Welcome to CCDC Fall Bootcamp!

Info + Business + Networking Week

Sign-in

jessh.zip/2026ccdcfallweek1

Weekly Schedule

Date	CCDC (1PM-4PM)
Aug 29	Intro, Business, and Networking
Sep 5	Securing Linux and Windows
Sep 12	Common services + Q&A
Sep 19-20	CCDC Tryouts (1-5 PM)

Agenda

1 **Info**

Information you should know about CCDC

2 **Business**

Injects!!!! (and some stressful situations)

3 **Networking**

Computers yap with each other

Info on CCDC Bootcamp (Fall Edition)

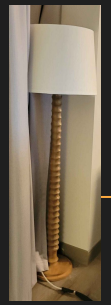
CCDC Information

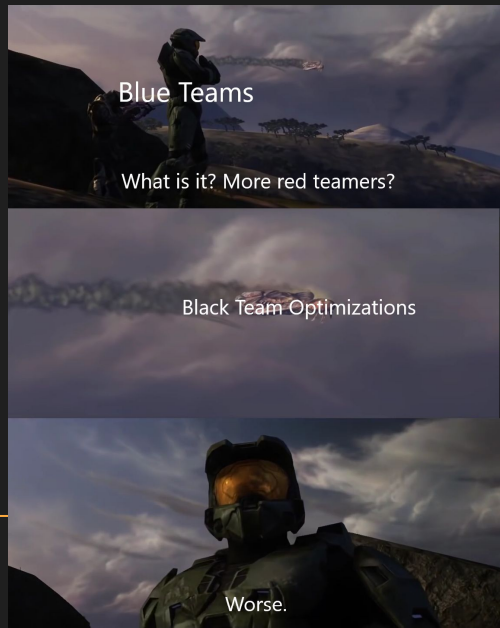
What is *CCDC*?

- Collegiate Cyber Defense Competition
  - National competition
  - 2x National Runner-up
- Focuses on system administration, incident response, computer networking, and cloud engineering
- **DEFENSE**
- Simulates IT/incident response teams
- Build, secure, and defend various business infra
- 8 main roster, up to 4 alternate

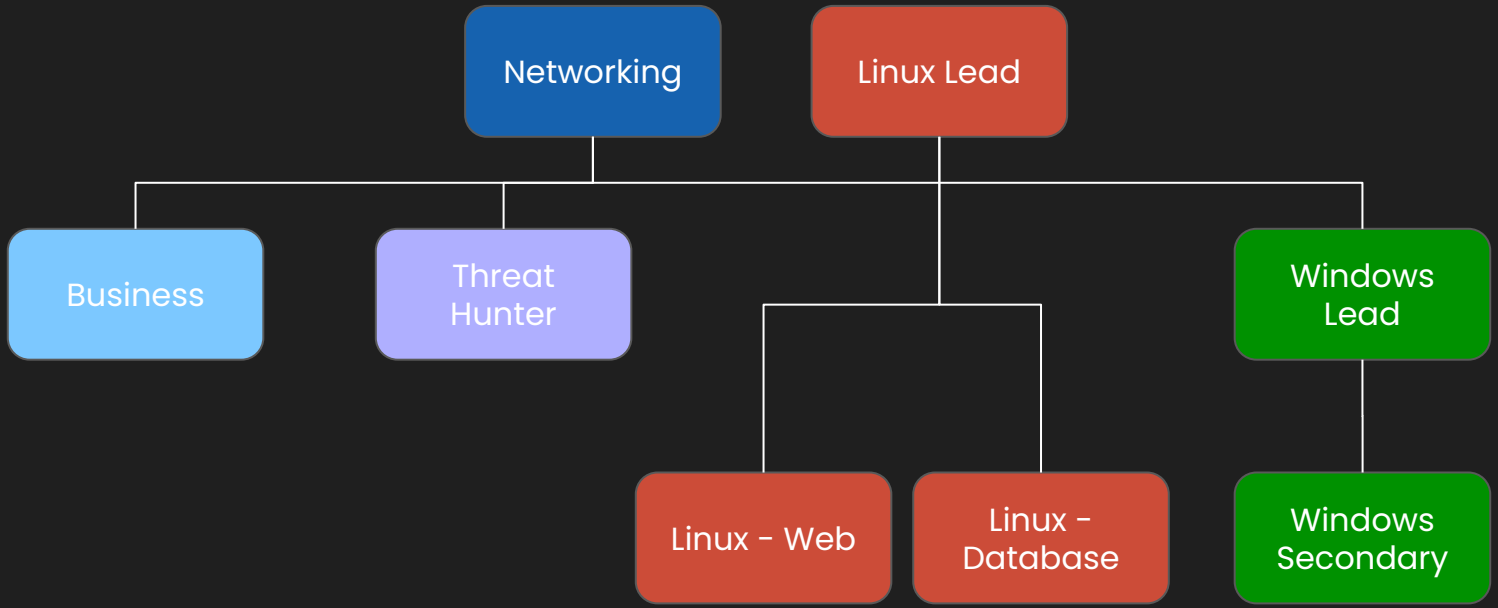
CCDC

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION





Team Structure



THINGS YOU'LL LEARN

- Services
  a. Active Directory
  b. DNS
  c. HTTP
  d. SQL
  e. SSH
  f. Email
  g. SMB
  h. Database
  i. And more...
- Tools
  - Group Policy
  - Nmap
  - Sysinternals
  - VPN
  - Firewalls
  - Tmux
  - And more...
- Procedures
  - User management
  - Incident Response
  - Patching / Hardening
  - Creating and restoring backups
  - Inventory
  - And more...
- OS's
  - CentOS, Ubuntu, Alpine Linux, Debian, Slack, Rocky
  - Windows Server, Windows Workstation

Meet the Team!

CCDC

Natalie
Tran

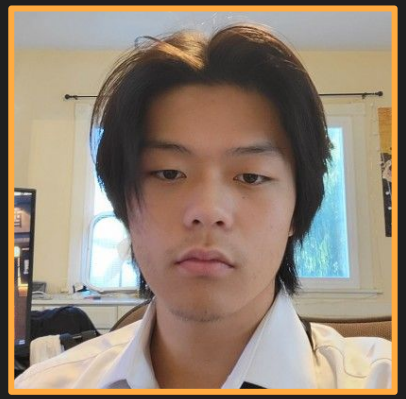
Annabel
Wen

Adam
Cheung

Anthony
Rivera

Special Mentions

Anson Ng



Daniel Lee

1.1 Bootcamp Objectives

Our goals for you

Cyber Bootcamp Objectives

Learn to Learn

Gain confidence in your ability to learn rapidly, and independently

Build Team Skills

Build relationships and showcase interpersonal skills

Prepare for the Future

Set a solid foundation and discover opportunities in cybersecurity

1.2
CCDC Timeline

Time commitments

Weekly Schedule

Date	CCDC (1PM-4PM)
Aug 29	Intro, Business, and Networking
Sep 5	Securing Linux and Windows
Sep 12	Common services + Q&A
Sep 19-20	CCDC Tryouts (1-5 PM)

CCDC Team Schedule

- Meet at least once a week (usually Saturdays) for practice
  - The more the better!
- Competition weekends

Month	CCDC
November	Invitationals #1*
December	Invitationals #2*
January	Invitationals #3*
February	Regional Qualifier
March	Regional Finals
April	National Finals

1.3
Tryout Details

How to get on the teams

September 19 or 20

Pick either day!

Selection Requirements & Rubric

CCDC Team

- **Full-time** CPP Student (Attend **Fall 2026** & **Spring 2027)**
  - non-masters :(
- **Good** academic standing (2.0 GPA)
- Stand out during the bootcamp

Homework	30%
Teamwork	20%
Participation	15%
Tryouts	35%

Bootcamp Tips

- Be involved
- Take notes and research out of class
- Stay organized and (mostly) professional
- Google things and ask questions
- Work well in a team
- Stay determined/committed

And the most important thing:

- Bring a growth mindset

Q&A

Any questions at this point?

