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 maquina víctima como se muestra a continuación.

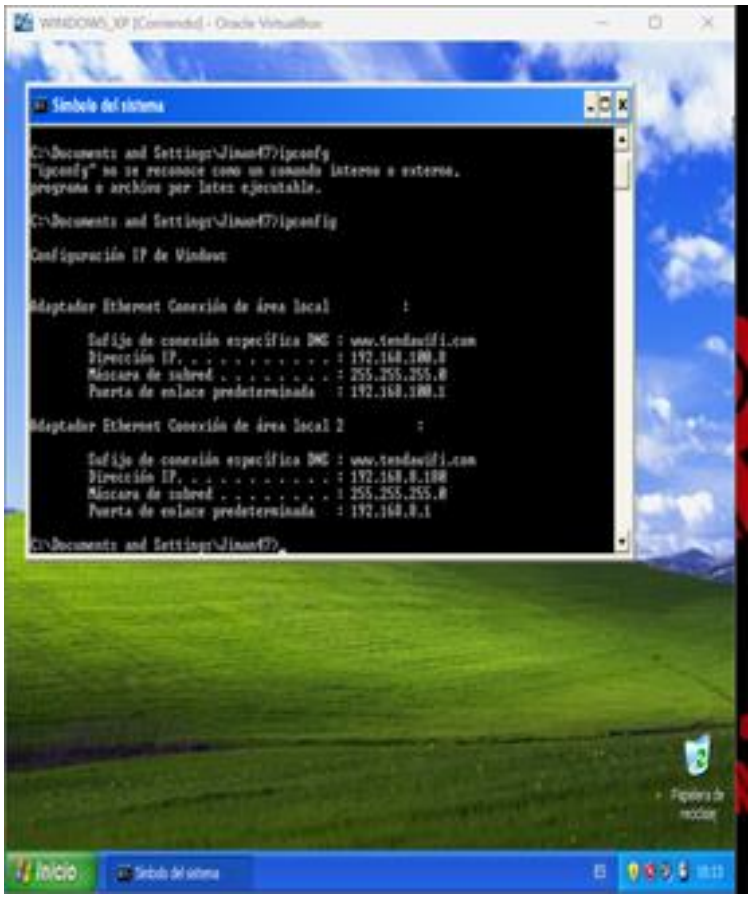


