M11 – Seguretat Informàtica – UF1

Pràctica 1 - Els Firewall personals de Windows i Linux (UFW)_v04

Nil Massó

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

Table of Contents

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

• A l'hora d'avaluar i qualificar el treball es tindran en compte els aspectes estètics, de correctesa lingüística (sintàctica i ortogràfica) a més del que s'hagi comentat al cicle formatiu sobre la redacció de documentació tècnica i manuals.

• El mòdul professional pertany a uns estudis orientats al món laboral, cosa que fa que un cop complerts els requisits mínims la nota resultant serà condicionada per la quantitat i qualitat del treball individual realitzat per cada alumne.

Pràctica 1 – Els Firewall personals de Windows i Linux (UFW)

Els tallafocs personals s'instal·len generalment en àmbits domèstics o negocis molt petits. Aquest tallafoc normalment ha de protegir un únic ordinador o una petita xarxa, fins i tot és probable que s'instal·li en el mateix equip de treball. Alguns sistemes operatius inclouen un tallafoc instal·lat pensat per a ús domèstic, per exemple el Windows i l'Ubuntu

Aquests sistemes poden configurar-se amb regles addicionals per indicar quines connexions s'acceptaran o no.

Exercici 1: El Firewall de Windows (5 punts)

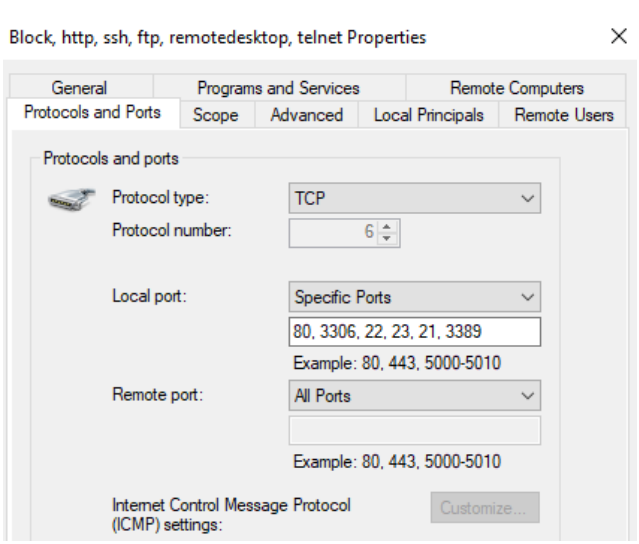
Mireu el següent vídeo per a saber com accedir i configurar algunes regles amb el Firewall: https://www.youtube.com/watch?v=qQXYfcfpyeM

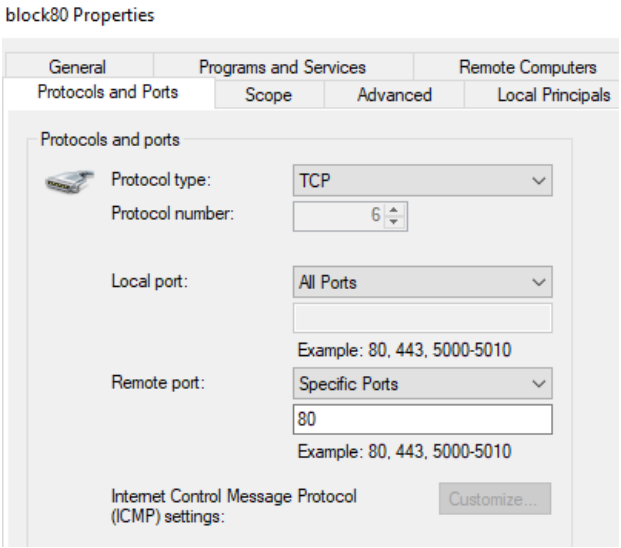
A partir d'aquí, feu servir una màquina virtual amb Windows **a la que hi tingueu accés des del vostre host** (per exemple amb una interfície posada en mode només amfitrió, only host). Per a poder fer proves i permetre i bloquejar serveis, en aquesta màquina hi instal·leu serveis com un servidor Apache i un servidor de base de dades amb **el XAMP** i un servidor FTP.

