

## PRÁCTICA #2

### DATOS DEL ESTUDIANTE

Nombre y apellidos	María Victoria Maldonado Bao
E-mail	mvictoriamb0425@uma.es
Grupo (A / B)	A
Fecha	10/2025

## EJERCICIO 1. FUERZA BRUTA Y CONTRAMEDIDAS

### 1.1: FUERZA BRUTA Y LISTAS NEGRAS

```
(kali@kali)~[~/Desktop]
$ hydra -l admin -P fasttrack.txt -f 192.168.122.1 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill
ses (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-25 10:43:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 262 login tries (l:1/p:262), ~17 tries per task
[DATA] attacking ssh://192.168.122.1:22/
[STATUS] 172.00 tries/min, 172 tries in 00:01h, 94 to do in 00:01h, 12 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-25 10:45:16
```

No consiguió adivinar el usuario-contraseña del router (no estaba en el archivo fasttrack.txt).

Ahora crearé 3 listas: 1-whitelist (IPs que nunca se bloquearán), 2-suspects(sospechosos pero aún no bloqueados), y 3-blocked(IPs bloqueadas sin derecho a acceso).

```
[admin@K1] > ip firewall address-list add list=whitelist address=2.2.2.254 comment="es un ordenador de confianza"
[admin@K1] > clear
bad command name clear (line 1 column 1)
[admin@K1] > ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=!whitelist
action=add-src-to-address-list address-list=suspects address-list-timeout=1h comment="SSH: Sospechosos"
[admin@K1] > ip firewall filter add chain=input src-address-list=suspects protocol=tcp dst-port=22 action=add-src-to-addr
ess-list address-list=blocked address-list-timeout=24h comment="Bloquear tras intentos repetidos"
[admin@K1] > ip firewall filter add chain=input src-address-list=blocked action=drop comment="Omitir paquetes de bloquead
os"
[admin@K1] > ip firewall address-list print
Columns: LIST, ADDRESS, CREATION-TIME
# LIST ADDRESS CREATION-TIME
;; es un ordenador de confianza
0 whitelist 2.2.2.254 2025-10-25 14:59:03
[admin@K1] > []
```

Añado el KaliLinux B (IP 2.2.2.254) en la whitelist (para comprobar luego que no bloqueará esta IP a pesar de intentar hacer luego un Brute Force Attack ya que está en la whitelist). Cualquier nuevo intento de conexión será considerado sospechoso, y tras varios intentos repetidos de inicio de sesión pasará a estar bloqueada esa IP. Los paquetes de IPs bloqueadas no serán recibidos (línea en gris👁).

Ahora haré el ataque desde la IP de la Whitelist y desde la otra IP que no está en la whitelist, veremos que será bloqueada por el router mientras que la IP de la whitelist seguirá pudiendo enviar paquetes.

```
KaliLinux SSPI A [Running] - Oracle VirtualBox
File Machine View Input Devices Help

kali@kali: ~/Desktop
Session Actions Edit View Help
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-25 10:45:16

(kali@kali)-[~/Desktop]
$ hydra -l admin -P fasttrack.txt -f 192.168.122.1 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill
egal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-25 11:10:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 262 login tries (l:1/p:262), ~17 tries per task
[DATA] attacking ssh://192.168.122.1:22/
[ERROR] could not connect to ssh://192.168.122.1:22 - Connection refused
```

El KaliLinux A, cuya IP no estaba en la whitelist, fue bloqueada por el router y no se le permite conectarse.

```
(kali@kali)-[~/Desktop]
$ hydra -l admin -P fasttrack.txt -f 192.168.122.1 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill
ses (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-25 10:43:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 262 login tries (l:1/p:262), ~17 tries per task
[DATA] attacking ssh://192.168.122.1:22/
[STATUS] 172.00 tries/min, 172 tries in 00:01h, 94 to do in 00:01h, 12 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-25 10:45:16

(kali@kali)-[~/Desktop]
$ hydra -l admin -P fasttrack.txt -f 192.168.122.1 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill
egal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-25 11:10:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 262 login tries (l:1/p:262), ~17 tries per task
[DATA] attacking ssh://192.168.122.1:22/
[ERROR] could not connect to ssh://192.168.122.1:22 - Connection refused

(kali@kali)-[~/Desktop]
```