2

Let’s get down to *BUSINESS*

This is important (trust)

SWIFT

Table of Contents

2.1 Business???

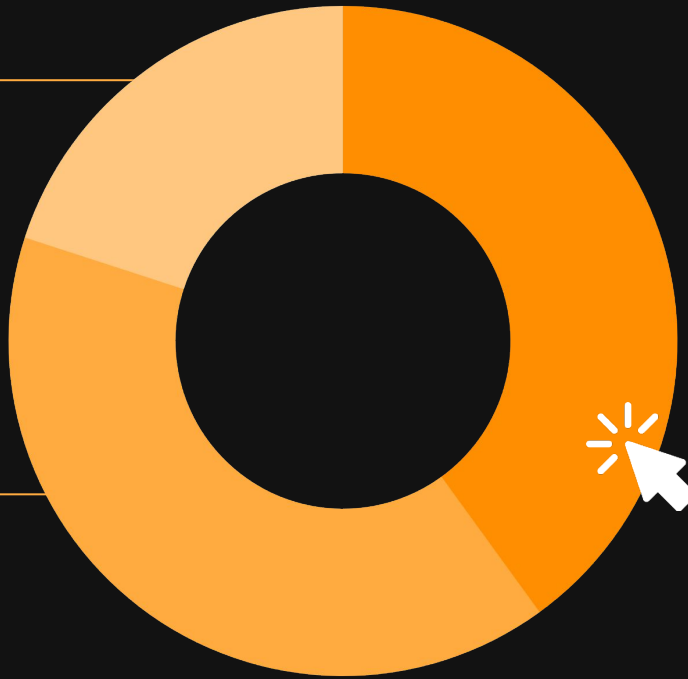
Da heck I thought this was a cyber defense competition??!!!!

Whoa!

Before you roll your eyes…
Cybersecurity serves as a *function of business*

CCDC score breakdown

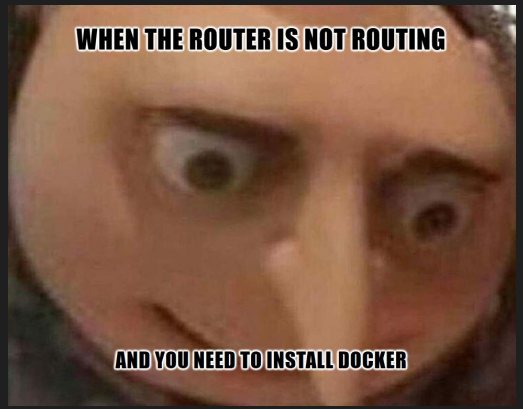
20%
Orange team



40%
Services

40%
Business injects

It’s more challenging than you think…



Technical tasks

Why do we need three ~~firewalls~~ VPNs??

Broad understanding

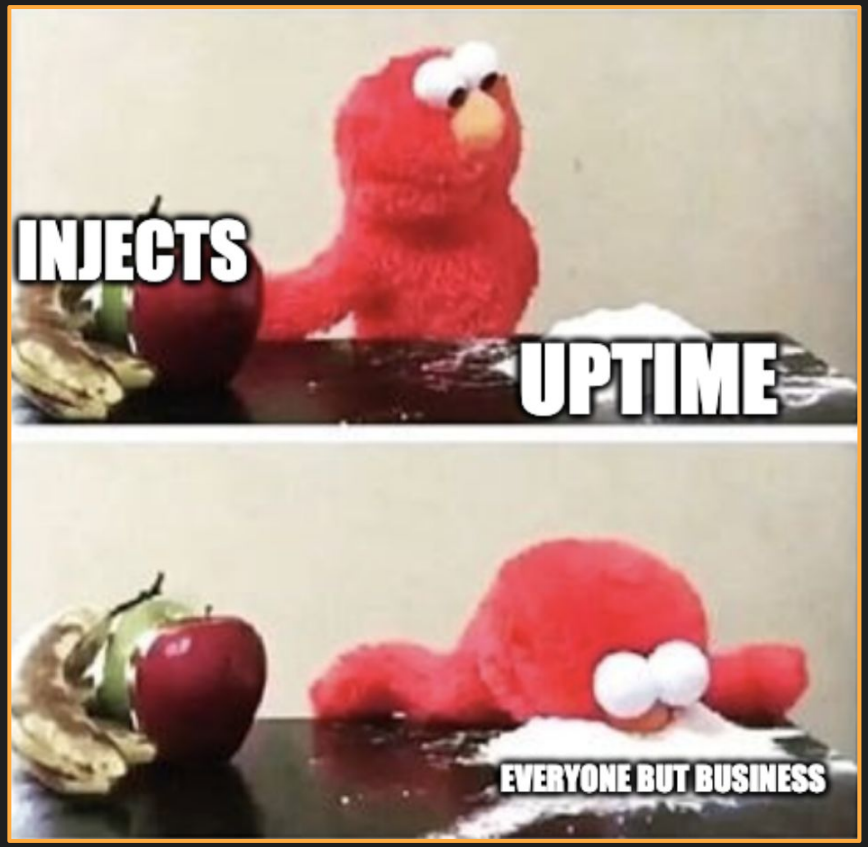
What even is logging and where are the trees???

Who is Ms. Configuration???

What is a kernel and where is the corn???

2.2
Injects

No doctors were involved in the making of these slides



Da heck is an inject?

- Tasks from business execs
- Complete within some short timeframe
- Write-ups, infographics, *presentations*
- Examples
  - Conduct a security assessment
  - Recommend a cloud solution
  - Write a Disaster Recovery Policy
  - Set up and configure a company VPN
  - Create an infographic to promote security awareness

