

John Gavigan
IST 451
04/09/2023

Network Mapping Lab

Exercise 1 - Scanning with Nmap

Task 1: Scan using CIDR notation

Step 1:

```
ubuntu@PLABUBNTU: ~  
ubuntu@PLABUBNTU:~$ docker container list  
CONTAINER ID   IMAGE      COMMAND                  CREATED        STATUS  
PORTS  
NAMES  
4e23e1a85198   lab-base   "/bin/bash"             55 minutes ago Up 55 m  
1nutes        192.168.0.113:22->22/tcp, 192.168.0.113:443->443/tcp, 192.168.0.113:9001->  
9001/tcp, 192.168.0.113:9030->9030/tcp  
baddie3
```

Step 2:

```
kali@Kali: ~  
File Actions Edit View Help  
kali@Kali:~$ nmap 192.168.0.0/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-09 11:10 EDT  
Nmap scan report for Kali (192.168.0.1)  
Host is up (0.00036s latency).  
All 1000 scanned ports on Kali (192.168.0.1) are closed  
  
Nmap scan report for 192.168.0.2  
Host is up (0.00079s latency).  
All 1000 scanned ports on 192.168.0.2 are closed  
  
Nmap scan report for 192.168.0.12  
Host is up (0.00081s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
  
Nmap scan report for 192.168.0.13  
Host is up (0.00067s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
3306/tcp   open  mysql  
  
Nmap scan report for 192.168.0.14  
Host is up (0.00068s latency).
```

Step 3:

```
kali@Kali: ~  
File Actions Edit View Help  
  
Nmap scan report for 192.168.0.250  
Host is up (0.0022s latency).  
All 1000 scanned ports on 192.168.0.250 are closed  
  
Nmap done: 256 IP addresses (27 hosts up) scanned in 45.04 seconds  
kali@Kali:~$ nmap 192.168.0.2-150 -p --open  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-09 11:32 EDT  
Error #486: Your port specifications are illegal. Example of proper form:  
"-100,200-1024,T:3000-4000,U:60000-"  
QUITTING!  
kali@Kali:~$ nmap 192.168.0.2-150 -p 80 --open  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-09 11:34 EDT  
Nmap scan report for 192.168.0.125  
Host is up (0.00090s latency).  
  
PORT      STATE SERVICE  
80/tcp    open  http
```

Step 4:

```
kali@Kali: ~  
File Actions Edit View Help  
  
kali@Kali:~$ nmap 192.168.0.2-150 -p 1024-65535  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-09 11:41 EDT  
Nmap scan report for 192.168.0.2  
Host is up (0.0031s latency).  
All 64512 scanned ports on 192.168.0.2 are closed  
  
Nmap scan report for 192.168.0.12  
Host is up (0.00073s latency).  
All 64512 scanned ports on 192.168.0.12 are closed  
  
Nmap scan report for 192.168.0.13  
Host is up (0.00068s latency).  
Not shown: 64511 closed ports  
PORT      STATE SERVICE  
3306/tcp  open  mysql  
  
Nmap scan report for 192.168.0.14  
Host is up (0.00062s latency).  
Not shown: 64510 closed ports  
PORT      STATE SERVICE  
1433/tcp  open  ms-sql-s  
1434/tcp  open  ms-sql-m
```

