Royaume du Maroc
UNIVERSITÉ HASSAN II DE CASABLANCA
NATIONALE SUPÉRIEURE D'ÉLECTRICITÉ ET DE MÉCANIQUE

ENSEM

المملكة المغربية
جامعة الحسن الثاني بالدار البيضاء
مدرسة الوطنية العليا للكهرباء والميكانيك

Mini projet :

Mise en œuvre d'un VPN avec Open VPN sous Linux

Elaboré par : **MERYEM ESSAFI**

Encadré par : **Mr. BOUKHDIR**

Année universitaire : 2021/2022

OBJECTIF DU PROJET :

L’objectif de ce mini-projet est de mettre en œuvre un Virtual Private Network (VPN) avec open VPN sous Linux

MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d’électricité et de mécanique

REMERCIEMENT

Nous remercions Mr Boukhdir, enseignant, de par sa disponibilité à répondre à toutes les questions liées à la réalisation de ce mini-projet.

Et Au terme de ce projet, nous tenons à témoigner notre profonde reconnaissance à notre cher professeur pour son encadrement et son encouragement, ses précieux conseils, et pour l'intérêt qu'il a porté pour ce travail ainsi que de nous avoir donner l'opportunité d'avoir une expérience en domaine de sécurité informatique, qui est un domaine vaste et très intéressant.

Ce genre de travaux est indispensable car ils peuvent nous servir dans plusieurs situations. Grâce à vous, on est désormais capable de manipuler l'outil **Open VPN**.

SOMMAIRE

INTRODUCTION

La sécurité informatique consiste à protéger un système informatique contre toute violation, intrusion, dégradation ou vol de données au sein du système d'information.

Avec **l'essor d'internet**, et l'utilisation par la majorité des entreprises et des organisations de **processus informatisés**, les **menaces** visant les systèmes d'informations **n'ont cessés d'augmenter** et de **se sophistiquer**, faisant aujourd'hui de la sécurité informatique une **nécessité pour tous les types de structure**.

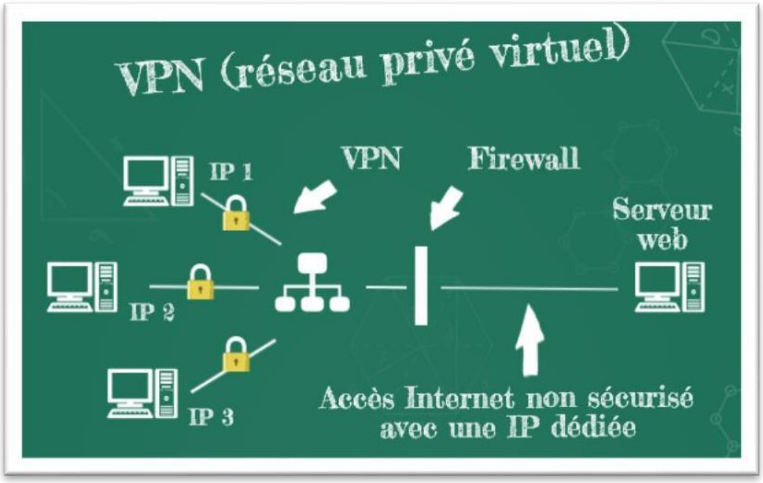
Définition de VPN

Un réseau privé virtuel (***Virtual Private Network***) est un tunnel sécurisé à l'intérieur d'un réseau (Internet notamment). Il permet d'échanger des informations de manière sécurisée et anonyme en utilisant une adresse **IP** différente de celle de votre ordinateur.

Ce système est pratique pour surfer sur Internet avec une localisation différente de la vôtre. Un autre intérêt est le faible coût de l'accès Internet, à partir de 2,75 euros par mois pour les services les plus courants.

Le VPN est parfaitement légal : de nombreuses entreprises y ont recours pour protéger les échanges d'informations entre deux filiales à l'étranger par exemple.

➔ **Le VPN permet de surfer sur le web de manière anonyme et de choisir la géolocalisation de son adresse IP.**



Présentation de logiciel Open VPN

OpenVPN est une solution logicielle libre complète permettant de créer différentes configurations de VPN (Virtual Private Network) ou réseaux privés virtuels pour accéder à des ordinateurs distants, créer un tunnel sécurisé de site à site, sécuriser une connexion Wifi, etc.

Avec OpenVPN, vous allez pouvoir enfermer votre sous-réseau dans un tunnel, protéger un réseau avec de l'OpenSSL ou encore accéder à distance à un ordinateur. OpenVPN vous permet d'accéder à un réseau local distant de manière sécurisée afin de pouvoir consulter des fichiers hébergés sur des ordinateurs distants.

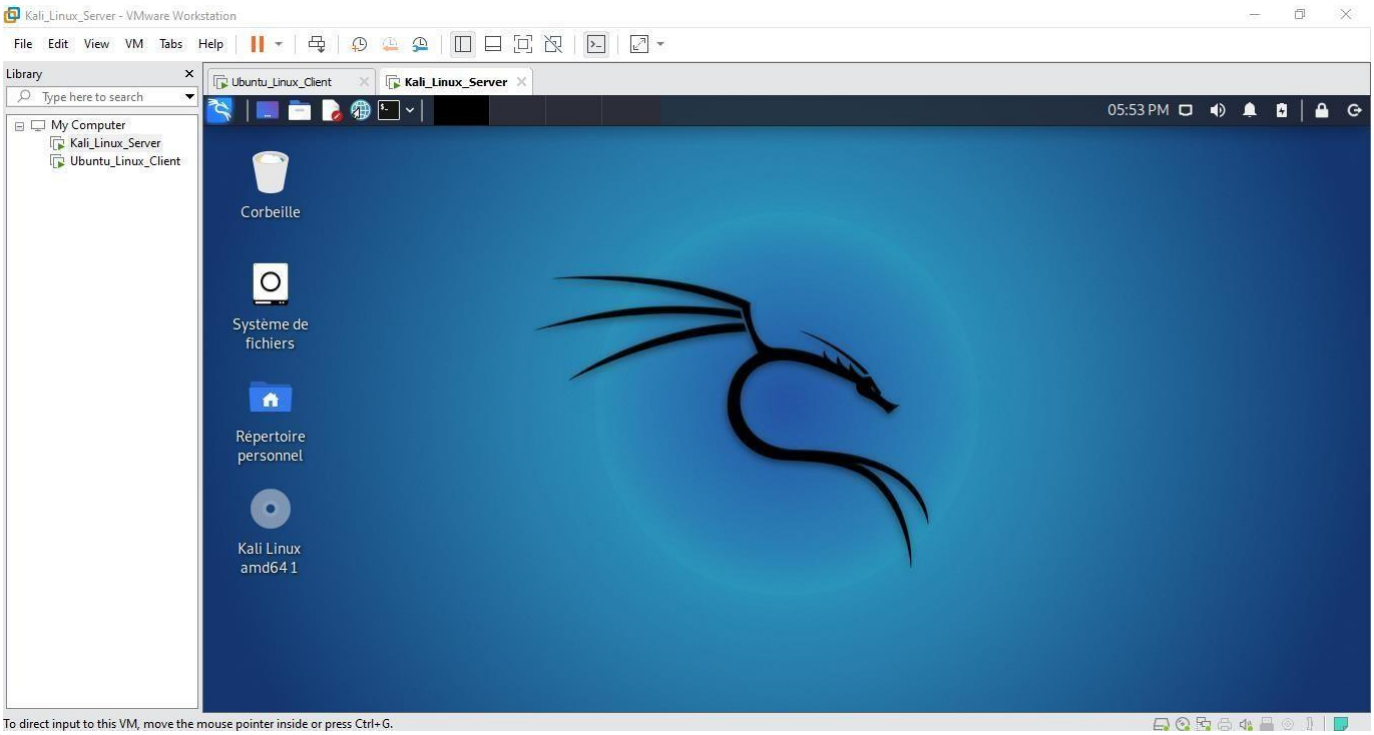
Mise en place d'un VPN compressé et non-crypté

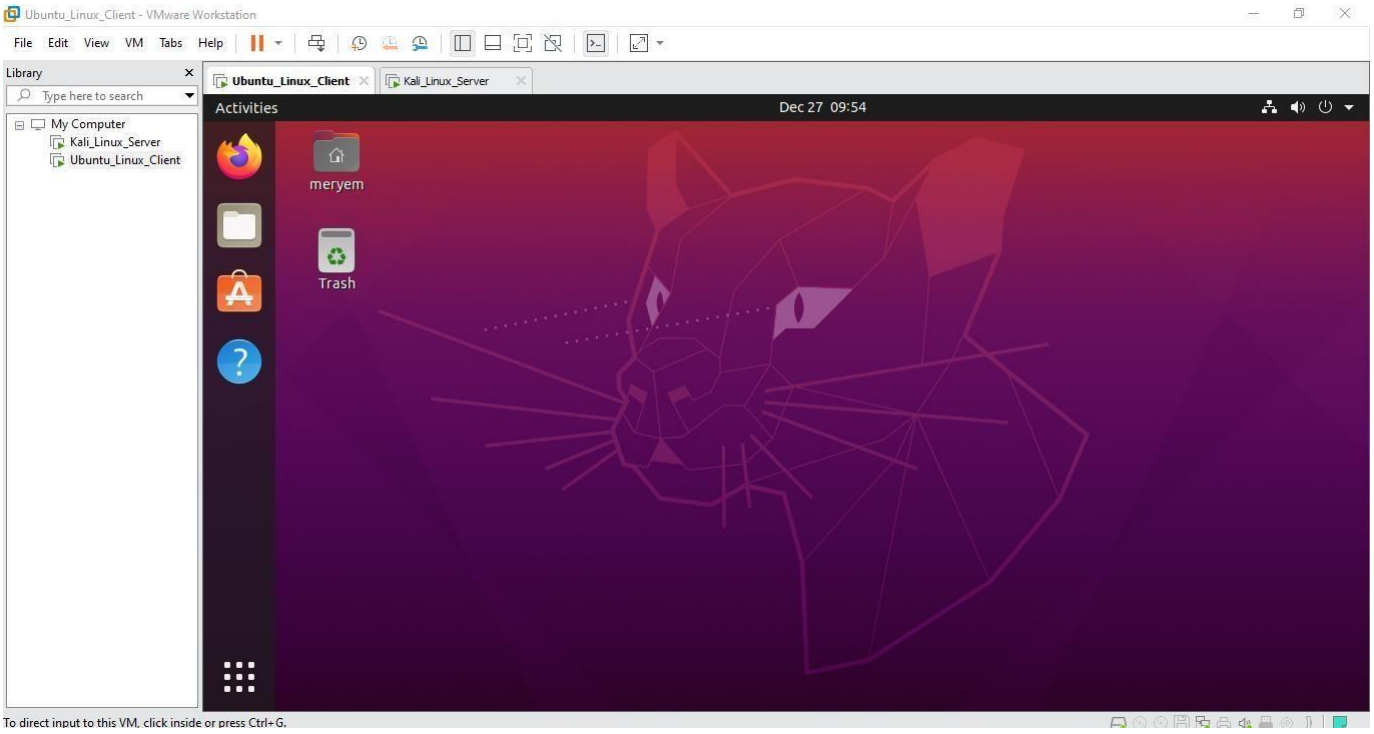
On démarre la machine virtuelle **VMware Workstation,** après l'installation de deux versions de Linux sous cette machine virtuelle : **Kali Linux et Ubuntu Linux.**

Le client : Ubuntu

Le serveur : Kali

Puis on lance les deux systèmes d'exploitation.

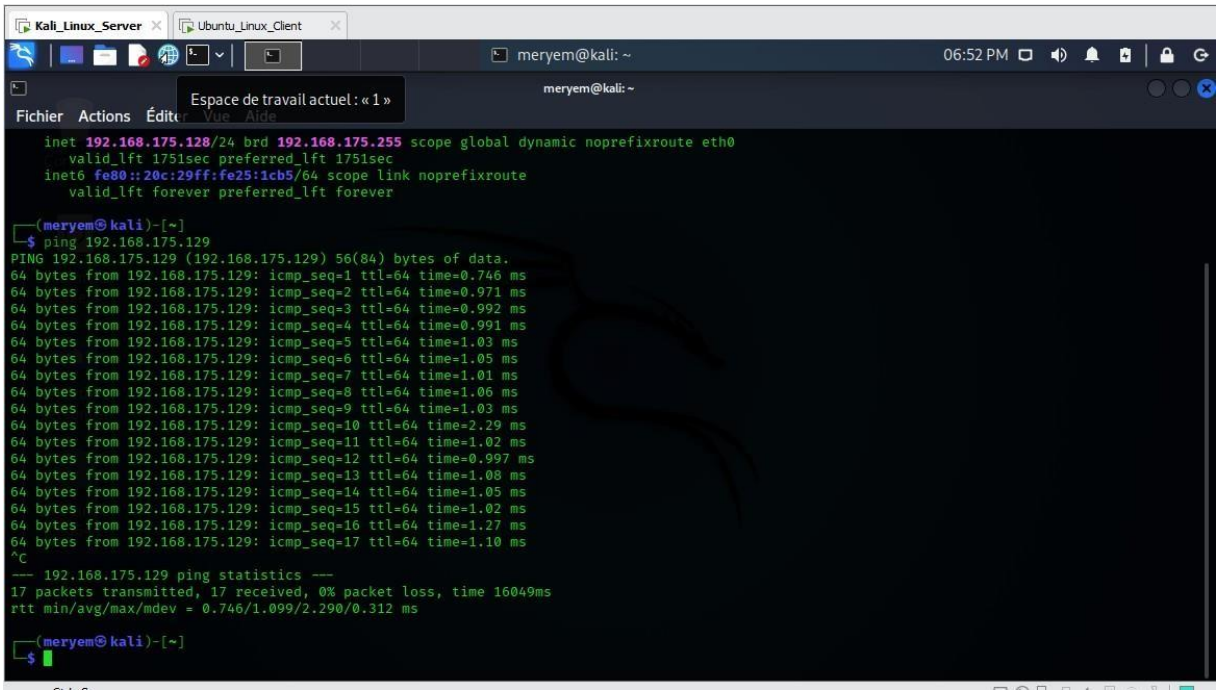




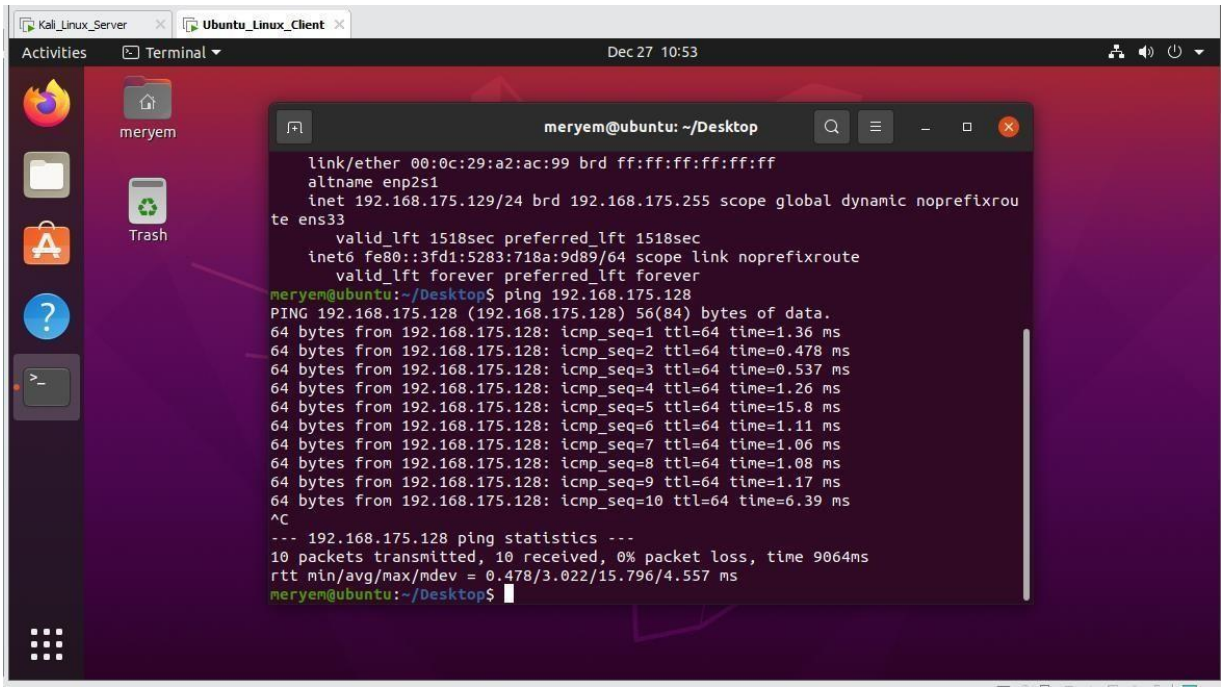
On fait la configuration nécessaire et on vérifier la connectivité.

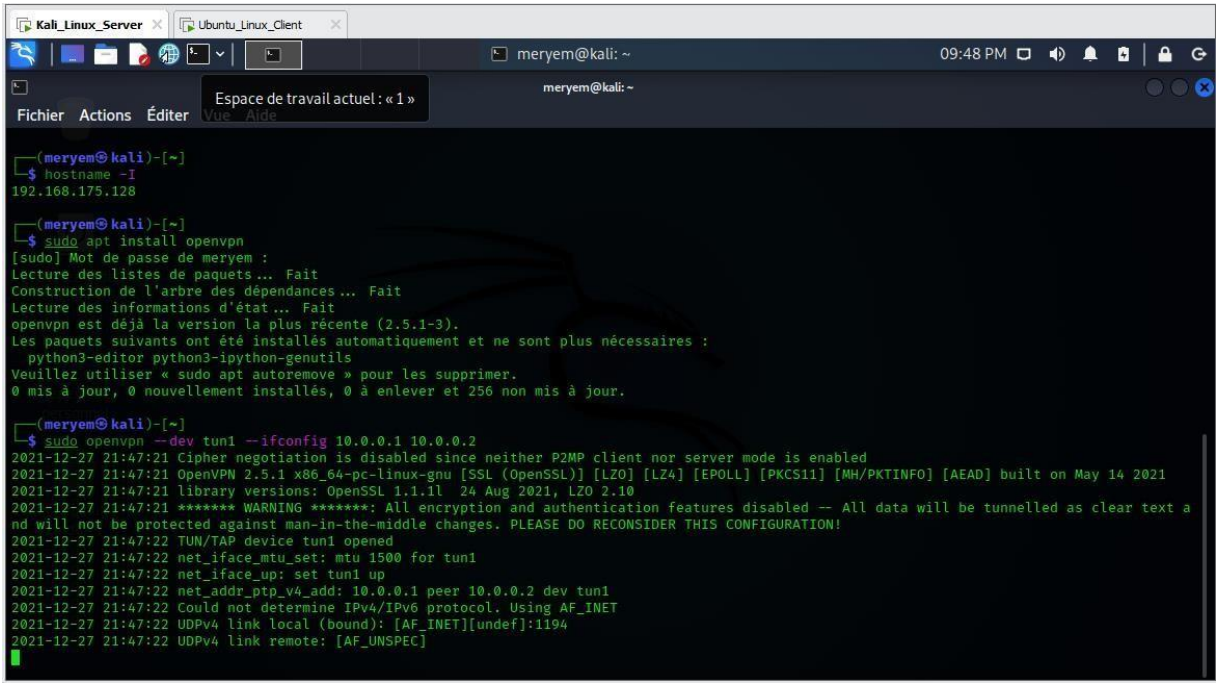
Pour tester la connectivite réseau, il existe la commande **ping.**

➔ Pour **la machine serveur Kali,** on tape la commande **ping** suivi par l'adresse IP de la machine client : 192.168.175.129.



