



M011-SEGURETAT INFORMÀTICA i ALTA SEGURETAT

UF2- Seguretat Activa i Accés remot

M011-Uf2 PRÀCTICA 7

Curs: 2018-19

CFGS: ASIX2

Alumne : Arnau Subirós Puigarnau

Data : 01-02-2019

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

M011 UF2-PRACTICA 7

PART 1 : Creació bàsica d'una VPN amb configuració de certificacions del túnel

Documentació

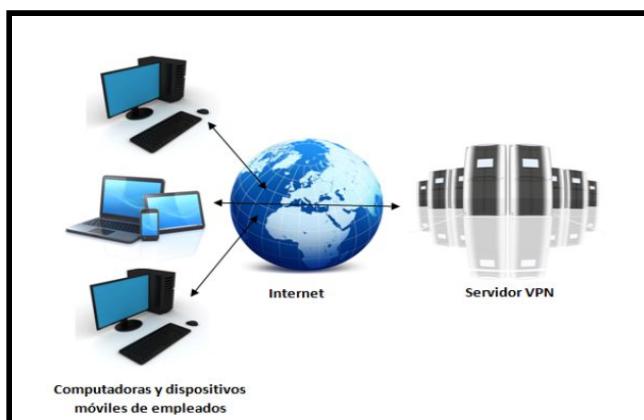
- <https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-16-04>
- https://www.youtube.com/watch?v=sd-X_y1c-F4&t=437s

Es recomana que abans de seguir amb la pràctica s'hagi fet una visualització completa del vídeo i una lectura general de la guia per tenir una idea general dels passos que es duran a terme són els mateixos.

Per a realitzar aquesta part elaboreu un document on expliqueu el procés d'instal·lació i configuració explicant amb detall i amb captures de pantalla de les vostres màquines els passos que venen a continuació

Una **VPN (Virtual Private Network)** és una tecnologia de xarxa que s'utilitza per a connectar una o més computadores a una xarxa privada utilitzant Internet.

- Les empreses solen utilitzar una VPN perquè els seus empleats des de les seves cases, hotels, etc., puguin accedir a recursos corporatius que d'una altra manera, no podrien.
- Conectar la computadora d'un empleat als recursos corporatius és només una funció d'una VPN.
- Una implementació correcta d'aquesta tecnologia permet assegurar la confidencialitat i integritat de la informació.



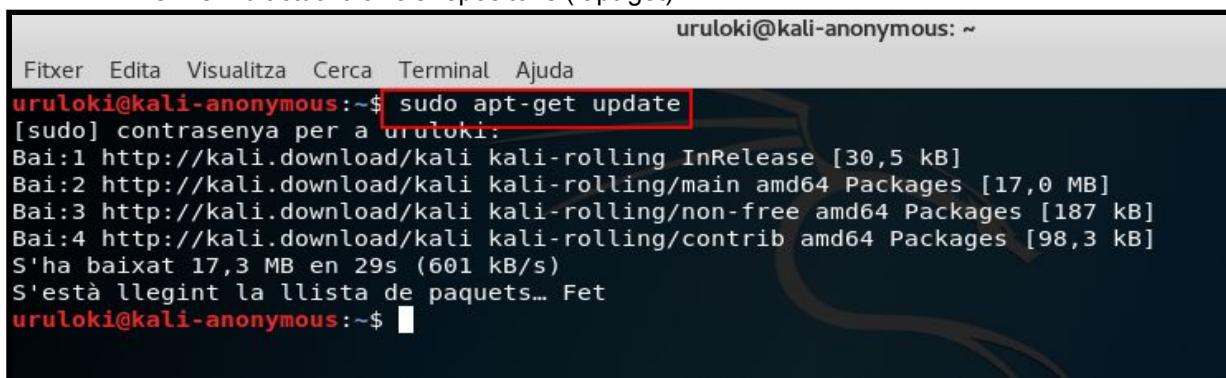
Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

En aquesta pràctica haurem de configurar el Servidor i el Client perquè pugui funcionar correctament

SERVIDOR OpenVPN

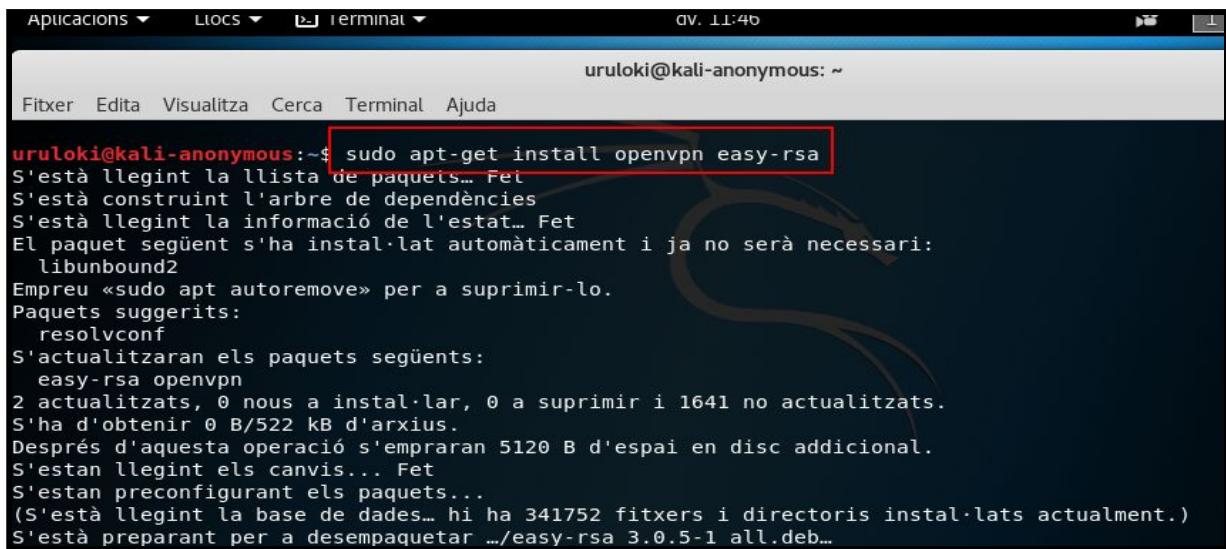
1. Instal.lar OpenVPN

- Realitzarem l'instal.lació en la màquina virtual Kali Linux
- Primer hem d'actualitzar els repositoris (apt-get)



```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo apt-get update
[sudo] contrasenya per a uruloki:
Bai:1 http://kali.download/kali kali-rolling InRelease [30,5 kB]
Bai:2 http://kali.download/kali kali-rolling/main amd64 Packages [17,0 MB]
Bai:3 http://kali.download/kali kali-rolling/non-free amd64 Packages [187 kB]
Bai:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [98,3 kB]
S'ha baixat 17,3 MB en 29s (601 kB/s)
S'està llegint la llista de paquets... Fet
uruloki@kali-anonymous:~$
```

- Instal.larem el software openvpn i easy-rsa(ens ajudarà a configurar l'autoritat de certificació

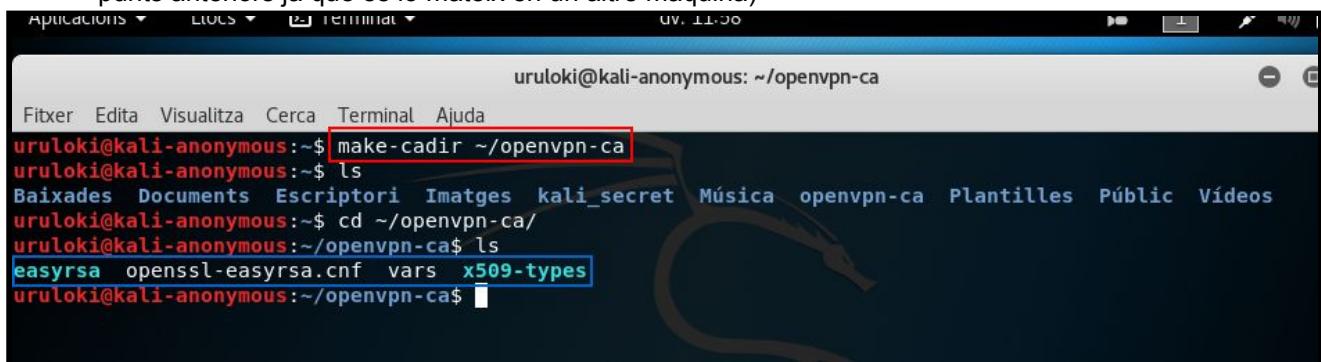


```
Aplicacions ▾ Llocs ▾ Terminal ▾ DV. 11:46
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo apt-get install openvpn easy-rsa
S'està llegint la llista de paquets... Fet
S'està construint l'arbre de dependències
S'està llegint la informació de l'estat... Fet
El paquet següent s'ha instal·lat automàticament i ja no serà necessari:
libunbound2
Empreu «sudo apt autoremove» per a suprimir-lo.
Paquets suggerits:
  resolvconf
S'actualitzaran els paquets següents:
  easy-rsa openvpn
2 actualitzats, 0 nous a instal·lar, 0 a suprimir i 1641 no actualitzats.
S'ha d'obtenir 0 B/522 kB d'arxius.
Després d'aquesta operació s'empraran 5120 B d'espai en disc addicional.
S'estan llegint els canvis... Fet
S'estan preconfigurant els paquets...
(S'està llegint la base de dades... hi ha 341752 fitxers i directoris instal·lats actualment.)
S'està preparant per a desempaquetar .../easy-rsa 3.0.5-1 all.deb...
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

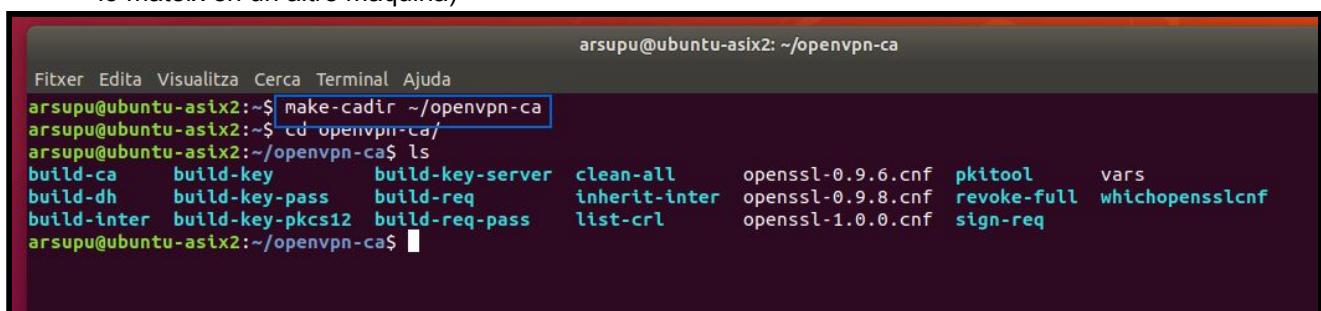
2. Configurar el directori de CA (autoritat de certificació)

- Per a començar, podem copiar el easy-*rsa directori de plantilles en el nostre directori d'inici amb el make-*cadir. He revisat els arxius i s'ha m'han instal·lat pocs respecte a la guia. I he decidit tornar a començar amb una màquina amb sistema Ubuntu. (omiteixo els punts anteriors ja que és lo mateix en un altre màquina)



```
uruloki@kali-anonymous:~/openvpn-ca
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ make-cadir ~/openvpn-ca
uruloki@kali-anonymous:~$ ls
Baixades Documents Escriptori Imatges kali_secret Música openvpn-ca Plantilles Públic Vídeos
uruloki@kali-anonymous:~$ cd ~/openvpn-ca/
uruloki@kali-anonymous:~/openvpn-ca$ ls
easyrsa openssl-easyrsa.cnf vars x509-types
uruloki@kali-anonymous:~/openvpn-ca$
```

- He revisat els arxius i s'ha m'han instal·lat pocs respecte a la guia. I he decidit tornar a començar amb una màquina amb sistema Ubuntu. (omiteixo els punts anteriors ja que és lo mateix en un altre màquina)



```
arsupu@ubuntu-asix2:~/openvpn-ca
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~$ make-cadir ~/openvpn-ca
arsupu@ubuntu-asix2:~$ cd openvpn-ca/
arsupu@ubuntu-asix2:~/openvpn-ca$ ls
build-ca build-key build-key-server clean-all openssl-0.9.6.cnf pktool vars
build-dh build-key-pass build-req inherit-inter openssl-0.9.8.cnf revoke-full whichopensslcnf
build-inter build-key-pkcs12 build-req-pass list-crl openssl-1.0.0.cnf sign-req
arsupu@ubuntu-asix2:~/openvpn-ca$
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

3. Configurar les variables de CA (autoritat de certificació)

- Ara haurem de editar l'arxiu **vars**

```

Fitxer Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.3
va

# the top level of the easy-rsa
# tree.
export EASY_RSA=`pwd`


#
# This variable should point to
# the requested executables
#
export OPENSSL="openssl"
export PKCS11TOOL="pkcs11-tool"
export GREP="grep"

# This variable should point to
# the openssl.cnf file included
# with easy-rsa.
export KEY_CONFIG="$EASY_RSA/openssl-1.0.0.cnf"

# Edit this variable to point to
# your soon-to-be-created key

```

```

GNU nano 2.9.3

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="Catalunya"
export KEY_PROVINCE="Barcelona"
export KEY_CITY="Barcelona"
export KEY_ORG="SEARS"
export KEY_EMAIL="arnausubiros@gmail.com"
export KEY_OU="Community"

# X509 Subject Field
export KEY_NAME="server"

# PKCS11 Smart Card
# export PKCS11_MODULE_PATH="/usr/lib/changeme.so"
# export PKCS11_PTN=1234

```

Nom i Cognoms	Data
Arnaud Subirós Puigarnau	01-02-2019

4. Construir la nostre CA (autoritat de certificació)

```
arsupu@ubuntu-asix2: ~/openvpn-ca
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/openvpn-ca$ source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /home/arsupu/openvpn-ca/keys
arsupu@ubuntu-asix2:~/openvpn-ca$
```

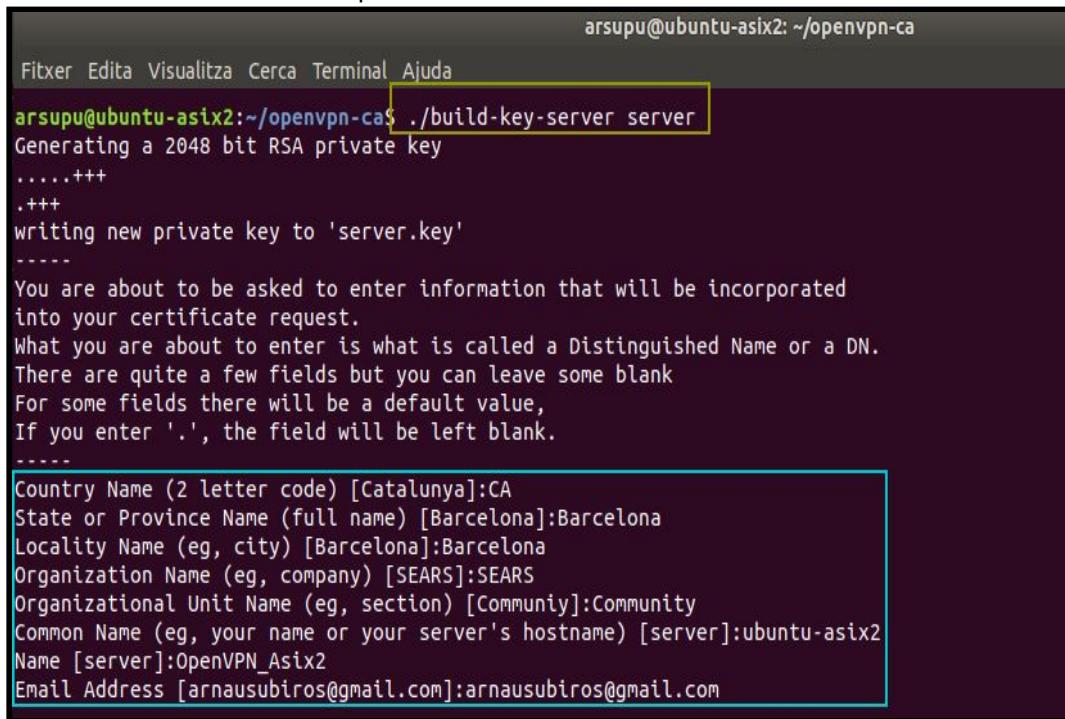
- Primer hem de netejar la CA
- Després construir la nostra CA arrel

```
arsupu@ubuntu-asix2: ~/openvpn-ca
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/openvpn-ca$ ./clean-all
arsupu@ubuntu-asix2:~/openvpn-ca$ ./build-ca
Generating a 2048 bit RSA private key
.....+
.....+
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [Catalunya]:CA
State or Province Name (full name) [Barcelona]:Barcelona
Locality Name (eg, city) [Barcelona]:Barcelona
Organization Name (eg, company) [SEARS]:SEARS
Organizational Unit Name (eg, section) [Community]:Community
Common Name (eg, your name or your server's hostname) [SEARS CA]:ubuntu-asix2
Name [server]:OpenVPN_Asix2
Email Address [arnausubiros@gmail.com]:arnausubiros@gmail.com
arsupu@ubuntu-asix2:~/openvpn-ca$
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

5. Crear el certificat de servidor, la clau i els arxius de xifrat

- A continuació, generarem el nostre certificat de servidor i parell de claus, així com alguns arxius addicionals utilitzats durant el procés de xifrat.



