



## Exploración del objetivo

**Sku:** 3865EC

**Horas:** 10

## OBJETIVOS

- Profundizar en el concepto de escaneo.
- Analizar las contramedidas para ping sweeps y de consultas ICPM.
- Distinguir los tipos de escaneo.
- Identificar los servicios TCP y UDP en ejecución.
- Conocer los escáneres de puertos basados en Windows.
- Estudiar la detección del sistema operativo.

## CONTENIDOS

### 1. Escaneo. 2. Determinar si el sistema está vivo.

1. Contramedidas para Ping Sweeps.
2. Contramedidas de consultas ICMP.

### 3. Determinación de los servicios que se ejecutan o escuchan.

1. Tipos de escaneo.
2. Identificación de servicios TCP y UDP en ejecución. 2.1. Strobe. 2.2. UDP\_Scan. 2.3. Netcat. 2.4. Mapeador de red (Nmap)
3. Escáneres de puertos basados en Windows. 3.1. SuperScan. 3.2. Wups. 3.3. Scanline.
4. Contramedidas de exploración de puertos.

### 4. Detección del sistema operativo.

1. Fingerprinting de pila activa.
2. Contramedidas de detección de sistemas operativos.
3. Fingerprinting de pila pasiva. 3.1. Firmas pasivas.