A continuació, implementeu les regles següents al Firewall de la vostra màquina virtual i proveu-les des del vostre host i la màquina virtual**. Inseriu captures de la configuració de les regles i la demostració des del vostre host.**

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

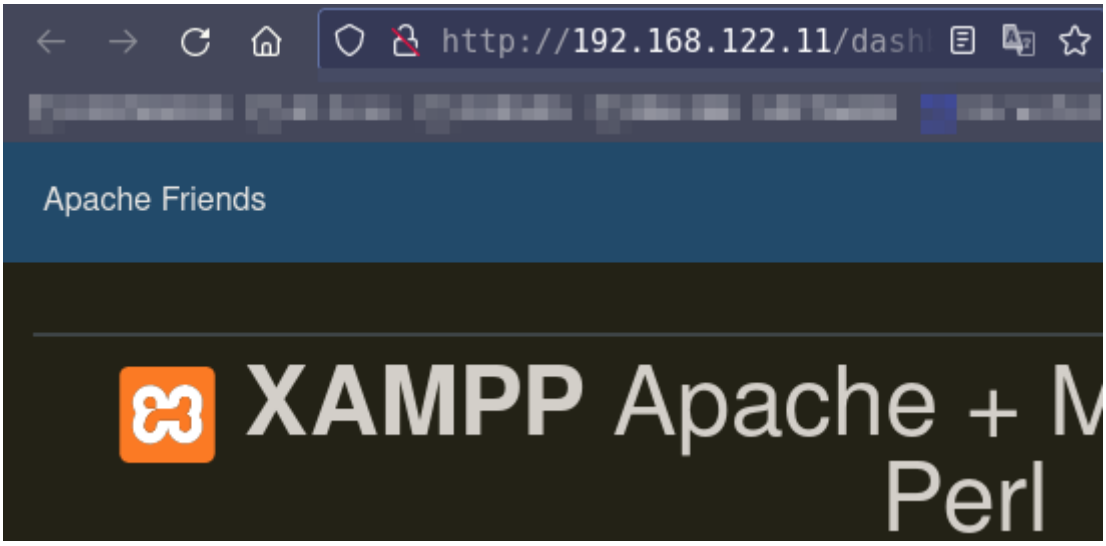
Inbound **outbound**

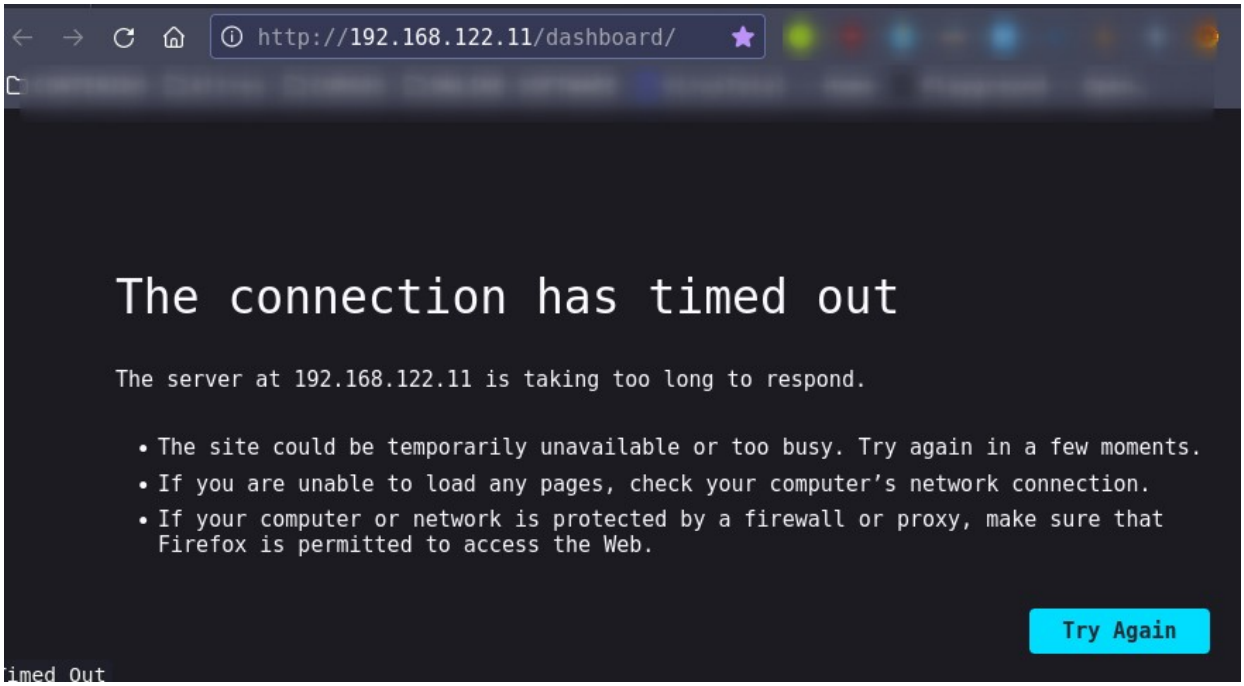




