Cyber Defense Organization

Spring 2019 - Intro to Specialties

Linux

3 characteristics

- Flexible
  - Learn new technologies quickly
  - Adapt to changing environments
- Motivated
  - Constantly learning, in and out of classroom
  - Wanting to know more - going in depth
- Persistent
  - Troubleshooting wears a person down
  - Takes time, dedication and practice
  - *Never* be afraid to ask questions/say you don't know

SERVICES

SYSADMIN

Manager of services - more developer oriented

Tasks:

Upkeep of services

- web (http,https) - apache, nginx
- ftp - vsftpd, proftpd
- dns - bind
- and more...

Hardening of services

- Patching
- Secure Configuration

Spends 99% of time on help forums and reading documentation

Managing of systems

Tasks:

User Management

- adding/deleting/segmentation etc.

Authentication of users

- Policy, encryption, secure protocols

Networking

- Ip-addressing, host based firewalls,

System integrity

- Secure configurations
- File integrity checks
- Backups

Windows - not just for houses*

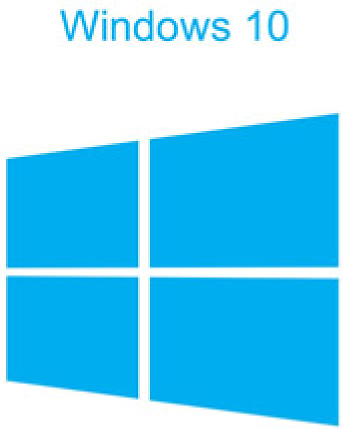
Windows makes the business world go round. Employees and users need to be able to access their workstation to get their job done.

Windows Server Administrators are concerned with the team. “What do I need to give the LAN to let others do their job?”

Windows Server

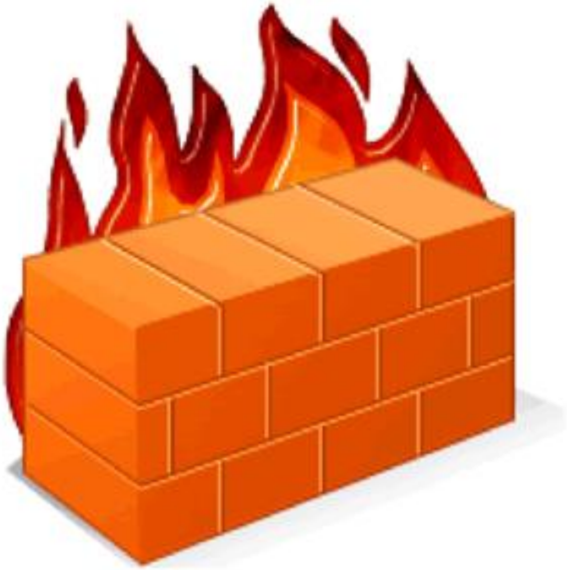
- **Active Directory**
- **Network Essentials (DNS/DHCP)**
- Provide services like Websites/File Transfer/Virtualization

*(Joke stolen from UBNETDEF) (Windows is currently under-represented so talk to me!)



Firewall

- Focus on Network Security
- Administer Network devices including:
  - Firewall
  - Switches
  - Routers
- Your tasks include:
  - creating firewall rules
  - configuring IDS/IPS
  - monitoring traffic
  - Secure firewall from attacks



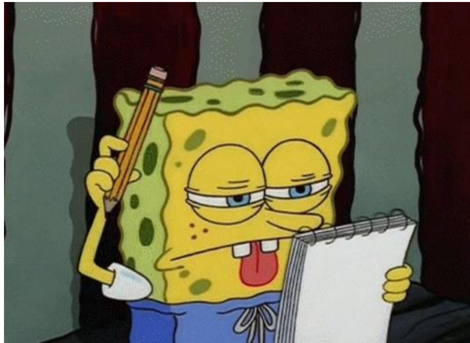
Other Roles Within the Team

Team Captain

- Manages strategic team operations (team roster, practice & competition schedule)
- Administrative: liaison between team and third-party elements (CDO, School of Business)
- Competition Ops: communicates technical concepts to senior leadership (Board of Directors)
- Designated cheerleader/gets on everyone's nerves

