NMAP
(Network Mapper)

What is Nmap?

- Nmap, short for Network Mapper, is a network discovery and security auditing tool
- Nmap is one of the most commonly used tools by penetration testing or by ethical hackers
- It is known for its simple and easy to remember flags that provide powerful scanning options

What is Nmap? Cont.

- Nmap is widely used by network administrators to scan for:
  - Open ports and services
  - Discover services along with their versions
  - Guess the operating system running on a target machine
  - Get accurate packet routes till the target machine
  - Monitoring hosts

Nmap Scan Types

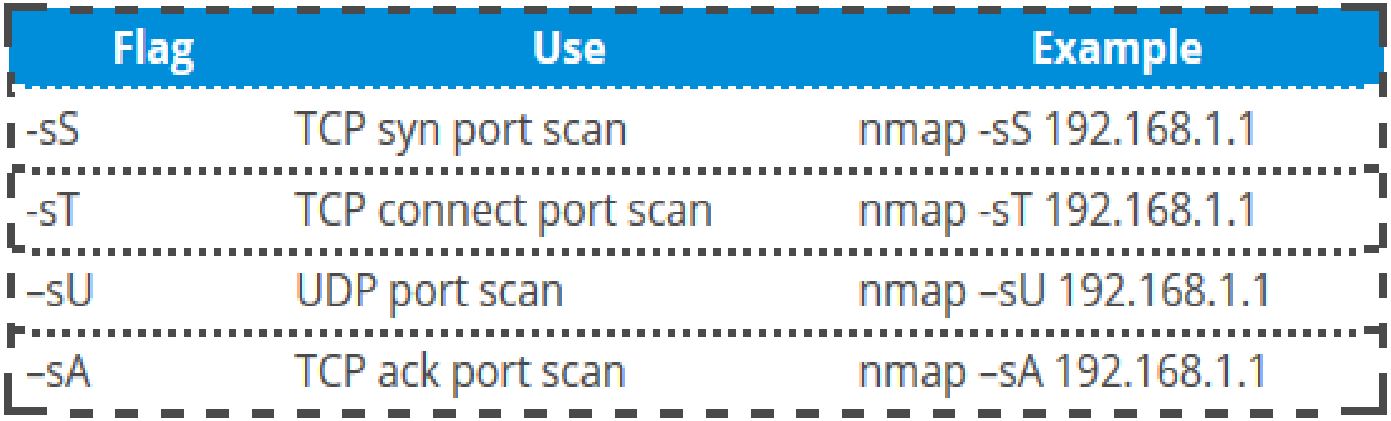
❖ A variety of scans can be performed using Nmap. Below are the types of scans:

- ❑ TCP SCAN
- ❑ UDP SCAN
- ❑ SYN SCAN
- ❑ ACK SCAN
- ❑ FIN SCAN
- ❑ NULL SCAN
- ❑ XMAS SCAN
- ❑ RPC SCAN
- ❑ IDLE SCAN

Nmap Commands

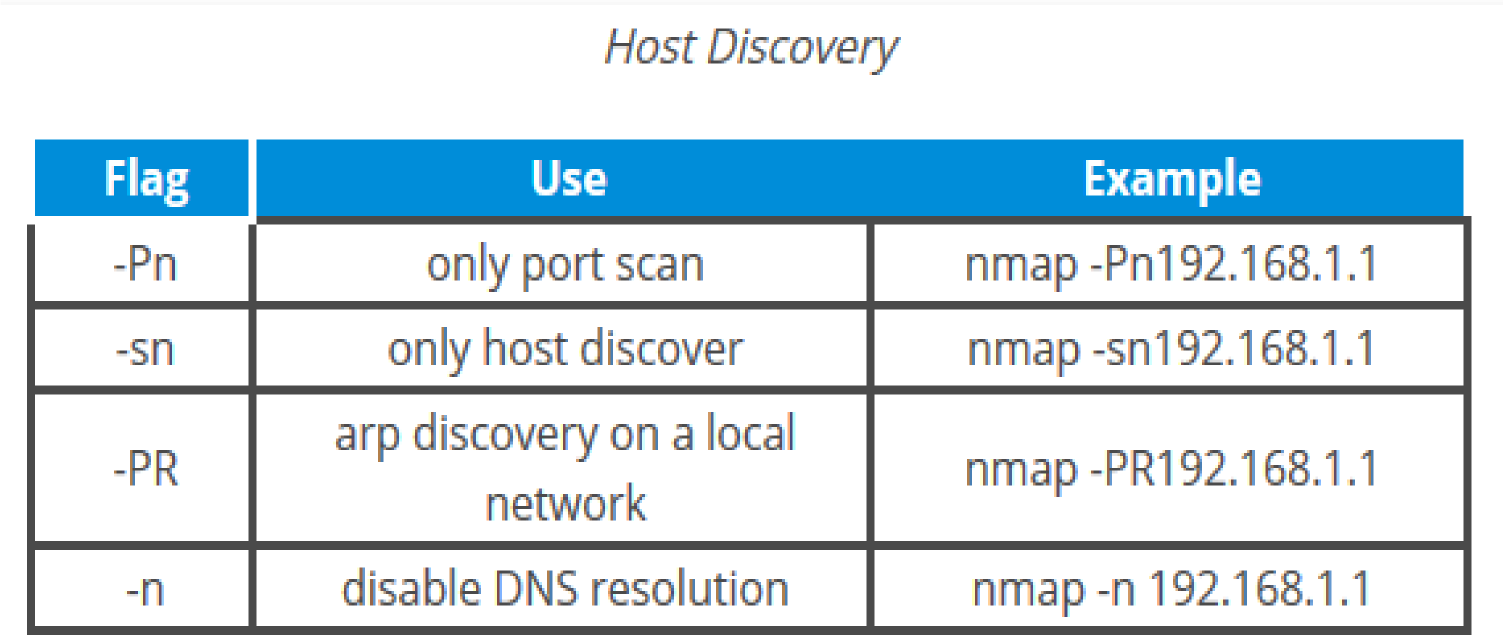
- The various commands you can use in Nmap along with their flag and usage description with an example on how to use it

Scanning Techniques



Flag	Use	Example
-sS	TCP syn port scan	nmap -sS 192.168.1.1
-sT	TCP connect port scan	nmap -sT 192.168.1.1
–sU	UDP port scan	nmap –sU 192.168.1.1
–sA	TCP ack port scan	nmap –sA 192.168.1.1

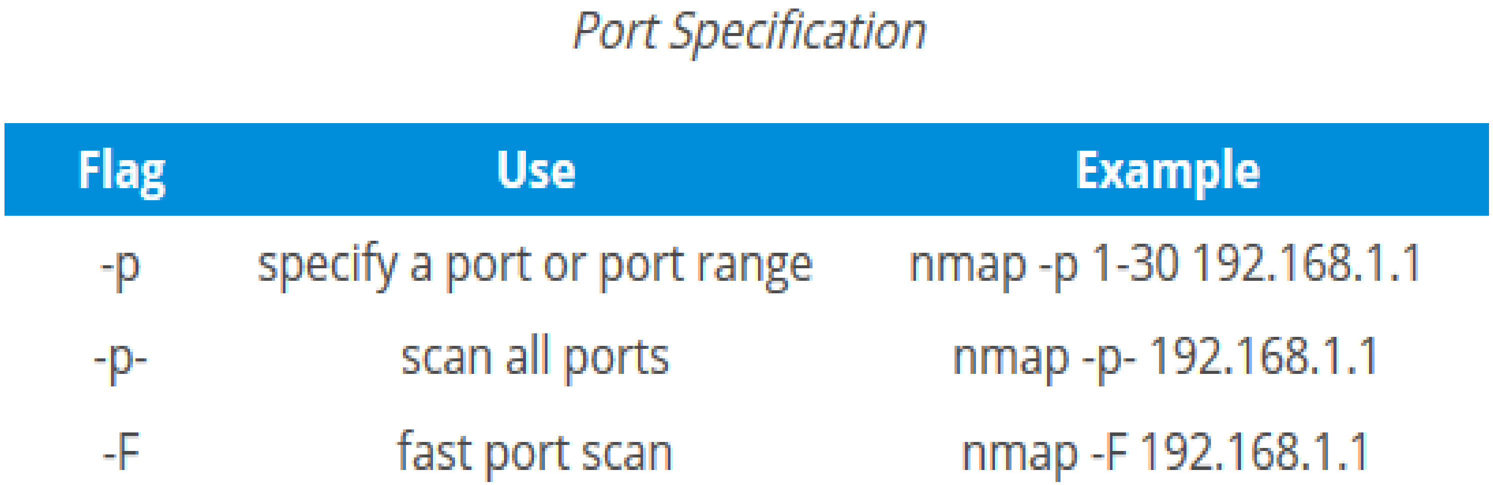
Nmap Commands Cont.