Secret sauce to good injects

be thorough

use clear and concise language

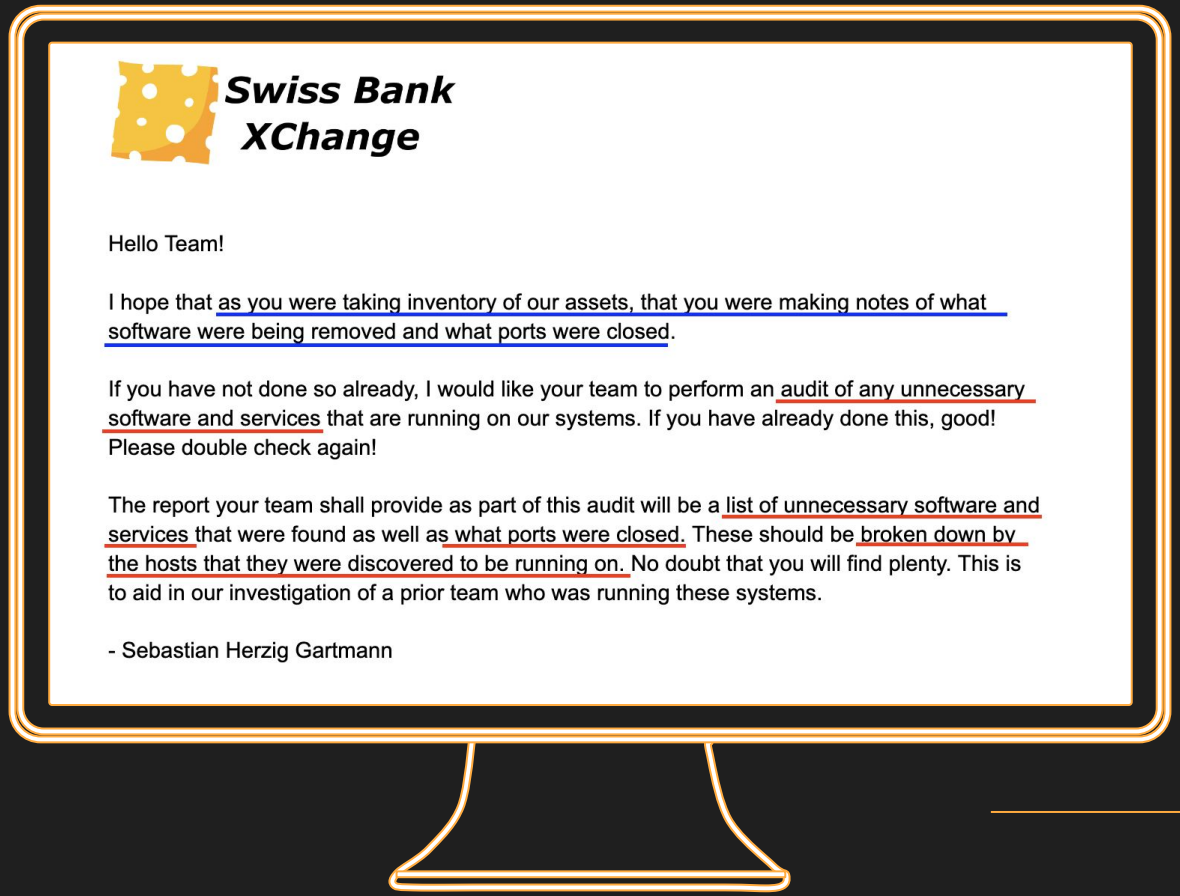
provide supporting evidence

Secret secret sauce to good injects

be
consistent

submit
something!

Being thorough



Swiss Bank XChange

Hello Team!

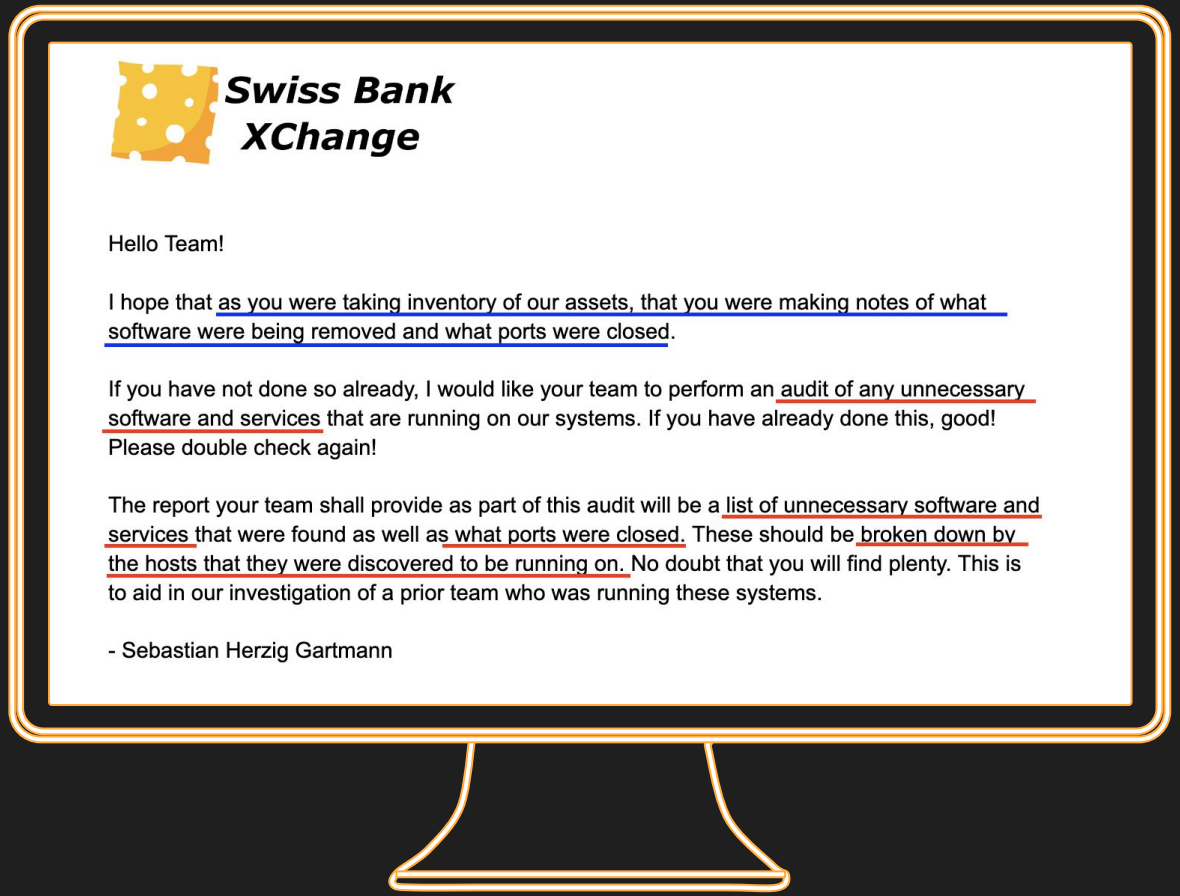
I hope that as you were taking inventory of our assets, that you were making notes of what software were being removed and what ports were closed.

If you have not done so already, I would like your team to perform an audit of any unnecessary software and services that are running on our systems. If you have already done this, good! Please double check again!

The report your team shall provide as part of this audit will be a list of unnecessary software and services that were found as well as what ports were closed. These should be broken down by the hosts that they were discovered to be running on. No doubt that you will find plenty. This is to aid in our investigation of a prior team who was running these systems.

- Sebastian Herzig Gartmann

Being thorough



Swiss Bank XChange

Hello Team!

I hope that as you were taking inventory of our assets, that you were making notes of what software were being removed and what ports were closed.

If you have not done so already, I would like your team to perform an audit of any unnecessary software and services that are running on our systems. If you have already done this, good! Please double check again!

The report your team shall provide as part of this audit will be a list of unnecessary software and services that were found as well as what ports were closed. These should be broken down by the hosts that they were discovered to be running on. No doubt that you will find plenty. This is to aid in our investigation of a prior team who was running these systems.

- Sebastian Herzig Gartmann

Requirements:

1. Perform an audit of unnecessary software and services
   a. Including everything removed prior to this inject
2. List the software and services removed
   a. Make note of ports that were closed
3. Organize findings by host

Tips:

- ALWAYS take notes on what you are doing
- Anticipate inject prompts

Using clear and concise language

Address the recipient

Take into account ***who*** your audience is

Write with intention, get to the point

DON'T use colloquial language

DON'T neglect formatting

DON'T guess about information – always check with the team

Provide supporting evidence

YOU ARE TRYING TO CONVINCE YOUR "BOSS" THAT YOUR SOLUTION IS THE BEST SOLUTION

Provide supporting evidence

- **Give background about the issue.**
  - Would there be fines if we fail to fix it? Potential loss?
- **WHY did you choose that solution?**
  - What other solutions were there?
- **HOW MUCH does your solution cost?**
  - How does that compare to other solutions?
- **WHO is going to implement your solution?**
  - Who is going to maintain it?

!!! Provide supporting evidence - MUST DOs

SHOW YOUR WORK!!

- Screenshots
- Logs
- Examples of config
- Scripts that were run

NEATLY

- Categorize your evidence
  - Host
  - OS

Be consistent

- **Make and use an Inject Template**
  - aka "prefiring" the angle or crosshair placement
  - Have a template you'll copy & paste for every inject

Be consistent

Do's:

- **Always have a header**
  - Company name/logo with colors
- **Use a basic email format**
  - Salutation, Closing, Team #

Don'ts:

- **Address the wrong person...**
- **Obscure the letters**
  - Weird font (comic sans 😭)
  - Logo in background
  - Cover words with screenshots

Be sure to change your placeholders during competition!

Submit something!

