

Firewall iptables

26/10/2023

Guillermo Bellettini

Seguridad

Creado por: Nicolas Pavel Ballesteros Barrado



Contenido

- Firewall iptables 1
 - Instalamos el software proftpd 3
 - Activamos el servicio 3
 - Instalamos sevicio ssh 4
 - Vemos el estado del servicio 4
 - Instalamos el servicio telnet 5
 - Vemos el servicio HTTP 6
 - Vemos la lista 6
 - Accedemos a los servicios 7
 - Conexión FTP 7
 - Conexión Telnet 8
 - Conexión SSH 9
 - Bloqueamos los servicios 10
 - Bloqueamos Telnet 10
 - Bloqueamos ssh 11
 - Bloqueamos HTTP 12
 - Bloqueamos ftp 13

Instalamos el software proftpd

```
[root@localhost ~]# dnf install proftpd
Última comprobación de caducidad de metadatos hecha hace 3:16:33, el lun 23 oct 2023 16:00:09.
El paquete proftpd-1.3.8a-1.fc38.x86_64 ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[root@localhost ~]#
```

Activamos el servicio

```
[root@localhost ~]# systemctl status proftpd
● proftpd.service - ProFTPD FTP Server
   Loaded: loaded (/usr/lib/systemd/system/proftpd.service; disabled; preset: disabled)
   Drop-In: /usr/lib/systemd/system/service.d
            └─10-timeout-abort.conf
   Active: active (running) since Mon 2023-10-23 19:18:34 CEST; 13s ago
   Process: 3002 ExecStartPre=/usr/sbin/proftpd --configtest (code=exited, status=0/SUCCESS)
  Main PID: 3003 (proftpd)
    Tasks: 1 (limit: 2293)
   Memory: 3.5M
      CPU: 77ms
   CGroup: /system.slice/proftpd.service
           └─3003 "proftpd: (accepting connections)"

oct 23 19:18:33 localhost.localdomain systemd[1]: Starting proftpd.service - ProFTPD FTP Server...
oct 23 19:18:33 localhost.localdomain proftpd[3002]: Checking syntax of configuration file
oct 23 19:18:33 localhost.localdomain proftpd[3002]: 2023-10-23 19:18:33,929 localhost.localdomain proftpd[3002]: mod_tl
oct 23 19:18:34 localhost.localdomain systemd[1]: Started proftpd.service - ProFTPD FTP Server.
oct 23 19:18:34 localhost.localdomain proftpd[3003]: 2023-10-23 19:18:34,038 localhost.localdomain proftpd[3003]: mod_tl
oct 23 19:18:34 localhost.localdomain proftpd[3003]: daemon[3003] 127.0.0.1: ProFTPD 1.3.8a (maint) (built Mon Oct 9 202
lines 1-19/19 (END)
```

```
[root@localhost ~]# systemctl enable proftpd
Created symlink /etc/systemd/system/multi-user.target.wants/proftpd.service → /usr/lib/systemd/system/proftpd.service.
[root@localhost ~]# systemctl status proftpd
● proftpd.service - ProFTPD FTP Server
   Loaded: loaded (/usr/lib/systemd/system/proftpd.service; enabled; preset: disabled)
   Drop-In: /usr/lib/systemd/system/service.d
            └─10-timeout-abort.conf
   Active: active (running) since Mon 2023-10-23 19:18:34 CEST; 52s ago
  Main PID: 3003 (proftpd)
    Tasks: 1 (limit: 2293)
   Memory: 3.5M
      CPU: 79ms
   CGroup: /system.slice/proftpd.service
           └─3003 "proftpd: (accepting connections)"

oct 23 19:18:33 localhost.localdomain systemd[1]: Starting proftpd.service - ProFTPD FTP Server...
oct 23 19:18:33 localhost.localdomain proftpd[3002]: Checking syntax of configuration file
oct 23 19:18:33 localhost.localdomain proftpd[3002]: 2023-10-23 19:18:33,929 localhost.localdomain proftpd[3002]: mod_tl
oct 23 19:18:34 localhost.localdomain systemd[1]: Started proftpd.service - ProFTPD FTP Server.
oct 23 19:18:34 localhost.localdomain proftpd[3003]: 2023-10-23 19:18:34,038 localhost.localdomain proftpd[3003]: mod_tl
oct 23 19:18:34 localhost.localdomain proftpd[3003]: daemon[3003] 127.0.0.1: ProFTPD 1.3.8a (maint) (built Mon Oct 9 202
lines 1-18/18 (END)
```

