IASA 10/04/19 – NMAP/PORTS/NETSTAT

DON'T FORGET TO SIGN IN!

AGENDA

- MAKE SURE YOU SIGN IN AND GRAB SOME PIZZA!
- GO OVER PORTS AND SERVICES
- GO OVER TCP AND UDP
- GO OVER NMAP – HOW IT WORKS, WHY WE USE IT, ETC.
- RUN NMAP – LIVE DEMO

WHAT ARE PORTS?

Ports are like appt. Numbers, although they share the same address, the traffic needs to go to specific rooms.

Ports are included in the ethernet frame and generally determine the type of traffic as well as make it easier for firewall admins to block certain types of traffic and for applications to work with the traffic.

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

This Photo by Unknown Author is licensed under CC BY-ND

WHAT ARE MOST COMMON PORTS?

Most Notable ports:

20 – FTP
21 – FTP Start
22 – SSHSecure Socket Shell
23 – Telnet is used to connect to devices.
25 – SMTP (Simple Mail Transfer Protocol)
53 – DNS
67/68 – DHCP
80 – HTTP (Hyper Text Transfer Protocol)
88 – Kerberos
110 – POP mail (retrieval of mail)
123 – Time Service
143 – iMAP
443 – HTTPS (HTTP with ssl)
445 – SMB (Server Message Block)
3389 – RDP (Remote Desktop Protocol)
5800/5900 – VNC(Virtual Network Computing)
8080 – Web Server

TCP/UDP PROTOCOLS

- UDP does not establish a connection or even acknowledge the client-side host.
- TCP acknowledges the client-side host and check/acknowledges all sent packets to make sure spoofing hasn't

- UDP(One way road)
- TCP(Two way road)

WHAT IS NMAP

- Port scanner, security scanner and network exploitation tool.
- Used to show open ports, services running on those ports, OS/version detection, etc, within a specified IP address(s).
- Zenmap is the GUI version – runs on windows, mac OS X, and almost all linux distros.

ROOT

For most nmap commands you will need to have root privileges. It is recommended to use sudo instead of logging into root. (this is good practice)

`su -` - log into root (BE CAUTIOUS)

`sudo` - command to run as root

`sudo !!` - if you forget sudo run this to re-run the previous command as root

INSTALLING NMAP

```
apt install nmap – Debian based linux
```

```
yum install nmap – Redhat based linux
```

```
Brew install nmap – Mac OS x
```

BASIC NMAP COMMANDS

`nmap 192.168.1.1` - scan single IP

`nmap www.emuiasa.com` - scan a domain

`nmap 192.168.1.0/24` - scan a subnet

`nmap 192.168.1.0-254` - scan a range of IP

`nmap -iL *.txt doc with ip’s*` - scan from a file

`ipcalc 192.168.1.1` – Calculate subnet / range of ip’s

BASIC NMAP PORT COMMANDS

```
nmap -p 22 192.168.1.1 – specified ports
nmap -p 1-200 192.168.1.1 – scan range of IP’s
nmap -p- 192.168.1.1 – scan all ports
nmap -F 22 192.168.1.1 – ‘fast’ scan
```

BASIC NMAP PORT COMMANDS

```
nmap -sU -p- 192.168.1.1  – scan UDP ports
nmap -sS -p- 192.168.1.1  – scan with TCP SYN
nmap -sT -p- 192.168.1.1  – scan with TCP connect
```

```
* -p- scanning all ports *
```

NMAP OS/SERVICE DETECTION COMMANDS

```
nmap -A 192.168.1.1 – OS and service detection
nmap -sV 192.168.1.1 – service detection(common)
nmap -sO 192.168.1.1 – OS detection(common)
```

NMAP OUTPUTING TO A FILE

```
nmap -oN filename.txt 192.168.1.1 - Output to .txt
nmap -oX filename.xml 192.168.1.1 - Output to .xml
nmap -oG filename.txt 192.168.1.1 - Output in grep
nmap -oA filename 192.168.1.1 - output in a formats
```

NMAP SCRIPTS

nmap -sV -sC 192.168.1.1 – scan using safe scripts

nmap --script-help=*scriptname* – help with scripts

locate nse | grep script – locates and displays the available scripts

* -sV service detection before running scripts *

* Locate is used to locate files within linux *

* | grep pipe the info into grep to be printed out if it includes ‘script’ *

NMAP GOOD TRICKS

-PN - drop the initial ping in case you have a firewall causing you issues.

-D

NETSTAT

- Utility that shows network connections for TCP, UDP, Routing tables, and network statistics.
- Built into almost all OS's
- We us this to find out whose connected and/or trying to connect.

NETSTAT

```
Netstat -t   - check TCP connections
Netstat -u   - check UDP connections
Netstat -s   - print network statistics
Netstat -n   - show numerical values
Netstat -p   - show PID/processes
Netstat -l   - show “Listening” processes
```

- –n and –p can be used cohesively with –t and -u *
- Example(netstat –tulpn) *Demo

DEMO TIME

- Login to GCP(google cloud) & startup your VM.
- Teams of 2
  - 1 person netstat
  - 1 person nmap

DEMO NMAP

Lets run an nmap scan against our partners VM.

```
nmap –F –A -oG results [ip address]
```

put the ip address of your partners VM

DEMO NMAP

```
cat results
```

Now we can see what ports, and services are open on your partners VM. In grep format.

DEMO NMAP

```
nmap –F –A -oG results [ip address] –D 10.0.0.1,10.0.0.2,10.0.0.3
```

Here we are being discrete, by this we are spoofing our IP to the ones we designated. This prevents for example a firewall blocking us from scanning open ports.(being banned)