Ilustración 1 identificacion IP maquina victima

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

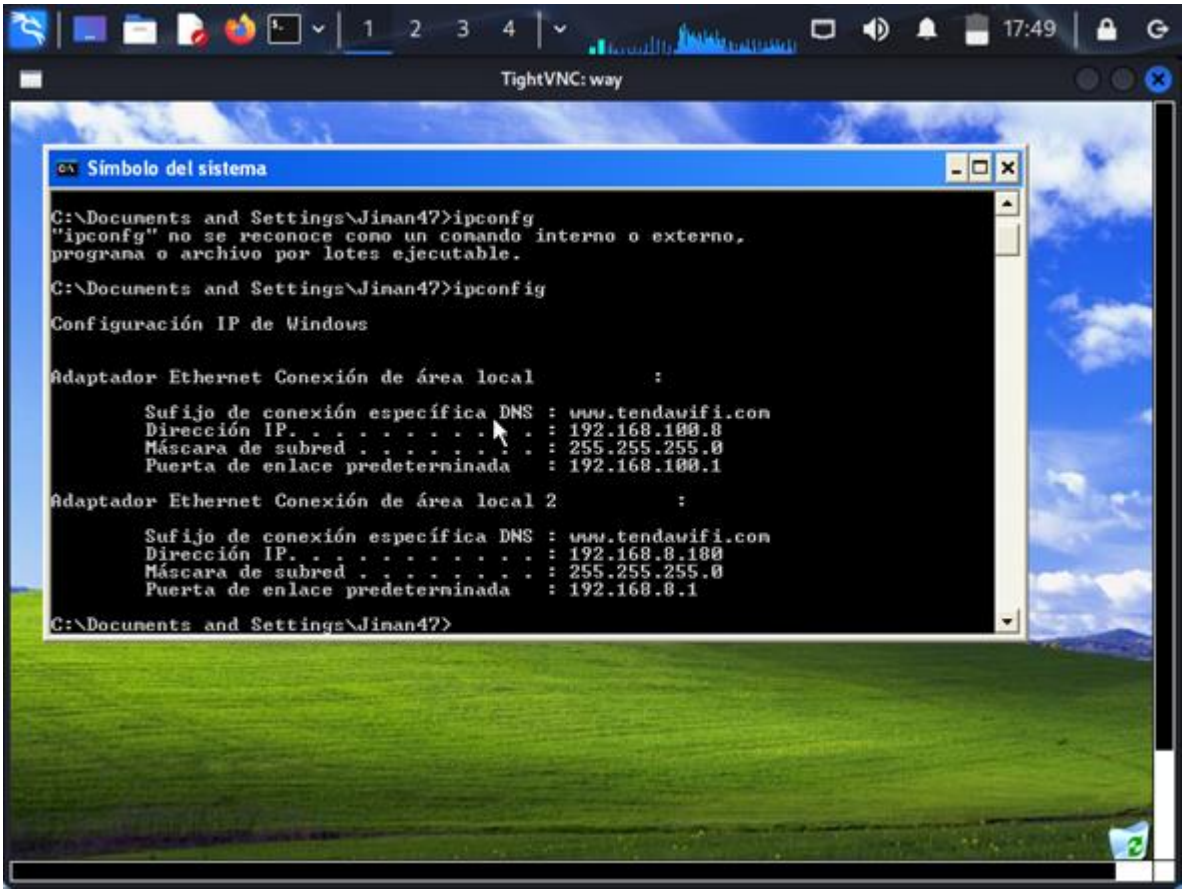
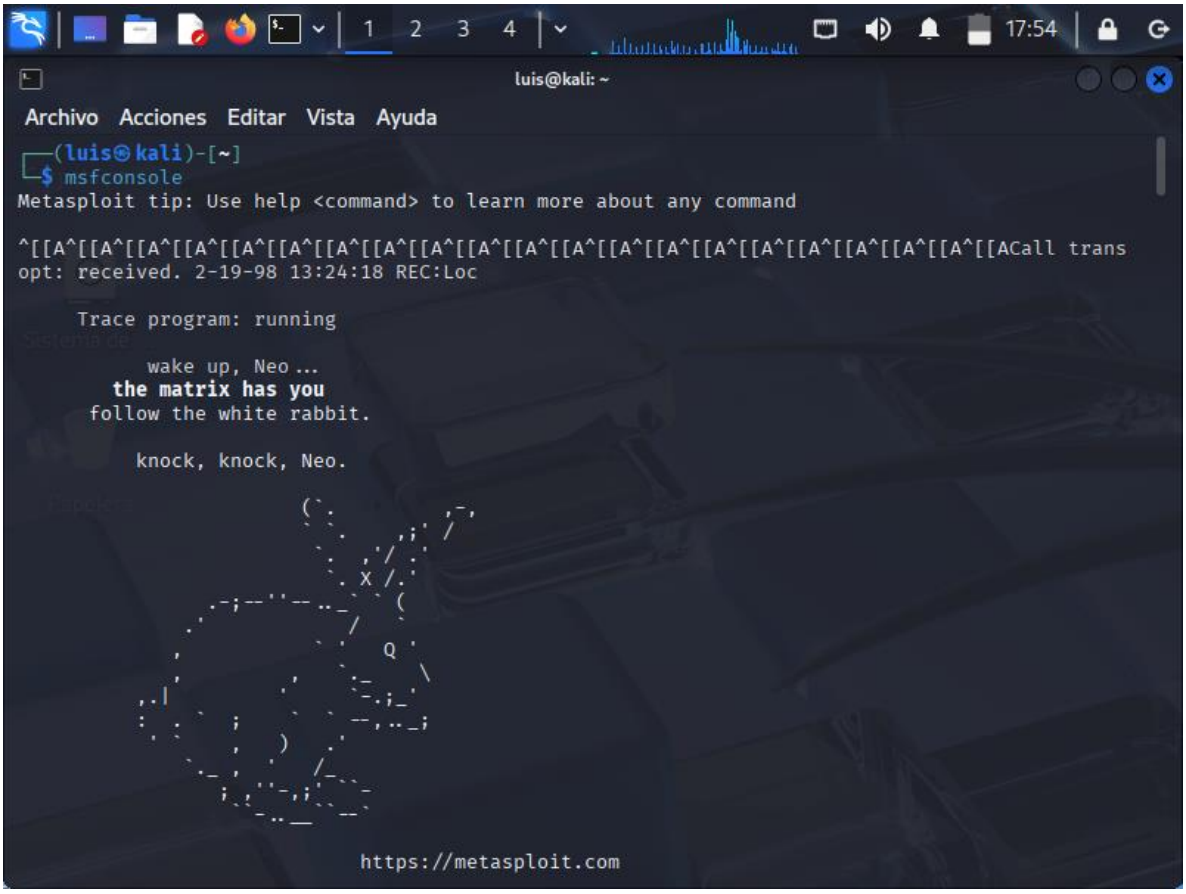


