

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



TITULO O TEMA:

OpenVpn Con Kali Linux

NOMBRE DE ESTUDIANTES:

Cristian Enrique Sánchez Sosa

Rafael Enrique Castillo García

Renato Ernesto Castillo Martínez

Jorge Daniel Vázquez Viera

Santos Alexis Morataya Ruiz

Kenia Dalila Campos Ramírez

Elizabeth Guadalupe Rodríguez Alfaro

ASIGNATURA:

Redes II

DOCENTE:

Rafael Diaz

CICLO/AÑO:

II/2024

INDICE

INTRODUCCIÓN.....	1
1. OBJETIVOS.....	2
1.1 OBJETIVO GENERAL.....	2
1.2. OBJETIVOS ESPECÍFICOS	2
2. JUSTIFICACIÓN	3
4. SELECCIÓN DE DISPOSITIVOS Y SOFTWARE	5
5. ESQUEMA DE DIRECCIONAMIENTO IP.....	6
5. CONFIGURACION Y EJECUCION TECNICA	7
5.1. Instalacion de VirtualBox y Kali Linux.....	7
1. Descargamos VirtualBox desde su pagina oficial	7
5.2. Instalación de OpenVPN en Kali Linux	8
6. FUNCIONAMIENTO DE LA VPN	13
7. DECISIONES DE DISEÑO Y JUSTIFICACIONES	14
8. MANUAL DE USUARIO	15
INTRODUCCIÓN.....	16
1. OBJETIVOS.....	17
1.1 OBJETIVO GENERAL.....	17
1.2. OBJETIVOS ESPECÍFICOS	17
2. JUSTIFICACIÓN	18
3. QUE ES VPN Y KALI LINUX	19
4. CONFIGURACION Y EJECUCION TECNICA	20
4.1. Instalacion de VirtualBox y Kali Linux.....	20
15. Descargamos VirtualBox desde su pagina oficial	20

4.2. Instalación de OpenVPN en Kali Linux	21
5. DIAGRAMAS	26
6. ALCANCES	29
7. CONSLUSION.....	30

INTRODUCCIÓN

En un mundo digitalmente conectado, la tecnología desempeña un papel fundamental en la transformación de los procesos educativos. Con el propósito de mejorar la accesibilidad y facilitar la gestión de cursos y contenido educativo, nos complace presentar nuestra innovadora aplicación móvil diseñada para ofrecer una experiencia de aprendizaje moderna y eficiente.

Nuestra app de cursos, desarrollada con Ionic, Angular y Firebase, está pensada para optimizar el aprendizaje para estudiantes. Gracias a su interfaz amigable e intuitiva, la aplicación permite gestionar y acceder a una variedad de cursos de manera rápida y sencilla. A través de su diseño innovador, buscamos brindar a los usuarios una plataforma interactiva que fomente el aprendizaje continuo y la colaboración.

Una de las características más destacadas de la aplicación es su capacidad para gestionar contenido multimedia, como documentos. Además, Firebase proporciona una infraestructura robusta para la gestión en tiempo real, permitiendo un acceso rápido y seguro a la información.

Con esta app, transformamos la forma en que los estudiantes y docentes se conectan, mejorando la experiencia educativa y haciendo más efectiva la gestión de los cursos.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Implementar una solución de red segura basada en una VPN utilizando Kali Linux y OpenVPN, con configuraciones y medidas de seguridad adecuadas, que permita proteger el tráfico de datos y garantizar la privacidad y autenticidad en las comunicaciones.

1.2. OBJETIVOS ESPECÍFICOS

- Diseñar la topología de red y asignar el direccionamiento IP.
- Configurar el servidor OpenVPN en Kali Linux.
- Validar la funcionalidad de la VPN mediante pruebas de conectividad.

2. JUSTIFICACIÓN

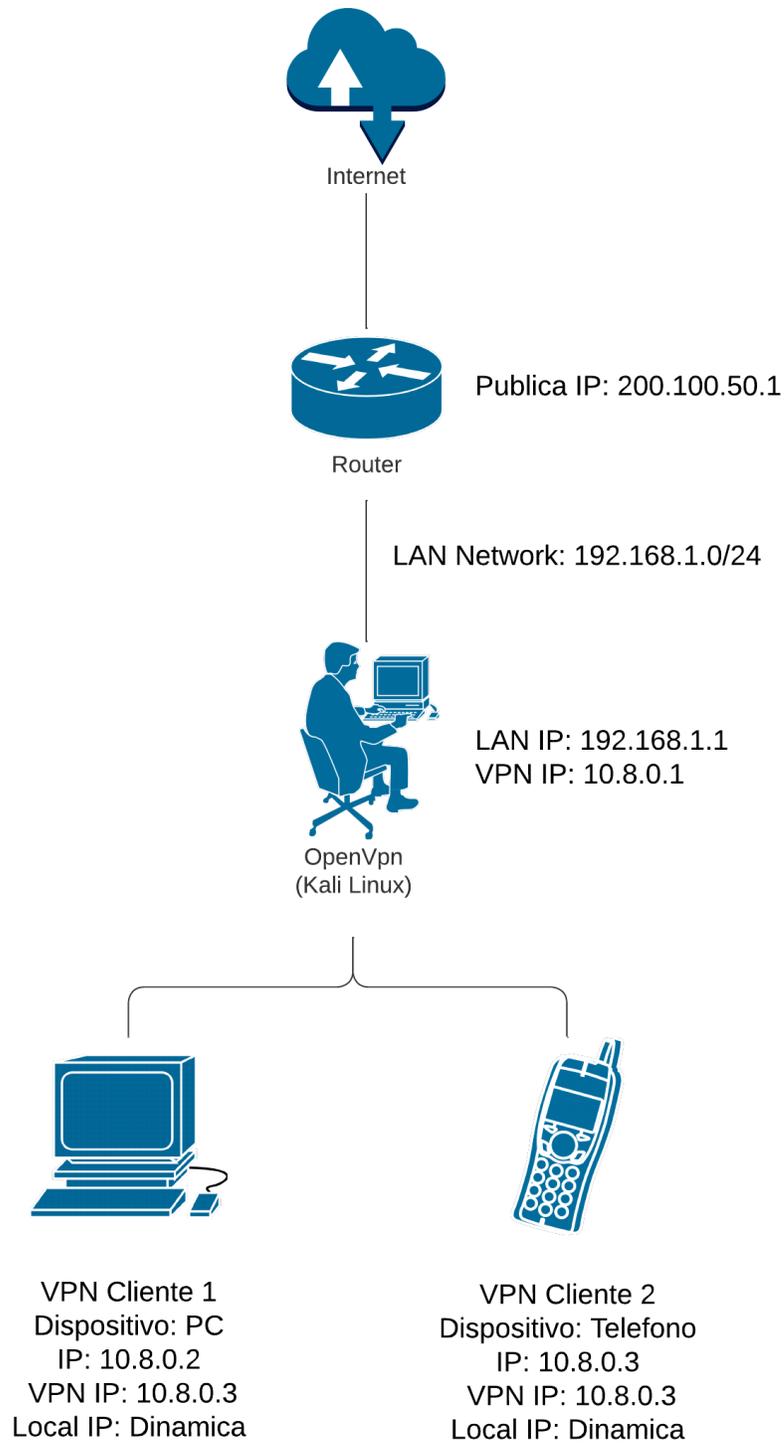
El desarrollo de este proyecto de implementación de una VPN con Kali Linux y OpenVPN se fundamenta en la creciente necesidad de proteger la privacidad y seguridad de los datos en un entorno digital cada vez más interconectado. Las amenazas cibernéticas actuales y el aumento del uso de redes públicas destacan la importancia de contar con soluciones efectivas que garanticen conexiones seguras y confiables.

La elección de OpenVPN, junto con la versatilidad de Kali Linux, responde a la necesidad de crear un entorno controlado y seguro, asegurando la confidencialidad, integridad y autenticidad del tráfico de datos. Esta implementación no solo aborda problemas de seguridad, sino que también proporciona una herramienta práctica para el aprendizaje y la mejora de habilidades técnicas en redes y seguridad informática.

Asimismo, el proyecto tiene relevancia educativa, ya que permite experimentar con tecnologías avanzadas y explorar configuraciones reales en un entorno seguro. La documentación y el manual de usuario facilitan su replicabilidad, permitiendo a otros interesados aplicar este conocimiento en sus propios entornos, contribuyendo a la difusión de buenas prácticas de seguridad en redes.

Finalmente, la implementación de esta VPN es coherente con las tendencias actuales en ciberseguridad y privacidad, destacando su utilidad tanto en el ámbito personal como profesional. La solución planteada promueve la adopción de tecnologías seguras y refuerza la importancia de mantener la seguridad en la era digital.

3. TOPOLOGIA DE RED



4. SELECCIÓN DE DISPOSITIVOS Y SOFTWARE

Para el desarrollo del proyecto de VPN con Kali Linux y OpenVPN, se seleccionaron los siguientes dispositivos y herramientas basándose en su funcionalidad, disponibilidad, compatibilidad y facilidad de implementación en un entorno virtualizado.