- Bloquegeu les peticions que entren cap al port 80 (0,5 punts)

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			



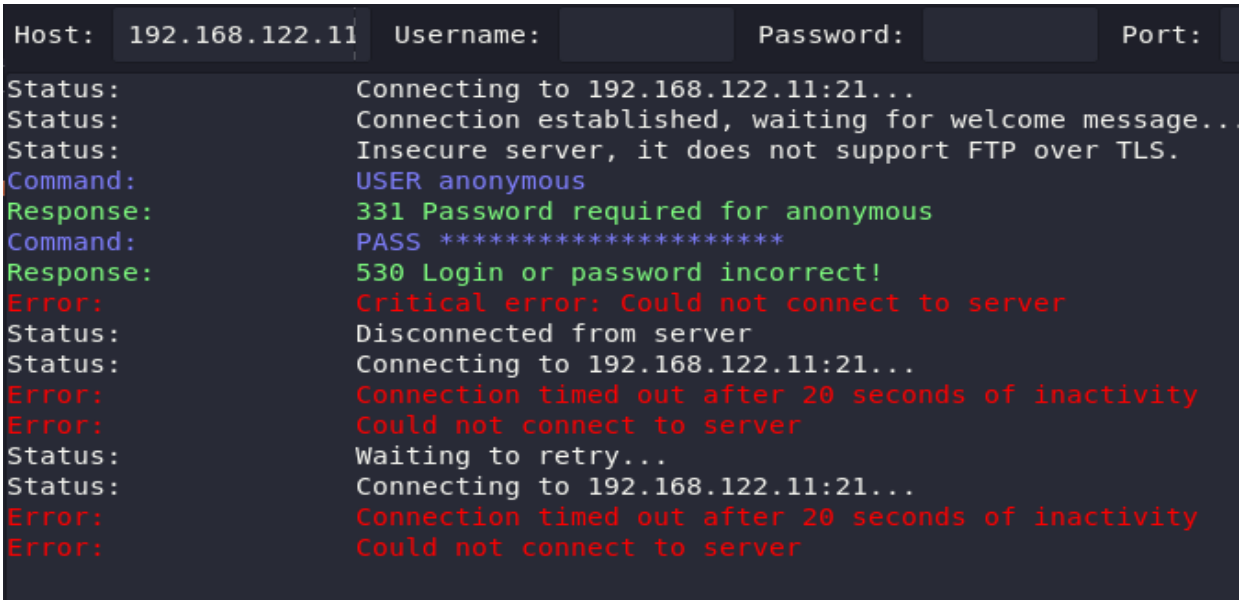


-
- Bloquegeu les peticions que entren cap al port del servidor de BBDD (0,5 punts)
- No permeteu accedir a la màquina virtual amb SSH (0,5 punts)
- No permeteu realitzar un Telnet cap a una altra màquina (0,5 punts)