Ilustración 2 Identificacion IP maquina atacante Kali linux

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



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

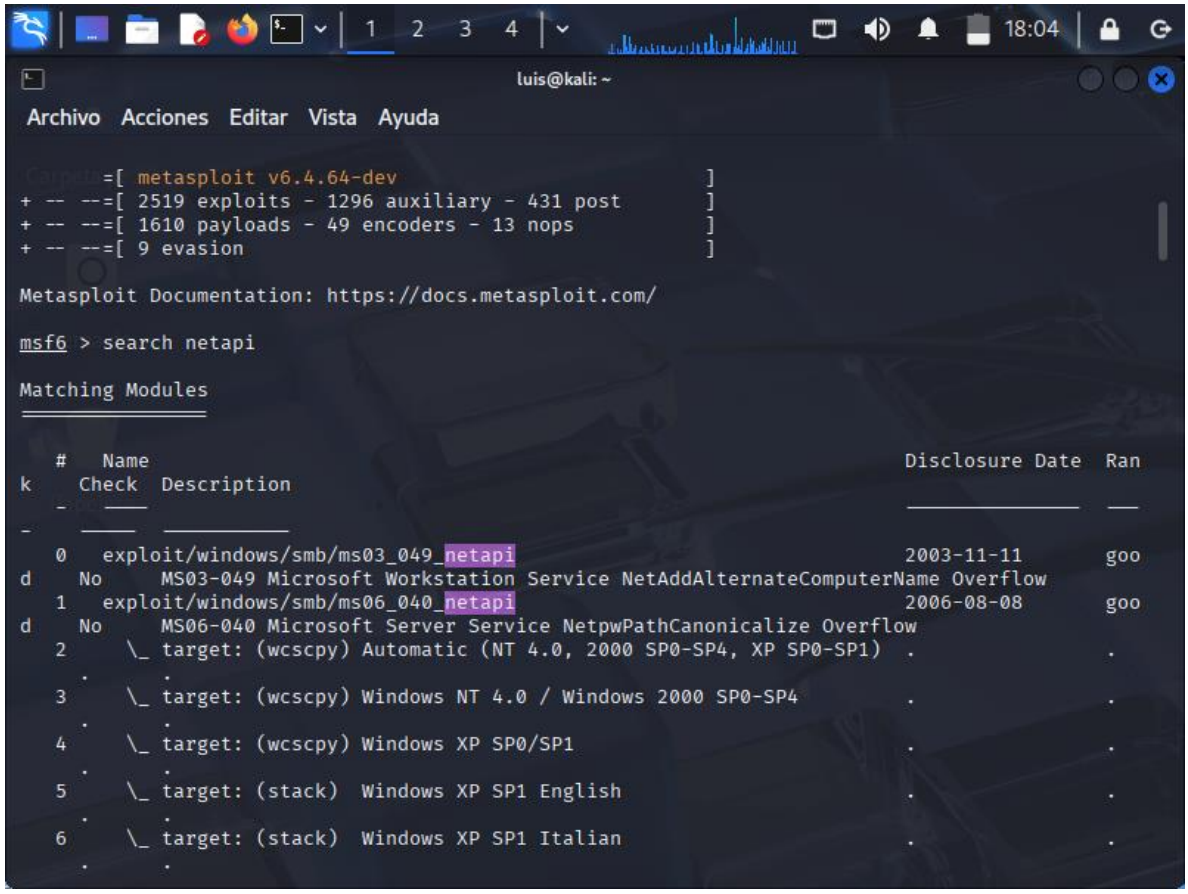


Ilustración 3 escaneo modulos search netapi

