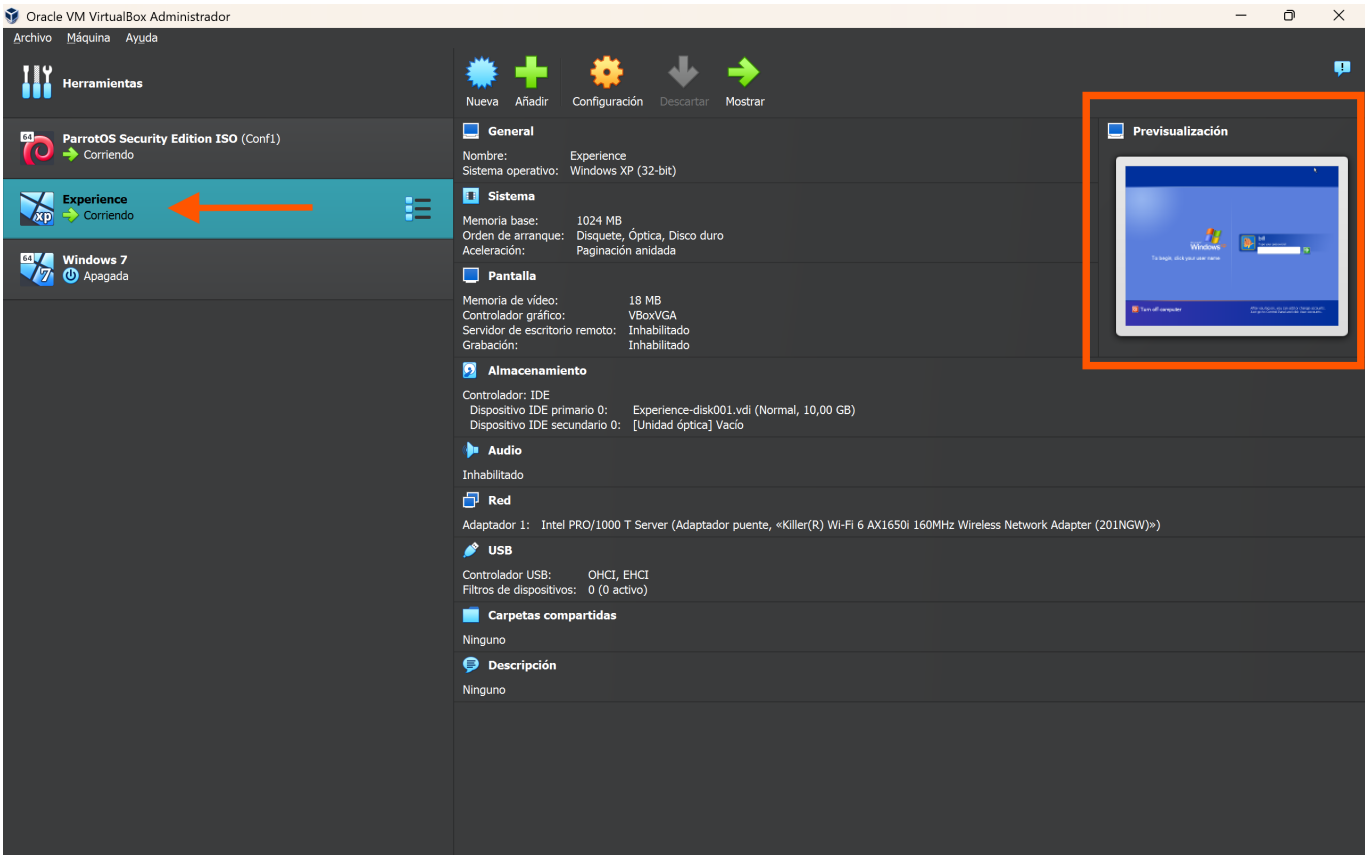
Writeup: [Experience]

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

1. Reconocimiento (Recon)

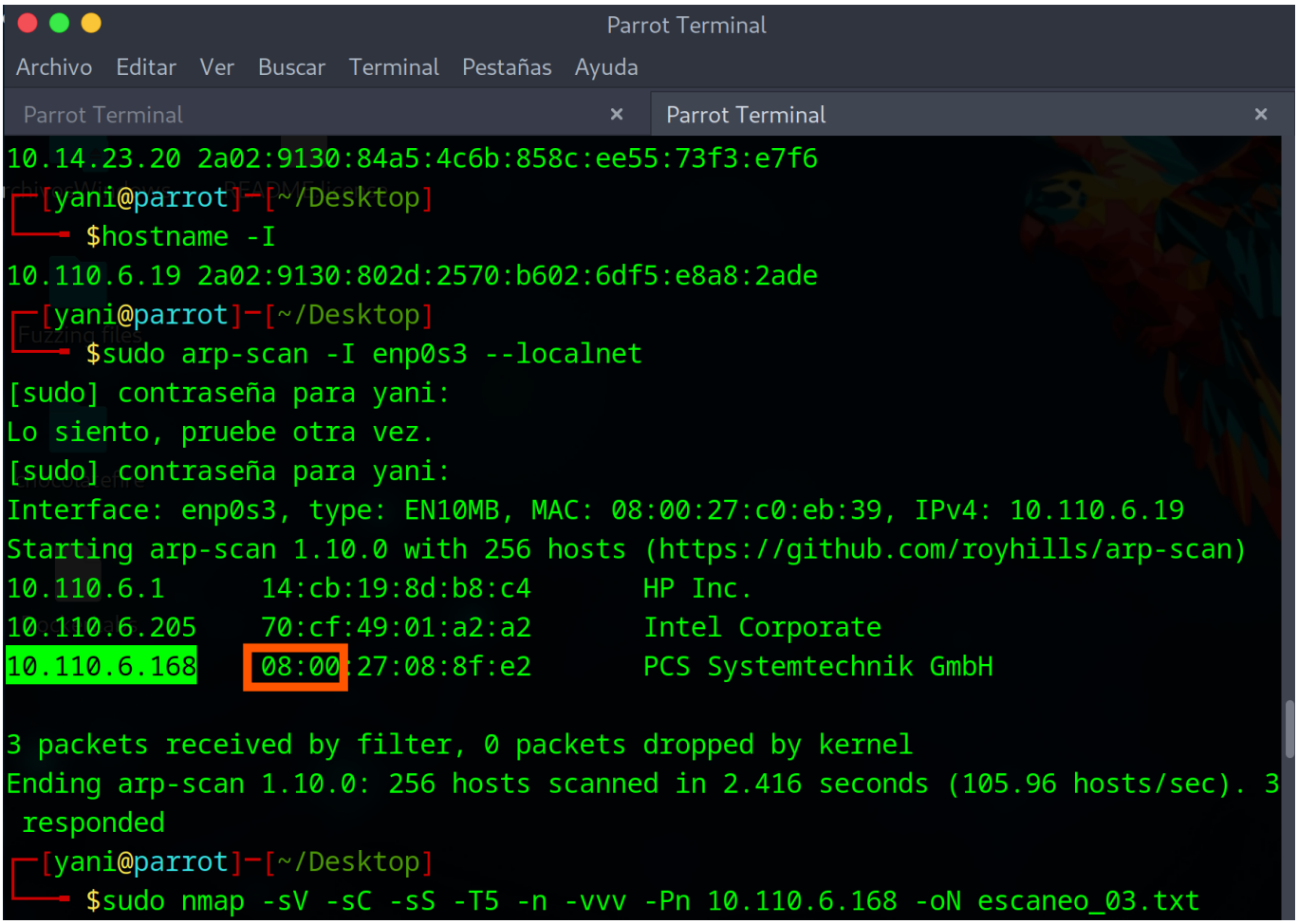
Escaneo de Puertos

