Week 1:
Info, Business, & Networking

Sign-in

https://jessh.zip/ccdcfallweek1

CPP VPN Access

https://jessh.zip/ccdcfallvpnaccess

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)

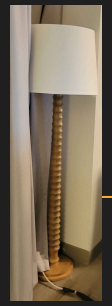
CCDC Information

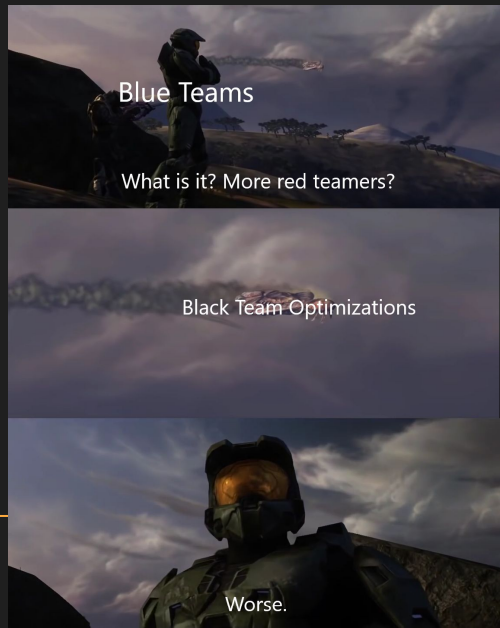
What is *CCDC*?

- 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, 4 alternate

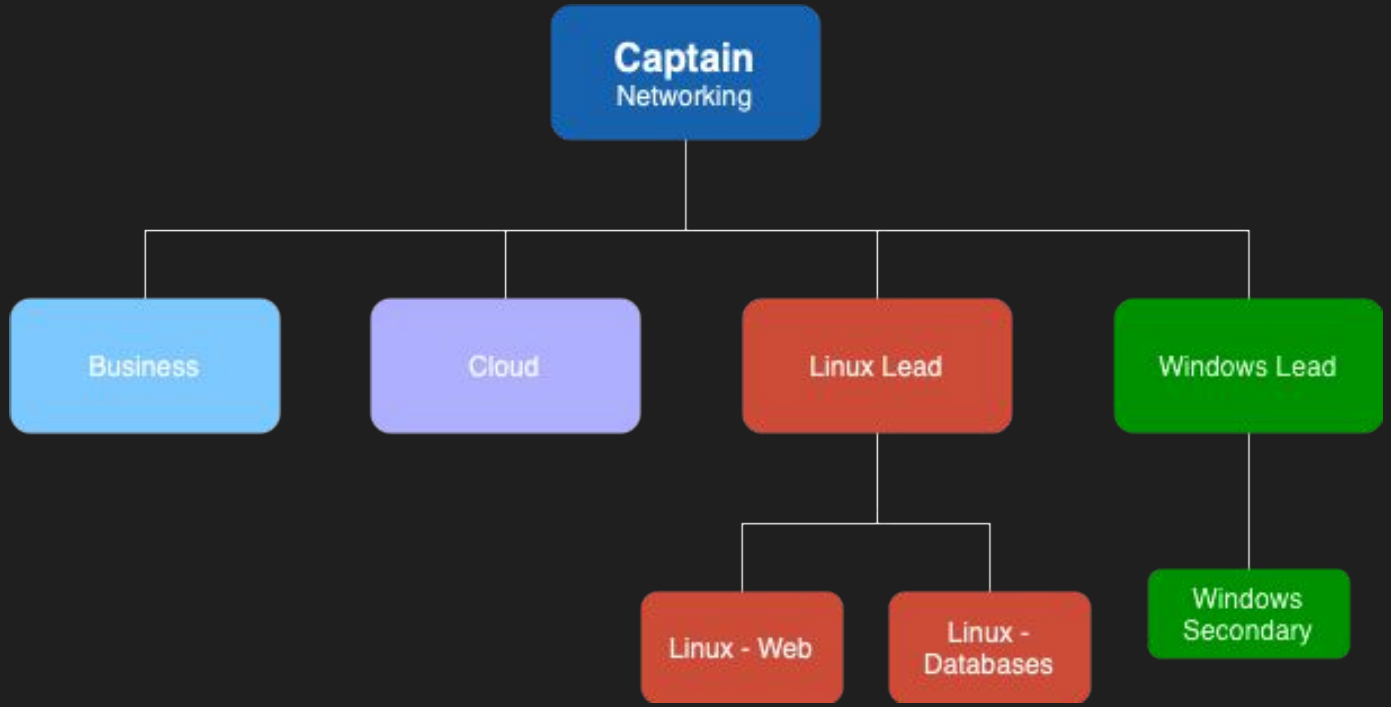
CCDC

NATIONAL
COLLEGIATE
CYBER
DEFENSE
COMPETITION





Team Structure



THINGS YOU'LL LEARN

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

Meet the Team!

Natalie
Tran

Medha
Swarnachandrabalaji

Sara
Downing

Info Agenda

1 **Objectives**

Key goals for the bootcamp

2 **Timeline**

Content and schedule

3 **Tryout Info**

Requirements and other details

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

2
Bootcamp Timeline

Time commitments

Weekly Schedule

Date	CCDC (1PM-4PM)
Aug 30	Intro, Business, and Networking
Sep 6	Common Services and Securing Linux
Sep 13	Securing Windows and Review/Tryouts AMA
Sep 20-21	CCDC Tryouts (1-5 PM)

3
Tryout Details

How to get on the teams

September 20-21

Tryout Date

Selection Requirements

CCDC Team

- **Full-time** CPP Student
- Attend **Fall 2025** & **Spring 2026**
- **Good** academic standing (2.0 GPA)
- Stand out during the bootcamp

CCDC Rubric (Fall)

Homework	30%
Teamwork	15%
Participation	10%
Tryouts	45%

Bootcamp Tips

- Be involved
- Take notes and research out of class
- Stay organized
- Google things and ask questions
- Work well in a team

And the most important thing:

- Bring a growth mindset

CCDC Team Schedule

- Meet at least once a week (usually Saturdays) for practice
- Ad-hoc working/research meetings
- Competition weekends

Month	CCDC
October - January	Invitationals #1-6*
February	Regional Qualifier
March	Regional Finals
April	National Finals

Q&A

Any questions for the team?

