

HACKING ÉTICO:

Sistemas Operativos en Seguridad Informática (Kali Linux)

Luis Felipe Narváez Gómez. E-mail: luis.narvaez@usantoto.edu.co. Cod: 2312660. Facultad de Ingeniería de Sistemas.

KALI LINUX

Kali fue lanzado por primera vez el 13 de marzo de 2013 bajo el nombre oficial de Back Track, desarrollado para la empresa de seguridad OFFENSIVE SECURITY, siendo una de las distribuciones forenses centradas en la seguridad basada en la rama de pruebas de Debian. El diseño de Kali esta orientado a la penetración, la recuperación de datos y la detección de amenazas.

Kali es una de las distribuciones mas famosas para Hacking, muy utilizado en el tema de seguridad informática y hacking ético debido a su amplio catálogo de herramientas. Posee un gran recorrido y soporte en su plataforma. Las herramientas que posee Kali van desde llevar a cabo múltiples pruebas, recopilar información, escanear redes, etc. Kali Linux es de carácter gratuito y su fin es siempre serlo, con el fin de brindar al usuario un amplio catalogo de utilidades que van de las 600 y contando características incorporadas dentro de la instalación de la propia distribución.

Actualmente la piratería es un tema famoso en la cultura popular, esto gracias a la difusión del trabajo de Hacking por la televisión, el cine y series de seguridad informática.

Kali comparte similitud con otras distribuciones de Linux, repleta de herramientas relacionadas con la seguridad y dirigida a expertos en seguridad informática y de redes, su diferencia esta en su enfoque de diseño y programación, pues es Kali directamente programado en temas orientados en seguridad y análisis forense.

Como Sabemos una distribución de Linux no es mas que un paquete que contiene el kernel de Linux, un conjunto de utilidades, aplicaciones principales y algunas configuraciones predeterminadas; por lo tanto Kali no ofrece algo único en este sentido, pues la mayoría de estas herramientas pueden instalarse en cualquier distribución de Linux; pero como ya habíamos estipulado, su diferencia esta en el diseño específico, pues cumple con los requisitos de eficiencia óptimos en los temas de penetración profesional y auditorias de seguridad.

*"Nuestra distribución de pruebas de penetración más avanzada que jamás haya existido". –
Desarrolladores de Kali Linux.*

Kali está dirigido a un subconjunto particular de usuarios de Linux, Pentesters, piratas informáticos, etc; por lo que no es un entorno en el cual se esperaría encontrar a diseñadores de software, diseño web, programación de juegos, Oficinistas, etc.

Antes de empezar con una prueba básica de Hacking Etico, debemos asegurarnos que Kali Linuz se encuentra en optimas condiciones para trabajar, para esto debemos configurar el repositorio y actualizar dependencias.

REPOSITORIO PRINCIPAL Y ACTUALIZACIONES

PASO 1: Configurar el repositorio.

Es de suma importancia configurar el repositorio correctamente. El modelo de lanzamiento continuo de Kali Linux tiene como objetivo proporcionar utilidades de seguridad actualizadas a los usuarios que utilizan esta distribución. La parte del repositorio hace referencia a los medios que se están utilizando para la instalación, un problema derivado de las distribuciones recientemente instaladas.

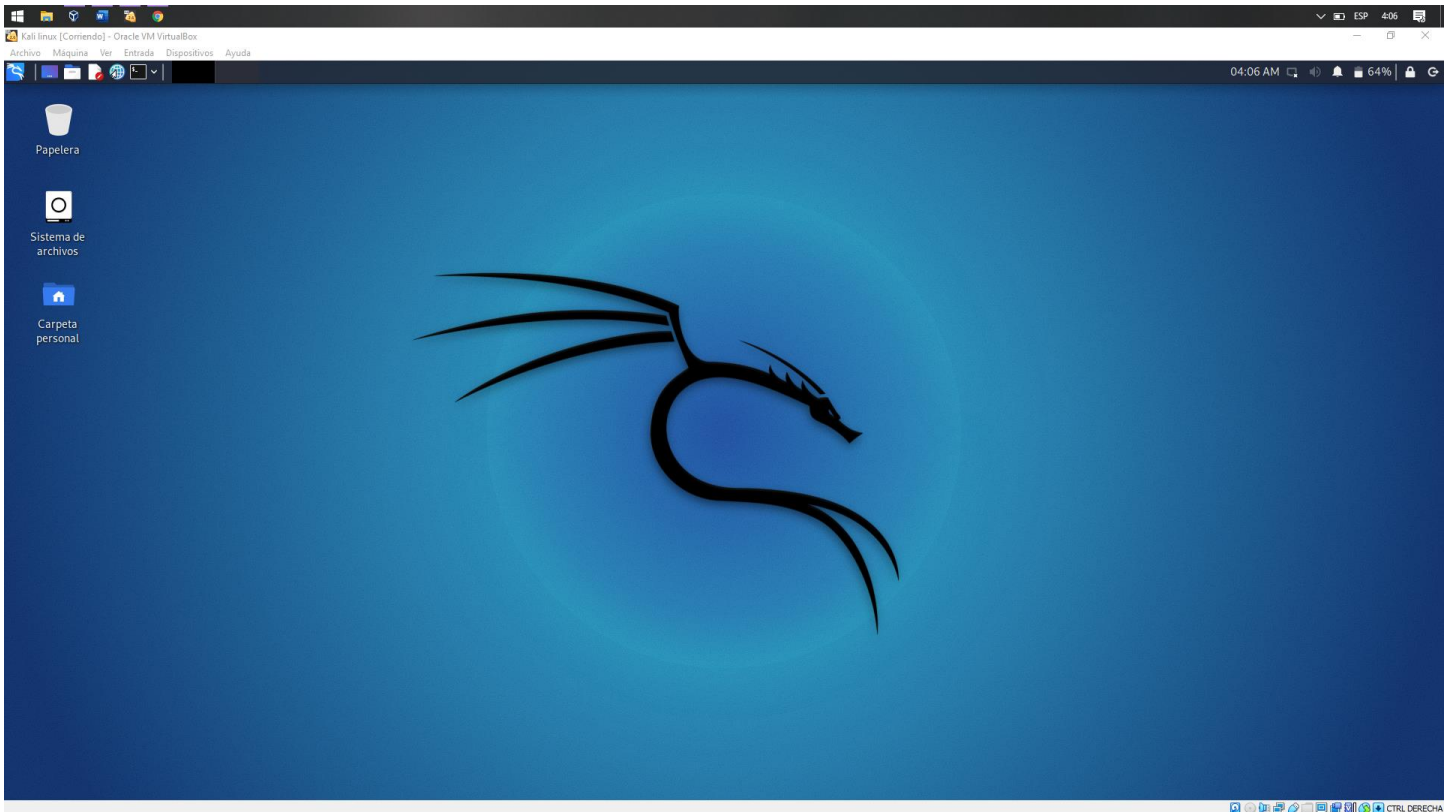
Para solucionar este problema se debe cambiar el repositorio por defecto al repositorio oficial de Kali Linux. El archivo que vamos a necesitar se encuentra en la siguiente ruta:

/etc/apt/sources.list

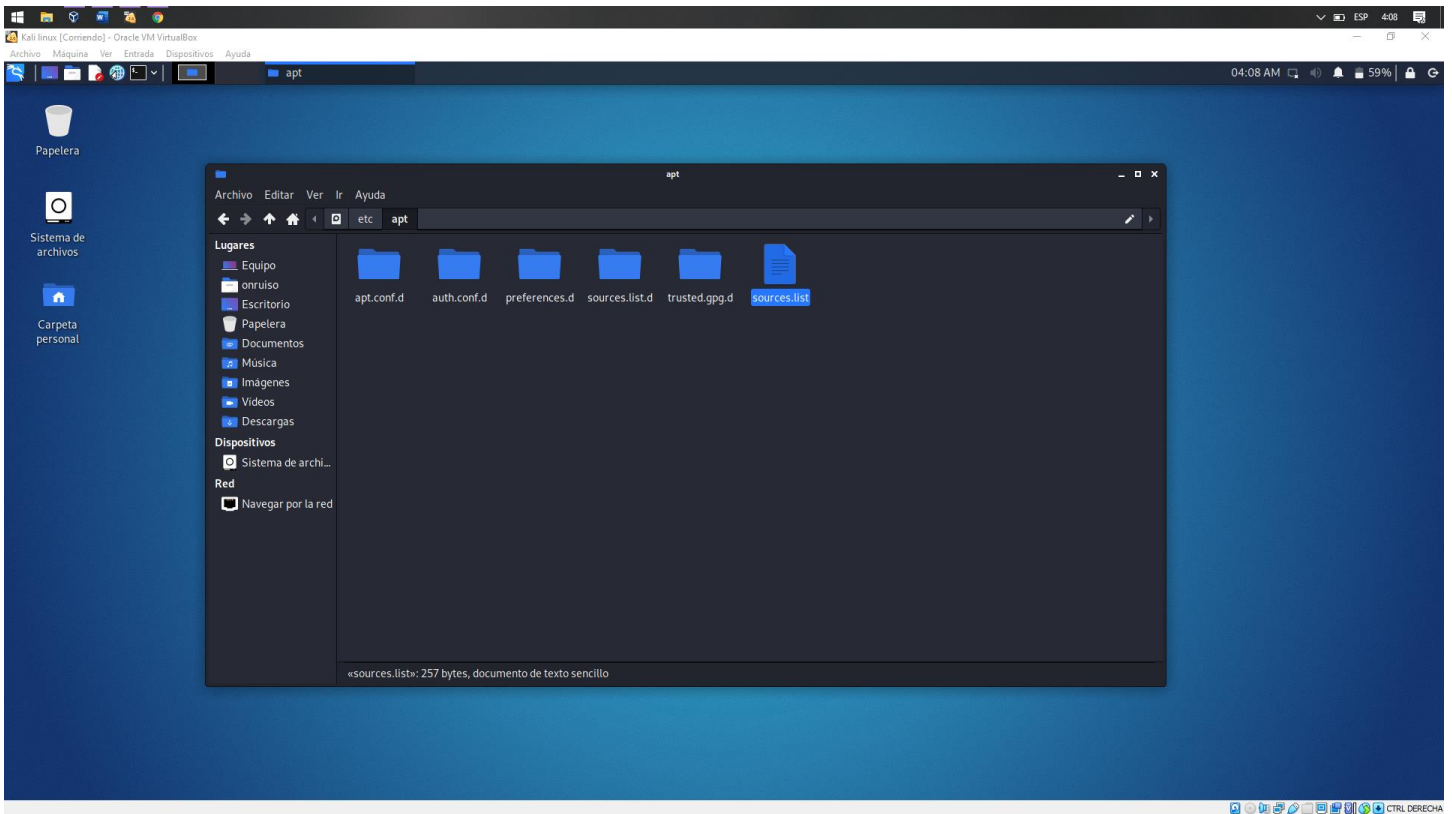
Debemos abrir el archivo con un editor de texto plano como leafpad y reemplazar el repositorio predeterminado a este repositorio oficial de Kali Linux, Kali Rolling:

```
deb http://http.kali.org/kali kali-rolling main contrib non-free
# For source package access, uncomment the following line
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free
```