Servidor VPN

Dispositivo: Máquina virtual en VirtualBox corriendo Kali Linux.

Especificaciones mínimas para VirtualBox:

Host (equipo anfitrión):

- Procesador: Dual-core (2.0 GHz o superior).
- Memoria RAM: 8 GB (recomendado para ejecutar máquinas virtuales sin afectar el rendimiento del host).
- Almacenamiento: 50 GB libres para VM y otros archivos de soporte.
- Sistema Operativo del host: Windows, macOS o Linux.

Máquina virtual (Kali Linux):

- RAM asignada: 2-4 GB.
- Almacenamiento asignado: 20 GB.
- Configuración de red: Adaptador en modo puente (Bridge Mode) o NAT con reenvío de puertos.

Justificación:

VirtualBox facilita la creación de entornos controlados y flexibles para pruebas. Kali Linux es ideal como servidor VPN debido a sus herramientas de red y compatibilidad con OpenVPN.

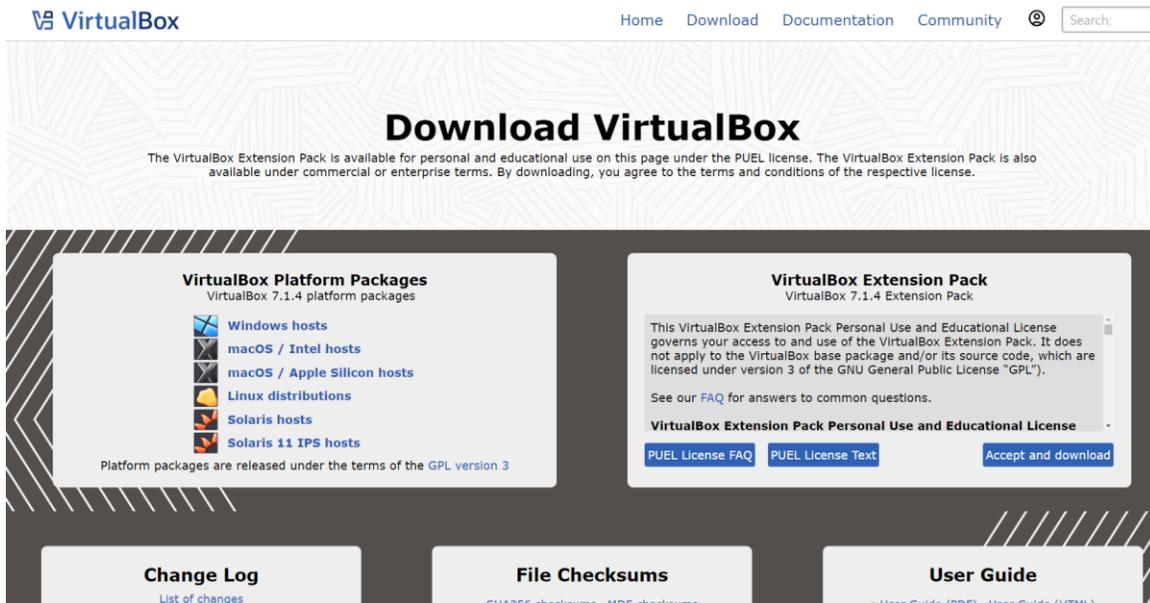
5. ESQUEMA DE DIRECCIONAMIENTO IP

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway
Internet	-	Asignada por ISP	255.255.255.0	Asignada por ISP
Router (WAN - hacia Internet)	Interfaz WAN	200.100.50.1	255.255.255.0	Asignada por ISP
Router (LAN - hacia la red interna)	Interfaz LAN	192.168.1.254	255.255.255.0	-
Servidor OpenVPN (Kali Linux)	Interfaz LAN física	192.168.1.1	255.255.255.0	192.168.1.254
Red VPN (OpenVPN)	Interfaz virtual (tun0)	10.8.0.1	255.255.255.0	-
Cliente VPN 1 (PC)	Interfaz VPN	10.8.0.2	255.255.255.0	10.8.0.1
Cliente VPN 2 (Móvil)	Interfaz VPN	10.8.0.3	255.255.255.0	10.8.0.1

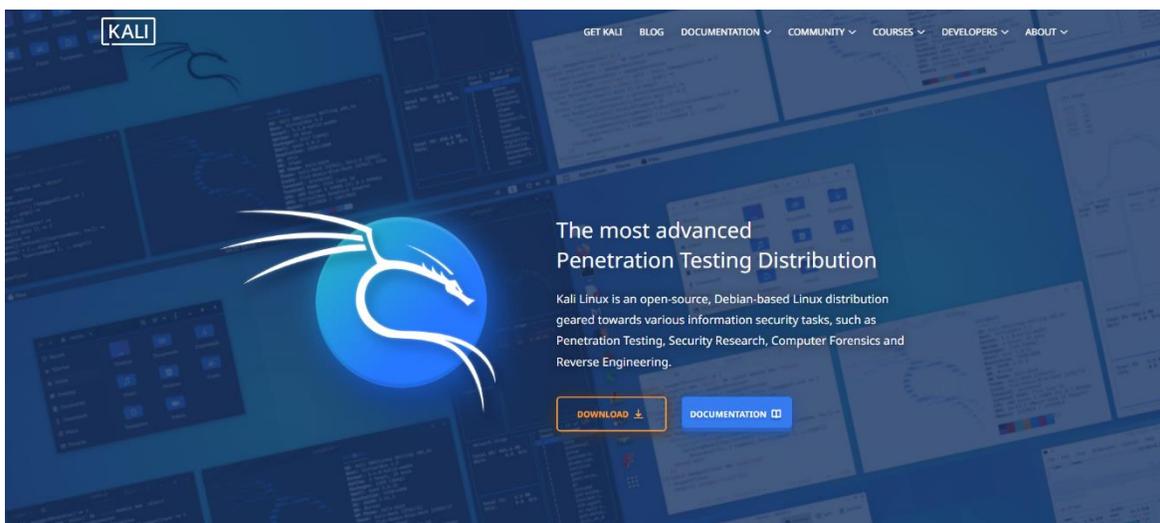
5. CONFIGURACION Y EJECUCION TECNICA

5.1. Instalacion de VirtualBox y Kali Linux

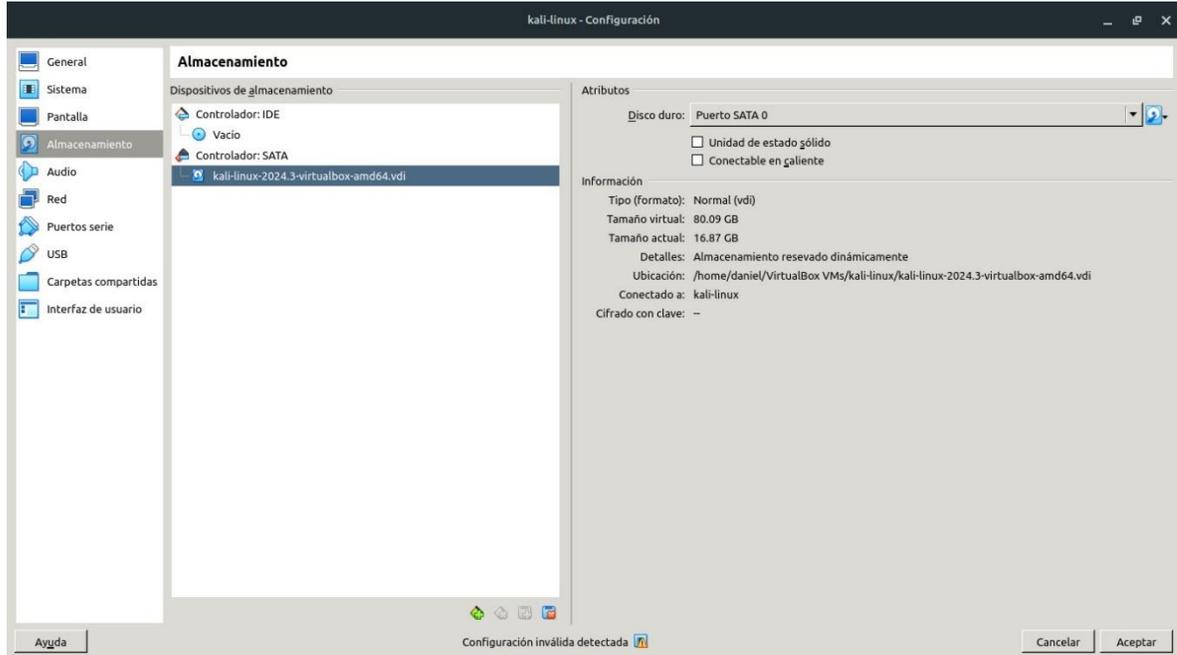
1. Descargamos VirtualBox desde su pagina oficial