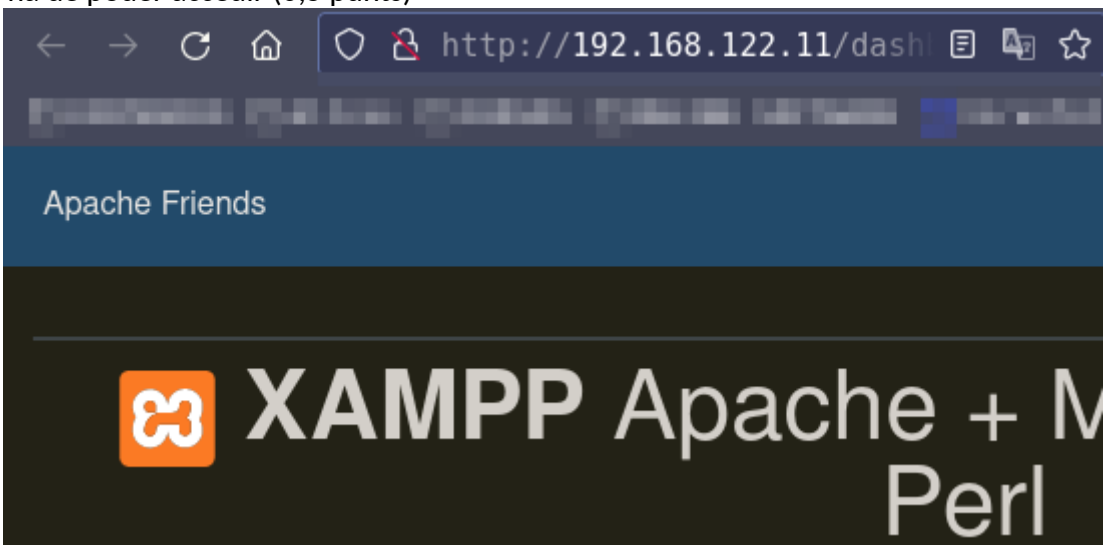
```
~$ telnet 192.168.122.11
Trying 192.168.122.11...
telnet: Unable to connect to remote host: Connection refused
```

- Bloquegeu les peticions que entren al servidor FTP (0,5 punts)

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

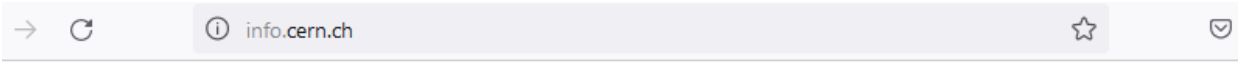


- Bloquegeu només l'accés al port 80 fetes des de la IP del vostre host. Un altre host si que hi ha de poder accedir (0,5 punts)



- No permeteu la connexió de sortida cap a les webs que facin servir http (sense certificat web ni encriptació) (0,5 punts)

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			



Unable to connect

Firefox can't establish a connection to the server at info.cern.ch.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

-
- No accepteu peticions de PING (0,5 punts)

```
tursu@tursu:~$ ping 192.168.122.11
PING 192.168.122.11 (192.168.122.11) 56(84) bytes of data.
64 bytes from 192.168.122.11: icmp_seq=19 ttl=128 time=9.28 ms
```

- Deshabilitar l'administració remota (1 punt)

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

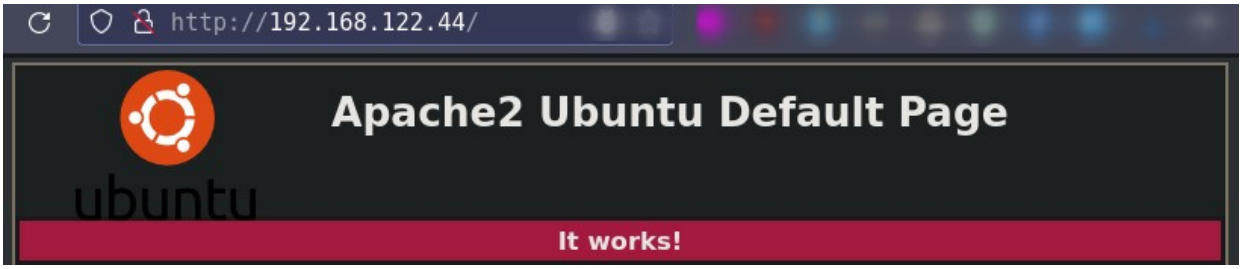
Exercici 2: El Firewall personal de Linux (UFW) (5 punts)