Selecionamos 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**

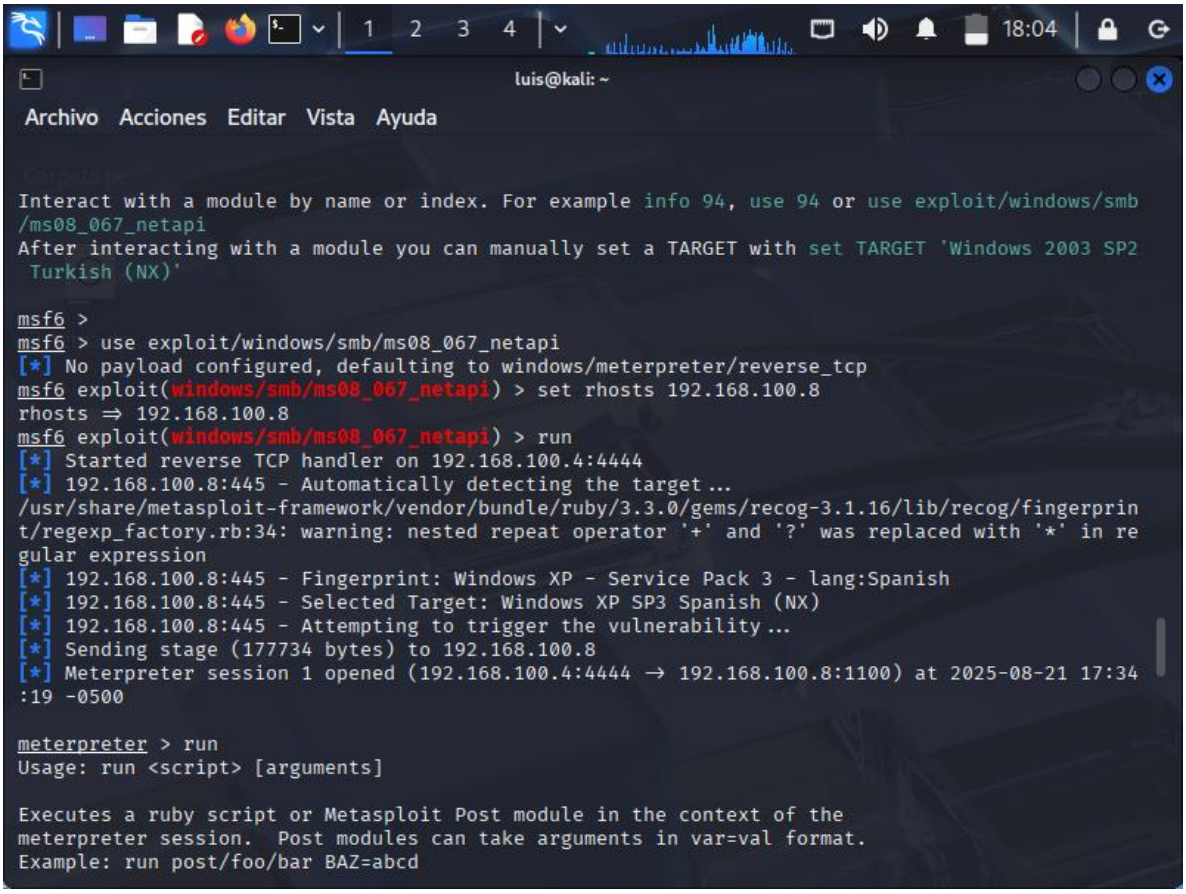


Ilustración 4 Penetracion exitosa

