

PRÁCTICA 4 (almellonesfernandez-practica4)

U.D.2. REDES DE COMPUTADORAS SEGURAS (I).

SEGURIDAD A NIVEL DE HOST. FIREWALL DE SERVIDOR. IDS

*** En esta práctica, el alumno debe realizar **TODAS** las comprobaciones que conozca y se hayan implementado a lo largo del curso. No bastará con comprobaciones simples. Se trata de demostrar todo lo que se sepa.

IPTABLES CON PORT-KNOCKING. HERRAMIENTA ESPECÍFICA.

1. (2,5 puntos) Usando exclusivamente iptables, configure el servicio sshd de Ubuntu Server, para que se active llamando a los puertos 7777, 8888, 9999. Se deja al alumno que muestre las evidencias necesarias (netstat, watch iptables -L -n -v, creación de reglas, apertura de puertos poco a poco, etc).

```
GNU nano 7.2 almallonesfernandez-iptables.sh
iptables -A INPUT -i $tarjeta -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 3306 -j ACCEPT
#iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -m connlimit --connlimit-above 3 -j DROP
#iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -m time --timestart 09:00 --timestop 17:00 --datestart 2024-11-24
#iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
#iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s 192.168.1.0/24 -j ACCEPT
#iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p icmp -j ACCEPT

# PORT-KNOCKING.

# Marca el primer golpe en el puerto 7777
iptables -A INPUT -p tcp --dport 7777 -m state --state NEW -m recent --name KNOCK1 --set

# Marca el segundo golpe en el puerto 8888 si el primer golpe fue recibido en los últimos 10 segundos
iptables -A INPUT -p tcp --dport 8888 -m state --state NEW -m recent --name KNOCK1 --rcheck --seconds 30 -m recent --name KNOCK2 --set

# Marca el tercer golpe en el puerto 9999 si el segundo golpe fue recibido en los últimos 10 segundos
iptables -A INPUT -p tcp --dport 9999 -m state --state NEW -m recent --name KNOCK2 --rcheck --seconds 30 -m recent --name KNOCK3 --set

# Permite el acceso al puerto SSH (22) si se recibieron los tres golpes en orden dentro de los últimos 10 segundos
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --name KNOCK3 --rcheck --seconds 30 -j ACCEPT
```

Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:~/scripts# nano almallonesfernandez-iptables.sh
root@Ubuntu-server-bastionado:~/scripts# ./almallonesfernandez-iptables.sh
Iniciandose cortafuegos de Host: Alvaro Almellones
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 1 packets, 32 bytes)
  pkts bytes target     prot opt in     out     source               destination
  0      0 ACCEPT     0     --  lo     *       0.0.0.0/0            0.0.0.0/0
  0      0 ACCEPT     6     --  enp0s3 *       0.0.0.0/0            0.0.0.0/0      tcp dpt:21
  0      0 ACCEPT     6     --  enp0s3 *       0.0.0.0/0            0.0.0.0/0      tcp dpt:80
  0      0 ACCEPT     6     --  enp0s3 *       0.0.0.0/0            0.0.0.0/0      tcp dpt:3306
  0      0 ACCEPT     1     --  enp0s3 *       0.0.0.0/0            0.0.0.0/0      tcp dpt:7777 state NEW recent: SET name: KN
0CK1 side: source mask: 255.255.255.255
  0      0          6     --  *       0.0.0.0/0            0.0.0.0/0      tcp dpt:8888 state NEW recent: CHECK second
s: 30 name: KNOCK1 side: source mask: 255.255.255.255 recent: SET name: KNOCK2 side: source mask: 255.255.255.255
  0      0          6     --  *       0.0.0.0/0            0.0.0.0/0      tcp dpt:9999 state NEW recent: CHECK second
s: 30 name: KNOCK2 side: source mask: 255.255.255.255 recent: SET name: KNOCK3 side: source mask: 255.255.255.255
  0      0          6     --  *       0.0.0.0/0            0.0.0.0/0      tcp dpt:22 state NEW recent: CHECK seconds:
30 name: KNOCK3 side: source mask: 255.255.255.255
  11 680 ACCEPT     0     --  enp0s3 *       0.0.0.0/0            0.0.0.0/0      state RELATED,ESTABLISHED
  0      0 LOG         6     --  *       0.0.0.0/0            0.0.0.0/0      tcp dpt:22 LOG flags 0 level 4 prefix "Inte
ntos-ataque-SSH Server-al"
  0      0 LOG         6     --  *       0.0.0.0/0            0.0.0.0/0      tcp dpt:3306 LOG flags 0 level 4 prefix "In
tentos-ataque-mysql-almello"
  0      0 LOG         6     --  *       0.0.0.0/0            0.0.0.0/0      tcp dpt:80 LOG flags 0 level 4 prefix "Inte
ntos-ataque-Web-Server-al"

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
```

```
almallonesfernandez@Ubuntu-server-bastionado: ~
root@almallonesfernandez-VirtualBox:/home/almallonesfernandez/scripts# ssh -i /root/miskeys/almallonesfernandez almallon
esfernandez@192.168.1.110 -p 7777
^C
root@almallonesfernandez-VirtualBox:/home/almallonesfernandez/scripts# ssh -i /root/miskeys/almallonesfernandez almallon
esfernandez@192.168.1.110 -p 8888
^C
root@almallonesfernandez-VirtualBox:/home/almallonesfernandez/scripts# ssh -i /root/miskeys/almallonesfernandez almallon
esfernandez@192.168.1.110 -p 9999
^C
root@almallonesfernandez-VirtualBox:/home/almallonesfernandez/scripts# ssh -i /root/miskeys/almallonesfernandez almallon
esfernandez@192.168.1.110
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almallonesfernandez. Está prohibida l
a conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Last login: Sat Nov 30 13:45:32 2024 from 192.168.1.108
almallonesfernandez@Ubuntu-server-bastionado:~$
```

Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 89 packets, 4622 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:21
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306
3 104 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
2 120 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:7777 state NEW recent: SET name: KN
OCK1 side: source mask: 255.255.255.255
4 240 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:8888 state NEW recent: CHECK second
s: 30 name: KNOCK1 side: source mask: 255.255.255.255 recent: SET name: KNOCK2 side: source mask: 255.255.255.255
2 120 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:9999 state NEW recent: CHECK second
s: 30 name: KNOCK2 side: source mask: 255.255.255.255 recent: SET name: KNOCK3 side: source mask: 255.255.255.255
1 60 ACCEPT 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 state NEW recent: CHECK seconds:
30 name: KNOCK3 side: source mask: 255.255.255.255
52 7818 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 LOG flags 0 level 4 prefix "Inte
ntos-ataque-SSH Server-al"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306 LOG flags 0 level 4 prefix "In
tentos-ataque-mysql-almello"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80 LOG flags 0 level 4 prefix "Inte
ntos-ataque-Web-Server-al"

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
42 8134 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
```

```
30 de nov 14:02
root@almellonesfernandez-VirtualBox /home/almellonesfernandez/scripts
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez/scripts# ssh -i /root/miskeys/almellonesfernandez almellon
esfernandez@192.168.1.110 -p 7777
^C
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez/scripts# ssh -i /root/miskeys/almellonesfernandez almellon
esfernandez@192.168.1.110 -p 8888
^C
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez/scripts# ssh -i /root/miskeys/almellonesfernandez almellon
esfernandez@192.168.1.110
^C
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez/scripts#
```

Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 154 packets, 8061 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:21
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306
5 160 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
4 240 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:7777 state NEW recent: SET name: KN
OCK1 side: source mask: 255.255.255.255
8 480 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:8888 state NEW recent: CHECK second
s: 30 name: KNOCK1 side: source mask: 255.255.255.255 recent: SET name: KNOCK2 side: source mask: 255.255.255.255
2 120 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:9999 state NEW recent: CHECK second
s: 30 name: KNOCK2 side: source mask: 255.255.255.255 recent: SET name: KNOCK3 side: source mask: 255.255.255.255
1 60 ACCEPT 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 state NEW recent: CHECK seconds:
30 name: KNOCK3 side: source mask: 255.255.255.255
123 13550 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
6 360 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 LOG flags 0 level 4 prefix "Inte
ntos-ataque-SSH Server-al"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306 LOG flags 0 level 4 prefix "In
tentos-ataque-mysql-almello"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80 LOG flags 0 level 4 prefix "Inte
ntos-ataque-Web-Server-al"

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

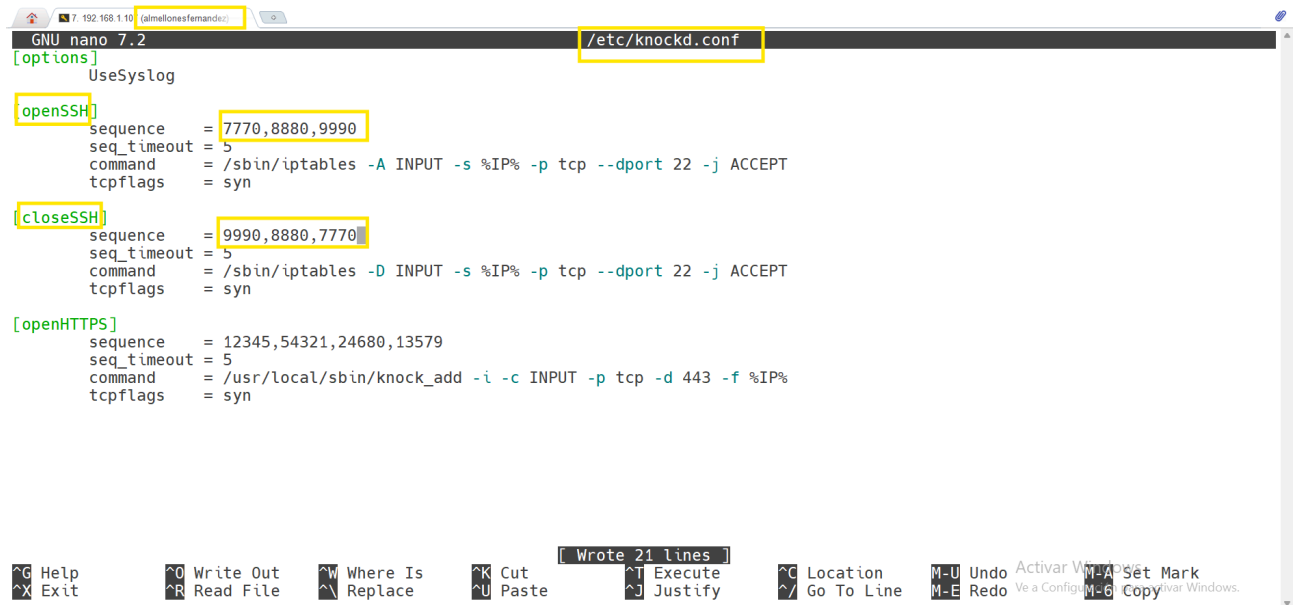
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
112 14426 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
```

Como podemos observar el Accept no ha aumentado porque a falta de realizar la secuencia correcta (hacer el tercer Knock), no deja acceder por ssh . En cambio los dos primeros si aumentan porque he realizado una prueba en la que la conexión falle

Álvaro Almellones Fernández

2. (1,5 puntos) Haciendo uso de la herramienta port-knocking, configure el servicio sshd de Ubuntu Server, para que se active llamando a los puertos 7770, 8880, 9990 y se desactive realizando la llamada en orden inverso. Se debe configurar un timeout máximo de 30 minutos una vez abierto el servicio.

Lo previo a este paso es instalar el demonio knockd



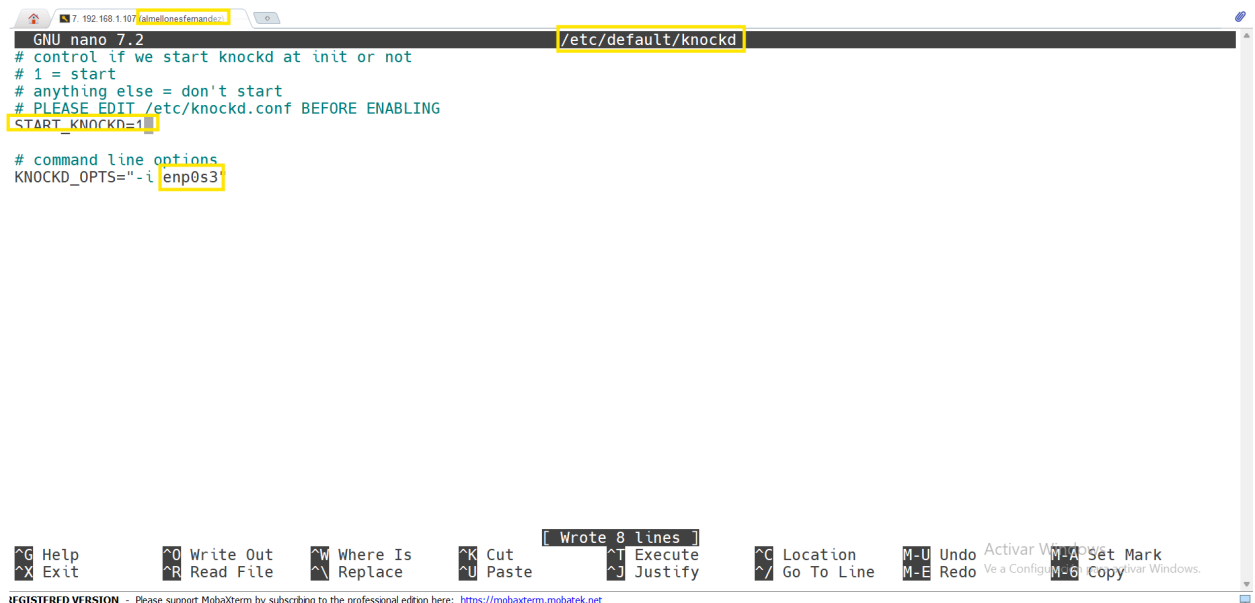
```
GNU nano 7.2 /etc/knockd.conf
[options]
  UseSyslog