CCDC:
Let’s get down to *BUSINESS*

This is important (trust)

SWIFT

whoami

- **Medha Swarnachandrabalaji @medl100**
- **3rd year CS Major and Cyber Minor**
- **CCDC**
  - Alternate Member 2024-2025
  - Member 2025-2026
- **SWIFT Alumni Relations Coordinator**
- yapper

Table of Contents

01 Business???

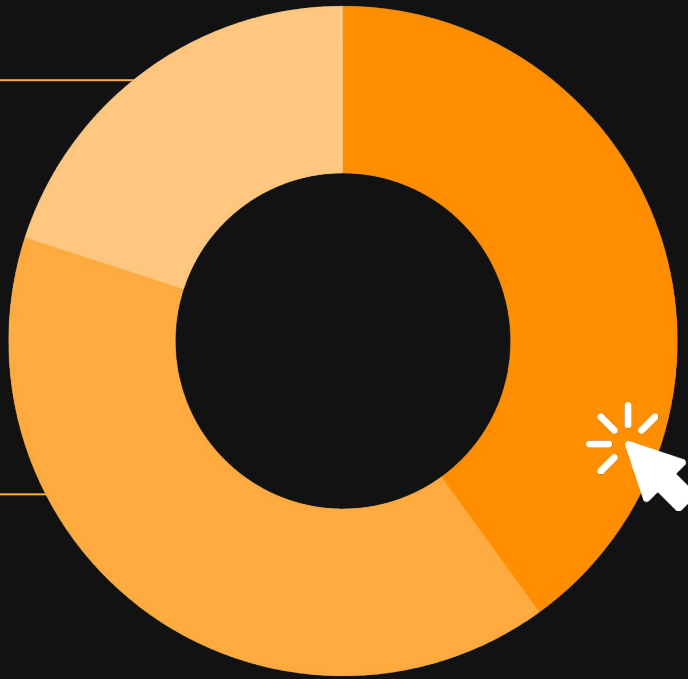
Da heck I thought this was a cyber defense competition??!!!!

Whoa!

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

CCDC score breakdown

20%
Orange team



40%
Services

40%
Business injects

Fundamental principles of cybersecurity

Integrity

Confidentiality

Availability

Fundamental principles of cybersecurity *(in the context of a business)*

loss of business-critical information

Integrity

damage to reputation and competitive advantage

Confidentiality

interruption of business functions

Availability

Fundamental principles of cybersecurity
(in the context of a business)

The risk of an interruption to business is why we are hired...

damage to reputation and competitive advantage

Confidentiality

Integrity

loss of business-critical information

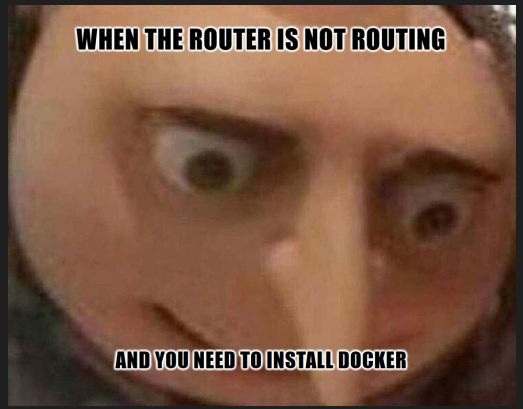
Availability

interruption of business functions

As a result...

we also have an obligation to support the business

It’s more challenging than you think…



Technical tasks

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

Broad understanding

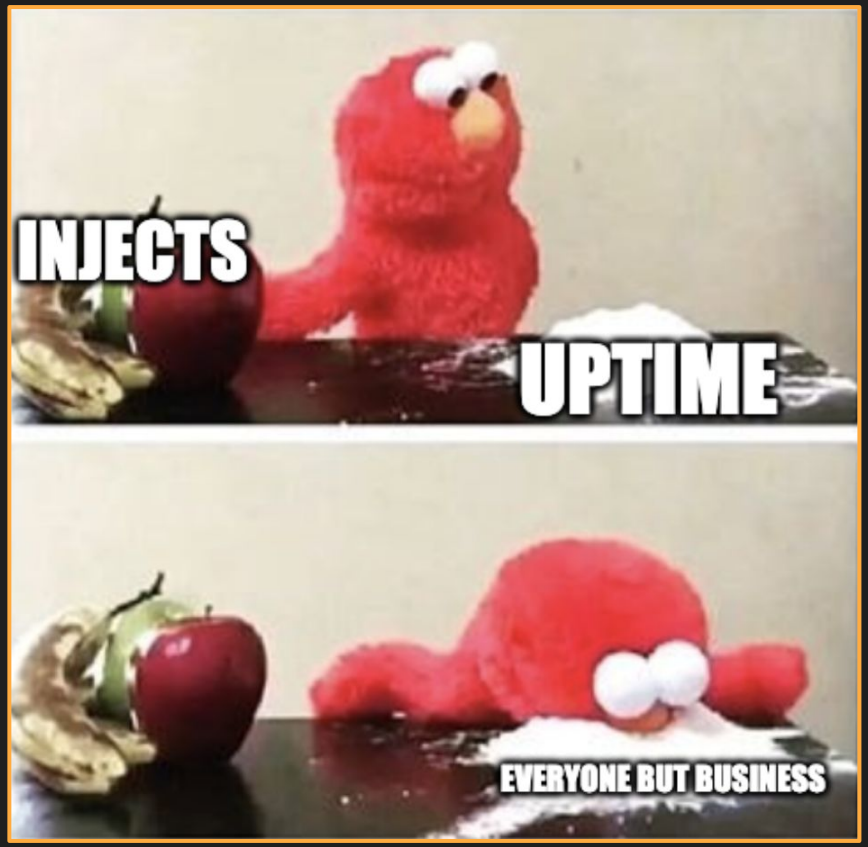
What even is logging and where are the trees???

Who is Ms. Configuration???