```
arsupu@ubuntu-asix2: ~/openvpn-ca$ ./build-key-server server
Generating a 2048 bit RSA private key
.....+
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [Catalunya]:CA
State or Province Name (full name) [Barcelona]:Barcelona
Locality Name (eg, city) [Barcelona]:Barcelona
Organization Name (eg, company) [SEARS]:SEARS
Organizational Unit Name (eg, section) [Community]:Community
Common Name (eg, your name or your server's hostname) [server]:ubuntu-asix2
Name [server]:OpenVPN_Asix2
Email Address [arnausubiros@gmail.com]:arnausubiros@gmail.com
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

```
arsupu@ubuntu-asix2: ~/openvpn-ca

Fitxer Edita Visualitza Cerca Terminal Ajuda
Country Name (2 letter code) [Catalunya]:CA
State or Province Name (full name) [Barcelona]:Barcelona
Locality Name (eg, city) [Barcelona]:Barcelona
Organization Name (eg, company) [SEARS]:SEARS
Organizational Unit Name (eg, section) [Community]:Community
Common Name (eg, your name or your server's hostname) [server]:ubuntu-asix2
Name [server]:OpenVPN_Asix2
Email Address [arnausubiros@gmail.com]:arnausubiros@gmail.com

>please enter the following 'extra' attributes
to be sent with your certificate request
# challenge password []:fjeclot2019
# an optional company name []:SEARS2019
Using configuration from /home/arsupu/openvpn-ca/openssl-1.0.0.cnf
Can't open /home/arsupu/openvpn-ca/keys/index.txt.attr for reading, No such file or directory
140326397411776:error:02001002:system library:fopen:No such file or directory.../crypto/bio/bss_file.c:74:fopen('/home/arsupu/openvpn-ca/keys/index.txt.attr','r')
140326397411776:error:2006D080: BIO routines: BIO_new_file: no such file:.../crypto/bio/bss_file.c:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'CA'
stateOrProvinceName  :PRINTABLE:'Barcelona'
localityName         :PRINTABLE:'Barcelona'
organizationName     :PRINTABLE:'SEARS'
organizationalUnitName:PRINTABLE:'Community'
commonName           :PRINTABLE:'ubuntu-asix2'
name                :T61STRING:'OpenVPN_Asix2'
emailAddress         :IA5STRING:'arnausubiros@gmail.com'
Certificate is to be certified until Jan 22 13:37:33 2029 GMT (3650 days)
Sign the certificate? [y/n]:
```

- A continuació, generarem alguns altres articles. Podem generar una clau **Diffie-Hellman** forta per a usar durant l'intercanvi de claus escrivint:

```
arsupu@ubuntu-asix2: ~/openvpn-ca

Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/openvpn-ca$ ./build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+.....+.....+.....+
.....+.....+.....+.....+
.....+.....+.....+.....+
.....+.....+.....+.....+
.....+.....+.....+.....+
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- Després, podem generar una signatura HMAC per a enfortir les capacitats de verificació d'integritat TLS del servidor:

```
arsupu@ubuntu-asix2: ~/openvpn-ca
Fitxa Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/openvpn-ca$ openvpn --genkey --secret keys/ta.key
arsupu@ubuntu-asix2:~/openvpn-ca$ █
```

```
arsupu@ubuntu-asix2:~/openvpn-ca/keys$ ls
build-ca      build-key      build-key-server  clean-all      list-crl      openssl-1.0.0.cnf  sign-req
build-dh      build-key-pass  build-req        inherit-inter openssl-0.9.6.cnf  pkictool    vars
build-inter   build-key-pkcs12 build-req-pass   keys          openssl-0.9.8.cnf  revoke-full  whichopensslcnf
arsupu@ubuntu-asix2:~/openvpn-ca$ cd keys
arsupu@ubuntu-asix2:~/openvpn-ca/keys$ ls
ca1.pem  ca.key  index.txt  index.txt.old  serial.old  server.csr  ta.key
ca.crt   dh2048.pem  index.txt.attr  serial       server.crt  server.key
arsupu@ubuntu-asix2:~/openvpn-ca/keys$
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

6. Generar un certificat de client i un par de claus

- Crear un conjunt de credencials protegit per contrasenya

```
arsupu@ubuntu-asix2:~/openvpn-ca
Fitxa Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/openvpn-ca$ source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /home/arsupu/openvpn-ca/keys
arsupu@ubuntu-asix2:~/openvpn-ca$ ./build-key-pass User_Kali1
Generating a 2048 bit RSA private key
....+++
....+++
writing new private key to 'User_Kali1.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [Catalunya]:CA
State or Province Name (full name) [Barcelona]:
```

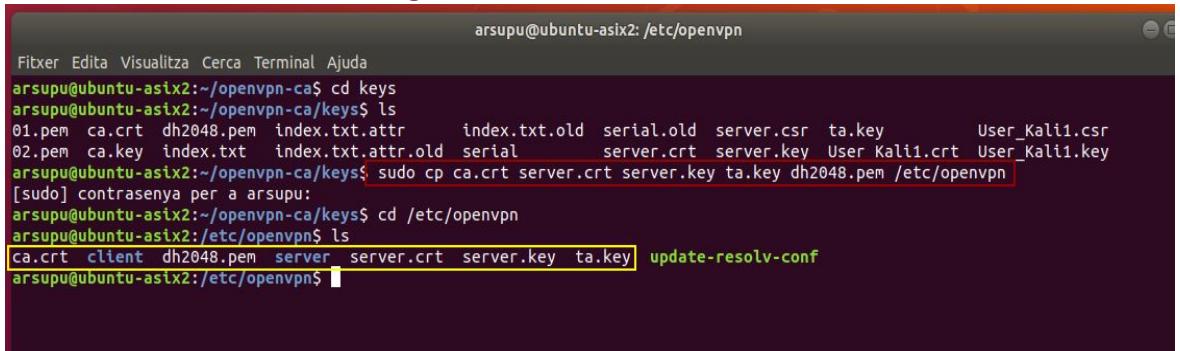
```
arsupu@ubuntu-asix2: ~/openvpn-ca
Fitxa Edita Visualitza Cerca Terminal Ajuda
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:fjeclot2019
An optional company name []:SEARS2019
Using configuration from /home/arsupu/openvpn-ca/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'CA'
stateOrProvinceName :PRINTABLE:'Barcelona'
localityName         :PRINTABLE:'Barcelona'
organizationName    :PRINTABLE:'SEARS'
organizationalUnitName:PRINTABLE:'Community'
commonName           :PRINTABLE:'ubuntu-asix2'
name                 :PRINTABLE:'OpenVPN-Asix2'
emailAddress         :IA5STRING:'arnausubiros@gmail.com'
Certificate is to be certified until Jan 22 16:34:10 2029 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
arsupu@ubuntu-asix2:~/openvpn-ca$
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

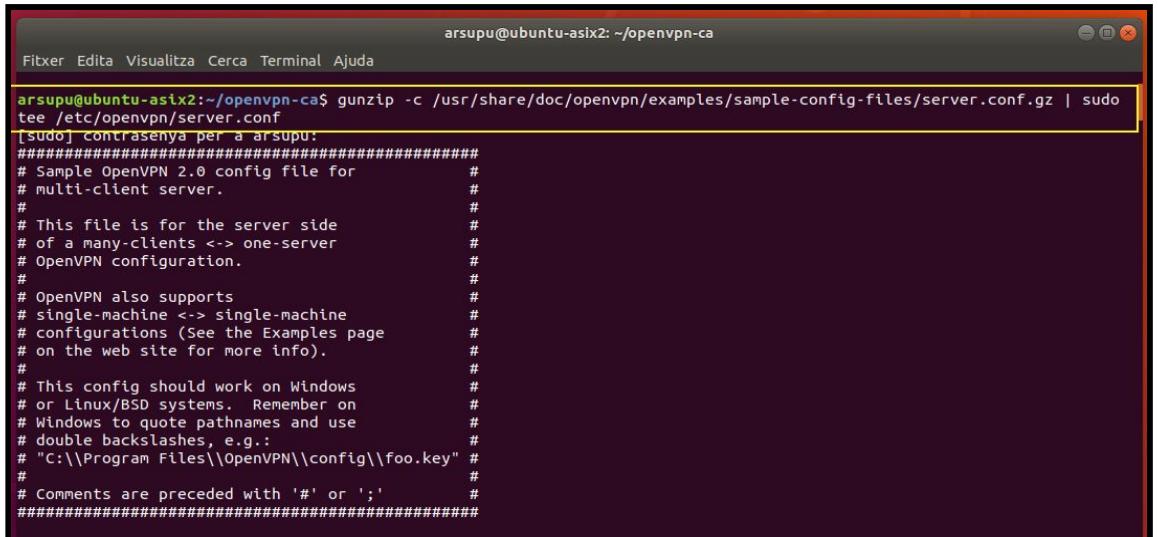
7. Configurar el servei OpenVPN

- Per a començar, necessitem copiar els arxius que necessitem al directori **/etc/openvpn**
- Podem començar amb tots els arxius que acabem de generar. Aquests van ser col·locats dins del **~/openvpn-ca/keys** com van ser creats. Necessitem transferir el nostre **certificat CA, la nostra clau i certificat de servidor, la signatura HMAC i l'arxiu Diffie-Hellman**



```
arsupu@ubuntu-asix2:~/openvpn-ca$ cd keys
arsupu@ubuntu-asix2:~/openvpn-ca/keys$ ls
01.pem ca.crt dh2048.pem index.txt.attr index.txt.old serial.old server.csr ta.key User_Kali1.csr
02.pem ca.key index.txt index.txt.attr.old serial server.crt server.key User_Kali1.crt User_Kali1.key
arsupu@ubuntu-asix2:~/openvpn-ca/keys$ sudo cp ca.crt server.crt server.key ta.key dh2048.pem /etc/openvpn
[sudo] contrasenya per a arsupu:
arsupu@ubuntu-asix2:~/openvpn-ca/keys$ cd /etc/openvpn
arsupu@ubuntu-asix2:/etc/openvpn$ ls
ca.crt client dh2048.pem server server.crt server.key ta.key update-resolv-conf
arsupu@ubuntu-asix2:/etc/openvpn$
```

- A continuació, hem de copiar i descomprimir un arxiu de configuració de OpenVPN de mostra en el directori de configuració perquè puguem usar-lo com a base per a la nostra configuració:



```
arsupu@ubuntu-asix2:~/openvpn-ca$ gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz | sudo tee /etc/openvpn/server.conf
[sudo] contrasenya per a arsupu:
#####
# Sample OpenVPN 2.0 config file for
# multi-client server.
#
# This file is for the server side
# of a many-clients <-> one-server
# OpenVPN configuration.
#
# OpenVPN also supports
# single-machine <-> single-machine
# configurations (See the Examples page
# on the web site for more info).
#
# This config should work on Windows
# or Linux/BSD systems. Remember on
# Windows to quote pathnames and use
# double backslashes, e.g.:
# "C:\\Program Files\\OpenVPN\\config\\foo.key"
#
# Comments are preceded with '#' or ';'#
#####
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- Ajustar la configuració de OpenVPN



```
arsupu@ubuntu-asix2: /etc/openvpn
Fitxa Edita Visualitza Cerca Terminal Ajuda
# Notify the client that when the server restarts so it
# can automatically reconnect.
arsupu@ubuntu-asix2:~/openvpn-ca$ clear

arsupu@ubuntu-asix2:~/openvpn-ca$ cd /etc/openvpn
arsupu@ubuntu-asix2:/etc/openvpn$ sudo nano server.conf
arsupu@ubuntu-asix2:/etc/openvpn$ sudo gedit server.conf
```

- Primer, busqui la secció HMAC buscant la **tls-auth directiva**. Trec el " ; " per a descomentar la **tls-auth** línia. Sota això, agregui el **key-*direction** conjunt de paràmetres a "0":



```
*server.conf
/etc/openvpn
Desa    E    ⌂    ⌂    ⌂    ⌂

#
# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
tls-auth ta.key 0 # This file is secret
key-direction 0

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
# Note that v2.4 client/server will automatically
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- A continuació, busqui la secció de xifrats criptogràfics buscant les cipher línies comentades . El AES-128-*CBC xifrat ofereix un bon nivell de xifrat i està ben suportat. Treu el ";" per a descomentar la cipher AES-128-*CBC.
- A continuació , s'agrega auth línia per a seleccionar l'algorisme de resum de missatges HMAC utilitzant **SHA256**

server.conf
 /etc/openvpn

```

# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
tls-auth ta.key 0 # This file is secret
key-direction 0

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
# Note that v2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.

# See also the ncp-cipher option in the manpage
cipher AES-256-CBC
auth SHA256
    
```

base.conf
 ~/client-config

```

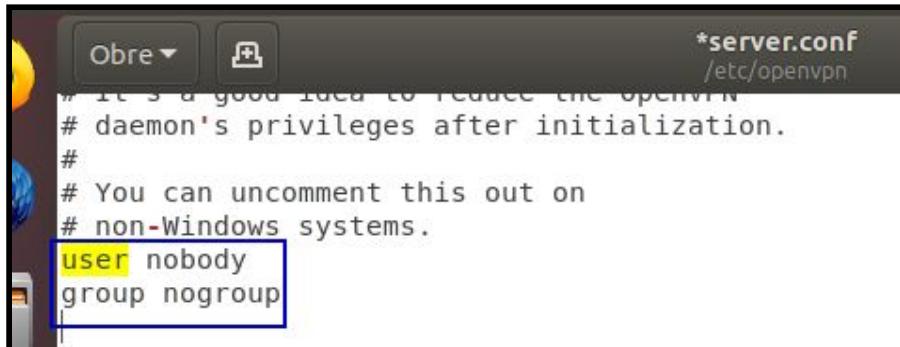
# then you must also specify it here.
# Note that v2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.

# See also the ncp-cipher option in the manpage

#####
### IMPORTANT !!La configuració cipher i auth han de ser al mateix que /etc/openvpn/serv.conf
cipher AES-256-CBC
auth SHA256
#####
    
```

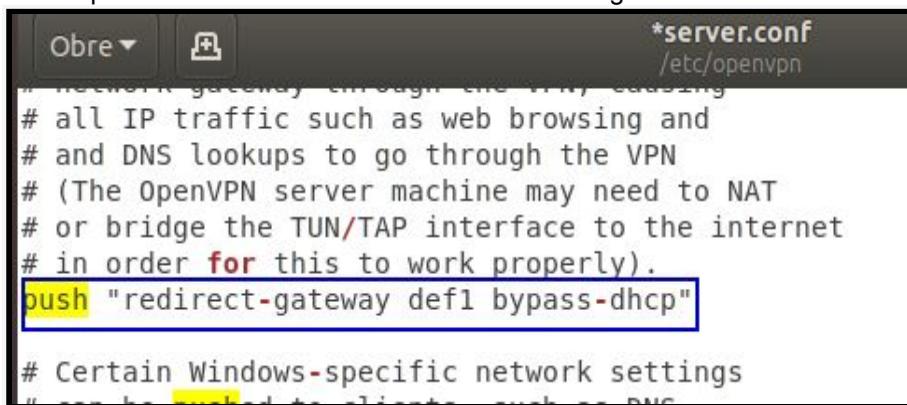
Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

Finalment descomentar les línies següents



```
*server.conf
/etc/openvpn
# It's a good idea to reduce the openvpn
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
user nobody
group nogroup
```

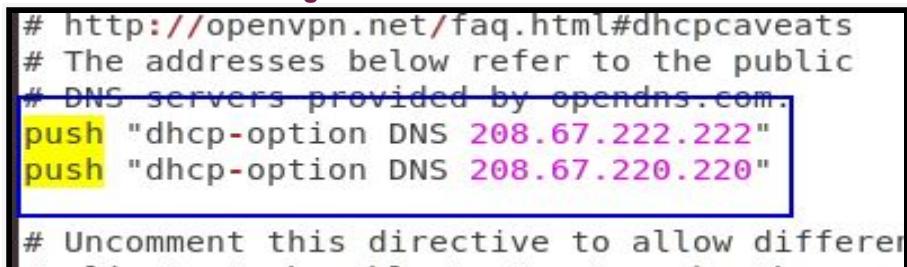
- **OPCIONAL:** Insereixi els canvis de DNS per a redirigir tot el trànsit a través de la VPN. Si desitja utilitzar la VPN per a enrutar tot el seu trànsit, és probable que desitgi enviar la configuració de DNS a les computadores client. S'ha de descomentar le següent línia



```
*server.conf
/etc/openvpn
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
push "redirect-gateway def1 bypass-dhcp"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
```

- **I descomentar les següents línies**



```
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 208.67.220.220"

# Uncomment this directive to allow different
# OpenVPN users to connect simultaneously
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- **OPCIONAL:** Ajustar el port i el protocol

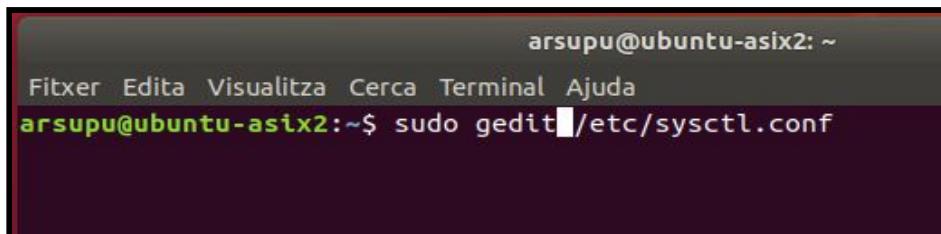
Per defecte, el servidor **OpenVPN** usa el port **1194** i el **protocol UDP** per a acceptar connexions de clients. Si necessita usar un port diferent a causa dels entorns de xarxa restrictius en els quals podrien estar els seus clients, pot canviar la portopció. Si no està allotjant contingut web en el seu servidor OpenVPN, el port **443** és una opció popular, ja que això generalment es permet a través de regles de firewall.

```
# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one. You will need to
# open up this port on your firewall.
port 443

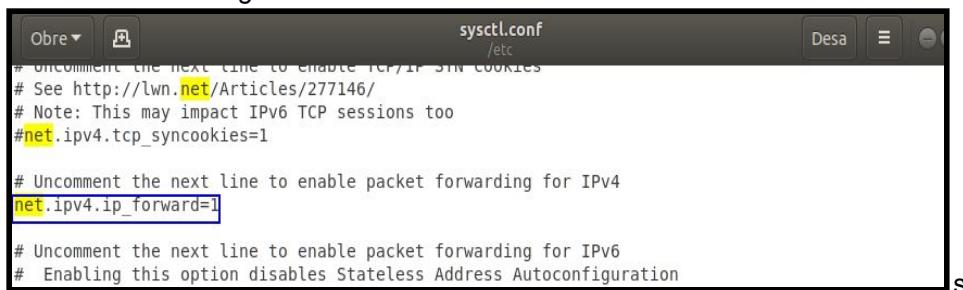
# TCP or UDP server?
proto tcp
;proto udp
```

8. Ajustar la configuració de red del servidor

- Permetre el reenviament de paquets IP



- Descomentar les següents línia



Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- Per llegir l'arxiu i ajustar els valors de la sessió actual

```
arsupu@ubuntu-asix2: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
arsupu@ubuntu-asix2:~$
```

★ Ajust les regles UFW per a emmascarar les connexions de clients

- Abans d'obrir l'arxiu de configuració del firewall per a agregar emmascarament, hem de trobar la interfície de xarxa pública de la nostra màquina

