

Practica 11

César Muñoz Reinoso

Ejercicio 1:

The image displays two terminal windows from a virtual machine environment. The left window, titled 'vagrant@nodo1: ~', shows the configuration of fail2ban and iptables. It starts with a timestamp '2021-12-03 09:43:08.126 fail2ban' and an error message '[3617]: ERROR Permission denied to socket: /var/run/fail2ban/fail2ban.sock, (you must be root)'. The user then runs 'sudo fail2ban-client set sshd unbanip 192.168.12.12'. Next, 'sudo fail2ban-client status' is executed, showing the status of the jail. Finally, 'sudo iptables -L -n' is run, displaying the current iptables rules. The right window, titled 'vagrant@nodo2: ~', shows the attempt to connect via SSH. It starts with 'vagrant@nodo2:~\$ ssh 192.168.12.11', followed by 'ssh: connect to host 192.168.12.11 port 22: Connection refused'. The user then enters the password for 'vagrant@192.168.12.11', and the terminal shows the Ubuntu login prompt: 'Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-90-generic x86_64)'. Below the login prompt, system information is displayed, including documentation, management, and support links, as well as system load, processes, users logged in, memory usage, and swap usage. The terminal also shows that 26 updates can be applied immediately, with 17 of these being standard security updates. The last login is recorded as 'Fri Dec 3 09:42:34 2021 from 192.168.12.12'.

```
vagrant@nodo1:~$ sudo fail2ban-client set sshd unbanip 192.168.12.12
vagrant@nodo1:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
|- Jail list:          sshd
vagrant@nodo1:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target prot opt source                destination
f2b-sshd tcp -- 0.0.0.0/0             0.0.0.0/0          multiport dports 22

Chain FORWARD (policy ACCEPT)
target prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target prot opt source                destination

Chain f2b-sshd (1 references)
target prot opt source                destination
REJECT all -- 192.168.12.12        0.0.0.0/0          reject-with icmp-port-unreachable
RETURN all -- 0.0.0.0/0         0.0.0.0/0

vagrant@nodo1:~$
```

```
vagrant@nodo2:~$ ssh 192.168.12.11
ssh: connect to host 192.168.12.11 port 22: Connection refused
vagrant@nodo2:~$ ssh 192.168.12.11
vagrant@192.168.12.11's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-90-generic x86_64)

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

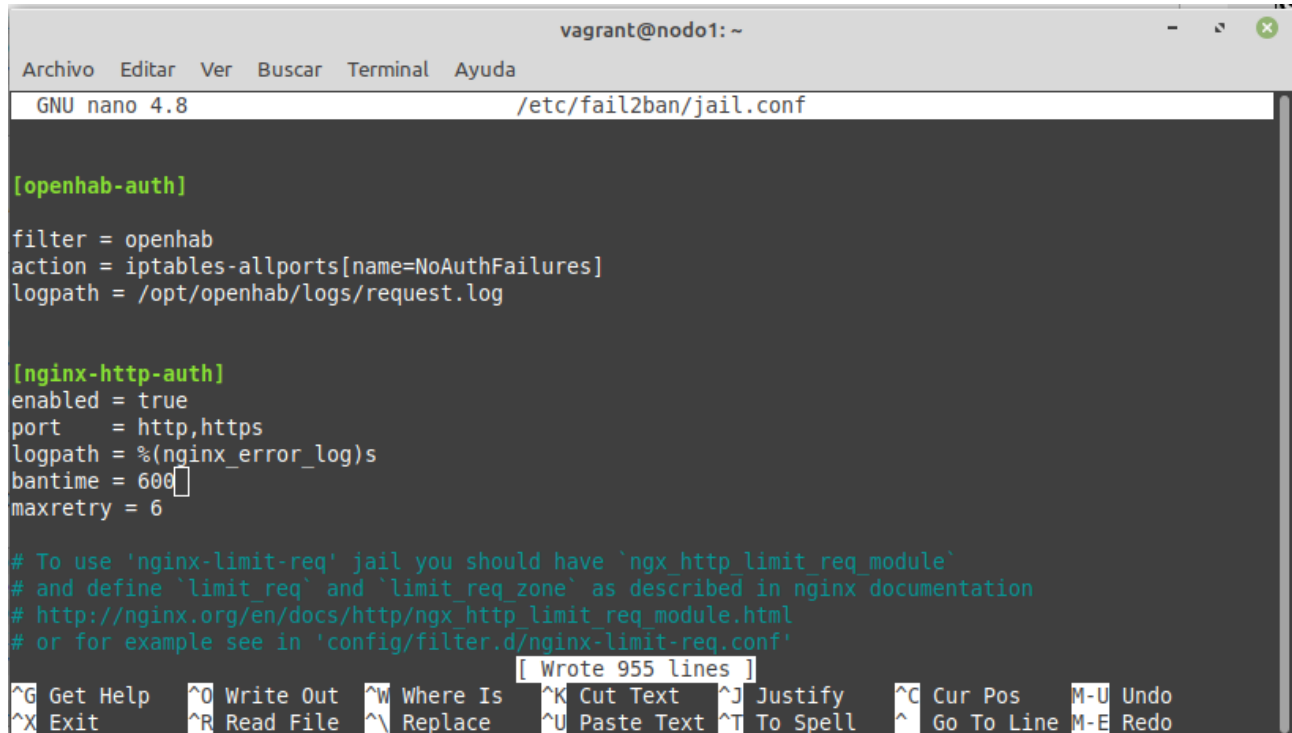
System information as of Fri Dec 3 09:46:01 UTC 2021

System load:  0.0               Processes:    107
Usage of /:   3.7% of 38.71GB   Users logged in: 1
Memory usage: 22%              IPv4 address for enp0s3: 10.0.2.15
Swap usage:   0%               IPv4 address for enp0s8: 192.168.12.11

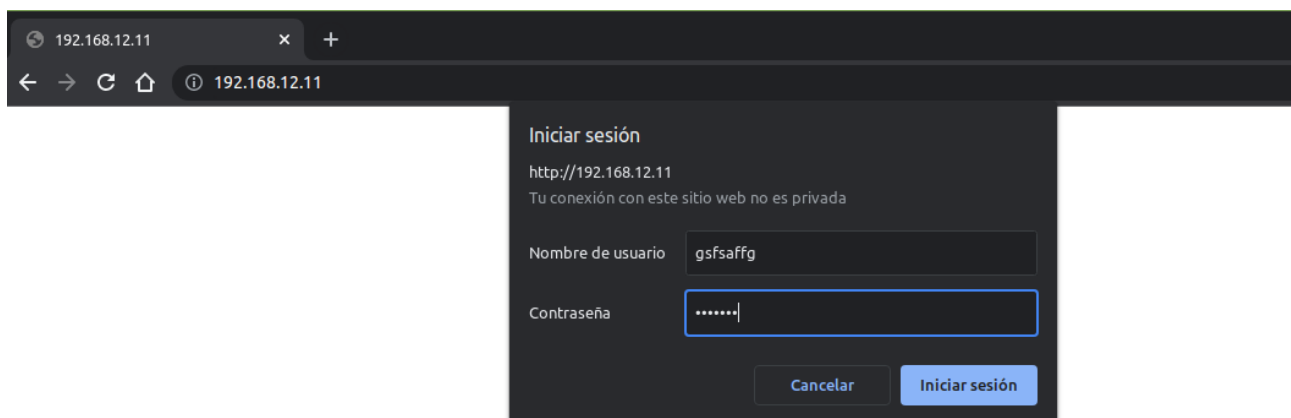
26 updates can be applied immediately.
17 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Fri Dec 3 09:42:34 2021 from 192.168.12.12
vagrant@nodo1:~$
```