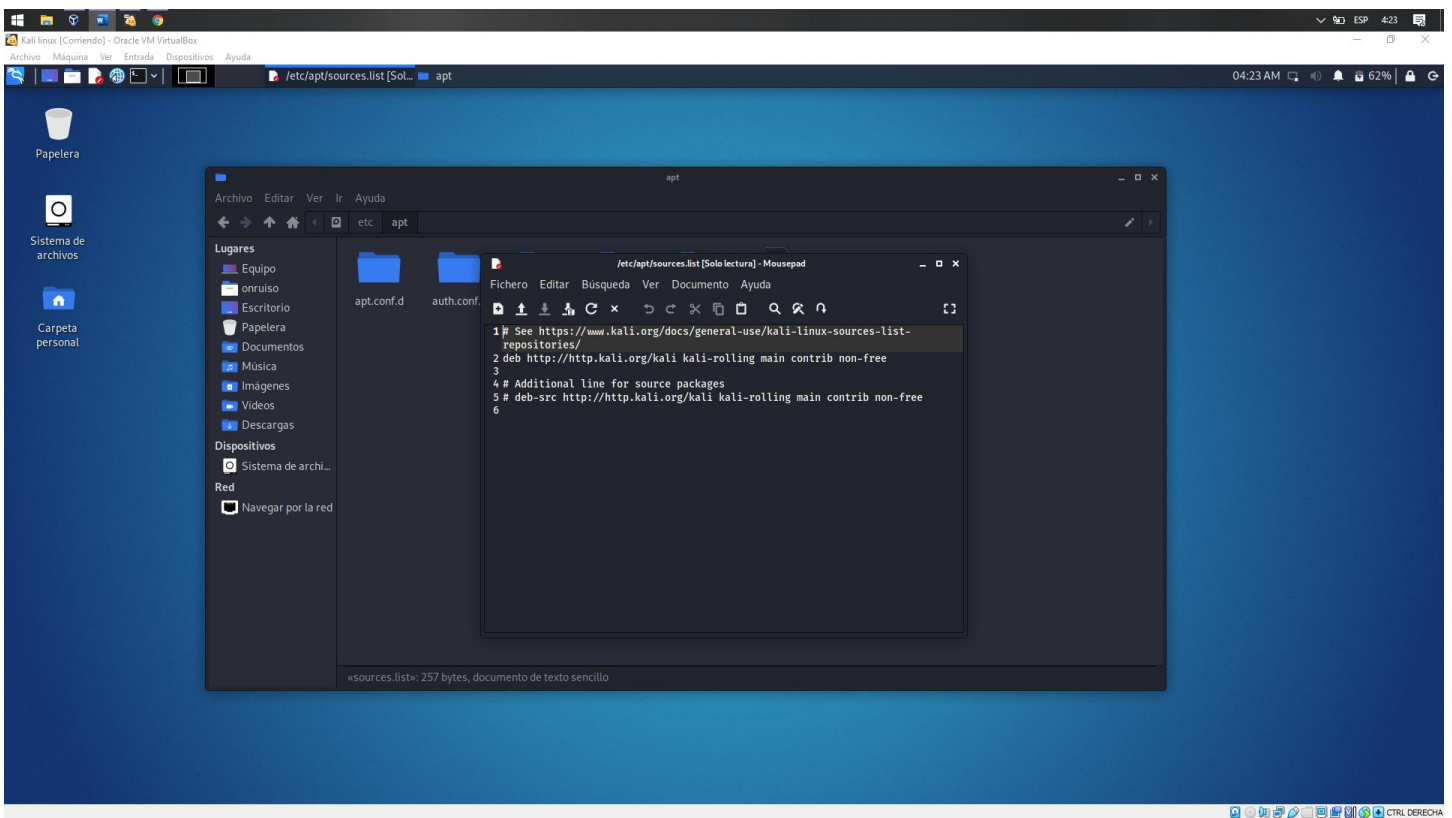
Visto de manera visual seria, abrir Kali Linux.



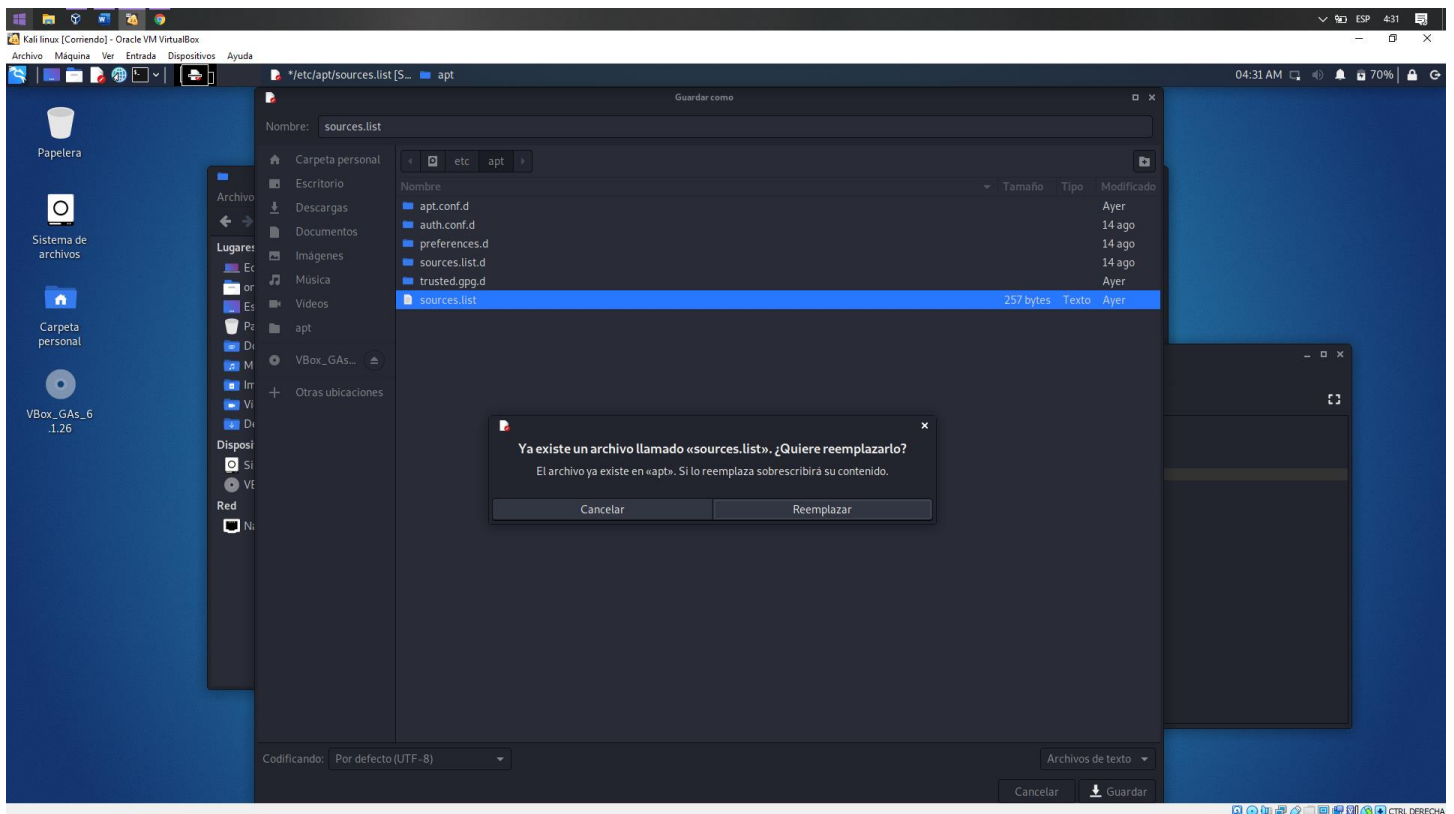
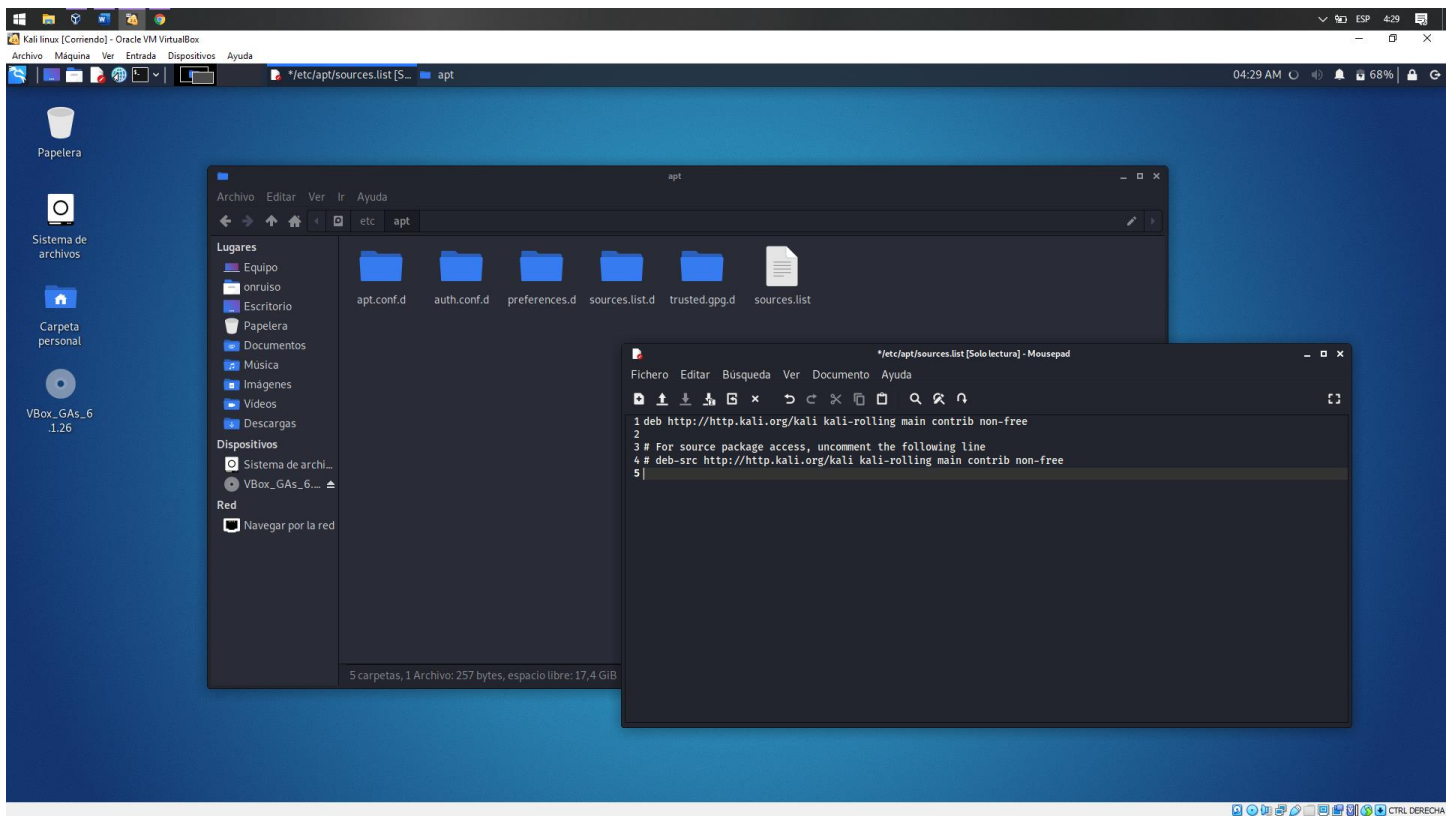
Buscar en la ruta que se nos ha proporcionado el archivo “sources.list”:



Una vez encontrado lo abrimos con el editor de texto plano, puesto que no se tienen conexión a una red inalámbrica por ahora, podemos abrir el archivo con MOUSEPAD.



Cambiamos el repositorio.



En caso de que por problemas de permisos no deje sobre escribir los archivos podemos ingresar por consola escribiendo el comando “`nano /etc/apt/sources.list`”. Esto claro debe hacerse como usuario root.

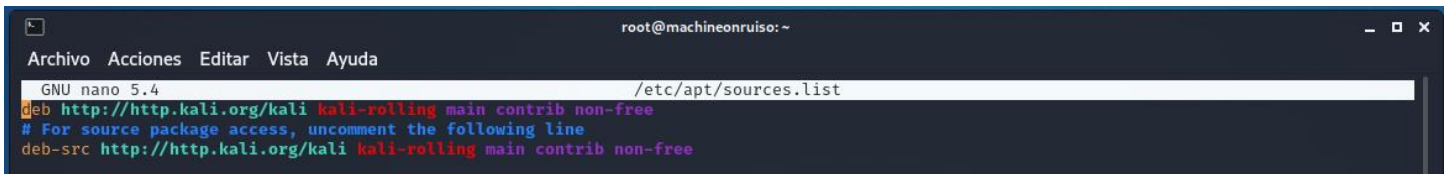


```
root@machineonruiso: ~  
Archivo Acciones Editar Vista Ayuda  
GNU nano 5.4 /etc/apt/sources.list  
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/  
deb http://http.kali.org/kali kali-rolling main contrib non-free  
  
# Additional line for source packages  
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free  
  
Dpkg sources:  
# deb http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb-src http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb http://ftp.ports.debian.org/debian-ports/ ports main  
# deb-src http://ftp.ports.debian.org/debian-ports/ ports main  
  
Dpkg sources:  
# deb http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb-src http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb http://ftp.ports.debian.org/debian-ports/ ports main  
# deb-src http://ftp.ports.debian.org/debian-ports/ ports main  
  
root@machineonruiso: ~  
Ayuda Guardar Buscar Cortar 5 líneas leídas Ejecutar Ubicación Deshacer Poner marca A llave  
Salir Leer fich. Reemplazar Pegar Justificar Ir a línea Rehacer Copiar Buscar atrás
```

```
root@machineonruiso: ~  
Archivo Acciones Editar Vista Ayuda  
GNU nano 5.4 /etc/apt/sources.list *  
deb http://http.kali.org/kali kali-rolling main contrib non-free  
# For source package access, uncomment the following line  
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free  
  
Dpkg sources:  
# deb http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb-src http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb http://ftp.ports.debian.org/debian-ports/ ports main  
# deb-src http://ftp.ports.debian.org/debian-ports/ ports main  
  
Dpkg sources:  
# deb http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb-src http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb http://ftp.ports.debian.org/debian-ports/ ports main  
# deb-src http://ftp.ports.debian.org/debian-ports/ ports main  
  
root@machineonruiso: ~  
Ayuda Guardar Buscar Cortar Ejecutar Ubicación Deshacer Poner marca A llave  
Salir Leer fich. Reemplazar Pegar Justificar Ir a línea Rehacer Copiar Buscar atrás
```