Host Discovery

Flag	Use	Example
-Pn	only port scan	nmap -Pn192.168.1.1
-sn	only host discover	nmap -sn192.168.1.1
-PR	arp discovery on a local network	nmap -PR192.168.1.1
-n	disable DNS resolution	nmap -n 192.168.1.1

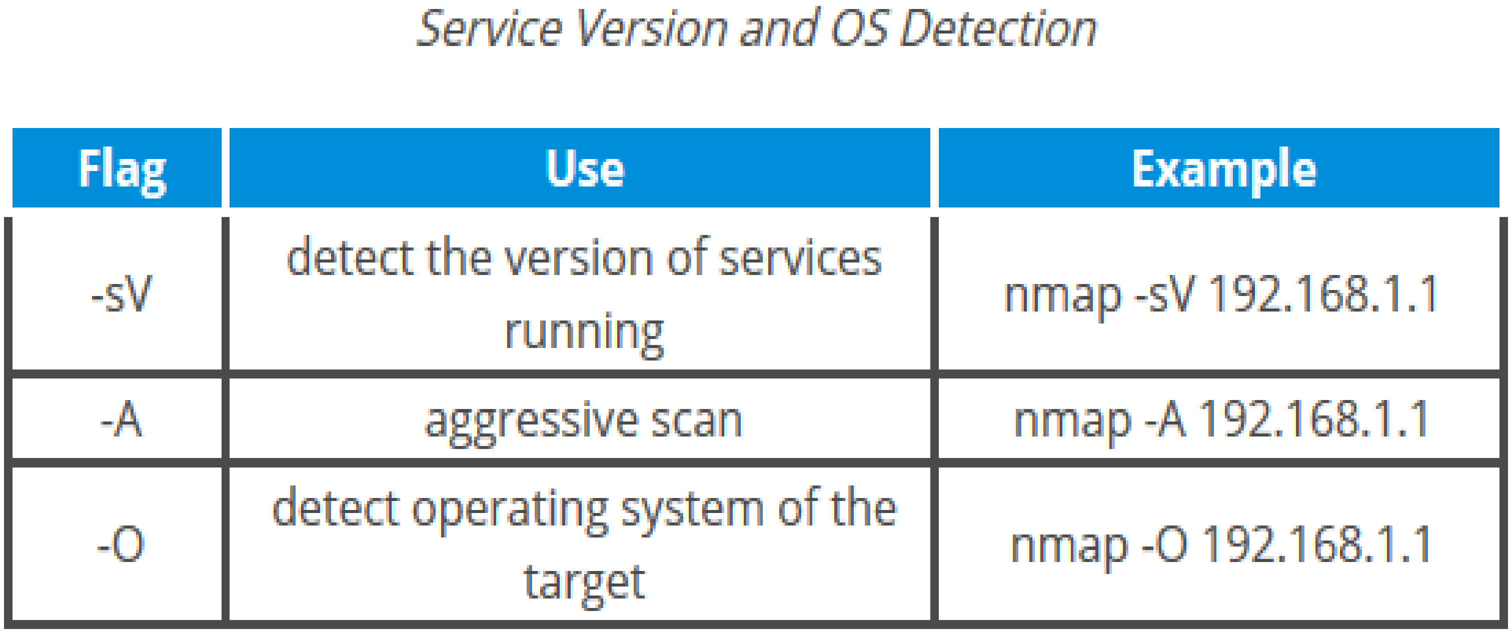
Nmap Commands Cont.



Port Specification

Flag	Use	Example
-p	specify a port or port range	nmap -p 1-30 192.168.1.1
-p-	scan all ports	nmap -p- 192.168.1.1
-F	fast port scan	nmap -F 192.168.1.1

Nmap Commands Cont.



Service Version and OS Detection

Flag	Use	Example
-sV	detect the version of services running	nmap -sV 192.168.1.1
-A	aggressive scan	nmap -A 192.168.1.1
-O	detect operating system of the target	nmap -O 192.168.1.1

Demo