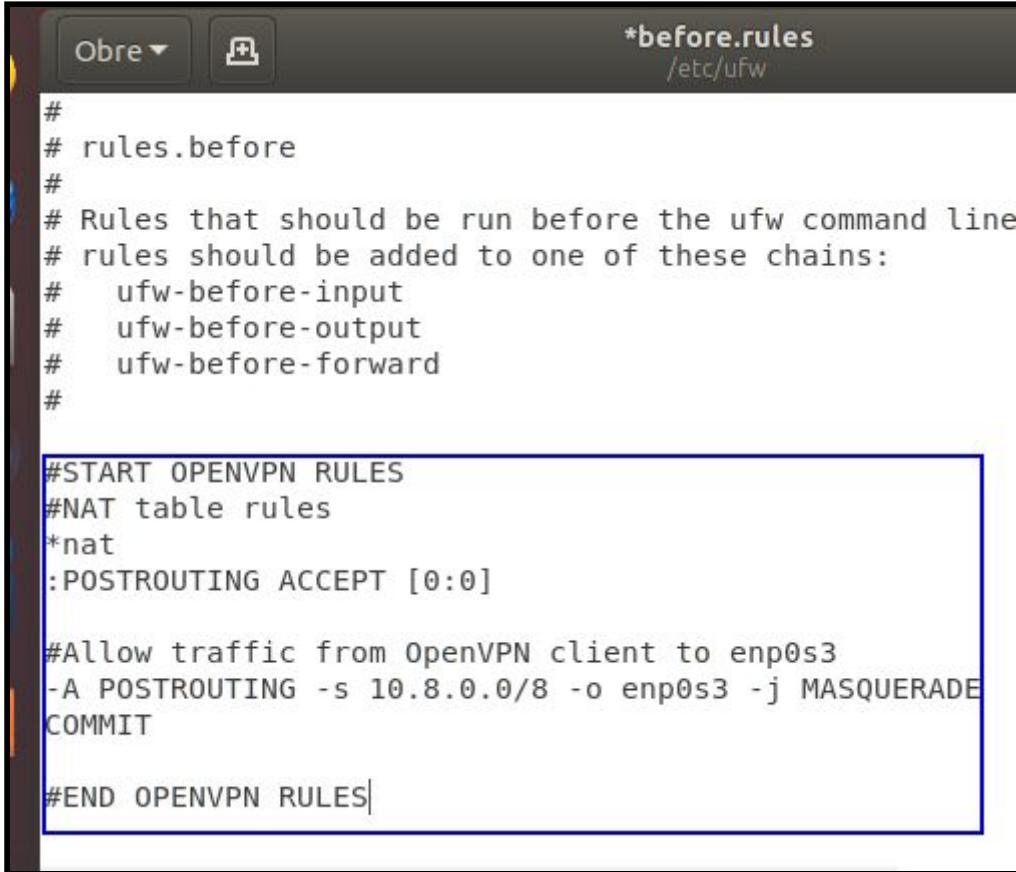
```
arsupu@ubuntu-asix2: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
arsupu@ubuntu-asix2:~$ ip route | grep default
default via 172.20.23.254 dev enp0s3 proto dhcp metric 100
arsupu@ubuntu-asix2:~$
```

- Quan tingui la interfície associada amb la seva ruta predeterminada, obri el [`/etc/ufw/*before.rules`](#), archivo per a agregar la configuració rellevant

```
arsupu@ubuntu-asix2: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~$ sudo gedit /etc/ufw/before.rules
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- o **IMPORTANT :** afegir la següents línia al codi



```
*before.rules
/etc/ufw

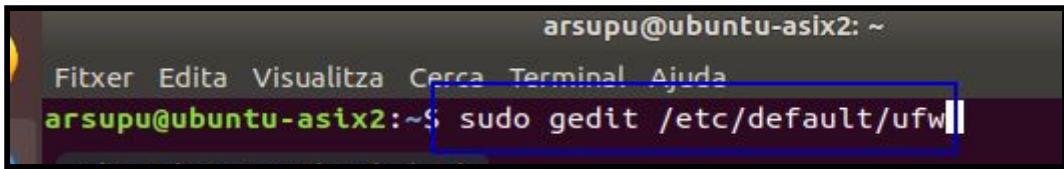
#
# rules.before
#
# Rules that should be run before the ufw command line
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#

#START OPENVPN RULES
#NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]

#Allow traffic from OpenVPN client to enp0s3
-A POSTROUTING -s 10.8.0.0/8 -o enp0s3 -j MASQUERADE
COMMIT

#END OPENVPN RULES|
```

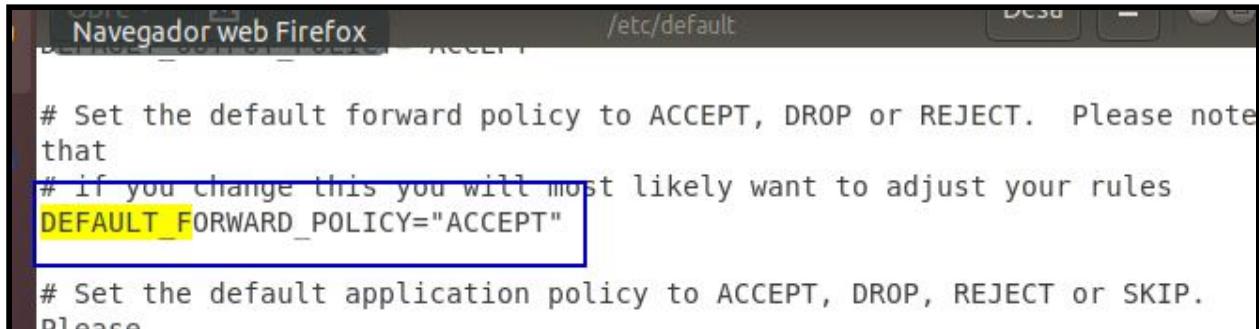
- Necessitem dir-li a UFW que també permeti paquets reenviats per defecte. Per a això, obrirem l'arxiu [/etc/default/ufw](#)



```
arsupu@ubuntu-asix2: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~$ sudo gedit /etc/default/ufw||
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

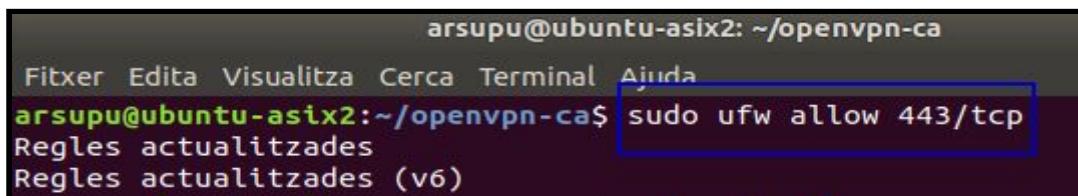
- Cambiar el següent paràmetre de **DROP**→**ACCEPT**



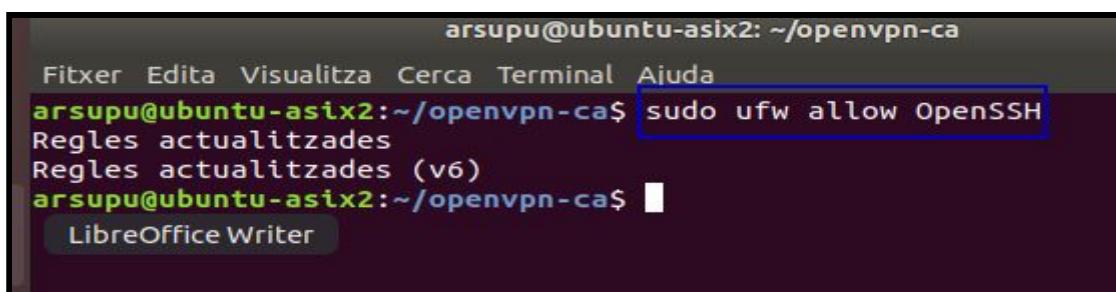
```
# Set the default forward policy to ACCEPT, DROP or REJECT. Please note
# that
# if you change this you will most likely want to adjust your rules
DEFAULT_FORWARD_POLICY="ACCEPT"

# Set the default application policy to ACCEPT, DROP, REJECT or SKIP.
# Please note
```

★ Obrir el port OpenVPN i habilitar els ports

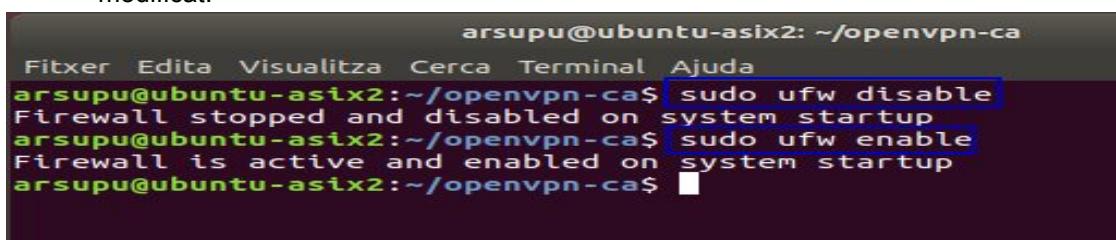


```
arsupu@ubuntu-asix2: ~/openvpn-ca
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/openvpn-ca$ sudo ufw allow 443/tcp
Regles actualitzades
Regles actualitzades (v6)
```



```
arsupu@ubuntu-asix2: ~/openvpn-ca
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/openvpn-ca$ sudo ufw allow OpenSSH
Regles actualitzades
Regles actualitzades (v6)
arsupu@ubuntu-asix2:~/openvpn-ca$
LibreOffice Writer
```

- Ara, podem deshabilitar i tornar a habilitar UFW per a carregar els canvis de tots els arxius que hem modificat:



```
arsupu@ubuntu-asix2: ~/openvpn-ca
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/openvpn-ca$ sudo ufw disable
Firewall stopped and disabled on system startup
arsupu@ubuntu-asix2:~/openvpn-ca$ sudo ufw enable
Firewall is active and enabled on system startup
arsupu@ubuntu-asix2:~/openvpn-ca$
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

9. Iniciar i habilitar el servei OpenVPN

- Necessitem iniciar el servidor OpenVPN especificant el nostre nom d'arxiu de configuració com una variable d'instància després del nom d'arxiu de la unitat systemd.
- Es diu al nostre arxiu de configuració per al nostre servidor , així que l'agregarem al final del nostre arxiu d'unitat quan el cridem:`/etc/openvpn/server.conf@server`

```
arsupu@ubuntu-asix2: /etc/openvpn
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:/etc/openvpn$ sudo systemctl status openvpn
● openvpn.service - OpenVPN service
   Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enabled)
   Active: active (exited) since Sat 2019-01-26 09:44:54 CET; 1min 15s ago
     Process: 7193 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 7193 (code=exited, status=0/SUCCESS)

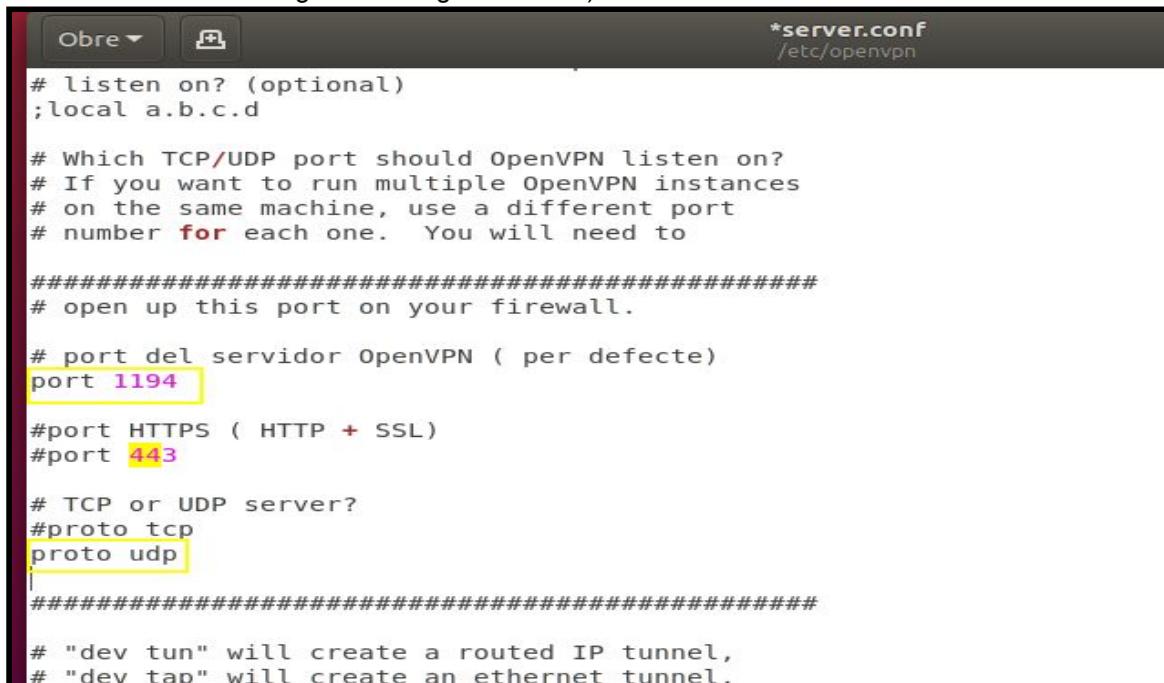
je gen. 26 09:44:54 ubuntu-asix2 systemd[1]: Starting OpenVPN service...
je gen. 26 09:44:54 ubuntu-asix2 systemd[1]: Started OpenVPN service.
arsupu@ubuntu-asix2:/etc/openvpn$ sudo systemctl start openvpn@server
Job for openvpn@server.service failed because the control process exited with error code.
See "systemctl status openvpn@server.service" and "journalctl -xe" for details.
arsupu@ubuntu-asix2:/etc/openvpn$
```

```
arsupu@ubuntu-asix2: /etc/openvpn
Fitxer Edita Visualitza Cerca Terminal Ajuda
ob for openvpn@server.service failed because the control process exited with error code.
ee "systemctl status openvpn@server.service" and "journalctl -xe" for details.
arsupu@ubuntu-asix2:/etc/openvpn$ sudo journalctl -xe
- Subject: Automatic restarting of a unit has been scheduled
- Defined-By: systemd
- Support: http://www.ubuntu.com/support
-
- Automatic restarting of the unit openvpn@server.service has been scheduled, as the result for
the configured Restart= setting for the unit.
je gen. 26 09:47:00 ubuntu-asix2 systemd[1]: Stopped OpenVPN connection to server.
- Subject: Unit openvpn@server.service has finished shutting down
- Defined-By: systemd
- Support: http://www.ubuntu.com/support
-
- Unit openvpn@server.service has finished shutting down.
je gen. 26 09:47:00 ubuntu-asix2 systemd[1]: Starting OpenVPN connection to server...
- Subject: Unit openvpn@server.service has begun start-up
- Defined-By: systemd
- Support: http://www.ubuntu.com/support
-
- Unit openvpn@server.service has begun starting up.
je gen. 26 09:47:00 ubuntu-asix2 ovpn-server[7302]: Options error: --explicit-exit-notify can only be used with --proto udp
je gen. 26 09:47:00 ubuntu-asix2 ovpn-server[7302]: Use --help for more information.
je gen. 26 09:47:00 ubuntu-asix2 systemd[1]: openvpn@server.service: Main process exited, code=exited, status=1/FAILURE
je gen. 26 09:47:00 ubuntu-asix2 systemd[1]: openvpn@server.service: Failed with result 'exit-code'.
je gen. 26 09:47:00 ubuntu-asix2 systemd[1]: Failed to start OpenVPN connection to server.
- Subject: Unit openvpn@server.service has failed
- Defined-By: systemd
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- Em dona error ja que anteriorment vaig afegir les opciones opcionals (del port segur 443, he fet varies proves i no he trobat el problema. He decidit tornar-ho a configurar amb el seu port per defecte)

Accedeixo a traves de : sudo gedit /etc/openvpn/server.conf per modificar els paràmetres 443 tcp (ho comento i afegeixo les següents línies)



```
*server.conf
/etc/openvpn

# listen on? (optional)
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one. You will need to

#####
# open up this port on your firewall.

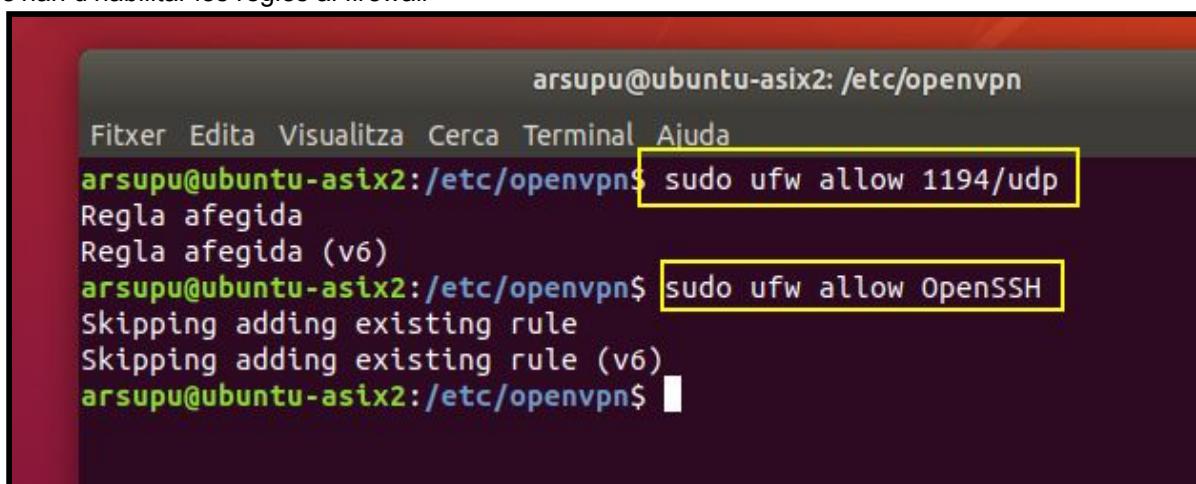
# port del servidor OpenVPN ( per defecte)
port 1194

#port HTTPS ( HTTP + SSL)
#port 443

# TCP or UDP server?
#proto tcp
proto udp

#####
# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel,
```

s'han d'habilitar les regles al firewall



```
arsupu@ubuntu-asix2: /etc/openvpn
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:/etc/openvpn$ sudo ufw allow 1194/udp
Regla afegida
Regla afegida (v6)
arsupu@ubuntu-asix2:/etc/openvpn$ sudo ufw allow OpenSSH
Skipping adding existing rule
Skipping adding existing rule (v6)
arsupu@ubuntu-asix2:/etc/openvpn$
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

```
arsupu@ubuntu-asix2: ~
Fitxa Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~$ sudo ufw disable
[sudo] contrasenya per a arsupu:
Firewall stopped and disabled on system startup
arsupu@ubuntu-asix2:~$ sudo ufw enable
Firewall is active and enabled on system startup
arsupu@ubuntu-asix2:~$
```

- Si tot funciona bé, iniciem el servidor (per si estava parat i revisem el seu estat)

```
arsupu@ubuntu-asix2: /etc/openvpn
Fitxa Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:/etc/openvpn$ sudo systemctl status openvpn
● openvpn.service - OpenVPN service
   Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enabled)
   Active: active (exited) since Sat 2019-01-26 09:44:54 CET; 16min ago
     Process: 7193 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 7193 (code=exited, status=0/SUCCESS)

de gen. 26 09:44:54 ubuntu-asix2 systemd[1]: Starting OpenVPN service...
de gen. 26 09:44:54 ubuntu-asix2 systemd[1]: Started OpenVPN service.
arsupu@ubuntu-asix2:/etc/openvpn$ sudo systemctl start openvpn@server
arsupu@ubuntu-asix2:/etc/openvpn$ sudo systemctl status openvpn@server
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

