NCAE Notes

17 FEB Meeting One

Tutorial

1. Ping tutorial.packetmanping.com

Static, ports, and services

1. Remove Connection Profile
2. Set the ip address to 192.168.23.7, netmask 255.255.255.0
3. Head to http://192.168.23.101 on firefox
4. Set the ip address to 192.168.42.7, netmask 255.255.255.0
    a. Sudo su, password → password
    b. cd /etc/ssh, nano sshd_config
    c. Change the listen address to 192.168.42.7
    d. Sudo systemctl restart sshd

21 FEB Meeting Two

DHCP 1

Dynamic Host Configuration Protocol - allows you to assign IP addresses automatically

1. Assign 192.168.3.66, netmask 255.255.255.0 to your Ubuntu machine

b. SSH into 192.168.3.1, password is ‘password’

```
ssh root@192.168.3.1
```

c. Change directory into /etc/dhcp
d. Nano dhcpd.conf
e. Change the subnet and netmask
f. Restart dhcpd
g. Visit 192.168.3.100 on Firefox

DHCP 2

Make DHCP server assign Ubuntu2 a new IP address

a. Ping 192.168.3.100
b. Arp -a (get MAC address)

c. SSH into 192.168.3.1
d. cd /etc/dhcp
e. Nano dhcpd.conf
f. uncomment lines host-rrc, IP address, MAC address, and bottom bracket
g. transfer the MAC address from 192.168.3.100
h. IP address is 192.168.3.200
i. Save file
j. systemctl restart dhcpd
k. SSH root@192.168.3.200
l. cat flag

24 FEB Meeting Three

Subnetting and Firewalls

The Class C network is split into 8 subnets .0 → .224

255.255.255.0 → 256 addresses

Split into 8 subnets → 32 addresses

(32*(n-1))

/24 → 111111111.111111111.111111111.0000000

/27 → 111111111.111111111.111111111.11100000

0-31 1st Subnet

32-63

64

96

128

160-191 6th Subnet

a. Set IP address to 192.168.99.161 and subnet to 255.255.255.224
b. cd /etc/ssh
    a. sudo nano sshd_config
    b. Change listen address: 192.168.99.161 and save.
    c. sudo systemctl restart ssh
c. ufw deny from 192.168.99.0/24
d. ufw allow from 192.168.99.160/27
e. ufw enable
f. Check files → Videos folder → flag

g. **If you are working on problem 7 right after, “sudo ufw disable”**

Websites and DNS

1. Configure SSH with 192.168.5.123 255.255.255.0
2. Move www.packetmanping.com.backup to /var/www/html/index.html

```
mv www.packetmanping.com.backup /var/www/html/index.html
```

1. cd /var/www/html, cat index.html (should say packetman is here)
2. ssh root@192.168.5.250
3. cd /etc/named/zones
4. nano forward.packetmanping.com
5. Change IP address 192.168.5.77 to 192.168.5.123
6. nano reverse.packetmanping.com
7. Change number 77 to 123
8. CD back into /etc
9. nano resolv.conf
10. Add “nameserver 192.168.5.250” to the file
11. systemctl restart named
12. Go back to 192.168.5.123
13. cd /home/packetmanping
14. ls and see if dnsflag has popped up

28 FEB

1. Login using bill:password
2. curl -k https://172.19.0.1/index.php

My notes from world of bills

Check version of CentOS:

`cat /etc/centos-release`

1. How to assign an IP address on CentOS

Learn Vim: https://danielmiessler.com/study/vim/

Assign static IP: https://www.linkedin.com/pulse/easy-guide-assign-static-ip-address-centos-rhel-7-8-linux-techlab/

> IP addr:

> Subnet Mask:

Change into root

```
sudo su
```

Change into systems internals directory for network configuration

```
cd /etc/
cd sysconfig
cd network-scripts
```

Configure the interface for ethernet0

```
sudo su
vim ifcfg-eth0
```

or

```
sudo su
vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

2.

pt 1: Create a privileged account for yourself

```
adduser [username]
passwd [username]
usermod -a -G wheel [username]
```

pt 2: Disable (don't delete) an account on CentOS

- Lock the user