Inject/IR Lead

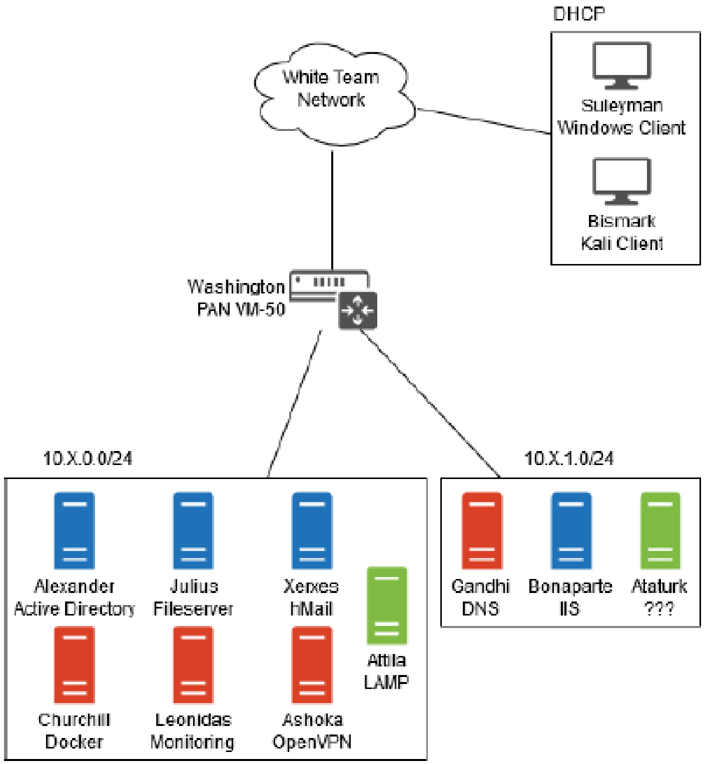
- Responsible for 50% of team score
- Completes assignments to maintain business continuity during competition
- Creates detailed incident reports
- Collaborates with technical elements to generate comprehensive injects



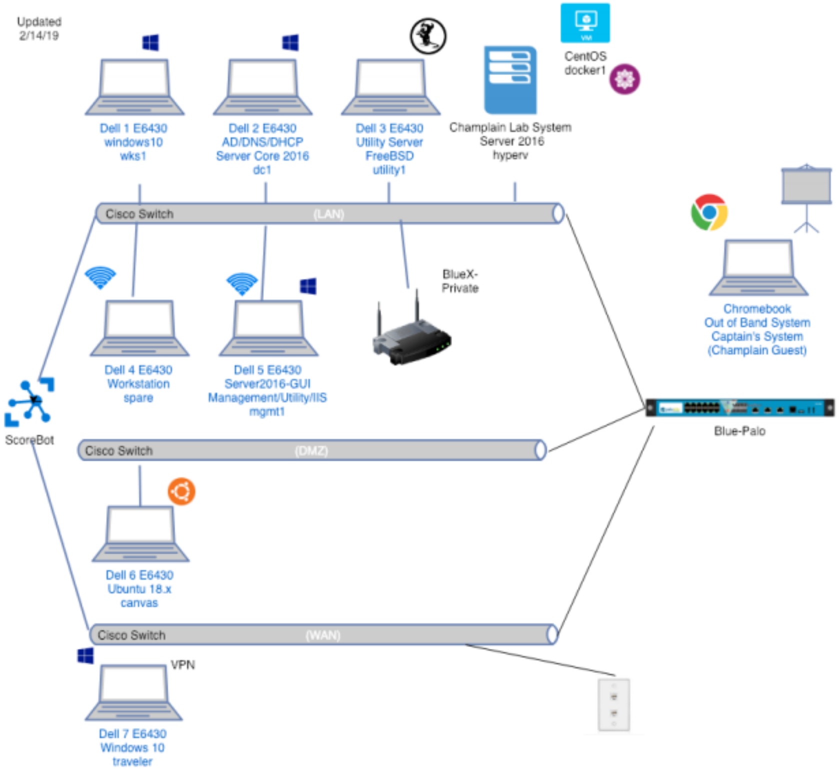
Competitions Available

1. CNY Hackathon:
    a. Date: April 5th & 6th, 2019
    b. Skill: Beginner
2. University of Buffalo Network Defense (UBNetDef):
    a. Date: April 27, 2019
    b. Skill: Beginner
3. RIT Information Security Talent Search (ISTS):
    a. Date: February 22-24, 2019
    b. Skill: Intermediate
4. DOE CyberForce (Potential Competition):
    a. Date: November 15 & 16, 2019
    b. Skill Level: Intermediate
5. North Eastern Collegiate Cyber Defense Competition (NECCDC):
    a. Date: March 15-17, 2019
    b. Skill: Advanced