Ejercicio 2



```
vagrant@nodo1: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
GNU nano 4.8 /etc/fail2ban/jail.conf  
  
[openhab-auth]  
filter = openhab  
action = iptables-allports[name=NoAuthFailures]  
logpath = /opt/openhab/logs/request.log  
  
[nginx-http-auth]  
enabled = true  
port    = http,https  
logpath = %(nginx_error_log)s  
bantime = 600  
maxretry = 6  
  
# To use 'nginx-limit-req' jail you should have 'ngx_http_limit_req_module'  
# and define 'limit_req' and 'limit_req_zone' as described in nginx documentation  
# http://nginx.org/en/docs/http/ngx_http_limit_req_module.html  
# or for example see in 'config/filter.d/nginx-limit-req.conf'  
[ Wrote 955 lines ]  
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo  
^X Exit      ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line  M-E Redo
```



192.168.12.11

← → ↻ 🏠 ⓘ 192.168.12.11

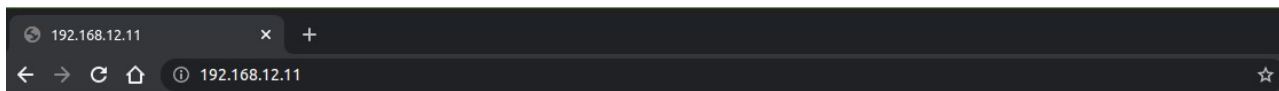
Iniciar sesión

http://192.168.12.11

Tu conexión con este sitio web no es privada

Nombre de usuario

Contraseña



No se puede acceder a este sitio web

La página **192.168.12.11** ha rechazado la conexión.

Prueba a:

- Comprobar la conexión
- [Comprobar el proxy y el cortafuegos](#)

ERR_CONNECTION_REFUSED

Detalles

Volver a cargar

Ejercicio 3

```
vagrant@nodo1: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 qrencode amd64 4.0.2-2 [24.0 kB]  
Fetched 24.0 kB in 0s (65.0 kB/s)  
Selecting previously unselected package qrencode.  
(Reading database ... 64333 files and directories currently installed.)  
Preparing to unpack .../qrencode_4.0.2-2_amd64.deb ...  
Unpacking qrencode (4.0.2-2) ...  
Setting up qrencode (4.0.2-2) ...  
Processing triggers for man-db (2.9.1-1) ...  
vagrant@nodo1:~$ google-authenticator  
  
Do you want authentication tokens to be time-based (y/n) y  
Warning: pasting the following URL into your browser exposes the OTP secret to Google:  
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/vagrant@nodo1%3Fsecret%3DB6K2LZHD2ZA64GK3XYIFEUIVSQ%26issuer%3Dnodo1  
  
  
  
Your new secret key is: B6K2LZHD2ZA64GK3XYIFEUIVSQ  
Your verification code is 944500  
Your emergency scratch codes are:  
51862676  
54035916  
63569937  
72602663  
72675037  
  
Do you want me to update your "/home/vagrant/.google_authenticator" file? (y/n) y
```

Account name:

nodo1

Secret key:

B6K2LZHD2ZA64GK3XYIFEUIVSQ

+ Add Cancel

One-time passwords 20

435973

nodo1