THE UNIVERSITY OF TENNESSEE CHATTANOOGA

NMAP

Mckenzie Mack
GenCyber Workshop

Agenda

- Introduction to NMAP
- Tips for Using NMAP
- Flags and their Uses
- Importance of NMAP as a Tool

Learning Objectives

- Describe how nmap can be used to scan hosts on the network
- Explain how the results of running nmap change when different flags are used
- Explore how nmap relates to the concept of cybersecurity

Introduction to NMAP

- Yesterday, you learned about several different ways to gather information about a network through the command line
- However, one key tool was left out: **nmap**
- nmap: an open source tool used to send packets across a network to gain more knowledge about hosts on a network
  - offered as a GUI for many operating systems
  - for this lesson, nmap will be run through the command line

Introduction to NMAP

- nmap can be used to find out more about a specific host
  - whether the host is active or not
  - latency of the host
  - the amount of time taken to scan the host

```
pi@raspberrypi:~ $ sudo nmap 10.161.238.74
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-29 21:10 EDT
Nmap scan report for Mckenzies-MBP.wireless.utc.edu (10.161.238.74)
Host is up (0.11s latency).
All 1000 scanned ports on Mckenzies-MBP.wireless.utc.edu (10.161.238.74) are filtered (720) or closed (280)

Nmap done: 1 IP address (1 host up) scanned in 3.04 seconds
pi@raspberrypi:~ $
```

Introduction to NMAP

- In the picture on the last slide, you may have seen the line, “All 1000 ports scanned…”
  - What exactly is a port?
    - port: software-based point where information flows from your computer to the Internet or to another host and vice versa
    - each port is associated with a certain service
      - service: application running at the network layer and above that performs certain operations
        - examples: email services, domain name system (DNS) services, Internet access, etc.
- nmap lists the state of each port
  - open, closed, filtered, etc.

Introduction to NMAP

- nmap can also be used to scan a range of addresses

```
pi@raspberrypi:~ $ sudo nmap 10.129.225.100-150
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-29 21:24 EDT
Nmap scan report for 10.129.225.100
Host is up (0.0052s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
8009/tcp open  ajp13
9080/tcp open  glrpc
MAC Address: 0C:EE:99:32:6D:3A (Unknown)

Nmap scan report for Galaxy-S9.wireless.utc.edu (10.129.225.120)
Host is up (0.053s latency).
All 1000 scanned ports on Galaxy-S9.wireless.utc.edu (10.129.225.120) are closed
MAC Address: 8C:45:00:A2:13:A8 (Murata Manufacturing)

Nmap scan report for libhow5373.wireless.utc.edu (10.129.225.122)
Host is up (0.066s latency).
All 1000 scanned ports on libhow5373.wireless.utc.edu (10.129.225.122) are filtered
MAC Address: 08:71:90:76:92:92 (Unknown)

Nmap scan report for 10.129.225.124
Host is up (0.19s latency).
All 1000 scanned ports on 10.129.225.124 are closed
MAC Address: 10:F1:F2:87:9C:74 (LG Electronics (Mobile Communications))
```

Tips for Using NMAP

- Some nmap commands require root privileges
  - to execute a command as the superuser, use the **sudo** command
- Some nmap commands can take minutes to execute
  - to see the progress of a command, press **Enter** as the command is running
    - displays percent completed and amount of time left

```
pi@raspberrypi:~ $ sudo nmap 10.161.238.1-50
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-30 20:45 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 50 undergoing Ping Scan
Ping Scan Timing: About 5.00% done; ETC: 20:46 (0:00:57 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 50 undergoing Ping Scan
Ping Scan Timing: About 57.50% done; ETC: 20:45 (0:00:04 remaining)
Stats: 0:00:06 elapsed; 49 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Stats: 0:00:33 elapsed; 49 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 70.37% done; ETC: 20:45 (0:00:12 remaining)
```

Flags and their Uses

- Many different flags are offered to customize the results of nmap
- ex: **-sP**
  - similar to the **ping** command that you learned yesterday but can be used to ping multiple hosts at once
    - ex: **nmap -sP 10.129.219.0/24** pings 254 different hosts
  - quick way to find out which hosts are up on the network