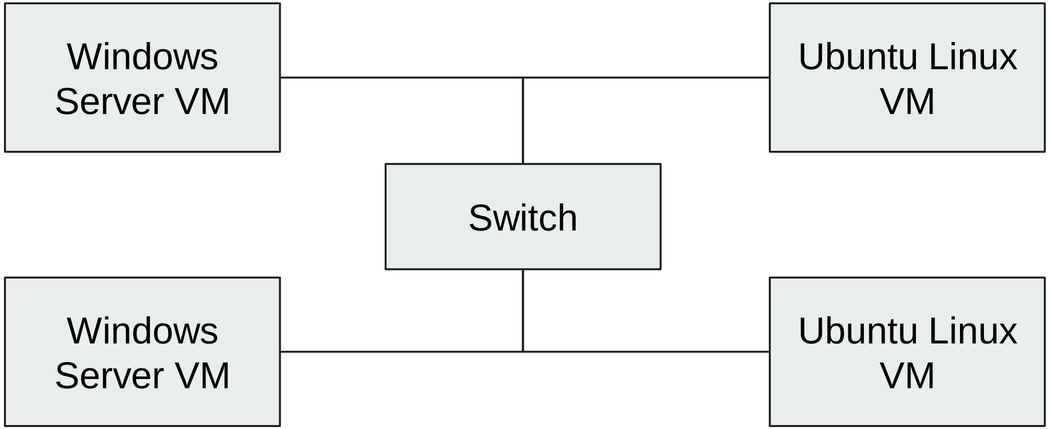
RIT ISTS


DHCP
White Team Network
Suleyman Windows Client
Bismark Kali Client
Washington PAN VM-50
10.X.0.0/24
Alexander Active Directory
Julius Fileserver
Xerxes hMail
Attila LAMP
Churchill Docker
Leonidas Monitoring
Ashoka OpenVPN
10.X.1.0/24
Gandhi DNS
Bonaparte IIS
Ataturk ???

CCDC 2019 Regionals



Goal for the Night!



Have all the VMs ping each other.
Have Windows RDP and Linux SSH.

Disclaimer - Yes we know we didn't explain anything → that’s the point

Key concepts

- Test our problem solving
- Practice working when given little instructions

Let’s practice -- Race

Split up into teams

Designate a team captain

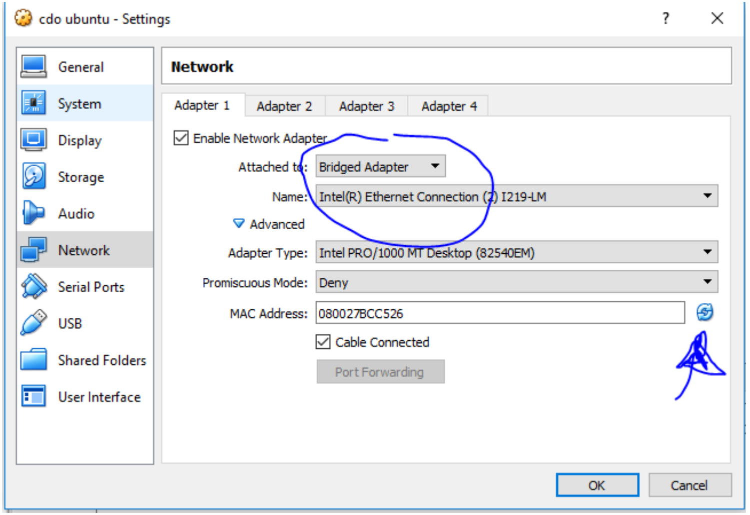
Team captains job is to ensure people are working together

Decide who is going to be

Windows admins and Linux admins

DONT START MACHINES YET

Steps 1:



cdo ubuntu - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Intel(R) Ethernet Connection (2) I219-LM