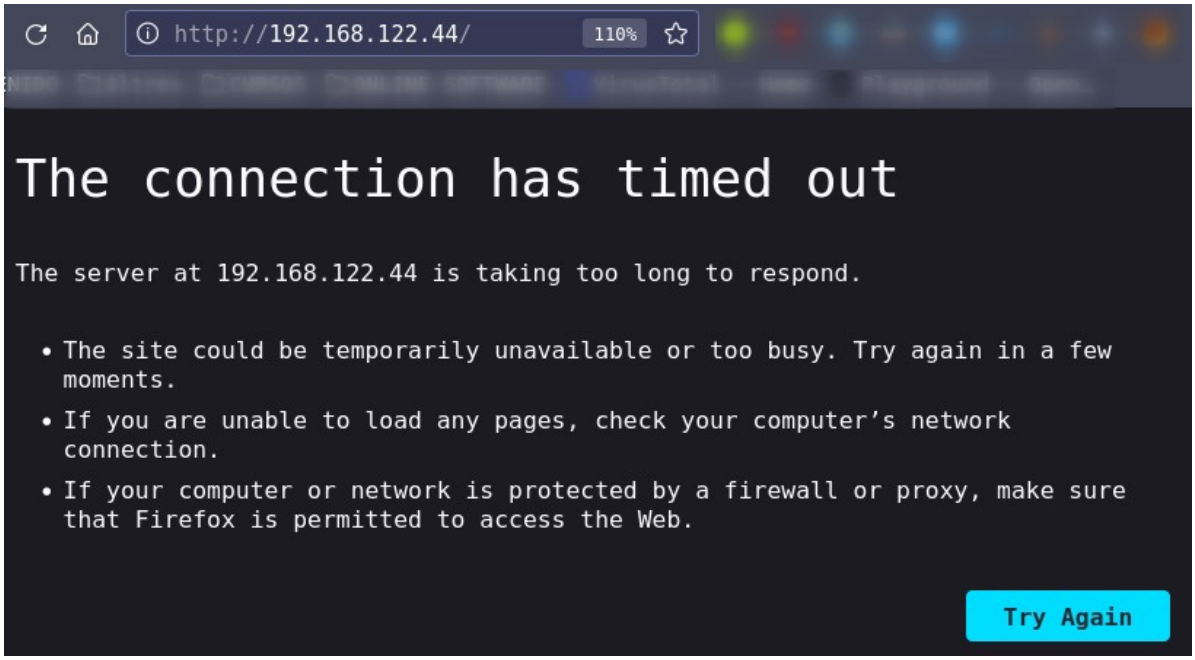
El **UFW** (uncomplicated firewall) permet activar-lo o desactivar-lo, posar la política per defecte com a permissiva o restrictiva, permetre/denegar/rebutjar/limitar l'accés i habilitar/deshabilitar el log (***/var/log/ufw.log***)

A partir d'aquí, feu servir una màquina (virtual o no) amb Linux a la que hi tingueu accés des del vostre host. En aquesta màquina hi instal·leu serveis com un servidor Apache i un servidor de base de dades amb el XAMP i un servidor FTP.

A continuació, implementeu aquestes regles al UFW i proveu-les des del vostre host i la màquina virtual. **Inseriu les comandes de la configuració de les regles i la demostració des del vostre host o remot. Inseriu captura del log de cada exercici per a demostrar que funciona correctament. I les captures que demostren que els serveis funcionen o no.**

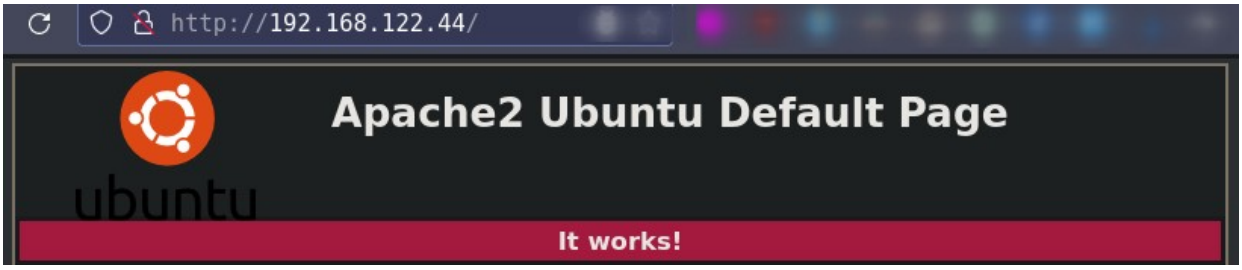
- **Bloquegeu** les peticions que entren cap al port 80 (0,5 punts)
  sudo ufw deny 80/tcp

