NCAE 3 Meeting Recap

MikroTik Router Config:

Default Credentials:　　　**u:admin**　　　**p:(no password, just press Enter)**

```
ip
/ip interface print
```

Make note of what interfaces are on the router (for example, ether5 and ether6)

```
/ip address add address=172.20.t.1/16 int=ether5
```

In this case, ether5 will act as outbound interface,

```
/ip address add address=192.168.t.1/24 int=ether6
/ip address print
/
```

/ will move back directories to root directory, if ever lost use tabbing to find out avail commands

At this point, this is technically all the terminal usage you need for the MikroTik Router, as it comes with a web interface for additional rules and setting up NAT translation, port forwarding, etc…   Just keep in mind that the web interface is hosted originally on HTTP, so if anyone logs into it, a credential change should be in place.

Ubuntu Network Config:

```
sudo nano /etc/netplan/01-...yaml
```

Don't remember the full filename but there should only be one file in the directory. Also use whatever text editor you want, i just think nano is the friendliest for this use case, just modifying a few lines in the yaml file. Also take note that yaml is very character sensitive, don't use tabs for spacing…

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens18:
    addresses:
      - 192.168.t.2/24
    gateway4: 192.168.t.1
```

After configuration, restart service

```
sudo netplan apply
```

After this point, if you want to access the web interface for the router, open a browser and type
http://172.20.t.1:8080 *(it is a HTTP connection at first!)*
At this point go take a look at what the interface has to offer, probably also change router credentials, change web port to be over something more secure, and enable all ur awesome security rules and requirements!!

Kali Network Config:

```
sudo nano /etc/network/interfaces
```

In this machine, network is managed my networking.service, not like netplan in ubuntu, other then that though, the rest of the set up is basically the same, slight different syntax

```
# comment1
Source /etc/network/interfaces.d/*
# comment2
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
      address 192.168.128.100
      netmask 255.255.255.0
```

after making changes, restart networking service

```
sudo systemctl restart networking
```

Basic Network Map and Scoring Distribution:

Internet

Scoring Engines

DNS
172.18.0.12

Remote Shell
172.18.13.15

Certificate Authority
172.18.0.38

172.18.0.0/16

Hackathon Router
172.18.0.1

Blue Team VMs

eth0 172.18.13.t

Team Router

eth1 192.168.t.1

172.18.14.t
Shell / FTP

172.18.15.t[1-4]
External Kali VMs
(DHCP Assigned)

Team Infrastructure

Blue Team LAN
192.168.t.0/24

192.168.t.5
Web Server

192.168.t.7
Database

192.168.t.12
DNS

192.168.t.15
Backup

192.168.t.10[1-6]
Internal Kali VMs

t = team number

Router:
500 if pingable

Web:
1500 if website displays correct
2000 if SSL certificate is working

DB:
1000 if user can use SQL commands
500 if user connect via SSH

DNS:
500 if can connect SSH internal
500 if internal DNS is correct
500 if external DNS is correct

FTP:
1500 if default files exist and pash checksum
500 if users can connect via SSH
500 if users are able to create files
500 if users can login via FTP

Infrastructure Total:
10,000 points
CTF Challenges:
2,000 points