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**

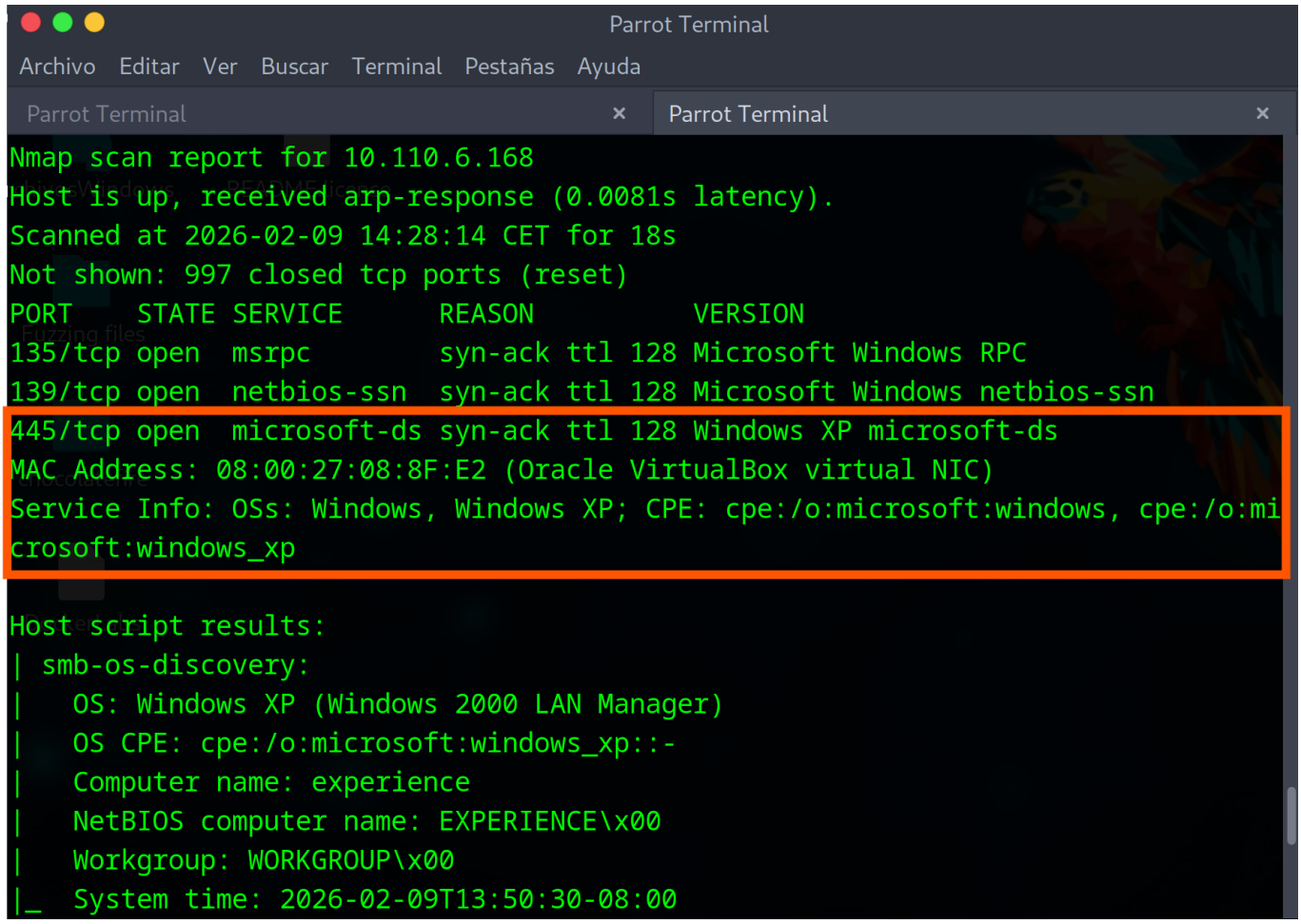


Realizo un escaneo avanzado para exponer los puertos abiertos y posibles vulnerabilidades.