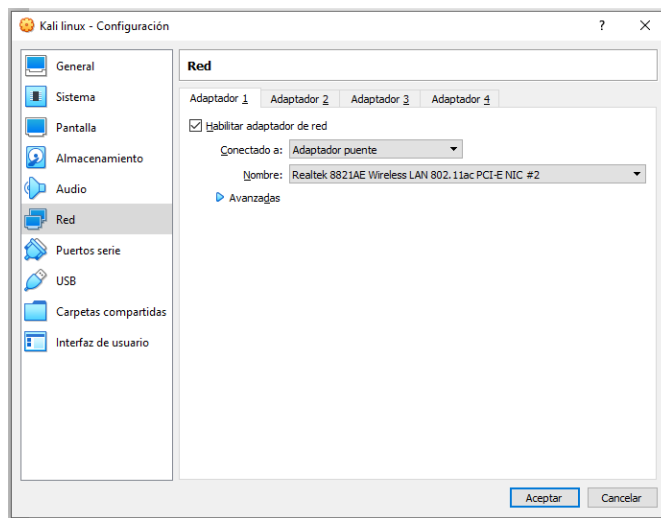
“CTRL + O” = Guardar cambios

También podemos probar con:



```
root@machineonruiso: ~  
Archivo Acciones Editar Vista Ayuda  
GNU nano 5.4 /etc/apt/sources.list  
deb http://http.kali.org/kali kali-rolling main contrib non-free  
# For source package access, uncomment the following line  
deb-src http://http.kali.org/kali kali-rolling main contrib non-free  
  
Dpkg sources:  
# deb http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb-src http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb http://ftp.ports.debian.org/debian-ports/ ports main  
# deb-src http://ftp.ports.debian.org/debian-ports/ ports main  
  
Dpkg sources:  
# deb http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb-src http://ftp.debian.org/debian/ debian main contrib non-free non-free-firmware  
# deb http://ftp.ports.debian.org/debian-ports/ ports main  
# deb-src http://ftp.ports.debian.org/debian-ports/ ports main  
  
root@machineonruiso: ~  
Ayuda Guardar Buscar Cortar Ejecutar Ubicación Deshacer Poner marca A llave  
Salir Leer fich. Reemplazar Pegar Justificar Ir a línea Rehacer Copiar Buscar atrás
```

Ahora bien, debemos asegurarnos de que las conexiones de red entre la Máquina anfitrión y la máquina virtual esten dadas, refiriéndose al adaptador de red.



SSID: OnRuisoWlan
 Protocolo: Wi-Fi 4 (802.11n)
 Tipo de seguridad: WPA2-Personal
 Banda de red: 2.4 GHz
 Canal de red: 6
 Velocidad de vínculo (recepción/transmisión): 54/57 (Mbps)
 Dirección IPv6 local de vínculo: fe80::59d3:8066:fdc7:ecf3%3
 Dirección IPv4: 192.168.1.53
 Servidores DNS IPv4: 190.157.8.109
 190.157.8.101
 Fabricante: Realtek Semiconductor Corp.
 Descripción: Realtek 8821AE Wireless LAN
 802.11ac PCI-E NIC #2
 Versión del controlador: 2023.70.306.2018
 Dirección física (MAC): 60-14-B3-C4-F0-8B

Comprobamos que efectivamente la conexión exista a internet, esto comparando las Ip para asegurarnos que tanto la maquina anfitrión como la máquina virtual están en la misma red y algún ping para asegurarnos que haya conexión real a internet.

De la parte de Kali Linux tenemos:

```

root@machineonruiso: ~
Archivo Acciones Editar Vista Ayuda
root@machineonruiso:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.51 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe07:d8f8 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:07:d8:f8 txqueuelen 1000 (Ethernet)
    RX packets 24 bytes 2290 (2.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 3814 (3.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@machineonruiso:~#
  
```

De la Parte de Windows 10 tenemos:

```

C:\Users\ruiiso>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de Ethernet VirtualBox Host-Only Network:

    Sufixo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::b9f6:bce4:48e4:4d8d%12
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de Ethernet Ethernet 2:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Wi-Fi 2:

    Sufixo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::59d3:8066:fdc7:ecf3%3
    Dirección IPv4. . . . . : 192.168.1.53
    Dirección de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.1.254

Adaptador de Ethernet Conexión de red Bluetooth:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

C:\Users\ruiiso>
  
```


De parte de Kali Linux tenemos:

```
(root@machineonruiso)~# ping www.google.com
PING www.google.com (172.217.173.36) 56(84) bytes of data.
64 bytes from bog02s12-in-f4.1e100.net (172.217.173.36): icmp_seq=1 ttl=118 time=20.2 ms
64 bytes from bog02s12-in-f4.1e100.net (172.217.173.36): icmp_seq=2 ttl=118 time=39.3 ms
64 bytes from bog02s12-in-f4.1e100.net (172.217.173.36): icmp_seq=3 ttl=118 time=164 ms
64 bytes from bog02s12-in-f4.1e100.net (172.217.173.36): icmp_seq=4 ttl=118 time=22.5 ms
64 bytes from bog02s12-in-f4.1e100.net (172.217.173.36): icmp_seq=5 ttl=118 time=107 ms
64 bytes from bog02s12-in-f4.1e100.net (172.217.173.36): icmp_seq=6 ttl=118 time=15.8 ms
64 bytes from bog02s12-in-f4.1e100.net (172.217.173.36): icmp_seq=7 ttl=118 time=22.4 ms
64 bytes from bog02s12-in-f4.1e100.net (172.217.173.36): icmp_seq=8 ttl=118 time=17.4 ms
^C
--- www.google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7008ms
rtt min/avg/max/mdev = 15.848/51.103/163.709/51.202 ms

(root@machineonruiso)~#
```