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

02
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

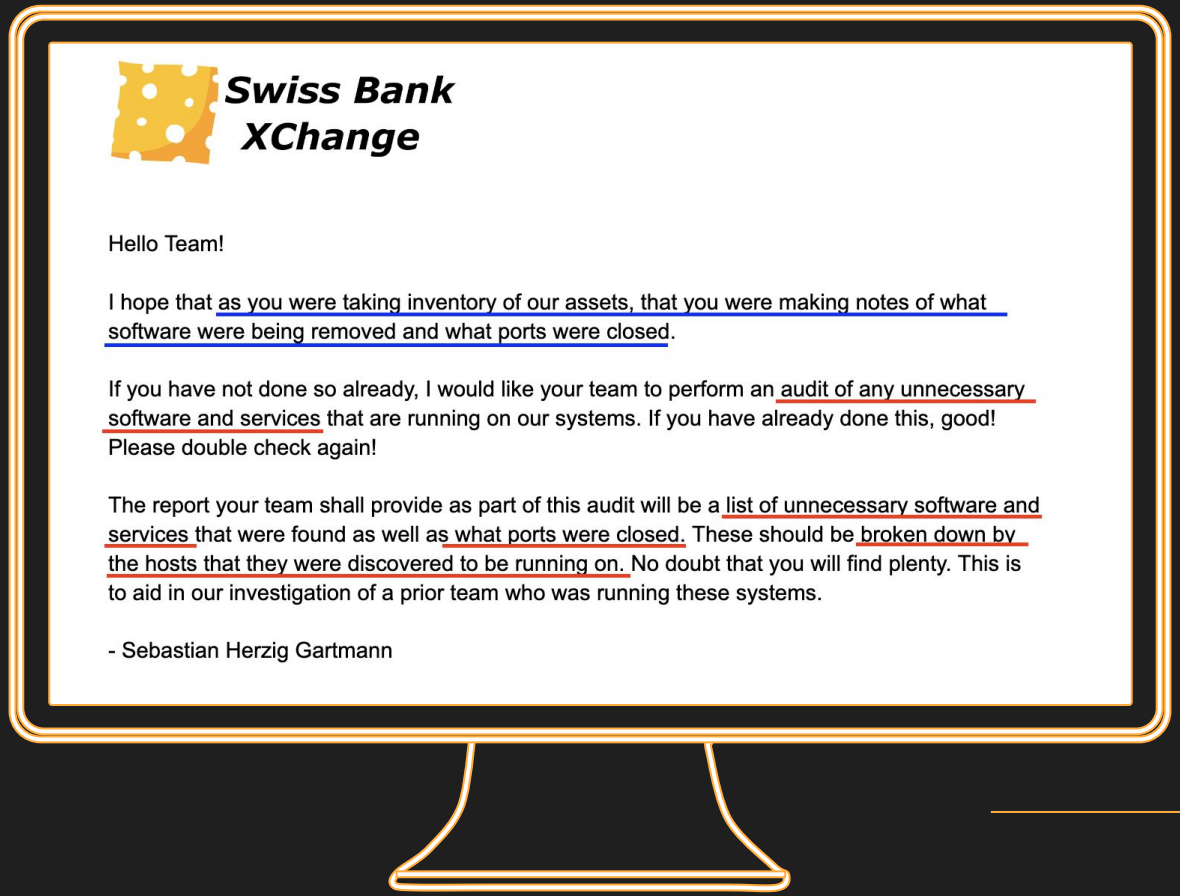
Secret sauce to good injects

be thorough

use clear and concise language

provide supporting evidence

Being thorough



Swiss Bank XChange

Hello Team!

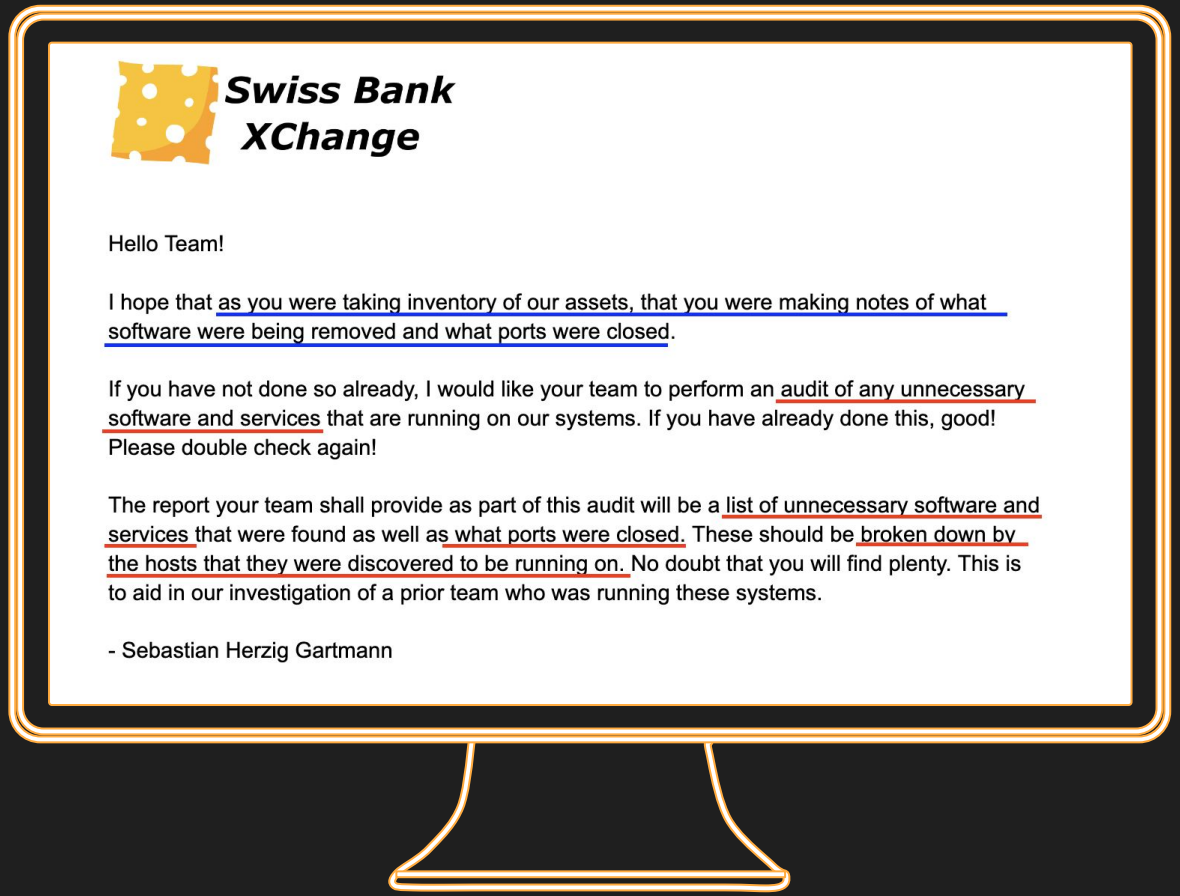
I hope that as you were taking inventory of our assets, that you were making notes of what software were being removed and what ports were closed.