2. Descargamos la ISO de Kali Linux desde su pagina oficial



3. Configuramos nuestra maquina virtual con las siguientes características

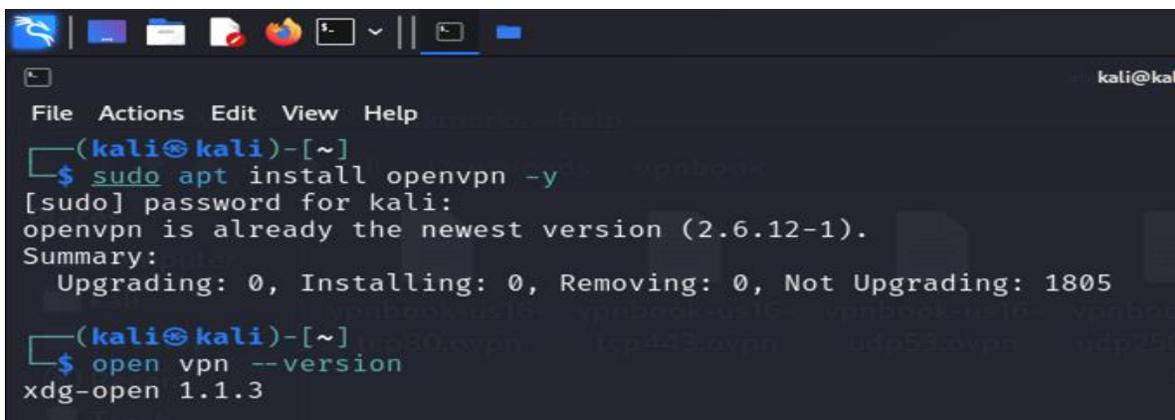


5.2. Instalación de OpenVPN en Kali Linux

4. Primero actualizamos los repositorios de nuestra máquina:

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ sudo apt update && sudo apt upgrade -y  
[sudo] password for kali:  
Get:1 https://mirror.cedia.org.ec/kali kali-rolling InRelease [41.5 kB]  
Get:2 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 Packages [20.3 MB]  
Get:3 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 Contents (deb) [49.4 MB]  
Get:4 https://mirror.cedia.org.ec/kali kali-rolling/contrib amd64 Packages [112 kB]  
Get:5 https://mirror.cedia.org.ec/kali kali-rolling/contrib amd64 Contents (deb) [274 kB]  
Get:6 https://mirror.cedia.org.ec/kali kali-rolling/non-free amd64 Packages [197 kB]  
Get:7 https://mirror.cedia.org.ec/kali kali-rolling/non-free amd64 Contents (deb) [877 kB]  
Get:8 https://mirror.cedia.org.ec/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]  
Get:9 https://mirror.cedia.org.ec/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.1 kB]  
Fetched 71.2 MB in 45s (1,589 kB/s)  
1805 packages can be upgraded. Run 'apt list --upgradable' to see them.  
The following packages were automatically installed and are no longer required:  
 fonts-liberation2          libfreerdp2-2t64          libgtk2.0-bin            libplist3                python3-hatch-vc  
 freerdp2-x11               libgail-common           libgtk2.0-common        libpostproc57           python3-hatchling  
 hydra-gtk                  libgail18t64             libibverbs1             librados2                 python3-pathspe  
 python3-hatchling
```

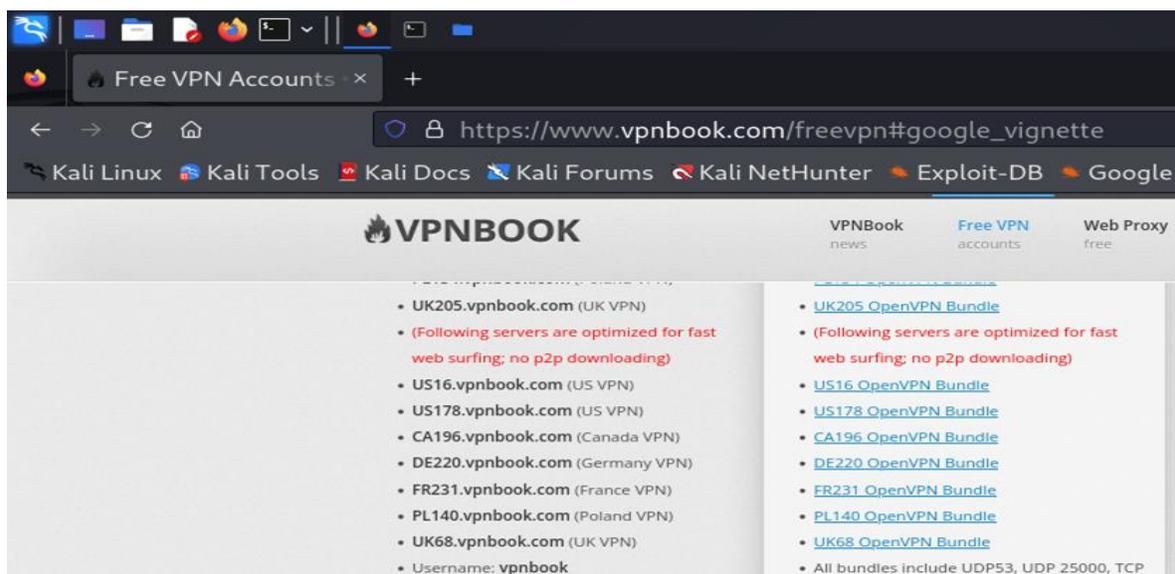
5. Ahora vamos a instalar OpenVPN, (en este caso ya esta instalado) y verificamos la versión.



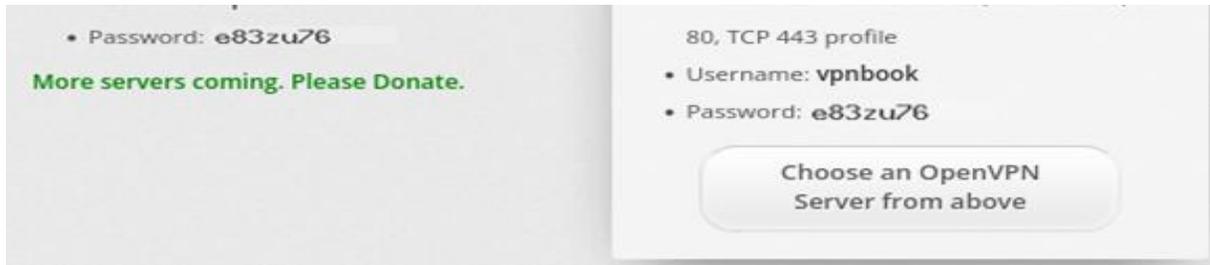
```
(kali@kali)-[~]
└─$ sudo apt install openvpn -y
[sudo] password for kali:
openvpn is already the newest version (2.6.12-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1805

(kali@kali)-[~]
└─$ open vpn --version
xdg-open 1.1.3
```

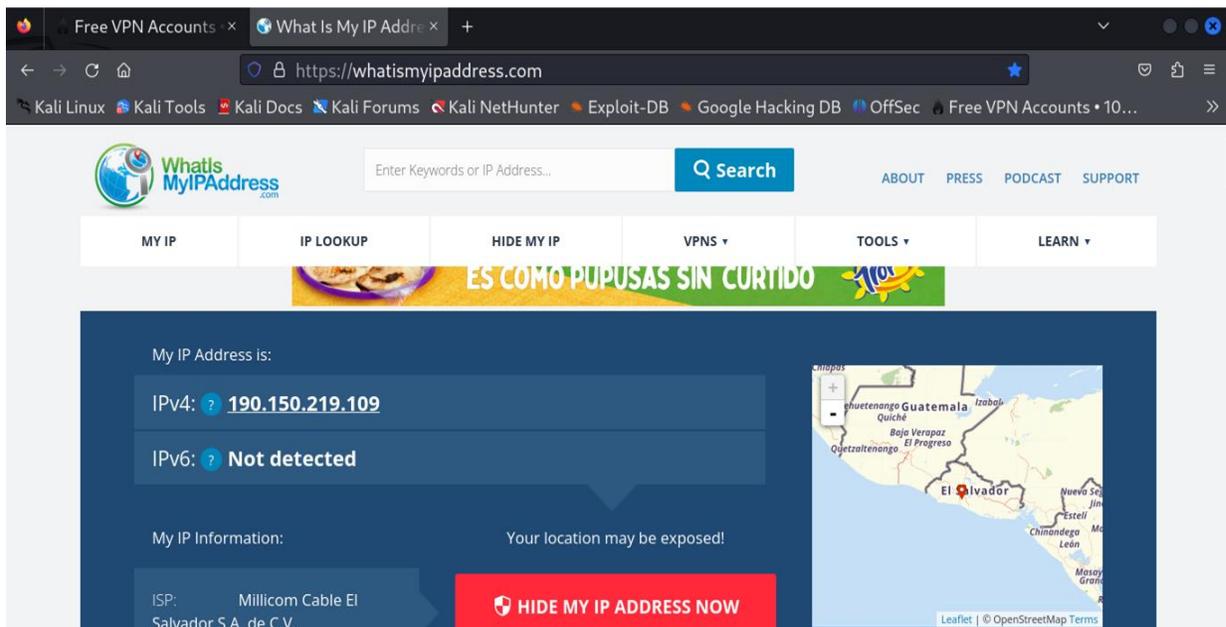
6. Descargamos los archivos de configuración de VPNBook:
7. Abrimos el navegador y nos dirigimos al sitio oficial de VPNBook:
8. En el apartado de FreeVPN, ahí descargaremos el archivo que deseemos.



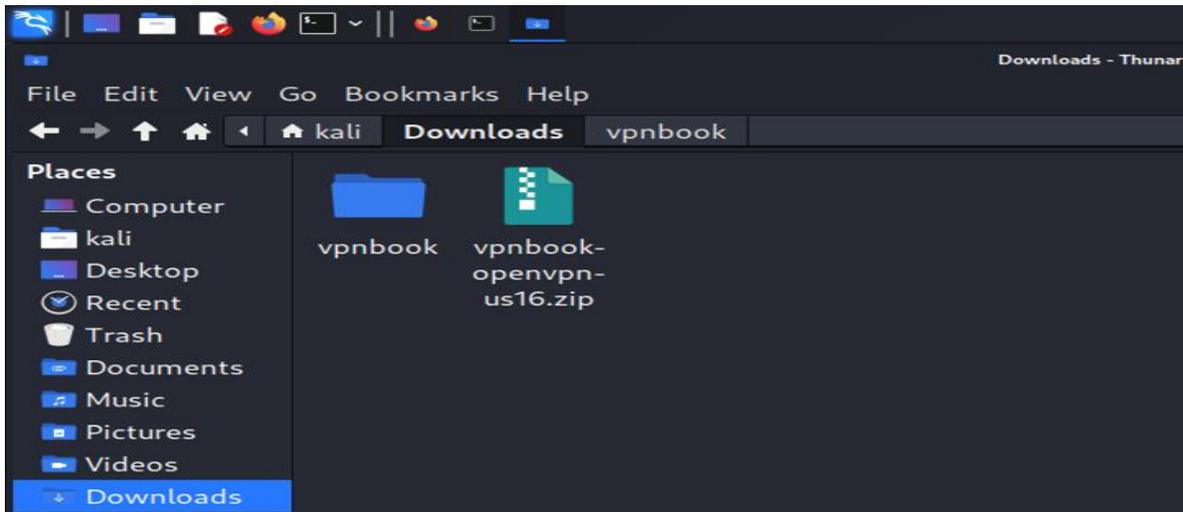
9. El sitio nos proporcionará un usuario y contraseña que lo ingresaremos más adelante al ejecutar el archivo.



10. Antes de iniciar con lo importante, buscaremos una pagina para saber nuestra IP actual



11. Cuando lo hayamos descargado vamos a extraer, una vez descomprimido nos dejará una carpeta con unos archivos de configuración para ejecutar.



12. En la terminal vamos a ir al directorio que extrajimos, luego y ahora con “sudo openvpn -agregar el nombre del archivo -” y ejecutamos.

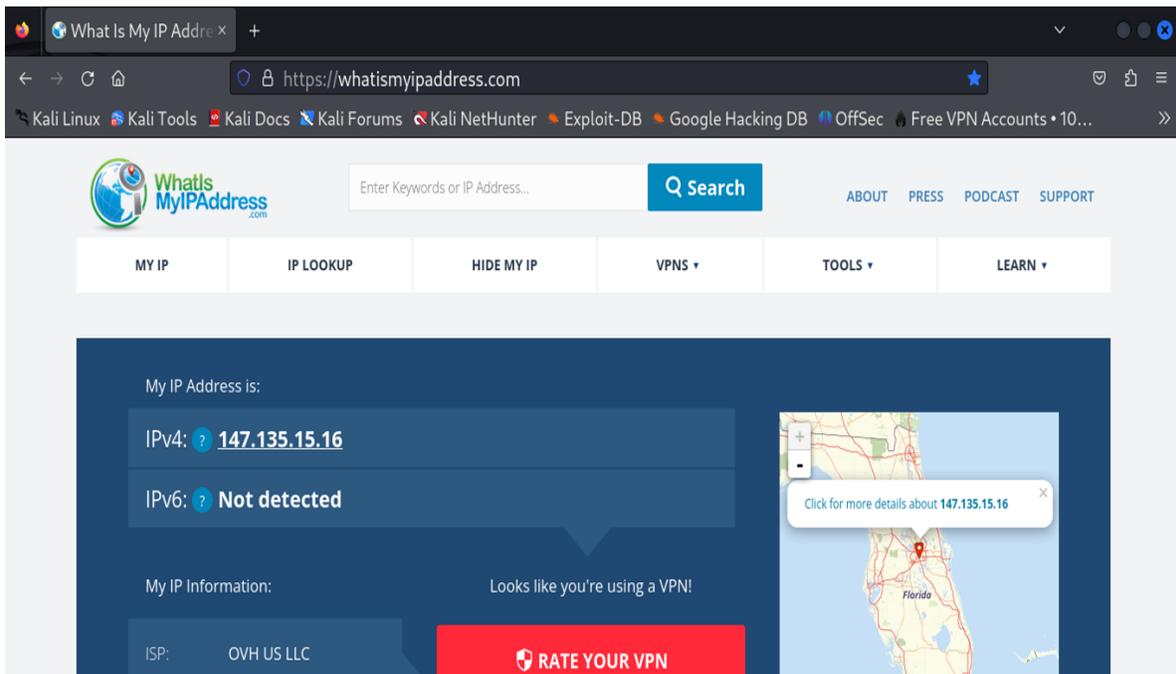
```
(kali@kali) [~]
└─$ cd Downloads/vpnbook

(kali@kali) - [~/Downloads/vpnbook]
└─$ sudo openvpn vpnbook-us16-udp25000.ovpn
[sudo] password for kali:
```

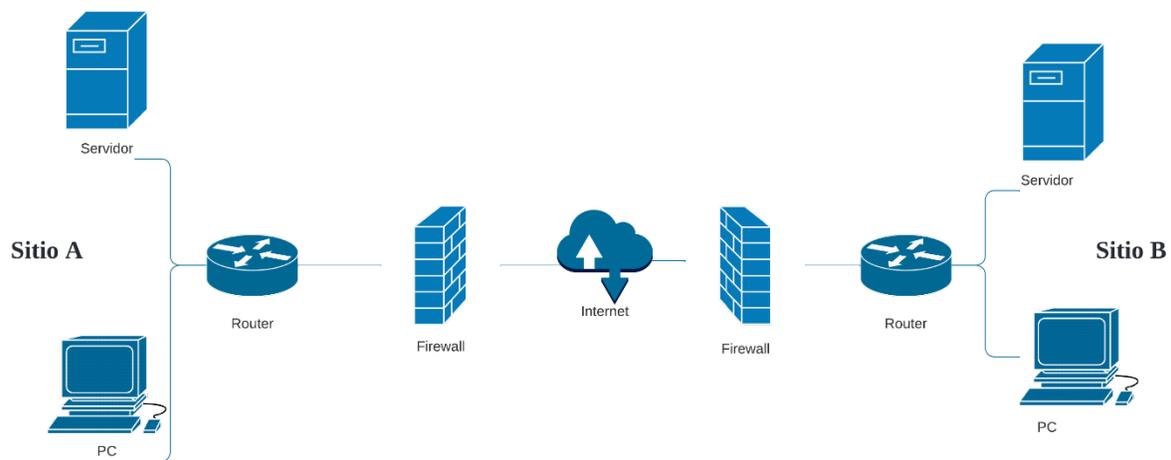
13. (Nos pedirá el usuario y contraseña anterior)

```
Enter Auth Username: vpnbook
Enter Auth Password: .....
```

14. Volvemos al navegador para verificar si nuestra dirección IP ha sido cambiada.



6. FUNCIONAMIENTO DE LA VPN



7. DECISIONES DE DISEÑO Y JUSTIFICACIONES

Para el proyecto, se optó por utilizar VirtualBox como entorno de virtualización, junto con Kali Linux como sistema operativo para el servidor VPN. VirtualBox se seleccionó por su capacidad de crear un entorno controlado y fácilmente replicable, evitando la necesidad de hardware físico adicional. Kali Linux, conocido por su robustez en herramientas de red y seguridad, resultó ideal para instalar y configurar OpenVPN, permitiendo manejar configuraciones avanzadas necesarias para el proyecto.

La red interna (LAN) fue diseñada utilizando el rango de direcciones IP 192.168.1.0/24, donde el servidor VPN tiene una IP estática asignada (192.168.1.1). Esta decisión garantiza una comunicación fluida y consistente entre los dispositivos internos, simplificando la administración de la red. Usar un rango de direcciones privadas evita conflictos y asegura que la red interna esté aislada del acceso externo no autorizado.

OpenVPN fue elegido como protocolo VPN debido a su solidez, seguridad y flexibilidad. Este protocolo, que emplea cifrado AES-256 y certificados SSL/TLS, garantiza la confidencialidad e integridad de los datos transmitidos. Además, su compatibilidad con múltiples plataformas permite que los usuarios se conecten desde distintos dispositivos (computadoras, teléfonos, etc.), lo que lo hace ideal para un entorno diverso como el planteado en este proyecto.

Manual de Usuario



OpenVpn y Kali Linux

INTRODUCCIÓN

Este manual de usuario ha sido diseñado para proporcionar una guía completa y práctica para el uso del servidor OpenVPN implementado en este proyecto. OpenVPN es una herramienta poderosa y segura que permite a los usuarios conectarse a una red privada virtual (VPN) desde cualquier lugar, garantizando la privacidad, la seguridad de los datos y el acceso remoto a los recursos internos de la red.

En las siguientes secciones, encontrará instrucciones claras para instalar y configurar el cliente OpenVPN en diferentes dispositivos, establecer una conexión segura con el servidor, y resolver problemas comunes que puedan surgir. Este documento está dirigido tanto a usuarios con experiencia técnica como a aquellos con conocimientos básicos, con el fin de garantizar una experiencia de usuario fluida y sencilla.

El objetivo principal de este manual es facilitar el uso del sistema VPN, asegurando que los usuarios puedan beneficiarse de sus funcionalidades de forma eficiente. Además, se destacan las buenas prácticas de seguridad para proteger la información y maximizar el rendimiento del sistema. Con esta guía, estará listo para aprovechar al máximo la infraestructura de red segura y funcional creada con OpenVPN.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Brindar a los usuarios una guía clara, práctica y detallada para la configuración, conexión y uso del servidor OpenVPN, asegurando un acceso seguro y funcional a la red virtual implementada.

1.2. OBJETIVOS ESPECÍFICOS

- Explicar de manera detallada y sencilla el proceso de instalación y configuración del cliente OpenVPN en distintos sistemas operativos.
- Garantizar que los usuarios comprendan las medidas de seguridad necesarias para proteger sus datos mientras usan la VPN
- Proporcionar instrucciones precisas para la conexión al servidor OpenVPN.

2. JUSTIFICACIÓN

La creación de este manual de usuario es fundamental para garantizar que todos los usuarios, independientemente de su nivel de conocimiento técnico, puedan utilizar de manera eficaz y segura el sistema VPN implementado en el proyecto. La implementación de una VPN proporciona un acceso seguro y privado a la red interna, pero para que los usuarios puedan aprovechar todas las ventajas de esta tecnología, es necesario ofrecer una guía clara y accesible que explique cada paso del proceso.

La justificación de este manual radica en la necesidad de empoderar a los usuarios para que puedan conectarse de manera sencilla y confiable a la red virtual privada, mientras mantienen la seguridad y la protección de sus datos. Sin un manual adecuado, los usuarios podrían enfrentar dificultades para instalar, configurar o mantener la conexión VPN, lo que podría generar frustración o incluso comprometer la seguridad de la red. Al proporcionar instrucciones detalladas y fáciles de seguir, el manual elimina estos obstáculos, haciendo el sistema más accesible para todos.

Además, dado que el uso de la VPN implica el manejo de información sensible y la configuración de dispositivos en entornos diversos, el manual también desempeña un papel crucial en la educación sobre buenas prácticas de seguridad. Este enfoque no solo mejora la experiencia del usuario, sino que también contribuye a la protección de la infraestructura de red al asegurar que los usuarios comprendan cómo conectarse de manera segura y evitar errores comunes.

3. QUE ES VPN Y KALI LINUX

Una VPN (Virtual Private Network, o Red Privada Virtual) es una tecnología que permite establecer una conexión segura y privada a través de una red pública, como Internet. Su principal objetivo es proteger la privacidad y la seguridad de los datos que se transmiten entre el usuario y un servidor, enmascarando la dirección IP del usuario y cifrando la información para evitar que terceros puedan interceptarla o acceder a ella.

Cuando un usuario se conecta a una VPN, su tráfico de Internet es redirigido a través de un túnel seguro hacia un servidor VPN, lo que hace que el tráfico sea más difícil de rastrear. Esto asegura la confidencialidad de la información y permite acceder a recursos internos de una red local de manera remota. Las VPNs son comúnmente utilizadas para acceder de forma segura a redes corporativas desde ubicaciones externas, proteger la información en redes Wi-Fi públicas y mantener el anonimato en línea.

Las VPNs se utilizan en una variedad de escenarios, como:

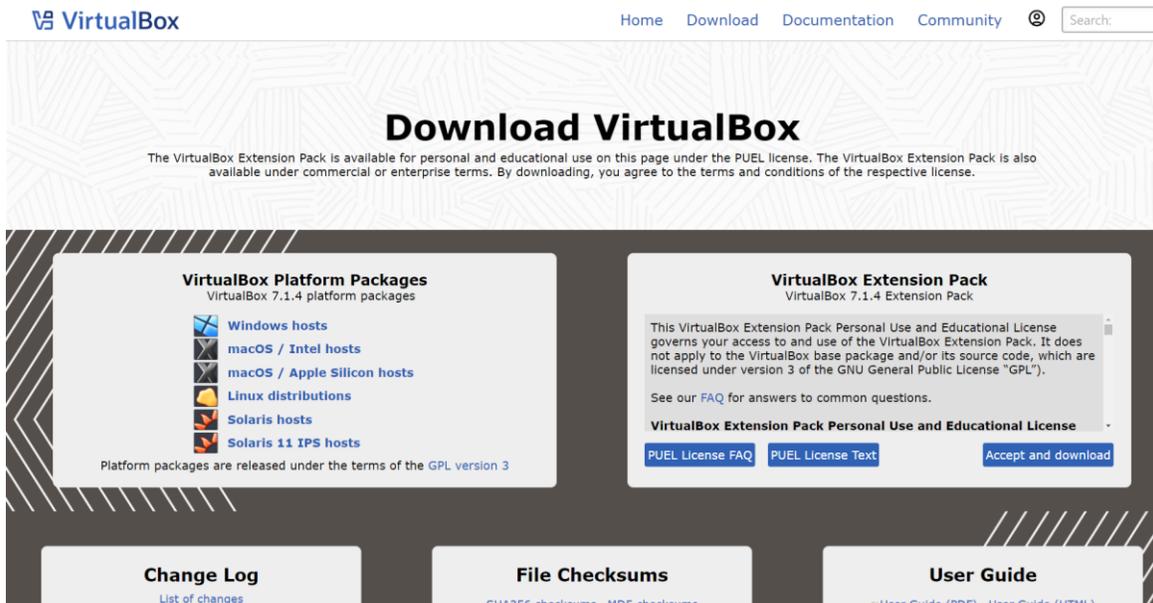
- Acceso remoto a redes privadas desde cualquier lugar del mundo.
- Protección de la privacidad al navegar por Internet.
- Acceso a contenido restringido o censurado geográficamente.

Kali Linux es una distribución de Linux basada en Debian, diseñada principalmente para la realización de pruebas de penetración (pentesting) y auditorías de seguridad. Es una herramienta muy utilizada por profesionales de la seguridad informática debido a su amplia colección de herramientas especializadas en la evaluación de vulnerabilidades, análisis de redes, y explotación de sistemas.

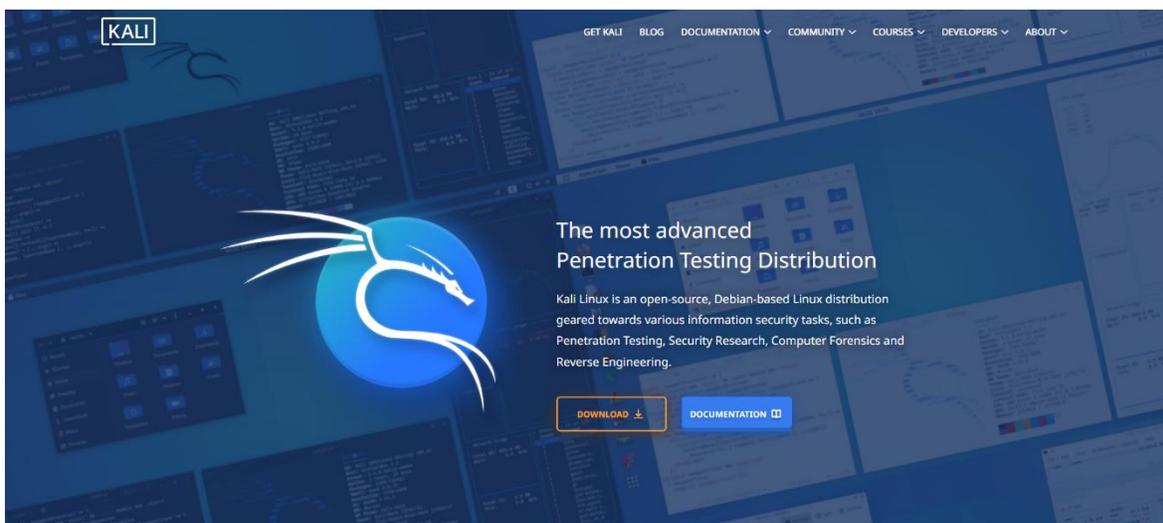
4. CONFIGURACION Y EJECUCION TECNICA

4.1. Instalacion de VirtualBox y Kali Linux

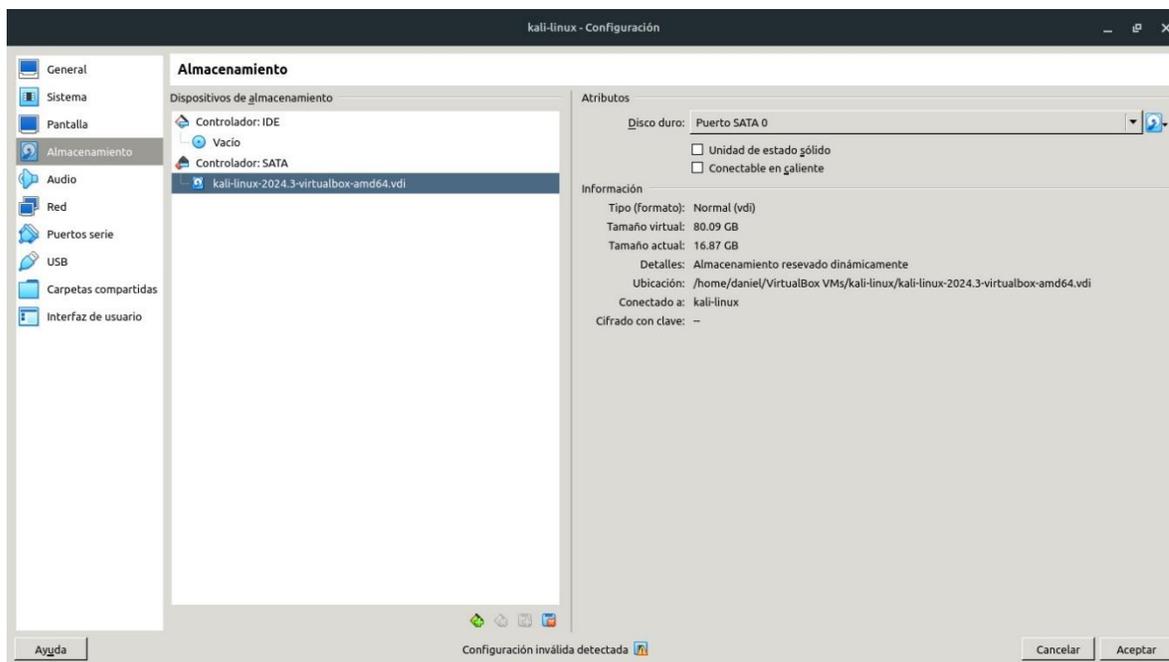
15. Descargamos VirtualBox desde su pagina oficial



16. Descargamos la ISO de Kali Linux desde su pagina oficial



17. Configuramos nuestra maquina virtual con las siguientes características

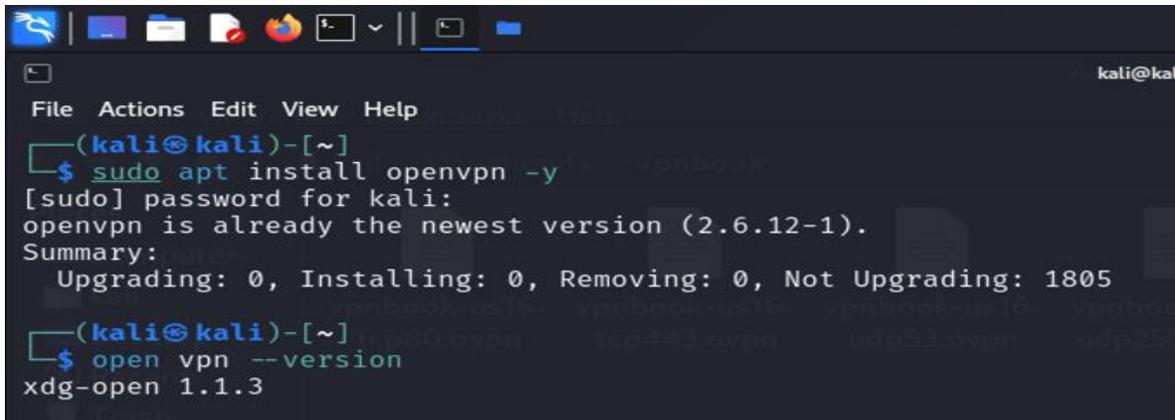


4.2. Instalación de OpenVPN en Kali Linux

18. Primero actualizamos los repositorios de nuestra máquina:

```
kali@kali: ~  
File Actions Edit View Help  
└─(kali@kali)-[~]  
└─$ sudo apt update 66 sudo apt upgrade -y  
[sudo] password for kali:  
Get:1 https://mirror.cedia.org.ec/kali kali-rolling InRelease [41.5 kB]  
Get:2 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 Packages [20.3 MB]  
Get:3 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 Contents (deb) [49.4 MB]  
Get:4 https://mirror.cedia.org.ec/kali kali-rolling/contrib amd64 Packages [112 kB]  
Get:5 https://mirror.cedia.org.ec/kali kali-rolling/contrib amd64 Contents (deb) [274 kB]  
Get:6 https://mirror.cedia.org.ec/kali kali-rolling/non-free amd64 Packages [197 kB]  
Get:7 https://mirror.cedia.org.ec/kali kali-rolling/non-free amd64 Contents (deb) [877 kB]  
Get:8 https://mirror.cedia.org.ec/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]  
Get:9 https://mirror.cedia.org.ec/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.1 kB]  
Fetched 71.2 MB in 45s (1,589 kB/s)  
1805 packages can be upgraded. Run 'apt list --upgradable' to see them.  
The following packages were automatically installed and are no longer required:  
 fonts-liberation2          libfreerdp2-2t64          libgtk2.0-bin             libplist3                 python3-hatch-vcs  
 freerdp2-x11               libgail-common            libgtk2.0-common         libpostproc57            python3-hatchling  
 hydra-gtk                  libgail18t64              libibverbs1               librados2                 python3-pathspect
```

19. Ahora vamos a instalar OpenVPN, (en este caso ya esta instalado) y verificamos la versión.



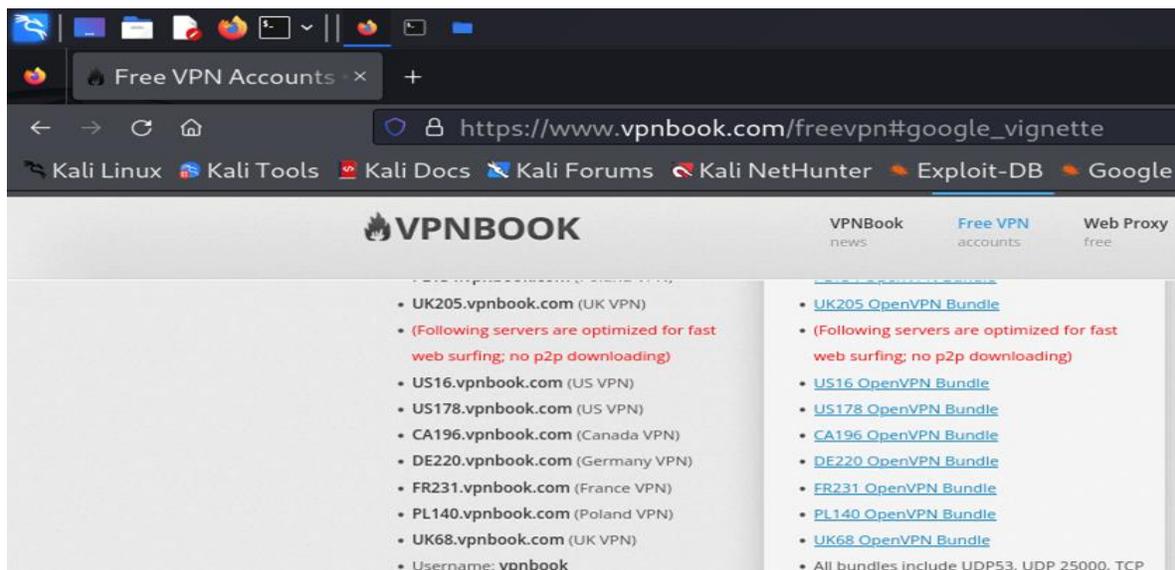
```
(kali@kali)-[~]
└─$ sudo apt install openvpn -y
[sudo] password for kali:
openvpn is already the newest version (2.6.12-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1805

(kali@kali)-[~]
└─$ open vpn --version
xdg-open 1.1.3
```

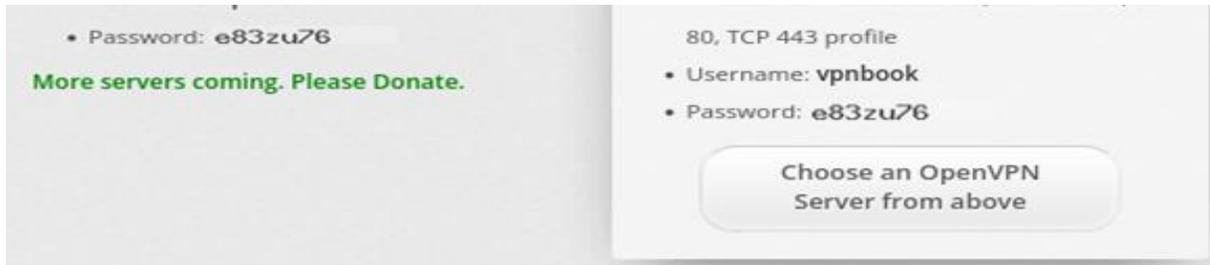
20. Descargamos los archivos de configuración de VPNBook:

21. Abrimos el navegador y nos dirigimos al sitio oficial de VPNBook:

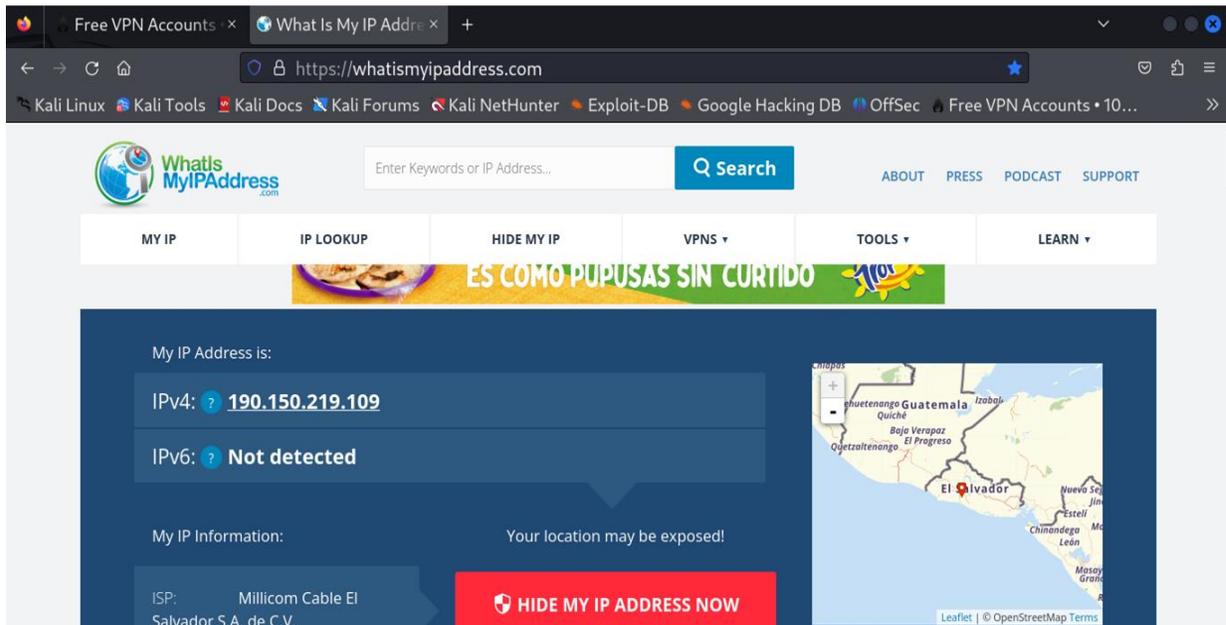
22. En el apartado de FreeVPN, ahí descargaremos el archivo que deseemos.



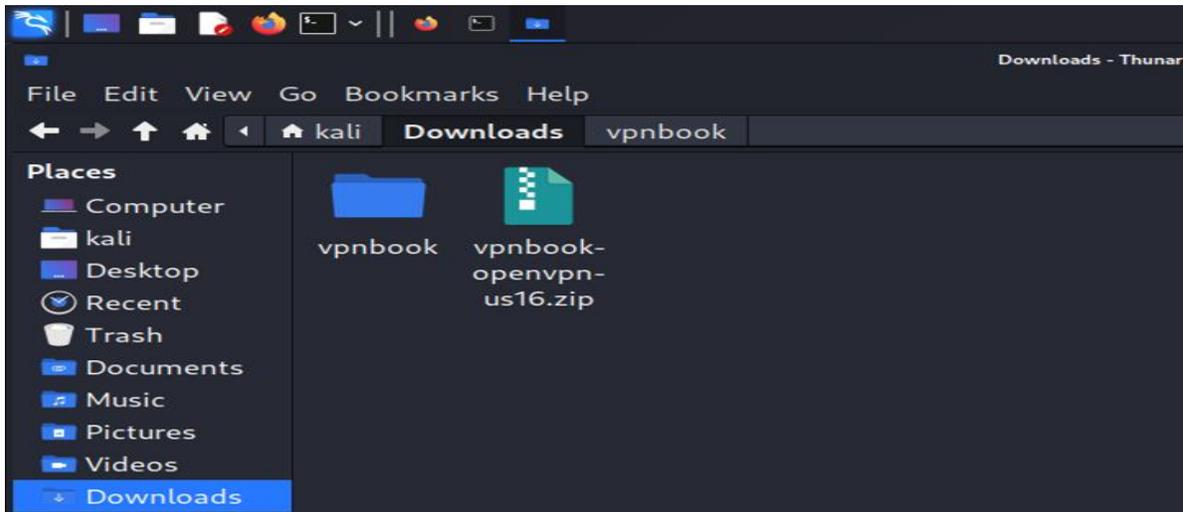
23. El sitio nos proporcionará un usuario y contraseña que lo ingresaremos más adelante al ejecutar el archivo.



24. Antes de iniciar con lo importante, buscaremos una pagina para saber nuestra IP actual



25. Cuando lo hayamos descargado vamos a extraer, una vez descomprimido nos dejará una carpeta con unos archivos de configuración para ejecutar.



26. En la terminal vamos a ir al directorio que extrajimos, luego y ahora con “sudo openvpn -agregar el nombre del archivo -” y ejecutamos.

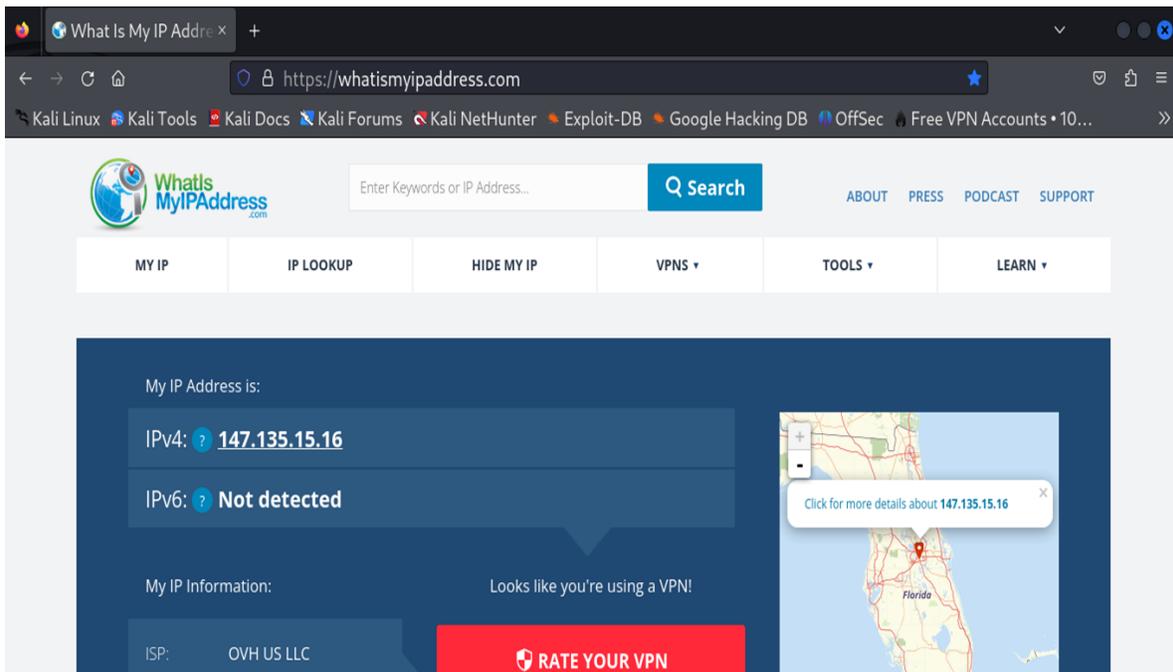
```
(kali@kali) [~]
└─$ cd Downloads/vpnbook