▽ Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027BCC526

☑ Cable Connected

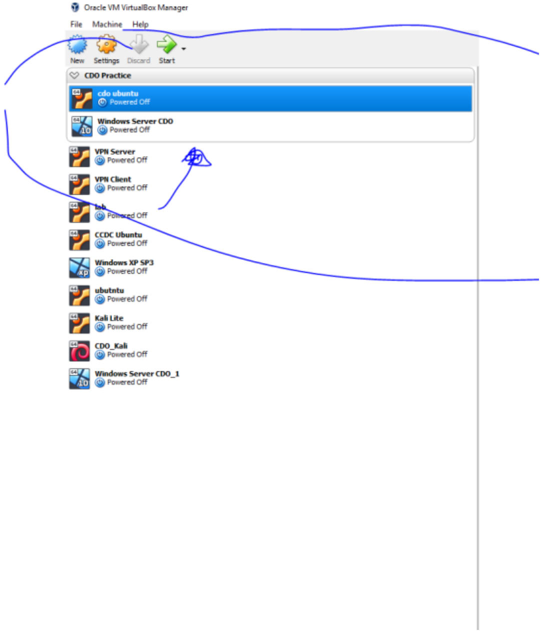
Set up the physical Switch.

Bridge Virtualbox interface (its in the settings)

Reinitialize the mac address by pressing the circle (NOTE MACHINE HAS TO BE OFF)

WHY? Because the switch is trying to forward traffic to machines that have the same MAC. It wouldn't know where to go!

And do promiscuous mode allow all/



CDO Practice

- cdo ubuntu — Powered Off
- Windows Server CDO — Powered Off
- VPN Server — Powered Off
- VPN Client — Powered Off
- lab — Powered Off
- CCDC Ubuntu — Powered Off
- Windows XP SP3 — Powered Off
- ubutntu — Powered Off
- Kali Lite — Powered Off
- CDO_Kali — Powered Off
- Windows Server CDO_1 — Powered Off

Linux credentials:
Username: cdo
Password: bb123#123

Windows server creds:
User: Administrator
Pass: Cyberdeforg1!

Step Two:

Statically Assignment of **Host Machines**. BEFORE CONFIGURING VM IPS

You need to give it a unique IP. 192.168.1.x

Release the old one. (ipconfig /release)