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 professional 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

Takeaways from experience

organization is key

everyone has to contribute

READ THE PROMPT!

03

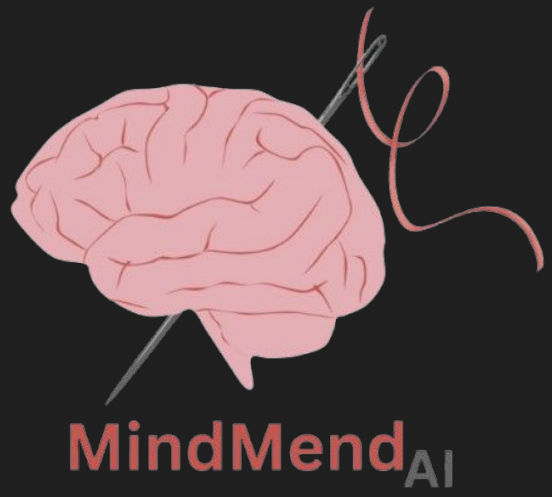
Report to your boss!

Congrats! You're hired :D

Background

The Company

- Name: MindMend
- About: MindMend is an AI therapy startup
- Athena: MindMend's AI assistant
  - Hotline for those who are seeking help with their mental health
  - Made up of database and web interface
  - Has a backup database



It's 4:30 AM, and you got an alert...

Scenario

- You are a part of MindMend's insanely talented AI security team
- Athena's source code files are under a ransomware attack and all of its files are encrypted and unusable
- The bad actors are asking for $1,000,000 in cryptocurrency to make the files usable again

Objective

- 1 page report in email format
- 30 minutes
- Technical report on what caused this for **your manager** who is rushing into the office

Submit: https://jessh.zip/25fall-ccdc-report1

8:30am... your CEO is awake and angry

Scenario

- CEO wakes to "RANSOMWARE ATTACK!" and stoppage of business
- "Why should you keep your jobs if you can't even prevent this?!"

Objectives

- 1 page report in email format to **The CEO**
- 30 minutes
- Explain and justify why the team should **not** be replaced

Submit: https://jessh.zip/25fall-ccdc-report2

Manager

- Technical rundown
- Immediately actionable steps
- Suggestions for alternative solutions
- Technical sources
- Actionable takeaways from the incident

Submit: https://jessh.zip/25fall-ccdc-report1

C-Suite

- Estimated time to restore source code files
- Explain why this task is difficult in layman's terms
- Justify why having the same security team is worth it
- Explain the team's reputation and why you were hired at all

Submit: https://jessh.zip/25fall-ccdc-report2

Q&A

Any questions?

You will love networking.

Yes. You will.