Instalamos servicio ssh

```
[root@localhost ~]# dnf install openssh-server
Última comprobación de caducidad de metadatos hecha hace 3:23:24, el lun 23 oct 2023 16:00:09.
El paquete openssh-server-9.0p1-14.fc38.1.x86_64 ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[root@localhost ~]# _
```

Vemos el estado del servicio

```
[root@localhost ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Drop-In: /usr/lib/systemd/system/service.d
            └─10-timeout-abort.conf
   Active: active (running) since Mon 2023-10-23 16:03:35 CEST; 3h 20min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 774 (sshd)
    Tasks: 1 (limit: 2293)
   Memory: 2.2M
      CPU: 87ms
   CGroup: /system.slice/sshd.service
           └─774 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

oct 23 16:03:35 localhost systemd[1]: Starting sshd.service - OpenSSH server daemon...
oct 23 16:03:35 localhost sshd[774]: Server listening on 0.0.0.0 port 22.
oct 23 16:03:35 localhost sshd[774]: Server listening on :: port 22.
oct 23 16:03:35 localhost systemd[1]: Started sshd.service - OpenSSH server daemon.
oct 23 18:10:35 localhost.localdomain sshd[17221]: error: kex_exchange_identification: read: Connection reset by peer
oct 23 18:10:35 localhost.localdomain sshd[17221]: Connection reset by 10.68.17.221 port 53425
[root@localhost ~]#
```

Instalamos el servicio telnet

```
[root@localhost ~]# dnf install telnet-server
Última comprobación de caducidad de metadatos hecha hace 3:27:24, el lun 23 oct 2023 16:00:09.
Dependencias resueltas.
```

Paquete	Arquitectura	Versión
Instalando: telnet-server	x86_64	1:0.17-88.fc38

Resumen de la transacción

Instalar 1 Paquete

Tamaño total de la descarga: 37 k

Tamaño instalado: 58 k

¿Está de acuerdo [s/N]? s

Descargando paquetes:

telnet-server-0.17-88.fc38.x86_64.rpm

Total

Ejecutando verificación de operación

Verificación de operación exitosa.

Ejecutando prueba de operaciones

Prueba de operación exitosa.

Ejecutando operación

Preparando :

Instalando : telnet-server-1:0.17-88.fc38.x86_64

Ejecutando scriptlet: telnet-server-1:0.17-88.fc38.x86_64

Habilitamos el servicio

```
[root@localhost ~]# systemctl start telnet.socket
```

```
[root@localhost ~]# systemctl enable telnet.socket
```

```
Created symlink /etc/systemd/system/sockets.target.wants/telnet.socket → /usr/lib/systemd/system/telnet.socket.
```

```
[root@localhost ~]# systemctl status telnet.socket
```

```
● telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; enabled; preset: disabled)
   Active: active (listening) since Mon 2023-10-23 19:30:05 CEST; 54s ago
     Docs: man:telnetd(8)
    Listen: [::]:23 (Stream)
  Accepted: 0; Connected: 0;
    Tasks: 0 (limit: 2293)
   Memory: 8.0K
      CPU: 1ms
   CGroup: /system.slice/telnet.socket
```

```
oct 23 19:30:05 localhost.localdomain systemd[1]: Listening on telnet.socket - Telnet Server Activation Socket.
```

```
[root@localhost ~]#
```