De parte de Windows 10 tenemos:

```
C:\Users\ruiso>ping www.google.com -t

Haciendo ping a www.google.com [172.217.173.36] con 32 bytes de datos:
Respuesta desde 172.217.173.36: bytes=32 tiempo=17ms TTL=118
Respuesta desde 172.217.173.36: bytes=32 tiempo=20ms TTL=118
Respuesta desde 172.217.173.36: bytes=32 tiempo=17ms TTL=118
Respuesta desde 172.217.173.36: bytes=32 tiempo=17ms TTL=118
Respuesta desde 172.217.173.36: bytes=32 tiempo=18ms TTL=118
Respuesta desde 172.217.173.36: bytes=32 tiempo=16ms TTL=118
Respuesta desde 172.217.173.36: bytes=32 tiempo=20ms TTL=118
Respuesta desde 172.217.173.36: bytes=32 tiempo=20ms TTL=118
Respuesta desde 172.217.173.36: bytes=32 tiempo=18ms TTL=118
Respuesta desde 172.217.173.36: bytes=32 tiempo=15ms TTL=118
Respuesta desde 172.217.173.36: bytes=32 tiempo=14ms TTL=118

Estadísticas de ping para 172.217.173.36:
    Paquetes: enviados = 11, recibidos = 11, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 14ms, Máximo = 20ms, Media = 17ms
Control-C
^C
C:\Users\ruiso>
```

Con una conexión a internet ya podemos por ejemplo instalar LEAFPAD para Kali, para eso abrimos una terminal de comandos y ponemos el comando “sudo apt-get install leafpad”.

```
root@machineonruiso: ~
Archivo Acciones Editar Vista Ayuda

(root@machineonruiso)-[~]
# sudo apt-get install leafpad
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  evince-gtk
Se instalarán los siguientes paquetes NUEVOS:
  leafpad
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 695 no actualizados.
Se necesita descargar 90,9 kB de archivos.
Se utilizarán 465 kB de espacio de disco adicional después de esta operación.
Des:1 http://kali.download/kali kali-rolling/main amd64 leafpad amd64 0.8.18.1-5 [90,9 kB]
Descargados 90,9 kB en 2s (37,6 kB/s)
Seleccionando el paquete leafpad previamente no seleccionado.
(Leyendo la base de datos ... 267021 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar ... /leafpad_0.8.18.1-5_amd64.deb ...
Desempaquetando leafpad (0.8.18.1-5) ...
Configurando leafpad (0.8.18.1-5) ...
update-alternatives: utilizando /usr/bin/leafpad para proveer /usr/bin/gnome-text-editor (gnome-text-editor) en modo automático
Procesando disparadores para kali-menu (2021.3.3) ...
Procesando disparadores para desktop-file-utils (0.26-1) ...
Procesando disparadores para hicolor-icon-theme (0.17-2) ...
Procesando disparadores para man-db (2.9.4-2) ...
Procesando disparadores para mailcap (3.70) ...

(root@machineonruiso)-[~]
```

PASO 2: Actualizar Kali Linux.

Ahora bien, debemos sincronizar Kali Linux con su ultima versión, para hacer esto podemos ejecutar tres comandos simultáneos como los son:

```
apt update -y && apt upgrade -y && apt dist-upgrade
```

Cada comando está separado por “&&” que de forma simple le dice al sistema que, ejecute el comando Uno (1) y luego haga el comando Dos (2) y luego el comando Tres (3).

E primer comando, “apt update” es el encargado de recuperar y recuperar la información de las listas de paquetes de los repositorios, actualizándolas para obtener información sobre las versiones mas recientes de los paquetes y sus dependencias.

El segundo comando, “apt upgrade”, se encarga de descargar e instalar una versión reciente de los paquetes de Kali Linux, esto siempre que existan errores en las dependencias.

El tercer comando, “apt dist-upgrade”, es el encargado de actualizar los paquetes a la versión mas reciente sin importar que estos tengan errores o ya estén en su versión mas reciente, de esta manera si o si sabemos que tenemos siempre lo mas reciente. También instala o elimina las dependencias según esto sea necesario, como es el caso de las dependencias huérfanas o dependencias que ya no necesitan de otras y las mismas ya se quedaron sin soporte.

HACKING DE UNA RED INALAMBRICA

Una vez hemos podido realizar con éxito los anteriores pasos, existen tres aspectos importantes que podemos hacer con Kali según el sistema de destino, estas son:

1. Piratería de redes inalámbricas: Piratería de Wifi, phishing, envenenamiento de ARP, etc.
2. Hacking de aplicaciones web, inyección de SQL, falsificación de solicitudes entre sitios (CSRF), phishing web, etc.
3. Hacking de dispositivos, explotar la máquina de un objetivo X para controlarla.

Aunque bien en la anterior lista no se incluya la piratería con tecnologías IOT, esto no significa que en Kali no se tenga la capacidad para este propósito, sin embargo, esto entra también dentro del área de device hacking, puesto que la mayoría de estos dispositivos tienen literalmente una apariencia y una forma física propias. Siempre debemos tener en cuenta que la mayoría de intromisiones que hagamos van ligados a una serie de pasos, siendo estos:

1. Reconocimiento: recopilación de información
2. Exploración
3. Explotación
4. Post Explotación

Cuando queremos hackear una red inalámbrica, el tipo de víctima que podemos atacar puede variar, esto es debido a que la red inalámbrica consta de varios aspectos como los son los ISP (proveedor de servicios de internet), el enrutador, el modelo, el concentrador, conmutador, etc., y los clientes como lo son el CCTV, usuarios, computadoras remotas, etc. Esto abre un amplio abanico de posibilidades para la vulneración.

Podemos ver a Internet como una gran plataforma de hardware diseñado para la red, redes conectadas entre sí mediante puertas de enlace y en las cuales los paquetes de información siguen rutas de puerta a puerta. Estos sitios a donde llegan los paquetes de datos o información tienen un determinado host o dirección IP de destino, así los paquetes no se confunden entre puertas.

Kali Linux posee una herramienta incorporada llamada Tracer Route, la cual utiliza el campo de “tiempo de vida” del protocolo IP e intenta obtener una respuesta ICMP TIME_EXCEEDED de cada puerta de enlace a lo largo de una ruta a algún host. De esta manera Tracer Route intenta rastrear la ruta que seguiría un paquete de datos IP hacia algún host de internet lanzando paquetes de prueba con un pequeño TTL (tiempo de vida) y luego escuchando una respuesta ICMP de “tiempo encendido desde una puerta de enlace.