Flags and their Uses

```
pi@raspberrypi:~ $ sudo nmap -sP 10.129.219.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-30 10:30 EDT
Nmap scan report for 10.129.219.1
Host is up (0.010s latency).
MAC Address: 0C:62:A6:21:87:F7 (Unknown)
Nmap scan report for Amarias-Air.wireless.utc.edu (10.129.219.34)
Host is up (0.056s latency).
MAC Address: A4:83:E7:81:C3:44 (Unknown)
Nmap scan report for EMCS438SP.wireless.utc.edu (10.129.219.47)
Host is up (0.0042s latency).
MAC Address: 98:5F:D3:58:03:74 (Microsoft)
Nmap scan report for EmileesTV.wireless.utc.edu (10.129.219.52)
Host is up (0.010s latency).
MAC Address: 10:3D:0A:07:9D:7C (Unknown)
Nmap scan report for FOU201DL02.wireless.utc.edu (10.129.219.61)
Host is up (0.013s latency).
MAC Address: 64:5A:ED:E9:41:11 (Unknown)
Nmap scan report for 10.129.219.67
Host is up (0.44s latency).
MAC Address: FC:DB:B3:BE:02:0B (Murata Manufacturing)
Nmap scan report for 10.129.219.75
Host is up (0.010s latency).
```

Flags and their Uses

- **-O**: compares response of host to database of operating systems to identify the host's OS and its version

```
pi@raspberrypi:~ $ sudo nmap -O  10.129.225.124
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-29 21:37 EDT
Nmap scan report for 10.129.225.124
Host is up (0.014s latency).
All 1000 scanned ports on 10.129.225.124 are closed
MAC Address: 10:F1:F2:87:9C:74 (LG Electronics (Mobile Communications))
Device type: remote management|phone|general purpose|webcam|storage-misc
Running: Avocent embedded, Google Android 2.X, Linux 2.6.X|3.X, AXIS embedded, ZyXEL embedded
OS CPE: cpe:/o:google:android:2.2 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.6.17
a cpe:/o:linux:linux_kernel:3.13 cpe:/h:zyxel:nsa-210
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.62 seconds
```

Flags and their Uses

- **-sV**: displays the service version of services used by the host
  - only displays the version of services associated with open ports

```
pi@raspberrypi:~ $ sudo nmap -sV utc.edu
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-30 21:27 EDT
Nmap scan report for utc.edu (172.19.31.14)
Host is up (0.023s latency).
rDNS record for 172.19.31.14: www.utc.edu
Not shown: 996 filtered ports
PORT     STATE  SERVICE     VERSION
80/tcp   open   http-proxy  F5 BIG-IP load balancer http proxy
443/tcp  open   ssl/http    nginx
5222/tcp closed xmpp-client
8080/tcp closed http-proxy
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.61 seconds
pi@raspberrypi:~ $
```

Flags and their Uses

- By default, nmap scans the top 1000 ports of a host
- **-p** can be used to scan specific ports for hosts on a network
  - format: **-p n** where **n** is one or more port numbers
  - if you are not sure which port number you are looking for, you can also filter by the name of the service
    - ex: **nmap -p ssh 10.121.3.3**
  - useful for identifying certain devices
    - ex: an IP address with port 80 open could be a web server

Flags and their Uses

```
pi@raspberrypi:~ $ sudo nmap -p 80 10.161.238.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-30 21:11 EDT
Nmap scan report for 10.161.238.33
Host is up (0.047s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for Mckenzies-MBP.wireless.utc.edu (10.161.238.74)
Host is up (0.088s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for Seths-iPhone.wireless.utc.edu (10.161.238.84)
Host is up (0.012s latency).

PORT   STATE  SERVICE
80/tcp closed http
```

Flags and their Uses

- Nmap offers many more flags for you to use!
  - use **nmap -h** or **man nmap** to see more options

Importance of NMAP as a Tool

- Why is NMAP an important tool in terms of security?
  - It helps network administrators:
    - perform pen testing
    - find out more information about malicious hosts on the network
    - detect common vulnerabilities across the network

- **Remember:** If you can use nmap to detect vulnerabilities in a network, so can an attacker

Resources

NMAP official website: https://nmap.org/
Using NMAP scripts to find network vulnerabilities:
https://www.youtube.com/watch?v=3U1pJ-eJrAU
An introduction to NSE:
https://www.youtube.com/watch?v=ceGywKe8RnY

LAB

- complete the questions for Lab - NMAP Practice