Vemos el servicio HTTP

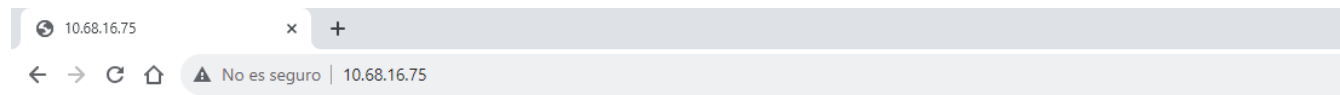
```
[root@localhost ~]# systemctl start httpd
[root@localhost ~]# systemctl enable httpd
[root@localhost ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Drop-In: /usr/lib/systemd/system/service.d
            └─10-timeout-abort.conf
   Active: active (running) since Mon 2023-10-23 18:27:51 CEST; 1h 7min ago
     Docs: man:httpd.service(8)
  Main PID: 2269 (httpd)
   Status: "Total requests: 53; Idle/Busy workers 100/0; Requests/sec: 0.0131; Bytes served/sec: 29 B/sec"
    Tasks: 230 (limit: 2293)
   Memory: 18.3M
      CPU: 6.674s
   CGroup: /system.slice/httpd.service
           └─2269 /usr/sbin/httpd -DFOREGROUND
             └─2272 /usr/sbin/httpd -DFOREGROUND
               └─2273 /usr/sbin/httpd -DFOREGROUND
                 └─2274 /usr/sbin/httpd -DFOREGROUND
                   └─2275 /usr/sbin/httpd -DFOREGROUND
                     └─2451 /usr/sbin/httpd -DFOREGROUND

oct 23 18:27:51 localhost.localdomain systemd[1]: Starting httpd.service - The Apache HTTP Server...
oct 23 18:27:51 localhost.localdomain httpd[2269]: AH00558: httpd: Could not reliably determine the server's fully quali
oct 23 18:27:51 localhost.localdomain httpd[2269]: Server configured, listening on: port 80
oct 23 18:27:51 localhost.localdomain systemd[1]: Started httpd.service - The Apache HTTP Server.
lines 1-23/23 (END)
```

Vemos la lista

```
oct 23 18:27:51 localhost.localdomain systemd[1]: Failed to s
[root@localhost ~]# firewall-cmd --list-all
FedoraServer (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ftp http ntp ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@localhost ~]#
```

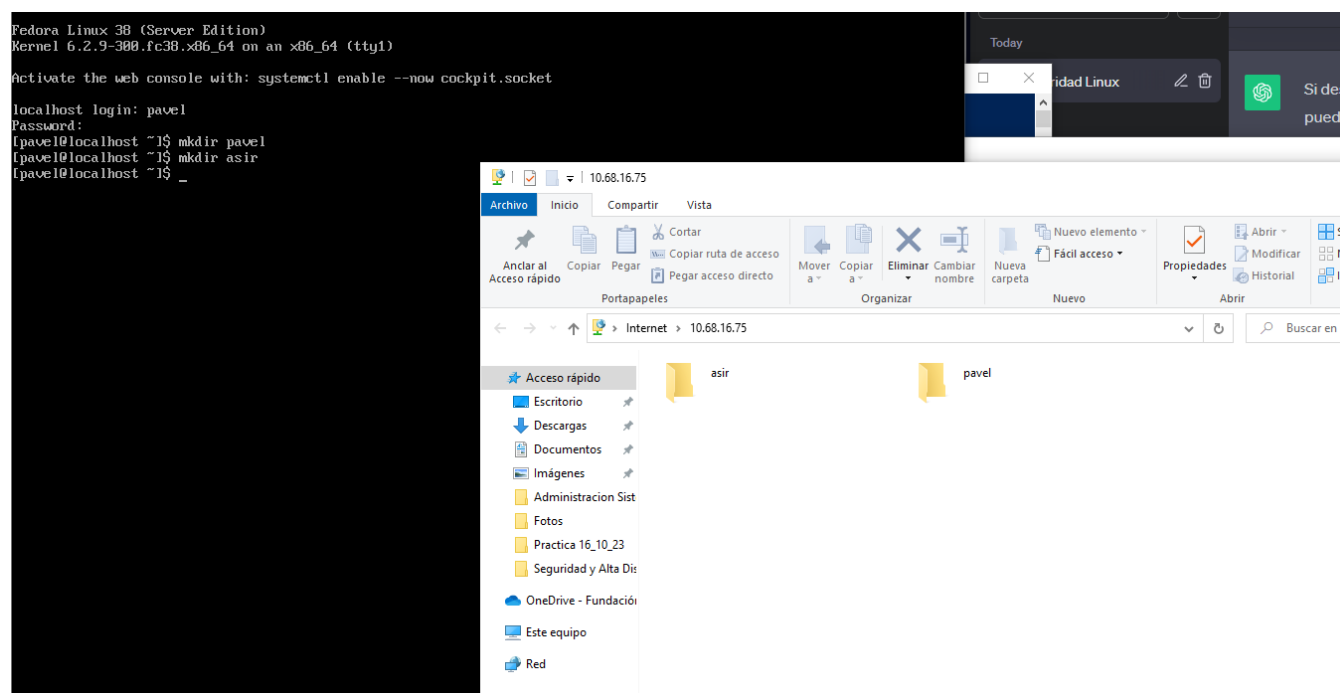
Accedemos a los servicios



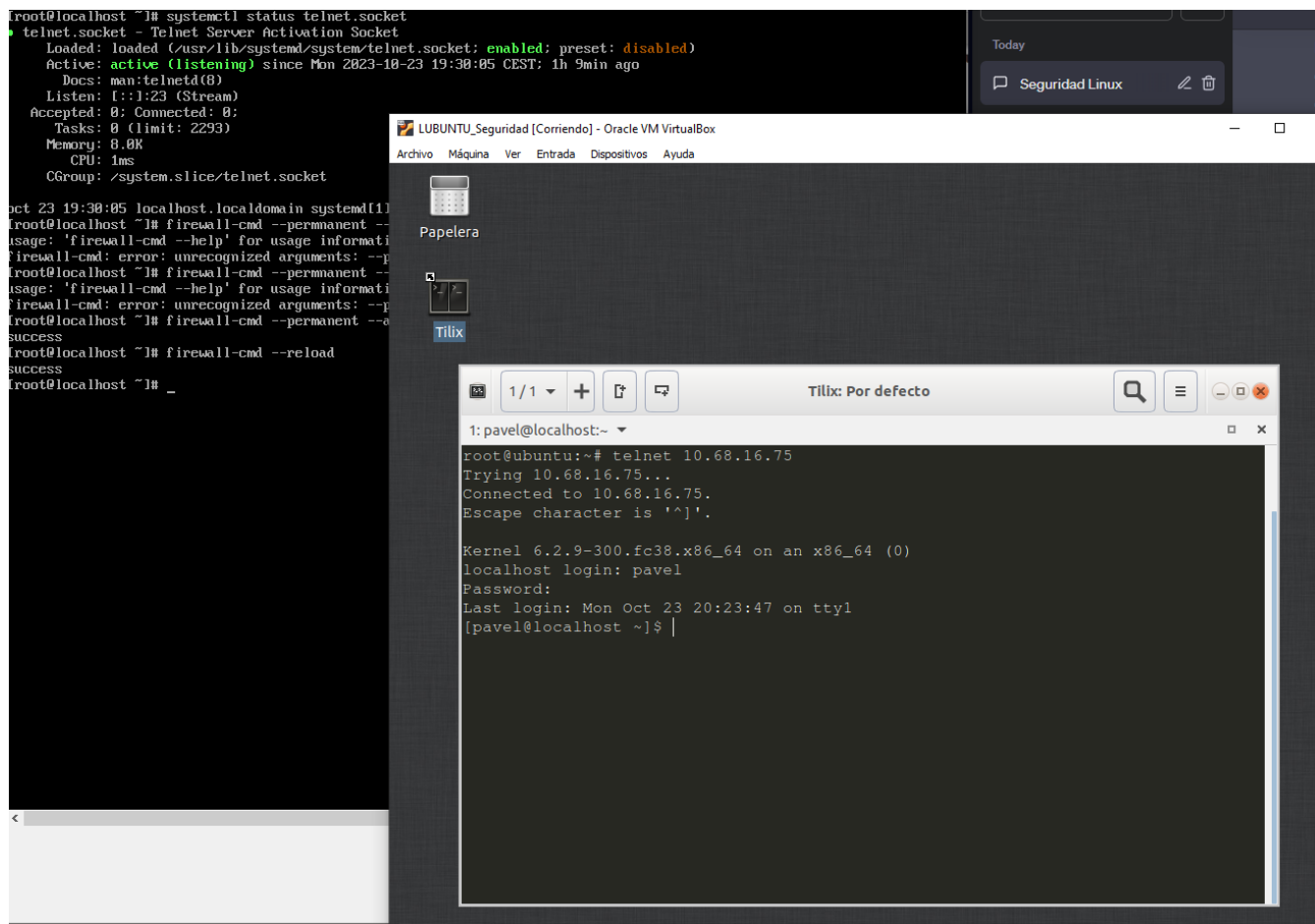
Bienvenidos a la clase del mejor profe, Guillermo Bellettini