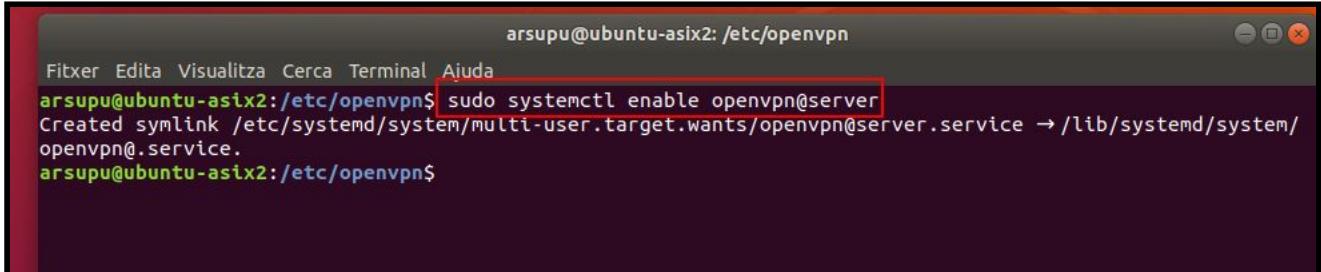
```
arsupu@ubuntu-asix2: /etc/openvpn
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:/etc/openvpn$ sudo systemctl status openvpn@server
● openvpn@server.service - OpenVPN connection to server
   Loaded: loaded (/lib/systemd/system/openvpn@.service; indirect; vendor preset: enabled)
   Active: active (running) since Sat 2019-01-26 09:58:33 CET; 15min ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/OpenVPN24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 7909 (openvpn)
      Status: "Initialization Sequence Completed"
        Tasks: 1 (limit: 1113)
       CGrou...
[...]
de gen. 26 09:58:33 ubuntu-asix2 ovpn-server[7909]: Could not determine IPv4/IPv6 protocol. Using AF_INET
de gen. 26 09:58:33 ubuntu-asix2 ovpn-server[7909]: Socket Buffers: R=[212992->212992] S=[212992->212992]
de gen. 26 09:58:33 ubuntu-asix2 ovpn-server[7909]: UDPv4 link local (bound): [AF_INET][undef]:1194
de gen. 26 09:58:33 ubuntu-asix2 ovpn-server[7909]: UDPv4 link remote: [AF_UNSPEC]
de gen. 26 09:58:33 ubuntu-asix2 ovpn-server[7909]: GID set to nogroup
de gen. 26 09:58:33 ubuntu-asix2 ovpn-server[7909]: UID set to nobody
de gen. 26 09:58:33 ubuntu-asix2 ovpn-server[7909]: MULTI: multi_init called, r=256 v=256
de gen. 26 09:58:33 ubuntu-asix2 ovpn-server[7909]: IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0
de gen. 26 09:58:33 ubuntu-asix2 ovpn-server[7909]: IFCONFIG POOL LIST
de gen. 26 09:58:33 ubuntu-asix2 ovpn-server[7909]: Initialization Sequence Completed
```

- Ara revisem la nova interfície OpenVPN

```
arsupu@ubuntu-asix2: /etc/openvpn
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:/etc/openvpn$ ip addr show tun0
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 100
    link/none
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::1ed0:fba1:a9fc:10c9/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
arsupu@ubuntu-asix2:/etc/openvpn$
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

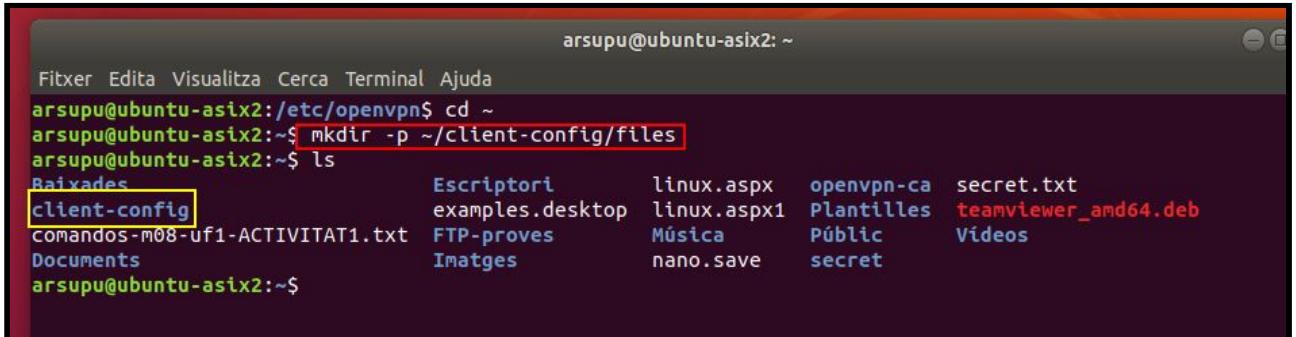
- Seguidament un cop tot funciona correctament, activarem el servei perquè funcioni al arrancar l'ordinador



```
arsupu@ubuntu-asix2: /etc/openvpn
Fitxa Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:/etc/openvpn$ sudo systemctl enable openvpn@server
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn@server.service → /lib/systemd/system/
openvpn@.service.
arsupu@ubuntu-asix2:/etc/openvpn$
```

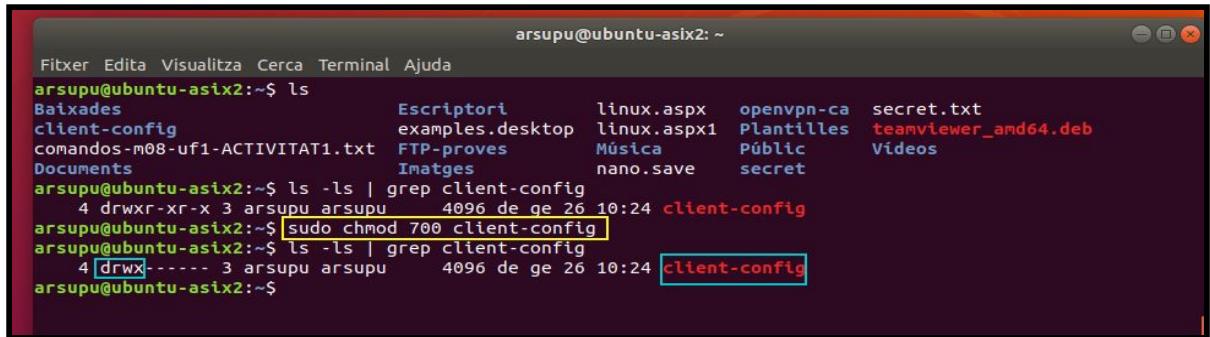
10. Crear la infraestructura de configuració del client

- Crearem una estructura de directoris en el directori d'inici per emmagatzemar els arxius



```
arsupu@ubuntu-asix2: ~
Fitxa Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:/etc/openvpn$ cd ~
arsupu@ubuntu-asix2:~$ mkdir -p ~/client-config/files
arsupu@ubuntu-asix2:~$ ls
Baixades           Escriptori      linux.aspx  openvpn-ca  secret.txt
client-config     examples.desktop  linux.aspx1 Plantilles teamviewer_amd64.deb
comandos-m08-uf1-ACTIVITAT1.txt  FTP-proves   Música      Públic    Vídeos
Documents          Imatges        nano.save   secret
arsupu@ubuntu-asix2:~$
```

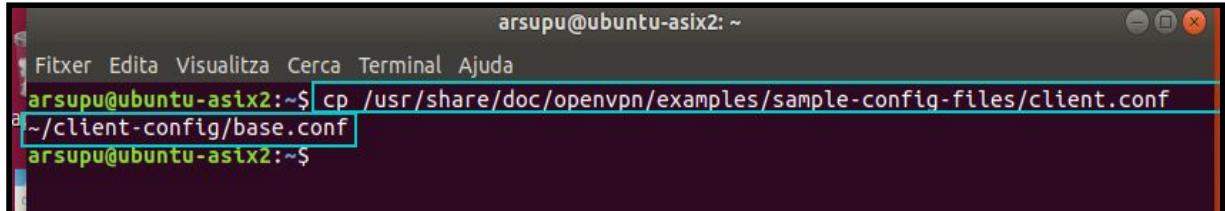
- Els nostres arxius de configuració del client tindran les claus de client integrades, hauríem de bloquejar els permisos en el nostre directori intern:



```
arsupu@ubuntu-asix2: ~
Fitxa Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~$ ls
Baixades           Escriptori      linux.aspx  openvpn-ca  secret.txt
client-config     examples.desktop  linux.aspx1 Plantilles teamviewer_amd64.deb
comandos-m08-uf1-ACTIVITAT1.txt  FTP-proves   Música      Públic    Vídeos
Documents          Imatges        nano.save   secret
arsupu@ubuntu-asix2:~$ ls -ls | grep client-config
4 drwxr-xr-x 3 arsupu arsupu 4096 de ge 26 10:24 client-config
arsupu@ubuntu-asix2:~$ sudo chmod 700 client-config
arsupu@ubuntu-asix2:~$ ls -ls | grep client-config
4 [drwx-----] 3 arsupu arsupu 4096 de ge 26 10:24 client-config
arsupu@ubuntu-asix2:~$
```

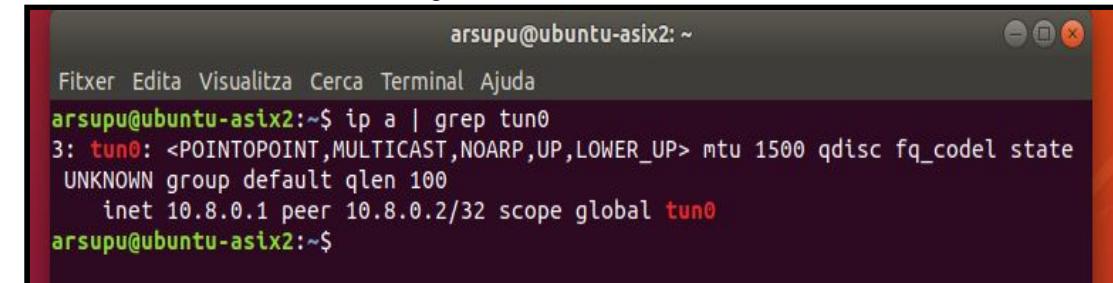
Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- Creació d'una configuració base

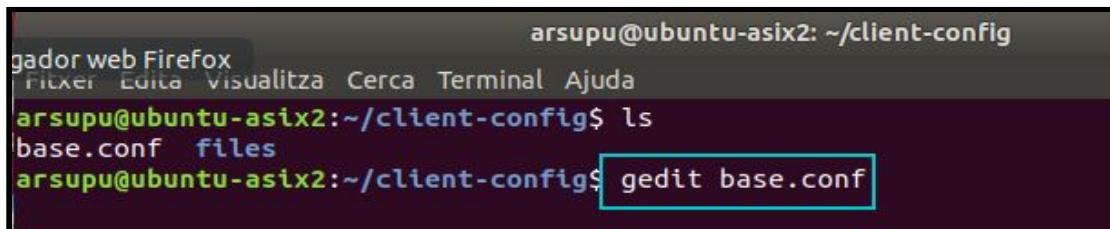


```
arsupu@ubuntu-asix2:~$ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf
~/client-config/base.conf
arsupu@ubuntu-asix2:~$
```

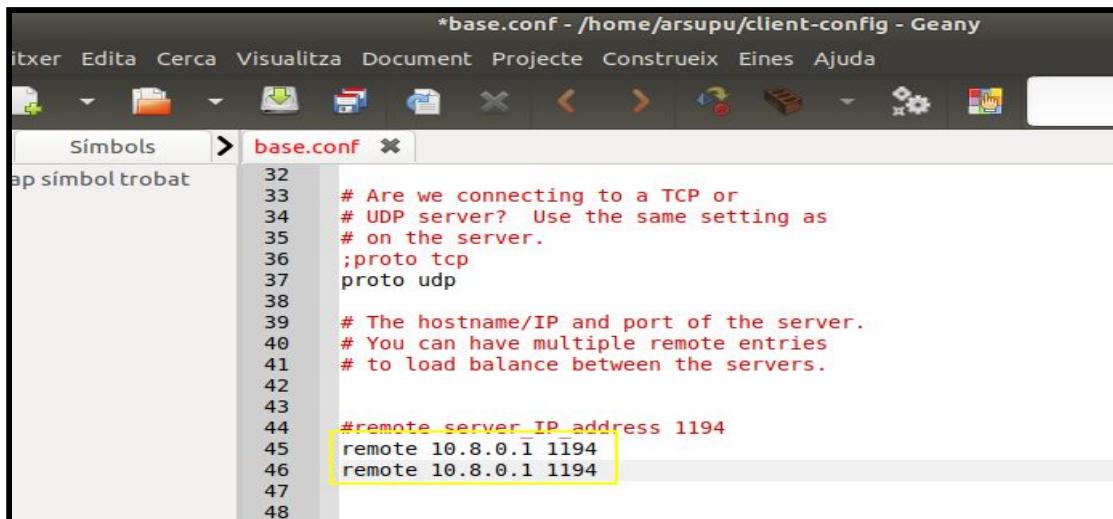
- Obrim l'arxiu base.conf i fer les següents modificacions:



```
arsupu@ubuntu-asix2:~$ ip a | grep tun0
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UNKNOWN group default qlen 100
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
arsupu@ubuntu-asix2:~$
```



```
gador web Firefox
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/client-config$ ls
base.conf  files
arsupu@ubuntu-asix2:~/client-config$ gedit base.conf
```



```
*base.conf - /home/arsupu/client-config - Geany
Fitxer Edita Cerca Visualitza Document Projecte Construeix Eines Ajuda
Símbols > base.conf x
32
33 # Are we connecting to a TCP or
34 # UDP server? Use the same setting as
35 # on the server.
36 ;proto tcp
proto udp
38
39 # The hostname/IP and port of the server.
40 # You can have multiple remote entries
41 # to load balance between the servers.
42
43
44 #remote_server_IP_address 1194
remote 10.8.0.1 1194
45
46
47
48
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

*base.conf
 ~/client-config

```
# Downgrade privileges after initialization (non-Windows only)
user nobody
group nogroup

# Try to preserve some state across restarts.
```

*base.conf
 ~/client-config

```
# This can be used for all clients.

#####
#comentem les següents directives ca.crt client.crt i client.key
#ja que agregarem els certificats i claus en el mateix arxiu

#ca ca.crt
#cert client.crt
#key client.key
#####
```

Editor de text

ds. 12:05 •

*base.conf
 ~/client-config

```
# If a tls-auth key is used on the server
# then every client must also have the key.
tls-auth ta.key 1

#afeqir la key-direction directiva en 1 per treballar amb el servidor
key-direction 1
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- Finalment, agregui algunes línies comentades . Volem incloure'ls amb cada configuració, però només hem d'habilitar-los per als clients Linux que s'envien amb un **/etc/openvpn/update-resolv-conf**. Aquesta seqüència de comandos utilitza la resolvconf utilitat per a actualitzar la informació de DNS per als clients de Linux.

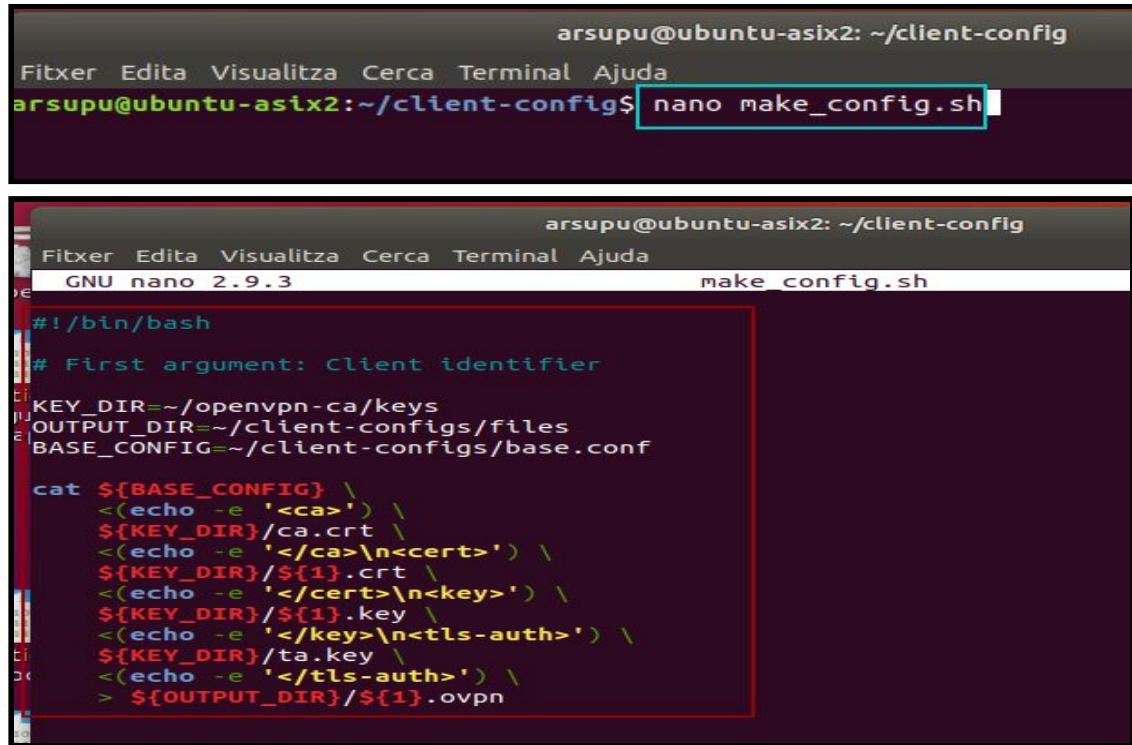


```
*base.conf
~/client-config
#####
##### habilitat per clients Linux per actualitzar la infomacio de DNS /etc/openvpn/update-resolv.conf
script-security 1
up /etc/openvpn/update-resolv.conf
down /etc/openvpn/update-resolv.conf
#####
#####

arsupu@ubuntu-asix2: ~/client-config$
```

Creació d'un script de generació de configuració

- Creació i obre un arxiu anomenat **make_config.sh** dins de **~/client-config**:



```
arsupu@ubuntu-asix2: ~/client-config
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/client-config$ nano make_config.sh