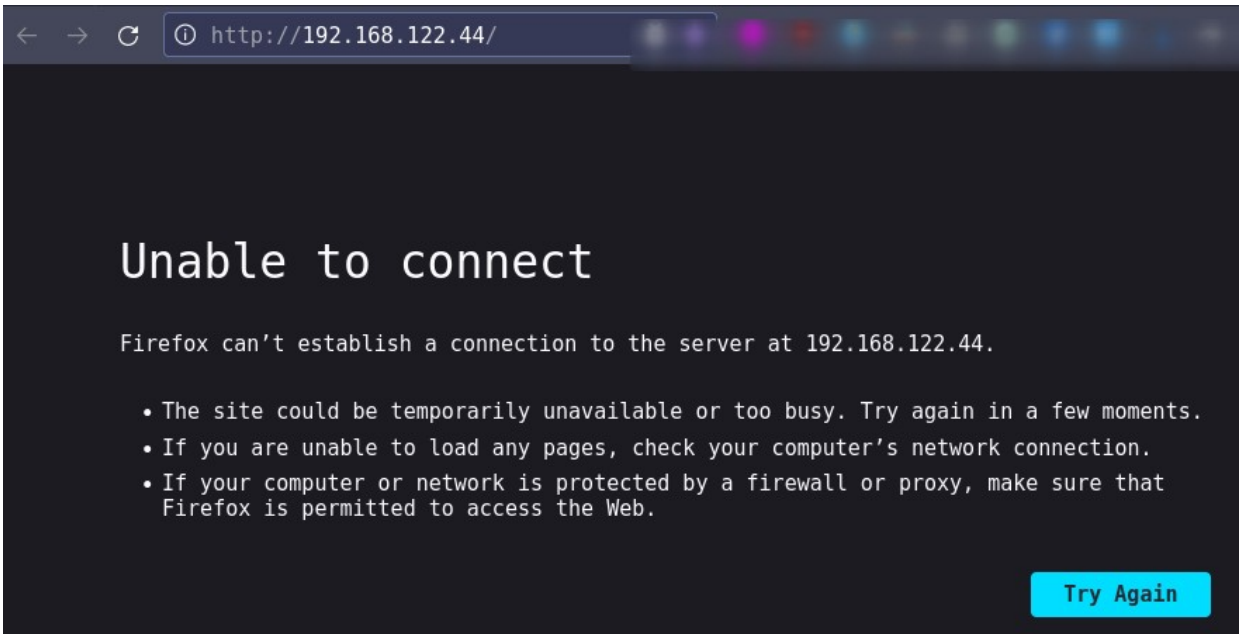




ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

- **Refuseu** les peticions que entren cap al port 80 (0,5 punts)
  sudo ufw reject in 80/tcp





- Bloquegeu les peticions que entren cap al port del servidor de BBDD (0,5 punts)
  sudo ufw deny in 3306/tcp

- No permeteu accedir a l'Ubuntu amb SSH (0,5 punts)
  sudo ufw deny in 22/tcp

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			

```
root@tursu:~# ssh nil@192.168.122.44
The authenticity of host '192.168.122.44 (192.168.122.44)' can't be established.
ECDSA key fingerprint is SHA256:r++ikbHZ1jeh/sJLeHgp9zsna+uuqCR/ge+r9bhh+Gs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.122.44' (ECDSA) to the list of known hosts.
nil@192.168.122.44's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.0.0-23-generic x86_64)

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

5 updates can be applied immediately.
5 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