Firmado Pavel

Conexión FTP



Conexión Telnet



Conexión SSH

```
[root@localhost ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Drop-In: /usr/lib/systemd/system/service.d
            └─10-timeout-abort.conf
   Active: active (running) since Mon 2023-10-23 16:03:35 CEST; 5h 12min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 774 (sshd)
     Tasks: 1 (limit: 2293)
    Memory: 4.4M
       CPU: 481ms
   CGroup: /system.slice/sshd.service
           └─774 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

oct 23 16:03:35 localhost systemd[1]: Started sshd.service - OpenSSH server daemon.
oct 23 18:10:35 localhost.localdomain sshd[1722]: error: kex_exchange_identification: read: Connection reset by peer
oct 23 18:10:35 localhost.localdomain sshd[1722]: Connection reset by 10.68.17.221 port 53425
oct 23 19:55:57 localhost.localdomain sshd[3263]: error: kex_exchange_identification: client sent invalid protocol ide
oct 23 19:55:57 localhost.localdomain sshd[3263]: banner exchange: Connection from 10.68.16.116 port 56084: invalid fo
oct 23 19:56:26 localhost.localdomain sshd[3264]: error: kex_exchange_identification: client sent invalid protocol ide
oct 23 19:56:26 localhost.localdomain sshd[3264]: banner exchange: Connection from 10.68.16.116 port 56088: invalid fo
oct 23 21:12:36 localhost.localdomain sshd[3808]: Connection reset by 10.68.18.178 port 58732 [preauth]
oct 23 21:14:07 localhost.localdomain sshd[3815]: Accepted password for pavel from 10.68.18.178 port 58745 ssh2
oct 23 21:14:07 localhost.localdomain sshd[3815]: pam_unix(sshd:session): session opened for user pavel(uid=1000) by (
[root@localhost ~]# _

C:\Users\nicolas.ballesteros>ssh -p22 pavel@10.68.16.75
The authenticity of host '10.68.16.75 (10.68.16.75)' can't be established.
ECDSA key fingerprint is SHA256:fz/xc3p1KHTQ/t2BOKwTbqo7wrZz58krIuGhKBbG+iY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.68.16.75' (ECDSA) to the list of known hosts.
pavel@10.68.16.75's password:
Last login: Mon Oct 23 20:42:37 2023 from ::ffff:10.68.16.116
[pavel@localhost ~]$
```