ANTES DE CREAR LAS LISTAS

DESPUES

Sin embargo, veremos que esto no afecta al KaliLinux B cuya IP está en la whitelist (no es bloqueado):

```
KaliLinux SSPI B [Running] - Oracle VirtualBox
File Machine View Input Devices Help

kali@kali: ~/Desktop
Session Actions Edit View Help
fasttrack.txt

(kali@kali)-[~/Desktop]
$ hydra -l admin -P fasttrack.txt -f 192.168.122.1 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bind
ing, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-25 11:19:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 262 login tries (l:1/p:262), ~17 tries per task
[DATA] attacking ssh://192.168.122.1:22/
[STATUS] 256.00 tries/min, 256 tries in 00:01h, 8 to do in 00:01h, 14 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-25 11:20:07

(kali@kali)-[~/Desktop]
```

NO FUE BLOQUEADO

Ahora lo hacemos pero en vez de con listas con la técnica del jump-target y return (nos dará el mismo resultado):

```
[admin@t1] > ip firewall filter add chain=input action=jump jump-target=bruteforce-check comment="Saltar a la revisin de fuerza bruta"
[admin@t1] > add chain=bruteforce-check protocol=tcp dst-port=22 connection-state=new src-address-list=!whitelist action=add-src-to-address-list address-list=suspects address-list-timeout=1h comment="Sospechoso"
bad command name add (line 1 column 1)
[admin@t1] > ip firewall filter add chain=bruteforce-check protocol=tcp dst-port=22 connection-state=new src-address-list=!whitelist action=add-src-to-address-list address-list=suspects address-list-timeout=1h comment="Sospechoso"
[admin@t1] > ip firewall filter add chain=bruteforce-check src-address-list=suspects action=add-src-to-address-list address-list=blocked address-list-timeout=24h comment="Bloquear si es muy sospechoso"
[admin@t1] > ip firewall filter add chain=bruteforce-check src-address-list=blocked action=drop comment="Ignorar paquetes de IPs bloqueadas"
[admin@t1] > ip firewall filter add chain=bruteforce-check action=return comment="Todo ok"
[admin@t1] > []
```

(Los resultados tras volver a realizar ambos ataques son los mismos que con las listas anteriores).

/export de las reglas (están “duplicadas” porque están con ambos métodos):

```
/ip firewall filter
add action=add-src-to-address-list address-list=suspects address-list-timeout=1h chain=input comment=\
"SSH: Sospechosos" connection-state=new dst-port=22 protocol=tcp src-address-list=!whitelist
add action=add-src-to-address-list address-list=blocked address-list-timeout=1d chain=input comment=\
"Bloquear tras intentos repetidos" dst-port=22 protocol=tcp src-address-list=suspects
add action=drop chain=input comment="Omitir paquetes de bloqueados" src-address-list=blocked
add action=jump chain=input comment="Saltar a la revisin de fuerza bruta" jump-target=bruteforce-check
add action=add-src-to-address-list address-list=suspects address-list-timeout=1h chain=bruteforce-check comment=\
Sospechoso connection-state=new dst-port=22 protocol=tcp src-address-list=!whitelist
add action=add-src-to-address-list address-list=blocked address-list-timeout=1d chain=bruteforce-check comment=\
"Bloquear si es muy sospechoso" src-address-list=suspects
add action=drop chain=bruteforce-check comment="Ignorar paquetes de IPs bloqueadas" src-address-list=blocked
add action=return chain=bruteforce-check comment="Todo ok"
```

## 1.2: PORT-KNOCKING (GOLPEO DE PUERTO)

```
[admin@t1] > ip firewall filter add chain=input protocol=tcp dst-port=831 action=add-src-to-address-list address-list=kno
ck1 address-list-timeout=15s comment="portknock1"
[admin@t1] > ip firewall filter add chain=input protocol=tcp dst-port=841 action=add-src-to-address-list address-list=kno
ck2 address-list-timeout=15s comment="portknock2"
[admin@t1] > ip firewall filter add chain=input protocol=tcp dst-port=851 action=add-src-to-address-list address-list=ssh
_access address-list-timeout=1m comment="Permitir SSH tras portknock"
[admin@t1] > ip firewall filter add chain=input protocol=tcp dst-port=22 action=drop comment="drop por defecto"
```