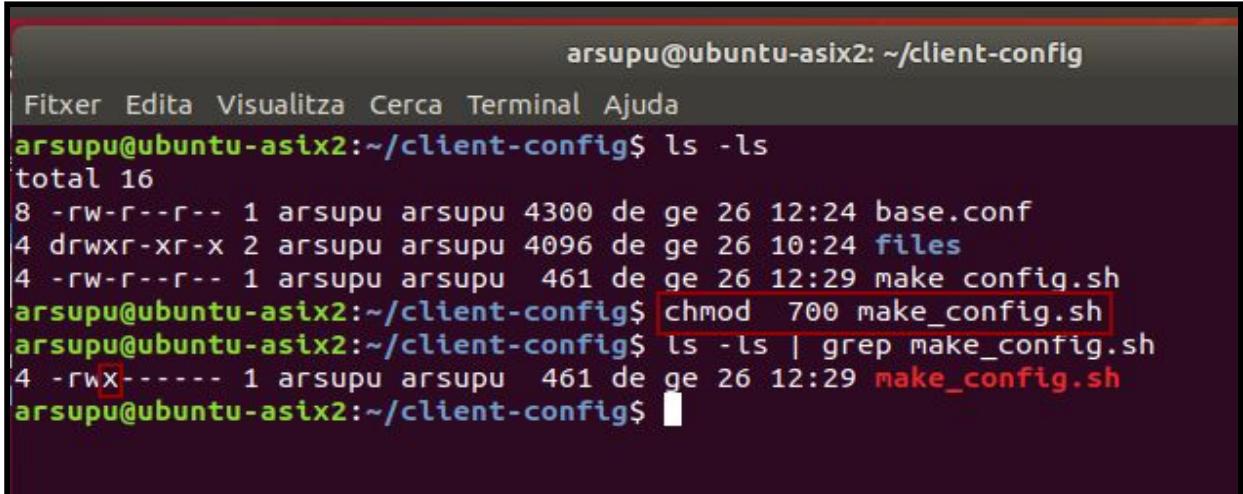
arsupu@ubuntu-asix2: ~/client-config
Fitxer Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.3                               make config.sh
#!/bin/bash

# First argument: Client identifier
KEY_DIR=~/openvpn-ca/keys
OUTPUT_DIR=~/client-configs/files
BASE_CONFIG=~/client-configs/base.conf

cat ${BASE_CONFIG} \
<(echo -e '<ca>' ) \
${KEY_DIR}/ca.crt \
<(echo -e '</ca>\n<cert>' ) \
${KEY_DIR}/${1}.crt \
<(echo -e '</cert>\n<key>' ) \
${KEY_DIR}/${1}.key \
<(echo -e '</key>\n<tls-auth>' ) \
${KEY_DIR}/ta.key \
<(echo -e '</tls-auth>' ) \
> ${OUTPUT_DIR}/${1}.ovpn
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- Marqui l'arxiu com a executable escrivint:



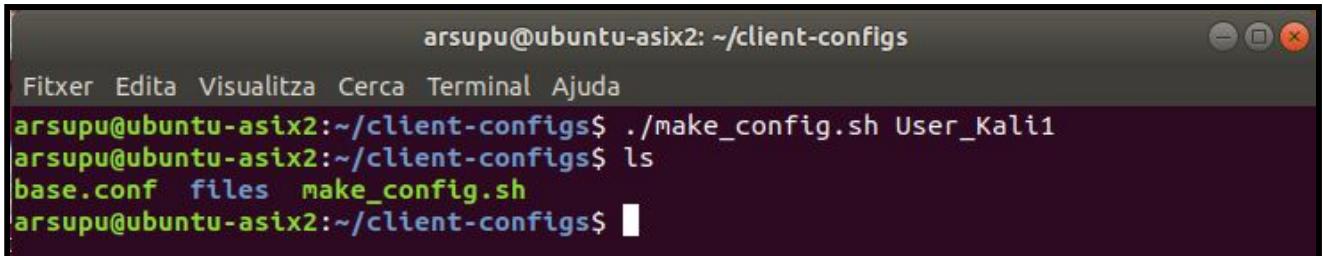
```

arsupu@ubuntu-asix2: ~/client-config
Fitxa Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/client-config$ ls -ls
total 16
8 -rw-r--r-- 1 arsupu arsupu 4300 de ge 26 12:24 base.conf
4 drwxr-xr-x 2 arsupu arsupu 4096 de ge 26 10:24 files
4 -rw-r--r-- 1 arsupu arsupu 461 de ge 26 12:29 make_config.sh
arsupu@ubuntu-asix2:~/client-config$ chmod 700 make_config.sh
arsupu@ubuntu-asix2:~/client-config$ ls -ls | grep make_config.sh
4 -rwx----- 1 arsupu arsupu 461 de ge 26 12:29 make_config.sh
arsupu@ubuntu-asix2:~/client-config$ 

```

11. Generar les configuracions del client

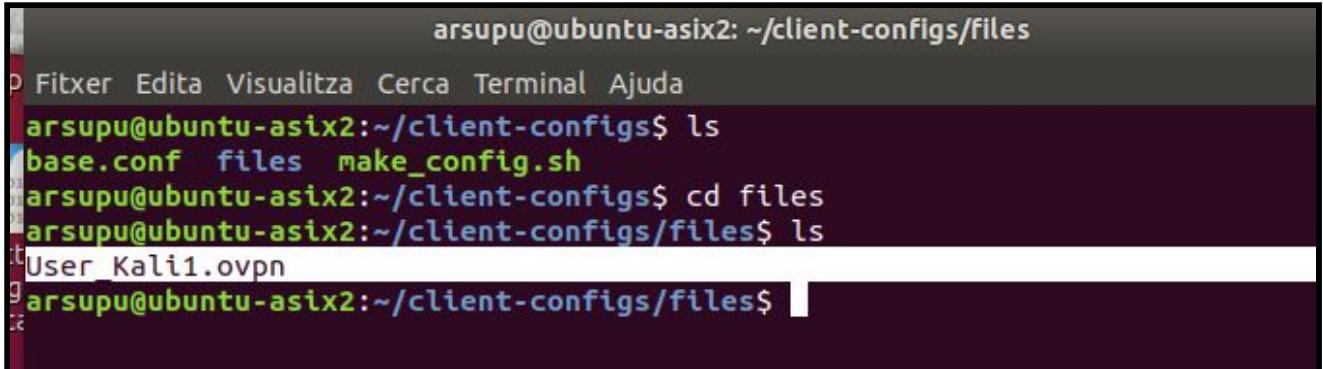
User_Kali1



```

arsupu@ubuntu-asix2: ~/client-configs
Fitxa Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/client-configs$ ./make_config.sh User_Kali1
arsupu@ubuntu-asix2:~/client-configs$ ls
base.conf files make_config.sh
arsupu@ubuntu-asix2:~/client-configs$ 

```



```

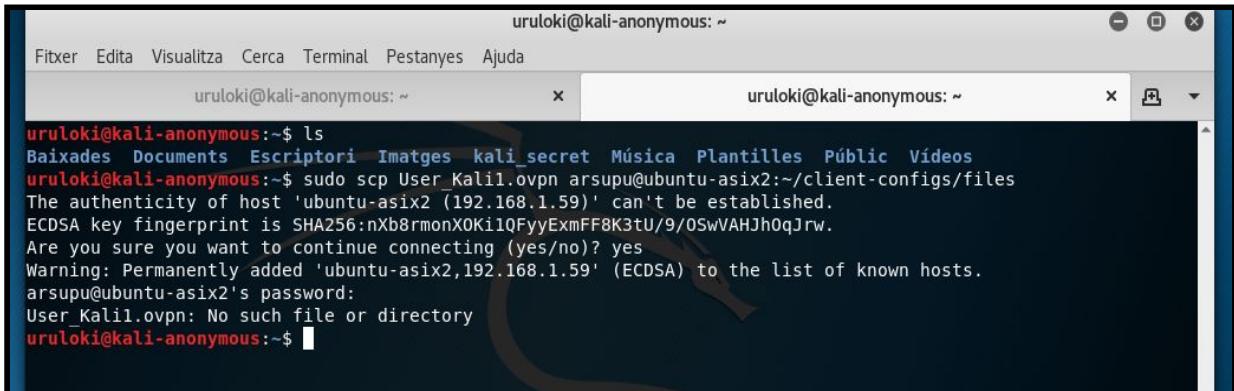
arsupu@ubuntu-asix2: ~/client-configs/files
P Fitxa Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/client-configs$ ls
base.conf files make_config.sh
arsupu@ubuntu-asix2:~/client-configs$ cd files
arsupu@ubuntu-asix2:~/client-configs/files$ ls
User_Kali1.ovpn
arsupu@ubuntu-asix2:~/client-configs/files$ 

```

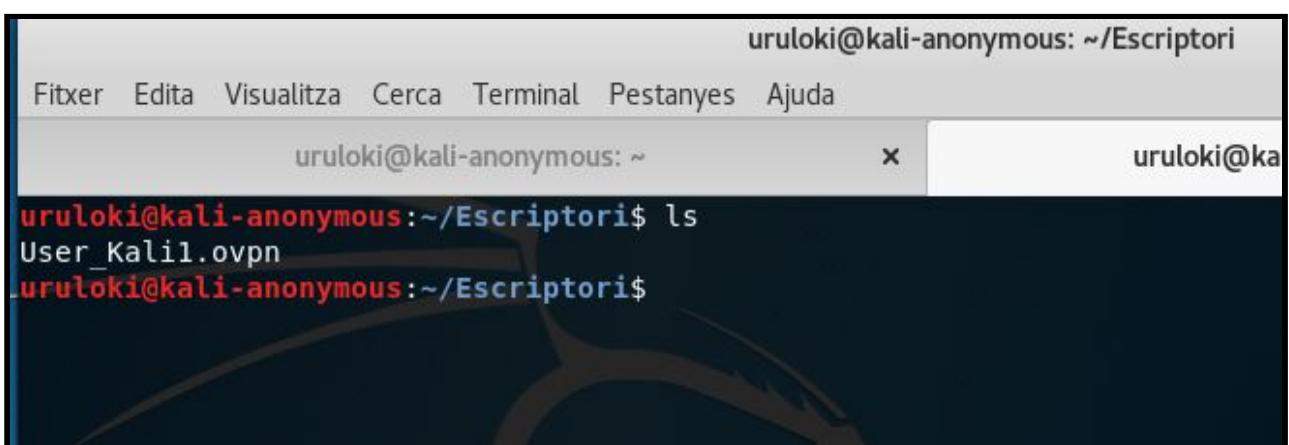
Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

CLIENT OpenVPN (Kali Linux)

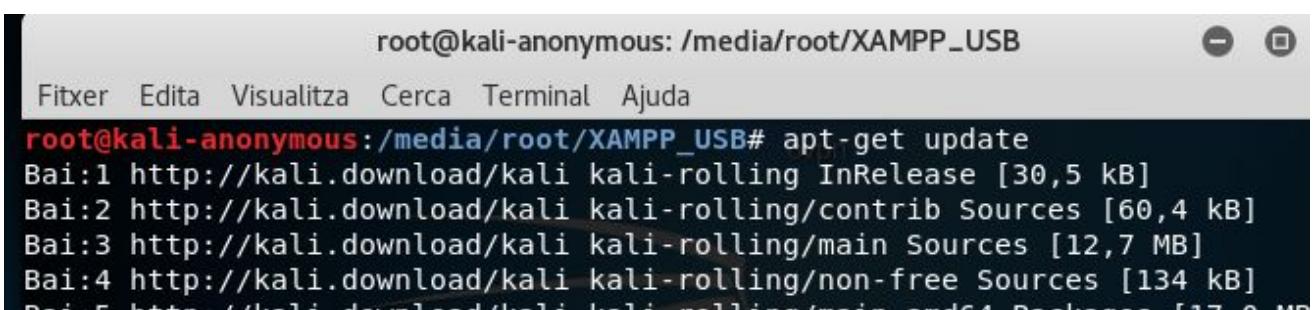
Ho volia copiar sense utilitzar el usb(però m'ha donat error) i per no realitzar més la pràctica he utilitzar un USB



```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Pestanyes Ajuda
uruloki@kali-anonymous: ~
uruloki@kali-anonymous:~$ ls
Baixades Documents Escriptori Imatges kali_secret Música Plantilles Públic Vídeos
uruloki@kali-anonymous:~$ sudo scp User_Kalil.ovpn arsupu@ubuntu-asix2:~/client-configs/files
The authenticity of host 'ubuntu-asix2 (192.168.1.59)' can't be established.
ECDSA key fingerprint is SHA256:nXb8rmonXOKi1QFyyExmFF8K3tU/9/OSwVAHjh0qJrw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ubuntu-asix2,192.168.1.59' (ECDSA) to the list of known hosts.
arsupu@ubuntu-asix2's password:
User Kalil.ovpn: No such file or directory
uruloki@kali-anonymous:~$
```



```
uruloki@kali-anonymous: ~/Escriptori
Fitxer Edita Visualitza Cerca Terminal Pestanyes Ajuda
uruloki@kali-anonymous: ~
uruloki@kali-anonymous:~/Escriptori$ ls
User_Kalil.ovpn
uruloki@kali-anonymous:~/Escriptori$
```



```
root@kali-anonymous: /media/root/XAMPP_USB
Fitxer Edita Visualitza Cerca Terminal Ajuda
root@kali-anonymous:/media/root/XAMPP_USB# apt-get update
Bai:1 http://kali.download/kali kali-rolling InRelease [30,5 kB]
Bai:2 http://kali.download/kali kali-rolling/contrib Sources [60,4 kB]
Bai:3 http://kali.download/kali kali-rolling/main Sources [12,7 MB]
Bai:4 http://kali.download/kali kali-rolling/non-free Sources [134 kB]
Bai:5 http://kali.download/kali kali-rolling/main amd64 Packages [17,0 MB]
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

```
root@kali-anonymous: /media/root/XAMPP_USB
Fitxa Edita Visualitza Cerca Terminal Ajuda
root@kali-anonymous:/media/root/XAMPP_USB# apt-get install openvpn
S'està llegint la llista de paquets... Fet
S'està construint l'arbre de dependències
S'està llegint la informació de l'estat... Fet
Paquets suggerits:
  resolvconf
  S'actualitzaran els paquets següents:

```

```
uruloki@kali-anonymous: ~/Escriptori
Fitxa Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~/Escriptori$ ls
User_Kali1.ovpn
uruloki@kali-anonymous:~/Escriptori$ nano User_Kali1.ovpn
uruloki@kali-anonymous:~/Escriptori$
```

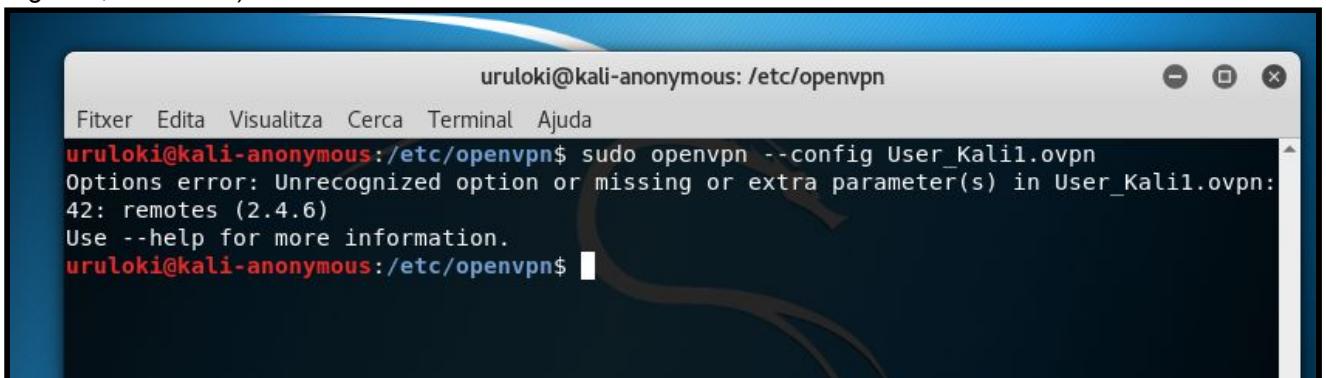
```
uruloki@kali-anonymous: ~/Escriptori
Fitxa Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.8          User_Kali1.ovpn          Modificat
# Set log file verbosity.
verb 3

# Silence repeating messages
mute 20

# para clientes linux
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
<ca>
-----BEGIN CERTIFICATE-----
MIIE/TCCA+WgAwIBAgIJANizXia0aga7MA0GCSqGSIb3DQEBCwUAMIGvMQswCQYD
/QQGEwJDQTESMBAGA1UECBMJQmFyY2Vsb25hMRIwEAYDVQQHEwlCYXJjZWxvbmx
LAMPNUVATPUNEOVJHPTLFAVNUQLE1b1d1LWE1LULWETATPNUVAMTBUWU
-----END CERTIFICATE-----
```

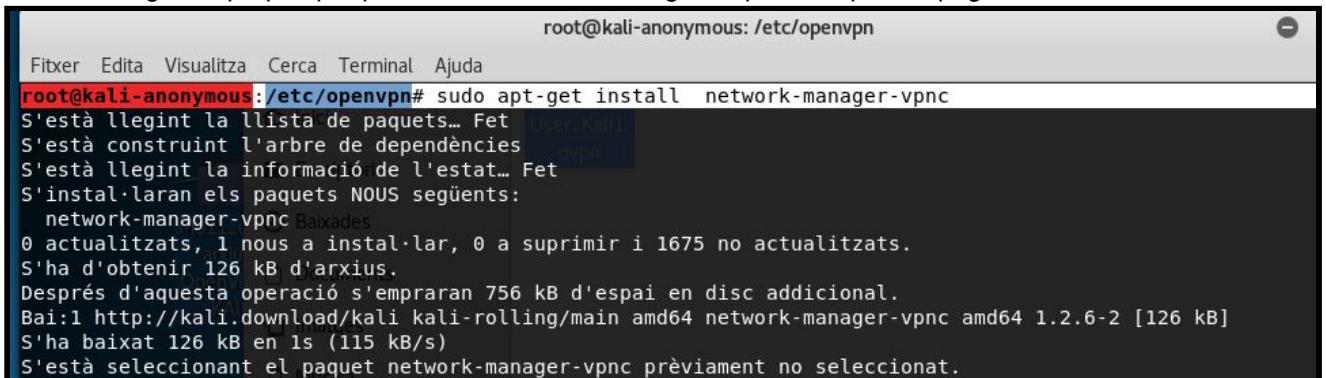
Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

Malauradament, només em falta la configuració del client, però em dona error. (ho he intentat fer varies vegades, sense èxit)

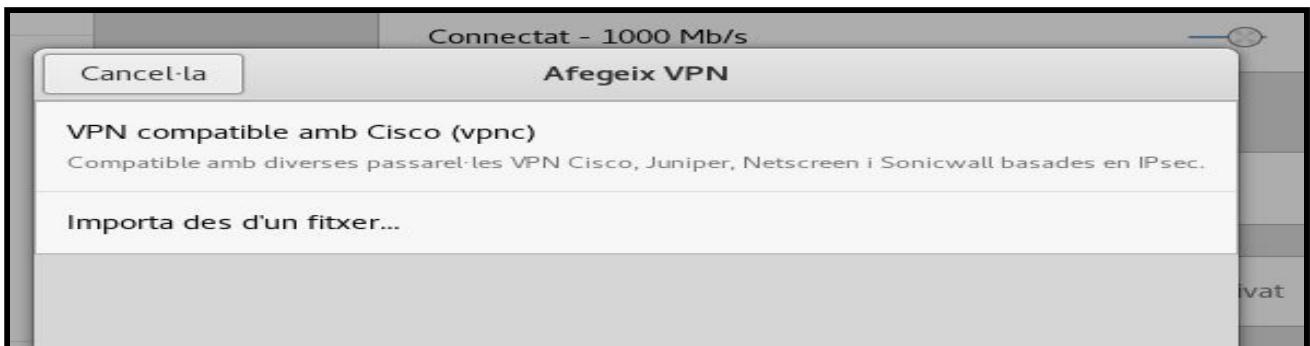


```
uruloki@kali-anonymous: /etc/openvpn
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc/openvpn$ sudo openvpn --config User_Kali1.ovpn
Options error: Unrecognized option or missing or extra parameter(s) in User_Kali1.ovpn:
42: remotes (2.4.6)
Use --help for more information.
uruloki@kali-anonymous:/etc/openvpn$
```

M'he descarregat un paquet per poder-ho fer amb entorn gràfic, però tampoc he pogut accedir.