```
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*.).



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

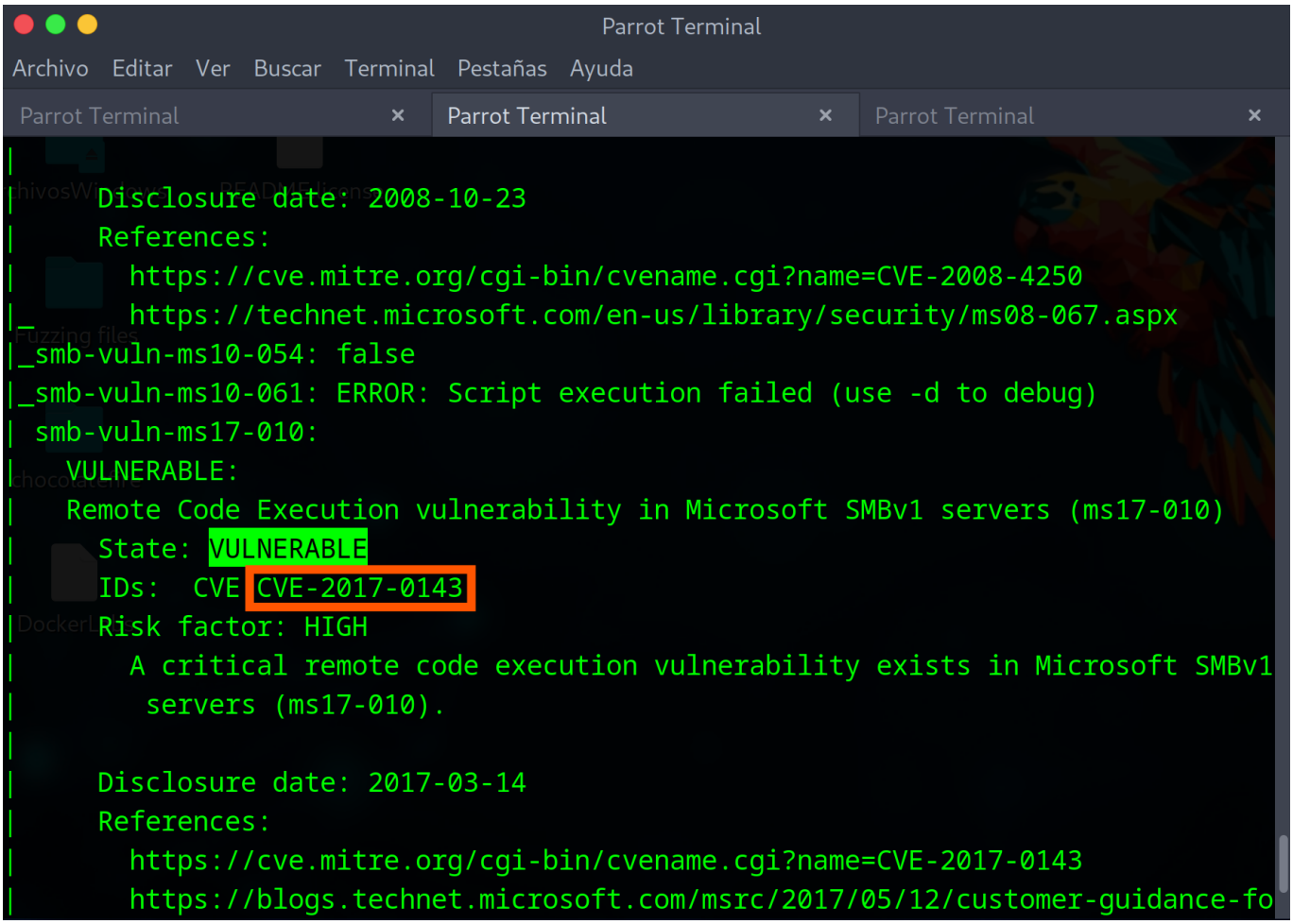
```
sudo nmap -p445 -sS --script=vuln -vvv -Pn 10.110.6.168