Step 5: identify active hosts on network and what services they are running
(Diagram below)

```
Nmap scan report for 192.168.0.13
Host is up (0.00068s latency).
Not shown: 64511 closed ports
PORT      STATE SERVICE
3306/tcp   open  mysql
```

```
Nmap scan report for 192.168.0.14
Host is up (0.00062s latency).
Not shown: 64510 closed ports
PORT      STATE SERVICE
1433/tcp   open  ms-sql-s
1434/tcp   open  ms-sql-m
```

```
Nmap scan report for 192.168.0.117
Host is up (0.0036s latency).
Not shown: 64511 closed ports
PORT      STATE SERVICE
4000/tcp   open  remoteanything
```

```
Nmap scan report for 192.168.0.125
Host is up (0.0039s latency).
Not shown: 64507 closed ports
PORT      STATE SERVICE
3910/tcp   open  prnrequest
3911/tcp   open  prnstatus
8080/tcp   open  http-proxy
9100/tcp   open  jetdirect
9220/tcp   open  unknown
```

```
Nmap scan report for 192.168.0.129
Host is up (0.0037s latency).
Not shown: 64511 closed ports
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server
```

```
Nmap scan report for 192.168.0.100
Host is up (0.0041s latency).
Not shown: 64511 closed ports
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server
```

```
Nmap scan report for 192.168.0.132
Host is up (0.0022s latency).
Not shown: 64511 closed ports
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server
```

```
Nmap scan report for 192.168.0.104
Host is up (0.0041s latency).
Not shown: 64511 closed ports
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server
```

```
Nmap scan report for 192.168.0.113
Host is up (0.0032s latency).
Not shown: 64510 closed ports
PORT      STATE SERVICE
9001/tcp   open  tor-orport
9030/tcp   open  unknown
```

```
Nmap scan report for 192.168.0.114
Host is up (0.0016s latency).
Not shown: 64510 closed ports
PORT      STATE SERVICE
5900/tcp   open  vnc
5901/tcp   open  vnc-1
```

```
Nmap scan report for 192.168.0.116
Host is up (0.0021s latency).
Not shown: 64509 closed ports
PORT      STATE SERVICE
5001/tcp   open  complex-link
9100/tcp   open  jetdirect
9600/tcp   open  micromuse-ncpw
```

```
Nmap scan report for 192.168.0.136
Host is up (0.0013s latency).
Not shown: 64507 closed ports
PORT      STATE SERVICE
3910/tcp   open  prnrequest
3911/tcp   open  prnstatus
8080/tcp   open  http-proxy
9100/tcp   open  jetdirect
9220/tcp   open  unknown
```

```
Nmap scan report for 192.168.0.138
Host is up (0.0036s latency).
Not shown: 64511 closed ports
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server
```

```
Nmap scan report for 192.168.0.145
Host is up (0.0046s latency).
Not shown: 64510 closed ports
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server
25565/tcp  open  minecraft
```