1. PASO DE RECONOCIMIENTO

En este paso, obtendremos la mayor cantidad posible de información útil que podamos obtener para luego utilizar la misma en otros pasos. Primero debemos abrir la terminal en forma de root y escribiremos el comando “tracert google.com”. En la siguiente imagen podemos ver un primer comando para comprobar la conexión a internet y el segundo para hacer el trazo de paquetes.

```
root@machineonruiso: ~  
Archivo Acciones Editar Vista Ayuda  
(root@machineonruiso)-[~]  
# ping www.google.com  
PING www.google.com (142.250.78.4) 56(84) bytes of data.  
64 bytes from bog02s14-in-f4.1e100.net (142.250.78.4): icmp_seq=1 ttl=118 time=436 ms  
64 bytes from bog02s14-in-f4.1e100.net (142.250.78.4): icmp_seq=2 ttl=118 time=24.5 ms  
64 bytes from bog02s14-in-f4.1e100.net (142.250.78.4): icmp_seq=3 ttl=118 time=24.2 ms  
64 bytes from bog02s14-in-f4.1e100.net (142.250.78.4): icmp_seq=4 ttl=118 time=107 ms  
^C64 bytes from 142.250.78.4: icmp_seq=5 ttl=118 time=17.7 ms  
--- www.google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4003ms  
rtt min/avg/max/mdev = 17.684/121.848/436.055/160.504 ms  
(root@machineonruiso)-[~]  
# traceroute google.com  
traceroute to google.com (142.250.78.142), 30 hops max, 60 byte packets  
1 192.168.1.254 (192.168.1.254) 4.773 ms 4.729 ms 4.716 ms  
2 static-ip-181510521.cable.net.co (181.51.52.1) 12.286 ms 12.904 ms 12.892 ms  
3 172.28.111.114 (172.28.111.114) 15.762 ms 16.086 ms 16.075 ms  
4 142.250.164.139 (142.250.164.139) 23.833 ms 22.727 ms 21.899 ms  
5 142.250.164.138 (142.250.164.138) 21.686 ms 21.883 ms 21.874 ms  
6 * * *  
7 142.250.210.116 (142.250.210.116) 17.233 ms 172.253.79.8 (172.253.79.8) 17.513 ms 142.250.210.126 (142.250.210.126) 20.118 ms  
8 142.250.210.141 (142.250.210.141) 17.456 ms 142.250.210.139 (142.250.210.139) 17.443 ms 142.250.210.141 (142.250.210.141) 18.603 ms  
9 bog02s18-in-f14.1e100.net (142.250.78.142) 18.591 ms 18.582 ms 18.574 ms  
(root@machineonruiso)-[~]  
#
```

2. PASO ESCANEO

La lista que vemos con anterioridad al lanzar el Traceroute, es una sucesión que nos muestra a donde ha ido nuestro paquete chiquitico en secuencia, como podemos ver obtuvimos 9 saltos antes de que nuestro paquete llegara a su destino. La primera ISP es la de mi enrutador, la cual actúa como puerta de enlace de mi maquina hacia internet, el resto hace referencia a los diferentes puntos de router externos ISP físicos a donde va mi paquete antes de llegar al destino.

Ahora bien, podemos revisar el servicio que se esta ejecutando usando NMAP. Con el podemos examinar los distintos puntos por donde paso el paquete, excepto el salto seis, donde bien está protegida su información o se perdió el paquete en este punto. Del mismo modo, tampoco podemos entrar a ver routers que no poseen un nombre legible.

El salto 3 no tiene host (0 hosts up).

```
(root@machineonruiso)-[~]  
# nmap -v -sS 172.28.111.114  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-26 06:27 -05  
Initiating Ping Scan at 06:27  
Scanning 172.28.111.114 [4 ports]  
Completed Ping Scan at 06:27, 3.03s elapsed (1 total hosts)  
Nmap scan report for 172.28.111.114 [host down]  
Read data files from: /usr/bin/../share/nmap  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds  
Raw packets sent: 8 (304B) | Rcvd: 0 (0B)  
(root@machineonruiso)-[~]  
#
```

El salto 4 tiene varios host (1000 hosts up)(Tuvo que interrumpirse CTRL+C).

```

(root@machineonruiso)-[~]
# nmap -v -sS 142.250.164.139
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-26 06:29 -05
Initiating Ping Scan at 06:29
Scanning 142.250.164.139 [4 ports]
Completed Ping Scan at 06:29, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:29
Completed Parallel DNS resolution of 1 host. at 06:29, 0.02s elapsed
Initiating SYN Stealth Scan at 06:29
Scanning 142.250.164.139 [1000 ports]
Increasing send delay for 142.250.164.139 from 0 to 5 due to 11 out of 23 dropped probes since last increase.
Increasing send delay for 142.250.164.139 from 5 to 10 due to max_successful_ryno increase to 4
Increasing send delay for 142.250.164.139 from 10 to 20 due to max_successful_ryno increase to 5
Increasing send delay for 142.250.164.139 from 20 to 40 due to max_successful_ryno increase to 6
Increasing send delay for 142.250.164.139 from 40 to 80 due to max_successful_ryno increase to 7
Increasing send delay for 142.250.164.139 from 80 to 160 due to 11 out of 29 dropped probes since last increase.
Increasing send delay for 142.250.164.139 from 160 to 320 due to max_successful_ryno increase to 8
SYN Stealth Scan Timing: About 16.21% done; ETC: 06:33 (0:02:40 remaining)
Increasing send delay for 142.250.164.139 from 320 to 640 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 142.250.164.139 from 640 to 1000 due to max_successful_ryno increase to 9
SYN Stealth Scan Timing: About 17.79% done; ETC: 06:35 (0:04:42 remaining)
SYN Stealth Scan Timing: About 19.59% done; ETC: 06:37 (0:06:14 remaining)
SYN Stealth Scan Timing: About 21.75% done; ETC: 06:39 (0:07:15 remaining)
SYN Stealth Scan Timing: About 23.09% done; ETC: 06:40 (0:08:23 remaining)
SYN Stealth Scan Timing: About 23.87% done; ETC: 06:42 (0:09:37 remaining)
Warning: 142.250.164.139 giving up on port because retransmission cap hit (10).
SYN Stealth Scan Timing: About 24.49% done; ETC: 06:44 (0:10:51 remaining)
SYN Stealth Scan Timing: About 25.55% done; ETC: 06:45 (0:11:42 remaining)
SYN Stealth Scan Timing: About 26.26% done; ETC: 06:47 (0:12:41 remaining)
SYN Stealth Scan Timing: About 27.29% done; ETC: 06:48 (0:13:38 remaining)
SYN Stealth Scan Timing: About 27.72% done; ETC: 06:50 (0:14:39 remaining)
SYN Stealth Scan Timing: About 28.05% done; ETC: 06:51 (0:15:41 remaining)
SYN Stealth Scan Timing: About 29.18% done; ETC: 06:53 (0:16:47 remaining)
SYN Stealth Scan Timing: About 29.71% done; ETC: 06:55 (0:18:01 remaining)
SYN Stealth Scan Timing: About 30.85% done; ETC: 06:57 (0:19:19 remaining)
SYN Stealth Scan Timing: About 31.59% done; ETC: 07:00 (0:20:43 remaining)
SYN Stealth Scan Timing: About 33.13% done; ETC: 07:03 (0:22:14 remaining)