```
root@kali-anonymous: /etc/openvpn
Fitxer Edita Visualitza Cerca Terminal Ajuda
root@kali-anonymous:/etc/openvpn# sudo apt-get install network-manager-vpnc
S'està llegint la llista de paquets... Fet
S'està construint l'arbre de dependències
S'està llegint la informació de l'estat... Fet
S'instal·laran els paquets NOUS següents:
  network-manager-vpnc Baixades
  0 actualitzats, 1 nous a instal·lar, 0 a suprimir i 1675 no actualitzats.
S'ha d'obtenir 126 kB d'arxius.
Després d'aquesta operació s'empraran 756 kB d'espai en disc addicional.
Bai:1 http://kali.download/kali kali-rolling/main amd64 network-manager-vpnc amd64 1.2.6-2 [126 kB]
S'ha baixat 126 kB en 1s (115 kB/s)
S'està seleccionant el paquet network-manager-vpnc prèviament no seleccionat.
```



Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

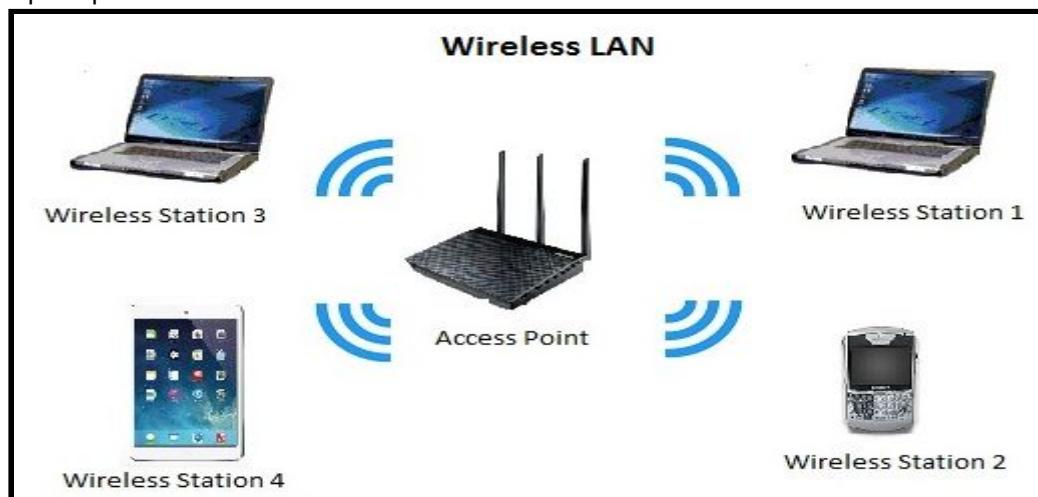
PART 2:Qüestionari: Seguretat de xarxes sense fils

Responiu a les següents qüestions a partir de la teoria que he s'ha donat a classe. Els apunts estaran penjats al Moodle.

- Perque, en general, les comunicacions inalàmbriques proporcionen un entorn de seguretat perimètric molt més insegur que les comunicacions per cable?[1 punt]

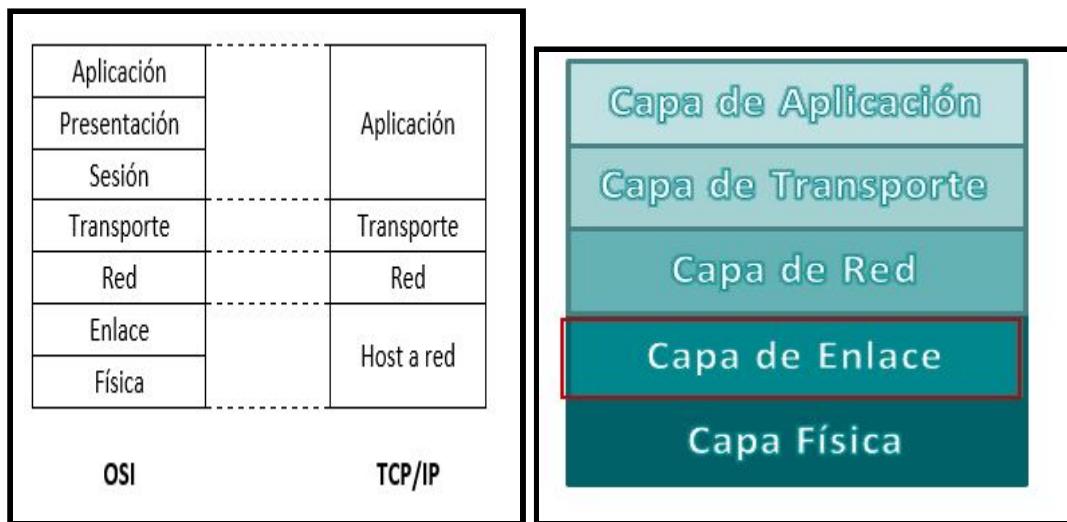
La tecnologia WLAN és regida per l'estàndard 802.11, especificat per l'Institute of Electrical and Electronics Engineers (IEEE), el mateix organisme encarregat d'especificar la resta de tecnologies de xarxa (com l'ethernet, la 802.3)

Una WLAN està disponible per a qualsevol que estigui dins el radi d'accio del punt d'accés; per tant, amb un dispositiu sense fil **i les tècniques de cracking oportunes**, qualsevol es podria associar a aquest punt d'accés i tindria accés a la xarxa i als seus recursos.



Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

2. A quins nivells de la capa OSI actuen els protocols de seguretat de xarxes inalàmbriques?[1 punt]



Corresponent a la **capa 2 del Model Osi** ([Enllaç de Dades](#)). que actúa com a intermediari entre la capa 3 - Red i la capa 1- Física, codificant les trames rebudes desde la capa 3 , encapsulant a la trama ethernet per la seva transmissió a la capa 1

En aquesta capa hi ha tots els protocols de seguretat per la comunicació:

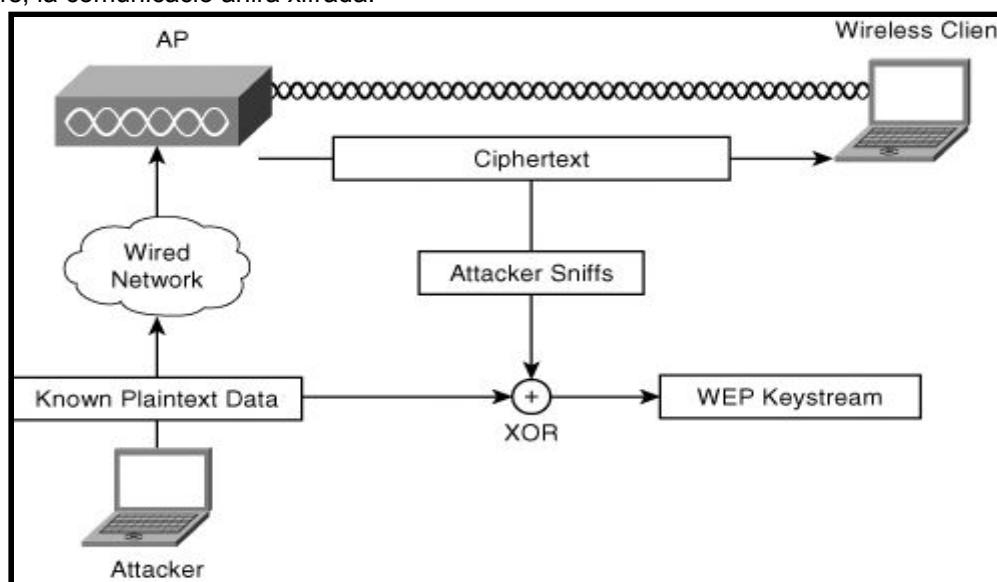
- Si utilitzem el mitjà inalàmbric
 - protocols : WEP, WPA, WPA-2
- Configuració de les xarxes virtuals
 - VLAN
- Altres protocols de la capa 2:
 - PPP
 - Ethernet
 - HDLC
 - Frame Relay
 - ATM

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

3. Quina és la principal debilitat del protocol WEP més enllà del fet que sigui un protocol sobre un medi inalàmbric?[1 punt]

Fins el març del 2006 també alguns únicament implementaven l'estàndard de seguretat WEP, que és fràgil i fàcilment atacable. En aquesta data va passar a ser obligatori implementar WPA2.

Wired Equivalent Privacy (WEP): Estàndard de seguretat que protegeix una xarxa sense fil. Utilitza claus de 64 bits o de 128 bits. Bèsicament, consisteix a implementar una clau en el punt d'accés que es demanarà al client quan intenti l'autenticació. Si el client s'autentifica de manera correcta, es produeix l'associació i, a partir de llavors, la comunicació anirà xifrada.

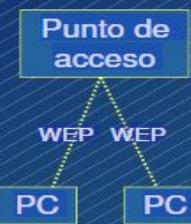


WEP: características

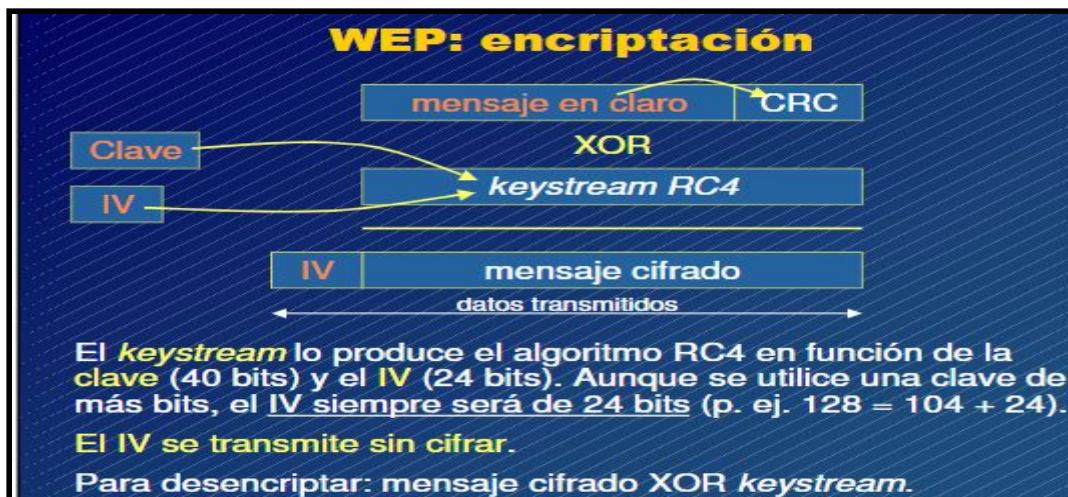
- **WEP (Wired Equivalent Privacy)**, mecanismo de seguridad incluido en la especificación IEEE 802.11.
 - Una sola clave, simétrica y estática
 - Distribución manual de claves
 - No autentifica usuarios
 - Algoritmo de encriptación: RC4
 - Claves de 64 bits (40 fijos + 24 cambiantes).
 - Los 24 bits son el vector de inicialización (IV). Se envía al destino sin encriptar.

Punto de acceso

```
graph TD; AP[Punto de acceso] -- "WEP" --> PC1[PC]; AP -- "WEP" --> PC2[PC]
```

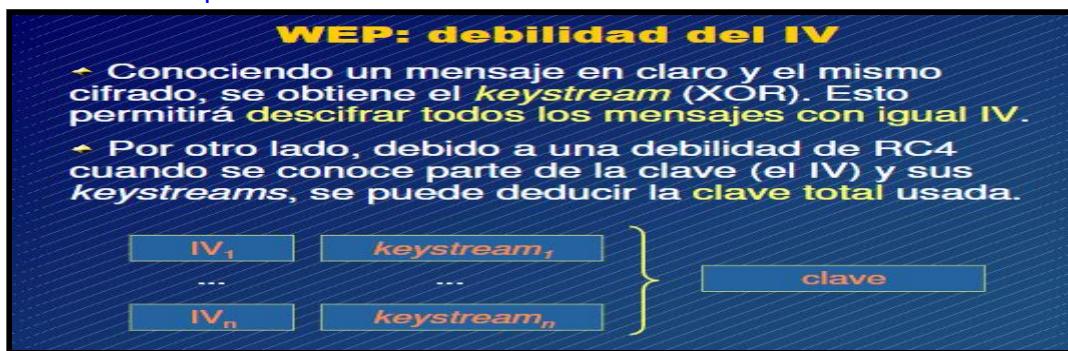


Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019



L'estàndard especifica que l'IV hauria de canviar-se en cada paquet, però no indica com.

- Existeixen 2^{24} combinacions de claus diferents:
 - no són tantes i a més unes poques s'utilitzen sovint (mala elecció dels IV)
 - Sol repetir-se la mateixa seqüència de IVs cada vegada que es reinicia la targeta.
 - Pel fet que no disposa d'un mecanisme de distribució de claves automàtiques, la clau no sol canviar-se mai.
 - La mateixa clau és emmagatzemada en el punt d'accés com en totes les estacions.
 - WEP li manca de mecanismes de protecció contra paquets falsificats o repetits (replay).
 - El CRC es va incloure com un mecanisme d'integritat, però s'ha demostrat que no serveix



Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

El programa Aircrack-ng serveix per crackear les claus WEP

```
Aircrack-ng

[00:00:00] Tested 76 keys (got 11090 IVs)

KB      depth   byte(vote)
0       0/     2   90(16896) 29(16128) 4D(15104) 8B(15104) 35(14848)
1       1/     3   46(17152) D5(15872) 38(15616) 19(14848) 36(14848)
2       0/     1   65(17920) BE(16384) 14(14592) 35(14336) 49(14336)
3       4/     5   12(14336) 31(14080) 8F(14080) 9D(14080) 16(13824)
4       2/     3   05(15616) 2D(15104) 60(15104) 22(14592) 2F(14592)