```

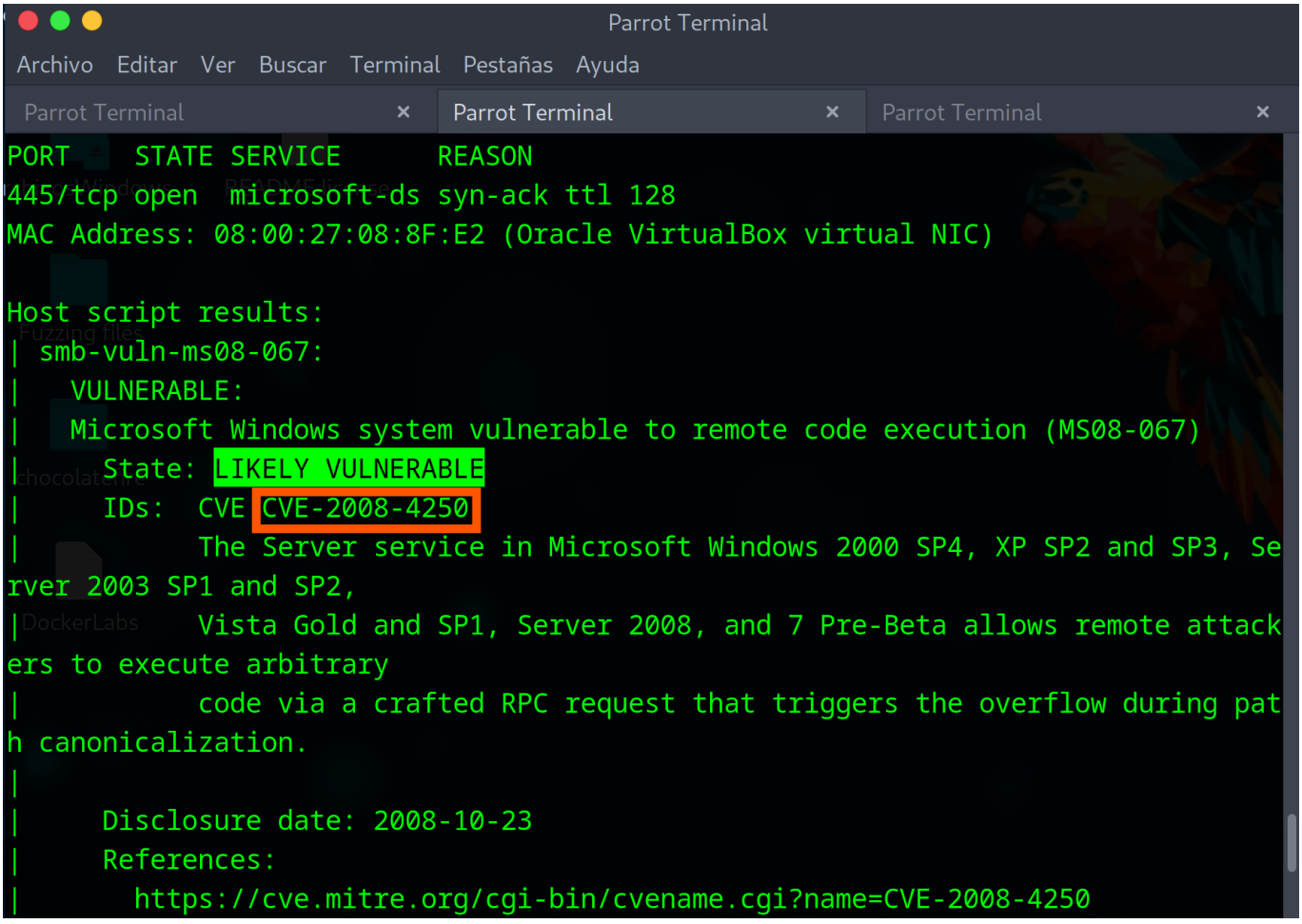
3. 💥 Explotación (User Flag)

Análisis de la Vulnerabilidad

nmap de **vuln** expone dos vulnerabilades:

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

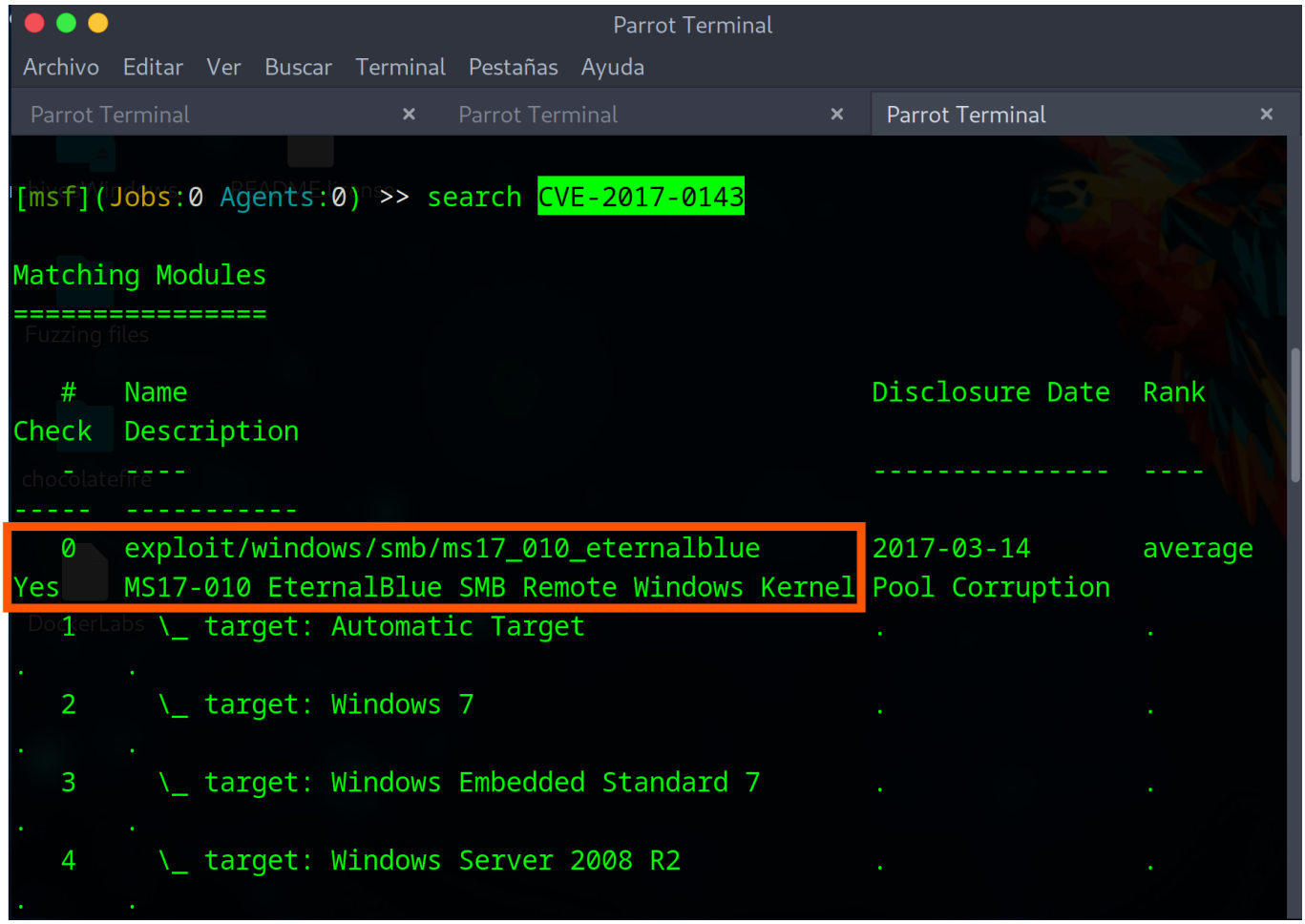




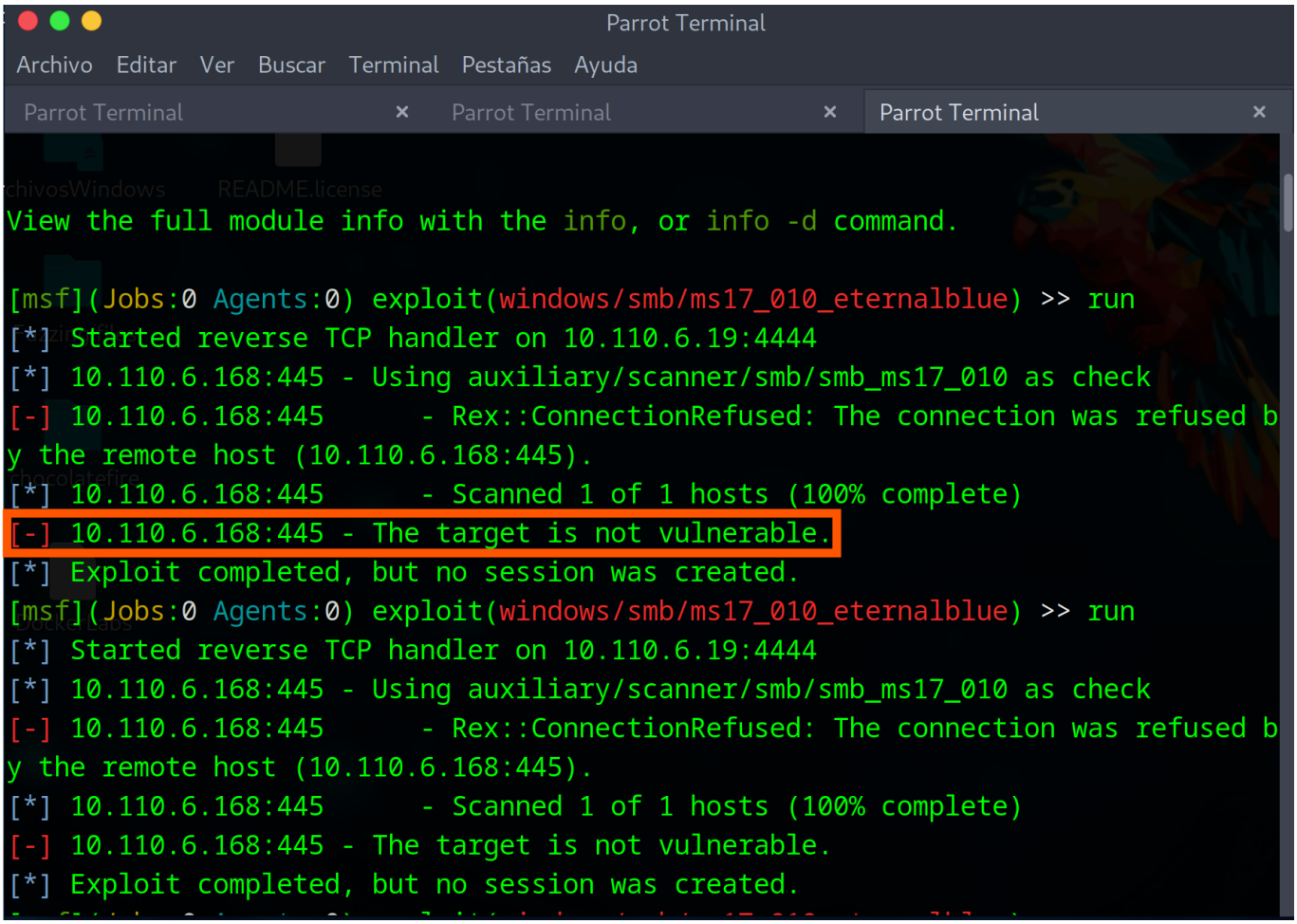
Ejecución del Exploit

Lanzo por consola ***metasploit***:

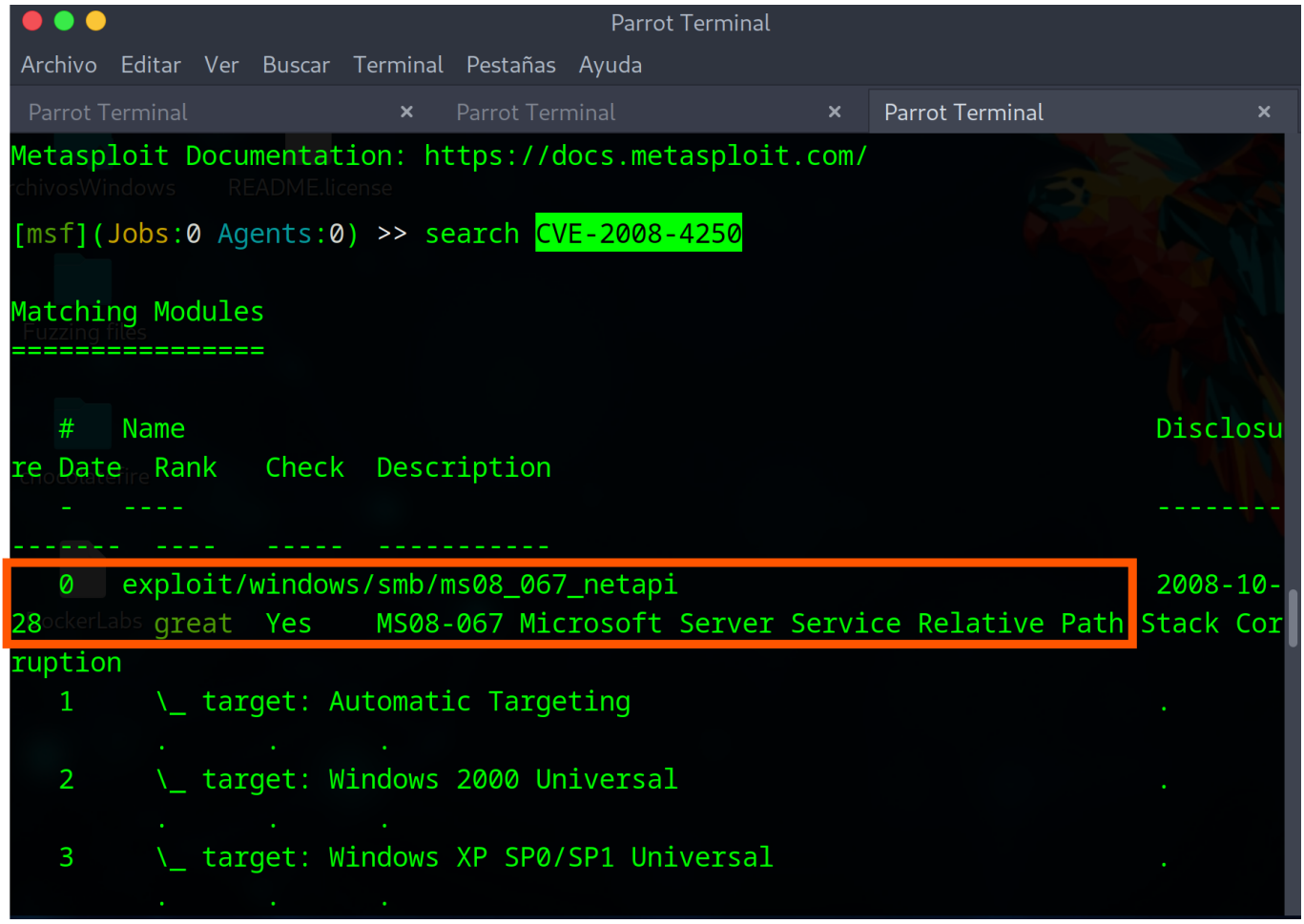