Agenda

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

1

Intro to Networking

Not the LinkedIn one

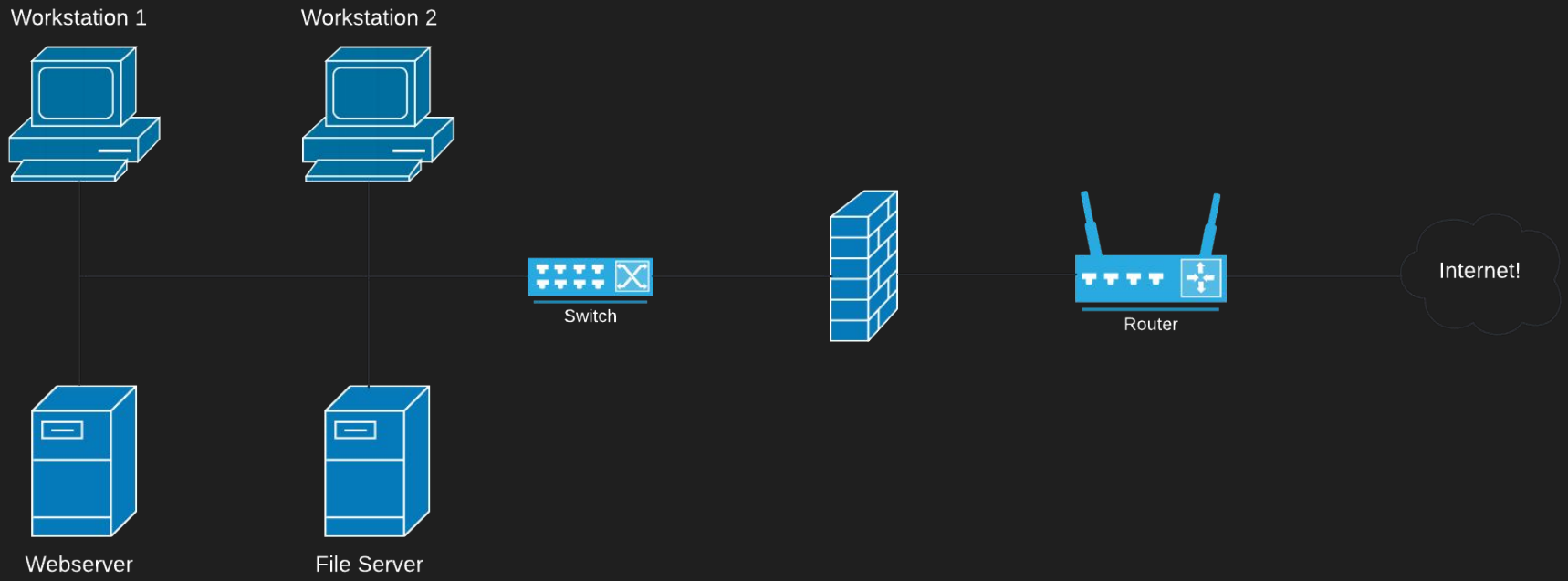
Network

System of interconnected network devices
- Communicate and share resources

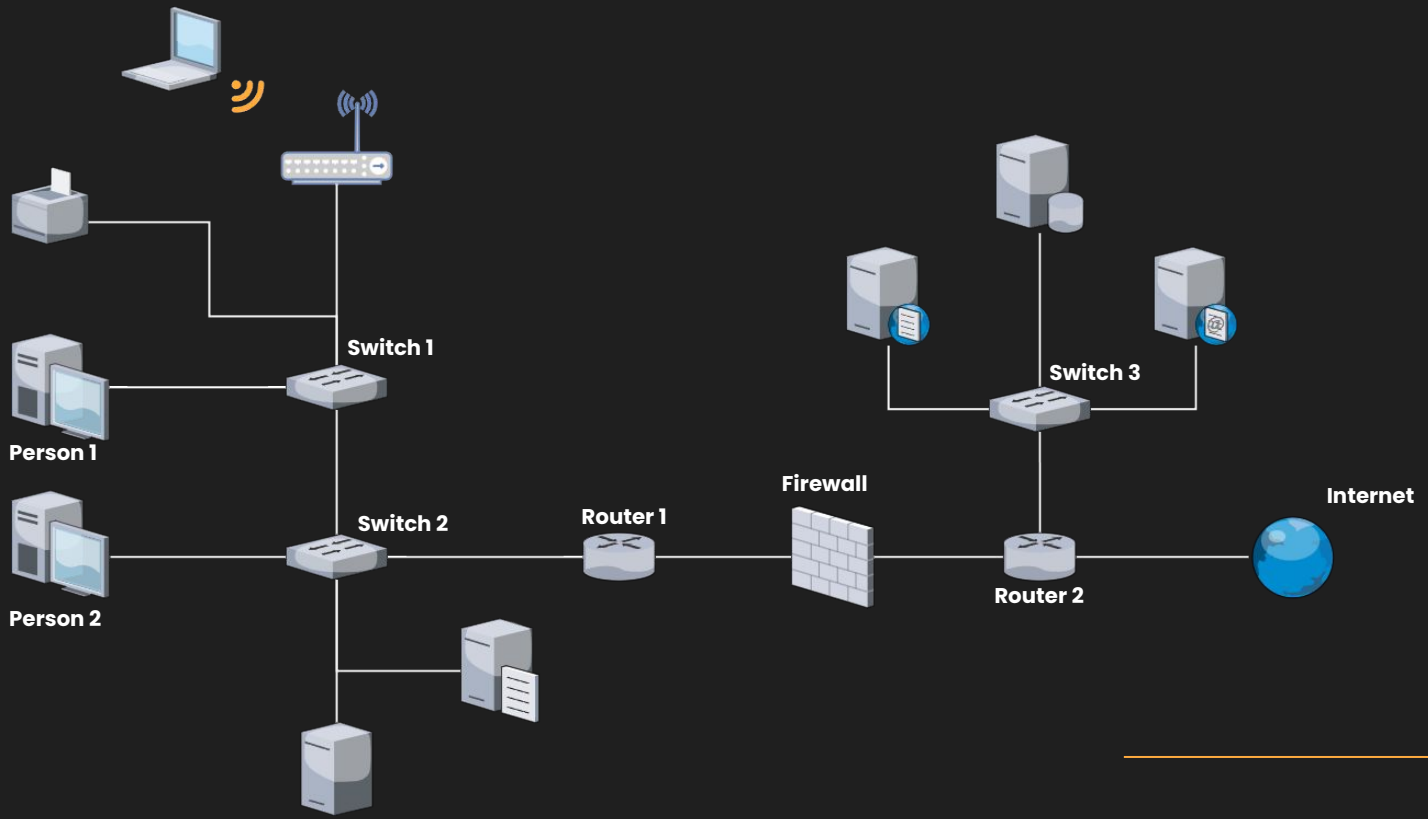
Network Devices

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

Subnet Masks

IPv4 address → 192.168.1.100

255.255.255.0 → **Subnet Mask**

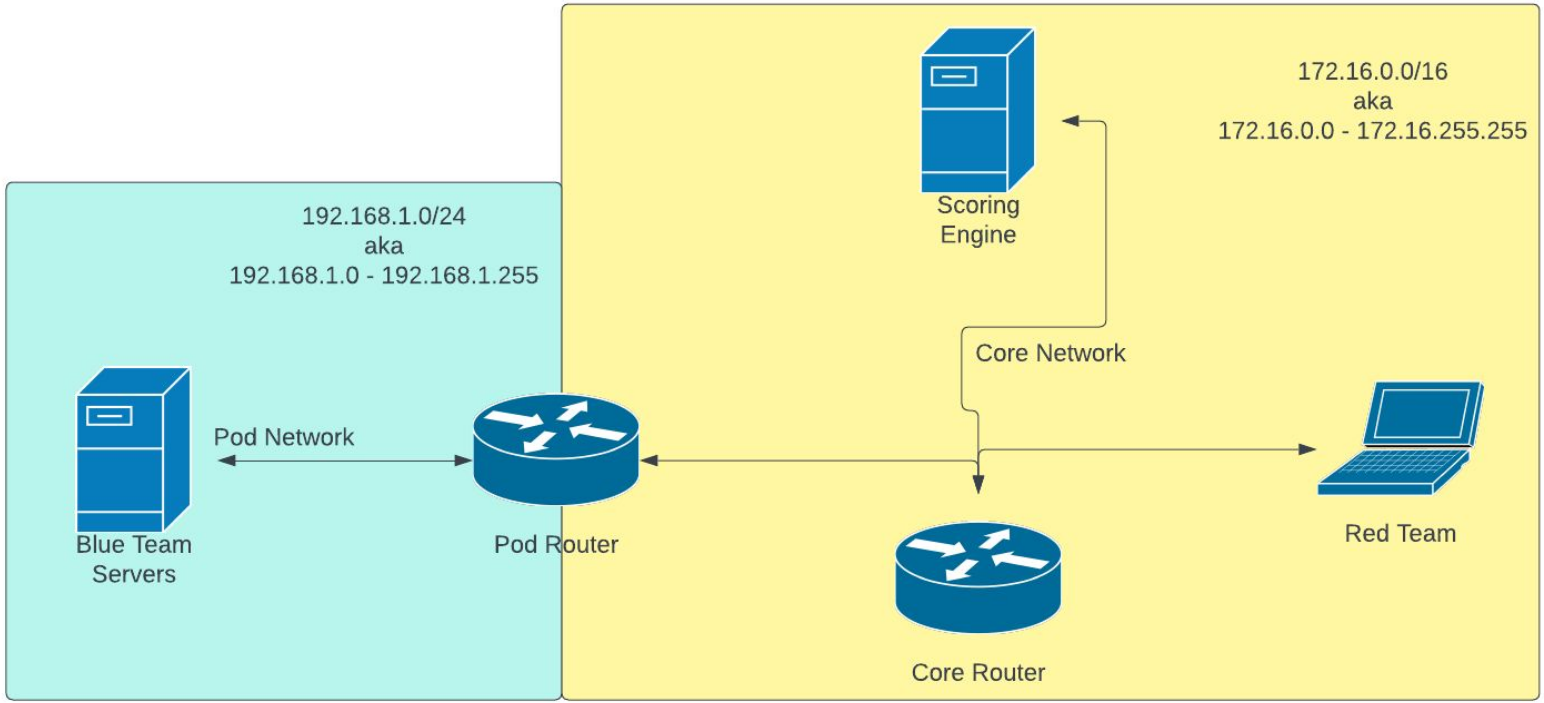
```
IPv4 Address. . . . . . . . . . . : 192.168.1.115
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
```