En la primera línea establecemos el primer paso de la secuencia del portknock (831->841->851), que si luego haces knock al segundo puerto correctamente (841) pasa a la siguiente línea que si haces knock al puerto 851 ya te permite acceso a SSH. Si fallas el portknock o haces knock al puerto ssh sin el portknock, se “droppea” el paquete por defecto.

```
(kali@kali)-[~]
$ knock 192.168.122.1 831 841 851

(kali@kali)-[~]
$ ssh admin@192.168.122.1
```

Esto es lo que pasa cuando falla el portknocking:

```
(kali@kali)-[~]
$ ssh usuario@192.168.122.1
ssh: connect to host 192.168.122.1 port 22: Connection refused
```

/export de las reglas del firewall:

```
/ip firewall filter
```



```
add action=add-src-to-address-list address-list=knock1 address-list-timeout=15s chain=input comment=portknock1 \
dst-port=831 protocol=tcp
add action=add-src-to-address-list address-list=knock2 address-list-timeout=15s chain=input comment=portknock2 \
dst-port=841 protocol=tcp
add action=add-src-to-address-list address-list=ssh_access address-list-timeout=1m chain=input comment=\
"Permitir SSH tras portknock" dst-port=851 protocol=tcp
add action=drop chain=input comment="drop por defecto" dst-port=22 protocol=tcp
/ip firewall nat
```

## EJERCICIO 2. OPENVPN

Establecemos una comunicación entre ambos en el puerto 4444:

```
KaliLinux SSPI A [Running] - Oracle VirtualBox
File Machine View Input Devices
(kali@kali)-[~]
$ nc -l -p 4444
mimi
esto es una prueba
```

```
KaliLinux SSPI B [Running] - Oracle VirtualBox
File Machine View Input Devices
$ nc 1.1.1.254 4444
mimi
esto es una prueba
```

Vemos que estos mensajes se transmiten en claro, sin cifrado (subrayo el mensaje en amarillo, se observa abajo a la izquierda en los paquetes desde Wireshark):

5	1.408543	1.1.1.254	1.1.1.1	TCP	71	4444 → 53024 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=5 TSval=1467398035 TSecr=570683001	
6	1.410919	1.1.1.1	1.1.1.254	TCP	66	53024 → 4444 [ACK] Seq=1 Ack=6 Win=126 Len=0 TSval=570827676 TSecr=1467398035	
7	6.130795	1.1.1.1	1.1.1.254	TCP	85	53024 → 4444 [PSH, ACK] Seq=1 Ack=6 Win=126 Len=19 TSval=570832399 TSecr=1467398035	
8	6.132696	1.1.1.254	1.1.1.1	TCP	66	4444 → 53024 [ACK] Seq=6 Ack=20 Win=128 Len=0 TSval=1467402762 TSecr=570832399	
9	6.430413	0c:04:20:b0:00:01	PCSSystemtec_dd:4d:4f	ARP	42	Who has 1.1.1.254? Tell 1.1.1.1	
10	6.432105	PCSSystemtec_dd:4d:4f	0c:04:20:b0:00:01	ARP	60	1.1.1.254 is at 08:00:27:dd:4d:4f	
11	30.004268	fe80::e04:20ff:feb0::ff02::1	MNDP	204	5678 → 5678 Len=142		
12	30.004714	1.1.1.1	255.255.255.255	MNDP	184	5678 → 5678 Len=142	
13	30.005396	0c:04:20:b0:00:01	CDP/VTP/DTP/PagP/UD...	CDP	116	Device ID: R1 Port ID: ether2	

> Frame 5: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface -, id 0

> Ethernet II, Src: PCSSystemtec\_dd:4d:4f (08:00:27:dd:4d:4f), Dst: 0c:04:20:b0:00:01 (0c:04:20:b0:00:01)

> Internet Protocol Version 4, Src: 1.1.1.254, Dst: 1.1.1.1

> Transmission Control Protocol, Src Port: 4444, Dst Port: 53024, Seq: 1, Ack: 1, Len: 5

> Data (5 bytes)

0000 0c 04 20 b0 00 01 08 00 27 dd 4d 4f 08 00 45 00 ...MO..E..

