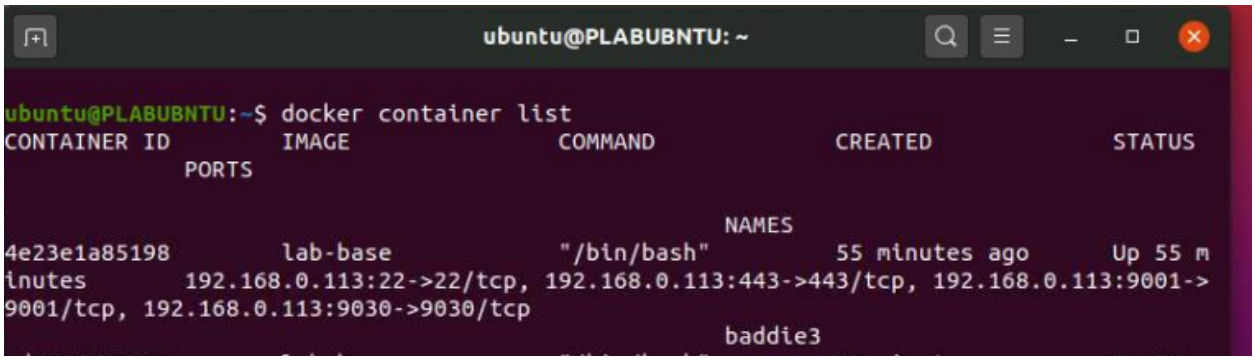
John Gavigan
IST 451
04/09/2023

Network Mapping Lab

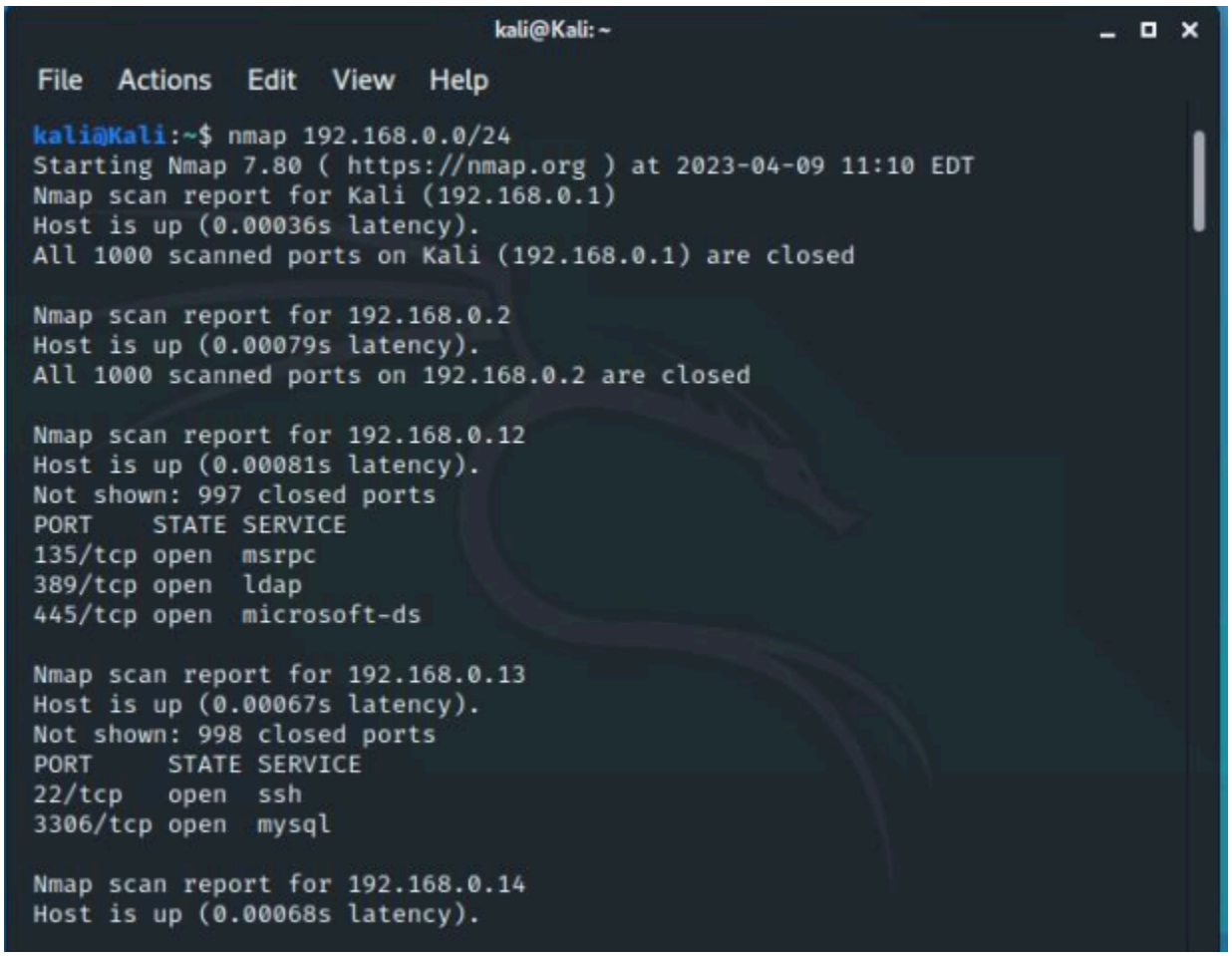