2

Competition Networking

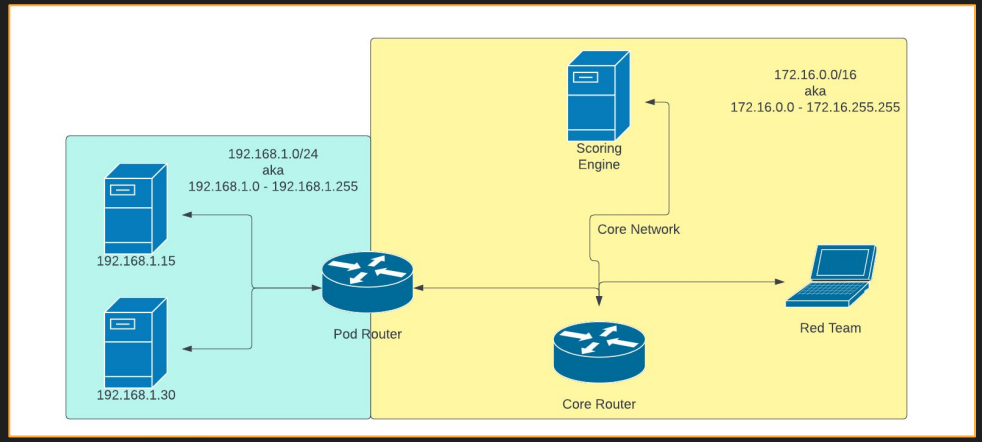
Services go brrrrr

Competition Topology

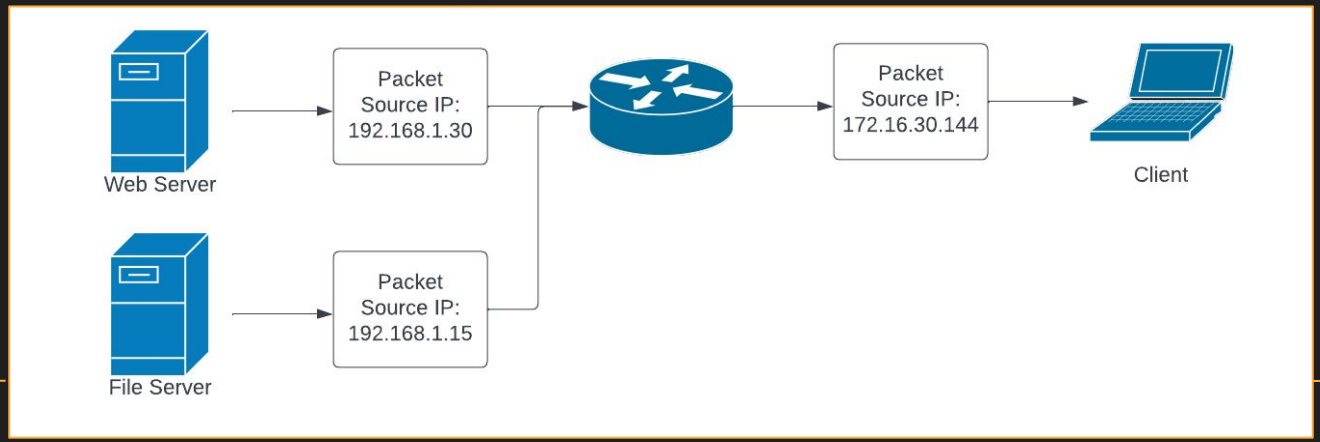


NAT

- Network Address Translation
- Built to conserve IP addresses

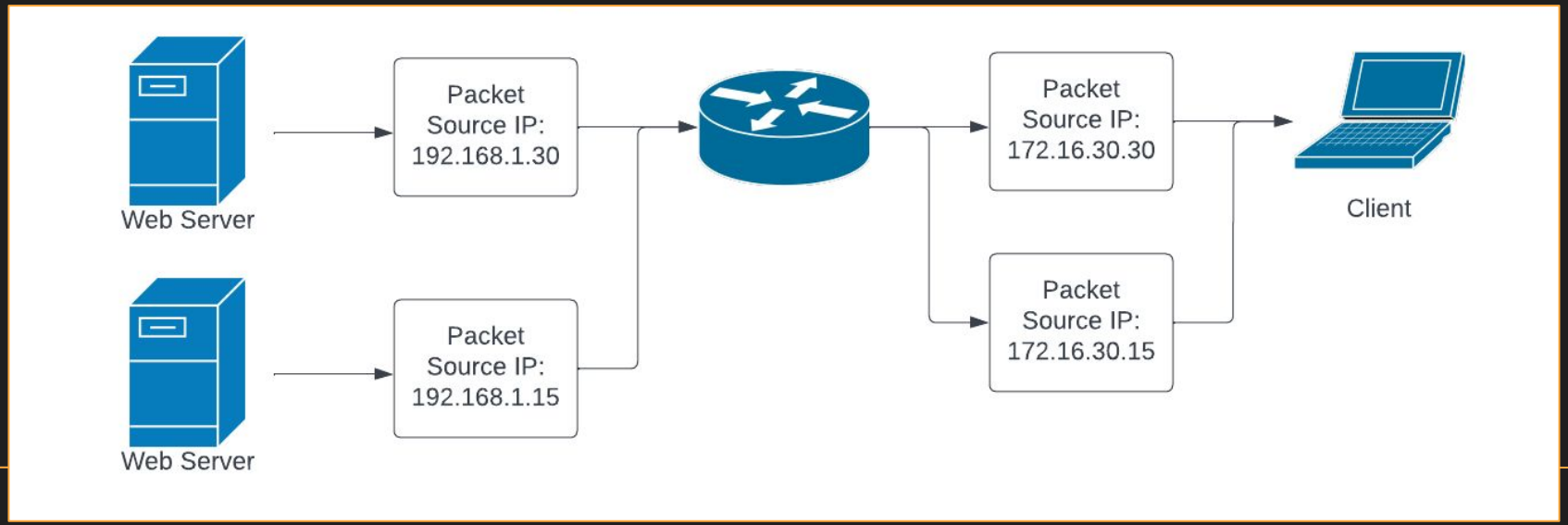


One-to-Many Translation:



1:1 NAT

- Direct Translations