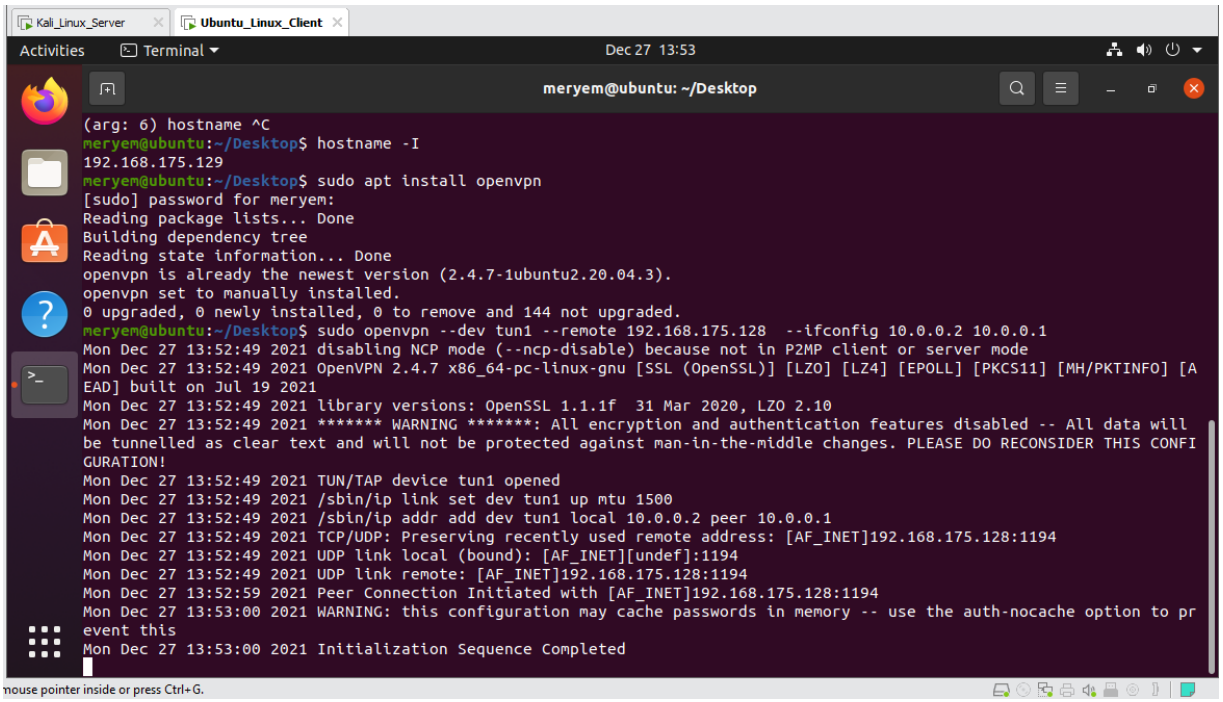
➔ Pour **la machine Client Ubuntu,** on tape la commande **ping** suivi par l'adresse IP de la machine Serveur : 192.168.175.128.



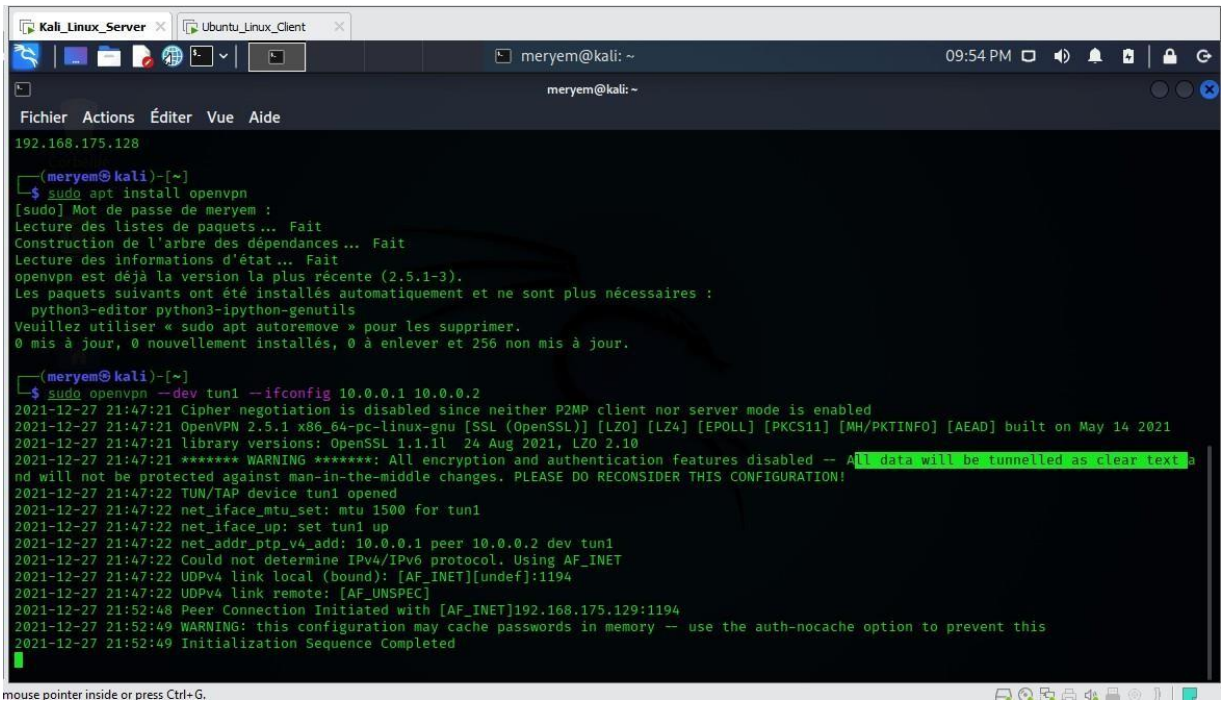


Pour avoir ces adresses IP, il suffit de taper la commande **hostname -I.**

Ensuite on essaye d'installer OpenVPN sur les deux machines.



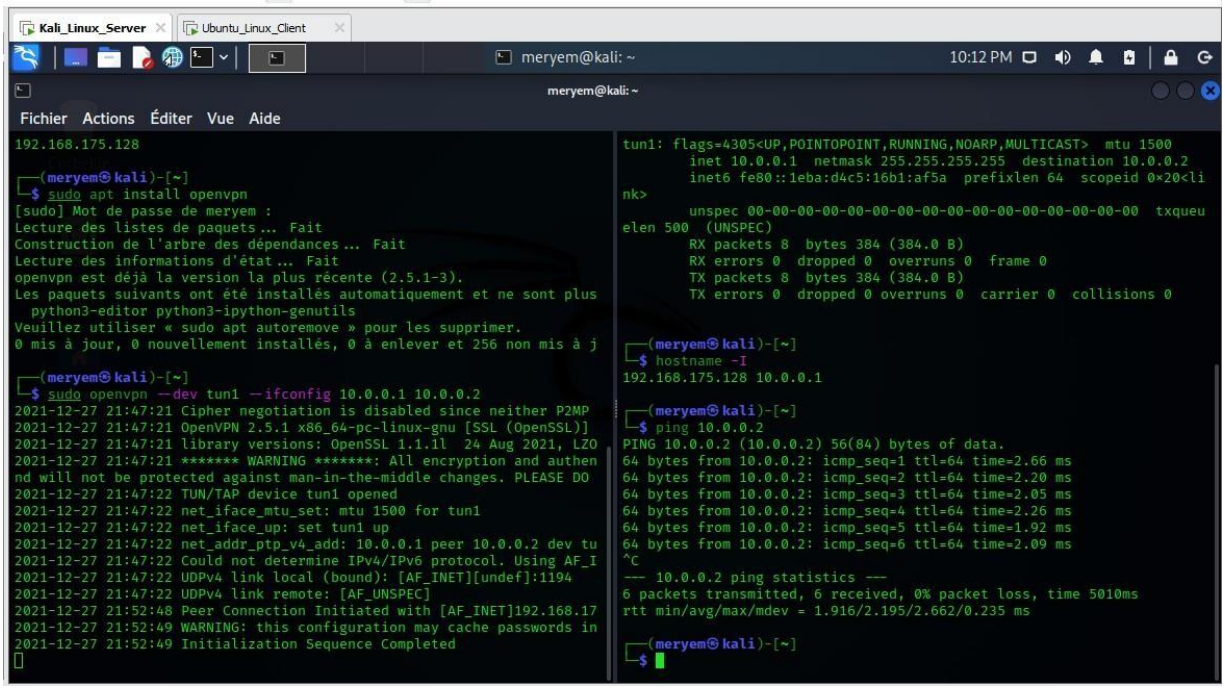
On va lancer le tunnel **tun1** à partir de la machine serveur.

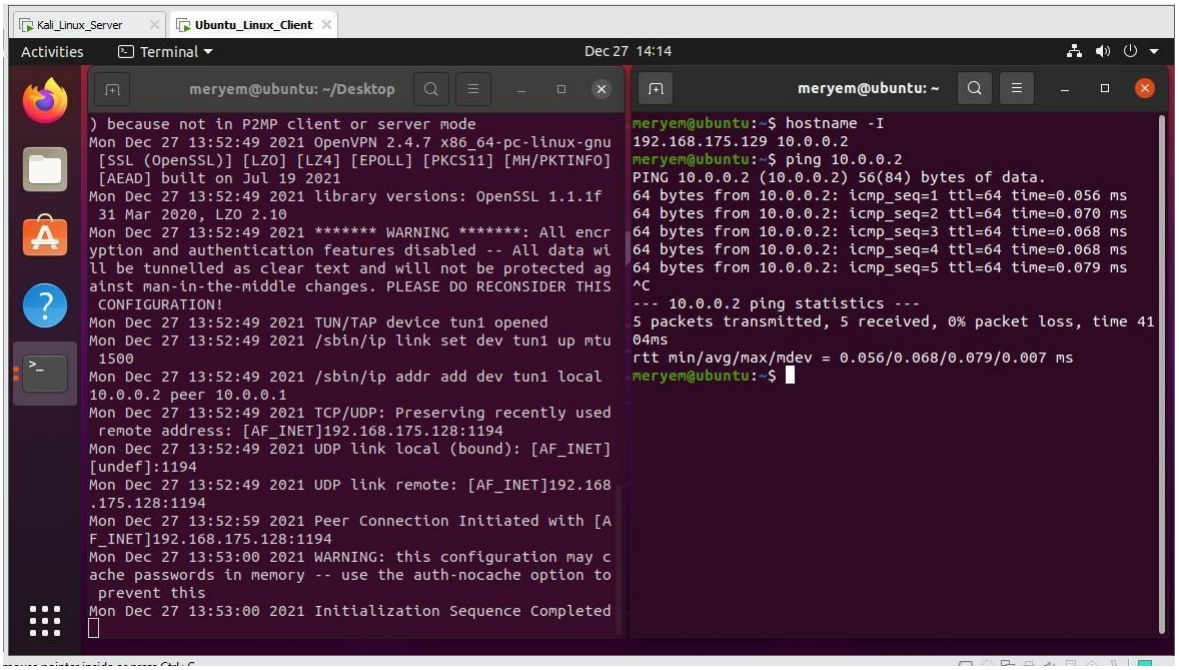


➔ Donc le tunnel est ouvert avec le port par défaut **1194**.

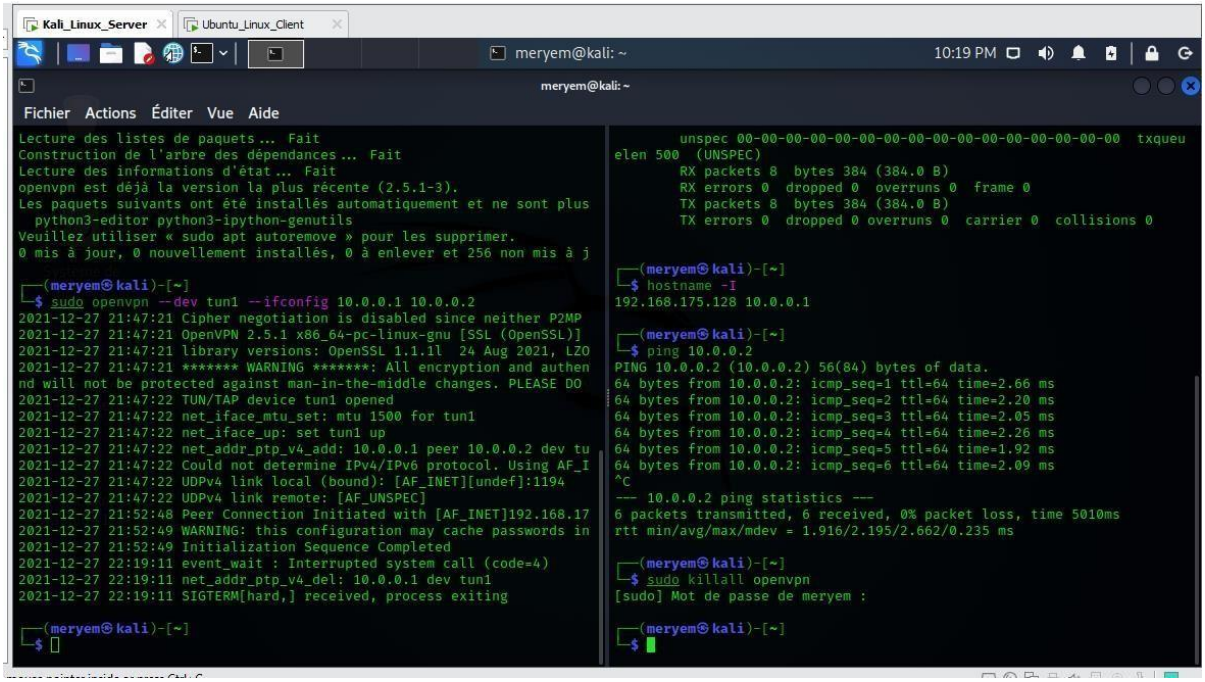
➔ Le Serveur en écoute.

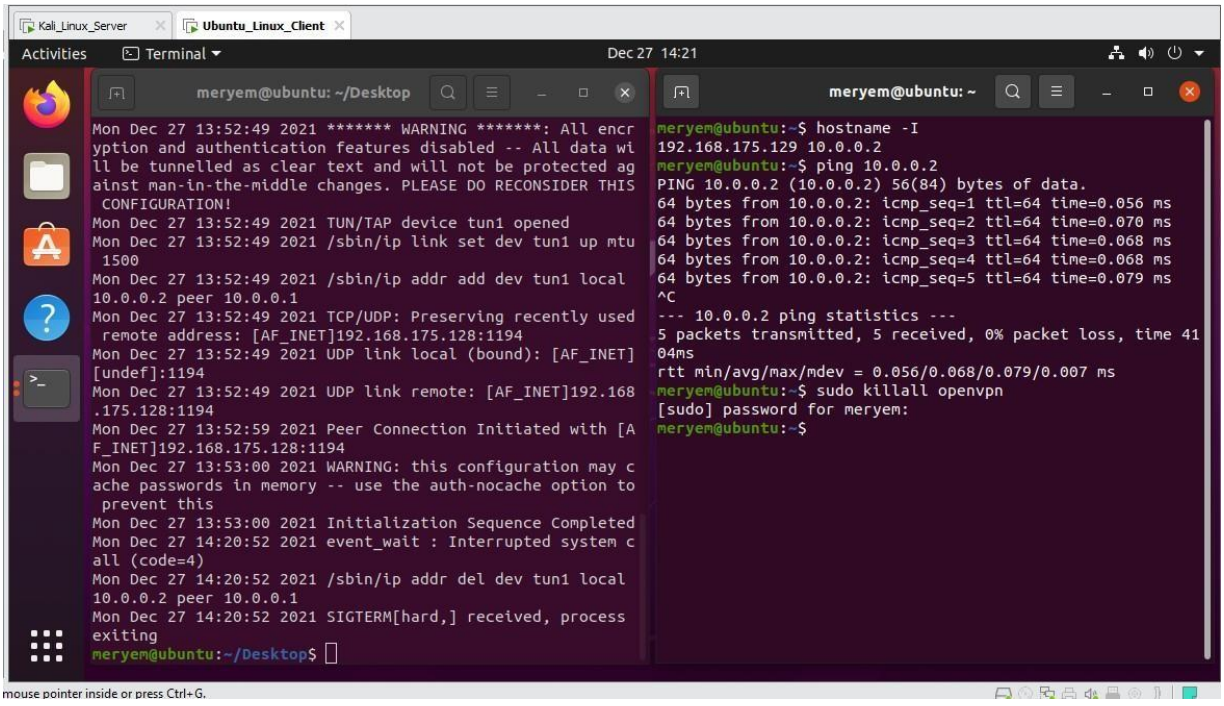
➔ On fera de même pour la machine Client (en **ajoutant l'adresse de la machine Serveur**).





MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d'électricité et de mécanique



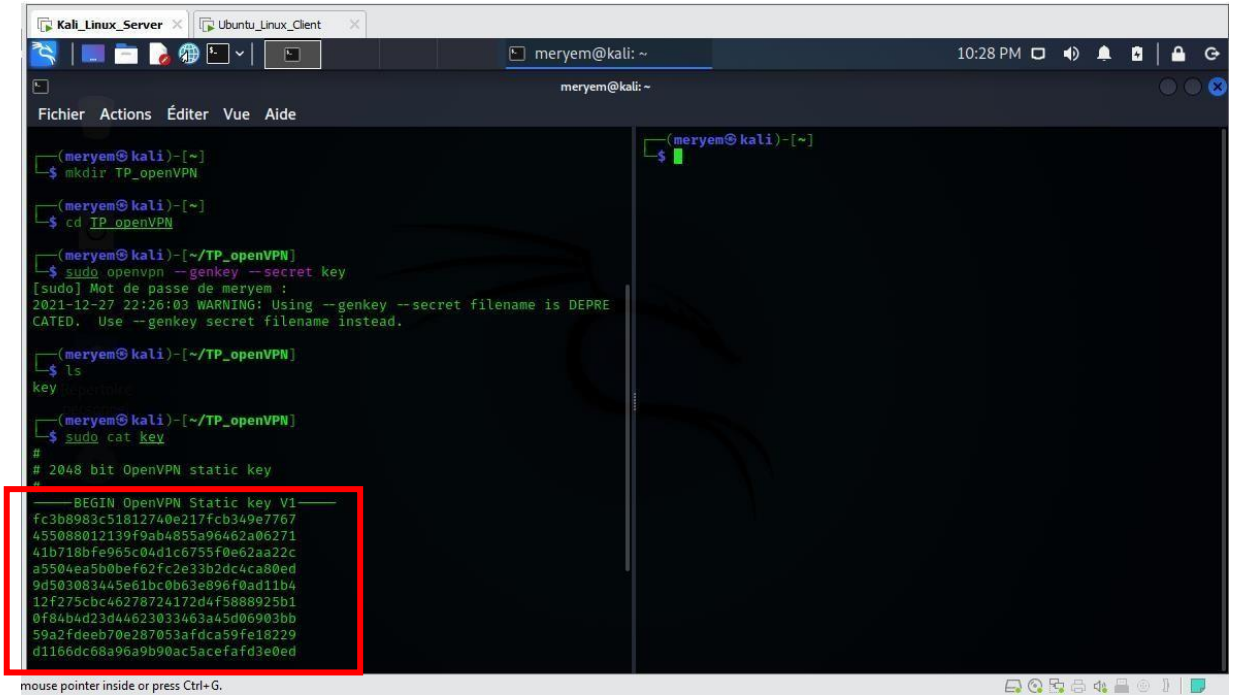


➔ Donc un tunnel virtuel est établi sans aucun problème (sans qu'il ça soit crypté).

