About Nmap

http://nmap.org/

Created by *Gordon Lyon* in 1997

Already installed on Kali Linux

GUI version called Zenmap (also on Kali Linux)

Using NMAP

- **Host discovery (ping based)**

  ```
  $ nmap -sP 10.0.1.0-255
  ```

- **OS detection**

  ```
  $ nmap -O 10.0.1.101
  ```

- **Full TCP port scanning**

  ```
  $ nmap -p0-65535 10.0.1.101
  ```

- **Version detection**

  ```
  $ nmap -sV 10.0.1.101
  ```

- **Export a full scan to a file**

  ```
  $ nmap -O —sV -p0-65535 10.0.1.101 -oN target.nmap
  ```