Lab 04 – Scanning

# Overview

Start using nmap to scan a host on a network. Reference the nmap cheat sheet for options. For all of the commands below, save the output using the **-oA** flag with a filename that is **first initial + last Name\_scanType**.

## nmap

1. Start by running a simple host discovery scan on the Docker network created once the VM is up and running. You will have to leave the VM running in another terminal tab to keep it up.

1. After locating the target, conduct a full port scan of the target with the following options
   1. TCP Scan
   2. Speed 4
   3. Version scan
   4. Only open ports
   5. No ping
   6. No DNS resolution
2. Complete any additional scans you feel are necessary.
3. Compile your findings into a professional report.