- 192.168.1.0/24 → 172.16.30.0/24

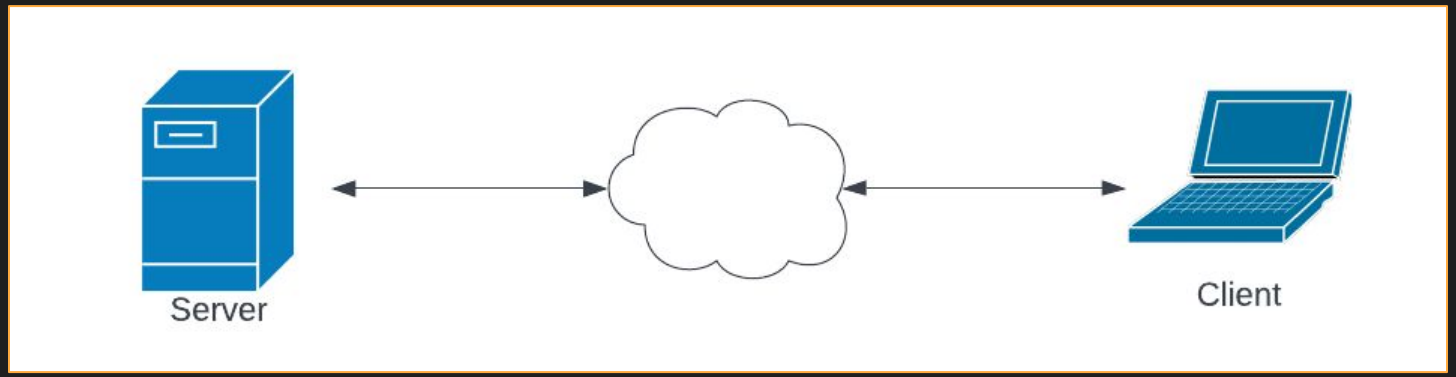


3

Client-Server Model

Packet restaurant

Client–Server Model



What are ports?

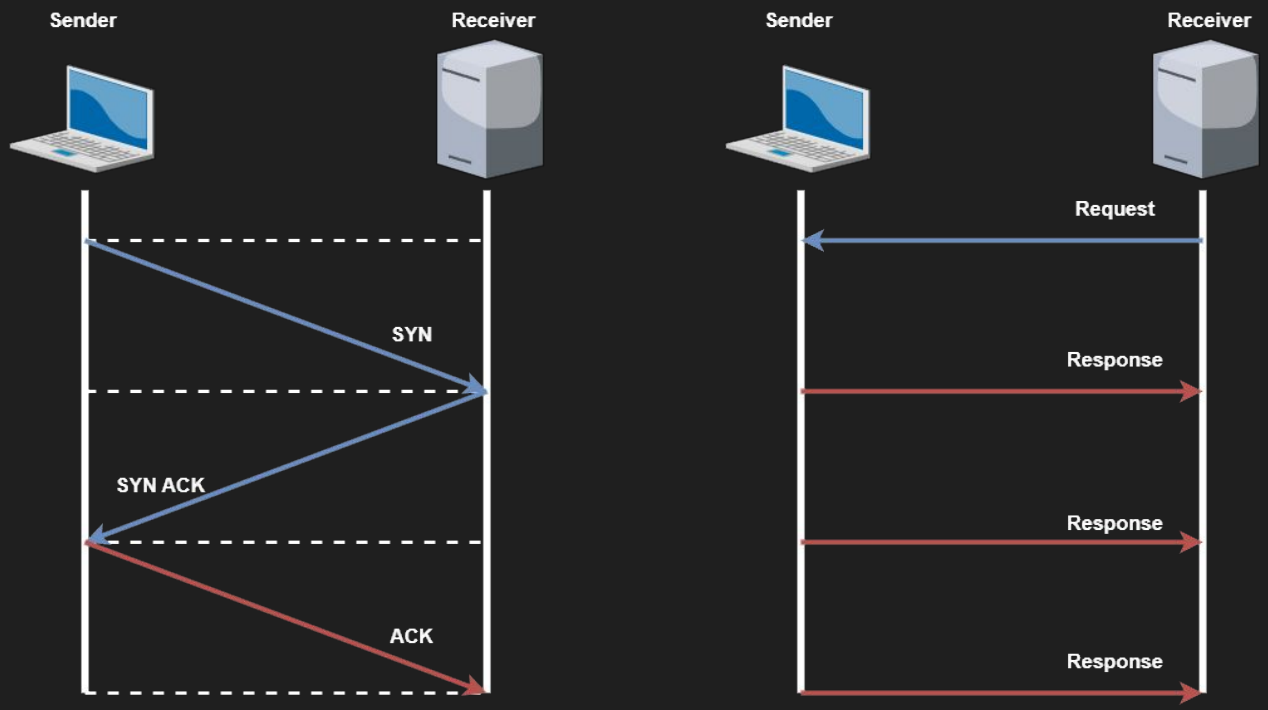
Numbers that identify, along with an IP address, which network socket to connect to on a given device.