- **Even if you don't have much...**
  - Submit whatever you have before the deadline
- **Getting some points is better than nothing!!!**
  - You'll always get points for organization and format

2.3

Inject Practice

Congrats! You're hired :D

Background

The Company

- Name: Pulsar Palace & Casino
- About: Hotel + Casino company that rivals "The Wormhole"
    - Provides online check-in service for guests as well as slot machines!
- You have recently joined the IT Security team to maintain service uptime and patch vulnerabilities

Practice 1: Troubleshoot RDP

Prompt

- The Senior Network Engineer, Anna Kin (she/her), recently purchased a new server and had it placed in a rack on Earth. For some reason, remote access via RDP is failing.
- "Can you figure out why I can't RDP into this new server? Document what you did regardless of whether it works or not. Thanks!"
- Server hostname: **ear-str-comp-01**

Objective

- 1-2 page report
- 20 minutes
- Write a report on this RDP problem to **the Senior Network Engineer**
- Use imagination!

Practice 2: Quick Request

Prompt

- The CEO of PPC, Gamma P. Ray (he/him), has a request:
- "I want to spread awareness of phishing attacks at PPC. Can you draft a list of common things phishing emails contain or try to do? I'll be speaking about this at the conference later, so be fast!"

Objective

- 1 page report
- 10 minutes
- List of phishing email content for **the CEO**
- Be creative and use your imagination!

Manager

- Technical rundown
  - More tech terms
- More details = better
- Screenshots
- Usually involve guides, audits, etc.

C-Suite

- Dumb it down
  - Simpler words that anyone can understand
- Concise, straight to the point
- Neat? Use a table!
- Strange requests

2.4??

Injects in Practice

in comp

What do real injects look like?

Overview

- Usually around 45 min - 1.5 hr to complete each
- 12-15 injects throughout the comp
- Examples
  - Take inventory of the environment
  - Install Ansible and run a playbook to gather OS info
  - Draw a new company logo
  - What's your favorite dinosaur?

Re: Inject 03 - PowerShell on Linux

Good Evening,

One of our engineers was given a Linux system to work with, but we found out that he was cursed to only know PowerShell syntax.

Please download PowerShell on one of the Linux machines, and once it's up and running, write a ps1 script that outputs the OS that it is running on and the version. Detail the steps you took to do so, and send me a report with pictures.

Sincerely,
Alison Maher
MindMend$_{AI}$ IT Manager

How do we do injects in real comps?

Inject Lead

- **In charge of looking out for and assigning injects**
- **Manage a whiteboard**
  - Write down deadlines and who is assigned to what
- **Make template before competition**
  - After given briefing packet
- **Submit most (if not all) injects**
  - Take screenshot of completion after comp

Pair up System

- You'll never be alone!
- One person does technical
- Another does writing

3
You will love networking.

Yes. You will.

