**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

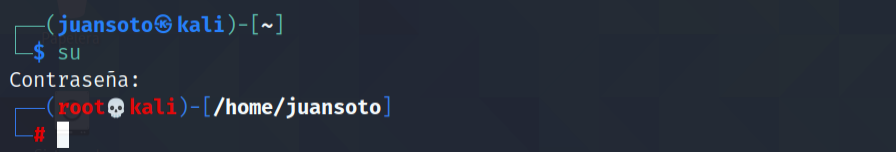
Configuración Openvpn

Estudiante: Juan Gabriel Soto Aldana

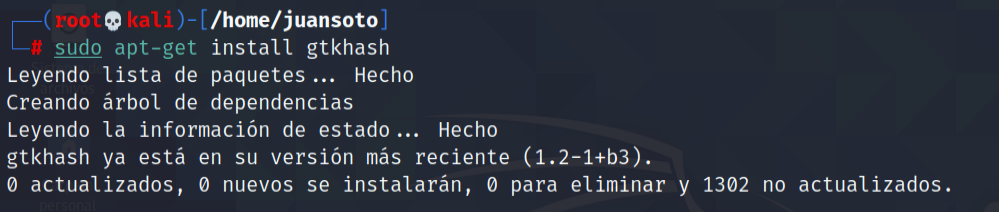
**Funciones Hash**

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

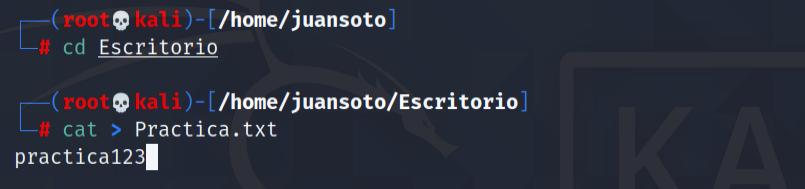
Como primer punto lo primero será lo guiarnos como super usuario en la terminal de nuestro Kali.



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



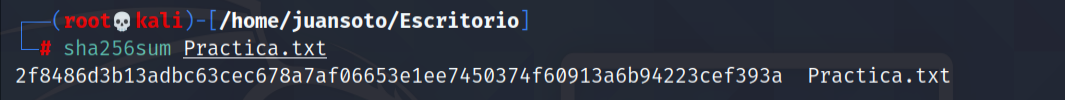
Nos redirigimos al Escritorio y luego crearemos un archivo con el nombre practica.txt el cual colocaremos un texto dentro como se muestra



Luego con la teclas Ctrl + d guardamos el contenido.

Asi el archvio se creara para conprovar tecleamos **ls -l** de la siguiente manera

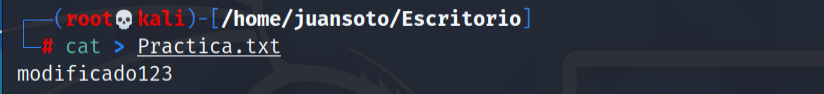
Por lo consiguiente se debe Ejecutar comando de generación de HASH de la siguiente manera:



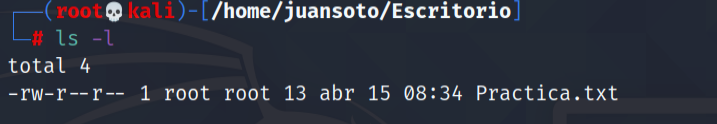
Esta misma captura la pondremos en una tabla.

Editar archive Practica.txt, ejecutar el comando

**cat > practica.txt**

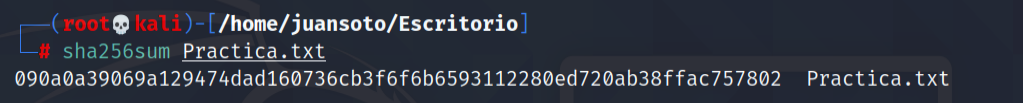
Modificar archive Practica.txt , nuevo mensaje “modificado123” y presionar Tecla “Ctrl + d”

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



Nuevamente se ejecuta el comando

**Sha256sum Practica.txt**



|  |  |  |  |
| --- | --- | --- | --- |
| No. | **Archivo** | **Función Hash** | **Pantalla** |
| 1 | **Practica.txt** | **SHA256** |  |
| 2 | **Practica.txt** | **SHA256** |  |
| 3 | **Practica.txt** | **SHA256** |  |

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 seria 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?**

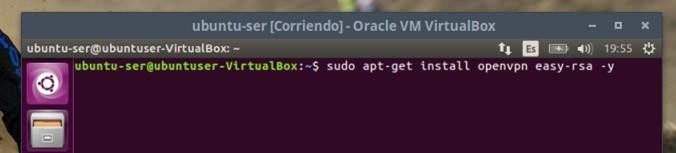
Verificar la fuente de información de tus correos entrantes.

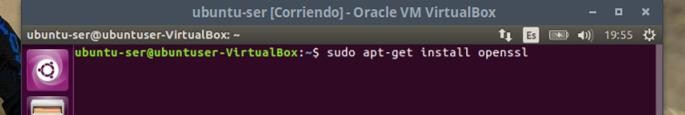
Aser una configuración de correo en el Back End y en el Front End para que el correo pueda ser detectado como spam.

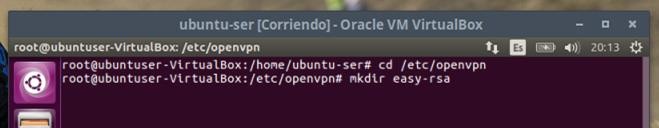
**Configuración de openVPN**

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

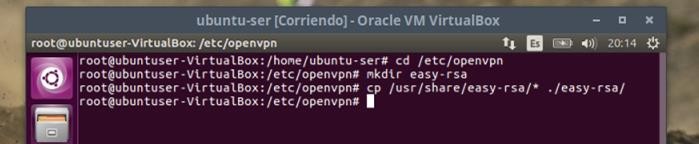
Lo primero es actualizar los paquetes con el comando **apt-get update.**

Ahora empezaremos instalando los paquetes necesarios de la siguiente manera.

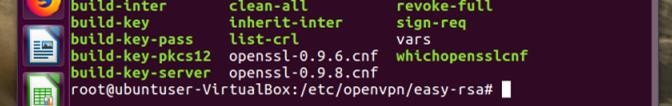
Con este comando instalamos el openvpn y tanbien openssl

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:

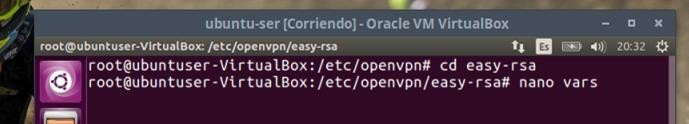
OpenVPN nos ofrece una serie de scripts para la creación de certificados auto firmados para identificar a nuestro servidor tanto como a los clientes, la ubicación de estos scripts es el directorio.

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

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.



Lo siguiente es proceder a modificarlo con el siguiente comando:



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 Savador"

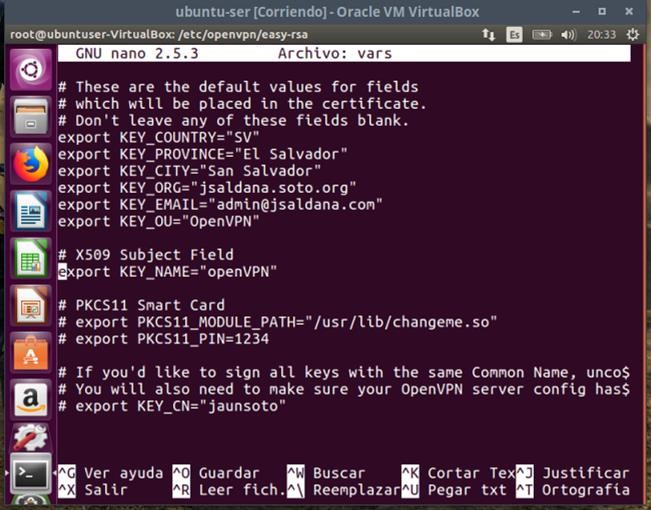
export KEY\_CITY="San Salvador"

export KEY\_ORG="jsaldana.soto.org"

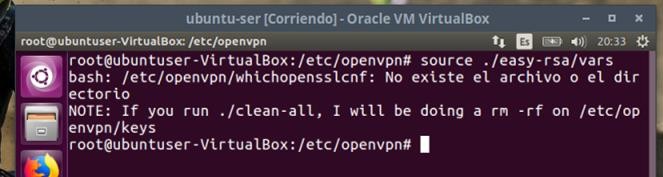
export KEY\_EMAIL="admin@jsaldana.com" export KEY\_OU="OpenVPN"

export KEY\_NAME=openVPN

export KEY\_CN=JuanluRamirez



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:

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

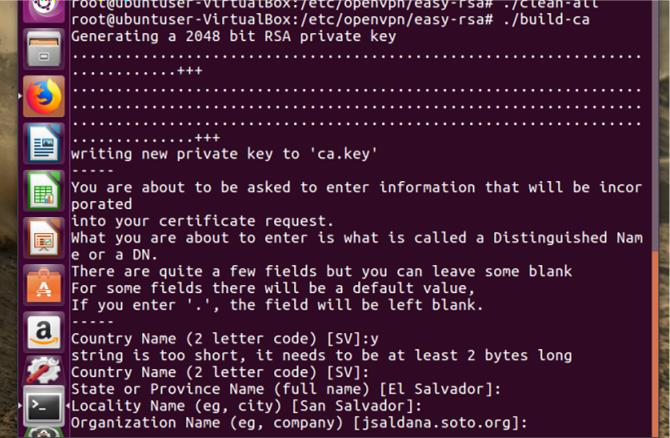
Creación llave diffies hellman

Es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autentificada). 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.

Para ello ejecutamos el script

**build-dh**

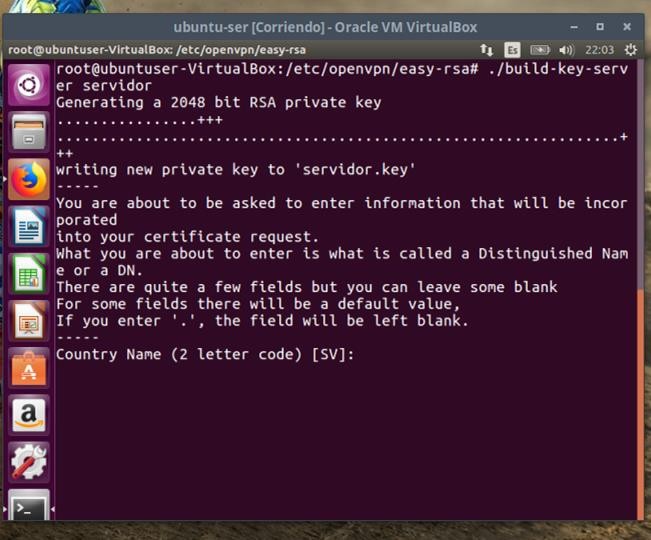
**Creación certificado Autoridad certificadora**

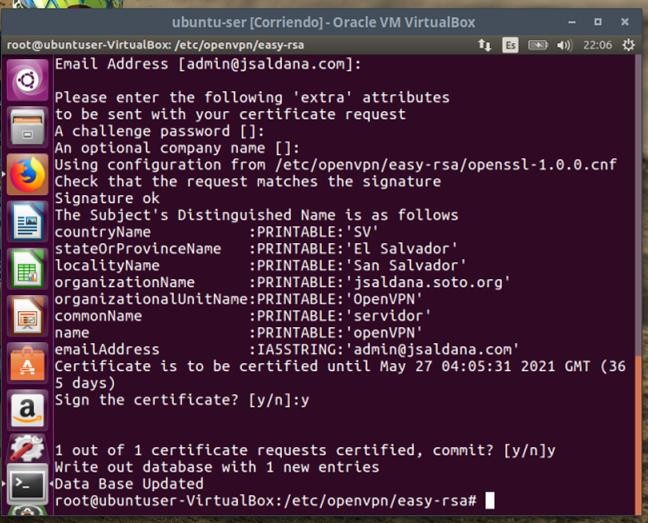
A continuación, lo que vamos a realizar la creación del certificado y se realiza ejecutando el siguiente fichero.

Solo damos Enter según sea necesario.

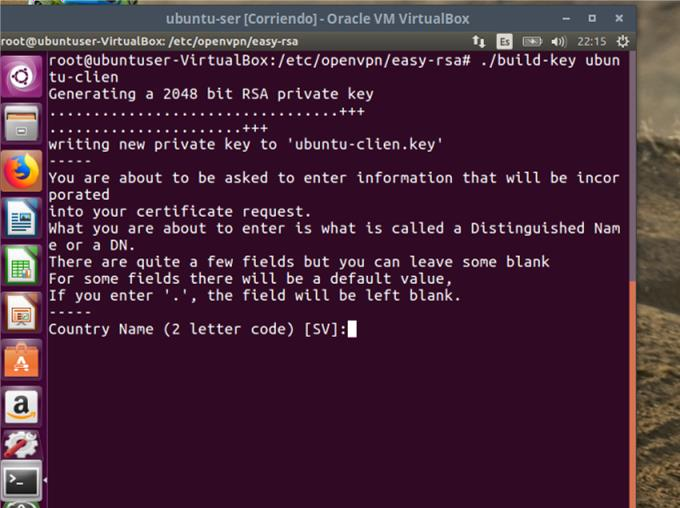
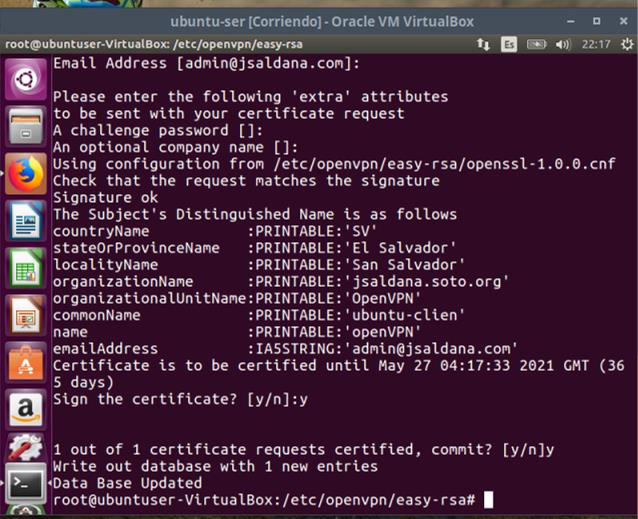
**Creación de Clave y Certificado raíz**

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.





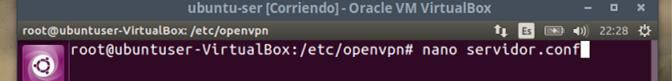
Acto seguido vamos realizar la creación del certificado de la segunda máquina que permitirá la conexión remota para ello vamos a ejecutar el fichero denominado build-key, seguido del nombre del equipo que en nuestro caso se denomina ubuntu-clien.

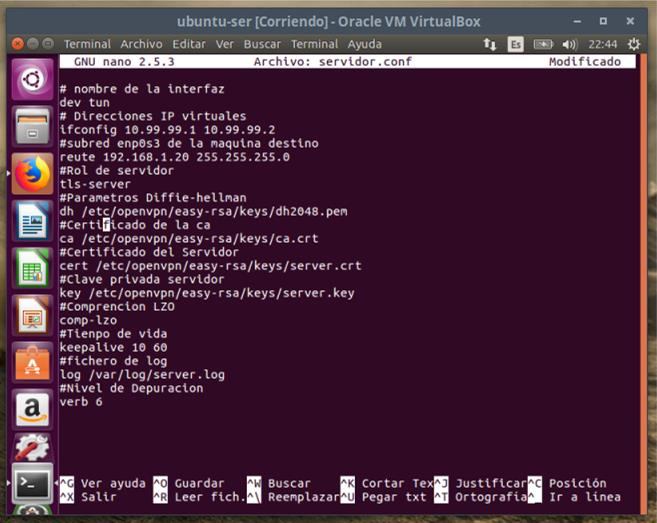


Ya tendremos todas las claves y certificados en el directorio.

**Configuración túnel en las dos maquinas**

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

De esta manera como se muestra:

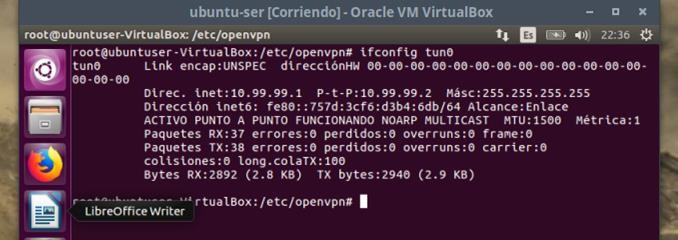
con el contenido siguiente:

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.

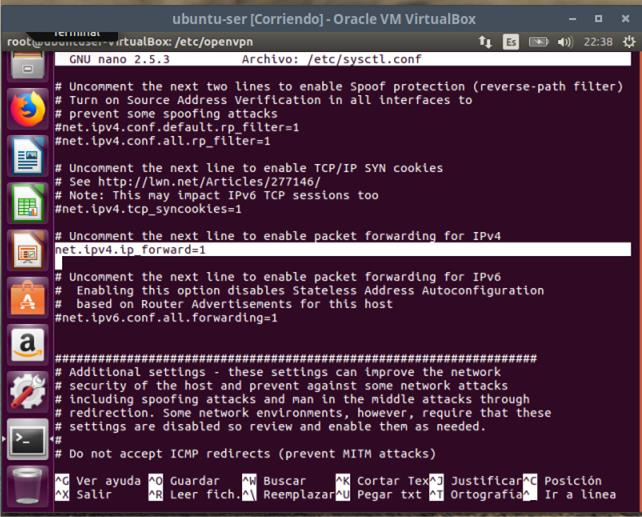
Una vez creado y guardado el fichero reiniciamos el servicio

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

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



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



Ahora procederemos a configurar nuestra maquina que actuara como cliente.

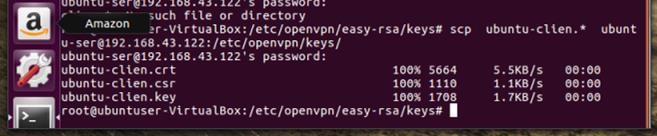
**Ubuntu-clien**

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**

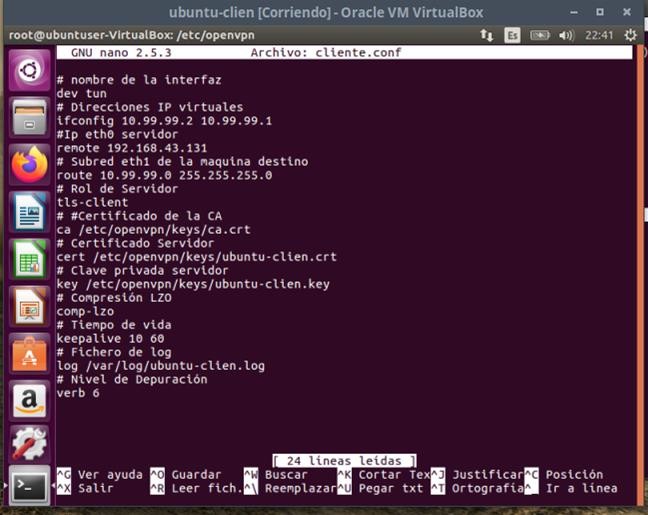
**apt-get instal openssl**

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

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 openvpn como super usuario

**nano cliente.conf**

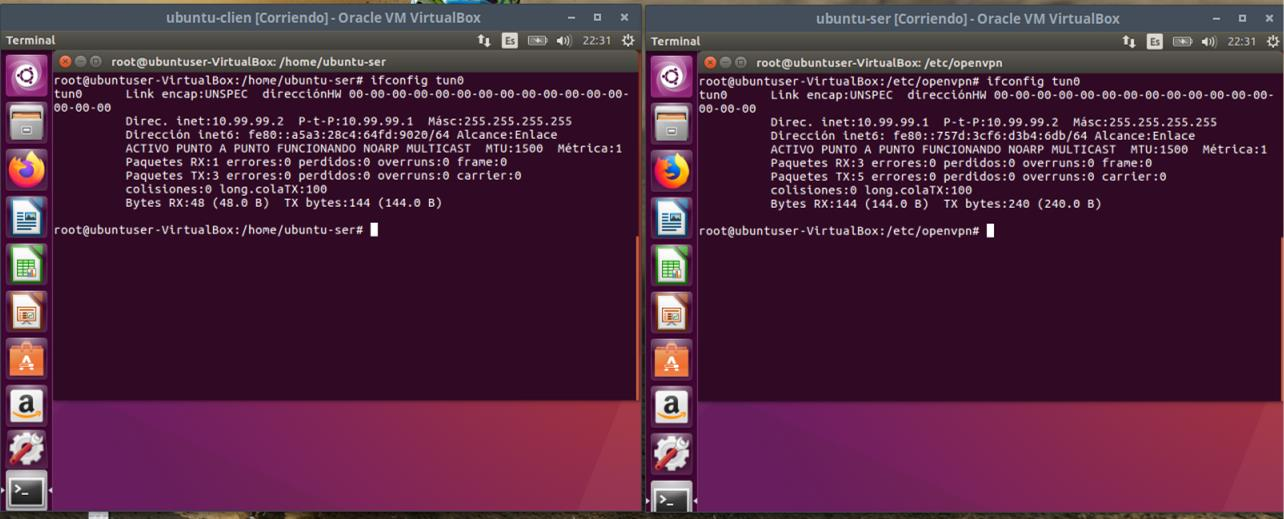
Dentro del archivo se escribirá lo siguiente:

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

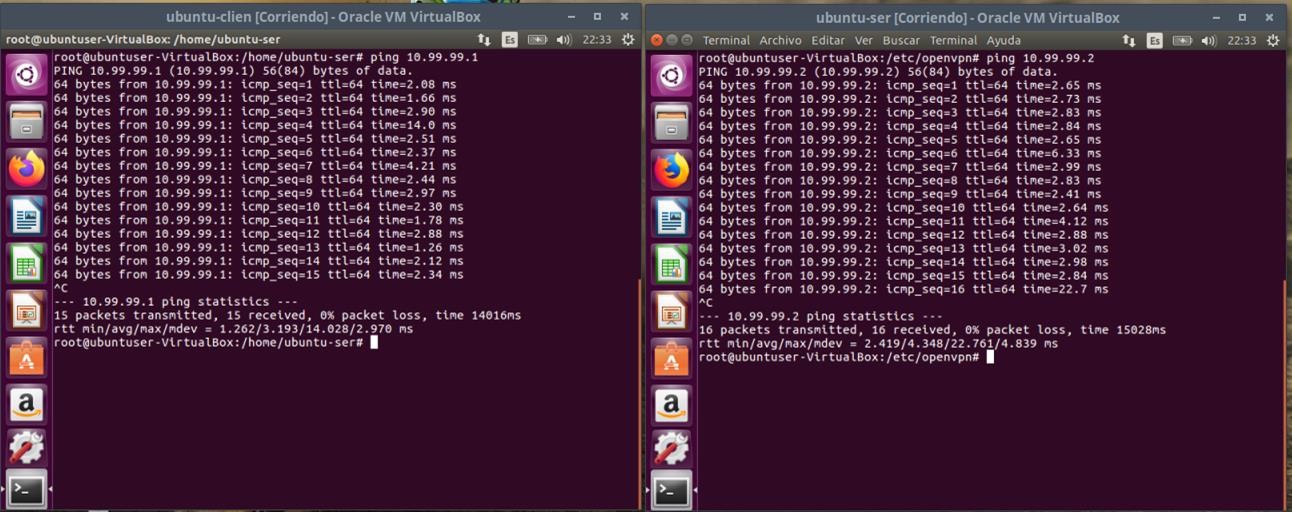
**/etc/init.d/openvpn restart**

Luego se reinician las máquinas.

**Comprobaciones túnel**



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:

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