**Sistemas de Gestión de Seguridad de la Información 2023/2024**

# Laboratorio 9 – NMap

---

**Objetivos:**

1. Familiarizarse con herramientas de escaneo de vulnerabilidades en redes.

---

## NMAP

**Nmap**[1] es un programa de código abierto que sirve para rastrear puertos y máquinas en una red[2]. Con **Nmap** se pueden descubrir fácilmente muchas características de las máquinas que están visibles en la red: qué máquinas están encendidas, que puertos tiene abiertos una máquina concreta, qué servicios está ejecutando y qué versiones de los mismos, qué sistema operativo y qué versión usa, etc.

- Ejecuta el siguiente comando para instalar NMap:

```
$ sudo apt install nmap
```

Describe los comandos necesarios para descubrir lo siguiente:

- Puertos abiertos en scanme.nmap.org y en tu servidor Google Cloud, servicios y versión de servicios.

- ¿Que máquinas están activas en la red desde tu máquina a tu servidor remoto? (pista: **traceroute**).

- ¿Qué puertos tiene abiertos una de las máquinas activas de la red?

- ¿Qué versiones de los servicios está usando una de las máquinas activas de la red?

- ¿Qué sistema operativo tiene una de las máquinas activas de la red?

- ¿Qué sistema operativo tiene tu servidor en Google Cloud (Según Nmap)?

- ¿Qué sistema operativo tiene scanme.nmap.org?

- Una vez determinado el Sistema Operativo, ¿Qué vulnerabilidades tiene? (pista: **https://cve.mitre.org**).

- ¿Cómo se puede usar nmap para detectar si una máquina tiene un firewall?

1 https://nmap.org/
2 Probablemente sea la herramienta de Hacking que aparece en más películas: https://nmap.org/movies/