0010 00 39 73 7c 40 00 40 06 c2 42 01 01 01 fe 01 01 ...s|@.?.B.....

0020 01 01 11 5c cf 20 bb be b3 32 b7 48 00 49 80 18 ...\.H.I...7...

0030 00 7e 6c cf 00 00 01 01 08 0a 22 06 36 0f 57 76 ...l....."6.Wv

0040 b7 93 65 73 74 6f 20 65 73 20 75 6e 61 20 70 72 ...esto e s una pr

0050 75 65 62 61 0a ueba

4	0.002139	0c:04:20:b0:00:01	LLDP_Multicast	LLDP	153	MA/0c:04:20:b0:00:00 IN/ether2 121 SysN=R1 SysD=MikroTik RouterOS 7.16 (stable) 2024-09-20 13:00:27 CHR	
5	1.408543	1.1.1.254	1.1.1.1	TCP	71	4444 → 53024 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=5 TSval=1467398035 TSecr=570683001	
6	1.410919	1.1.1.1	1.1.1.254	TCP	66	53024 → 4444 [ACK] Seq=1 Ack=6 Win=126 Len=0 TSval=570827676 TSecr=1467398035	
7	6.130795	1.1.1.1	1.1.1.254	TCP	85	53024 → 4444 [PSH, ACK] Seq=1 Ack=6 Win=126 Len=19 TSval=570832399 TSecr=1467398035	
8	6.132696	1.1.1.254	1.1.1.1	TCP	66	4444 → 53024 [ACK] Seq=6 Ack=20 Win=128 Len=0 TSval=1467402762 TSecr=570832399	

> Frame 7: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface -, id 0

> Ethernet II, Src: 0c:04:20:b0:00:01 (0c:04:20:b0:00:01), Dst: PCSSystemtec\_dd:4d:4f (08:00:27:dd:4d:4f)

> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 1.1.1.254

> Transmission Control Protocol, Src Port: 53024, Dst Port: 4444, Seq: 1, Ack: 6, Len: 19

> Data (19 bytes)

Data: 6573746f20657320756e61207072756562610a

[Length: 19]

0000 08 00 27 dd 4d 4f 0c 04 20 b0 00 01 08 00 45 00 ...MO..E..

0010 00 47 d9 0d 40 00 3f 06 5d a3 01 01 01 01 01 01 ...G..@.?.].....

0020 01 fe cf 20 11 5c b7 48 00 49 bb be b3 37 80 18 ...\.H.I...7...

0030 00 7e 6c cf 00 00 01 01 08 0a 22 06 36 0f 57 76 ...l....."6.Wv

0040 b7 93 65 73 74 6f 20 65 73 20 75 6e 61 20 70 72 ...esto e s una pr

0050 75 65 62 61 0a ueba

Observamos que sin VPN, los mensajes se envían sin cifrar.