➔ Pour passer a la deuxième parie on arrête le tunnel avec la commande **killall openvpn**.

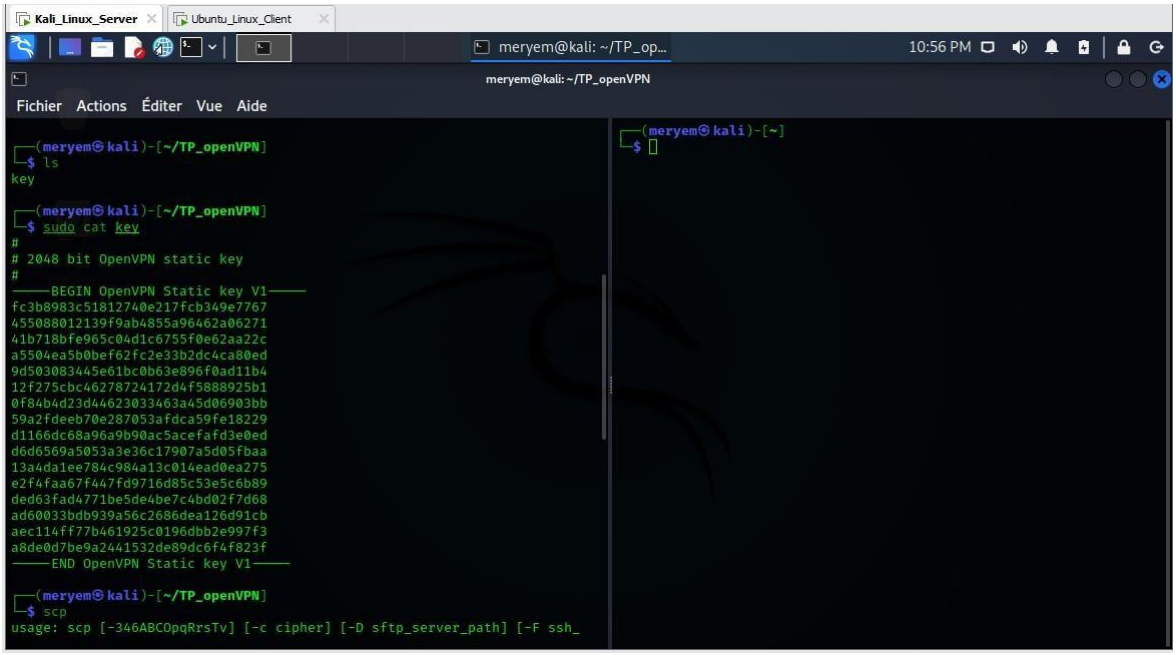
Partie 2

Dans cette partie, on va lancer les mêmes commandes tout en s'appuyions sur une clé partagée entre les deux machines.

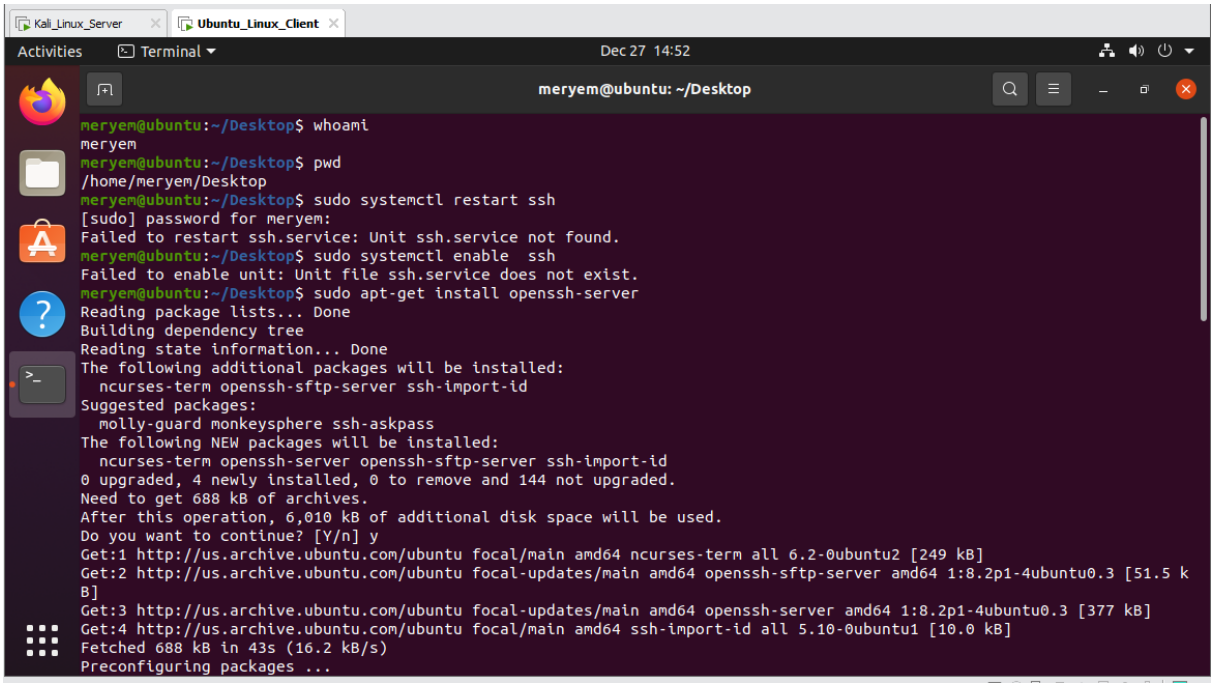


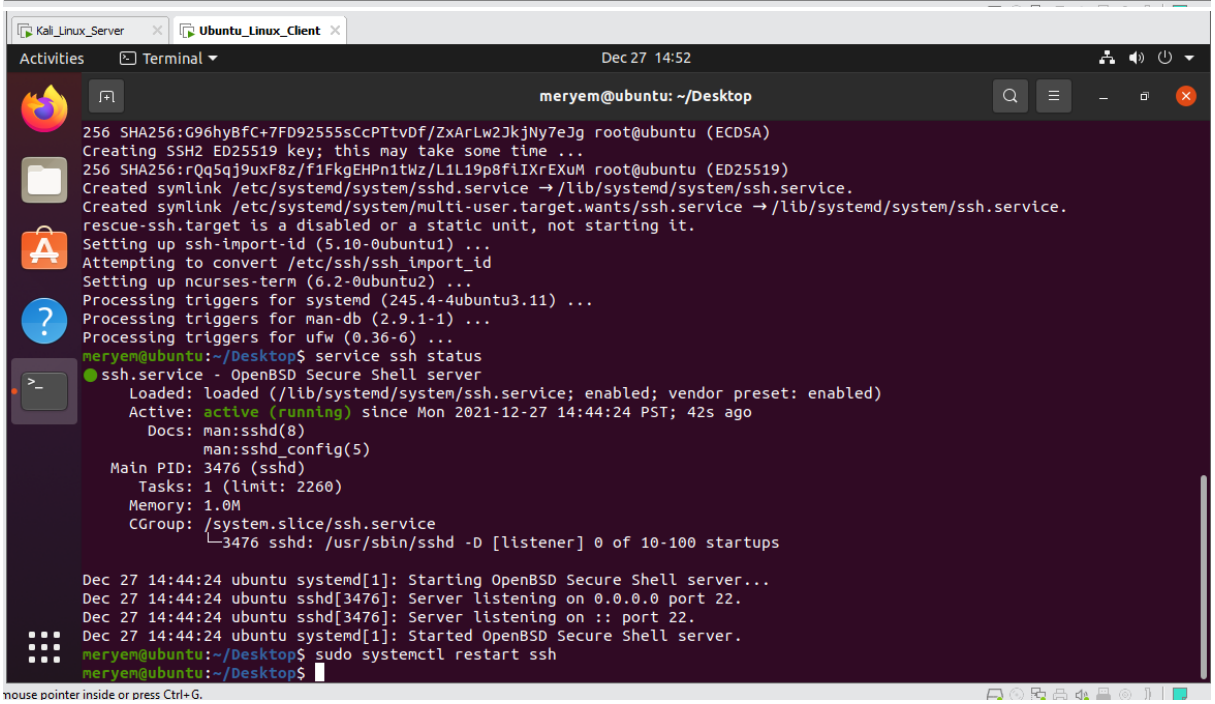
➔ On créer un répertoire : **TP_openVPN,** on y accède.

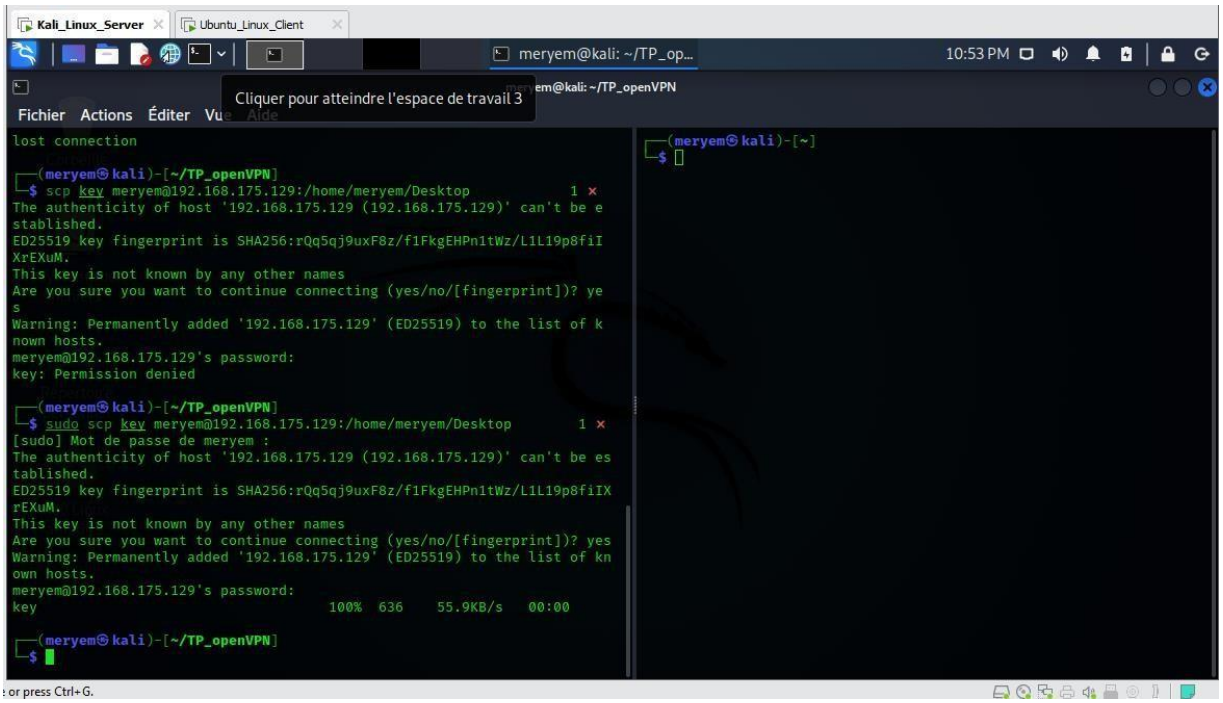
➔ Puis on va générer notre clé (clé de 2048 bit).

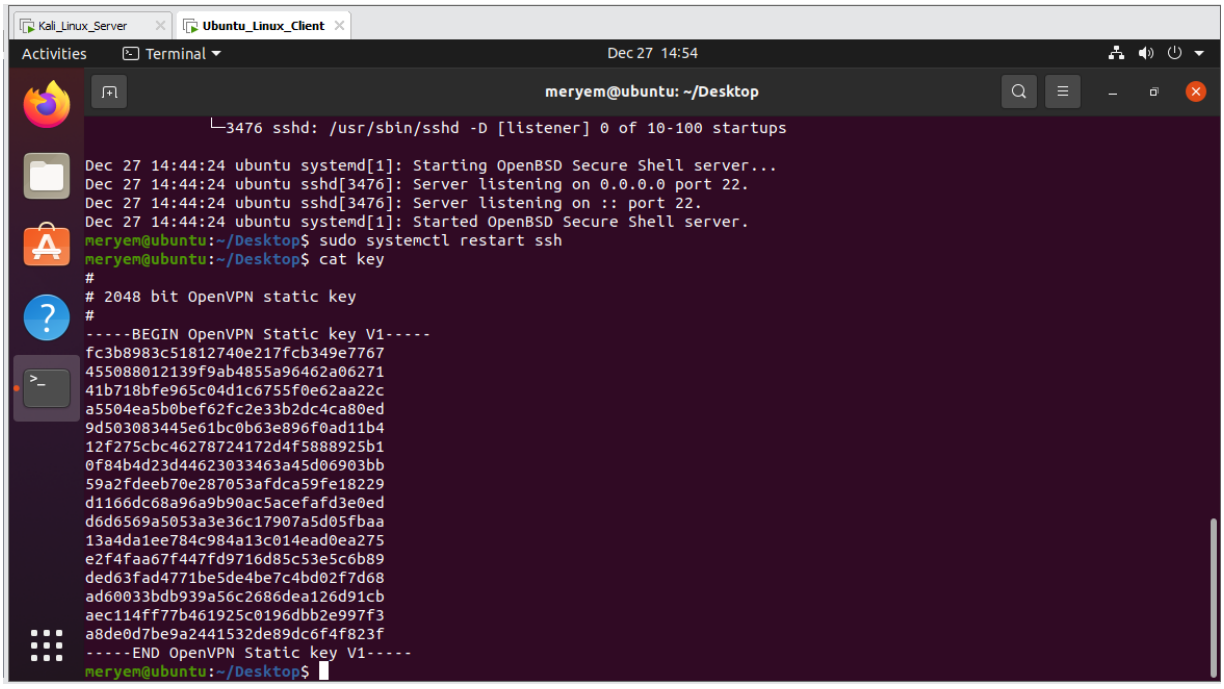


MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d'électricité et de mécanique

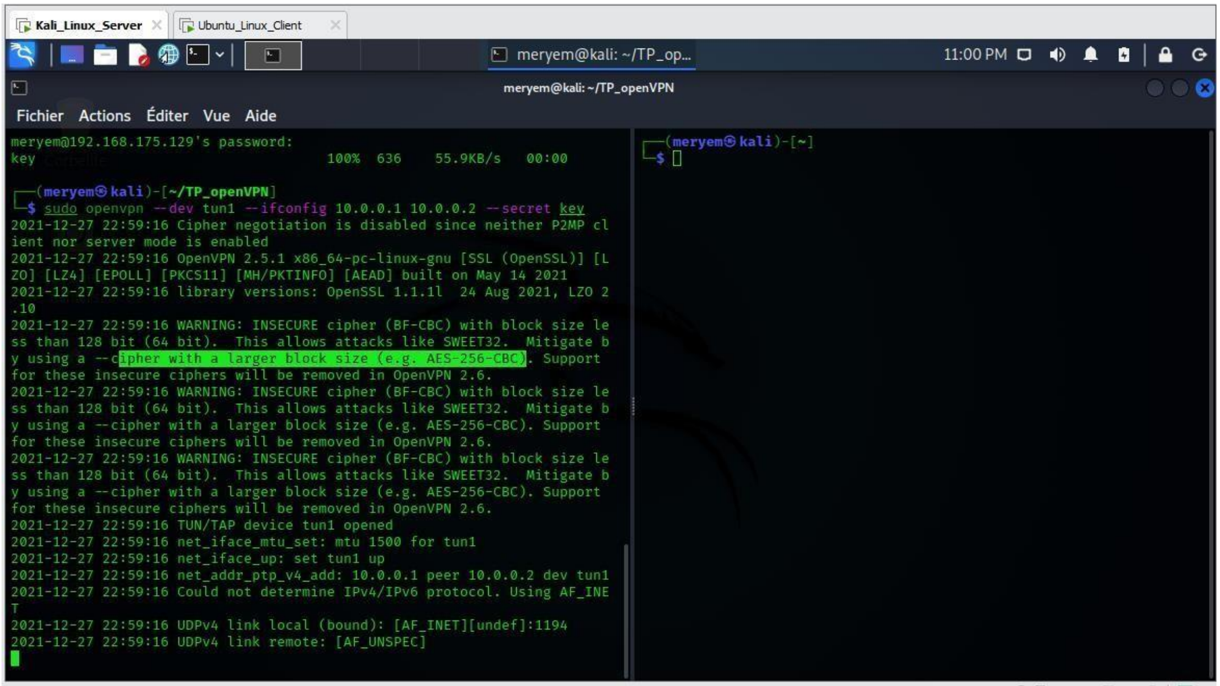

Kali_Linux_Server
Ubuntu_Linux_Client
Activities
Terminal
Dec 27 14:52
meryem@ubuntu: ~/Desktop
meryem@ubuntu:~/Desktop$ whoami
meryem
meryem@ubuntu:~/Desktop$ pwd
/home/meryem/Desktop
meryem@ubuntu:~/Desktop$ sudo systemctl restart ssh
[sudo] password for meryem:
Failed to restart ssh.service: Unit ssh.service not found.
meryem@ubuntu:~/Desktop$ sudo systemctl enable ssh
Failed to enable unit: Unit file ssh.service does not exist.
meryem@ubuntu:~/Desktop$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 144 not upgraded.
Need to get 688 kB of archives.
After this operation, 6,010 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 ncurses-term all 6.2-0ubuntu2 [249 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-sftp-server amd64 1:8.2p1-4ubuntu0.3 [51.5 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-server amd64 1:8.2p1-4ubuntu0.3 [377 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal/main amd64 ssh-import-id all 5.10-0ubuntu1 [10.0 kB]
Fetched 688 kB in 43s (16.2 kB/s)
Preconfiguring packages ...

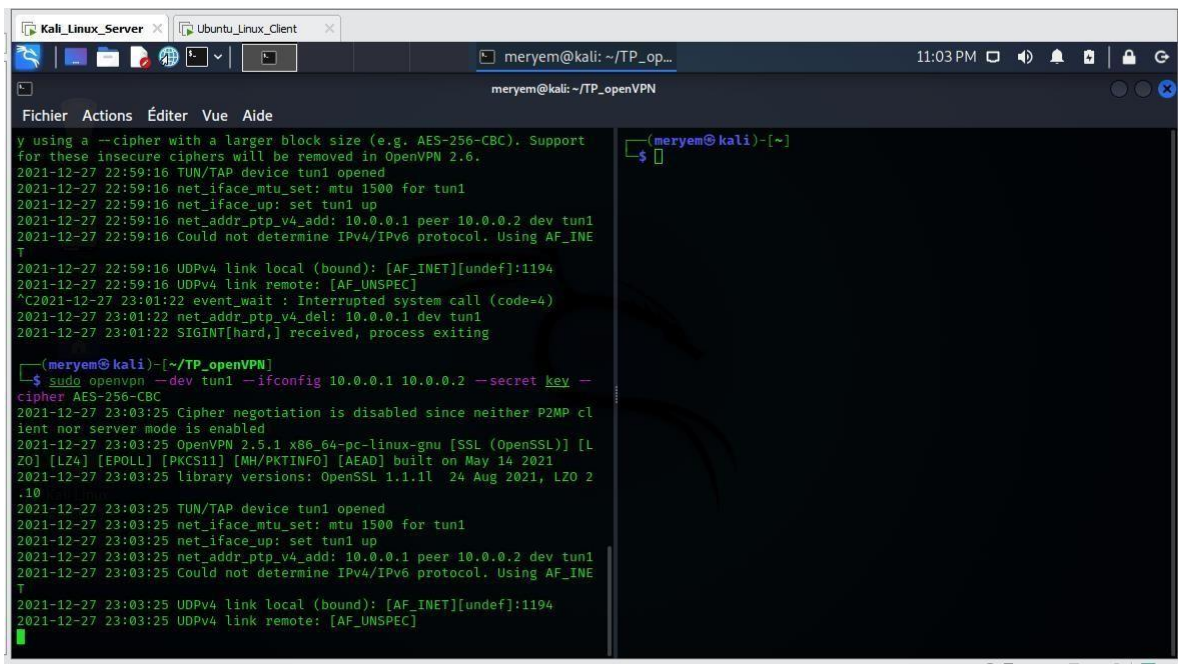

Kali_Linux_Server
Ubuntu_Linux_Client
Activities
Terminal
Dec 27 14:52
meryem@ubuntu: ~/Desktop
256 SHA256:G96hyBfC+7FD92555sCcPTtvDf/ZxArLw2JkjNy7eJg root@ubuntu (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:rQq5qj9uxF8z/f1FkgEHPn1tWz/L1L19p8fiIXrEXuM root@ubuntu (ED25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
Setting up ssh-import-id (5.10-0ubuntu1) ...
Attempting to convert /etc/ssh/ssh_import_id
Setting up ncurses-term (6.2-0ubuntu2) ...
Processing triggers for systemd (245.4-4ubuntu3.11) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for ufw (0.36-6) ...
meryem@ubuntu:~/Desktop$ service ssh status
ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
Active: active (running) since Mon 2021-12-27 14:44:24 PST; 42s ago
Docs: man:sshd(8)
man:sshd_config(5)
Main PID: 3476 (sshd)
Tasks: 1 (limit: 2260)
Memory: 1.0M
CGroup: /system.slice/ssh.service
└─3476 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
Dec 27 14:44:24 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Dec 27 14:44:24 ubuntu sshd[3476]: Server listening on 0.0.0.0 port 22.
Dec 27 14:44:24 ubuntu sshd[3476]: Server listening on :: port 22.
Dec 27 14:44:24 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
meryem@ubuntu:~/Desktop$ sudo systemctl restart ssh
meryem@ubuntu:~/Desktop$
mouse pointer inside or press Ctrl+G.