[openSSH]
  sequence       = 7770,8880,9990
  seq_timeout    = 5
  command        = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
  tcpflags       = syn

[closeSSH]
  sequence       = 9990,8880,7770
  seq_timeout    = 5
  command        = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
  tcpflags       = syn

[openHTTPS]
  sequence       = 12345,54321,24680,13579
  seq_timeout    = 5
  command        = /usr/local/sbin/knock_add -i -c INPUT -p tcp -d 443 -f %IP%
  tcpflags       = syn

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
^C Location   M-U Undo     Activar Windows
^_ Go To Line M-E Redo     Ve a Configur M-A Set Mark
                                     M-G Copy      Activar Windows.
```



```
GNU nano 7.2 /etc/default/knockd
# control if we start knockd at init or not
# 1 = start
# anything else = don't start
# PLEASE EDIT /etc/knockd.conf BEFORE ENABLING
START_KNOCKD=1

# command line options
KNOCKD_OPTS="-i enp0s3"

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
^C Location   M-U Undo     Activar Windows
^_ Go To Line M-E Redo     Ve a Configur M-A Set Mark
                                     M-G Copy      Activar Windows.
```

REGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Álvaro Almellones Fernández

En la última fila hay que es importante poner el nombre de la tarjeta de red y el la columna de start se pone un 1

```
root@Ubuntu-server-bastionado:~/scripts# systemctl start knockd
root@Ubuntu-server-bastionado:~/scripts# systemctl enable knockd
Synchronizing state of knockd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable knockd
Created symlink /etc/systemd/system/multi-user.target.wants/knockd.service → /usr/lib/systemd/system/knockd.service.
root@Ubuntu-server-bastionado:~/scripts# systemctl status knockd
● knockd.service - Port-Knock Daemon
   Loaded: loaded (/usr/lib/systemd/system/knockd.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-11-30 21:02:43 CET; 19s ago
     Docs: man:knockd(1)
  Main PID: 1675 (knockd)
    Tasks: 1 (limit: 2276)
  Memory: 1.7M (peak: 1.8M)
     CPU: 18ms
    CGroup: /system.slice/knockd.service
            └─1675 /usr/sbin/knockd -i enp0s3

Nov 30 21:02:43 Ubuntu-server-bastionado systemd[1]: Started knockd.service - Port-Knock Daemon.
Nov 30 21:02:44 Ubuntu-server-bastionado knockd[1675]: starting up, listening on enp0s3
root@Ubuntu-server-bastionado:~/scripts#
```

Ya hemos configurado el server , vamos a realizar las pruebas en el cliente

```
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez# apt install knockd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
knockd ya está en su versión más reciente (0.8-2build2).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 91 no actualizados.
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez# knock -v 192.168.1.110 7770 8880 9990
hitting tcp 192.168.1.110:7770
hitting tcp 192.168.1.110:8880
hitting tcp 192.168.1.110:9990
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez# ssh -i /root/miskeys/almellonesfernandez almellonesfernandez@192.168.1.110
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Last login: Sat Nov 30 21:11:54 2024 from 192.168.1.108
almellonesfernandez@Ubuntu-server-bastionado:~$ exit
logout
Connection to 192.168.1.110 closed.
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez# knock -v 192.168.1.110 9990 8880 7770
hitting tcp 192.168.1.110:9990
hitting tcp 192.168.1.110:8880
hitting tcp 192.168.1.110:7770
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez# ssh -i /root/miskeys/almellonesfernandez almellonesfernandez@192.168.1.110
^C
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez#
```

Como podemos observar si se pone la combinación que abre el puerto 22 y se prueba un ssh accede sin problemas, pero si realizamos la combinación que cierra el puerto y realizamos un ssh no me deja acceder

OTRAS HERRAMIENTAS RELACIONADAS CON IPTABLES

3. **(FailToBan-IDS)** Usando la herramienta failtoban, realice las siguientes actuaciones en el servidor de Ubuntu Server, para evitar problemas de ataque. Mínimo tiene que demostrarse:

a) Instalación y comprobación de servicio fail2ban. **(0,5 puntos)**

```
root@Ubuntu-server-bastionado:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-11-30 21:45:42 CET; 1min 46s ago
     Docs: man:fail2ban(1)
   Main PID: 2519 (fail2ban-server)
    Tasks: 5 (limit: 2276)
  Memory: 41.0M (peak: 41.2M)
     CPU: 790ms
    CGroup: /system.slice/fail2ban.service
            └─2519 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Nov 30 21:45:42 Ubuntu-server-bastionado systemd[1]: Started fail2ban.service - Fail2Ban Service.
Nov 30 21:45:43 Ubuntu-server-bastionado fail2ban-server[2519]: 2024-11-30 21:45:43,947 fail2ban.configreader [2519]: WARNING 'al
Nov 30 21:45:46 Ubuntu-server-bastionado fail2ban-server[2519]: Server ready
Lines 1-14/14 (END)
^C
root@Ubuntu-server-bastionado:~# fail2ban-client -V
1.0.2
root@Ubuntu-server-bastionado:~#
```

b) Haciendo uso de la configuración por defecto (/etc/fail2ban/jail.conf): **(2 puntos)**

i. Evidenciar que se produce un bloqueo después de X intentos fallidos desde Windows anfitrión mediante comando ssh manualmente (o bucle), según configuración por defecto. Fichero /var/log/auth, cliente de fail2ban (fail2ban-client status sshd).