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

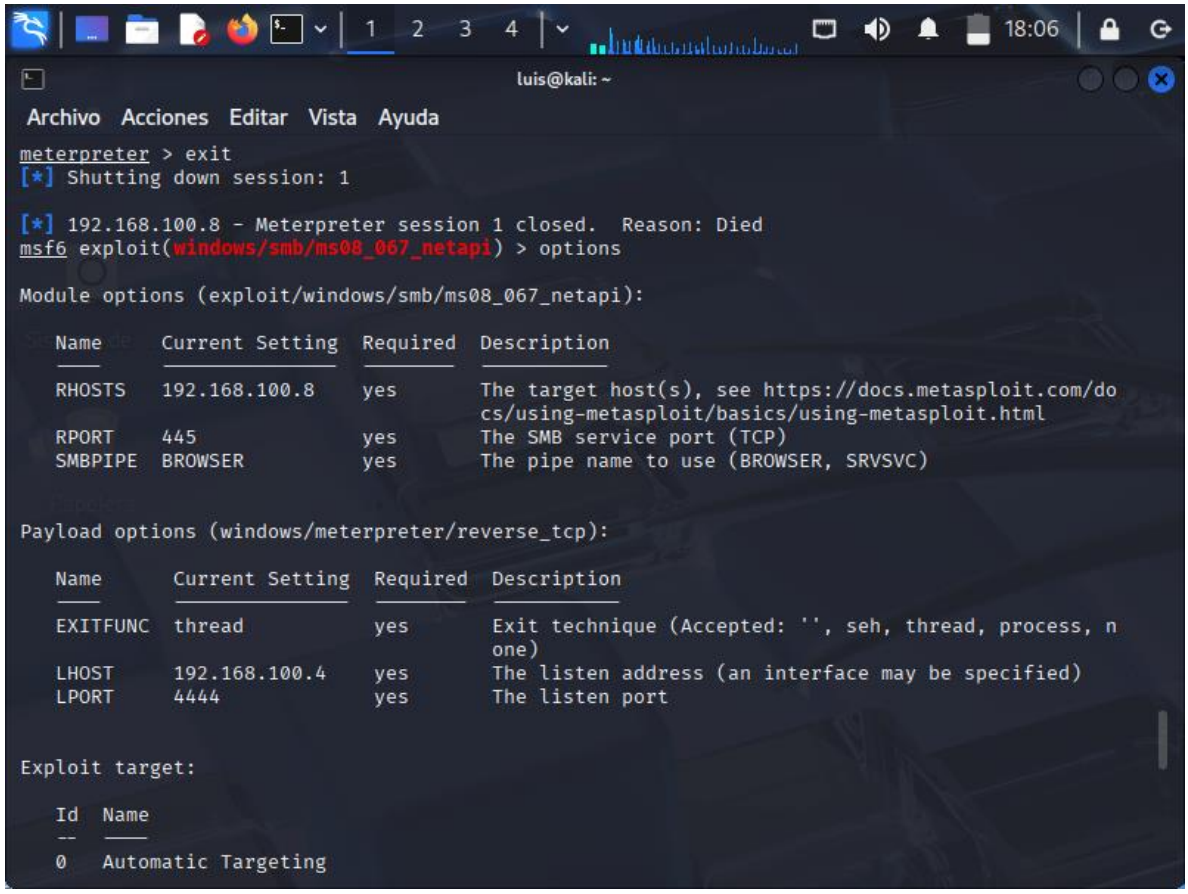
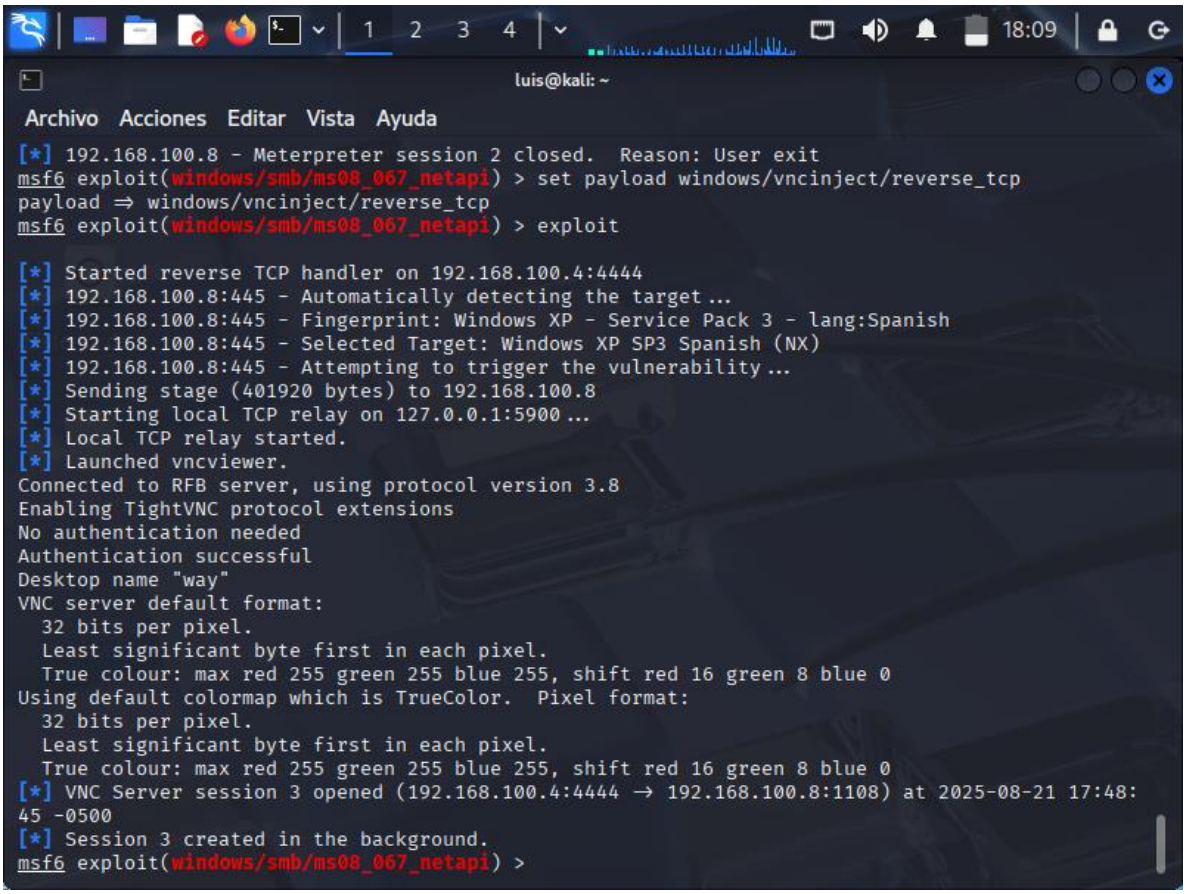