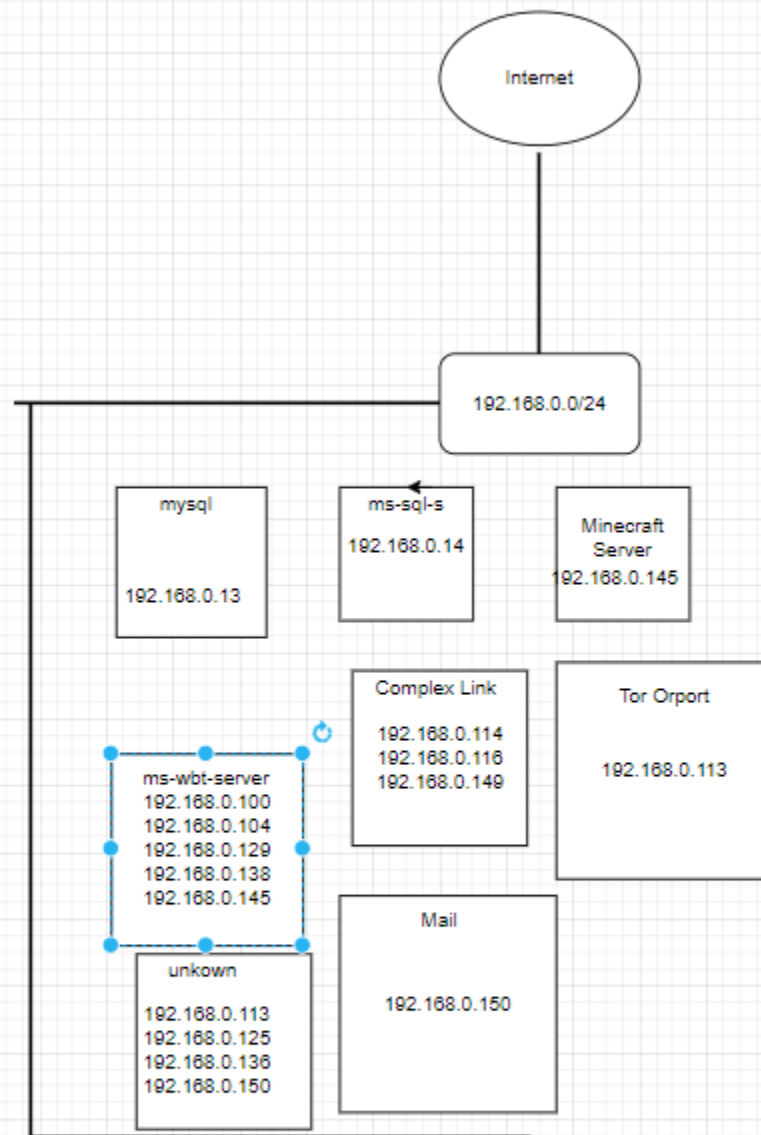
```
Nmap scan report for 192.168.0.149
Host is up (0.0027s latency).
Not shown: 64510 closed ports
PORT      STATE SERVICE
2501/tcp   open  rtsclient
5001/tcp   open  complex-link
```

```

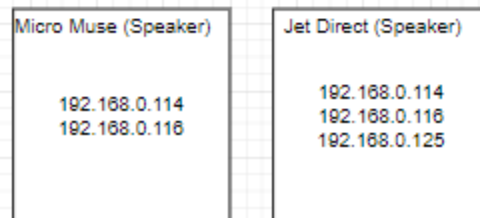
Nmap scan report for 192.168.0.150
Host is up (0.0034s latency).
Not shown: 64509 closed ports
PORT      STATE SERVICE
8080/tcp  open  http-proxy
9091/tcp  open  xmltec-xmlmail
51413/tcp open  unknown

```

Servers



Devices



Exercise 2: Document Findings

Task1: Write a report

1. Through the use of nmap, I was able to scan the network located on the 192.168.204.0/24 subnet and identify its ports and the activity on said ports.
2. Above is a network diagram
3. Lists of hosts in the network

1

```
      3306/tcp mysql
192.168.0.14
      1433/tcp ms-sql-s
      1434/tcp ms-sql-m
192.168.0.100
      3389/tcp ms-wbt-server
192.168.0.104
      3389/tcp ms-wbt-server
192.168.0.113
      9001/tcp tor-orport
      9030/tcp unknown
192.168.0.114
      5001/tcp complex-link
      9100/tcp jetdirect
      9600/tcp micromuse-ncpw
192.168.0.116
      5001/tcp complex-link
      9100/tcp jetdirect
      9600/tcp micromuse-ncpw
192.168.0.117
      4000/tcp remoteanything
192.168.0.125
      3190/tcp prnrequest
      3911/tcp prnstatus
      8080/tcp http-proxy
      9100/tcp jetdirect
      9220/tcp unknown
192.168.0.129
      3389/tcp ms-wbt-server
192.168.0.136
      3190/tcp prnrequest
      3911/tcp prnstatus
      8080/tcp http-proxy
      9100/tcp jetdirect
      9220/tcp unknown
192.168.0.138
      3389/tcp ms-wbt-server
```

192.168.0.145

3389/tcp ms-wbt-server

25565/tcp minecraft

192.168.0.149

2501/tcp rtsclient

5001/tcp complex link

192.168.0.150

8080/tcp http-proxy

9091/tcp xmltec-xmlmail

51413/tcp unknown

4. There were several indicators of compromise. A few of the ports were only labeled as "unknown" and there were also several complex links running on port 5001, which should be secured.