Ahora configuramos la VPN primero en el servidor (KaliLinux A):

```
(kali@kali)-[~]
$ cd /etc/openvpn
(kali@kali)-[/etc/openvpn]
$ sudo mkdir easy-rsa
(kali@kali)-[/etc/openvpn]
$ cd easy-rsa
(kali@kali)-[/etc/openvpn/easy-rsa]
$ make-cadir ~/openvpn-ca
(kali@kali)-[/etc/openvpn/easy-rsa]
$ cd ~/openvpn-ca
(kali@kali)-[~/openvpn-ca]
$ ./easyrsa init-pki
Using Easy-RSA 'vars' configuration:
* /home/kali/openvpn-ca/vars

Notice
'init-pki' complete; you may now create
your own CA keys and certificates.

Your newly created PKI dir is:
* /home/kali/openvpn-ca/pki

Using Easy-RSA configuration:
* /home/kali/openvpn-ca/vars
(kali@kali)-[~/openvpn-ca]
$ ./easyrsa build-ca
```

```
(kali@kali)-[~/openvpn-ca]
$ ./easyrsa sign-req client client1
Using Easy-RSA 'vars' configuration:
* /home/kali/openvpn-ca/vars
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
You are about to sign the following certificate:

Requested CN: 'usuario'
Requested type: 'client'
Valid for: '825' days

-----
subject=
Common Name = usuario

Type the word 'yes' to continue, or any other input to abort.
Confirm requested details: yes

Using configuration from /home/kali/openvpn-ca/pki/66ff3c55/temp.02
Enter pass phrase for /home/kali/openvpn-ca/pki/private/ca.key:
Check that the request matches the signature
Signature OK
The Subject's Distinguished Name is as follows
Common Name : ASN.1 12: 'usuario'
Certificate is to be certified until Jan 29 18:01:00 2028 GMT (825 days)

Write out database with 1 new entries
Database updated

WARNING:
INCOMPLETE inline file created:
* /home/kali/openvpn-ca/pki/inline/private/client1.inline

Notice
Certificate created at:
* /home/kali/openvpn-ca/pki/issued/client1.crt

(kali@kali)-[~/openvpn-ca]
$ sudo cp pki/ca.crt pki/dh.pem pki/issued/server.crt pki/private/server.key /etc/openvpn/
```

```
(kali@kali)-[~/openvpn-ca]
$ ./easyrsa gen-req server nopass
Using Easy-RSA 'vars' configuration:
* /home/kali/openvpn-ca/vars
Generating DH parameters, 2048 bit lo
```

```
(kali@kali)-[~/openvpn-ca]
$ ./easyrsa gen-dh
Using Easy-RSA 'vars' configuration:
* /home/kali/openvpn-ca/vars
Generating DH parameters, 2048 bit lo
```

```
(kali@kali)-[~/openvpn-ca]
$ ./easyrsa gen-req client1 nopass
```



Observamos el estado del servidor VPN recién montado:

```
(kali@kali)~[/openvpn-ca]
$ sudo systemctl start openvpn@server

(kali@kali)~[/openvpn-ca]
$ sudo systemctl enable openvpn@server
^[[D^[[DCreated symlink '/etc/systemd/system/multi-user.target.wants/openvpn@server.service' -> '/usr/lib/systemd/system/openvpn@.service'.

(kali@kali)~[/openvpn-ca]
$ sudo systemctl status openvpn@server
● openvpn@server.service - OpenVPN connection to server
   Loaded: loaded (/usr/lib/systemd/system/openvpn@.service; enabled; preset: disabled)
   Active: active (running) since Sun 2025-10-26 14:05:36 EDT; 14s ago
 Invocation: c9e111d309564b39936c8d377f484a33
    Docs: man:openvpn(8)
          https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
          https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 3338 (openvpn)
   Status: "Initialization Sequence Completed"
     Tasks: 1 (limit: 10)
    Memory: 3.4M (peak: 3.6M)
       CPU: 28ms
    CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
            └─3338 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/server.status 10 --cd /etc/openvpn --config /etc/openvpn/server.conf --w

Oct 26 14:05:36 kali ovpn-server[3338]: net_addr_ptp_v4 add: 10.8.0.1 peer 10.8.0.2 dev tun0
Oct 26 14:05:36 kali ovpn-server[3338]: net_route_v4 add: 10.8.0.0/24 via 10.8.0.2 dev [NULL] table 0 metric -1
Oct 26 14:05:36 kali ovpn-server[3338]: Could not determine IPv4/IPv6 protocol. Using AF_INET
Oct 26 14:05:36 kali ovpn-server[3338]: Socket Buffers: R=[212992→212992] S=[212992→212992]
Oct 26 14:05:36 kali ovpn-server[3338]: UDPv4 link local (bound): [AF_INET][undef]:1194
Oct 26 14:05:36 kali ovpn-server[3338]: UDPv4 link remote: [AF_UNSPEC]
Oct 26 14:05:36 kali ovpn-server[3338]: MULTI: multi_init called, r=256 v=256
Oct 26 14:05:36 kali ovpn-server[3338]: IFCONFIG POOL IPv4: base=10.8.0.4 size=62
Oct 26 14:05:36 kali ovpn-server[3338]: IFCONFIG POOL LIST
Oct 26 14:05:36 kali ovpn-server[3338]: Initialization Sequence Completed
[212992→212992]
ndef]:1194

e=62
```