Agenda

1. Intro to Networking
2. Competition Networking
3. Client Server Model
4. Firewalls!

3.1

Intro to Networking

Not the LinkedIn one

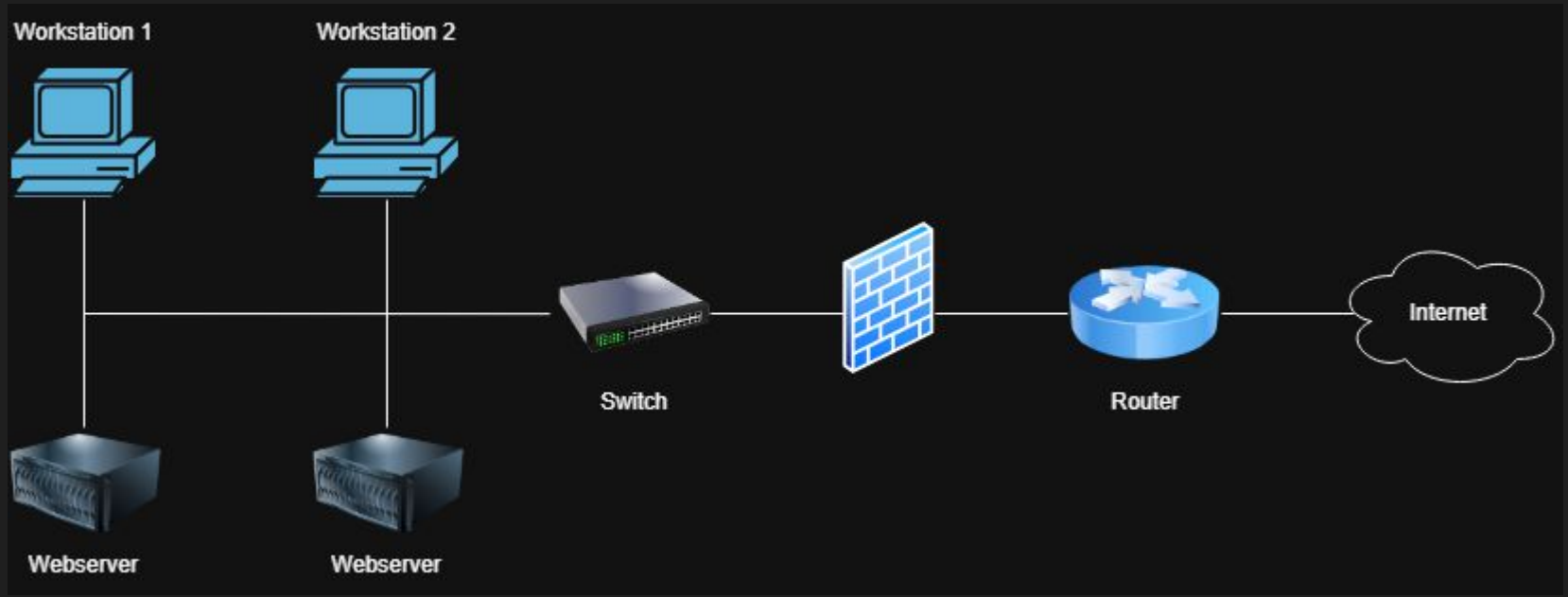
Network

System of interconnected network devices
- Communicate and share resources

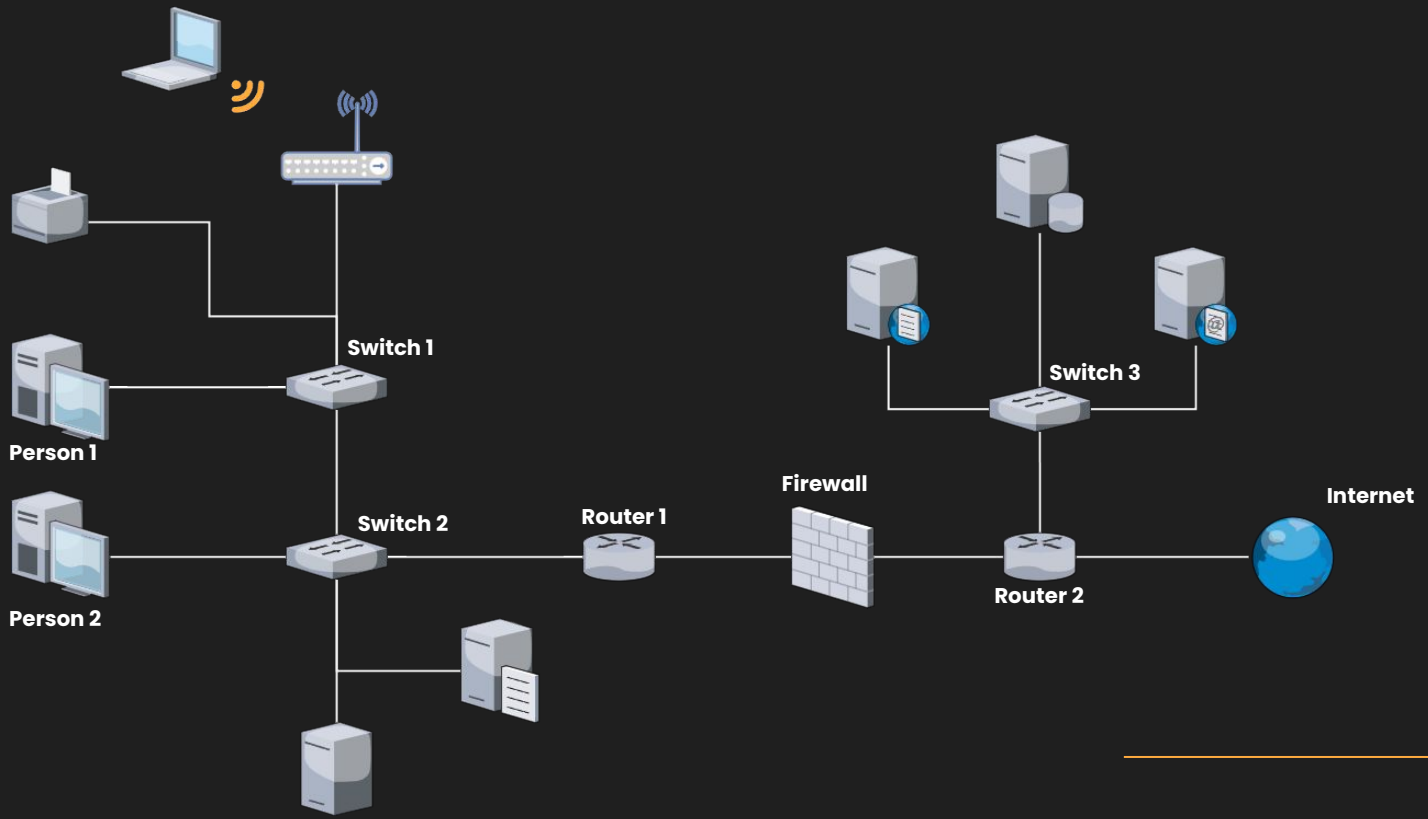
Network Devices

Anything on the network
- Computers, phones, routers, switches, etc.
- Contains at least one **Network Interface Card** (NIC)
  - Wired or wireless connection to internet

Basic Topology



Basic Topology?



Lingo

- IP Address
- Subnet Mask
- Router
- Default Gateway
- Service
- Protocol
- Port
- Interface
- Firewall

IPs & Subnet Masks

IPv4 address → `192.168.1.100`

`255.255.255.0` ← **Subnet Mask**

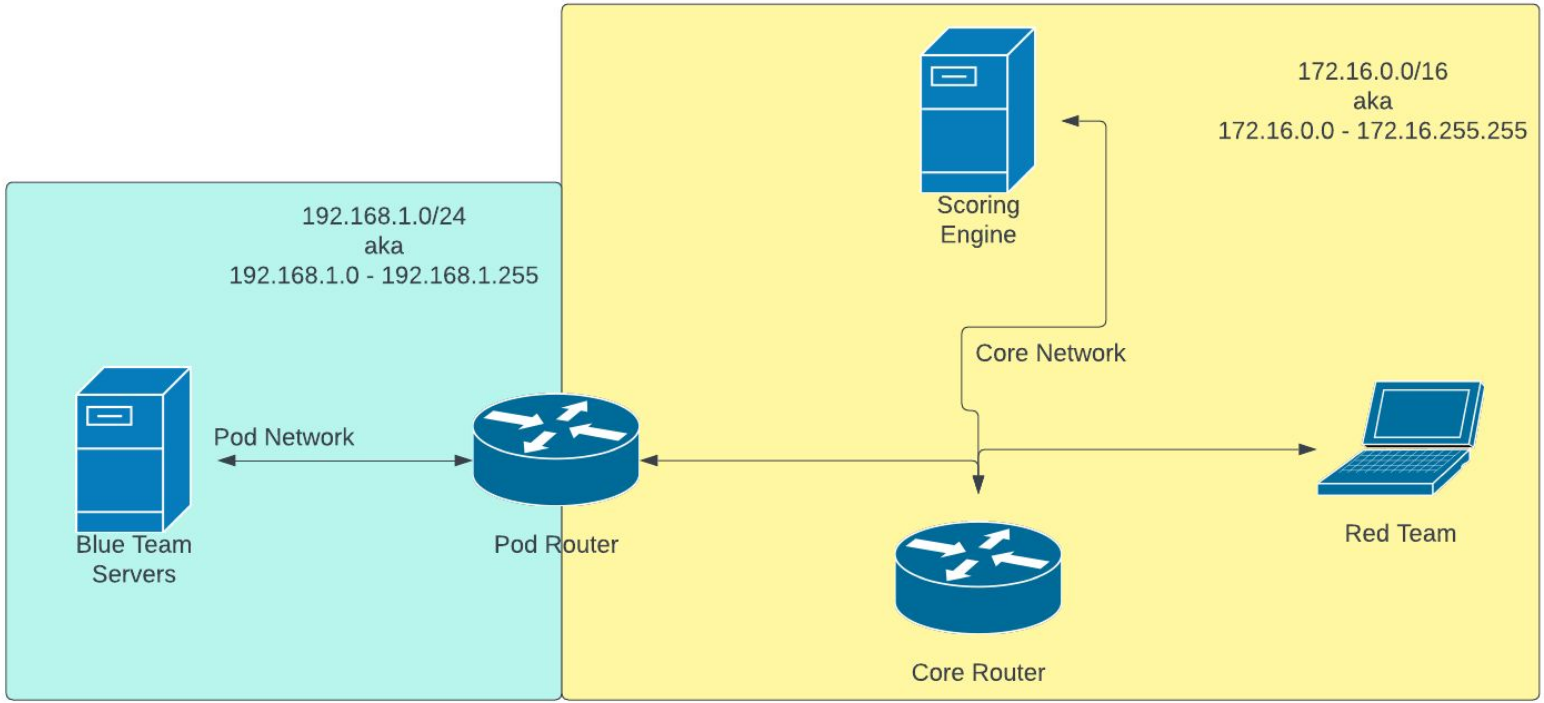
```
IPv4 Address. . . . . . . . . . . : 192.168.1.115
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
```