KEY FOUND! [ 90:45:65:12:05 ] →
Decrypted correctly: 100%
```

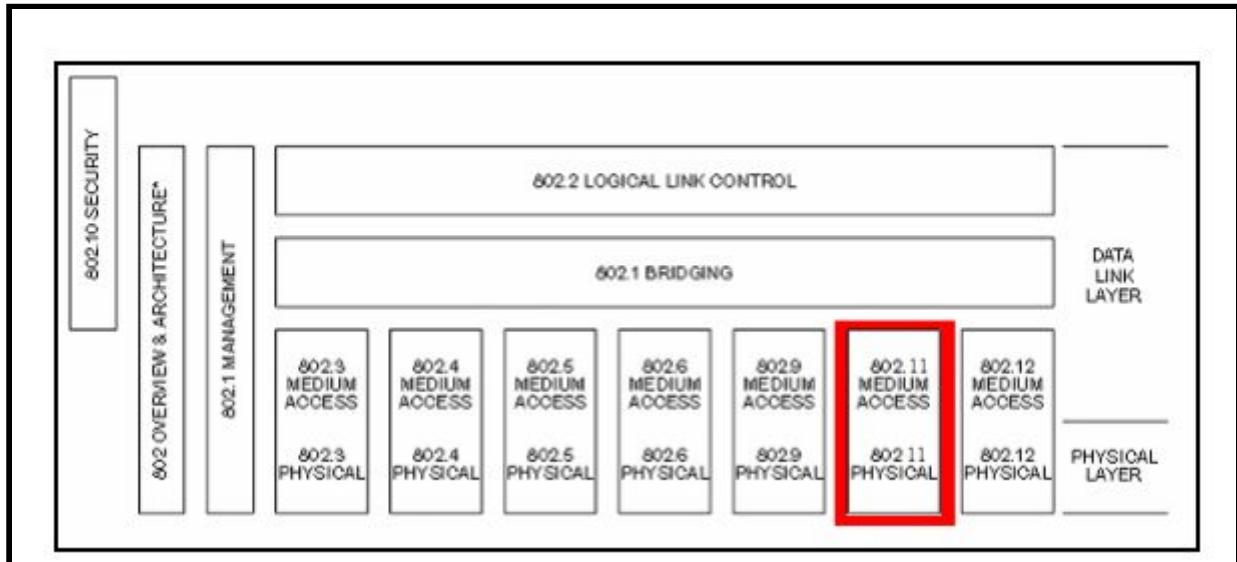
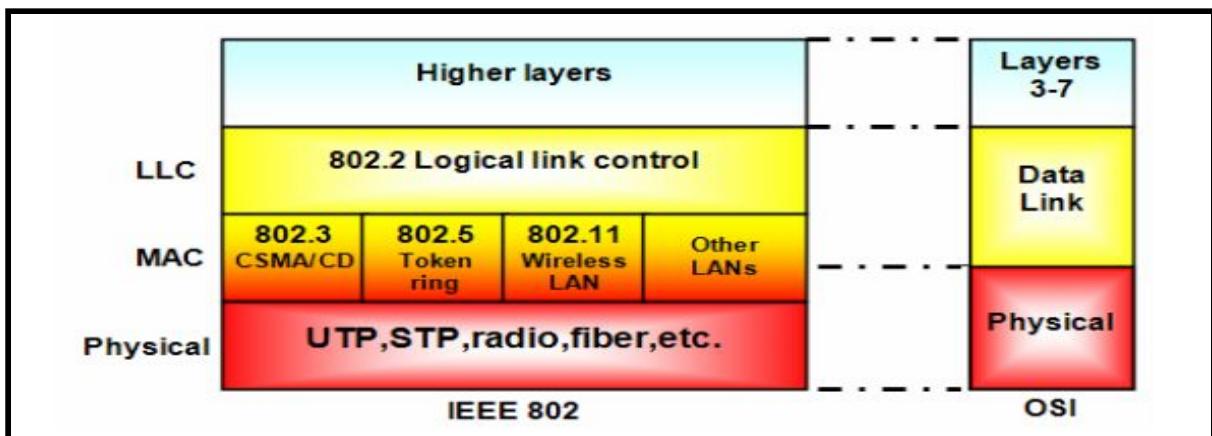
4. Explica de manera breu els components que intervenen en el procés d'encriptació del protocol WEP, els quals estan llistats a continuació:[2 punts]
- 802.11 Headers
 - Shared Key
 - Vector de Inicialització (IV)
 - CRC

WEP (Private Equivalet Wired): És un protocol d'encriptació de la capa 2 del model Osi per a connexions inalàmbriques

Pot ser WEP64 (40 bits reals) WEP128 (104 bits reals) i fins a 256 (208 bits reals)

- ❖ **802.11 Wireless LAN (WLAN):** defineix la modalitat d'interconnexió entre hosts utilitzant l'aire com a mitjà de propagació, gràcies a la seva peculiaritat de no necessitar cablejat algun en el àrea geogràfica coberta.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

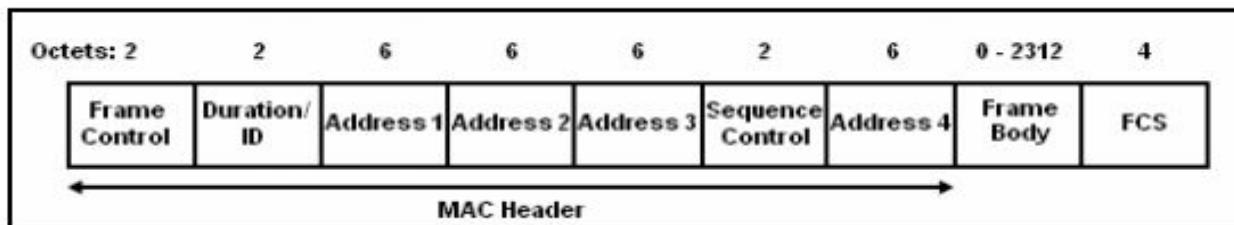


Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

Tabla 2.A: Estándares del IEEE 802.11

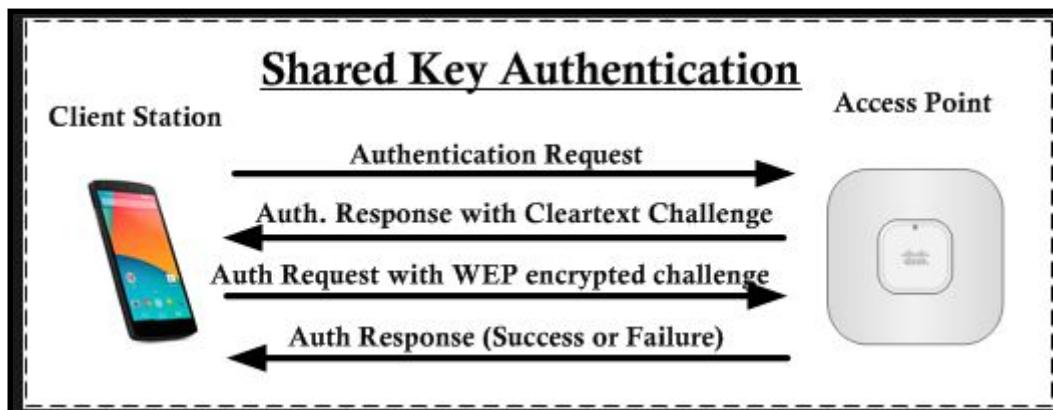
Estándar	Data Rate [Mbps]	Frecuencia	Modulación
802.11	1, 2	2.4 GHz	FHSS, DSSS, IR
802.11a	6, 9, 12, 18, 24, 36, 48, 54	5 GHz	OFDM
802.11b	1, 2, 5.5, 11	2.4 GHz	HR-DSSS
802.11g	6, 12, 24, 36, 48, 54	2.4 GHz	OFDM
802.11n	Aprox. 100 Mbps	-----	-----

Format general de la trama MAC 802.11

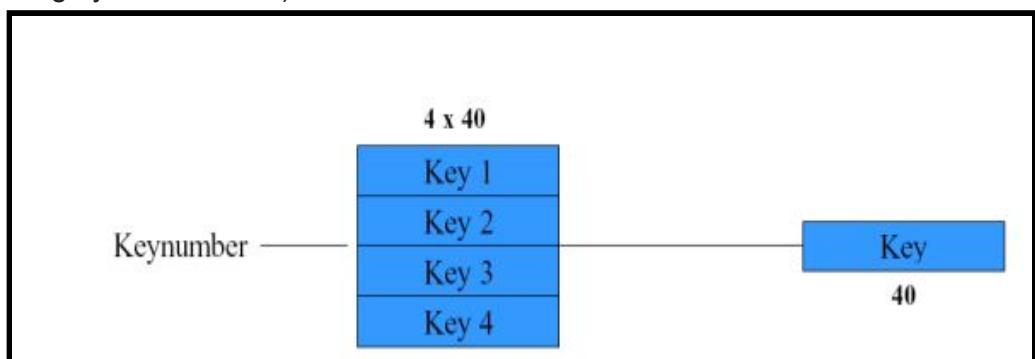


Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

- ❖ **Shared Key :** El procés d'autenticació de clau compartida comença quan un client envia una sol·licitud d'autenticació al punt d'accés de la xarxa. El punt d'accés després envia al client un arxiu xifrat, que el client ha de desxifrar utilitzant la contrasenya ingressada per l'usuari. El client torna el fitxer a ser examinat pel punt d'accés. Si l'arxiu és el mateix que el que té el punt d'accés al registre, el punt d'accés sap que el client està utilitzant la clau correcta, i s'atorga accés a la xarxa.

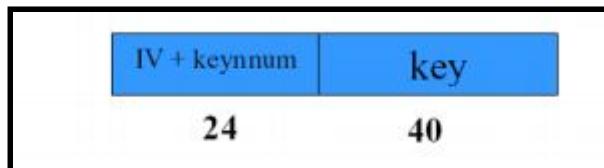


- ❖ **CRC:** Partim de la trama que es vol enviar. Aquesta trama sense xifrar està composta per una capçalera (Header) i conté unes dades (Payload). El primer pas és calcular el CRC de 32 bits del payload de la trama que es vol enviar.
- El CRC és un algoritme que genera un identificador únic del payload en concret, que ens servirà per verificar que el payload rebut és el mateix que el enviat, ja que el resultat del CRC serà el mateix.
 - Afegim aquest CRC a la trama com a valor de revisió d'integritat (ICV: Integrity Check Value):



Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

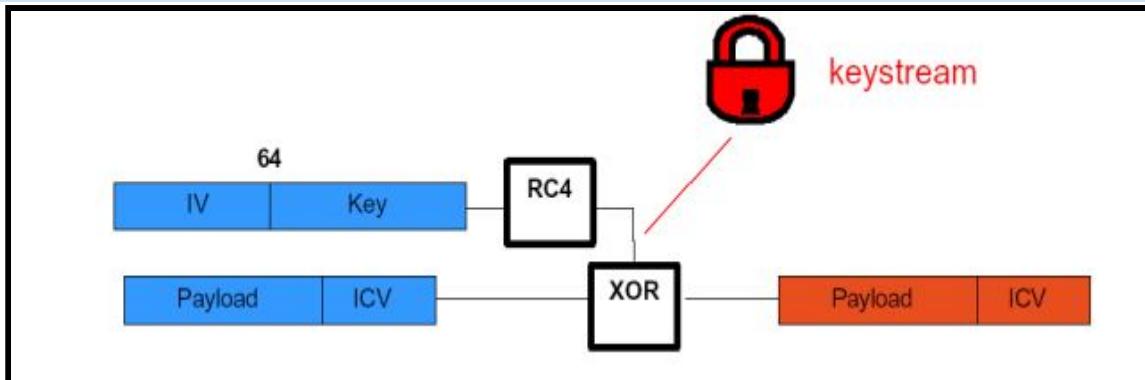
- D'altra banda vam seleccionar una clau de 40 bits, de les 4 claus possibles i afegim el **Vector d'Inicialització (IV)** de 24 bits al principi de la clau seleccionada:



❖ **Vector d'Inicialització (IV)**

- El IV és simplement un comptador que sol anar canviant de valor a mesura que anem enenyant trames, tot i que segons l'estàndard 802.11b també pot ser sempre zero.
- Amb el IV de 24 bits i la clau de 40 aconseguim els 64 bits de clau total que utilitzarem per a xifrar la trama. En el cas d'utilitzar encriptació de 128 bits tindriem 24 bits de IV i 104 de clau.
- Apliquem l'algoritme RC4 al conjunt IV + Key i aconseguirem el keystream o flux de clau. Realitzant una operació XOR amb aquest keystream i el conjunt Payload + ICV obtindrem el payload + ICV xifrat.

Aquest procés es pot veure en el següent gràfic. S'utilitza el IV i la clau per xifrar el Payload + ICV



Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

5. Quina és la diferència fonamental entre el WPA empresarial i el WPA Personal? El teu punt d'accés WIFI que utilitza?[1 punt]

La diferència fonamental és que WPA empresarial requereix de l'utilització d'un servidor RADIUS independent per gestionar l'autenticació dels usuaris a través del nom i contrasenya

- **WPA-Personal:** utilitza un sistema de codis PSK o claus precompartides on l'administrador especifica la seva pròpia contrasenya i tots els usuaris es connecten a la xarxa amb ella, de manera que sigui més fàcil de recordar-la.
- **WPA-Empressarial :** Enfocat a empreses, aquest sistema de seguretat es basa en un servidor RADIUS en el qual els usuaris han d'autenticar-se amb un usuari i una contrasenya diferent per a tots, en lloc de connectar-se tots amb una contrasenya global

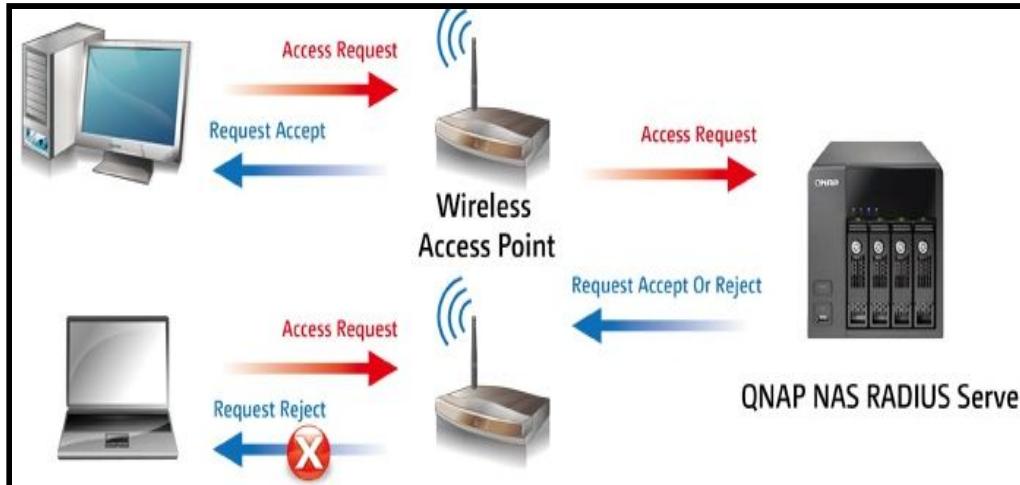
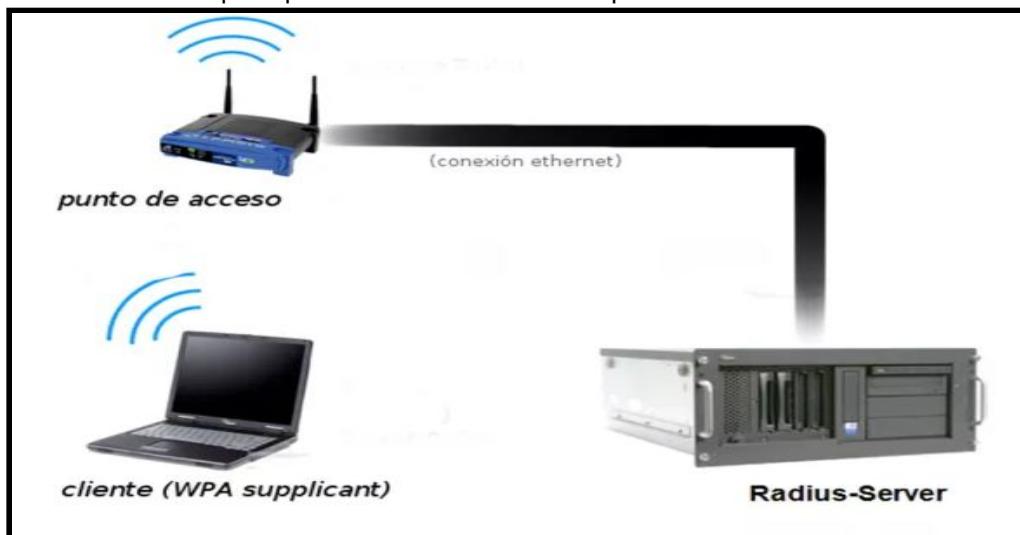
Security Standards Comparison			
Standards	Authentication Method	Encryption Standard	Cipher
802.11 Legacy 802.11a,b,g	Open system or Shared Key	WEP	RC4
WPA Personal	WPA Passphrase (PSK)	TKIP	RC4
WPA Enterprise	802.1x EAP, PEAP, EAP-TLS	TKIP	RC4
WPA2 Personal	WPA Passphrase (PSK)	CCMP TKIP	AES RC4
WPA2 Enterprise	802.1x EAP, PEAP, EPA-TLS	CCMP TKIP	AES RC4

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

6. Que és un servidor Radius?[1 punt]

SERVIDOR RADIUS: És una màquina connectada per cable al punt d'accés, que s'encarrega de les peticions d'autenticació a aquest servidor (normalment pel port UDP 1812 i 1813). Els servidors Radius també es fan servir, per exemple, quan un ISP vol validar les dades de la subscripció.

- **RADIUS (Remote Access Dial In User Service)** és un protocol que destaca sobretot per oferir un mecanisme de seguretat, flexibilitat, capacitat d'expansió i una administració simplificada de les credencials d'accés a un recurs de xarxa.
 - Aquest protocol s'utilitza en una arquitectura client-servidor



Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

7. Degut a la complexitat de les claus WPA, hi ha programes com el Pyrit que s'enfoquen aprofitar la potència gràfica de les GPU per trencar els codis. Explica en què consisteix un atac de força bruta, que és Pyrit amb exemples de captures del programa i que són els CUDA Cores i com estan relacionats amb els atacs de força bruta.[3 punts]

Pyrit li permet crear bases de dades massives de la fase d'autenticació WPA / WPA2-PSK pre-computada en un intercanvi d'espai-temps.

- En utilitzar el poder computacional de les CPUs de múltiples nuclis i altres plataformes a través de ATI-Stream, Nvidia CUDA i OpenCL
- Està escrit amb llenguatge Python ,és un programa de codi lliure de GPLv3
- Una característica bàsica de Pyrit es que permet dedicar els recursos de la GPU (la potència de la nostra tarjeta de video al crack de claus WPA
- Actualment **és l'atac més poderós contra un dels protocols de seguretat més utilitzats del món**

Els sistemes que permeten accedir a **Pyrit a les GPUs de les targetes gràfiques són CUDA** (en el cas de gràfiques **Nvidia**) i Stream (en el cas de ATI)

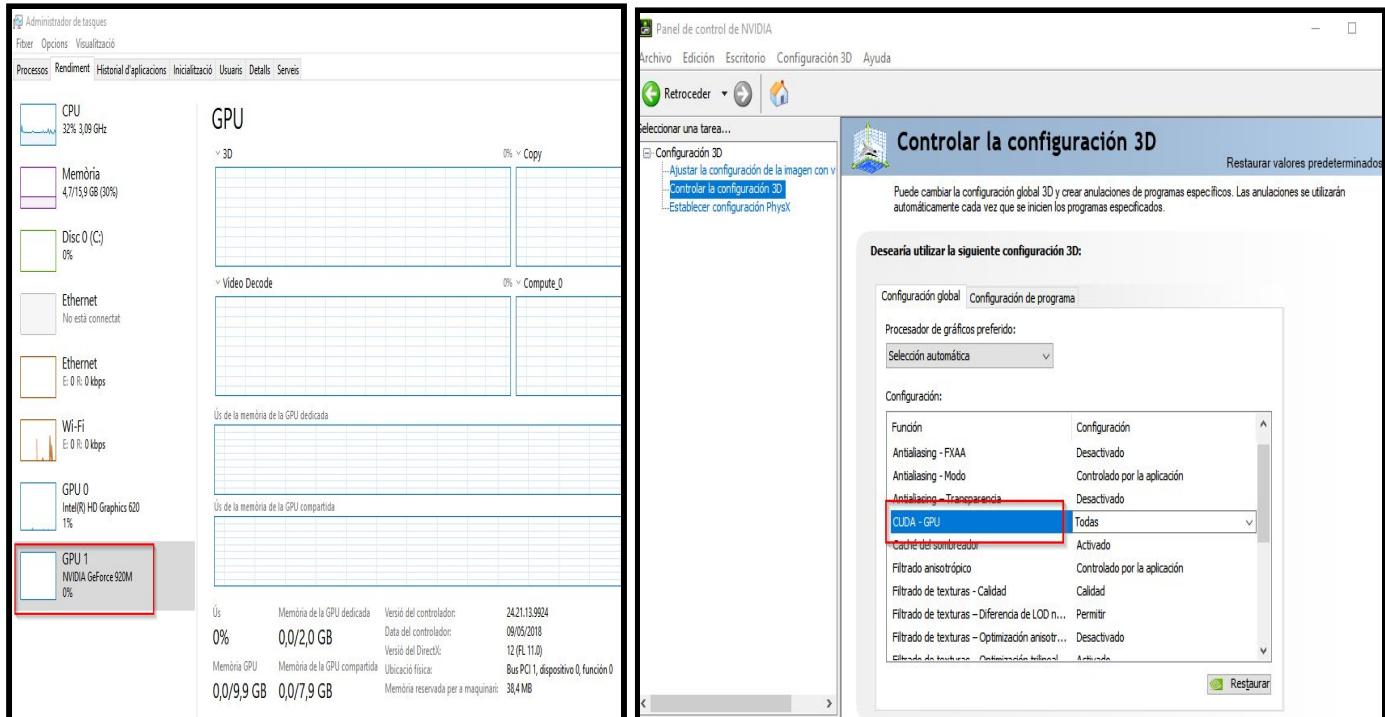
- Tan CUDA com Stream són tecnologies relativament recents i només suporten una sèrie de models més o menys nous

Cuda és una plataforma de computació paral·lela i un model de programació desenvolupat per NVIDIA per a computació general en unitats de processament gràfic (GPU). **Amb CUDA, els desenvolupadors poden accelerar dràsticament les aplicacions informàtiques aprofitant el poder de les GPU.**

- En les aplicacions accelerades per GPU, la part seqüencial de la càrrega de treball s'executa en la CPU, que està optimitzada per al rendiment d'un sol subprocess, mentre que la part d'ús intensiu de càlcul s'executa en milers de nuclis de GPU en paral·lel.
- Quan s'utilitza CUDA, els desenvolupadors programen en llenguatges populars com a C, C++, Fortran, Python i MATLAB i expressen el paral·lelisme a través d'extensions en forma d'algunes paraules clau bàsiques.
- El kit d'eines CUDA de NVIDIA ofereix tot el que necessita per a desenvolupar aplicacions accelerades per GPU. El kit d'eines CUDA inclou biblioteques accelerades per GPU, un compilador, eines de desenvolupament i el temps d'execució CUDA.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

En aquest imatge del meu host, es pot veure una exemple de GPU Nvidia (GPU1)



Els mètodes de xifrat de les xarxes sense fils actuals no són prou segurs, cabent sempre la posibilidad de ser sabotejades. En els casos particulars de **xifrat WPA** l'atac més habitual és l'ús d'atac mitjançant diccionari, o més aviat conegut com a atac de **força bruta**, que **CUDA** facilita enormement la qüestió.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

Pyrit

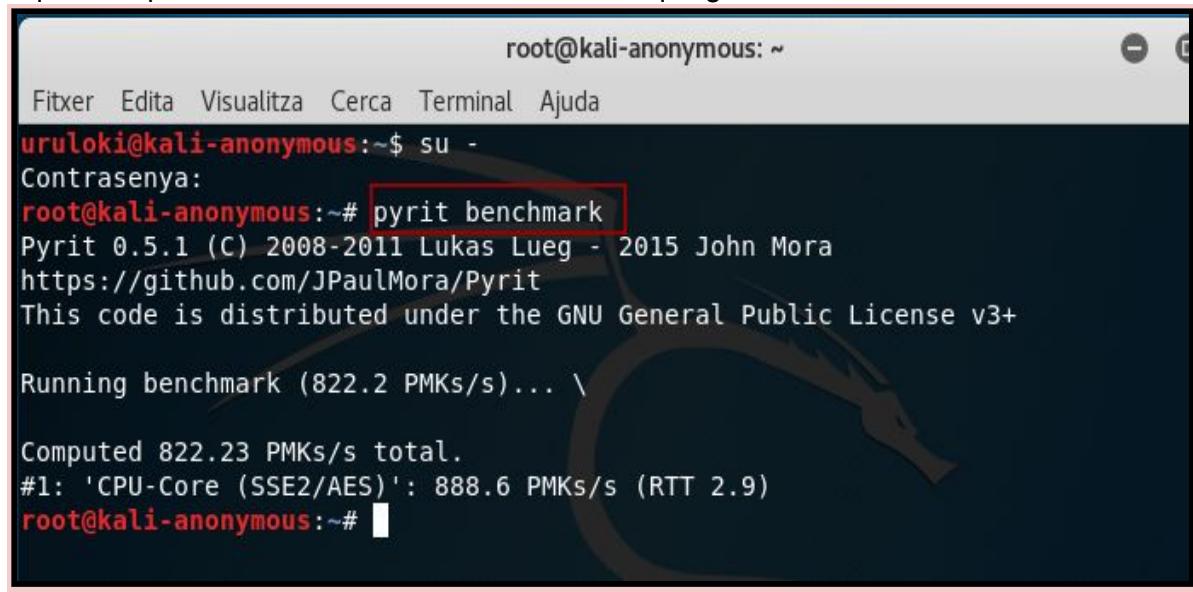
Per veure les eines incloses en **Pyrit** (ja està inclòs en Kali Linux)