Ilustración 5 inicion sesion meterprete exitoso



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.

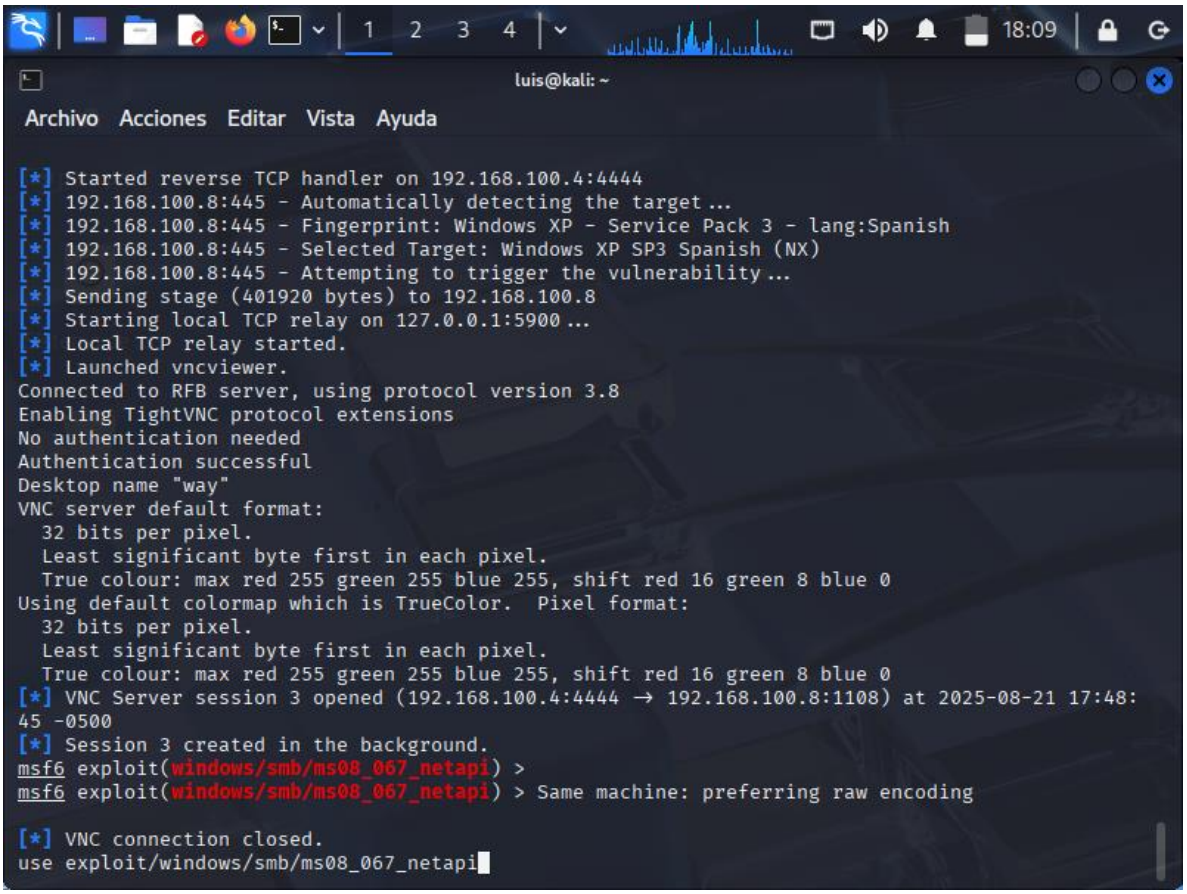


Ilustración 6 ejecucion de explotación

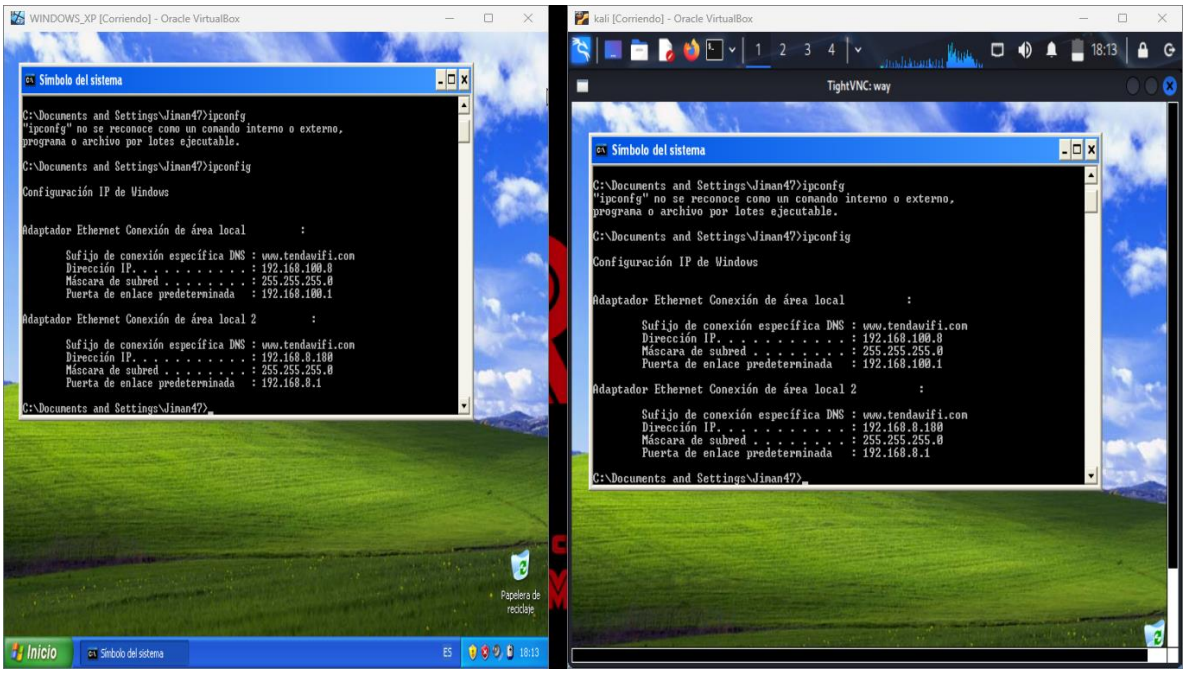