3.2

Competition Networking

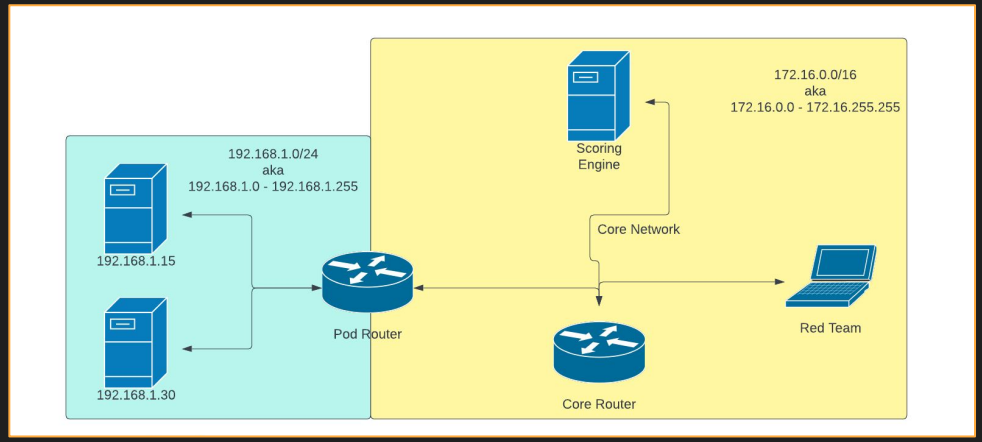
Services go brrrrr

Competition Topology

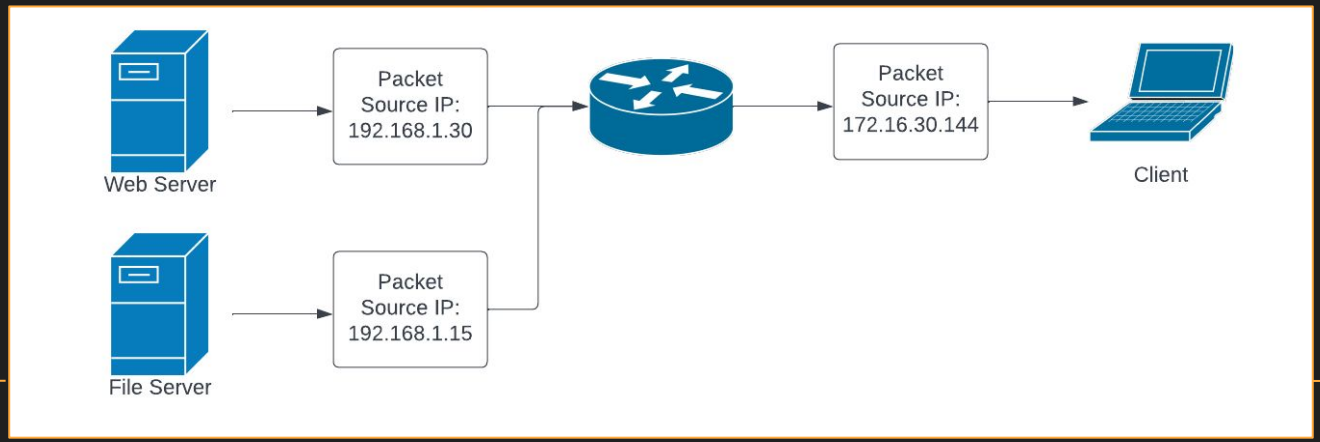


NAT

- Network Address Translation
- Built to conserve IP addresses

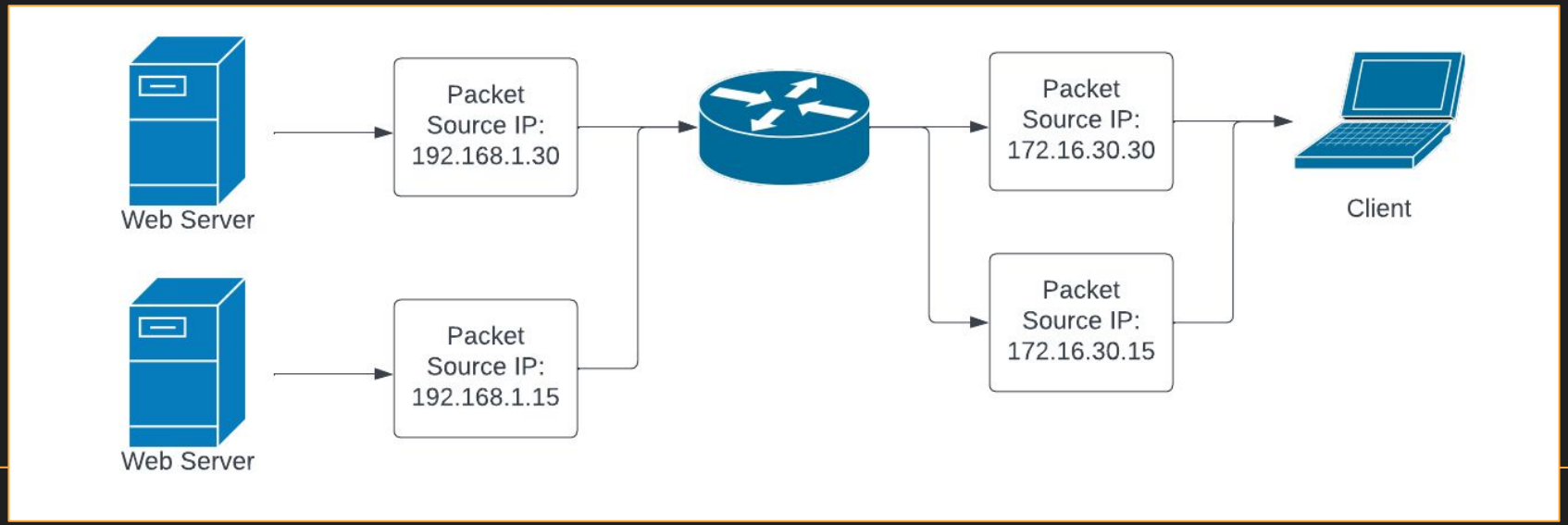


One-to-Many Translation:



1:1 NAT

- Direct Translations
- 192.168.1.0/24 → 172.16.30.0/24

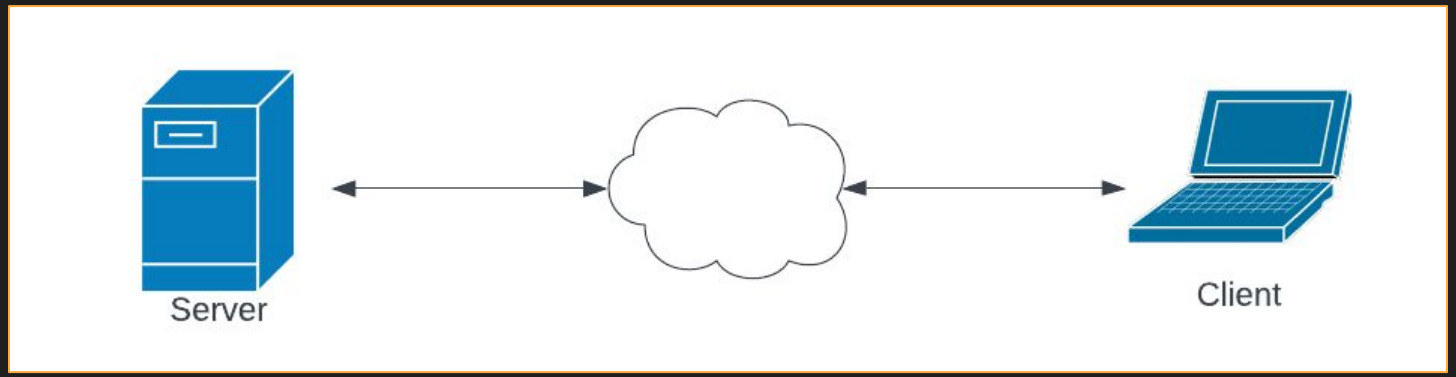


3.3

Client-Server Model

Packet restaurant

Client–Server Model



What are ports?

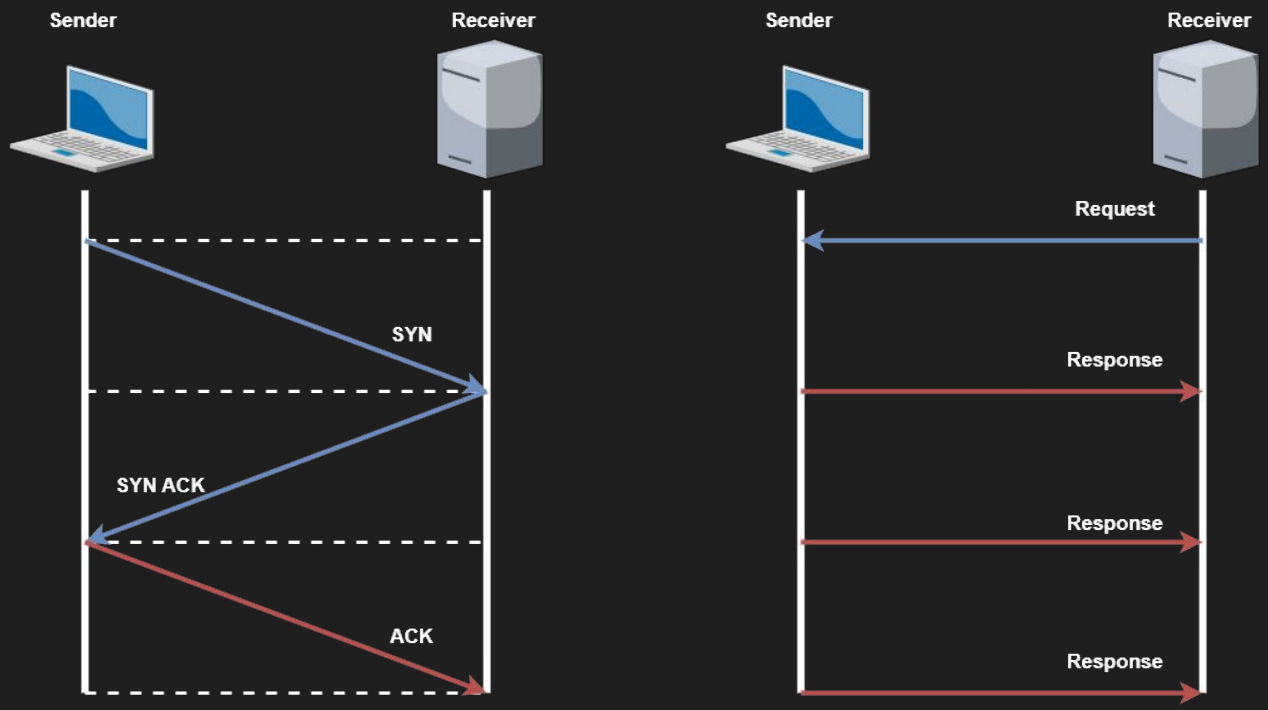
Numbers that identify, along with an IP address, which network socket to connect to on a given device.