```
GNU nano 7.2 /etc/fail2ban/jail.conf
# can be defined using space (and/or comma) separator.
#ignoreip = 127.0.0.1/8 ::1

# External command that will take an tagged arguments to ignore, e.g. <ip>,
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime = 10m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 10m

# "maxretry" is the number of failures before a host get banned.
maxretry = 5

# "maxmatches" is the number of matches stored in ticket (resolvable via tag <matches> in actions).
maxmatches = %(maxretry)s

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#
# pyinotify: requires pyinotify (a file alteration monitor) to be installed.
# If pyinotify is not installed, Fail2ban will use auto.
```

Álvaro Almellones Fernández

```
Símbolo del sistema X + -
C:\Users\alvar>ssh almellonesfernandez@192.168.1.110
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de
este sistema informático
Ubuntu 24.04.1 LTS
almellonesfernandez@192.168.1.110's password:
Permission denied, please try again.
almellonesfernandez@192.168.1.110's password:
Permission denied, please try again.
almellonesfernandez@192.168.1.110's password:
almellonesfernandez@192.168.1.110: Permission denied (publickey,password).

C:\Users\alvar>ssh almellonesfernandez@192.168.1.110
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de
este sistema informático
Ubuntu 24.04.1 LTS
almellonesfernandez@192.168.1.110's password:
Permission denied, please try again.
almellonesfernandez@192.168.1.110's password:
Permission denied, please try again.
almellonesfernandez@192.168.1.110's password:
ssh_dispatch_run_fatal: Connection to 192.168.1.110 port 22: Connection timed out

C:\Users\alvar>
```

Como podemos observar a la quinta vez que fallo la contraseña , al intentar una sexta no me deja