```
root@kali-anonymous:~#
Fitxer Edita Visualitza Cerca Terminal Ajuda
striplive      : Capture relevant packets from a live capture-source
verify        : Verify 10% of the results by recomputation
root@kali-anonymous:~# pyrit -h | more
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+
Usage: pyrit [options] command
Recognized options:
 -b          : Filters AccessPoint by BSSID
 -e          : Filters AccessPoint by ESSID
 -h          : Print help for a certain command
 -i          : Filename for input ('-' is stdin)
 -o          : Filename for output ('-' is stdout)
 -r          : Packet capture source in pcap-format
 -u          : URL of the storage-system to use
 --all-handshakes : Use all handshakes instead of the best one
 --aes       : Use AES
```

```
root@kali-anonymous:~# pyrit list_cores
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+
The following cores seem available...
#1: 'CPU-Core (SSE2/AES)'
```

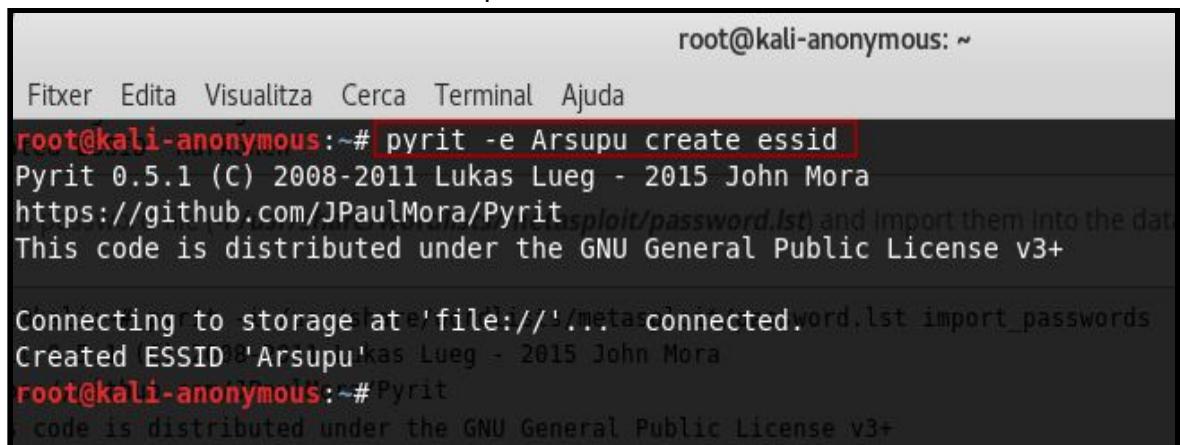
Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

Aquesta opció calcula i mostra la velocitat de craqueig dels seus sistemes



```
root@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ su -
Contrasenya:
root@kali-anonymous:~# pyrit benchmark
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+
Running benchmark (822.2 PMKs/s)... \
Computed 822.23 PMKs/s total.
#1: 'CPU-Core (SSE2/AES)': 888.6 PMKs/s (RTT 2.9)
root@kali-anonymous:~#
```

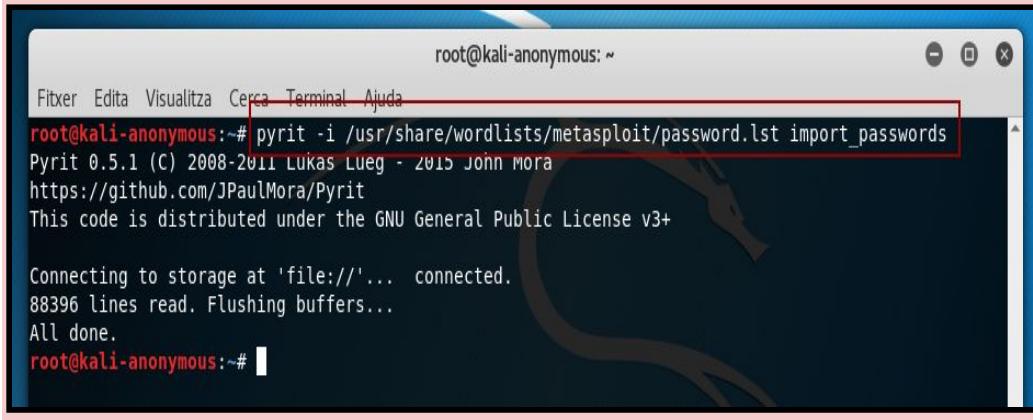
Creació d'un ESSID amb el nom Arsupu



```
root@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
root@kali-anonymous:~# pyrit -e Arsupu create essid
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+
Connecting to storage at /file:///tmp/.connectedword.lst import_passwords
Created ESSID 'Arsupu' Lukas Lueg - 2015 John Mora
root@kali-anonymous:~# Pyrit
This code is distributed under the GNU General Public License v3+
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

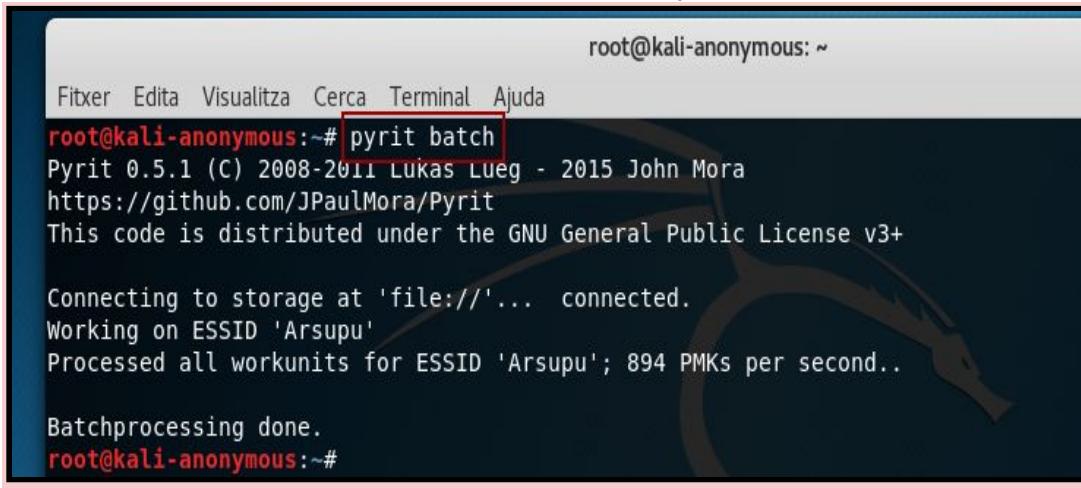
Llegeix un arxiu de contrasenya : **pyrit -i /usr/share/wordlists/metasploit/password.lst** i s'importa a la base de dades (**import_passwords**).



```
root@kali-anonymous:~# pyrit -i /usr/share/wordlists/metasploit/password.lst import_passwords
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'... connected.
88396 lines read. Flushing buffers...
All done.
root@kali-anonymous:~#
```

Calculi els PMK utilitzant el ESSID i les contrasenyes



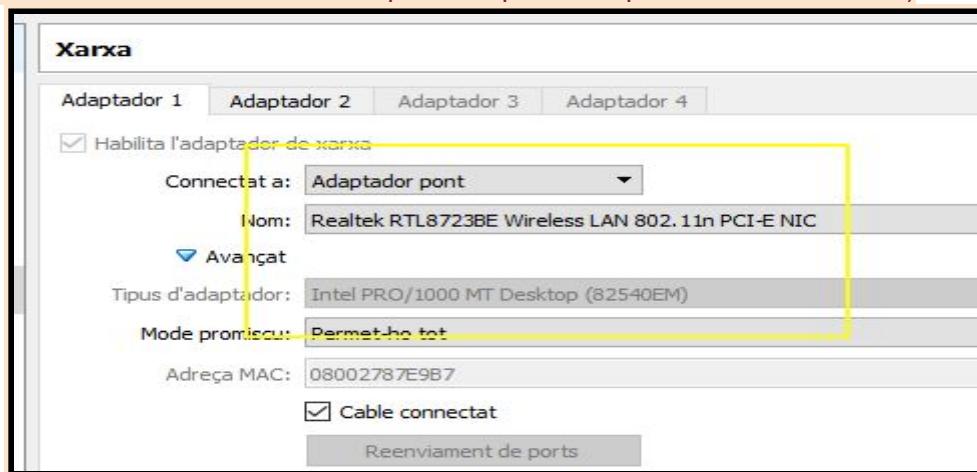
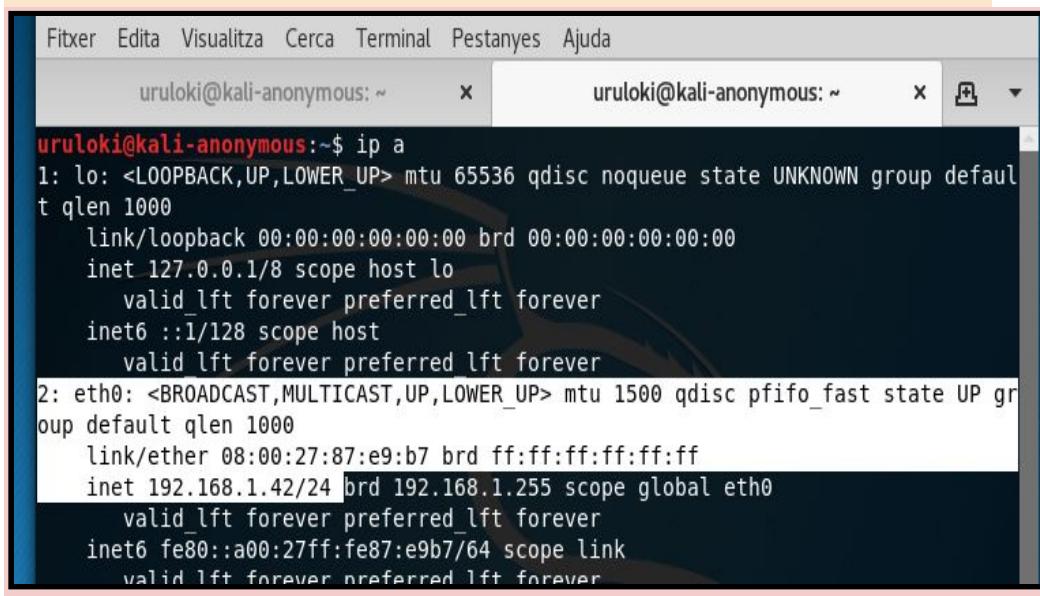
```
root@kali-anonymous:~# pyrit batch
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'... connected.
Working on ESSID 'Arsupu'
Processed all workunits for ESSID 'Arsupu'; 894 PMKs per second..

Batchprocessing done.
root@kali-anonymous:~#
```

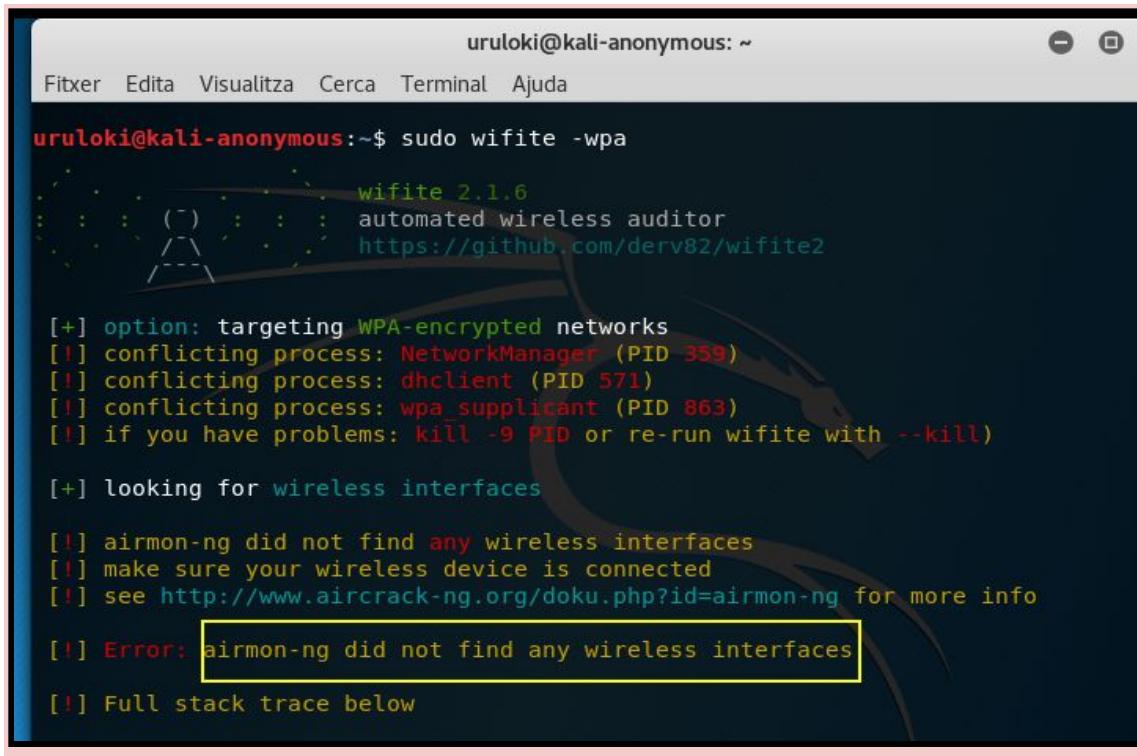
Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019

He tingut el problema que estic fent servir una màquina virtual, i encara que utilitizi adaptador pont (amb la tarjeta wireless) realment utilitzà "cable virtual amb el meu host físic". Pyrit està però no podrà fer realment la seva feina amb VirtualBox.(hauria de tenir una targeta de xarxa inalàmbrica usb o tenir un Kali portable per no dependre del VirtualBox)

```
uruloki@kali-anonymous:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:87:e9:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.42/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe87:e9b7/64 scope link
        valid_lft forever preferred_lft forever
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	01-02-2019



```
uruloki@kali-anonymous:~$ sudo wifite -wpa
[+/-] : wifite 2.1.6
[+/-] : automated wireless auditor
[+/-] : https://github.com/derv82/wifite2

[+] option: targeting WPA-encrypted networks
[!] conflicting process: NetworkManager (PID 359)
[!] conflicting process: dhclient (PID 571)
[!] conflicting process: wpa_supplicant (PID 863)
[!] if you have problems: kill -9 PID or re-run wifite with --kill

[+] looking for wireless interfaces

[!] airmon-ng did not find any wireless interfaces
[!] make sure your wireless device is connected
[!] see http://www.aircrack-ng.org/doku.php?id=airmon-ng for more info
[!] Error: airmon-ng did not find any wireless interfaces
[!] Full stack trace below
```

Com que no he pogut fer-ho, he buscat una captura del crackeig de password



```
File Edit View Terminal Help
root@bt:~# pyrit -r crack-01.cap -i /root/Desktop/Password.txt attack_passthrough
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+
Parsing file 'crack-01.cap' (1/1)...
Parsed 6 packets (6 802.11-packets), got 1 AP(s)

Picked AccessPoint 84:c9:b2:6a:a9:be ('Crack') automatically.
Tried 1 PMKs so far; 5 PMKs per second.

The password is '12332112'.
root@bt:~#
```