```
[redacted]$ ssh nil@192.168.122.44

ssh: connect to host 192.168.122.44 port 22: Connection timed out
```

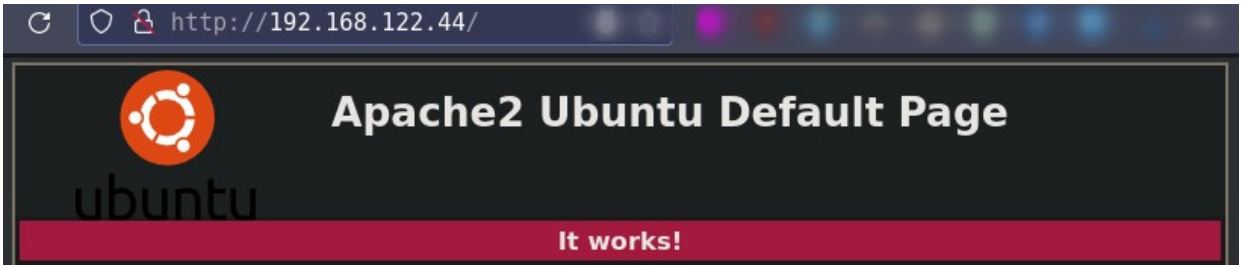
- No permeteu realitzar un Telnet cap a una altra màquina (0,5 punts)
  sudo ufw deny out 23/tcp

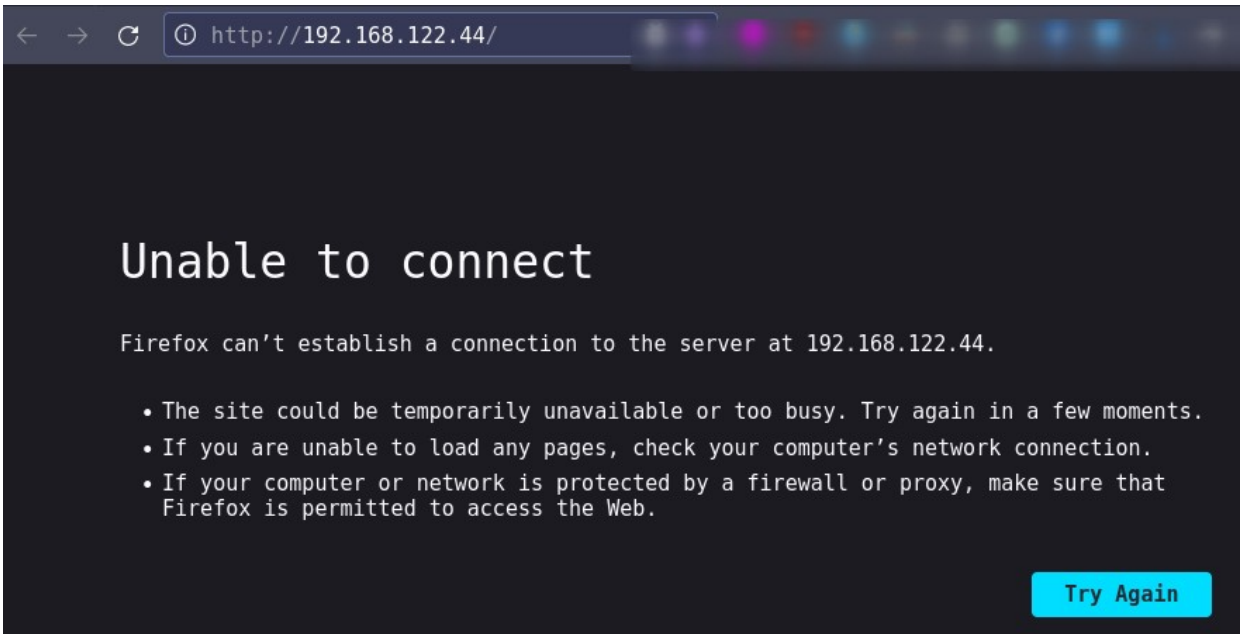
- Bloquegeu les peticions que entren al servidor FTP (0,5 punts)
  sudo ufw deny in 21/tcp

```
Status:                         Connecting to 192.168.122.44:21...
Status:                         Connection established, waiting for welcome message.
Status:                         Insecure server, it does not support FTP over TLS.
Command:                        USER root
Response:                       331 Password required for root
Command:                        PASS **********
Response:                       530 Login incorrect.
Error:                          Critical error: Could not connect to server
Status:                         Disconnected from server
Status:                         Connecting to 192.168.122.44:21...
Error:                          Connection timed out after 20 seconds of inactivity
Error:                          Could not connect to server
```

- Bloquegeu només l'accés al port 80 fetes des de la IP del vostre host. Un altre host si que hi ha de poder accedir (0,5 punts)
  sudo ufw deny 80/tcp from 192.168.122.1

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions:			





- No permeteu la connexió de sortida cap a les webs que facin servir http (sense certificat web ni encriptació) (0,5 punts)
  sudo ufw deny out http

- No accepteu peticions de PING. Amb UFW **no hi ha una regla directa**, però podeu investigar un work-around per a aconseguir-ho. **Com es faria?** (1 punt)
  nano /etc/ufw/before.rules

```
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j
ACCEPT
-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j AC-
CEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT
```

ASIX 2			
M11 – Seguretat Informàtica – UF1		**Tipus**	Individual
Cognoms, Nom:	**Massó Cabaña, Nil**	**Curs**	2022-23
Observacions: