Práctica 03 - Fase de Escaneo

1. Escaneo de red para identificar dispositivos activos

Utilizamos nmap para descubrir dispositivos en la red local:

```
nmap -sn 192.168.1.0/24
```

2. Escaneo de puertos abiertos en un dispositivo específico

Escaneamos los puertos abiertos en un dispositivo identificado:

```
nmap -sS 192.168.1.10
```

3. Identificación de servicios en los puertos abiertos

Descubrimos qué servicios están corriendo y sus versiones:

```
nmap -sV -p 22,80,443 192.168.1.10
```

4. Escaneo de vulnerabilidades

Realizamos un escaneo para detectar posibles vulnerabilidades:

```
nmap --script vuln 192.168.1.10
```

5. Generación de un informe

Guardamos los resultados del escaneo en un archivo para referencia futura:

```
nmap -sV 192.168.1.10 -oN escaneo_resultados.txt
```

6. Escaneo avanzado (opcional)

Incluímos opciones avanzadas como la detección de sistema operativo:

```
nmap -O 192.168.1.10
```