Ejecuto la explotación de la primera vulneravilidad : **CVE-2017-0143**



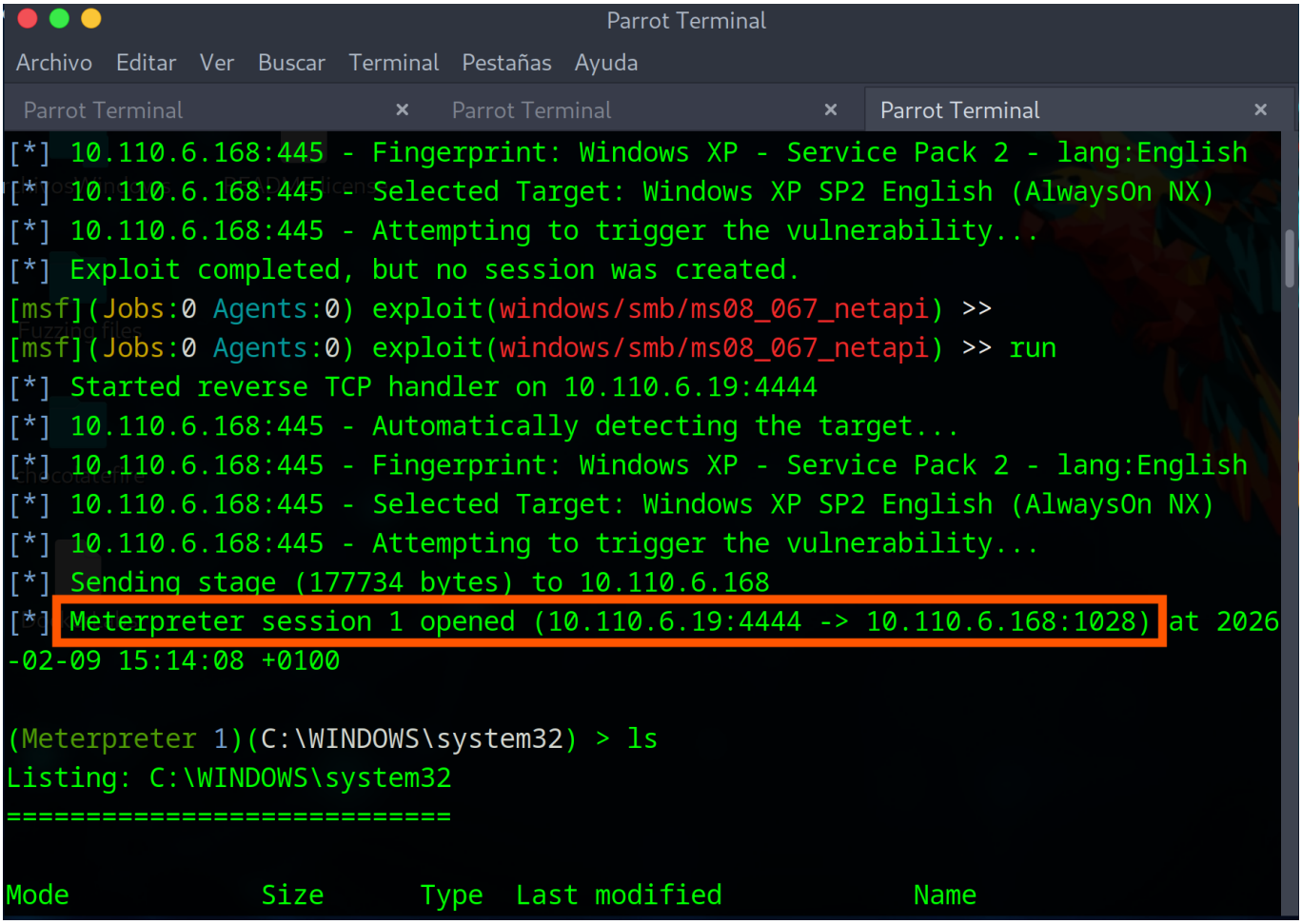
El exploit no logra comprometer la máquina.



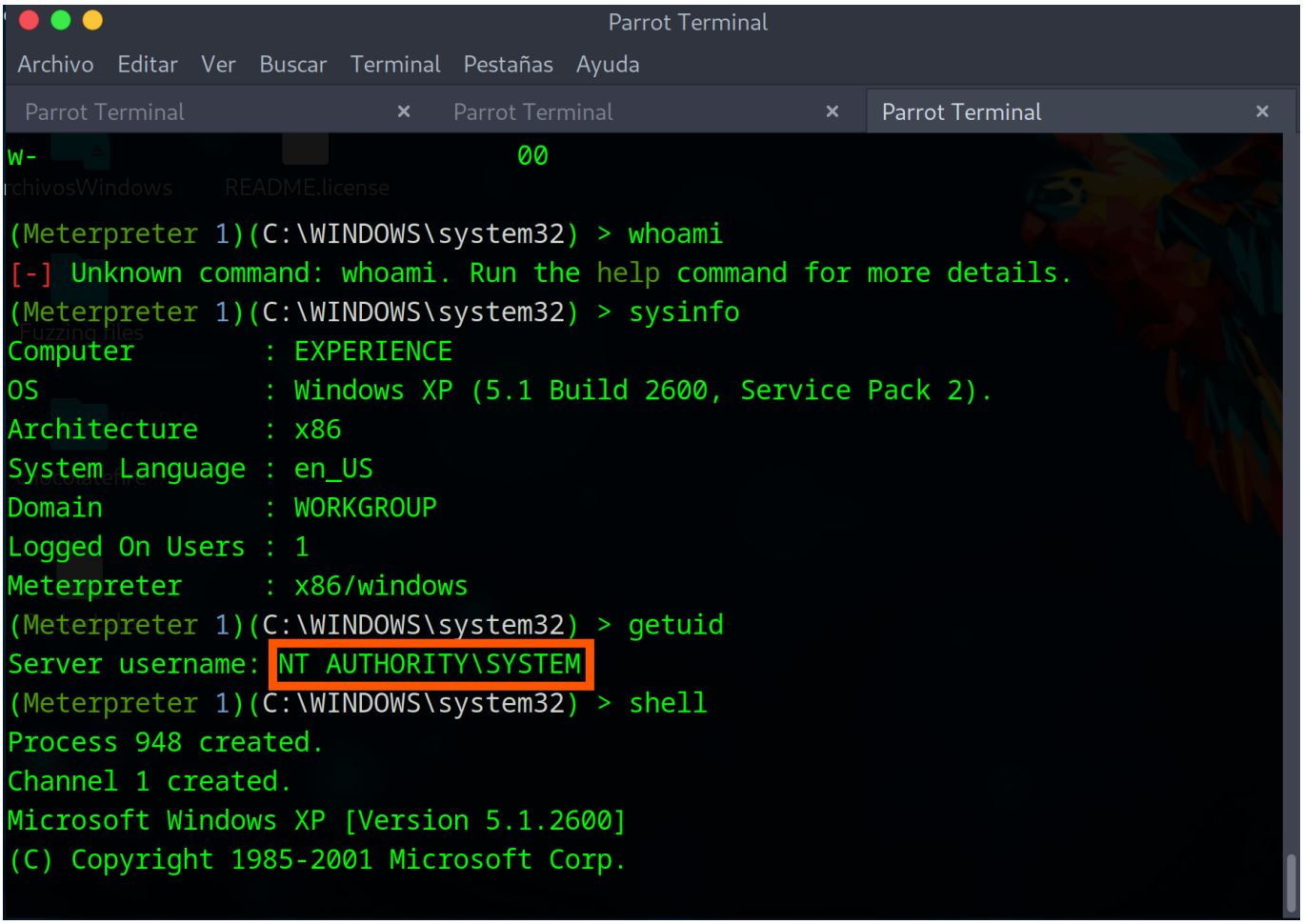
Procedo a lanzar el exploit de la segunda vulnerabilidad: **CVE-2008-4250**



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



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



4. 🚀 Escalada de Privilegios (Root Flag)

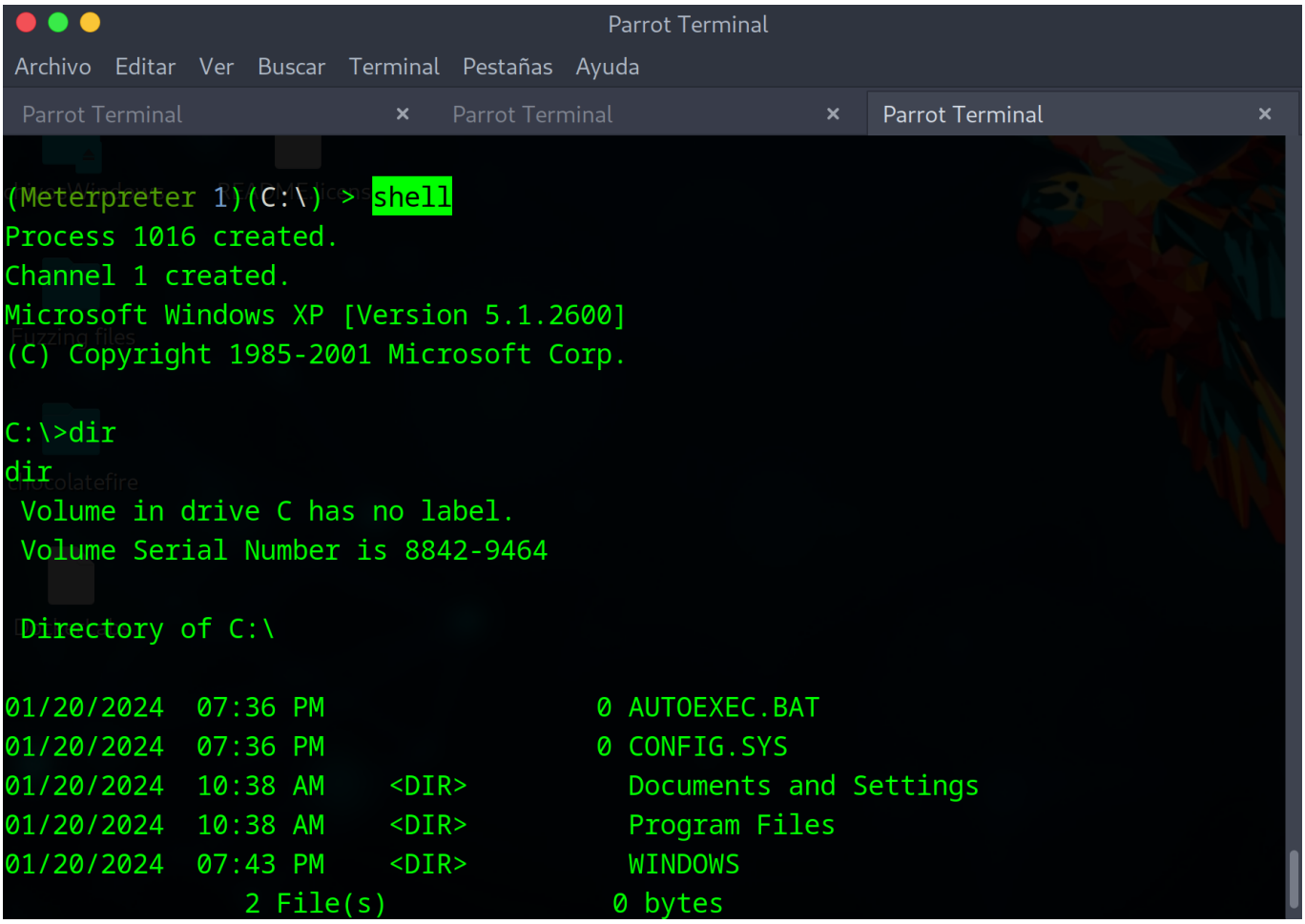
Enumeración Interna

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`



🏆 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/