Ahora configuramos la VPN en el cliente (KaliLinux B):

```
(kali@kali)~[/]
$ sudo chown root:root /etc/openvpn/ca.crt /etc/openvpn/client1.crt /etc/openvpn/client1.key

(kali@kali)~[/]
$ sudo chmod 600 /etc/openvpn/client1.key

(kali@kali)~[/]
$ sudo nano /etc/openvpn/client.conf

(kali@kali)~[/]
$ sudo systemctl enable --now openvpn@client
Created symlink '/etc/systemd/system/multi-user.target.wants/openvpn@client.service' -> '/usr/lib/systemd/system/openvpn@.service'.

(kali@kali)~[/]
$ sudo systemctl status openvpn@client --no-pager
● openvpn@client.service - OpenVPN connection to client
   Loaded: loaded (/usr/lib/systemd/system/openvpn@.service; enabled; preset: disabled)
   Active: active (running) since Sun 2025-10-26 14:23:50 EDT; 13s ago
 Invocation: 966ee0a196254a00880c64e01e8c9249
    Docs: man:openvpn(8)
          https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
          https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 3489 (openvpn)
   Status: "Initialization Sequence Completed"
     Tasks: 1 (limit: 10)
    Memory: 4M (peak: 4.3M)
       CPU: 30ms
    CGroup: /system.slice/system-openvpn.slice/openvpn@client.service
            └─3489 /usr/sbin/openvpn --daemon ovpn-client --status /run/openvpn/client.status 10 --cd /etc/openvpn --config /etc/openvpn/client.conf --writepid...

Oct 26 14:23:58 kali ovpn-client[3489]: ROUTE_GATEWAY 2.2.2.1/255.255.255.0 IFACE=eth1 HWADDR=08:00:27:71:91:b7
Oct 26 14:23:58 kali ovpn-client[3489]: TUN/TAP device tun0 opened
Oct 26 14:23:58 kali ovpn-client[3489]: net_iface_mtu_set: mtu 1500 for tun0
Oct 26 14:23:58 kali ovpn-client[3489]: net_iface_up: set tun0 up
Oct 26 14:23:58 kali ovpn-client[3489]: net_addr_ptp_v4 add: 10.8.0.6 peer 10.8.0.5 dev tun0
Oct 26 14:23:58 kali ovpn-client[3489]: net_route_v4 add: 10.8.0.1/32 via 10.8.0.5 dev [NULL] table 0 metric -1
Oct 26 14:23:58 kali ovpn-client[3489]: Initialization Sequence Completed
Oct 26 14:23:58 kali ovpn-client[3489]: Data Channel: cipher 'AES-256-GCM', peer-id: 0
Oct 26 14:23:58 kali ovpn-client[3489]: Timers: ping 10, ping-restart 120
Oct 26 14:23:58 kali ovpn-client[3489]: Protocol options: protocol-flags cc-exit tls-ekm dyn-tls-crypt
```

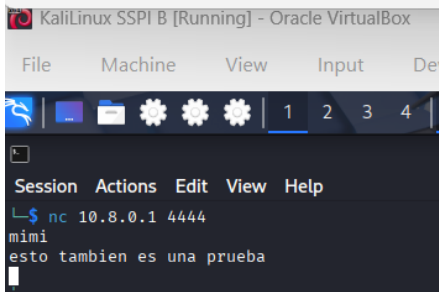
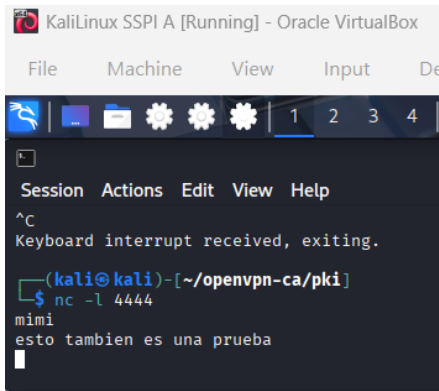
```
(kali@kali)-[~]
$ ip -brief a show tun0
tun0 UNKNOWN 10.8.0.6 peer 10.8.0.5/32 fe80::3975:7ae8:4ab:db8d/64

(kali@kali)-[~]
$ ip address show tun0
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
link/none
inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
valid_lft forever preferred_lft forever
inet6 fe80::3975:7ae8:4ab:db8d/64 scope link stable-privacy proto kernel_ll
valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ ip addr show tun0
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
link/none
inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
valid_lft forever preferred_lft forever
inet6 fe80::3975:7ae8:4ab:db8d/64 scope link stable-privacy proto kernel_ll
valid_lft forever preferred_lft forever

(kali@kali)-[~]
```