- Common port numbers and associated services
  - TCP 20 and 21 - FTP
  - TCP 22 - SSH
  - TCP 25 - SMTP
  - UDP 53 - DNS
  - TCP 80 - HTTP
  - TCP 443 - HTTPS
  - etc.

TCP and UDP

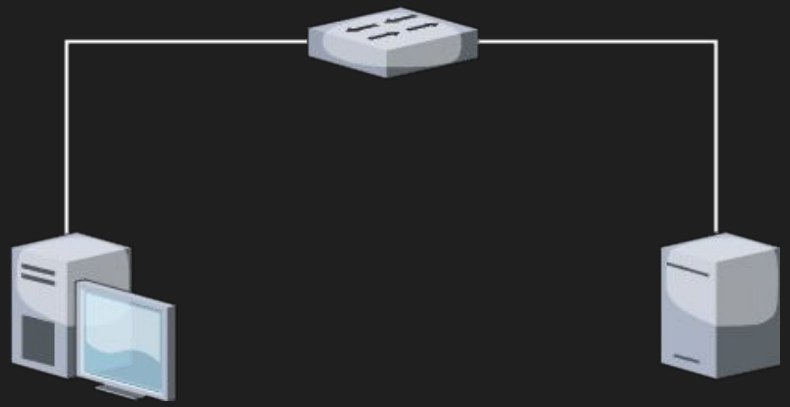
- TCP - Slow but reliable
  - Synchronization
  - Flow control
  - TCP Handshake
- UDP - Fast but unreliable
  - No error-checking
  - No acknowledgements
  - Just send data

TCP and UDP


Sender
Receiver
SYN
SYN ACK
ACK
Sender
Receiver
Request
Response
Response
Response

What are sockets?

Each end of a connection, basically a pairing between an IP and a port.



IP: 192.168.1.10
MAC: AA:AA:AA:AA:AA:AA

IP: 192.168.1.58
MAC: EE:EE:EE:EE:EE:EE

192.168.1.10:57138 → **192.168.1.58:80**

Why is this important?

Identify normal/abnormal traffic

- Is it coming from scoring engine/orange team? Or is it red team?

Troubleshooting services

- Firewall issue? Service disabled?

```
C:\Windows\System32>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1372
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       4868
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       4868
```

4

Firewalls

Not a waterwall.

Block IPs

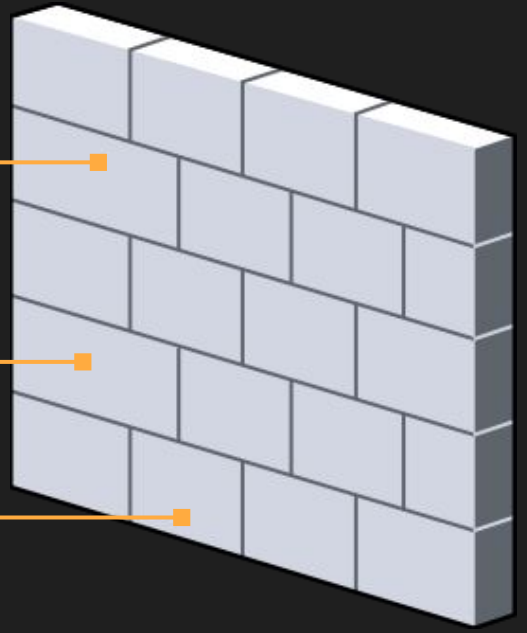
Can block a whole subnet or individual.

Block Ports

Block which ports the external network can access on the LAN

Filtering

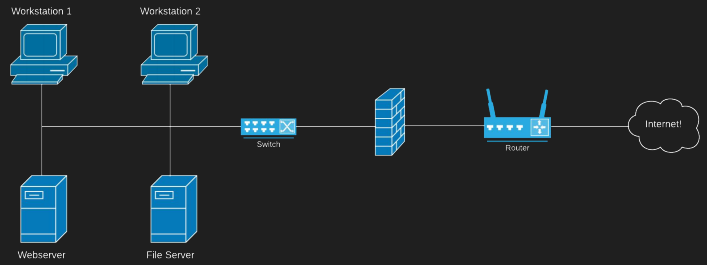
Ingress and Egress filtering rules.



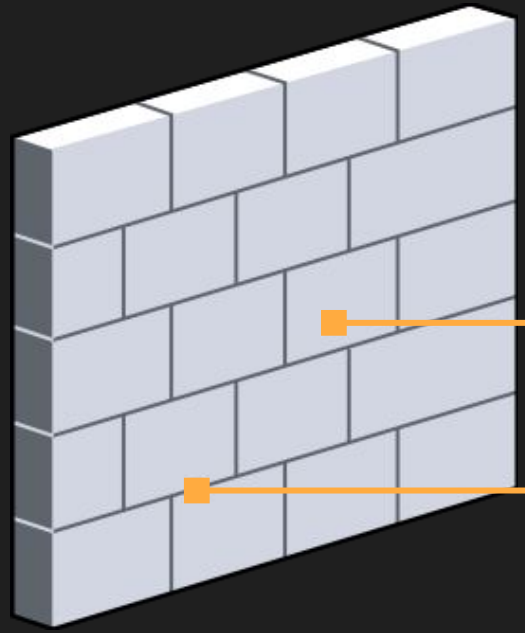
Host Firewall vs Network Firewall

- Host-based firewall
- Filters inbound and outbound traffic for a single device
- Two different rulesets
- Ex. a Windows file server has a Windows Firewall

- Network-based firewall
- Filters inbound and outbound traffic for LAN and WAN
- Four different rulesets
- Ex. a network has a Cisco Firepower Firewall



Stateless vs Stateful



Stateless

ACL. Looks at
Individual packets.

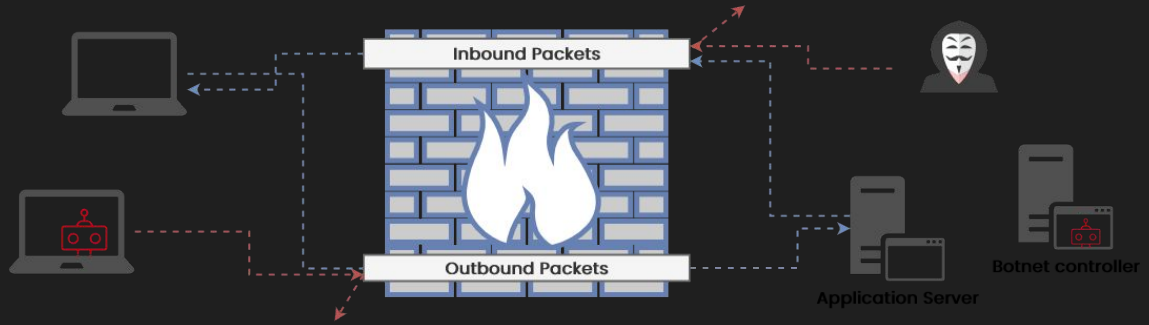
Stateful

Traffic patterns and flows.
Remembers connections.