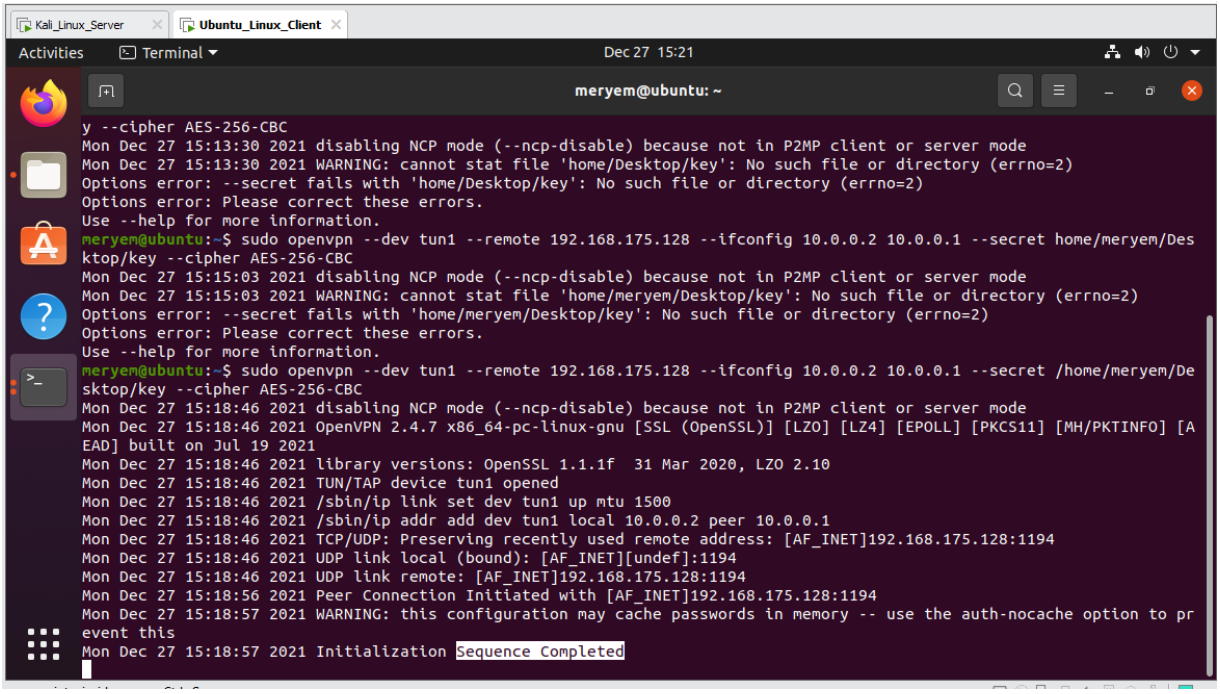


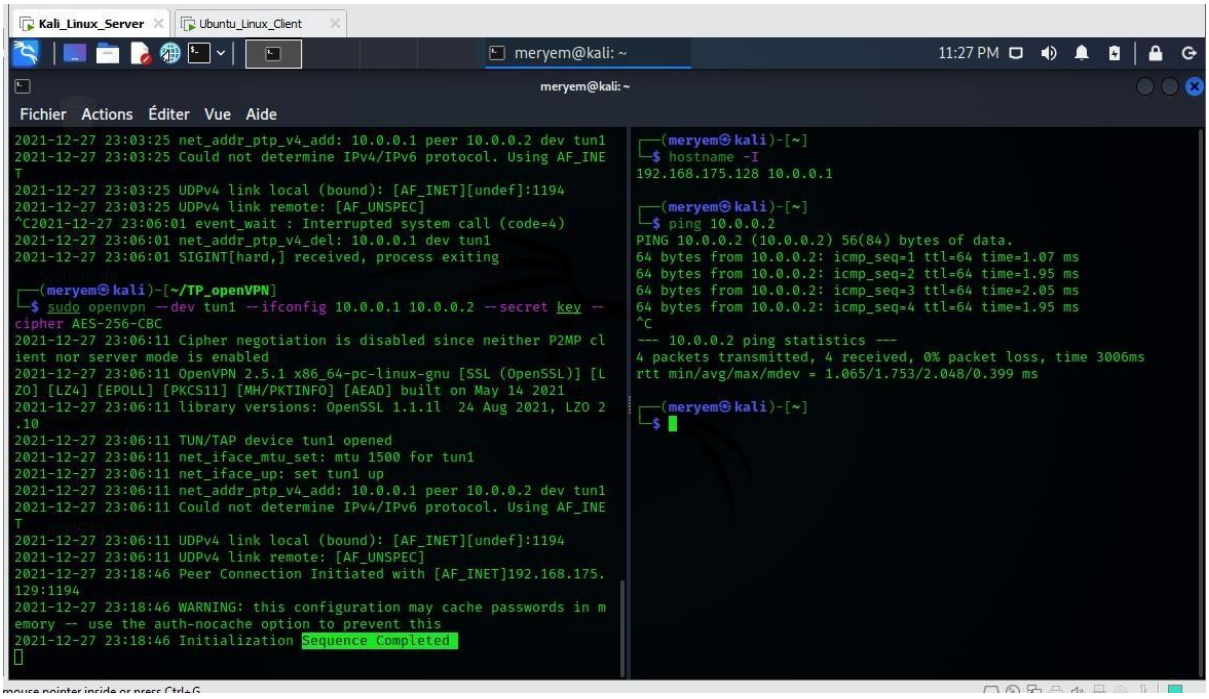


➔ la clé est partagée avec la machine client avec succès.


Kali_Linux_Server
Ubuntu_Linux_Client
meryem@kali: ~/TP_op...
11:00 PM
meryem@kali: ~/TP_openVPN
Fichier Actions Éditer Vue Aide
meryem@192.168.175.129's password:
key 100% 636 55.9KB/s 00:00
(meryem㉿kali)-[~/TP_openVPN]
$ sudo openvpn --dev tun1 --ifconfig 10.0.0.1 10.0.0.2 --secret key
2021-12-27 22:59:16 Cipher negotiation is disabled since neither P2MP client nor server mode is enabled
2021-12-27 22:59:16 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-27 22:59:16 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
2021-12-27 22:59:16 WARNING: INSECURE cipher (BF-CBC) with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC). Support for these insecure ciphers will be removed in OpenVPN 2.6.
2021-12-27 22:59:16 WARNING: INSECURE cipher (BF-CBC) with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC). Support for these insecure ciphers will be removed in OpenVPN 2.6.
2021-12-27 22:59:16 WARNING: INSECURE cipher (BF-CBC) with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC). Support for these insecure ciphers will be removed in OpenVPN 2.6.
2021-12-27 22:59:16 TUN/TAP device tun1 opened
2021-12-27 22:59:16 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 22:59:16 net_iface_up: set tun1 up
2021-12-27 22:59:16 net_addr_ptp_v4_add: 10.0.0.1 peer 10.0.0.2 dev tun1
2021-12-27 22:59:16 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-27 22:59:16 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 22:59:16 UDPv4 link remote: [AF_UNSPEC]
(meryem㉿kali)-[~]
$


Kali_Linux_Server
Ubuntu_Linux_Client
meryem@kali: ~/TP_op...
11:03 PM
meryem@kali: ~/TP_openVPN
Fichier Actions Éditer Vue Aide
y using a --cipher with a larger block size (e.g. AES-256-CBC). Support for these insecure ciphers will be removed in OpenVPN 2.6.
2021-12-27 22:59:16 TUN/TAP device tun1 opened
2021-12-27 22:59:16 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 22:59:16 net_iface_up: set tun1 up
2021-12-27 22:59:16 net_addr_ptp_v4_add: 10.0.0.1 peer 10.0.0.2 dev tun1
2021-12-27 22:59:16 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-27 22:59:16 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 22:59:16 UDPv4 link remote: [AF_UNSPEC]
^C2021-12-27 23:01:22 event_wait : Interrupted system call (code=4)
2021-12-27 23:01:22 net_addr_ptp_v4_del: 10.0.0.1 dev tun1
2021-12-27 23:01:22 SIGINT[hard,] received, process exiting
(meryem㉿kali)-[~/TP_openVPN]
$ sudo openvpn --dev tun1 --ifconfig 10.0.0.1 10.0.0.2 --secret key --cipher AES-256-CBC
2021-12-27 23:03:25 Cipher negotiation is disabled since neither P2MP client nor server mode is enabled
2021-12-27 23:03:25 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-27 23:03:25 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
2021-12-27 23:03:25 TUN/TAP device tun1 opened
2021-12-27 23:03:25 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 23:03:25 net_iface_up: set tun1 up
2021-12-27 23:03:25 net_addr_ptp_v4_add: 10.0.0.1 peer 10.0.0.2 dev tun1
2021-12-27 23:03:25 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-27 23:03:25 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 23:03:25 UDPv4 link remote: [AF_UNSPEC]
(meryem㉿kali)-[~]
$

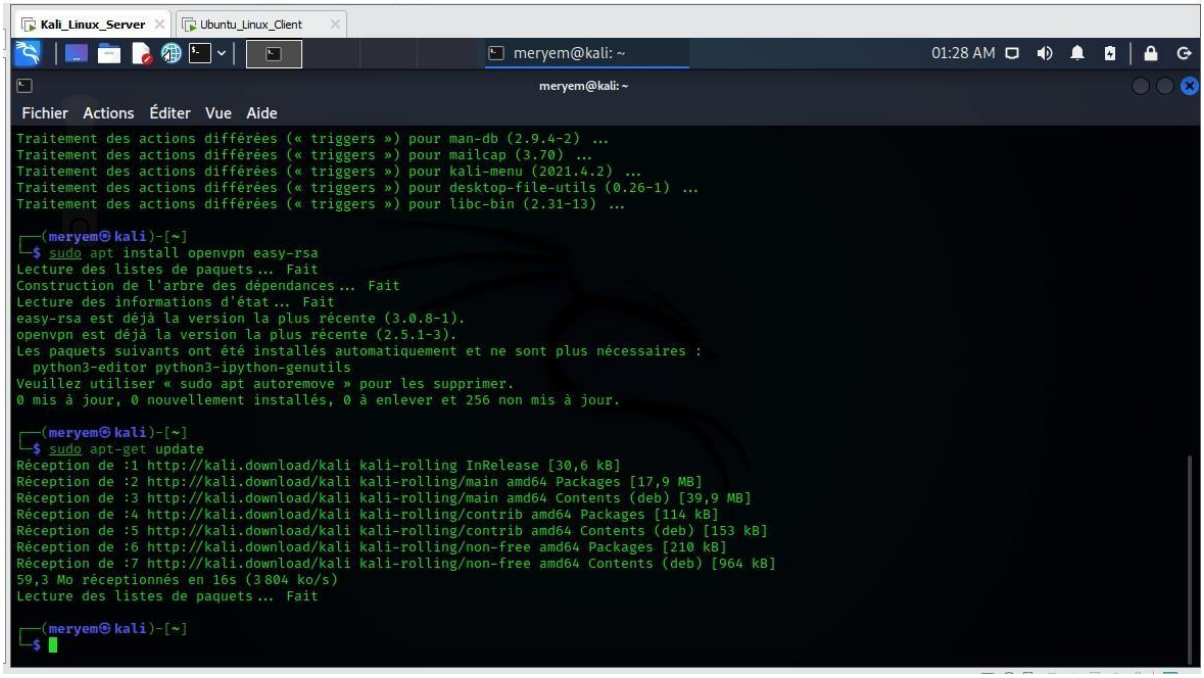




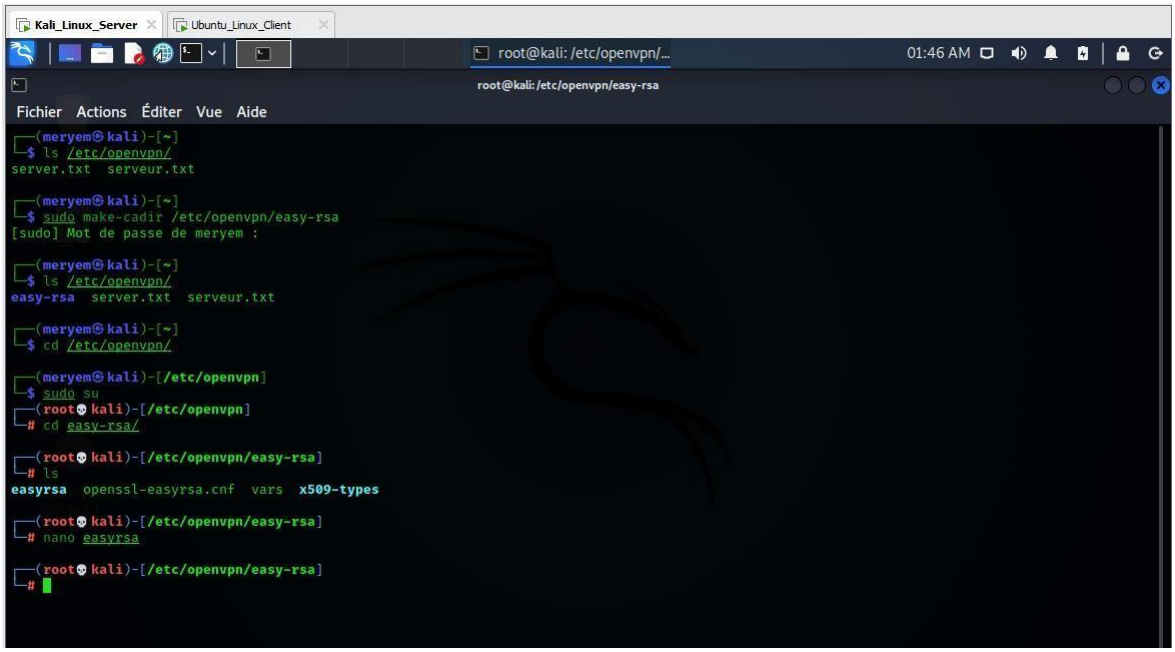
MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d'électricité et de mécanique

Partie 3

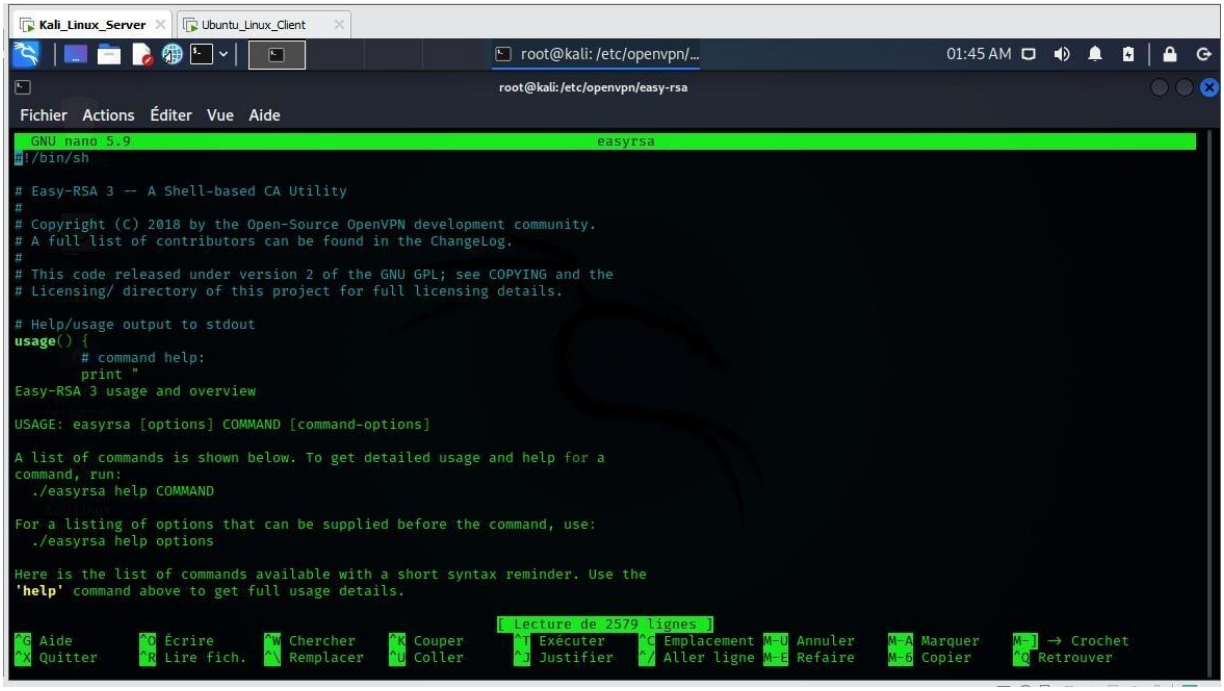
Le but est de chiffrer la communication.

