

**UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN**



Asignatura: Seminario de Seguridad Informática con énfasis en Hacking Ético

Ciclo: I 2021

Docente: Ing. José Roberto Rivas Magaña

TAREA: Función de hash, Preguntas sobre phishing Y

Configuración Openvpn

Estudiante: Juan Gabriel Soto Aldana

Funciones Hash

En esta practica veremos como funciona el **hash** el cual es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

Como primer punto lo primero será lo guiarnos como super usuario en la terminal de nuestro Kali.

```
(juansoto@kali)-[~]  
$ su  
Contraseña:  
(root@kali)-[/home/juansoto]  
#
```

A hora se instala el paquete de hash con el comando:

```
(root@kali)-[/home/juansoto]  
# sudo apt-get install gtkhash  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
gtkhash ya está en su versión más reciente (1.2-1+b3).  
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 1302 no actualizados.
```

Nos redirigimos al Escritorio y luego crearemos un archivo con el nombre practica.txt el cual colocaremos un texto dentro como se muestra

```
(root@kali)-[/home/juansoto]  
# cd Escritorio  
  
(root@kali)-[/home/juansoto/Escritorio]  
# cat > Practica.txt  
practica123
```

Luego con la teclas Ctrl + d guardamos el contenido.

Así el archivo se creara para conprovar tecleamos **ls -l** de la siguiente manera

```
(root@kali)-[/home/juansoto/Escritorio]
# ls -l
total 4
-rw-r--r-- 1 root root 11 abr 15 08:22 Practica.txt
```

Por lo consiguiente se debe Ejecutar comando de generación de HASH de la siguiente manera:

```
(root@kali)-[/home/juansoto/Escritorio]
# sha256sum Practica.txt
2f8486d3b13adbc63cec678a7af06653e1ee7450374f60913a6b94223cef393a Practica.txt
```

Esta misma captura la pondremos en una tabla.

Editar archive Practica.txt, ejecutar el comando

cat > practica.txt

Modificar archive Practica.txt , nuevo mensaje “modificado123” y presionar Tecla “Ctrl + d”

```
(root@kali)-[/home/juansoto/Escritorio]
# cat > Practica.txt
modificado123
```

Ejecutar comando “ls -l”, y valide que el archivo se encuentre creado.

```
(root@kali)-[/home/juansoto/Escritorio]
# ls -l
total 4
-rw-r--r-- 1 root root 13 abr 15 08:34 Practica.txt
```

Nuevamente se ejecuta el comando

Sha256sum Practica.txt

```
(root@kali)-[/home/juansoto/Escritorio]
# sha256sum Practica.txt
090a0a39069a129474dad160736cb3f6f6b6593112280ed720ab38ffac757802 Practica.txt
```

No.	Archivo	Función Hash	Pantalla
1	Practica.txt	SHA256	<pre>(root@kali)-[/home/juansoto/Escritorio] # sha256sum Practica.txt 2f8486d3b13adbc63cec678a7af06653e1ee7450374f60913a6b94223cef393a Practica.txt</pre>
2	Practica.txt	SHA256	<pre>(root@kali)-[/home/juansoto/Escritorio] # sha256sum Practica.txt 090a0a39069a129474dad160736cb3f6f6b6593112280ed720ab38ffac757802 Practica.txt</pre>
3	Practica.txt	SHA256	<pre>(root@kali)-[/home/juansoto/Escritorio] # sha256sum Practica.txt 2f8486d3b13adbc63cec678a7af06653e1ee7450374f60913a6b94223cef393a Practica.txt</pre>

Nota: al cambiar el archivo y volver aplicar la función de hash es te cambia ya no es el mismo como se muestra en la tabla, pero si este archivo lo volvemos a modificar le damos los valores que tenía anterior mente y aplicamos el hash este volverá hacer igual que la primera vez.

Preguntas sobre phishing

¿Qué tipo de ataque encontró Tricia?

El tipo de ataque sería phishing, porque ase uso de ingeniería social y suplantación de identidad.

¿Por qué el correo electrónico no se marca como spam?

Porque es de un correo conocido aparentemente por ello no se marca como un spam.

¿Cómo se puede controlar este tipo de ataque?

Verificar la fuente de información de tus correos entrantes.

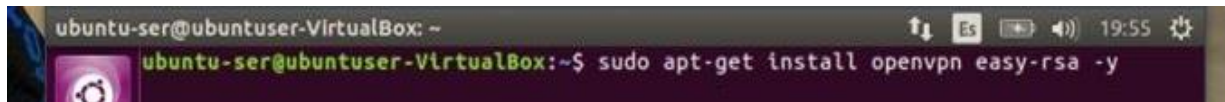
Aser una configuración de correo en el Back End y en el Front End para que el correo pueda ser detectado como spam.

Configuración de openVPN

Como primer paso debemos actualizar los paquetes esto en modo super usuario desde la terminal.

Lo primero es actualizar los paquetes con el comando **apt-get update**.

Ahora empezaremos instalando los paquetes necesarios de la siguiente manera.



```
ubuntu-ser@ubuntuser-VirtualBox: ~  
ubuntu-ser@ubuntuser-VirtualBox:~$ sudo apt-get install openvpn easy-rsa -y
```

Con este comando instalamos el openvpn y tambien openssl

```
ubuntu-ser@ubuntuser-VirtualBox:~$ sudo apt-get install openssl
```

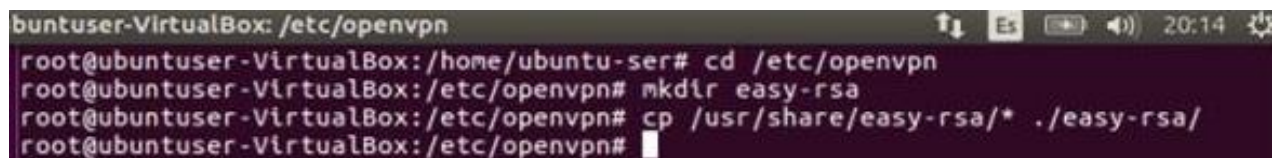
en la máquina que va a actuar de servidor «Server», una vez instalado creamos un directorio que se llamara **easy-rsa** como se muestra en la imagen:



```
buntuser-VirtualBox: /etc/openvpn  
root@ubuntuser-VirtualBox:/home/ubuntu-ser# cd /etc/openvpn  
root@ubuntuser-VirtualBox:/etc/openvpn# mkdir easy-rsa
```

OpenVPN nos ofrece una serie de scripts para la creación de certificados auto firmados para identificar a nuestro servidor tanto como a los clientes, la ubicación de estos scripts es el directorio.

Ahora paso seguido copiaremos las series de scripts al directorio de la siguiente manera:



```
buntuser-VirtualBox: /etc/openvpn  
root@ubuntuser-VirtualBox:/home/ubuntu-ser# cd /etc/openvpn  
root@ubuntuser-VirtualBox:/etc/openvpn# mkdir easy-rsa  
root@ubuntuser-VirtualBox:/etc/openvpn# cp /usr/share/easy-rsa/* ./easy-rsa/  
root@ubuntuser-VirtualBox:/etc/openvpn#
```

Para la creación de los certificados es necesario exportar una serie de variables para definir los datos en la creación de los certificados que vamos a crear. Esto lo realizamos editando el fichero **vars**, que se encuentra en los archivos que copiamos a la carpeta que creamos anterior mente.

```

build-inter      clean-all      revoke-full
build-key        inherit-inter   sign-req
build-key-pass   list-crl        vars
build-key-pkcs12 openssl-0.9.6.cnf whichopensslcnf
build-key-server openssl-0.9.8.cnf
root@ubuntuuser-VirtualBox:/etc/openvpn/easy-rsa#

```

Lo siguiente es proceder a modificarlo con el siguiente comando:

```

ubuntuuser-VirtualBox: /etc/openvpn/easy-rsa
root@ubuntuuser-VirtualBox:/etc/openvpn# cd easy-rsa
root@ubuntuuser-VirtualBox:/etc/openvpn/easy-rsa# nano vars

```

y dentro del directorio **vars** se harán ciertas modificaciones quedando de la siguiente manera:

```
export EASY_RSA="`pwd`"
```

```
export OPENSSL="openssl"
```

```
export PKCS11TOOL="pkcs11-tool"
```

```
export GREP="grep"
```

```
export KEY_CONFIG=`$EASY_RSA/whichopensslcnf`
```

```
$EASY_RSA` export KEY_DIR="$EASY_RSA/keys"
```

```
echo NOTE: If you run ./clean-all, I will be doing a rm -rf on $KEY_DIR
```

```
export PKCS11_MODULE_PATH="/usr/lib/changeme.so"
```

```
export PKCS11_PIN=usuario
```

```
export KEY_SIZE=2048
```

```
export CA_EXPIRE=365
```

```
export KEY_EXPIRE=365
```

```
export KEY_COUNTRY="SV"
```

```
export KEY_PROVINCE="El Salvador"
```

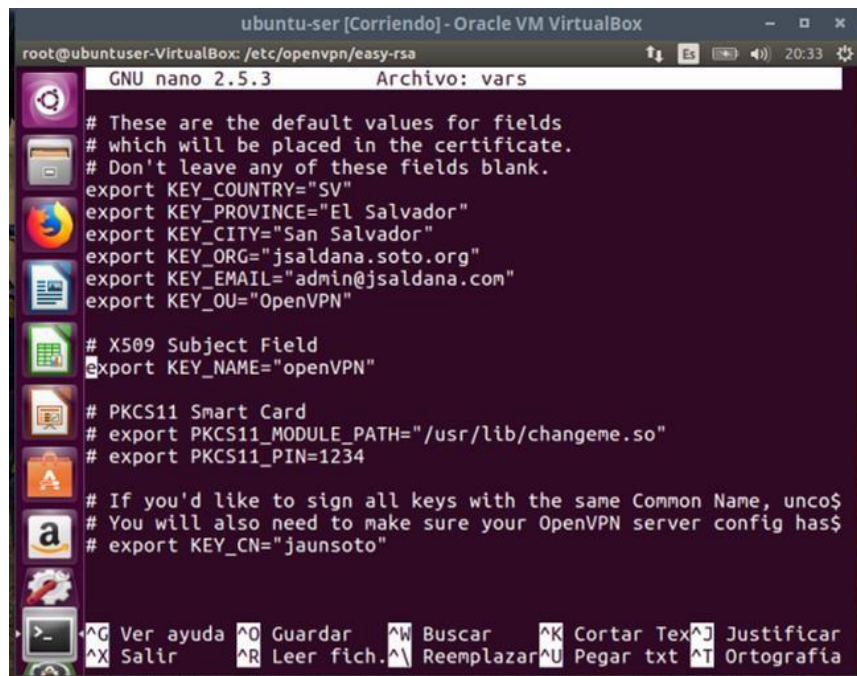
```
export KEY_CITY="San Salvador"
```

```
export KEY_ORG="jsaldana.soto.org"
```

```
export KEY_EMAIL="admin@jsaldana.com" export KEY_OU="OpenVPN"
```

```
export KEY_NAME=openVPN
```

```
export KEY_CN=JuanluRamirez
```

```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openvpn/easy-rsa
GNU nano 2.5.3 Archivo: vars

# 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="SV"
export KEY_PROVINCE="El Salvador"
export KEY_CITY="San Salvador"
export KEY_ORG="jsaldana.soto.org"
export KEY_EMAIL="admin@jsaldana.com"
export KEY_OU="OpenVPN"

# X509 Subject Field
export KEY_NAME="openVPN"

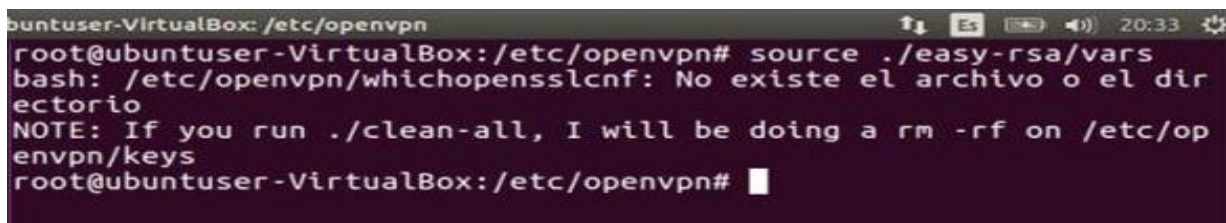
# PKCS11 Smart Card
# export PKCS11_MODULE_PATH="/usr/lib/changetime.so"
# export PKCS11_PIN=1234

# If you'd like to sign all keys with the same Common Name, uncomment
# You will also need to make sure your OpenVPN server config has
# export KEY_CN="jaunsoto"

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar texto ^T Ortografía
```

Luego de haber hecho las modificaciones en el archivo se guarda con Ctrl+o y Ctrl+x para salir

Ejecutamos el script modificado de la siguiente manera:



```
ubuntuser-VirtualBox: /etc/openvpn
root@ubuntuser-VirtualBox:/etc/openvpn# source ./easy-rsa/vars
bash: ./easy-rsa/vars: No existe el archivo o el directorio
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/keys
root@ubuntuser-VirtualBox:/etc/openvpn#
```

Con esto tenemos todas las configuraciones previas a la creación de certificados.

Creación llave diffies hellman

Es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada). Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión (establecer clave de sesión). Siendo no autenticado, sin embargo, provee las bases para varios protocolos autenticados.

build-dh

```
ubuntu-VirtualBox: /etc/openvpn/easy-rsa
root@ubuntu-VirtualBox:/etc/openvpn/easy-rsa# ./build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+.....
.....+.....
.....+.....
.....+.....
.....+.....
.....+.....
```

A continuación, lo que vamos a realizar la creación del certificado y se realiza ejecutando el siguiente fichero.

```

root@buntuser-VirtualBox:/etc/openvpn/easy-rsa# ./clean-all
root@buntuser-VirtualBox:/etc/openvpn/easy-rsa# ./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) [SV]:y
string is too short, it needs to be at least 2 bytes long
Country Name (2 letter code) [SV]:
State or Province Name (full name) [El Salvador]:
Locality Name (eg, city) [San Salvador]:
Organization Name (eg, company) [jsaldana.soto.org]:

```

Creación de Clave y Certificado raíz

Para que OpenVPN pueda funcionar correctamente tendremos que crear un certificado y una key en el servidor para que así se pueda realizar la conexión correctamente, para ello vamos a ejecutar el siguiente fichero, seguido del nombre del servidor que en nuestro caso vamos a poner servidor.


```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
ubuntuser-VirtualBox: /etc/openvpn/easy-rsa
root@ubuntuser-VirtualBox: /etc/openvpn/easy-rsa# ./build-key-server servidor
Generating a 2048 bit RSA private key
.....+++
.....++
writing new private key to 'servidor.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) [SV]:
```

```
ubuntuser-VirtualBox: /etc/openvpn/easy-rsa
Email Address [admin@jsaldana.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'SV'
stateOrProvinceName     :PRINTABLE:'El Salvador'
localityName            :PRINTABLE:'San Salvador'
organizationName        :PRINTABLE:'jsaldana.soto.org'
organizationalUnitName  :PRINTABLE:'OpenVPN'
commonName              :PRINTABLE:'servidor'
name                   :PRINTABLE:'openVPN'
emailAddress            :IASSTRING:'admin@jsaldana.com'
Certificate is to be certified until May 27 04:05:31 2021 GMT (36
5 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
root@ubuntuser-VirtualBox: /etc/openvpn/easy-rsa#
```

Acto seguido vamos realizar la creación del certificado de la segunda máquina que permitirá la conexión remota para ello vamos a ejecutar el fichero denominado build-key, seguido del nombre del equipo que en nuestro caso se denomina ubuntu-clien.

```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
buntuser-VirtualBox: /etc/openvpn/easy-rsa
root@buntuser-VirtualBox:/etc/openvpn/easy-rsa# ./build-key ubuntu-clien
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'ubuntu-clien.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) [SV]:
```

```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
buntuser-VirtualBox: /etc/openvpn/easy-rsa
Email Address [admin@jsaldana.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'SV'
stateOrProvinceName  :PRINTABLE:'El Salvador'
localityName         :PRINTABLE:'San Salvador'
organizationName     :PRINTABLE:'jsaldana.soto.org'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName           :PRINTABLE:'ubuntu-clien'
name                 :PRINTABLE:'openVPN'
emailAddress         :IASSTRING:'admin@jsaldana.com'
Certificate is to be certified until May 27 04:17:33 2021 GMT (36
5 days)
Sign the certificate? [y/n]:y

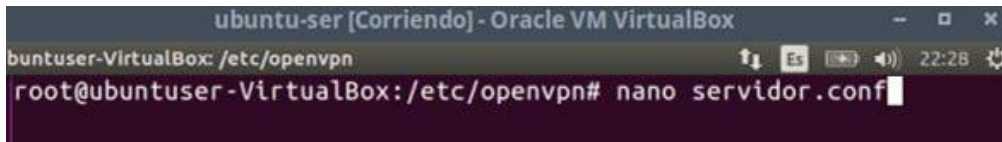
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@buntuser-VirtualBox:/etc/openvpn/easy-rsa#
```

Ya tendremos todas las claves y certificados en el directorio.

Configuración túnel en las dos maquinas

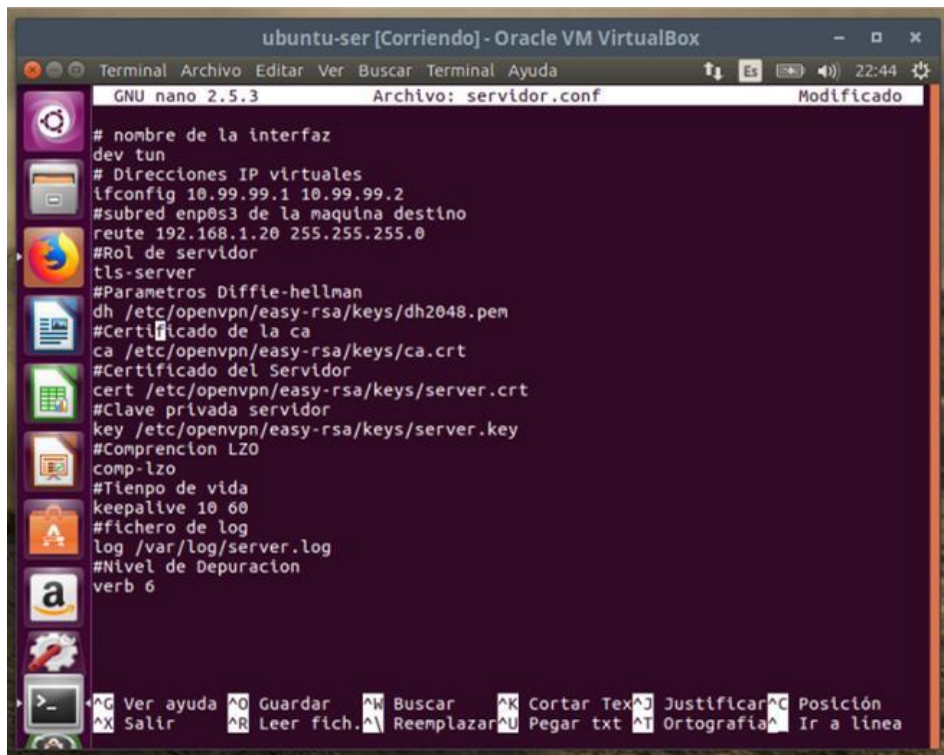
El siguiente paso es crear un fichero que se llamara servidor.conf.

De esta manera como se muestra:



```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
buntuser-VirtualBox: /etc/openvpn
root@buntuser-VirtualBox:/etc/openvpn# nano servidor.conf
```

con el contenido siguiente:



```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
GNU nano 2.5.3 Archivo: servidor.conf Modificado
# nombre de la interfaz
dev tun
# Direcciones IP virtuales
ifconfig 10.99.99.1 10.99.99.2
#subred enp0s3 de la maquina destino
route 192.168.1.20 255.255.255.0
#Rol de servidor
tls-server
#Parametros Diffie-hellman
dh /etc/openvpn/easy-rsa/keys/dh2048.pem
#Certificado de la ca
ca /etc/openvpn/easy-rsa/keys/ca.crt
#Certificado del Servidor
cert /etc/openvpn/easy-rsa/keys/server.crt
#Clave privada servidor
key /etc/openvpn/easy-rsa/keys/server.key
#Compresion LZ0
comp-lzo
#Tiempo de vida
keepalive 10 60
#fichero de log
log /var/log/server.log
#Nivel de Depuracion
verb 6
```

en el archivo modificado se coloco las direcciones ip virtuales el rol que tendrá la configuración, así como también la subred de la maquina destino y las rutas de los certificados.

Una vez creado y guardado el fichero reiniciamos el servicio

/etc/init.d/openvpn restart && reboot

, al volver a arrancar la maquina realizamos un **ip a** y observamos ya tenemos nuestro túnel:


```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
buntuser-VirtualBox: /etc/openvpn
root@buntuser-VirtualBox: /etc/openvpn# ifconfig tun0
tun0      Link encap:UNSPEC  direcciónHW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          Direc. inet:10.99.99.1  P-t-P:10.99.99.2  Másc:255.255.255.255
          Dirección inet6: fe80::757d:3cf6:d3b4:6db/64 Alcance:Enlace
          ACTIVO PUNTO A PUNTO FUNCIONANDO NOARP MULTICAST MTU:1500  Métrica:1
          Paquetes RX:37 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:38 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:100
          Bytes RX:2892 (2.8 KB)  TX bytes:2940 (2.9 KB)
root@buntuser-VirtualBox: /etc/openvpn#
```

El último paso en el servidor es permitir el enrutamiento para ello modificamos la siguiente línea en **/etc/sysctl.conf**.

```
ubuntu-ser [Corriendo] - Oracle VM VirtualBox
GNU nano 2.5.3      Archivo: /etc/sysctl.conf
# 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

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex^J Justificar^C Posición
^X Salir ^R Leer fich.^L Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Ahora procederemos a configurar nuestra maquina que actuara como cliente.

Ubuntu-clien

Esta máquina actuara como cliente y de igual manera se instalaran los paquete de openvpn, ssh, y openssl.

apt-get instal openvpn

apt-get instal ssh

apt-get instal openssl

una vez instalado, vamos a adquirir los certificados creados en nuestro servidor, para ello vamos a utilizar el comando

```
ubuntu-ser@192.168.43.122's password:
Amazon s such file or directory
er-VirtualBox:/etc/openssl/easy-rsa/keys# scp ubuntu-clien.* ubuntu-
u-ser@192.168.43.122:/etc/openssl/keys/
ubuntu-ser@192.168.43.122's password:
ubuntu-clien.crt          100% 5664      5.5KB/s   00:00
ubuntu-clien.csr         100% 1110      1.1KB/s   00:00
ubuntu-clien.key          100% 1708      1.7KB/s   00:00
root@ubuntuser-VirtualBox:/etc/openssl/easy-rsa/keys#
```

De esta manera a través de **ssh** hemos compartido los certificados para nuestro maquina cliente para tener la certeza que no fueran modificados enviándolos de manera segura.

Creamos fichero cliente.conf dentro del archivo openssl como super usuario

nano cliente.conf

Dentro del archivo se escribirá lo siguiente:

```
ubuntu-clien [Corriendo] - Oracle VM VirtualBox
buntuser-VirtualBox: /etc/openssl
GNU nano 2.5.3 Archivo: cliente.conf

# nombre de la interfaz
dev tun
# Direcciones IP virtuales
ifconfig 10.99.99.2 10.99.99.1
#Ip eth0 servidor
remote 192.168.43.131
# Subred eth1 de la maquina destino
route 10.99.99.0 255.255.255.0
# Rol de Servidor
tls-client
# Certificado de la CA
ca /etc/openssl/keys/ca.crt
# Certificado Servidor
cert /etc/openssl/keys/ubuntu-clien.crt
# Clave privada servidor
key /etc/openssl/keys/ubuntu-clien.key
# Compresión LZ0
comp-lzo
# Tiempo de vida
keepalive 10 60
# Fichero de log
log /var/log/ubuntu-clien.log
# Nivel de Depuración
verb 6

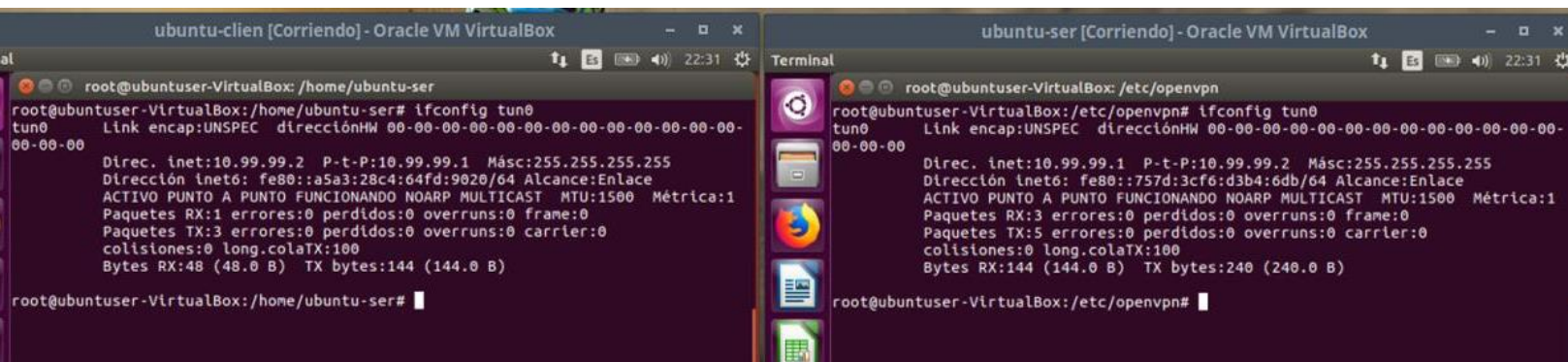
[ 24 líneas leídas ]
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```


Guardamos la configuración Ctrl + O y Ctrl + X para salir, reiniciamos el servicio y reiniciamos la maquina como super usuario con el siguiente comando:

/etc/init.d/openvpn restart

Luego se reinician las máquinas.

Comprobaciones túnel



```
ubuntu-clien [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /home/ubuntu-ser
root@ubuntuser-VirtualBox:/home/ubuntu-ser# ifconfig tun0
tun0    Link encap:UNSPEC  direcciónHW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        Direc. inet:10.99.99.2 P-t-P:10.99.99.1 Másc:255.255.255.255
        Dirección inet6: fe80::a5a3:28c4:64fd:9020/64 Alcance:Enlace
        ACTIVO PUNTO A PUNTO FUNCIONANDO NOARP MULTICAST MTU:1500 Métrica:1
        Paquetes RX:1 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:3 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colataTX:100
        Bytes RX:48 (48.0 B) TX bytes:144 (144.0 B)

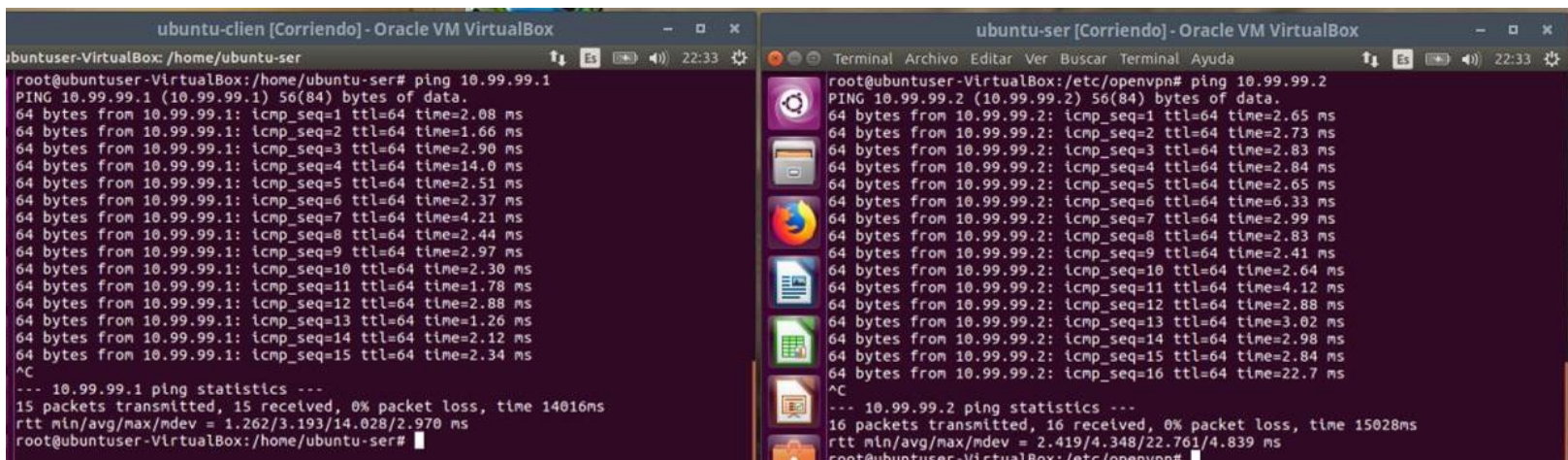
root@ubuntuser-VirtualBox:/home/ubuntu-ser#

ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openvpn
root@ubuntuser-VirtualBox:/etc/openvpn# ifconfig tun0
tun0    Link encap:UNSPEC  direcciónHW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        Direc. inet:10.99.99.1 P-t-P:10.99.99.2 Másc:255.255.255.255
        Dirección inet6: fe80::757d:3cf6:d3b4:6db/64 Alcance:Enlace
        ACTIVO PUNTO A PUNTO FUNCIONANDO NOARP MULTICAST MTU:1500 Métrica:1
        Paquetes RX:3 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:5 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colataTX:100
        Bytes RX:144 (144.0 B) TX bytes:240 (240.0 B)

root@ubuntuser-VirtualBox:/etc/openvpn#
```

Ya las dos máquinas tienen la configuración y podemos comprobar con **ifconfig tun0** que las maquinas tienen activa el acceso túnel.

