M2-A2: Escaneo de puertos (Nmap y Masscan)

Objetivo: descubrir y analizar servicios expuestos en un host de laboratorio (puedes utilizar la máquina Metasploitable 2 como objetivo) https://docs.rapid7.com/metasploit/metasploitable-2/

1. Descubrimiento rápido de puertos con Masscan

Se escanean todos los puertos TCP en el host `10.0.0.133`:

```
sudo masscan 10.0.0.133 -p1-65535 --rate=1000 -oL masscan.txt
```

2. Parseo de resultados

Extraemos **la IP** y la **lista de puertos**:

```
host=$(awk '!/^#/ {print $4}' masscan.txt | sort -u | tr -d '\r' | tr -d ' ')
ports=$(awk '!/^#/ {print $3}' masscan.txt | sort -n | uniq | paste -sd, -)
```

Verificamos:

```
echo "Host: $host"
echo "Puertos: $ports"
```

3. Escaneo detallado con Nmap

Ahora se usa la IP y los puertos descubiertos para un análisis profundo:

```
nmap -sS -sV -O -p$ports $host -oA nmap_resultados
```

Entregar:

- Tabla con: **puerto – servicio – versión detectada – posible vulnerabilidad**.
- 5–10 frases de análisis:
  - ¿Qué servicios representan mayor riesgo?
  - ¿Qué vulnerabilidades conocidas podrían existir según las versiones detectadas?