```
root@Ubuntu-server-bastionado:~/scripts# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 5
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| |- Currently banned: 1
| |- Total banned: 1
| \- Banned IP list: 192.168.1.106
root@Ubuntu-server-bastionado: ~/scripts# _
```

La captura se ve en negro ya que al banearme la ip no podía acceder al server desde el Moba tampoco

ii. Evidenciar que se produce un desbloqueo automáticamente pasado el tiempo determinado en el fichero por defecto.

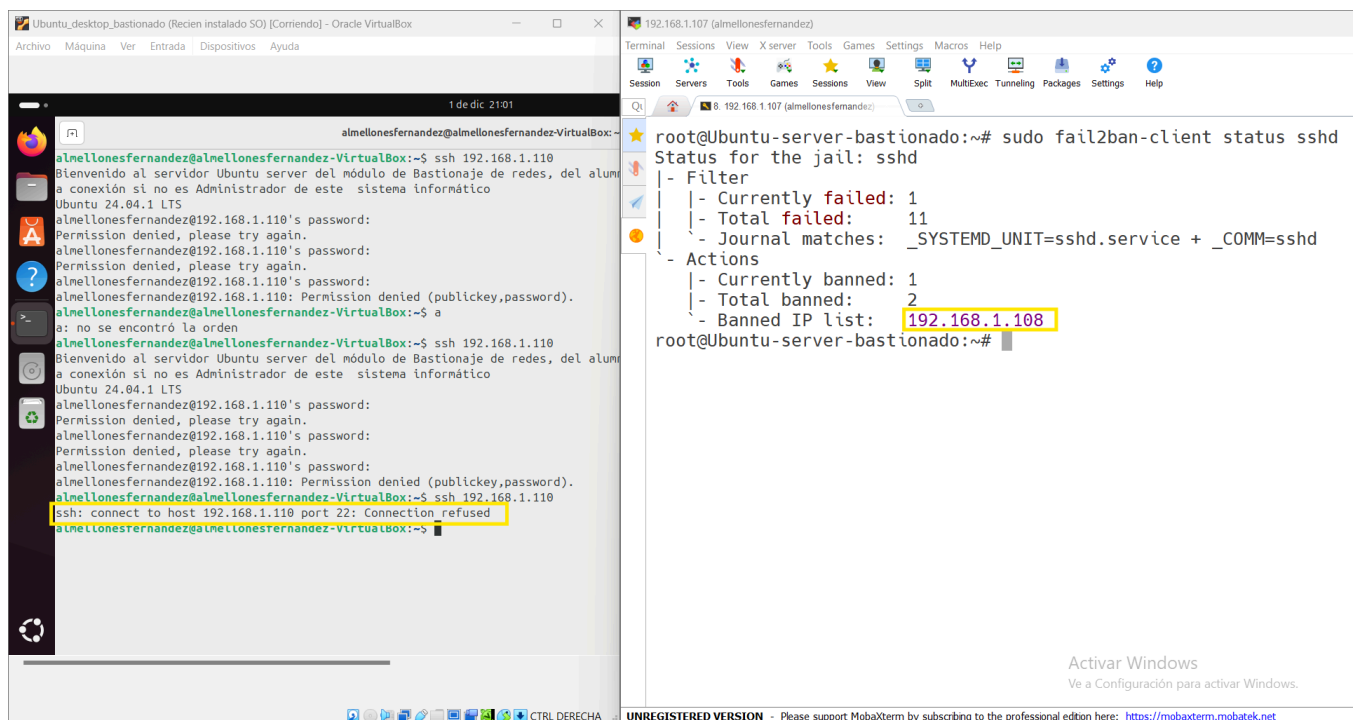
```
root@Ubuntu-server-bastionado:~/scripts# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 5
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| |- Currently banned: 1
| |- Total banned: 1
| \- Banned IP list: 192.168.1.106
root@Ubuntu-server-bastionado: ~/scripts# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 5
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| |- Currently banned: 0
| |- Total banned: 1
| \- Banned IP list:
root@Ubuntu-server-bastionado:~/scripts# _
```


Álvaro Almellones Fernández

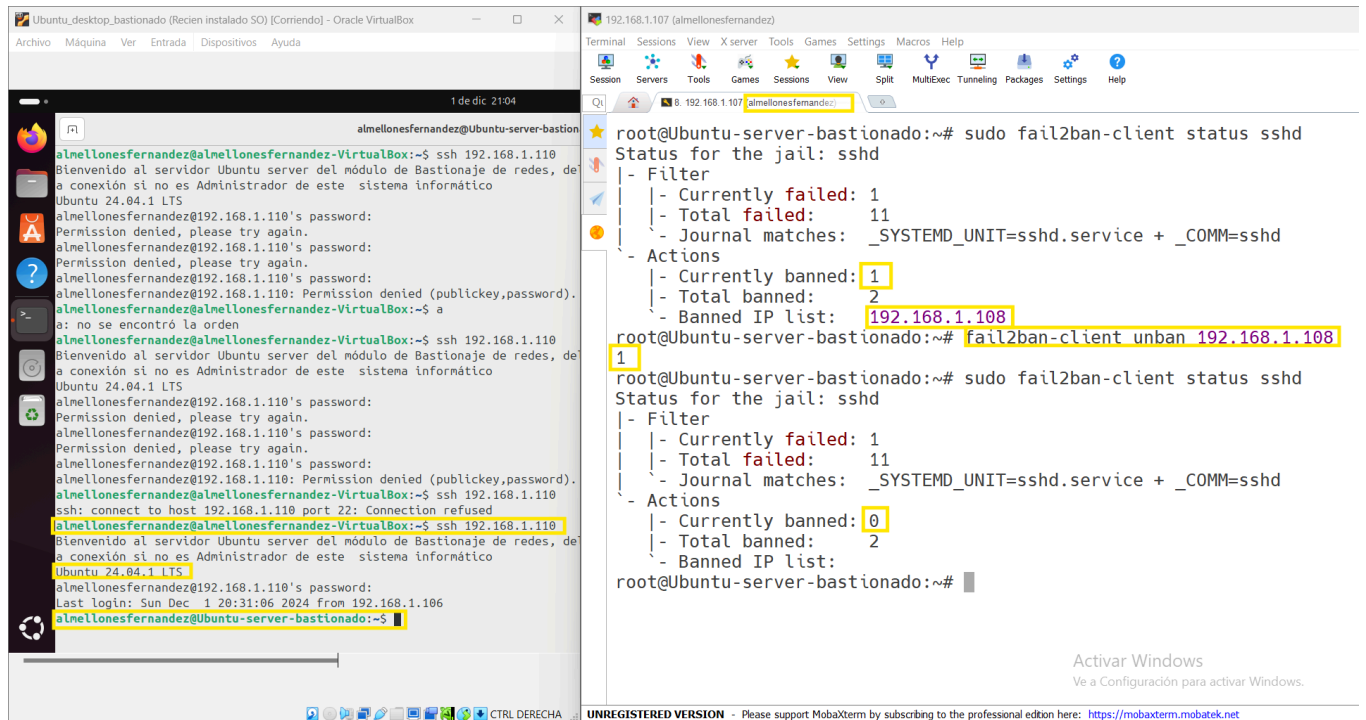
```
almellonesfernandez@Ubuntu x + v
C:\Users\alvar> ssh almellonesfernandez@192.168.1.110
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
almellonesfernandez@192.168.1.110's password:
Last login: Sun Dec 1 19:51:00 2024 from 192.168.1.106
almellonesfernandez@Ubuntu-server-bastionado:~$ sudo fail2ban-client status sshd
[sudo] password for almellonesfernandez:
Status for the jail: sshd
|- Filter
| - Currently failed: 0
| - Total failed: 5
| - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
-- Actions
| - Currently banned: 0
| - Total banned: 1
| - Banned IP list:
almellonesfernandez@Ubuntu-server-bastionado:~$
```

Ya me deja acceder desde el Moba y se observa que actualmente no esta la ip baneada pero en Total banned se queda guardado como que se ha baneado una ip

iii. Evidenciar el bloqueo de nuevo, y desbloquear mediante comando (#fail2ban-client unban).



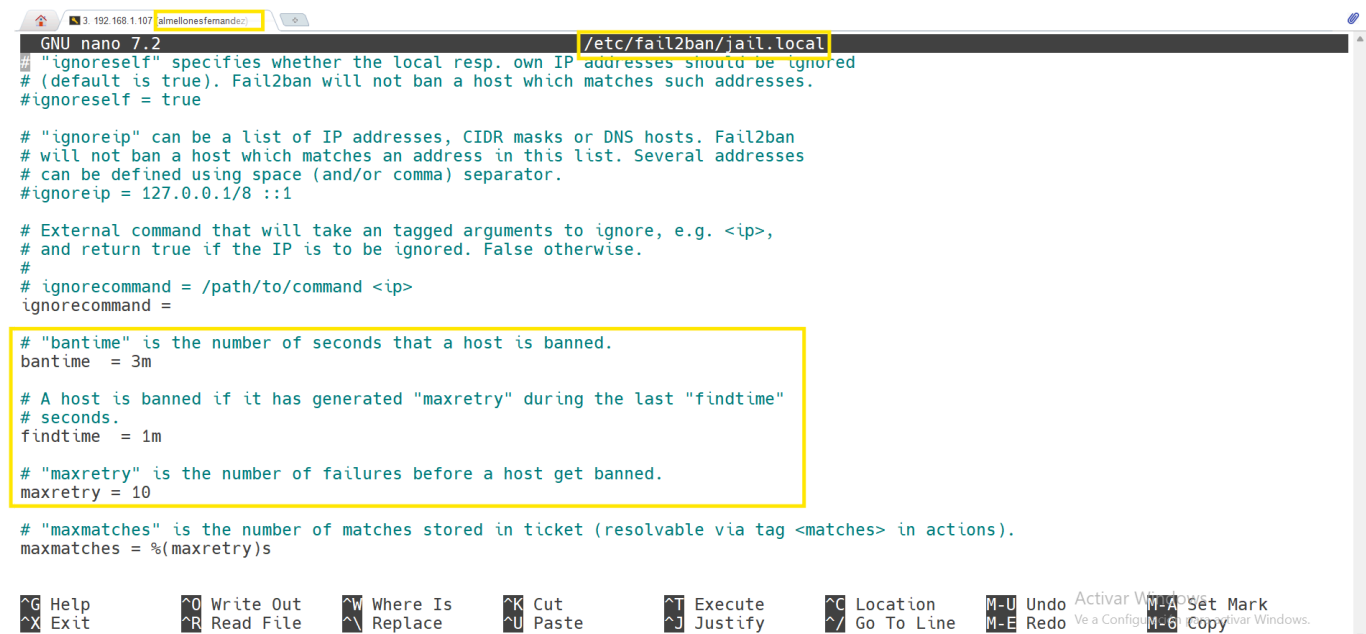
Esta vez he usado Ubuntu Desktop para banear la ip pa que las capturas se vean en fondo blanco