Y esto es lo que pasa si intentamos ver los paquetes al activar la VPN mientras se comunican, que esta vez la comunicación está cifrada:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	1.1.1.1	1.1.1.254	OpenVPN	123	MessageType: P_DATA_V2
2	0.002999	1.1.1.254	1.1.1.1	OpenVPN	118	MessageType: P_DATA_V2
3	0.871808	1.1.1.1	1.1.1.254	OpenVPN	114	MessageType: P_DATA_V2
4	9.178837	1.1.1.254	1.1.1.1	OpenVPN	145	MessageType: P_DATA_V2
9	11.609193	1.1.1.254	1.1.1.1	OpenVPN	145	MessageType: P_DATA_V2

> Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface -, id 0

> Ethernet II, Src: PCSSystemtec\_dd:4d:4f (08:00:27:dd:4d:4f), Dst: 0c:04:20:b0:00:01 (0c:04:20:b0:00:01)

> Internet Protocol Version 4, Src: 1.1.1.254, Dst: 1.1.1.1

> User Datagram Protocol, Src Port: 1194, Dst Port: 45816

> OpenVPN Protocol

0000	0c 04 20 b0 00 01 08 00 27 dd 4d 4f 08 00 45 00	..MO--E-
0010	00 68 ed 54 40 00 40 11 48 30 01 01 01 fe 01 01	..hT@_H0....
0020	01 01 04 aa b2 f8 00 54 80 ff 48 00 00 00 00 00	...d_@?.....
0030	00 0d 1b 4c d3 cd 75 62 39 9d fe f7 a3 0a 8c 2e	...L..ub 9.....
0040	70 69 68 bb 1e 21 6c 94 7e 9d e1 36 c9 68 23 c6	pih..ll..6.h#..
0050	c9 14 5f 91 1a cb d6 26 f3 e9 f5 1f 2f 2e 67 93	...&.../g....
0060	bc c2 8b 03 3c 9a c8 41 24 16 20 7e aa f7 73 33	...<A\$-----s3
0070	12 f0 29 1a 77 9e	...)w..

1	0.000000	1.1.1.1	1.1.1.254	OpenVPN	123	MessageType: P_DATA_V2
2	0.002999	1.1.1.254	1.1.1.1	OpenVPN	118	MessageType: P_DATA_V2
3	0.871808	1.1.1.1	1.1.1.254	OpenVPN	114	MessageType: P_DATA_V2
4	9.178837	1.1.1.254	1.1.1.1	OpenVPN	145	MessageType: P_DATA_V2
9	11.609193	1.1.1.254	1.1.1.1	OpenVPN	145	MessageType: P_DATA_V2

> Frame 3: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface -, id 0

> Ethernet II, Src: 0c:04:20:b0:00:01 (0c:04:20:b0:00:01), Dst: PCSSystemtec\_dd:4d:4f (08:00:27:dd:4d:4f)

> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 1.1.1.254

> User Datagram Protocol, Src Port: 45816, Dst Port: 1194

> OpenVPN Protocol

0000	08 00 27 dd 4d 4f 0c 04 20 b0 00 01 08 00 45 00	..MO--E-
0010	00 64 9c e3 40 00 3f 11 99 a5 01 01 01 01 01 01	..d_@?.....
0020	01 fe b2 f8 04 aa 00 50 4c 82 48 00 00 00 00 00	...P L.H.....
0030	00 12 ca 7e 85 49 0b 88 34 1e e5 71 0b ce e8 8e	...I..4..q....
0040	ed 31 e3 cf 6a 2e 60 dc 41 90 a0 6f 19 6d e2 32	..1..j..A..om2
0050	bc 91 ac e5 88 ac b3 58 4f 27 55 a7 50 0f 5e f5	...X O'U.P ^..
0060	4d 47 bb 30 1f 52 60 77 6a 6d 8b 16 6f 48 d6 ab	MG:0 R'w jm..oH..
0070	0e 23	..8

Ya no son observables los mensajes sin cifrar desde Wireshark, como hemos podido comprobar.