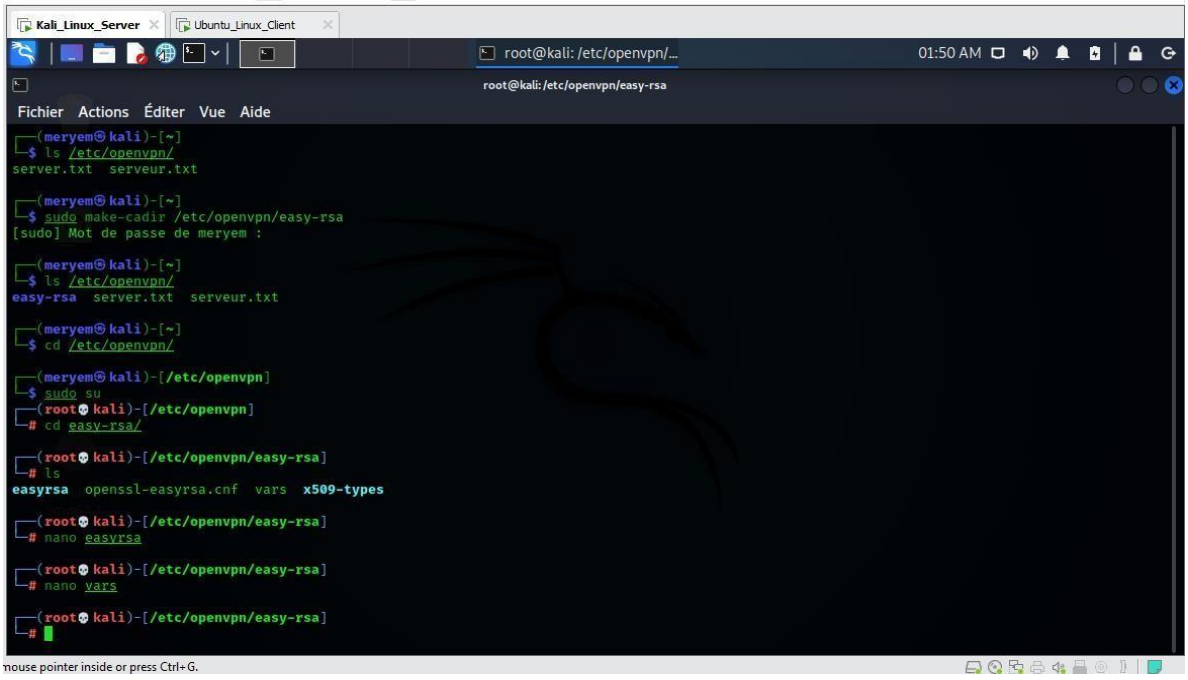


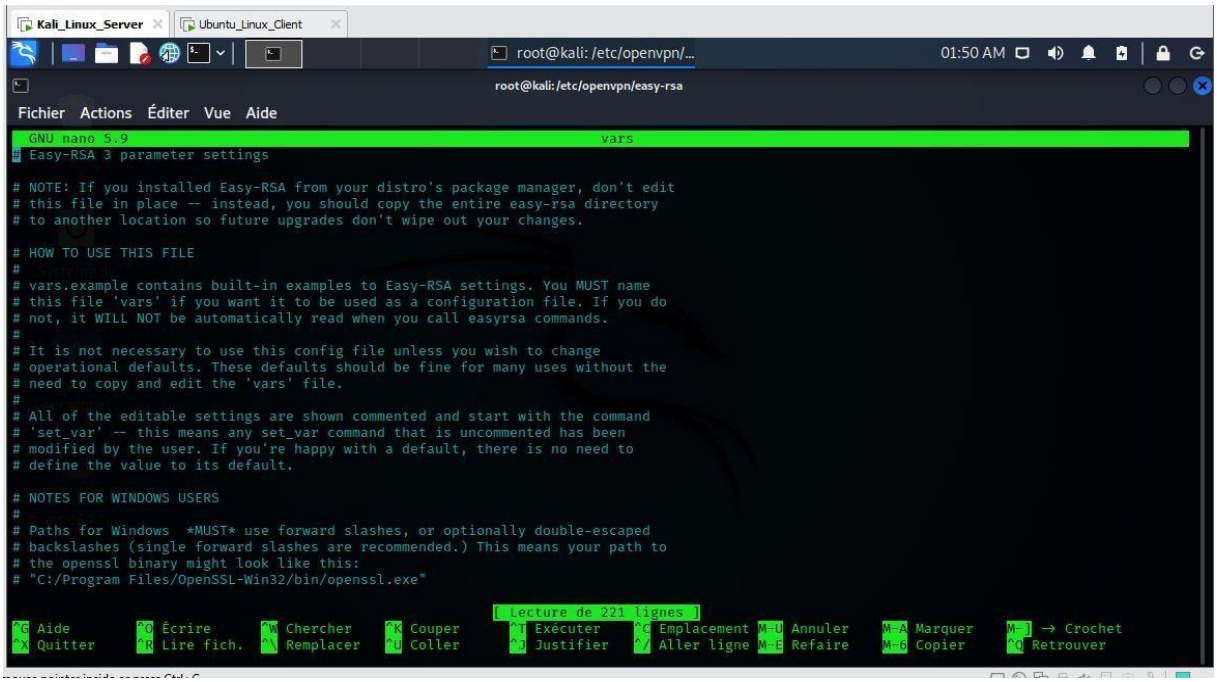
➔ On installe **OpenVPN easy-rsa,** ensuite on le met à jour avec la commande apt-get update et on relance l'installation.

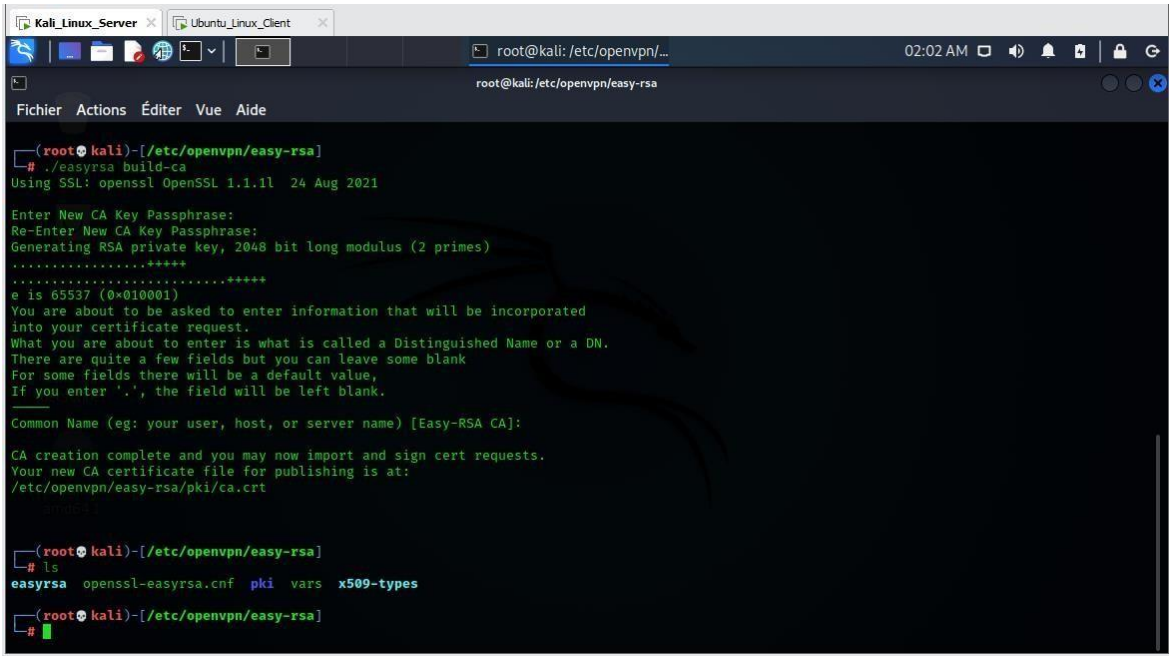


➔ On copie easy-rsa dans le répertoire openvpn.

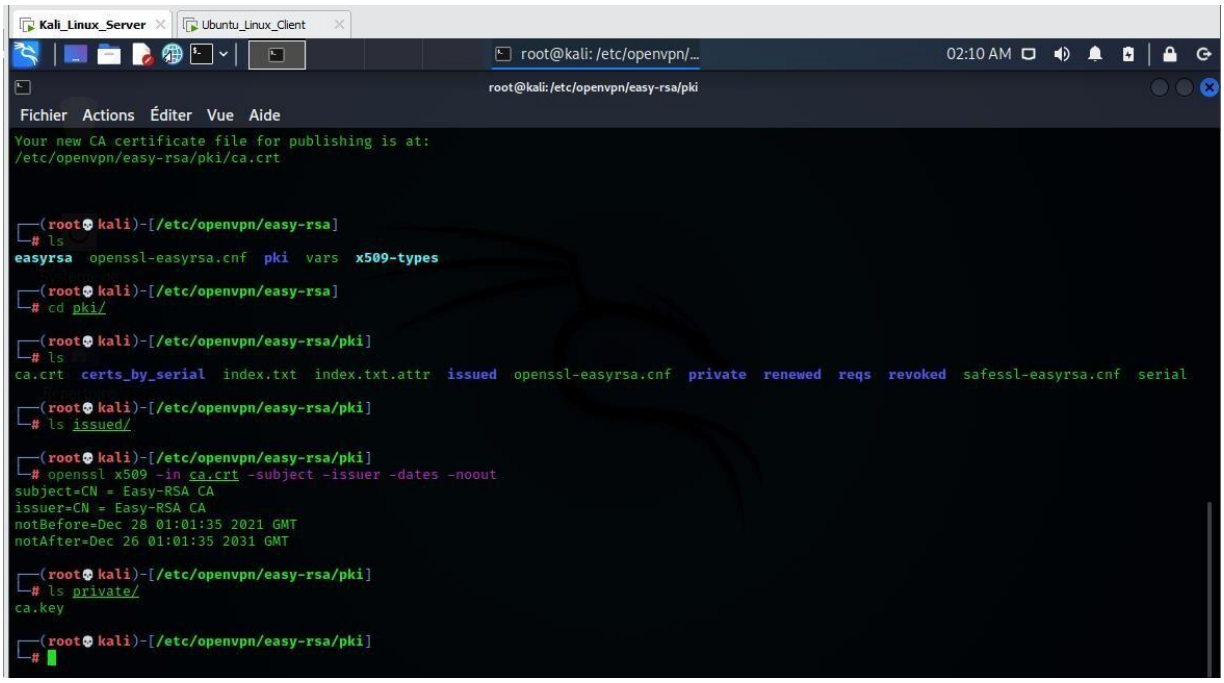


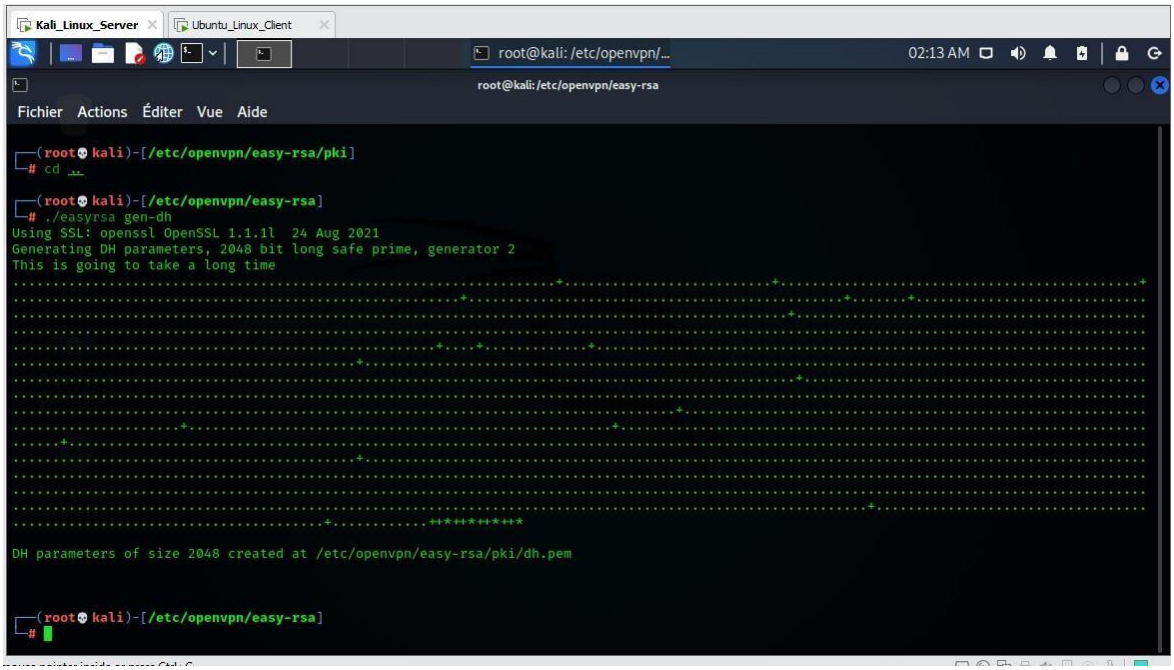




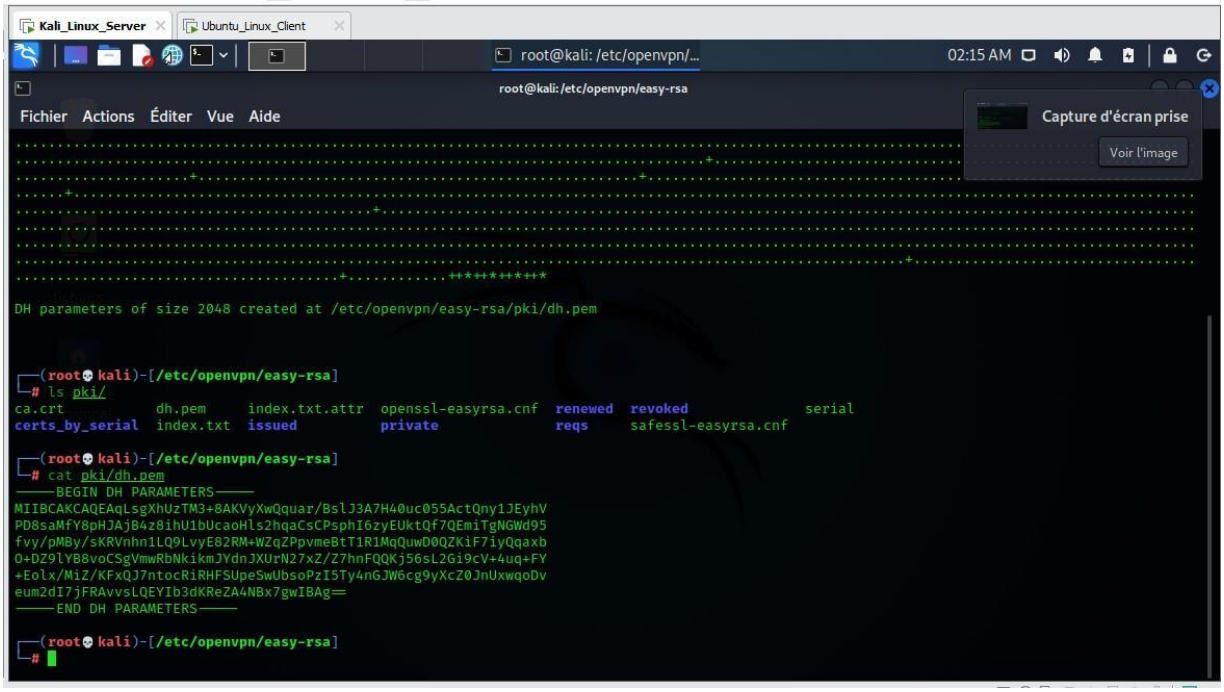


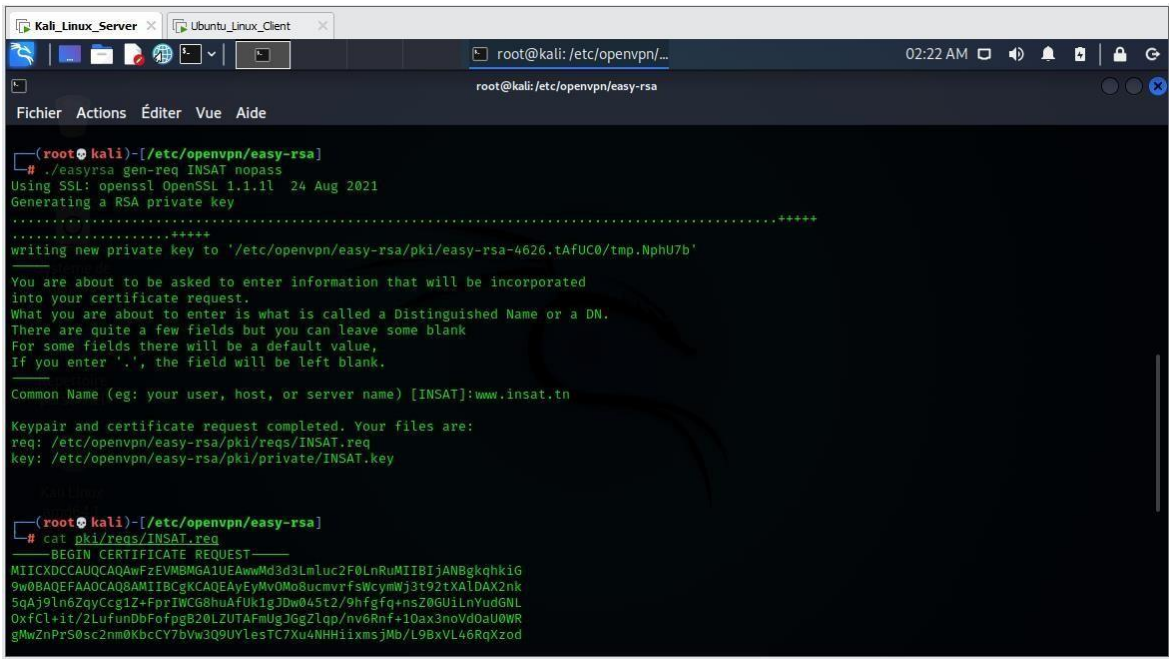
MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d'électricité et de mécanique



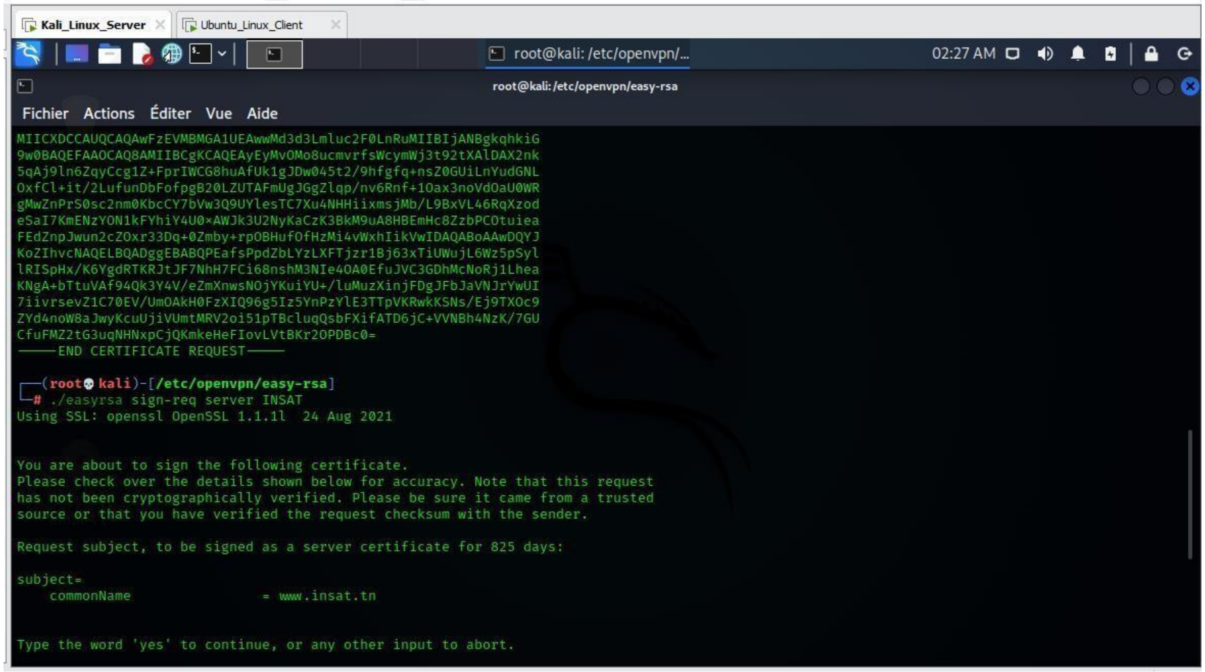


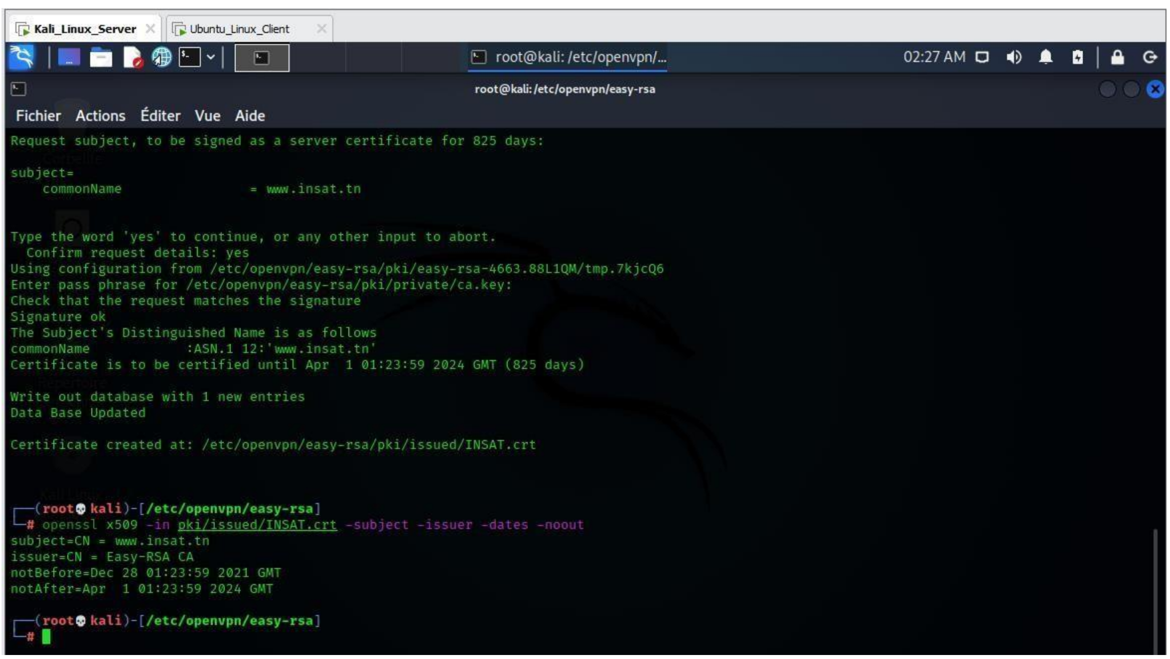
MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d'électricité et de mécanique