Step

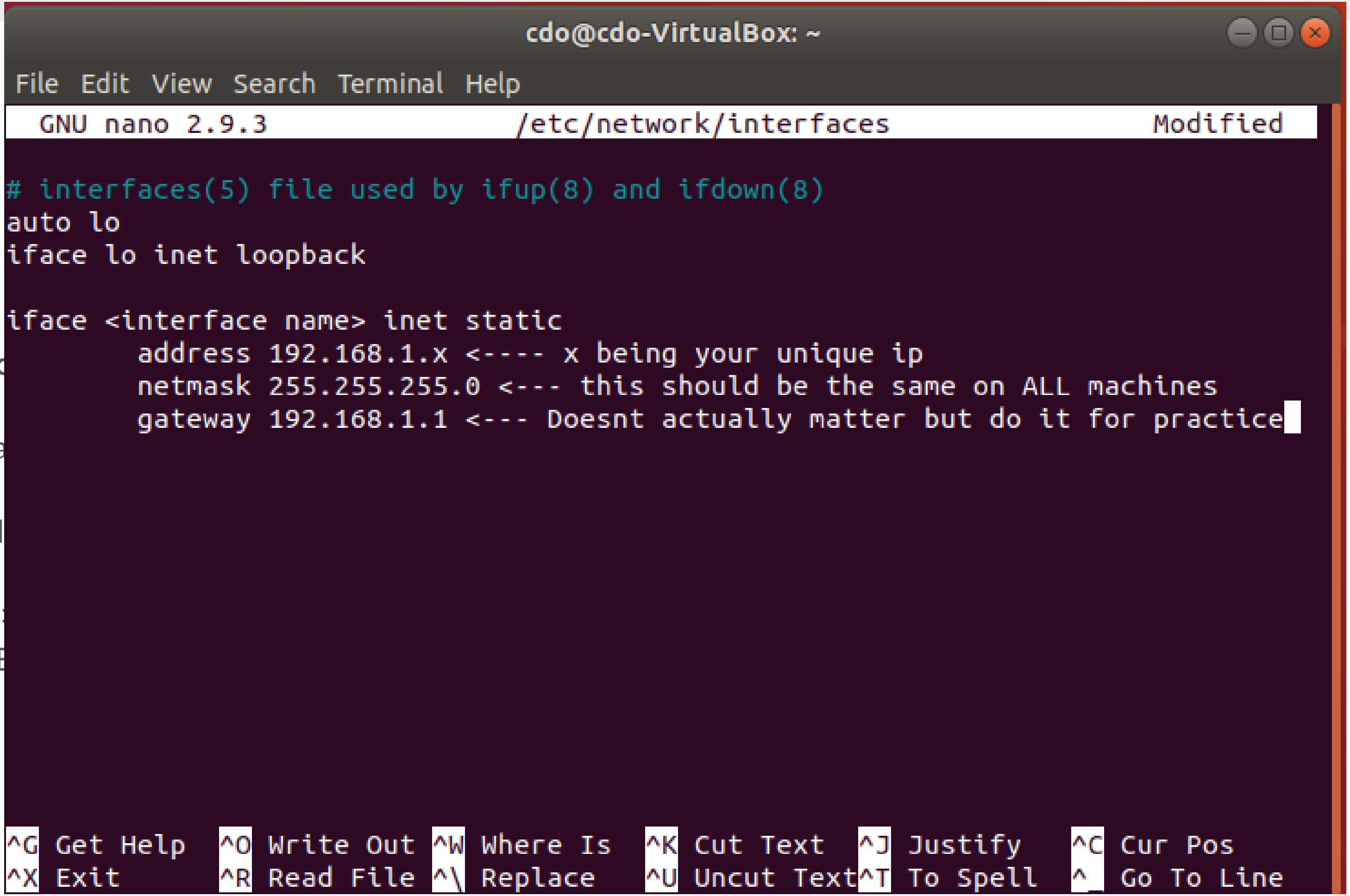
Windows Get

Log in to the ma

Assign a Static I

Control Panel -
and Sharing -> E
> IPv4

Set IP address.



```
  GNU nano 2.9.3              /etc/network/interfaces                   Modified

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

iface <interface name> inet static
        address 192.168.1.x <---- x being your unique ip
        netmask 255.255.255.0 <--- this should be the same on ALL machines
        gateway 192.168.1.1 <--- Doesnt actually matter but do it for practice

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text^T To Spell    ^_ Go To Line
```

Step Four:

Windows Allow RDP:

Turn off firewall.

Test Pinging the other machines!

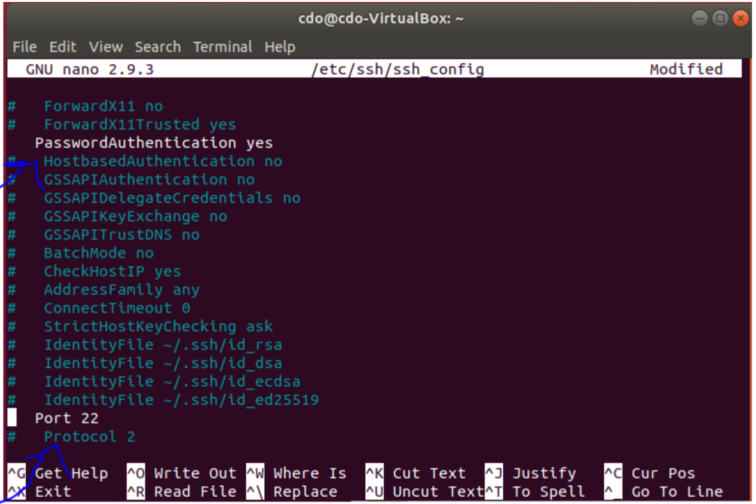
Open RDP and remote into the other machine!

(Use the user linuxLover).

ssh on linux:

sudo nano /etc/ssh/sshd_config

uncomment the following lines



```
  GNU nano 2.9.3                  /etc/ssh/ssh_config                  Modified

#   ForwardX11 no
#   ForwardX11Trusted yes
  PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
  Port 22
#   Protocol 2

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Restart ssh after you edit a configuration file