```
usermod -L [username]
```

- Unlock the user

```
usermod -U [username]
```

- Disable the user

```
vim /etc/passwd
```

Change login shell [/bin/bash] to [/sbin/nologin]

Activity Three

Activity 4

- **Create jrice account —>** sudo useradd jrice

    - Add privileges to jrice —> sudo usermod -g wheel jrice
    - **Optional password —>** sudo passwd jrice
- Login into the jrice account and **cd ~**
- **Setting up /home/jrice/.ssh/authorized_keys**
    - **Make .ssh directory —>** mkdir ~/.ssh
    - Change ownership —> sudo chown jrice:jrice /home/jrice/.ssh
    - **Create authorized keys file —>** touch ~/.ssh/authorized_keys
    - Change ownership —> sudo chown jrice:jrice /home/jrice/.ssh/authorized_keys
- **Copy public key to authorized_keys —>** curl -k -o ~/.ssh/authorized_keys https://172.19.0.1/data/id_rsa_jrice.pub

Mini Hacks

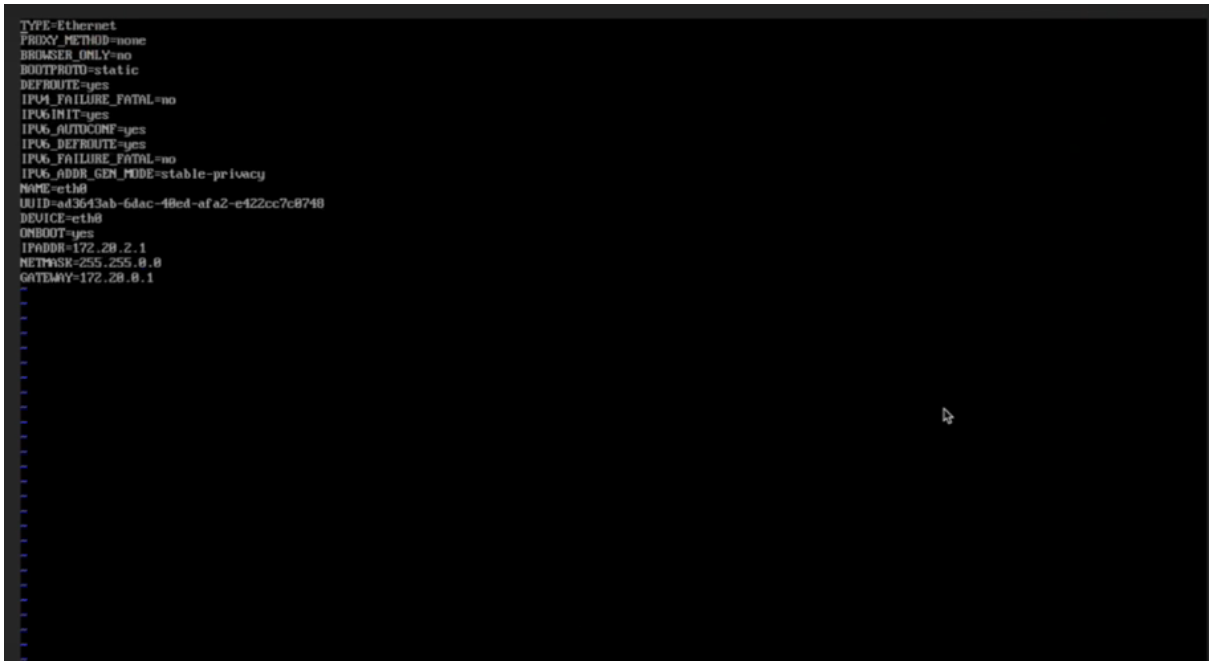
Setting up router

- Open `external kali` box and go to the browser.
    - Open `external kali` box and go to the browser.
    - In one of the bookmarks, there's a `scoreboard` bookmark then click on it.
    - On the top right, click on login and enter username and password.
        - Username: sandbox
        - Password: password
    - Hover over the top right and click on dashboard.
    - On the top that'll be your team number (used for ip addresses)
- In one of the bookmarks, there's a `scoreboard` bookmark then click on it.
- On the top right, click on login and enter username and password.
    - Username: sandbox
    - Password: password
- Hover over the top right and click on dashboard.
- On the top that'll be your team number (used for ip addresses)
- Go to the centos box and login.
- `cd /etc/sysconfig/network-scripts`
- `sudo vi ifcfg-eth0`
    - Configure eth0 accordingly

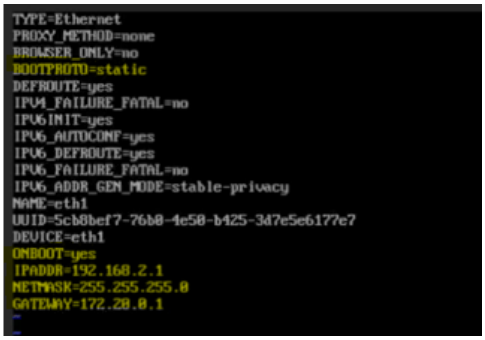
eth0 Configuration

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=eth0
DEVICE=eth0
ONBOOT=no
```

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=eth0
DEVICE=eth0
ONBOOT=yes
IPADDR=172.20.<TEAM #>.1
NETMASK=255.255.0.0
GATEWAY=172.20.0.1
```



- `sudo vi ifcfg-eth1`
- Address: 192.168.<team #>.1



- When you've made and saved your changes, `systemctl restart network`

- Go to `ubuntu desktop` VM and configure static ip address.
- On the top right, click on the icons and click on wired.
- Click on the gear box and set the connection to **manual**
- Change ip address: 192.168.<team #>.2
  - Change netmask: 255.255.255.0
  - Change gateway: 192.168.<team #>.1
- `sudo systemctl restart apache2`
- Go to centos VM, enable ip forwarding.

```
cd /etc
sudo vi sysctl.conf
```

- To the file add this text:

> net.ipv4.ip_forward=1

- Exit out of file.
- Type these commands:

```
sudo sysctl -p
sudo sysctl --system
```

- and add these iptables rules

```
sudo iptables -F
sudo iptables -F -t nat
sudo iptables -t nat -A PREROUTING -d 172.20.<team_num>.1 -p tcp --dport 80 -j DNAT --to-destination 192.168.<team_num>.2:80
sudo iptables -t nat -A POSTROUTING -j MASQUERADE
```

- Go back ubuntu desktop.
- cd /var/www/html
- Change the content of index.html:
  - sudo nano index.html
- Change “team0” to “team<number>”

Extra Resources

https://docs.google.com/document/d/1PEzDskD6JPvAzcW-BrULrbiY7AsXWP2qwjr_yX37hZ8/edit?usp=sharing

Things we need to learn:

Setting up IP Addresses on Ubuntu and CentOS

Setting up a mock environment

- Bash, particularly awk, sed
- Anti red teaming strategies
- Hardening

Things to do:

- Ask NCAE organizers about checklists

They gave us a sneak peek:

- Password
- Users
- File permissions, owner, file name

- Passwords / User permissions
- Static IP
- Nmap 127.0.0.1