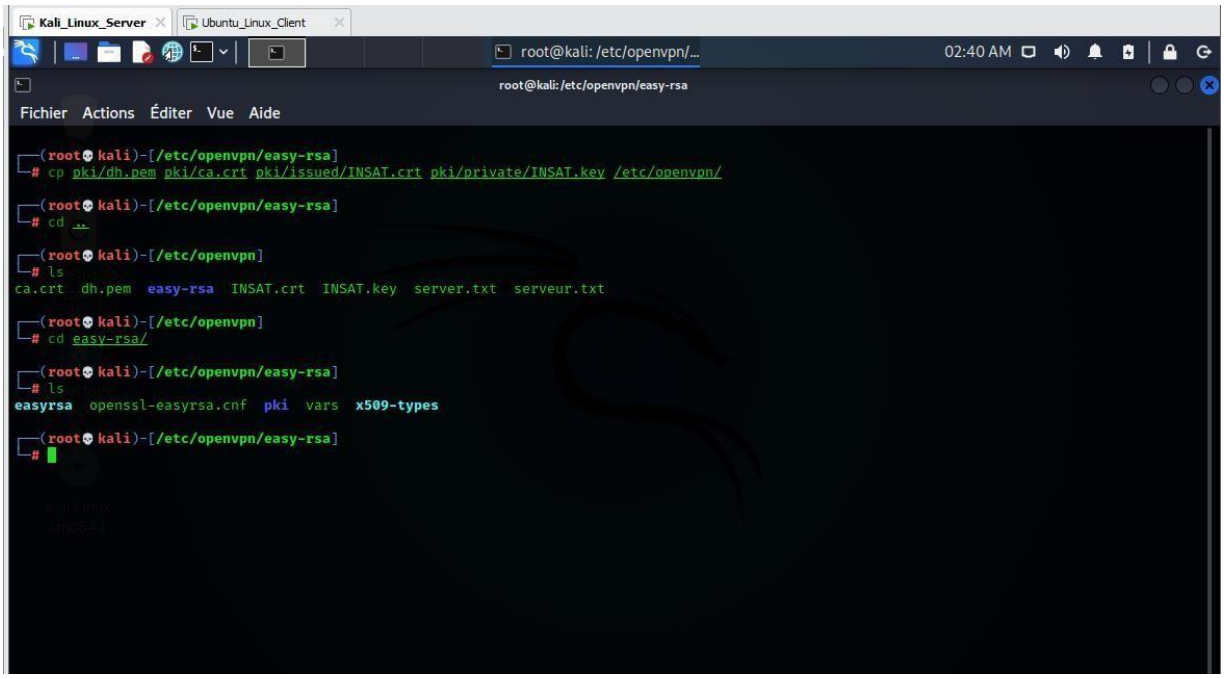




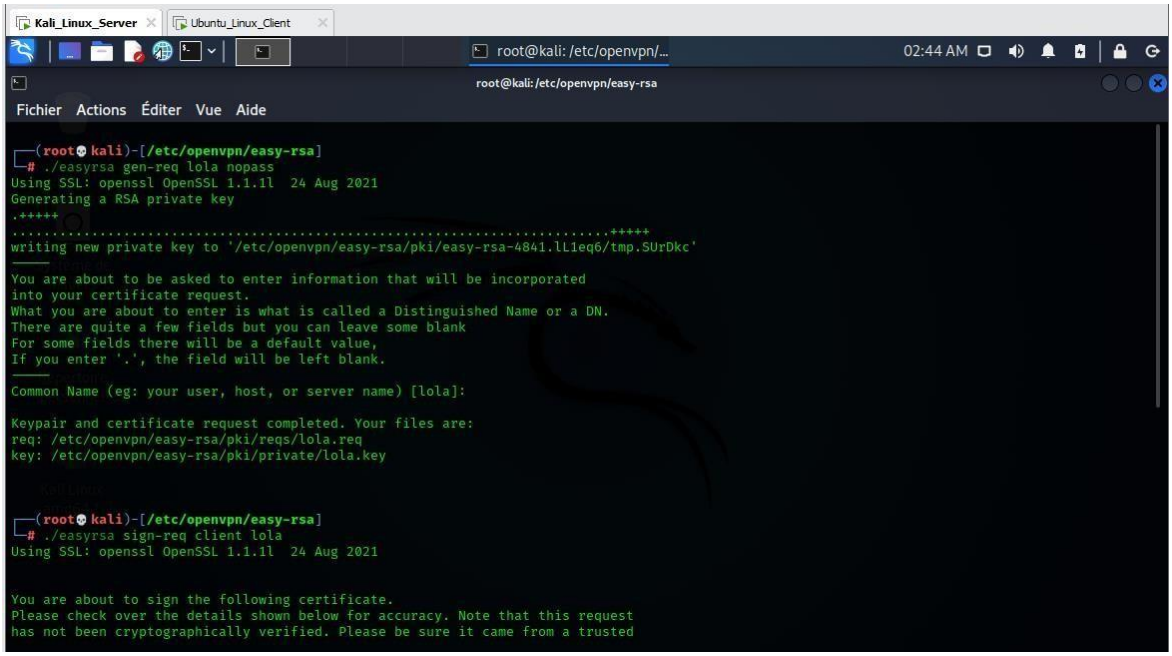
MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d'électricité et de mécanique

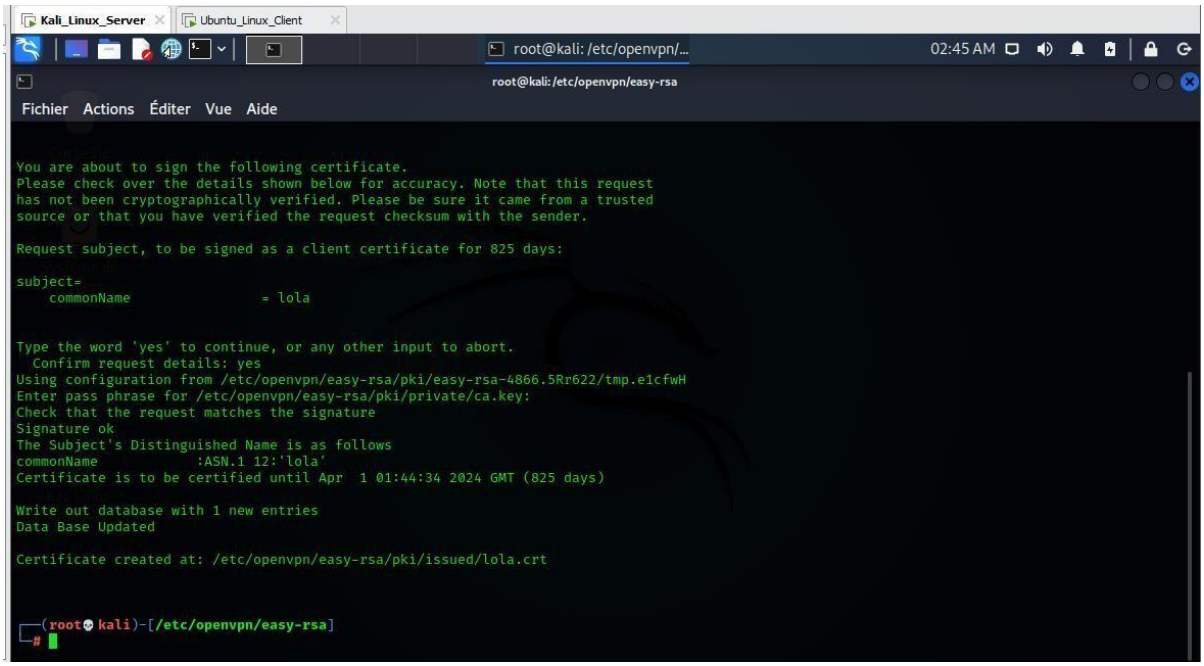

Kali_Linux_Server
Ubuntu_Linux_Client
root@kali: /etc/openvpn/...
02:27 AM
root@kali: /etc/openvpn/easy-rsa
Fichier Actions Éditer Vue Aide
MIICXDCCAUQCAQAwFzEVMBMGA1UEAwwMd3d3Lmluc2F0LnRuMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyEyMvOMo8ucmvrfsWcymWj3t92tXAlDAX2nk
5qAj9ln6ZqyCcg1Z+FprIWCG8huAfUk1gJDw045t2/9hfgfq+nsZ0GUiLnYudGNL
OxfCl+it/2LufunDbFofpgB20LZUTAFmUgJGgZlqp/nv6Rnf+1Oax3noVdOaU0WR
gMwZnPrS0sc2nm0KbcCY7bVw3Q9UYlesTC7Xu4NHHiixmsjMb/L9BxVL46RqXzod
eSaI7KmENzYON1kFYhiY4U0×AWJk3U2NyKaCzK3BkM9uA8HBEmHc8ZzbPCOtuiea
FEdZnpJwun2cZOxr33Dq+0Zmby+rpOBHufOfHzMi4vWxhIikVwIDAQABoAAwDQYJ
KoZIhvcNAQELBQADggEBABQPEafsPpdZbLYzLXFTjzr1Bj63xTiUWujL6Wz5pSyl
lRISpHx/K6YgdRTKRJtJF7NhH7FCi68nshM3NIe4OA0EfuJVC3GDhMcNoRj1Lhea
KNgA+bTtuVAf94Qk3Y4V/eZmXnwsNOjYKuiYU+/luMuzXinjFDgJFbJaVNJrYwUI
7iivrsevZ1C70EV/UmOAkH0FzXIQ96g5Iz5YnPzYlE3TTpVKRwkKSNs/Ej9TXOc9
ZYd4noW8aJwyKcuUjiVUmtMRV2oi51pTBcluqQsbFXifATD6jC+VVNBh4NzK/7GU
CfuFMZ2tG3uqNHNxpCjQKmkeHeFIovLVtBKr2OPDBc0=
-----END CERTIFICATE REQUEST-----
┌──(root💀kali)-[/etc/openvpn/easy-rsa]
└─# ./easyrsa sign-req server INSAT
Using SSL: openssl OpenSSL 1.1.1l 24 Aug 2021
You are about to sign the following certificate.
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.
Request subject, to be signed as a server certificate for 825 days:
subject=
commonName = www.insat.tn
Type the word 'yes' to continue, or any other input to abort.

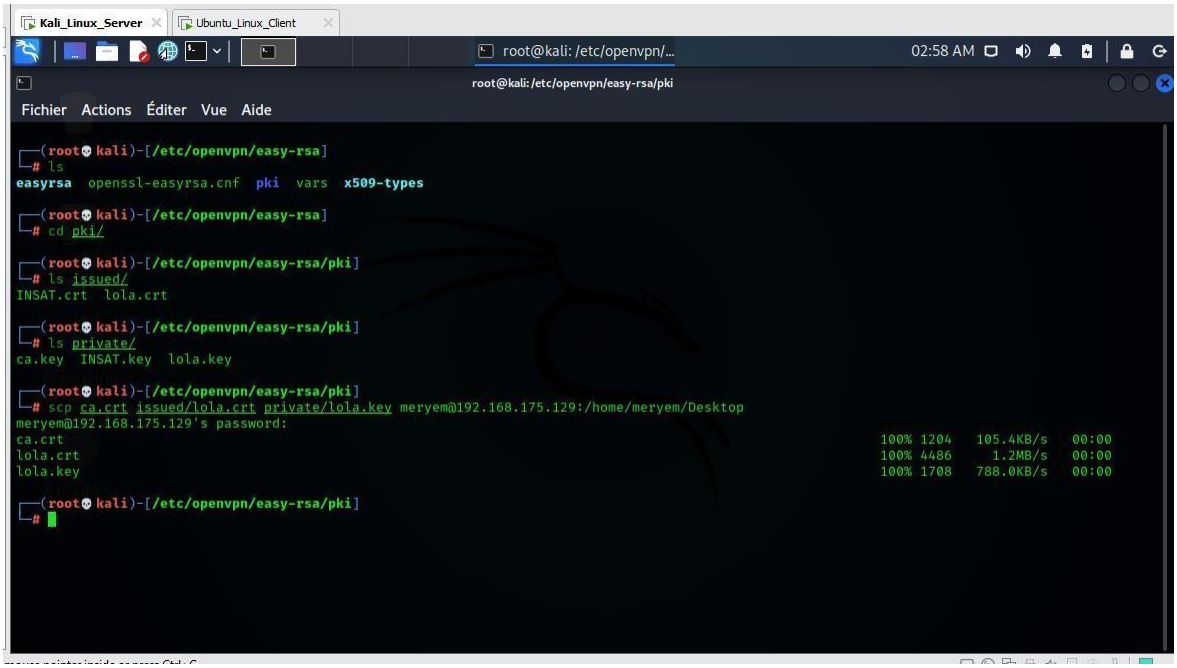

Kali_Linux_Server
Ubuntu_Linux_Client
root@kali: /etc/openvpn/...
02:27 AM
root@kali: /etc/openvpn/easy-rsa
Fichier Actions Éditer Vue Aide
Request subject, to be signed as a server certificate for 825 days:
subject=
commonName = www.insat.tn
Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-4663.88L1QM/tmp.7kjcQ6
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName :ASN.1 12:'www.insat.tn'
Certificate is to be certified until Apr 1 01:23:59 2024 GMT (825 days)
Write out database with 1 new entries
Data Base Updated
Certificate created at: /etc/openvpn/easy-rsa/pki/issued/INSAT.crt
┌──(root💀kali)-[/etc/openvpn/easy-rsa]
└─# openssl x509 -in pki/issued/INSAT.crt -subject -issuer -dates -noout
subject=CN = www.insat.tn
issuer=CN = Easy-RSA CA
notBefore=Dec 28 01:23:59 2021 GMT
notAfter=Apr 1 01:23:59 2024 GMT
┌──(root💀kali)-[/etc/openvpn/easy-rsa]
└─#



