**NMap**

Introduction

Nmap stands for network mapping.

* Nmap utilizes raw IP packets to detect:
  + Available hosts on the network.
  + Services offered (application name and version).
  + Operating systems and their versions.
  + Packet filters/firewalls in use.
* It is capable of scanning both large networks and single hosts efficiently.

Commands

 Nmap list scan (-sL )

enumerates every IP address in the given target netblock

/24 after IP , it scans IPs from 0 – 255

-p-

scan *every* port from 1-65535

-A

This shortcut option turns on *A*dvanced and *A*ggressive features such as OS and service detection

-T4

Adjusts timing to the aggressive level (#4 of 5).

To see If nmap is already installed :  **nmap –version**

To download nmap: <https://nmap.org/download.html>

**host -t ns target.com**

shows the DNS queries for the domain that it's associated with