(kali@kali) - [~/Downloads/vpnbook]
└─$ sudo openvpn vpnbook-us16-udp25000.ovpn
[sudo] password for kali:
```

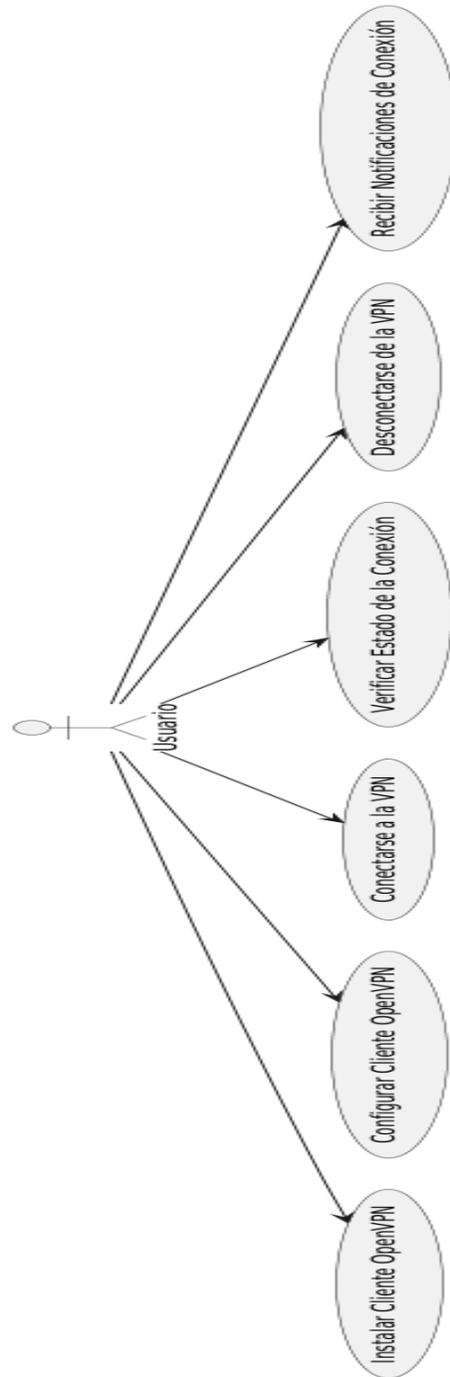
27. (Nos pedirá el usuario y contraseña anterior)

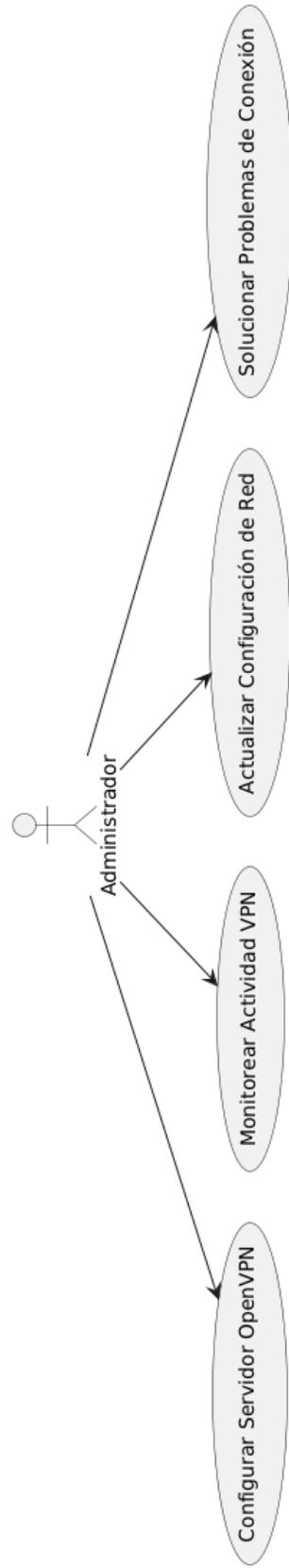
```
Enter Auth Username: vpnbook
Enter Auth Password: .....
```

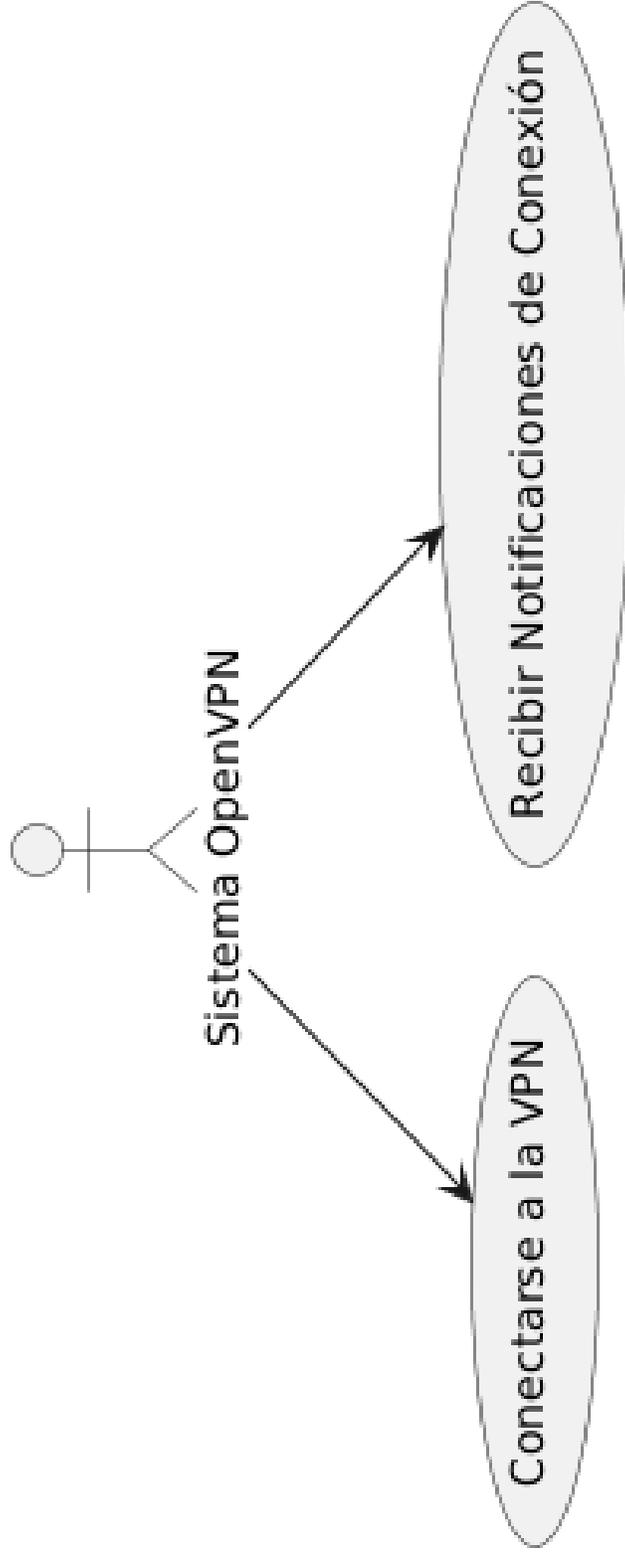
28. Volvemos al navegador para verificar si nuestra dirección IP ha sido cambiada.



5. DIAGRAMAS







6. ALCANCES

El alcance de este proyecto consiste en la implementación de una Red Privada Virtual (VPN) utilizando OpenVPN sobre un servidor Kali Linux, con el objetivo de permitir que los usuarios remotos se conecten de manera segura a una red interna. Se llevará a cabo la configuración de OpenVPN en Kali Linux, asegurando que el servidor actúe como un punto de acceso seguro mediante un túnel cifrado para la transmisión de datos, lo que garantiza la protección de la información y la privacidad de las comunicaciones.

Además, se proporcionará acceso remoto seguro a los usuarios autorizados, permitiendo que puedan acceder a los recursos internos de la red como si estuvieran físicamente conectados, pero con la seguridad que ofrece la tecnología VPN. El proyecto también incluye la configuración del cliente OpenVPN para distintos dispositivos (PC, teléfonos, tabletas), lo que permitirá a los usuarios conectarse de manera flexible y desde diferentes plataformas.

El proyecto también está diseñado para ser escalable, lo que permitirá añadir más usuarios o dispositivos a la red en el futuro, sin comprometer la seguridad ni el rendimiento del sistema. Se gestionarán los permisos de acceso para asegurar que solo los usuarios autorizados puedan conectarse a la red interna a través de la VPN, protegiendo así los recursos y la infraestructura. Sin embargo, la implementación de este proyecto estará limitada a un entorno virtualizado y a un número específico de usuarios, lo que puede generar diferencias respecto a una configuración en hardware físico real.

7. CONCLUSION

En conclusión, la implementación de una Red Privada Virtual (VPN) utilizando OpenVPN sobre un servidor Kali Linux ha demostrado ser una solución eficaz y segura para permitir el acceso remoto a una red interna, protegiendo la confidencialidad y la integridad de los datos transmitidos. A través de la configuración adecuada de la VPN, se garantiza que los usuarios autorizados puedan acceder a los recursos de la red de manera segura, independientemente de su ubicación, manteniendo la privacidad de sus comunicaciones.

El proyecto ha cumplido con los objetivos propuestos, proporcionando una infraestructura escalable y segura, con medidas de protección adecuadas para asegurar la autenticación, el cifrado y el control de acceso. Además, el manual de usuario desarrollado facilita la implementación y el uso del sistema, permitiendo que tanto usuarios técnicos como no técnicos puedan aprovechar las ventajas de la VPN sin dificultades.