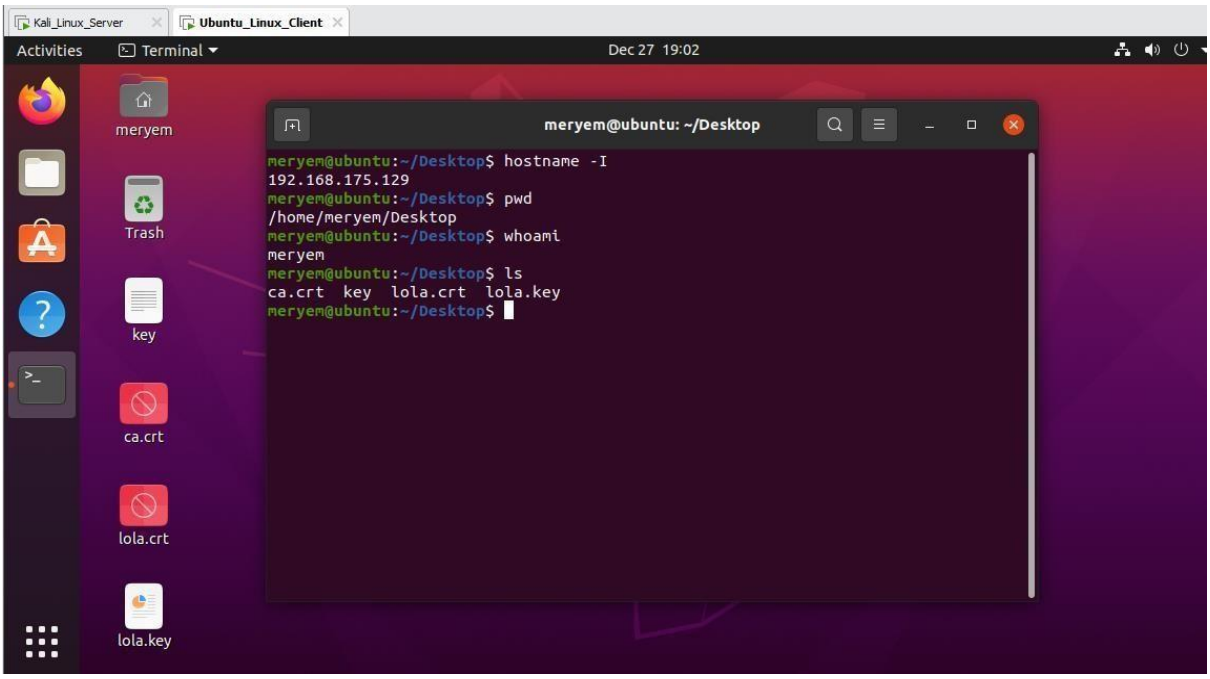
Maintenat on va passer au client

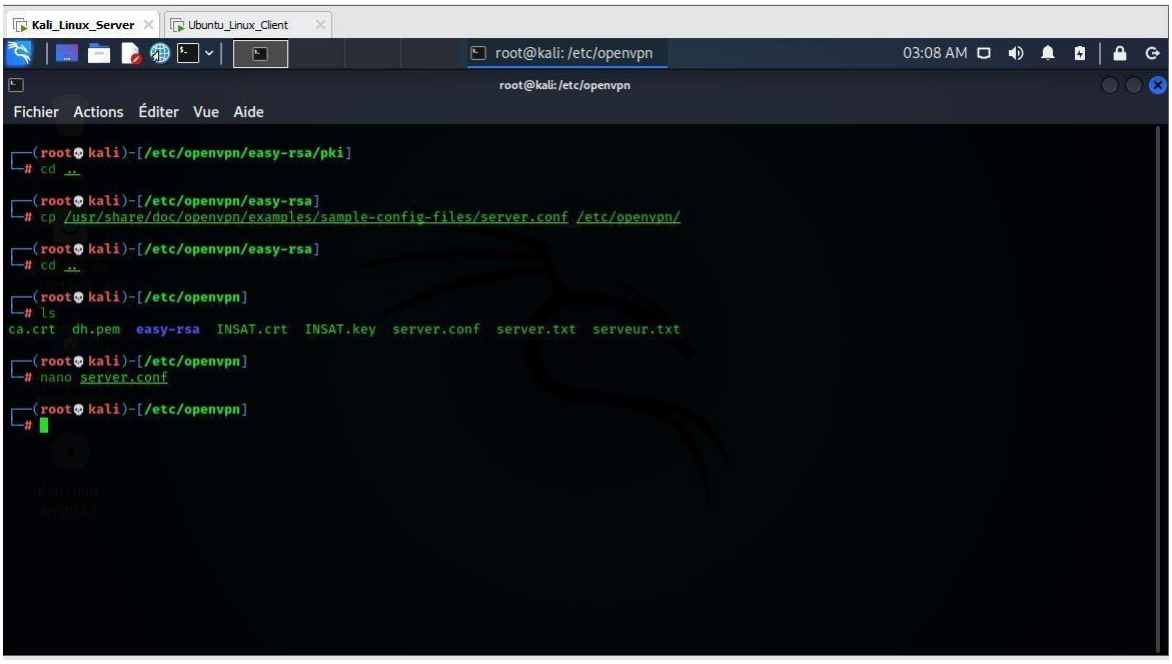




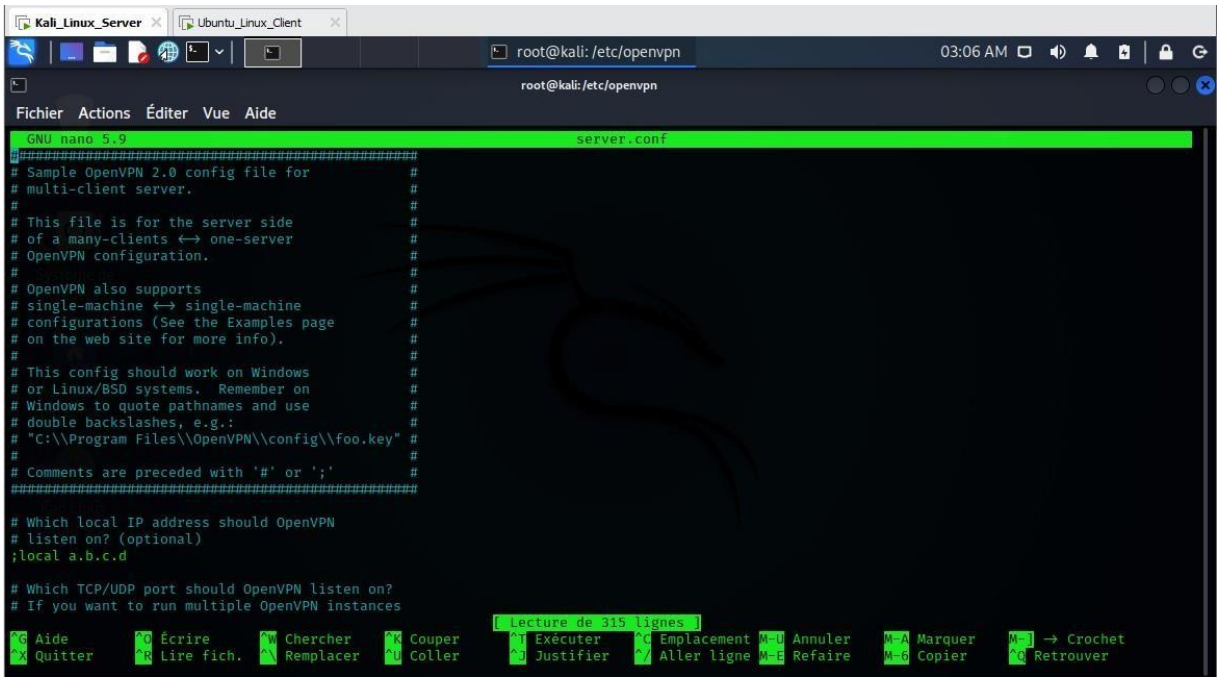


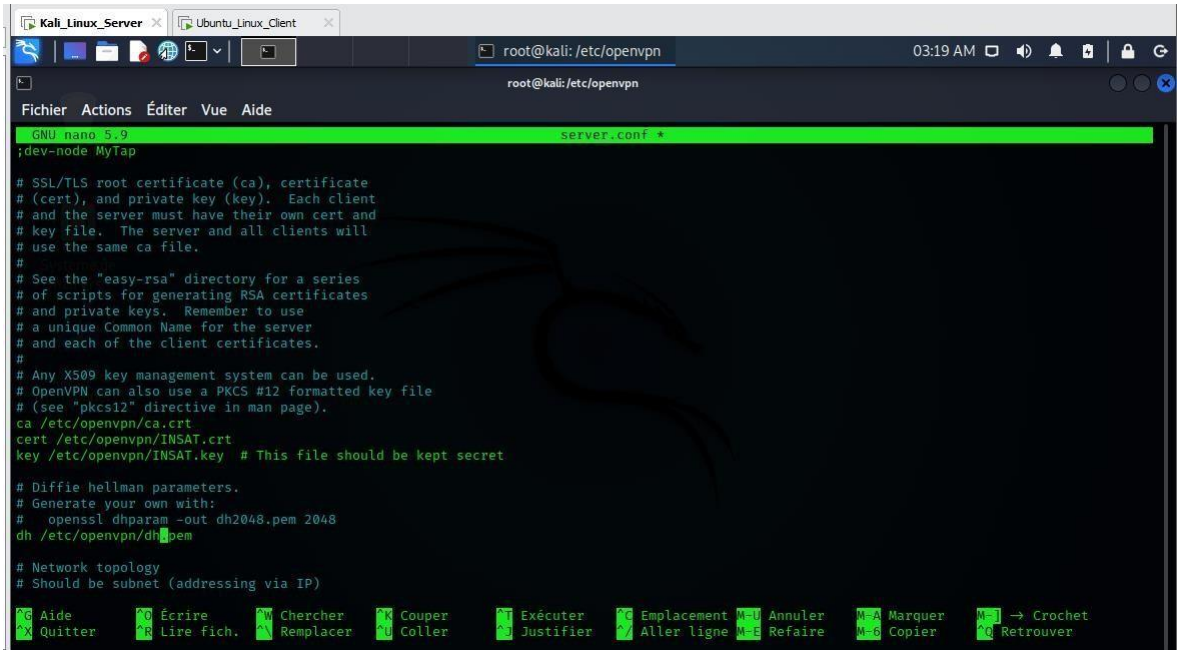
MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d'électricité et de mécanique

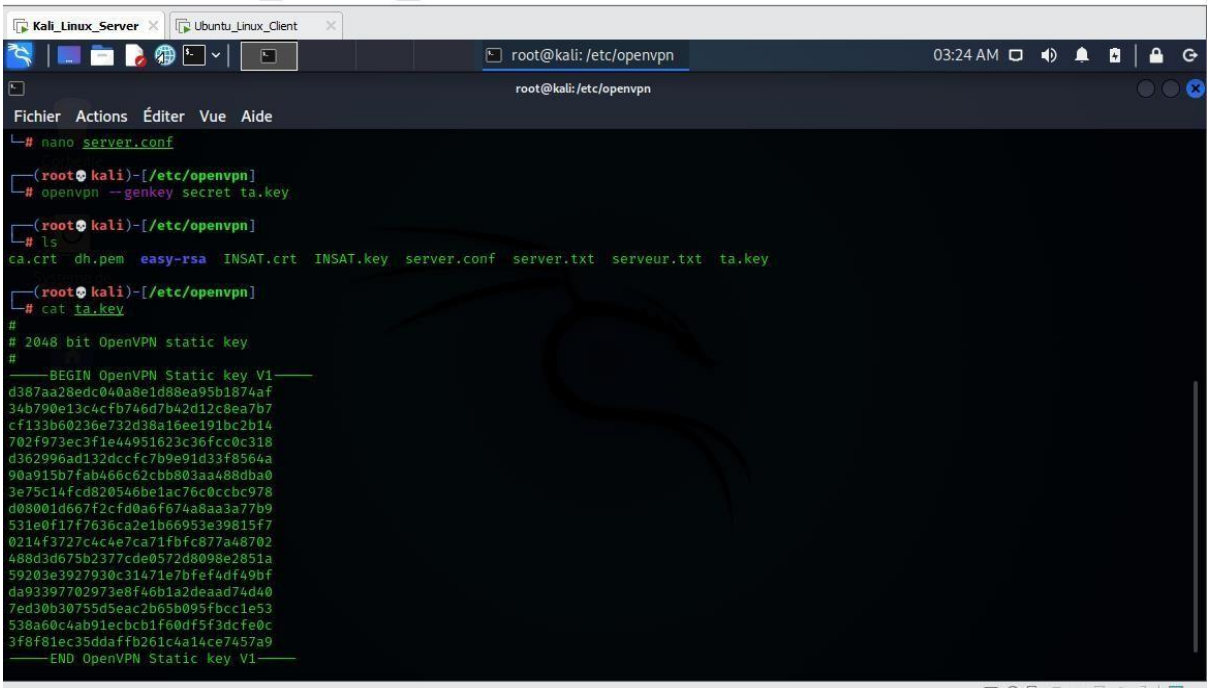


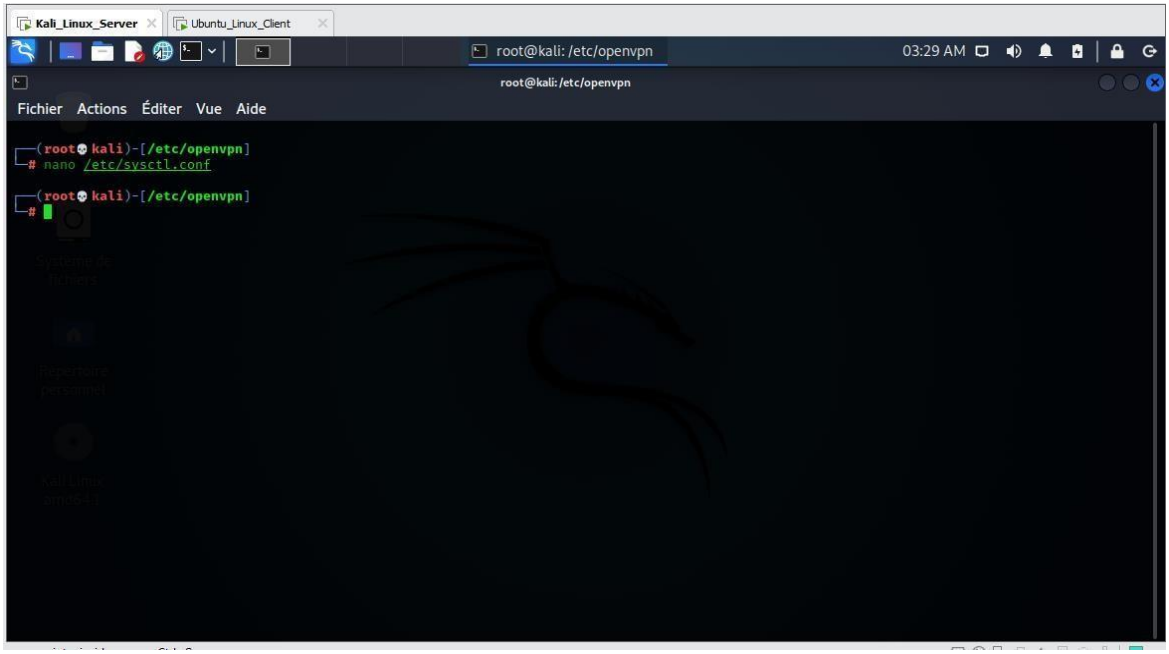


MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d'électricité et de mécanique

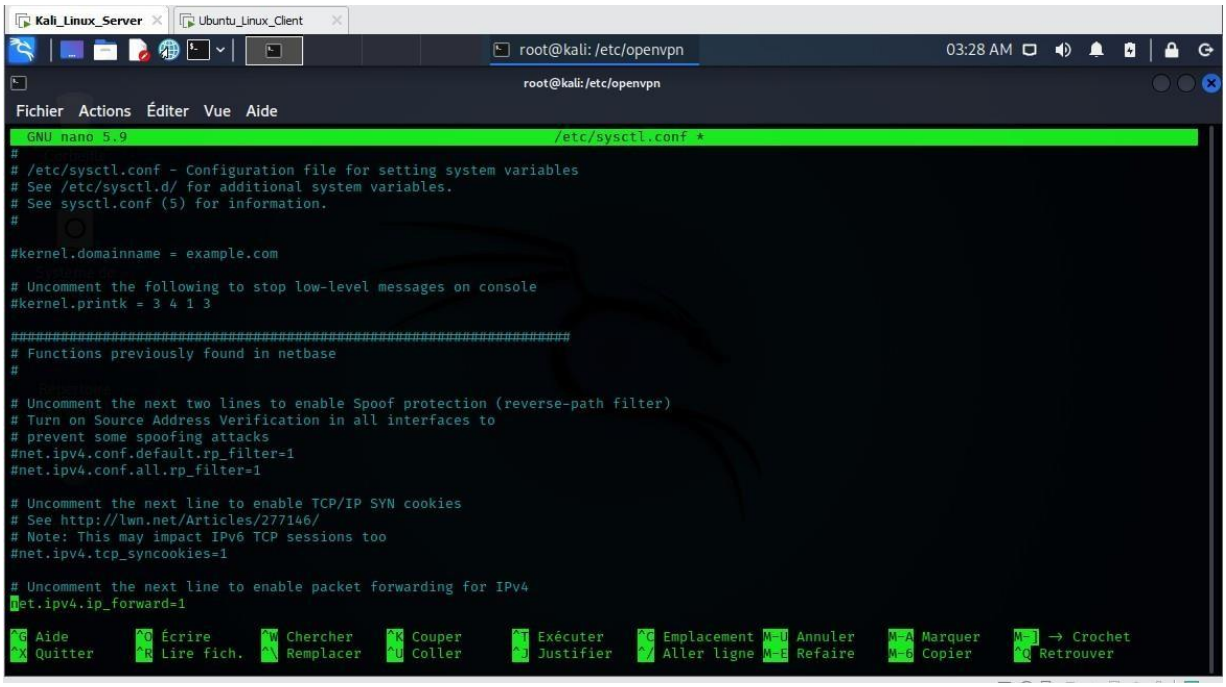

Kali_Linux_Server
Ubuntu_Linux_Client
root@kali: /etc/openvpn
03:06 AM
root@kali: /etc/openvpn
Fichier Actions Éditer Vue Aide
GNU nano 5.9 server.conf
Sample OpenVPN 2.0 config file for
multi-client server.
This file is for the server side
of a many-clients <-> one-server #
OpenVPN configuration.
OpenVPN 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 ';'
Which local IP address should 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
[Lecture de 315 lignes]
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement M-U Annuler M-A Marquer M-] → Crochet
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne M-E Refaire M-6 Copier ^Q Retrouver

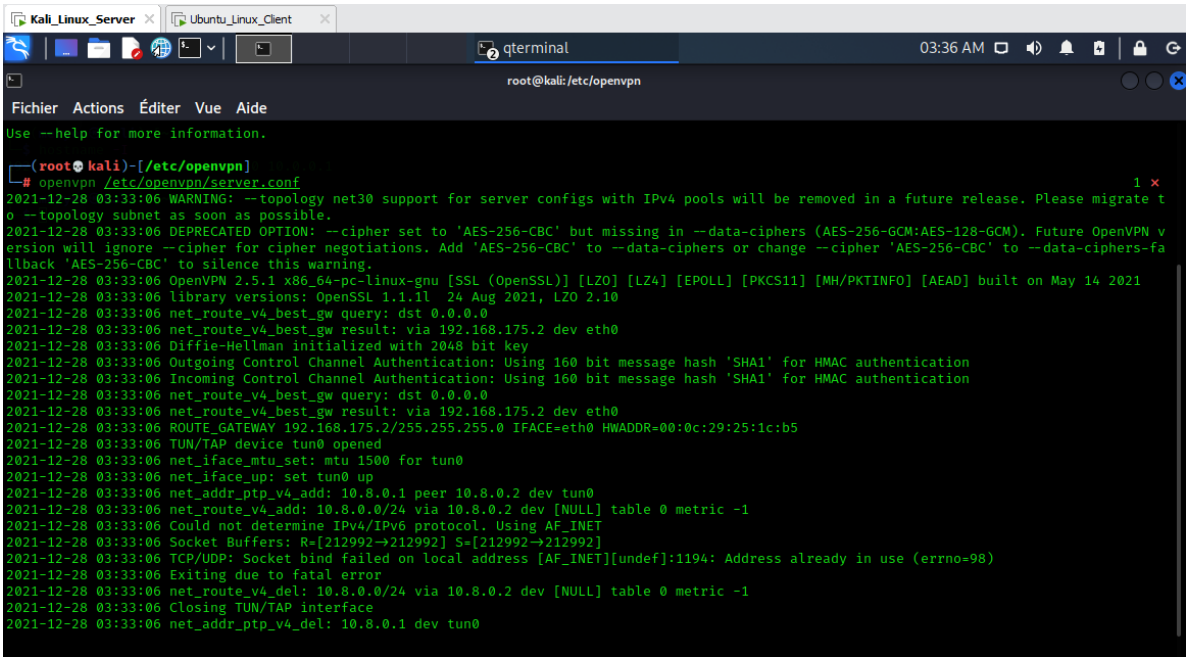

Kali_Linux_Server
Ubuntu_Linux_Client
root@kali: /etc/openvpn
03:19 AM
root@kali: /etc/openvpn
Fichier Actions Éditer Vue Aide
GNU nano 5.9 server.conf *
;dev-node MyTap
SSL/TLS root certificate (ca), certificate
(cert), and private key (key). Each client
and the server must have their own cert and
key file. The server and all clients will
use the same ca file.
See the "easy-rsa" directory for a series
of scripts for generating RSA certificates
and private keys. Remember to use
a unique Common Name for the server
and each of the client certificates.
Any X509 key management system can be used.
OpenVPN can also use a PKCS #12 formatted key file
(see "pkcs12" directive in man page).
ca /etc/openvpn/ca.crt
cert /etc/openvpn/INSAT.crt
key /etc/openvpn/INSAT.key # This file should be kept secret
Diffie hellman parameters.
Generate your own with:
openssl dhparam -out dh2048.pem 2048
dh /etc/openvpn/dh.pem
Network topology
Should be subnet (addressing via IP)
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement M-U Annuler M-A Marquer M-] → Crochet
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne M-E Refaire M-6 Copier ^Q Retrouver

