnu/libkrb5.so.3 (0x00007f308e0ab000)
        libk5crypto.so.3 => /lib/x86_64-linux-gnu/libk5crypto.so.3 (0x00007f308e8a8000)
        libcom_err.so.2 => /lib/x86_64-linux-gnu/libcom_err.so.2 (0x00007f308e8a2000)
        libkrb5support.so.0 => /lib/x86_64-linux-gnu/libkrb5support.so.0 (0x00007f308e894000)
        libkeyutils.so.1 => /lib/x86_64-linux-gnu/libkeyutils.so.1 (0x00007f308e88b000)
        libresolv.so.2 => /lib/x86_64-linux-gnu/libresolv.so.2 (0x00007f308e09a000)
root@fso2025:~#
root@fso2025:~# ldd /bin/ftp
        linux-vdso.so.1 (0x00007fffeedd1000)
        libedit.so.2 => /lib/x86_64-linux-gnu/libedit.so.2 (0x00007f8787879000)
        libssl.so.3 => /lib/x86_64-linux-gnu/libssl.so.3 (0x00007f87877d0000)
        libcrypto.so.3 => /lib/x86_64-linux-gnu/libcrypto.so.3 (0x00007f8787200000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f878701f000)
        libtinfo.so.6 => /lib/x86_64-linux-gnu/libtinfo.so.6 (0x00007f878779d000)
        libbsd.so.0 => /lib/x86_64-linux-gnu/libbsd.so.0 (0x00007f8787785000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f8787912000)
        libmd.so.0 => /lib/x86_64-linux-gnu/libmd.so.0 (0x00007f8787778000)
root@fso2025:~# ldd /bin/inetutils-telnet
        linux-vdso.so.1 (0x00007ffca6dea000)
        libtinfo.so.6 => /lib/x86_64-linux-gnu/libtinfo.so.6 (0x00007f5e9bdb6000)
        libkrb5.so.3 => /lib/x86_64-linux-gnu/libkrb5.so.3 (0x00007f5e9bcdc000)
        libk5crypto.so.3 => /lib/x86_64-linux-gnu/libk5crypto.so.3 (0x00007f5e9bcaf000)
        libcom_err.so.2 => /lib/x86_64-linux-gnu/libcom_err.so.2 (0x00007f5e9bca9000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f5e9bac8000)
        libkrb5support.so.0 => /lib/x86_64-linux-gnu/libkrb5support.so.0 (0x00007f5e9bab8000)
        libkeyutils.so.1 => /lib/x86_64-linux-gnu/libkeyutils.so.1 (0x00007f5e9bab1000)
        libresolv.so.2 => /lib/x86_64-linux-gnu/libresolv.so.2 (0x00007f5e9baa0000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f5e9be37000)
root@fso2025:~# ldd /bin/telnet
        linux-vdso.so.1 (0x00007fffe26fc000)
        libtinfo.so.6 => /lib/x86_64-linux-gnu/libtinfo.so.6 (0x00007ff77a0ef000)
        libkrb5.so.3 => /lib/x86_64-linux-gnu/libkrb5.so.3 (0x00007ff77a015000)
        libk5crypto.so.3 => /lib/x86_64-linux-gnu/libk5crypto.so.3 (0x00007ff779fe8000)
        libcom_err.so.2 => /lib/x86_64-linux-gnu/libcom_err.so.2 (0x00007ff779fe2000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007ff779e01000)
        libkrb5support.so.0 => /lib/x86_64-linux-gnu/libkrb5support.so.0 (0x00007ff779df1000)
        libkeyutils.so.1 => /lib/x86_64-linux-gnu/libkeyutils.so.1 (0x00007ff779dea000)
        libresolv.so.2 => /lib/x86_64-linux-gnu/libresolv.so.2 (0x00007ff779dd9000)
        /lib64/ld-linux-x86-64.so.2 (0x00007ff77a170000)
```

13. (MAQUINA1) Para el protocolo ftp (puerto 21) usa nftables para establecer la acción DROP para las conexiones en las redes 192.168.2.X, 192.168.3.X y REJECT para

192.168.12.X y 192.168.13.X

Normalmente esto se configuraría en /etc/nftables.conf, pero en este caso revisando /etc/inid.d se puede observar que las nftables están siendo gestionadas por lxc-net debido a que estamos usando containers en las máquinas. por lo que en este caso las configuraciones no van a funcionar`.



14. (MAQUINA1) Para el protocolo ssh (puerto 22) usa nftables para hacer un DROP para las conexiones en 192.168.12.x y 192.168.13.x y para hacer reject para las redes 192.168.2.x y 192.168.3.x