Ilustración 7 Conexion aseso remoto de kali a windows xp

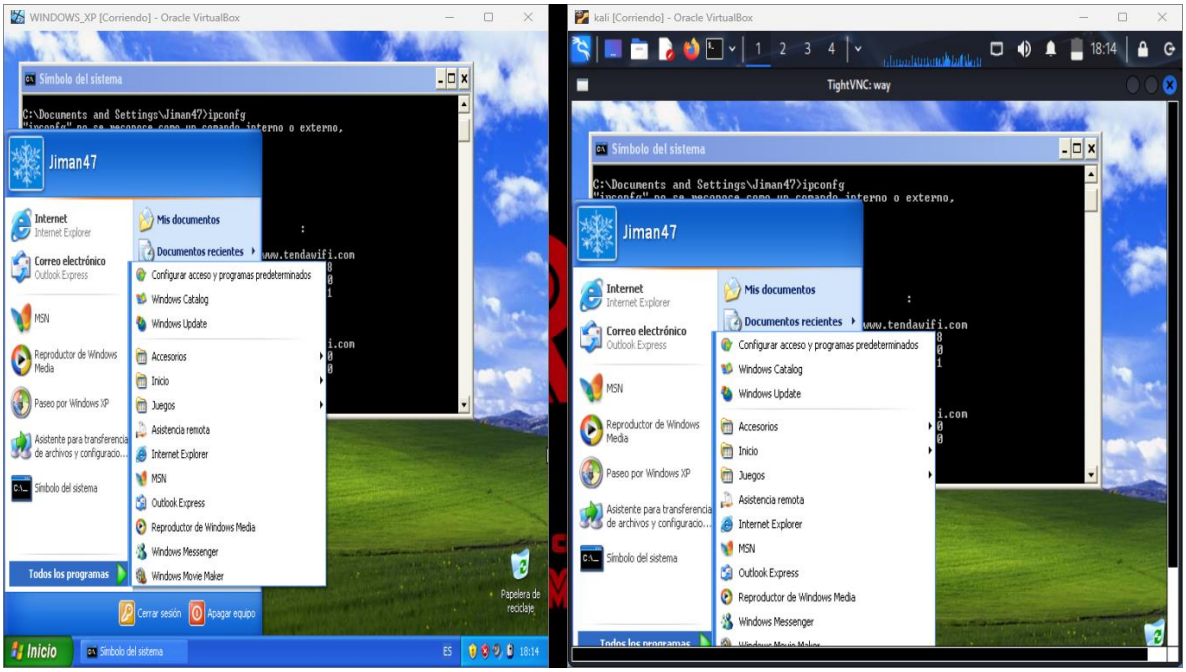


Ilustración 8 Conexion aseso remoto de kali a windows xp imagen 2

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