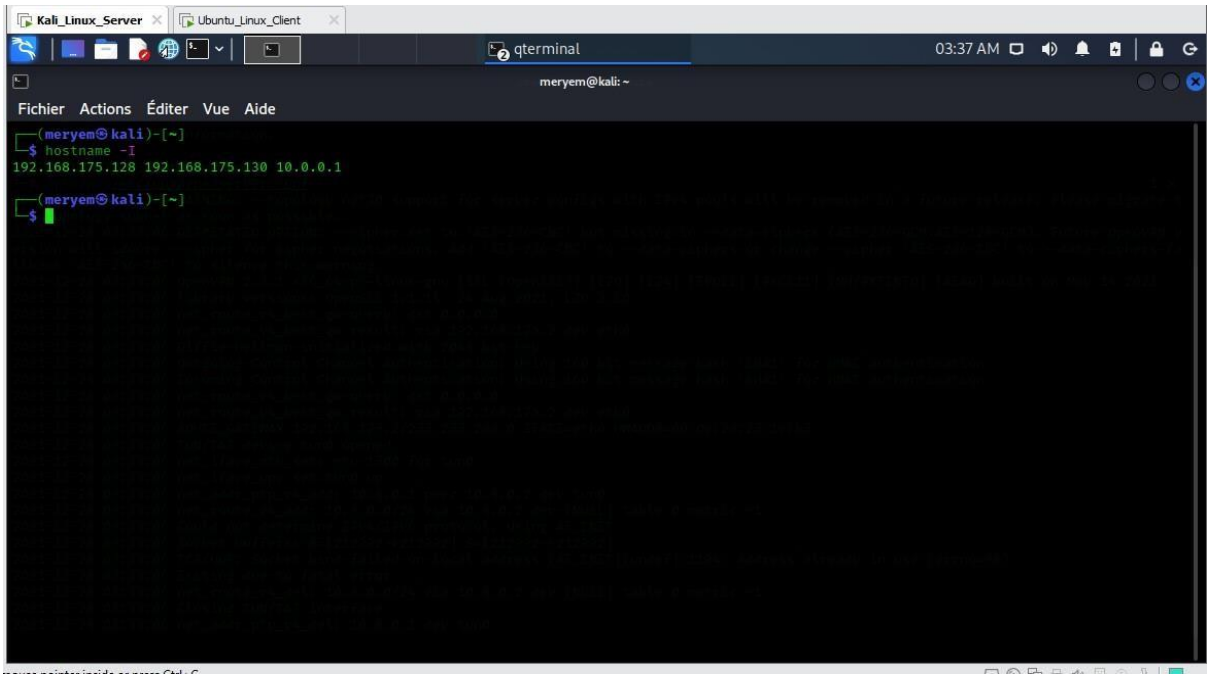


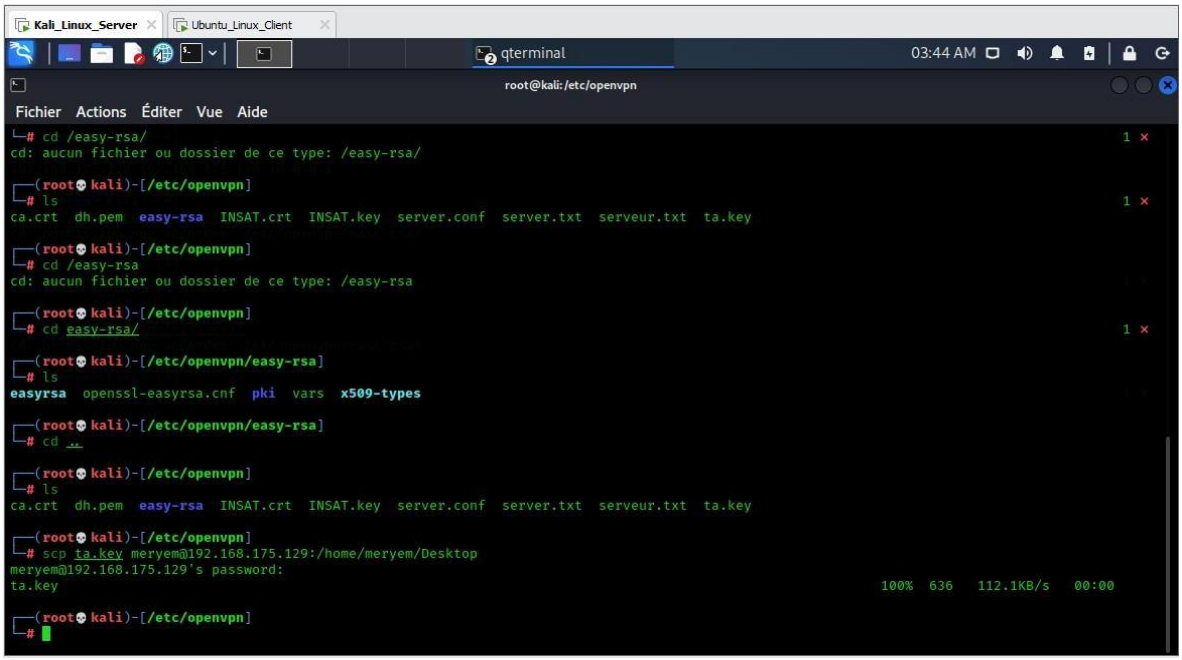


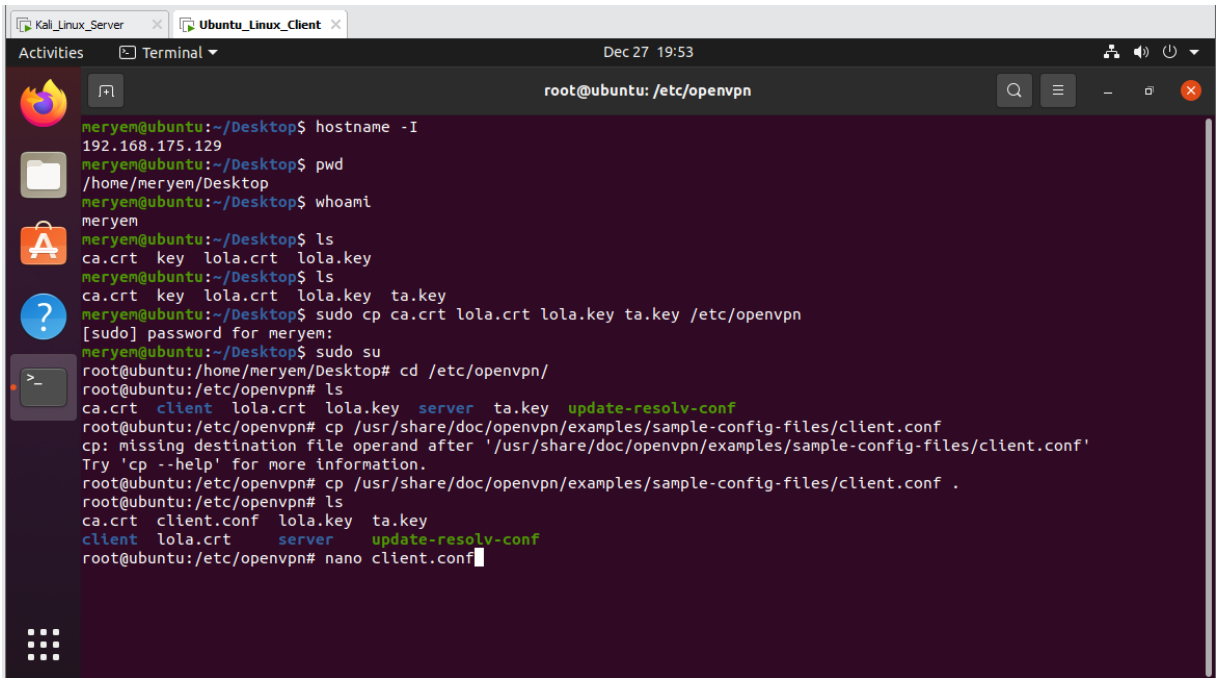
MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d'électricité et de mécanique

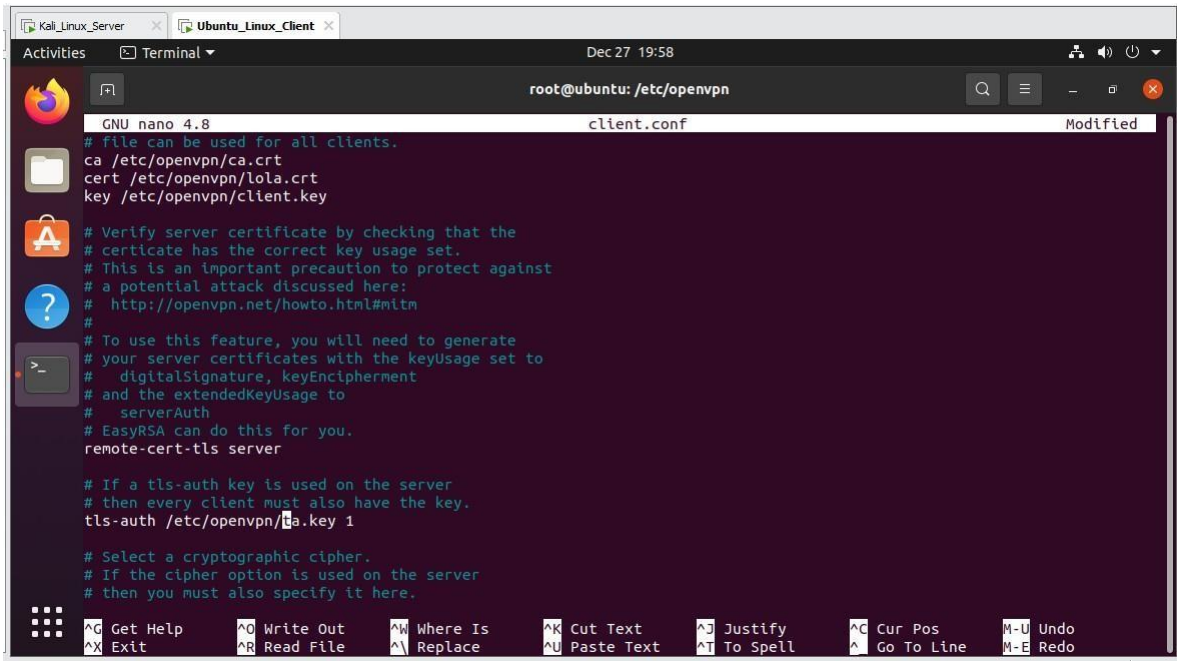

Kali_Linux_Server
Ubuntu_Linux_Client
root@kali: /etc/openvpn
03:28 AM
root@kali: /etc/openvpn
Fichier Actions Éditer Vue Aide
GNU nano 5.9 /etc/sysctl.conf *
/etc/sysctl.conf - Configuration file for setting system variables
See /etc/sysctl.d/ for additional system variables.
See sysctl.conf (5) for information.
#kernel.domainname = example.com
Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
Functions previously found in netbase
Uncomment the next two lines to enable Spoof protection (reverse-path filter)
Turn on Source Address Verification in all interfaces to
prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
Uncomment the next line to enable TCP/IP SYN cookies
See http://lwn.net/Articles/277146/
Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement M-U Annuler M-A Marquer M-] → Crochet
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne M-E Refaire M-6 Copier ^Q Retrouver


Kali_Linux_Server
Ubuntu_Linux_Client
qterminal
03:36 AM
root@kali: /etc/openvpn
Fichier Actions Éditer Vue Aide
Use --help for more information.
(root kali)-[/etc/openvpn]
openvpn /etc/openvpn/server.conf
2021-12-28 03:33:06 WARNING: --topology net30 support for server configs with IPv4 pools will be removed in a future release. Please migrate to --topology subnet as soon as possible.
2021-12-28 03:33:06 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-256-CBC' to --data-ciphers or change --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to silence this warning.
2021-12-28 03:33:06 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-28 03:33:06 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
2021-12-28 03:33:06 net_route_v4_best_gw query: dst 0.0.0.0
2021-12-28 03:33:06 net_route_v4_best_gw result: via 192.168.175.2 dev eth0
2021-12-28 03:33:06 Diffie-Hellman initialized with 2048 bit key
2021-12-28 03:33:06 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2021-12-28 03:33:06 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2021-12-28 03:33:06 net_route_v4_best_gw query: dst 0.0.0.0
2021-12-28 03:33:06 net_route_v4_best_gw result: via 192.168.175.2 dev eth0
2021-12-28 03:33:06 ROUTE_GATEWAY 192.168.175.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:25:1c:b5
2021-12-28 03:33:06 TUN/TAP device tun0 opened
2021-12-28 03:33:06 net_iface_mtu_set: mtu 1500 for tun0
2021-12-28 03:33:06 net_iface_up: set tun0 up
2021-12-28 03:33:06 net_addr_ptp_v4_add: 10.8.0.1 peer 10.8.0.2 dev tun0
2021-12-28 03:33:06 net_route_v4_add: 10.8.0.0/24 via 10.8.0.2 dev [NULL] table 0 metric -1
2021-12-28 03:33:06 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-28 03:33:06 Socket Buffers: R=[212992→212992] S=[212992→212992]
2021-12-28 03:33:06 TCP/UDP: Socket bind failed on local address [AF_INET][undef]:1194: Address already in use (errno=98)
2021-12-28 03:33:06 Exiting due to fatal error
2021-12-28 03:33:06 net_route_v4_del: 10.8.0.0/24 via 10.8.0.2 dev [NULL] table 0 metric -1
2021-12-28 03:33:06 Closing TUN/TAP interface
2021-12-28 03:33:06 net_addr_ptp_v4_del: 10.8.0.1 dev tun0

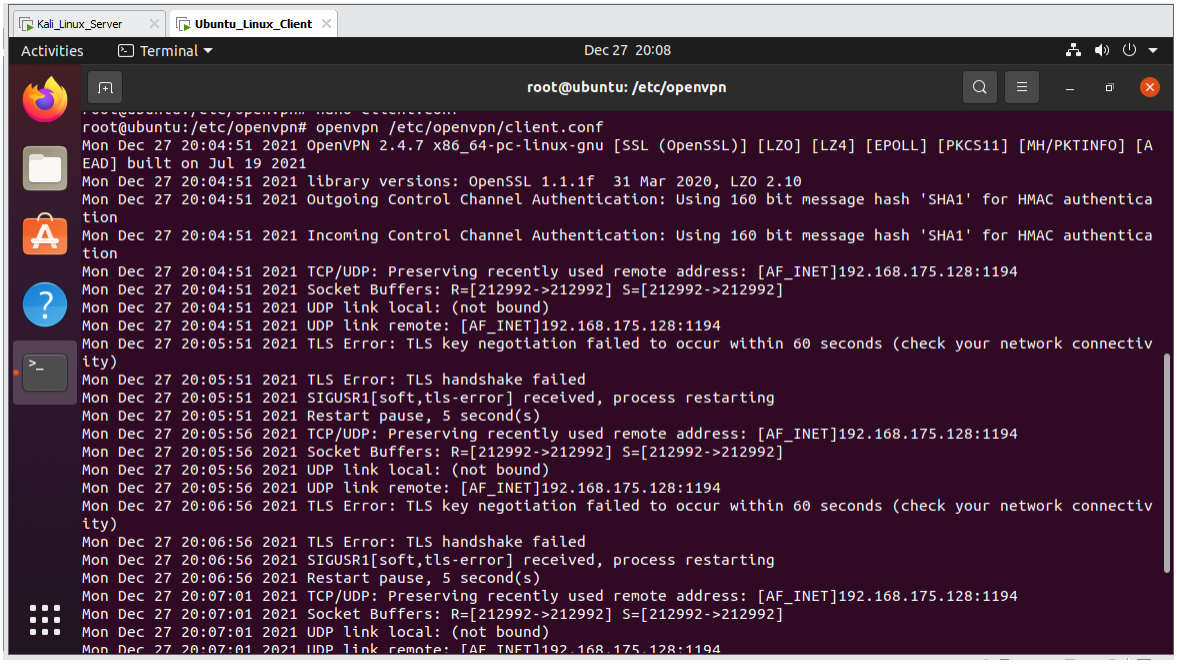

Kali_Linux_Server
Ubuntu_Linux_Client
qterminal
03:37 AM
meryem@kali: ~
Fichier Actions Éditer Vue Aide
┌──(meryem㉿kali)-[~]
└─$ hostname -I
192.168.175.128 192.168.175.130 10.0.0.1
┌──(meryem㉿kali)-[~]
└─$


Kali_Linux_Server
Ubuntu_Linux_Client
qterminal
03:44 AM
root@kali: /etc/openvpn
Fichier Actions Éditer Vue Aide
└─# cd /easy-rsa/
cd: aucun fichier ou dossier de ce type: /easy-rsa/
┌──(root㉿kali)-[/etc/openvpn]
└─# ls
ca.crt dh.pem easy-rsa INSAT.crt INSAT.key server.conf server.txt serveur.txt ta.key
┌──(root㉿kali)-[/etc/openvpn]
└─# cd /easy-rsa
cd: aucun fichier ou dossier de ce type: /easy-rsa
┌──(root㉿kali)-[/etc/openvpn]
└─# cd easy-rsa/
┌──(root㉿kali)-[/etc/openvpn/easy-rsa]
└─# ls
easyrsa openssl-easyrsa.cnf pki vars x509-types
┌──(root㉿kali)-[/etc/openvpn/easy-rsa]
└─# cd ..
┌──(root㉿kali)-[/etc/openvpn]
└─# ls
ca.crt dh.pem easy-rsa INSAT.crt INSAT.key server.conf server.txt serveur.txt ta.key
┌──(root㉿kali)-[/etc/openvpn]
└─# scp ta.key meryem@192.168.175.129:/home/meryem/Desktop
meryem@192.168.175.129's password:
ta.key 100% 636 112.1KB/s 00:00
┌──(root㉿kali)-[/etc/openvpn]
└─#





MERYEM ESSAFI
Rapport de mini projet
Ecole nationale supérieure d'électricité et de mécanique


Kali_Linux_Server
Ubuntu_Linux_Client
Activities
Terminal
Dec 27 20:08
root@ubuntu: /etc/openvpn
root@ubuntu:/etc/openvpn# openvpn /etc/openvpn/client.conf
Mon Dec 27 20:04:51 2021 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jul 19 2021
Mon Dec 27 20:04:51 2021 library versions: OpenSSL 1.1.1f 31 Mar 2020, LZO 2.10
Mon Dec 27 20:04:51 2021 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Mon Dec 27 20:04:51 2021 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Mon Dec 27 20:04:51 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.175.128:1194
Mon Dec 27 20:04:51 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Mon Dec 27 20:04:51 2021 UDP link local: (not bound)
Mon Dec 27 20:04:51 2021 UDP link remote: [AF_INET]192.168.175.128:1194
Mon Dec 27 20:05:51 2021 TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
Mon Dec 27 20:05:51 2021 TLS Error: TLS handshake failed
Mon Dec 27 20:05:51 2021 SIGUSR1[soft,tls-error] received, process restarting
Mon Dec 27 20:05:51 2021 Restart pause, 5 second(s)
Mon Dec 27 20:05:56 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.175.128:1194
Mon Dec 27 20:05:56 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Mon Dec 27 20:05:56 2021 UDP link local: (not bound)
Mon Dec 27 20:05:56 2021 UDP link remote: [AF_INET]192.168.175.128:1194
Mon Dec 27 20:06:56 2021 TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
Mon Dec 27 20:06:56 2021 TLS Error: TLS handshake failed
Mon Dec 27 20:06:56 2021 SIGUSR1[soft,tls-error] received, process restarting
Mon Dec 27 20:06:56 2021 Restart pause, 5 second(s)
Mon Dec 27 20:07:01 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.175.128:1194
Mon Dec 27 20:07:01 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Mon Dec 27 20:07:01 2021 UDP link local: (not bound)

CONCLUSION

Actuellement souscrire à un VPN devient une nécessité, puisqu'il présente plusieurs avantages à savoir, être anonyme sur le Net, contourner les restrictions géographique s, télécharger sans être tracé, la prévention contre le piratage des données personnelles, et il est simple à utiliser.

Dans ce contexte, OpenVPN est l'un des protocoles les plus connus, grâce à son haut niveau de sécurité, sa compatibilité avec tous les systèmes d'exploitation, et aussi le fait qu'il est Open Source.

WEBOGRAPHIE

- https://www.futura-sciences.com/tech/definitions/connection-vpn-1819/