```
almellonesfernandez@Ubuntu-server-bastionado:~$ ssh 192.168.1.110
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, de
a conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
almellonesfernandez@192.168.1.110's password:
Permission denied, please try again.
almellonesfernandez@192.168.1.110's password:
Permission denied, please try again.
almellonesfernandez@192.168.1.110: Permission denied (publickey,password).
almellonesfernandez@Ubuntu-server-bastionado:~$ a
a: no se encontró la orden
almellonesfernandez@Ubuntu-server-bastionado:~$ ssh 192.168.1.110
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, de
a conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
almellonesfernandez@192.168.1.110's password:
Permission denied, please try again.
almellonesfernandez@192.168.1.110's password:
Permission denied, please try again.
almellonesfernandez@192.168.1.110: Permission denied (publickey,password).
almellonesfernandez@Ubuntu-server-bastionado:~$ ssh 192.168.1.110
ssh: connect to host 192.168.1.110 port 22: Connection refused
almellonesfernandez@Ubuntu-server-bastionado:~$ ssh 192.168.1.110
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, de
a conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
almellonesfernandez@192.168.1.110's password:
Last login: Sun Dec 1 20:31:06 2024 from 192.168.1.106
almellonesfernandez@Ubuntu-server-bastionado:~$
```

```
root@Ubuntu-server-bastionado:~# sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| - Currently failed: 1
| - Total failed: 11
| - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| - Currently banned: 1
| - Total banned: 2
| - Banned IP list: 192.168.1.108
root@Ubuntu-server-bastionado:~# fail2ban-client unban 192.168.1.108
1
root@Ubuntu-server-bastionado:~# sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| - Currently failed: 1
| - Total failed: 11
| - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| - Currently banned: 0
| - Total banned: 2
| - Banned IP list:
root@Ubuntu-server-bastionado:~#
```

c) Haciendo uso de una configuración personalizada (/etc/fail2ban/jail.local) (nº de intentos de 10 por cada minuto y banear durante 3 minutos, usando iptables (#watch iptables -L -n -v): (2 puntos)



```
GNU nano 7.2 /etc/fail2ban/jail.local
# "ignoreself" specifies whether the local resp. own IP addresses should be ignored
# (default is true). Fail2ban will not ban a host which matches such addresses.
# ignoreself = true

# "ignoreip" can be a list of IP addresses, CIDR masks or DNS hosts. Fail2ban
# will not ban a host which matches an address in this list. Several addresses
# can be defined using space (and/or comma) separator.
# ignoreip = 127.0.0.1/8 ::1

# External command that will take an tagged arguments to ignore, e.g. <ip>,
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime = 3m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 1m

# "maxretry" is the number of failures before a host get banned.
maxretry = 10

# "maxmatches" is the number of matches stored in ticket (resolvable via tag <matches> in actions).
maxmatches = %(maxretry)s
```

i. Evidenciar que se produce un bloqueo después de 10 intentos mediante fuerza bruta (#nmap - -script ssh-brute -p 22 <IP>) desde Ubuntu Desktop y se añaden reglas de iptables (#watch iptables -L -n -v), Fichero /var/log/auth, cliente de fail2ban (fail2ban-client status sshd).

Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
15 936 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:21
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306
0 0 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 LOG flags 0 level 4 prefix "Inte
ntos-ataque-SSH Server-al"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306 LOG flags 0 level 4 prefix "In
tentos-ataque-mysql-almello"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80 LOG flags 0 level 4 prefix "Inte
ntos-ataque-Web-Server-al"

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT 0 -- * * lo 0.0.0.0/0 0.0.0.0/0
10 912 ACCEPT 0 -- * * enp0s3 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 ACCEPT 1 -- * * enp0s3 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT 17 -- * * enp0s3 0.0.0.0/0 0.0.0.0/0 udp dpt:53
0 0 ACCEPT 6 -- * * enp0s3 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
0 0 ACCEPT 6 -- * * enp0s3 0.0.0.0/0 0.0.0.0/0 tcp dpt:443
0 0 ACCEPT 17 -- * * enp0s3 0.0.0.0/0 193.204.114.231 udp dpt:123
0 0 ACCEPT 17 -- * * enp0s3 0.0.0.0/0 216.239.35.0 udp dpt:123
0 0 ACCEPT 6 -- * * enp0s3 0.0.0.0/0 0.0.0.0/0 tcp dpt:25
```

REGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

```
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez# nmap --script
ssh-brute -p 22 192.168.1.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 13:15 CET
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: user:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456

root@Ubuntu-server-bastionado:~/scripts# fail2ban-client status s
Status for the jail: sshd
- Filter
| - Currently failed: 0
| - Total failed: 355
| - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| - Currently banned: 0
| - Total banned: 4
| - Banned IP list:
root@Ubuntu-server-bastionado:~/scripts# fail2ban-client status s
Status for the jail: sshd
- Filter
| - Currently failed: 1
| - Total failed: 403
| - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| - Currently banned: 1
| - Total banned: 5
| - Banned IP list: 192.168.1.108
root@Ubuntu-server-bastionado:~/scripts#
```

```
root@Ubuntu-server-bastionado:~/scripts# tail -f /var/log/auth.log
2024-12-03T13:22:05.765673+01:00 Ubuntu-server-bastionado sshd[2249]: Invalid user test from 192.168.1.108 port 44180
2024-12-03T13:22:05.765777+01:00 Ubuntu-server-bastionado sshd[2249]: Failed none for invalid user test from 192.168.1.108 port 4418
0 ssh2
2024-12-03T13:22:05.786353+01:00 Ubuntu-server-bastionado sshd[2232]: Failed password for invalid user test from 192.168.1.108 port
44014 ssh2
2024-12-03T13:22:05.822743+01:00 Ubuntu-server-bastionado sshd[2248]: Connection closed by invalid user web 192.168.1.108 port 44162
[preauth]
2024-12-03T13:22:05.886183+01:00 Ubuntu-server-bastionado sshd[2249]: Connection closed by invalid user test 192.168.1.108 port 4418
0 [preauth]
2024-12-03T13:22:05.942278+01:00 Ubuntu-server-bastionado sshd[2232]: Connection closed by invalid user test 192.168.1.108 port 4401
4 [preauth]
2024-12-03T13:22:06.169253+01:00 Ubuntu-server-bastionado sshd[2256]: Invalid user admin from 192.168.1.108 port 44260
2024-12-03T13:22:06.169447+01:00 Ubuntu-server-bastionado sshd[2256]: error: Could not get shadow information for NOUSER
2024-12-03T13:22:06.169670+01:00 Ubuntu-server-bastionado sshd[2253]: Failed password for root from 192.168.1.108 port 44234 ssh2
2024-12-03T13:22:06.169962+01:00 Ubuntu-server-bastionado sshd[2256]: Failed password for invalid user admin from 192.168.1.108 port
44260 ssh2
```

```

Every 2.0s: iptables -L -n -v
Chain INPUT (policy DROP 49 packets, 2653 bytes)
pkts bytes target prot opt in out source destination
318 40884 f2b-sshd 6 -- * * 0.0.0.0/0 0.0.0.0/0 multiport dports 22
8 753 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
745 103K ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:21
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
0 0 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306
2 56 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
2 275 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 LOG flags 0 level 4 prefix "Inte
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-SSH Server-al"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306 LOG flags 0 level 4 prefix "In
tentos-ataque-mysql-almello"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80 LOG flags 0 level 4 prefix "Inte
ntos-ataque-Web-Server-al"

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 15 packets, 1452 bytes)
pkts bytes target prot opt in out source destination
8 753 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
703 141K ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
2 156 ACCEPT 17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 udp dpt:53
0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 tcp dpt:443
0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 193.204.114.231 udp dpt:123
0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 216.239.35.0 udp dpt:123

```

ii. Evidenciar que se produce un desbloqueo automáticamente pasado el tiempo determinado en el fichero por defecto.

```

root@Ubuntu-server-bastionado:~/scripts# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| - Currently failed: 0
| - Total failed: 95
| - File list: /var/log/auth.log
|- Actions
| - Currently banned: 1
| - Total banned: 3
| - Banned IP list: 192.168.1.108
root@Ubuntu-server-bastionado:~/scripts# date
Wed Dec 4 11:02:20 CET 2024
root@Ubuntu-server-bastionado:~/scripts# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| - Currently failed: 0
| - Total failed: 95
| - File list: /var/log/auth.log
|- Actions
| - Currently banned: 0
| - Total banned: 3
| - Banned IP list:
root@Ubuntu-server-bastionado:~/scripts# date
Wed Dec 4 11:03:01 CET 2024
root@Ubuntu-server-bastionado:~/scripts#

```

El baneo se realizó sobre las 11 en punto pero entre que prepare para hacer la captura se muestra de primera hora las 11:02 y se desbloquea automáticamente a las 11:03 ,pero que realmente respeta los 3 minutos de baneo que se pone en la configuración

iii. Evidenciar el bloqueo de nuevo, y desbloquear mediante comando (#fail2ban-client unban IP).

Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:~/scripts# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 110
| |- File list: /var/log/auth.log
|- Actions
| |- Currently banned: 1
| |- Total banned: 4
| |- Banned IP list: 192.168.1.108
root@Ubuntu-server-bastionado:~/scripts# date
Wed Dec 4 11:08:37 CET 2024
root@Ubuntu-server-bastionado:~/scripts# fail2ban-client unban 192.168.1.108
1
root@Ubuntu-server-bastionado:~/scripts# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 110
| |- File list: /var/log/auth.log
|- Actions
| |- Currently banned: 0
| |- Total banned: 4
| |- Banned IP list:
root@Ubuntu-server-bastionado:~/scripts# date
Wed Dec 4 11:09:15 CET 2024
root@Ubuntu-server-bastionado:~/scripts#
```

Pongo la hora para que corroborar que no se desbloquee por el tiempo sino por el comando unban

iv. Realice lo anterior para quitar la regla usando comando iptables manualmente.

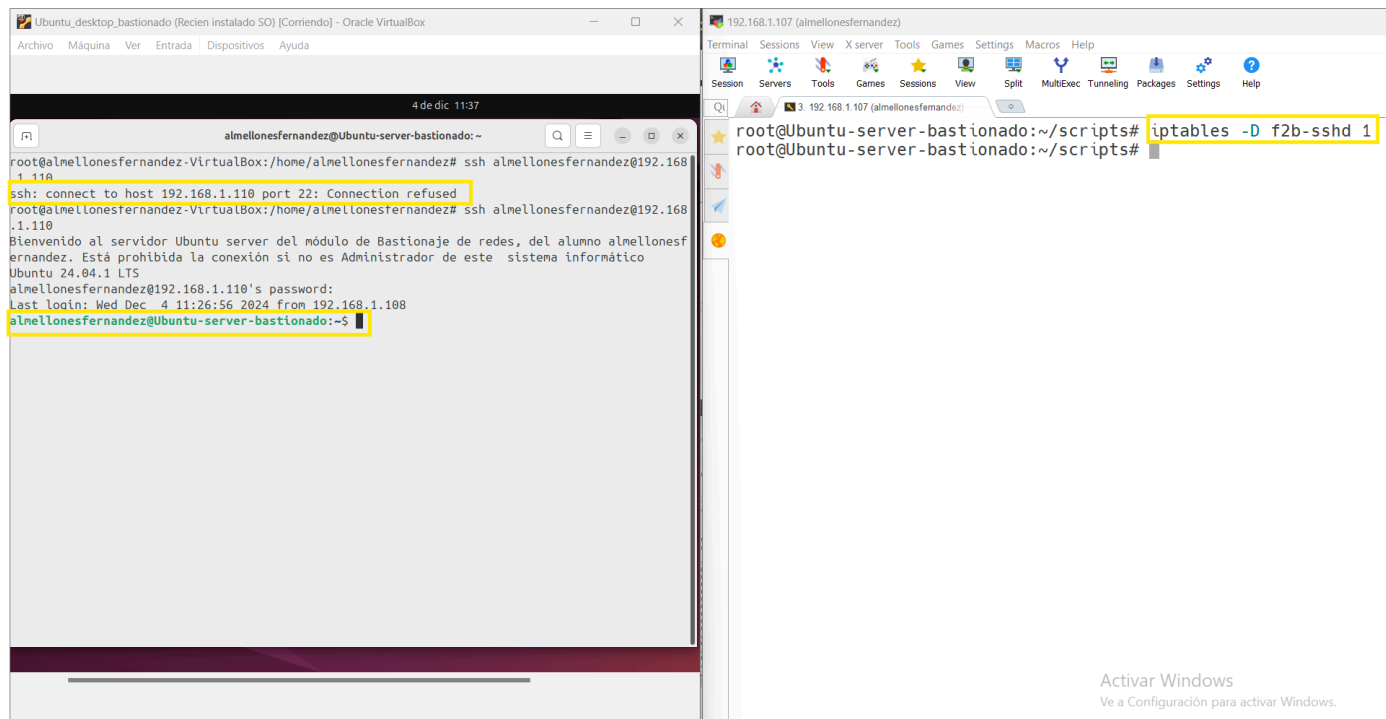
The screenshot shows a terminal window with the following content:

```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# ssh 192.168.1.110
ssh: connect to host 192.168.1.110 port 22: Connection refused
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez#
```

Below this, the terminal shows the fail2ban status and the iptables rules:

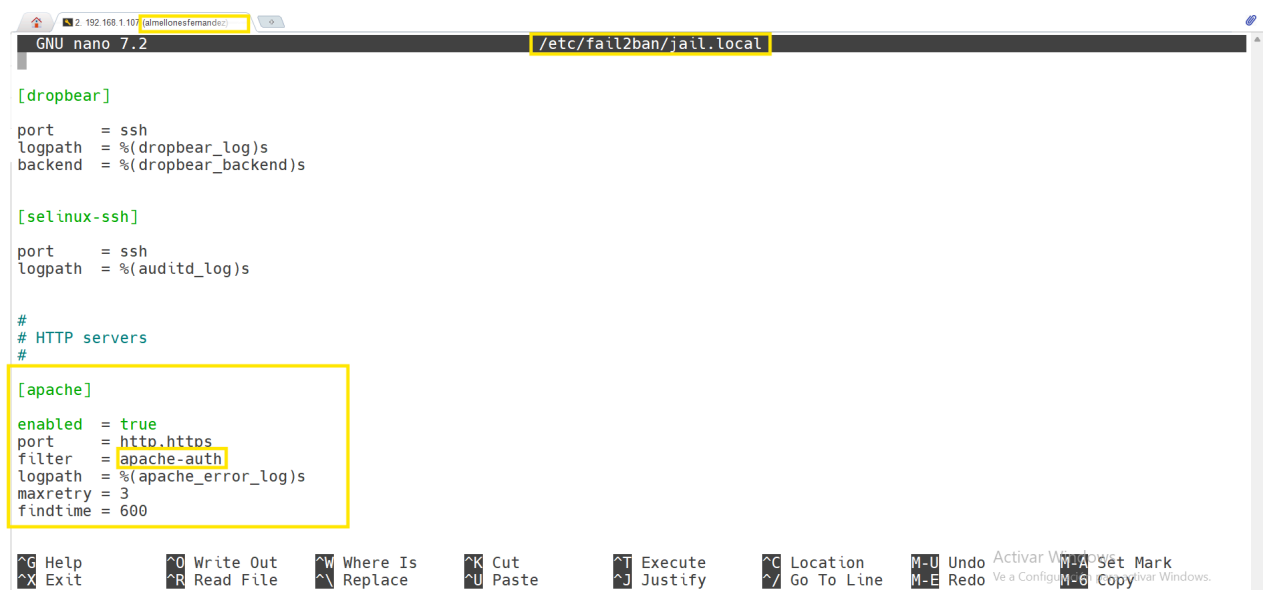
```
root@Ubuntu-server-bastionado:~/scripts# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 27
| |- File list: /var/log/auth.log
|- Actions
| |- Currently banned: 1
| |- Total banned: 4
| |- Banned IP list: 192.168.1.108
root@Ubuntu-server-bastionado:~/scripts# sudo iptables -L -n --line-numbers
Chain INPUT (policy DROP)
num target prot opt source destination multiport dpo
1 f2b-sshd 6 -- 0.0.0.0/0 0.0.0.0/0 multiport dpo
2 ACCEPT 0 -- 0.0.0.0/0 0.0.0.0/0
3 ACCEPT 6 -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
4 ACCEPT 6 -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:21
5 ACCEPT 6 -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
6 ACCEPT 6 -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306
7 ACCEPT 1 -- 0.0.0.0/0 0.0.0.0/0 state RELATED
8 ACCEPT 0 -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 LO
9 LOG 6 -- 0.0.0.0/0 0.0.0.0/0
10 LOG 6 -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306
11 LOG 6 -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:80 LO
level 4 prefix "Intentos-ataque-SSH-Server-al"
level 4 prefix "Intentos-ataque-mysql-almello"
level 4 prefix "Intentos-ataque-Web-Server-al"
```

Álvaro Almellones Fernández



Para desbloquear la ip baneada mediante iptable solo, primero miro en que linea del iptable se encuentra la regla de fail2ban y la elimino , y como podemos observar en la pantalla de Ubuntu Desktop al realizar la conexión por ssh puedo acceder sin problema

d) Investigar y evidenciar, la configuración para proteger mediante fail2ban contra fuerza bruta en autenticación básica vía web (http/https), mediante el filtro auth-filter (1,5 puntos).



Álvaro Almellones Fernández

He configurado una jail en fail2ban para apache con el filtro que trae por defecto fail2ban apache-auth

```
root@Ubuntu-server-bastionado:~# sudo nano /etc/fail2ban/jail.local
root@Ubuntu-server-bastionado:~# sudo fail2ban-client status
Status
|- Number of jail: 2
|- Jail list: apache sshd
root@Ubuntu-server-bastionado:~# sudo fail2ban-client status apache
Status for the jail: apache
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| |- File list: /var/log/apache2/error.log
|- Actions
| |- Currently banned: 0
| |- Total banned: 0
| |- Banned IP list:
root@Ubuntu-server-bastionado:~#
```

Como se puede observar ya aparecen 2 jail , la de ssh y la de apache. En principio ya estaría en funcionamiento. Lo que no he conseguido es evidenciar que bloquea la ip , porque no he conseguido añadir un usuario y contraseña al servidor para realizar el ataque a fuerza bruta de autenticación

CRITERIOS DE EVALUACIÓN	
5.a	Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.c.	Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
5.d	Se han implementado contramedidas frente a comportamientos no deseados en una red.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
7.c	Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.
7.d	Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.