Exercise 1 - Scanning with Nmap

Task 1: Scan using CIDR notation

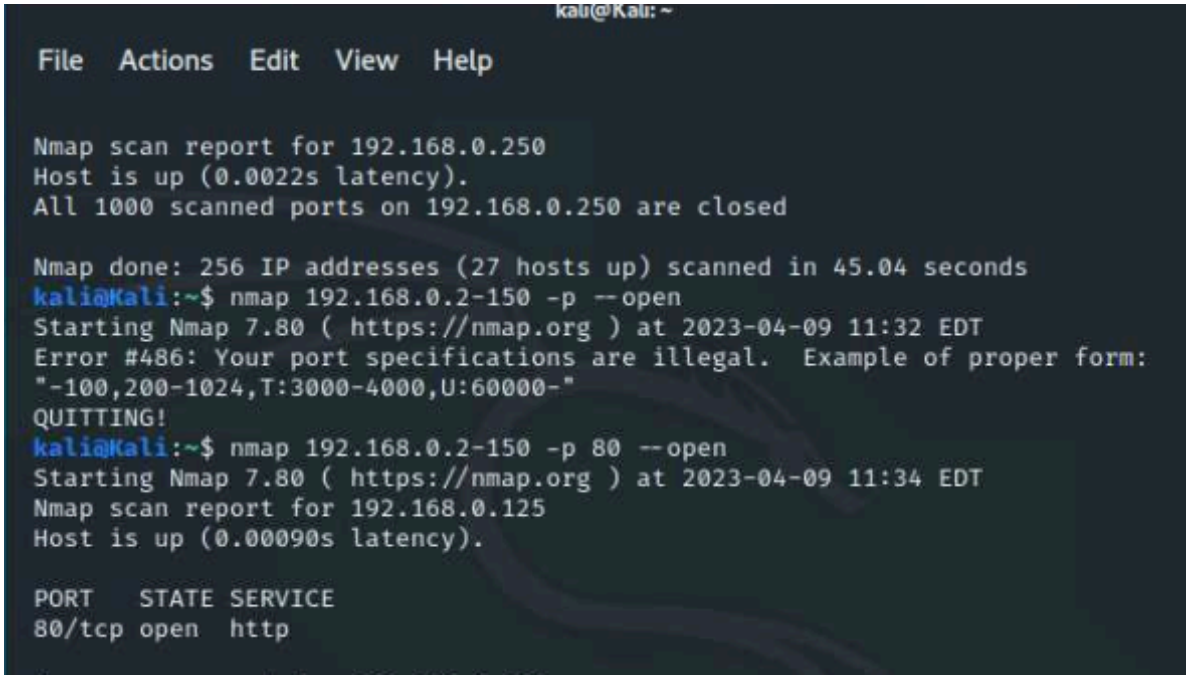
Step 1:



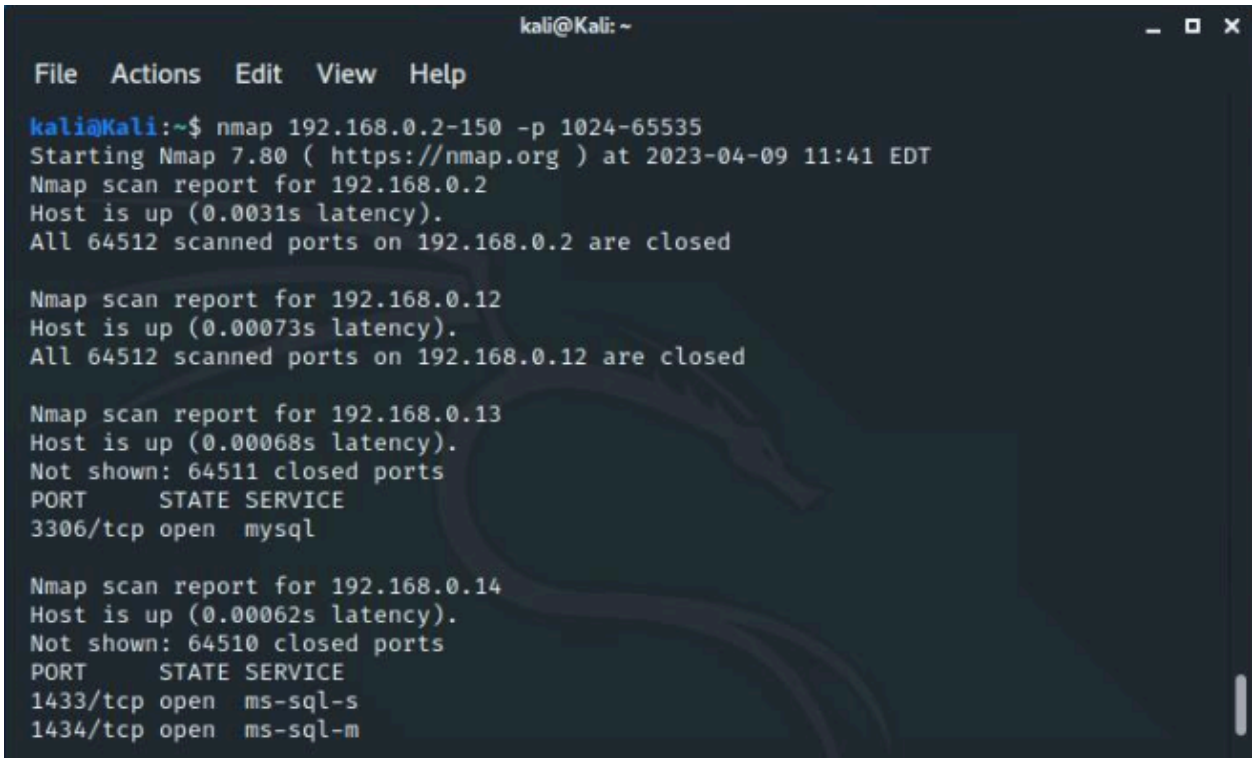
Step 2:



Step 3:



Step 4:



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

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

Nmap scan report for 192.168.0.132
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  commplex-link
9100/tcp open  jetdirect
9600/tcp open  micromuse-ncpw
```

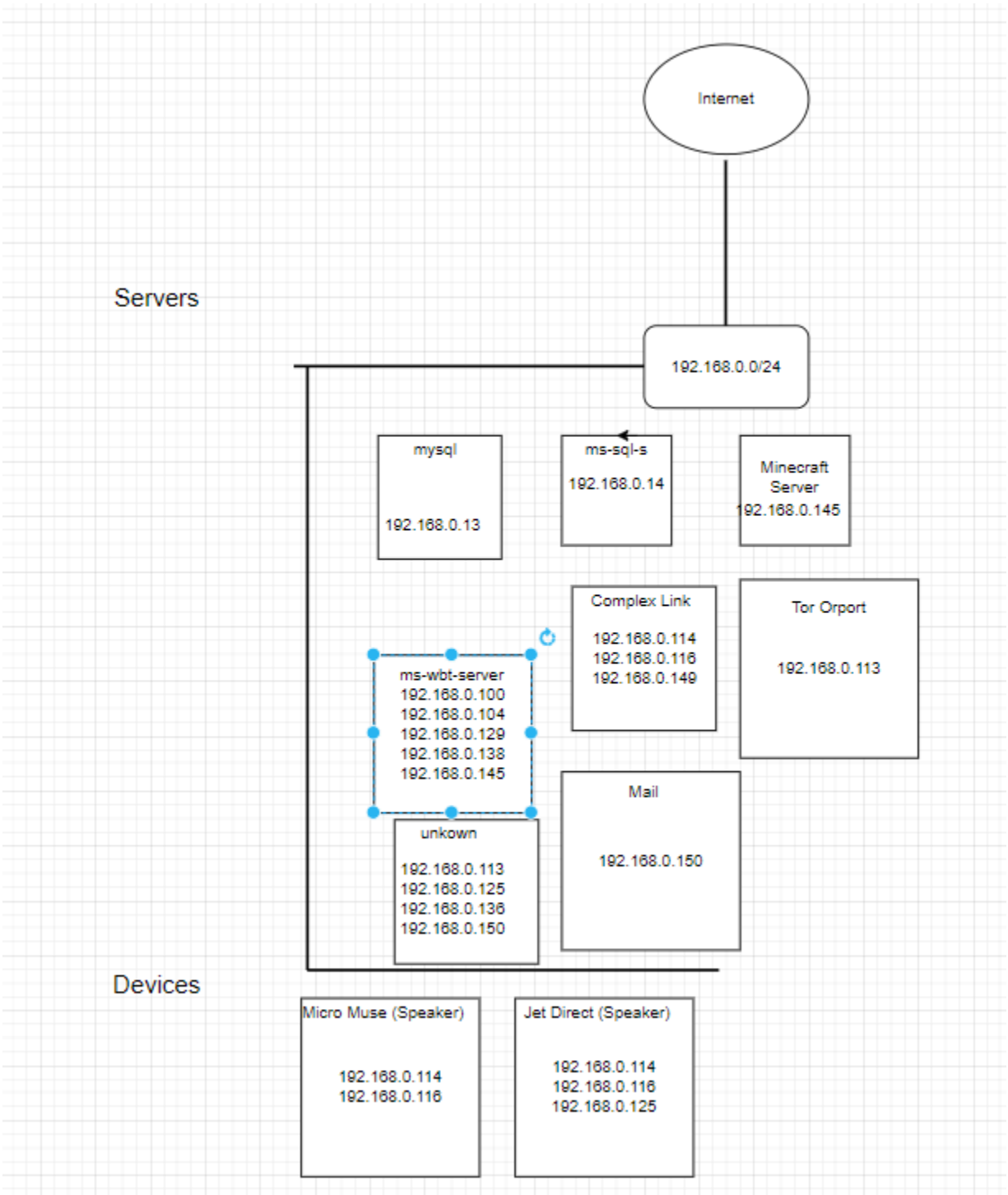
```
Nmap scan report for 192.168.0.136
Host is up (0.0013s latency).
Not shown: 64507 closed ports
PORT     STATE SERVICE
3910/tcp open  prnrequest
3911/tcp open  prnstatus
8080/tcp open  http-proxy
9100/tcp open  jetdirect
9220/tcp open  unknown

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  commplex-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
```



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 commplex 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.