Bloqueamos los servicios

Listado de las reglas de iptable con comando sudo iptables -L

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:telnet

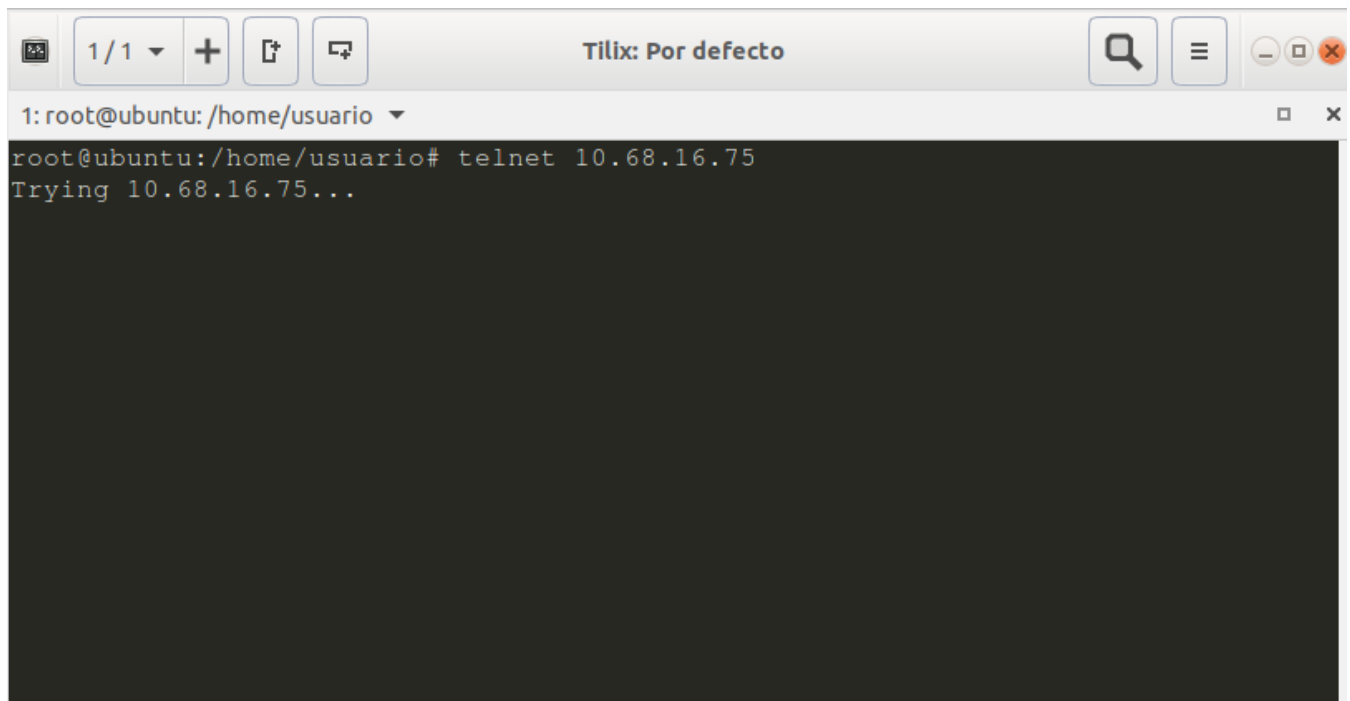
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@localhost ~]# _
```

Bloqueamos Telnet

```
[root@localhost ~]# iptables -A INPUT -p tcp --dport 23 -j DROP
[root@localhost ~]# _
```

Ponemos el comando para bloquear telnet

A screenshot of a terminal window titled "Tilix: Por defecto". The terminal shows a user at the root@ubuntu:/home/usuario prompt. They enter the command "telnet 10.68.16.75". The output shows "Trying 10.68.16.75..." followed by a blank screen, indicating a connection failure. The terminal window has standard Ubuntu window controls and a search icon in the title bar.

No se puede conectar

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:telnet
DROP       tcp  --  anywhere               anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@localhost ~]# _
```

Bloqueamos ssh

```
[root@localhost ~]# iptables -A INPUT -s 10.68.16.75 -p tcp --dport 22 -j DROP
[root@localhost ~]# _
```

```
target     prot opt source                destination
[root@localhost ~]# iptables -A INPUT -p tcp --dport 22 -j DROP
```