Ahora comprobaremos si existe comunicación entre las dos máquinas, asiendo ping, de la siguiente manera:



```
ubuntu-clien [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /home/ubuntu-ser
root@ubuntuser-VirtualBox:/home/ubuntu-ser# ping 10.99.99.1
PING 10.99.99.1 (10.99.99.1) 56(84) bytes of data.
64 bytes from 10.99.99.1: icmp_seq=1 ttl=64 time=2.08 ms
64 bytes from 10.99.99.1: icmp_seq=2 ttl=64 time=1.66 ms
64 bytes from 10.99.99.1: icmp_seq=3 ttl=64 time=2.90 ms
64 bytes from 10.99.99.1: icmp_seq=4 ttl=64 time=14.0 ms
64 bytes from 10.99.99.1: icmp_seq=5 ttl=64 time=2.51 ms
64 bytes from 10.99.99.1: icmp_seq=6 ttl=64 time=2.37 ms
64 bytes from 10.99.99.1: icmp_seq=7 ttl=64 time=4.21 ms
64 bytes from 10.99.99.1: icmp_seq=8 ttl=64 time=2.44 ms
64 bytes from 10.99.99.1: icmp_seq=9 ttl=64 time=2.97 ms
64 bytes from 10.99.99.1: icmp_seq=10 ttl=64 time=2.30 ms
64 bytes from 10.99.99.1: icmp_seq=11 ttl=64 time=1.78 ms
64 bytes from 10.99.99.1: icmp_seq=12 ttl=64 time=2.88 ms
64 bytes from 10.99.99.1: icmp_seq=13 ttl=64 time=1.26 ms
64 bytes from 10.99.99.1: icmp_seq=14 ttl=64 time=2.12 ms
64 bytes from 10.99.99.1: icmp_seq=15 ttl=64 time=2.34 ms
^C
--- 10.99.99.1 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14016ms
rtt min/avg/max/mdev = 1.262/3.193/14.028/2.970 ms
root@ubuntuser-VirtualBox:/home/ubuntu-ser#

ubuntu-ser [Corriendo] - Oracle VM VirtualBox
root@ubuntuser-VirtualBox: /etc/openvpn
root@ubuntuser-VirtualBox:/etc/openvpn# ping 10.99.99.2
PING 10.99.99.2 (10.99.99.2) 56(84) bytes of data.
64 bytes from 10.99.99.2: icmp_seq=1 ttl=64 time=2.65 ms
64 bytes from 10.99.99.2: icmp_seq=2 ttl=64 time=2.73 ms
64 bytes from 10.99.99.2: icmp_seq=3 ttl=64 time=2.83 ms
64 bytes from 10.99.99.2: icmp_seq=4 ttl=64 time=2.84 ms
64 bytes from 10.99.99.2: icmp_seq=5 ttl=64 time=2.65 ms
64 bytes from 10.99.99.2: icmp_seq=6 ttl=64 time=6.33 ms
64 bytes from 10.99.99.2: icmp_seq=7 ttl=64 time=2.99 ms
64 bytes from 10.99.99.2: icmp_seq=8 ttl=64 time=2.83 ms
64 bytes from 10.99.99.2: icmp_seq=9 ttl=64 time=2.41 ms
64 bytes from 10.99.99.2: icmp_seq=10 ttl=64 time=2.64 ms
64 bytes from 10.99.99.2: icmp_seq=11 ttl=64 time=4.12 ms
64 bytes from 10.99.99.2: icmp_seq=12 ttl=64 time=2.88 ms
64 bytes from 10.99.99.2: icmp_seq=13 ttl=64 time=3.02 ms
64 bytes from 10.99.99.2: icmp_seq=14 ttl=64 time=2.98 ms
64 bytes from 10.99.99.2: icmp_seq=15 ttl=64 time=2.84 ms
64 bytes from 10.99.99.2: icmp_seq=16 ttl=64 time=22.7 ms
^C
--- 10.99.99.2 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15028ms
rtt min/avg/max/mdev = 2.419/4.348/22.761/4.839 ms
root@ubuntuser-VirtualBox:/etc/openvpn#
```

como vemos ambas maquinas se encuentran comunicadas entre ellas de esta manera podemos comprobar que la configuración de openvpn fue configurada con éxito.