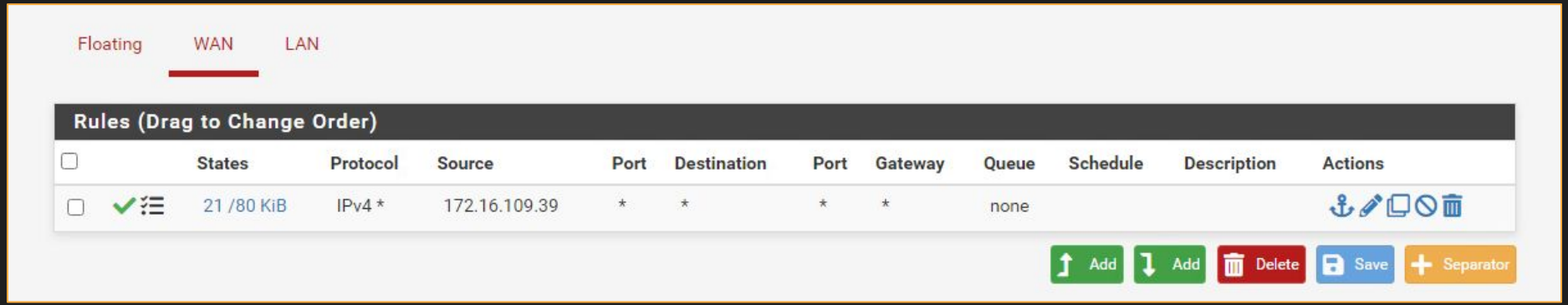
FW Example

Inbound
- Only allow required services
- Allow certain subnets
- Allow certain ip addresses

Outbound
- Block everything going outbound (break internet)



WAN Firewall



LAN Firewall

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0 /3.83 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
☐	✗	0 /0 B	IPv4 *	*	*	*	*	*	none			
☐	✓	3 /2.07 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
☐	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

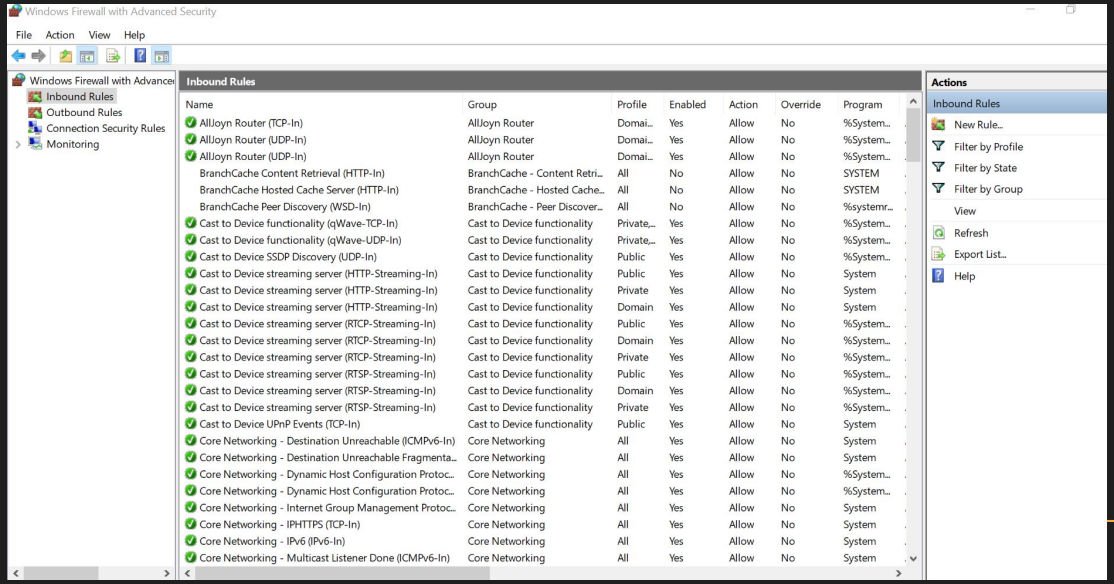
4.5

Comp Firewalls

Phoenix flash is broken

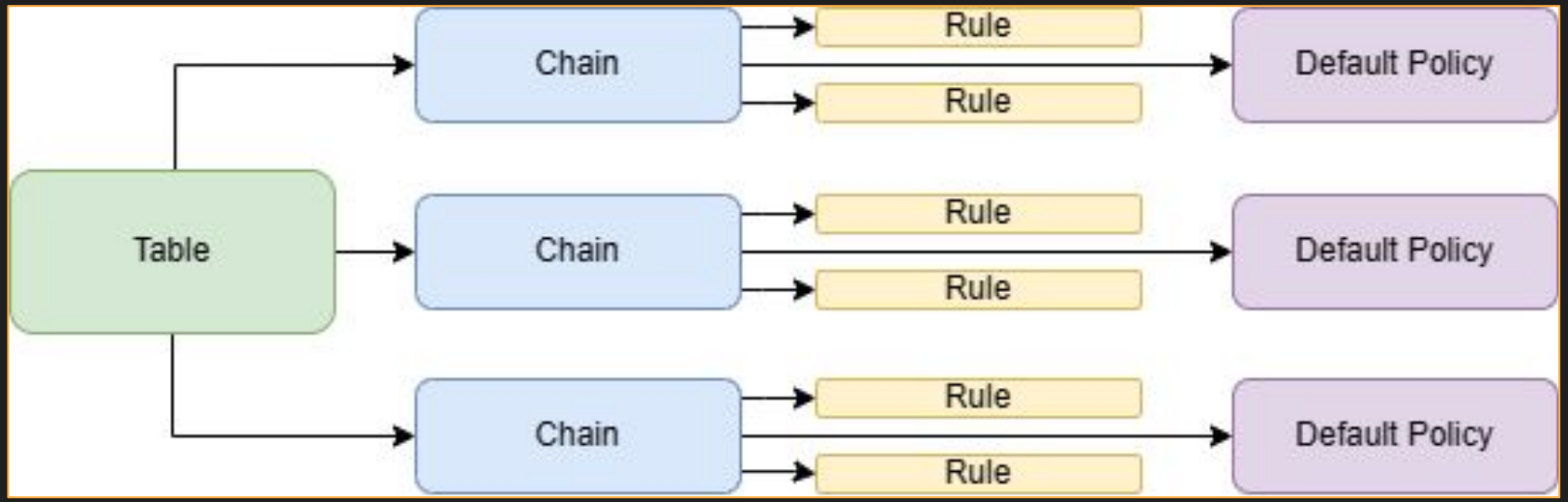
Windows Defender Firewall

- A **stateful** firewall that uses defined rules
  - Goes down list until the packet matches a rule
- Installed on all Windows OSes by default



iptables

- A **stateless** firewall that has a list of rules
  - Goes down list until the packet matches a rule
- May not be enabled by default (some use ufw 🤮)



Homework

Due September 4th @ 11:59 PM
https://jessh.zip/2026ccdcfallhw1

Deploy a pod

- Connect to the VPN and visit kamino.sdc.cpp
- Navigate to Pods > Click "CCDC Bootcamp 2026" > Clone
- This will be used for both this HW and future in-session activities!
- **DO NOT DELETE YOUR POD UNTIL THE END OF BOOTCAMP (September 18th)!!!**

Thanks!

Any questions? Please ask questions; we are available to help :D