Guardamos los cambios

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:telnet
DROP       tcp  --  anywhere               anywhere
DROP       tcp  --  localhost.localdomain  anywhere               tcp dpt:ssh
DROP       tcp  --  localhost.localdomain  anywhere               tcp dpt:ssh
DROP       tcp  --  anywhere               anywhere               tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@localhost ~]# _
```

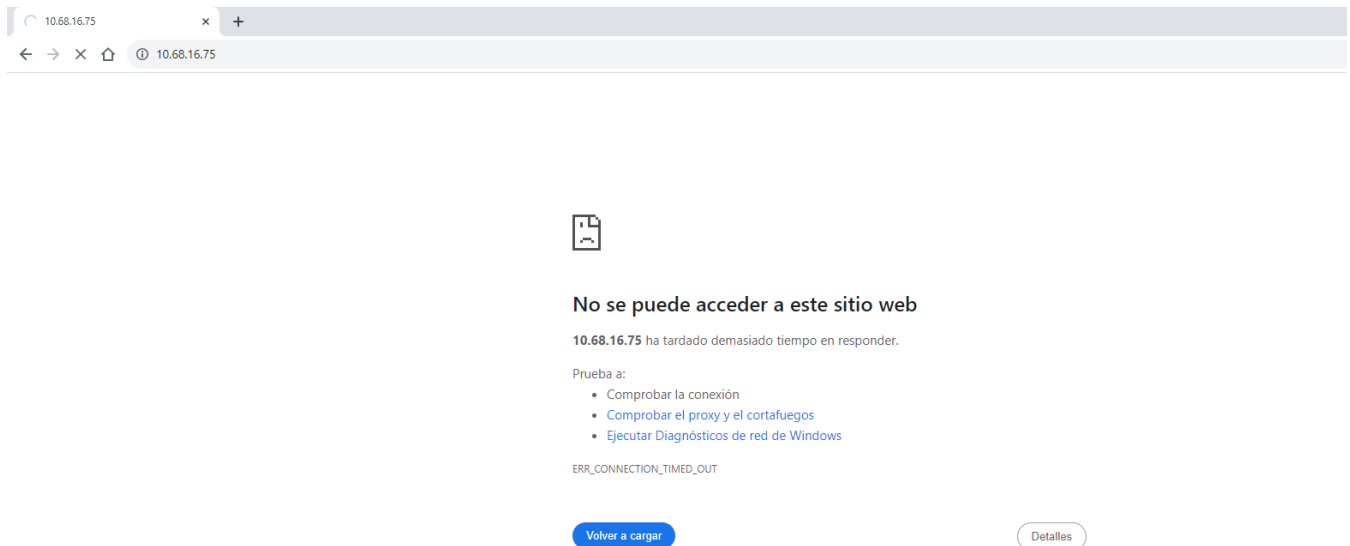
```
C:\Users\nicolas.ballesteros>ssh -p22 pavel@10.68.16.75
ssh: connect to host 10.68.16.75 port 22: Connection timed out

C:\Users\nicolas.ballesteros>
```

Bloqueamos HTTP

```
[root@localhost ~]# iptables -A INPUT -p tcp --dport 80 -j DROP
[root@localhost ~]#
```

Accedemos a la página web para comprobar



```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:telnet
DROP       tcp  -- anywhere              anywhere               tcp dpt:ssh
DROP       tcp  -- localhost.localdomain anywhere               tcp dpt:ssh
DROP       tcp  -- localhost.localdomain anywhere               tcp dpt:ssh
DROP       tcp  -- anywhere              anywhere               tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@localhost ~]#
```

Bloqueamos ftp

```
[root@localhost ~]# iptables -A INPUT -p tcp --dport 21 -j DROP
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           tcp dpt:telnet
DROP      tcp  -- localhost.localdomain anywhere              tcp dpt:ssh
DROP      tcp  -- localhost.localdomain anywhere              tcp dpt:ssh
DROP      tcp  -- anywhere              anywhere              tcp dpt:ssh
DROP      tcp  -- anywhere              anywhere              tcp dpt:http
DROP      tcp  -- anywhere              anywhere              tcp dpt:ftp

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@localhost ~]# _
```

Comprobamos

The screenshot shows a terminal window on the left and a Windows File Explorer window on the right. The terminal window displays the following commands and output:

```
[root@localhost ~]# iptables -A INPUT -p tcp --dport 80 -j DROP
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           tcp dpt:telnet
DROP      tcp  -- localhost.localdomain anywhere              tcp dpt:ssh
DROP      tcp  -- localhost.localdomain anywhere              tcp dpt:ssh
DROP      tcp  -- anywhere              anywhere              tcp dpt:ssh
DROP      tcp  -- anywhere              anywhere              tcp dpt:http
DROP      tcp  -- anywhere              anywhere              tcp dpt:ftp

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@localhost ~]# _
```

The File Explorer window shows the path **Internet > 10.68.16.75**. A dialog box titled "Error de carpeta FTP" is displayed, stating: "Windows no tiene acceso a esta carpeta. Asegúrese de haber escrito correctamente el nombre del archivo y de tener permiso para el acceso a la carpeta." The details section says: "Detalles: No se pudo establecer una conexión con el servidor." The "Aceptar" button is highlighted.