```

El salto 5 contiene varios puertos (4 hosts up).

```

(root@machineonruiso)-[~]
# nmap -v -sS 142.250.164.138
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-26 06:47 -05
Initiating Ping Scan at 06:47
Scanning 142.250.164.138 [4 ports]
Completed Ping Scan at 06:47, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:47
Completed Parallel DNS resolution of 1 host. at 06:47, 0.02s elapsed
Initiating SYN Stealth Scan at 06:47
Scanning 142.250.164.138 [1000 ports]
SYN Stealth Scan Timing: About 35.05% done; ETC: 06:49 (0:00:57 remaining)
Completed SYN Stealth Scan at 06:49, 85.76s elapsed (1000 total ports)
Nmap scan report for 142.250.164.138
Host is up (0.084s latency).
All 1000 scanned ports on 142.250.164.138 are filtered

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 85.95 seconds
Raw packets sent: 2004 (88.152KB) | Rcvd: 1 (28B)

(root@machineonruiso)-[~]
#

```

El salto 7 contiene varios puertos (1000 hosts up).

```

(root@machineonruiso)-[~]
# nmap -v -sS 142.250.210.116
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-26 06:54 -05
Initiating Ping Scan at 06:55
Scanning 142.250.210.116 [4 ports]
Completed Ping Scan at 06:55, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:55
Completed Parallel DNS resolution of 1 host. at 06:55, 0.16s elapsed
Initiating SYN Stealth Scan at 06:55
Scanning 142.250.210.116 [1000 ports]
SYN Stealth Scan Timing: About 37.55% done; ETC: 06:56 (0:00:52 remaining)
Completed SYN Stealth Scan at 06:56, 81.15s elapsed (1000 total ports)
Nmap scan report for 142.250.210.116
Host is up (0.080s latency).
All 1000 scanned ports on 142.250.210.116 are filtered

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 81.48 seconds
Raw packets sent: 2004 (88.152KB) | Rcvd: 1 (28B)

(root@machineonruiso)-[~]
#

```

El salto 8 contiene puertos (1000 hosts up).

```

(root@machineonruiso)-[~]
# nmap -v -sS 142.250.210.141
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-26 07:04 -05
Initiating Ping Scan at 07:04
Scanning 142.250.210.141 [4 ports]
Completed Ping Scan at 07:04, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:04
Completed Parallel DNS resolution of 1 host. at 07:04, 0.02s elapsed
Initiating SYN Stealth Scan at 07:04
Scanning 142.250.210.141 [1000 ports]
SYN Stealth Scan Timing: About 39.05% done; ETC: 07:06 (0:00:48 remaining)
Completed SYN Stealth Scan at 07:06, 78.17s elapsed (1000 total ports)
Nmap scan report for 142.250.210.141
Host is up (0.077s latency).
All 1000 scanned ports on 142.250.210.141 are filtered

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 78.36 seconds
Raw packets sent: 2004 (88.152KB) | Rcvd: 1 (28B)

(root@machineonruiso)-[~]
#

```

El comando utilizado es “nmap -v -sS [IP Target] -Pn” el cual esta constituido por varias partes, tales como:

- [-v] Habilita el modo verbosidad
- [-sS] Usa la técnica de escaneo TCP SYN
- [-Pn] Tratar todos los hosts como en línea u omitir el descubrimiento de host

La mayoría de puertas de enlace por donde paso el paquete están filtradas, salvo la del salto 3 y salto 4 por descarte, sin embargo, debemos tener indicado en los mismos los puertos TCP abiertos, lo cual no es el caso. Un puerto filtrado tiene todas las conexiones TCP entrantes bloqueadas por IDS o por Firewall en esta IP.

3. PASO EXPLOTACION

Debido a que no tenemos puertos libres que atacar, solo se nombrara el procedimiento de cómo podríamos explotarlos. Según el resultado con NMAP, podemos saber a que IP tiene un numero de puertos libres o abiertos bajo protocolos como lo es el SSH. Esta entrada es un agujero en el sistema y por donde podemos intentar acceder. Hay varias herramientas de Linux que nos permiten explotar esta vulnerabilidad dependiendo de que queremos hacer, estas herramientas se clasifican en ataques de fuerza bruta o de diccionario contra el protocolo SSH o bien para otros protocolos. Una de las herramientas más utilizadas es “hydra”.

REFERENCIAS:

1. Conoce los mejores sistemas Operativos para Hacking Etico. RZ Redes Zone. Jabier Jimenez. Publicacion creada el Treinta de Abril del año 2021. Enlace Web: <https://www.redeszone.net/tutoriales/seguridad/mejores-distribuciones-linux-hacking-etico/>
2. Tutorial de Kali Linux. Linux Hint. Bima Fajar Ramadhan. Repositorio creado en el año 2017. Enlace Web: <https://linuxhint.com/kali-linux-tutorial/>
3. Distribución de Linux Kali. Version de Kali Bare Metal. Kali ORG sitio official. Enlace web: <https://www.kali.org/get-kali/#kali-bare-metal>
4. Installing Kali Linux on desktops & laptops using ".ISO" files (x64/x86). Kali Linux ORG. Guia Oficial de Instalacion de Kali Linux Actualizada al momento del 26 de oct. de 21. Enlace Web: <https://www.kali.org/docs/installation/>
5. Configurar Wi-Fi en Kali Linux VirtualBox y Guest Additions. Profesional Rewiew. Jose Antonio Castillo. Enero 02 de 2019. Enlace web: <https://www.profesionalreview.com/2019/01/02/wi-fi-kali-linux-virtualbox/>