- 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

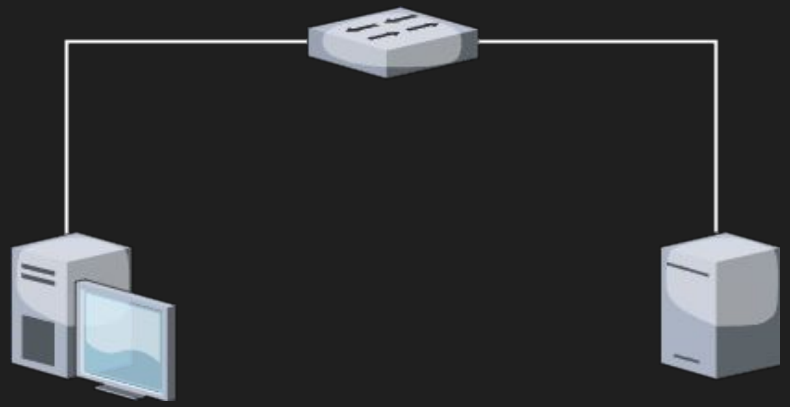
- TCP - Slow but reliable
  - Synchronization
  - Flow control
  - TCP Handshake
- UDP - Fast but unreliable
  - No error-checking
  - No acknowledgements
  - Just send data

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

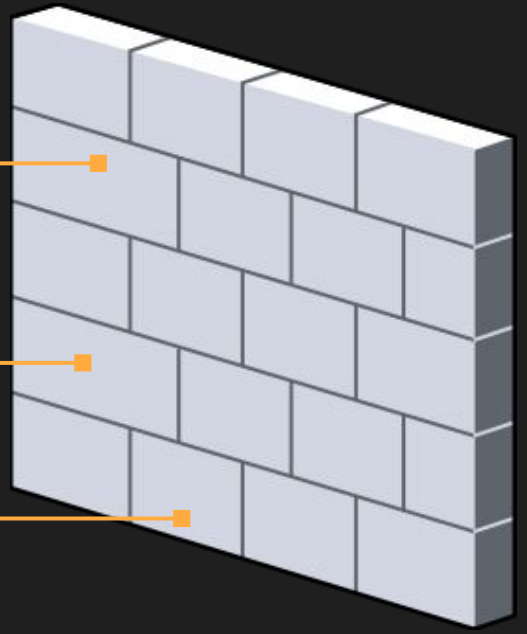
Can block a whole subnet or individual.

Block Ports

Block which ports the external network can access on the LAN

Filtering

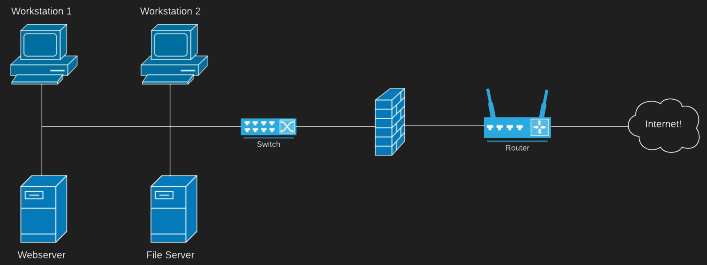
Ingress and Egress filtering rules.



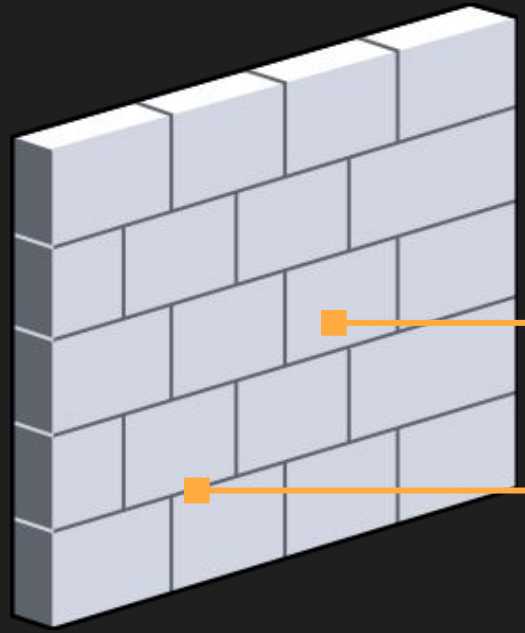
Host Firewall vs Network Firewall

- 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



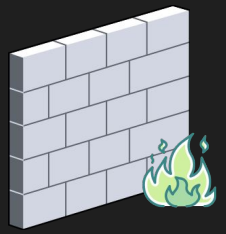
Stateless

ACL. Looks at
Individual packets.

Stateful

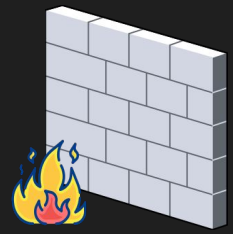
Traffic patterns and flows.
Remembers connections.

NGFW vs Traditional



- Stateful Inspection on incoming and outgoing traffic
- Comprehensive application control and visibility
- Easy to install, configure, integrate security tools, reducing administrative controls
- SSL traffic can be decrypted and inspected.
- IPS & IDS are integrated

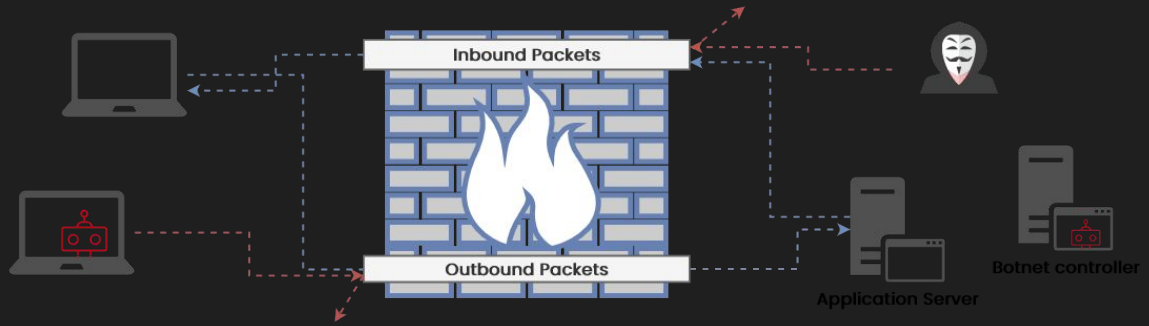
- Stateful Inspection on incoming and outgoing traffic
- Partial application control and visibility only
- Managing security tools separately is $$$
- Cannot decrypt and inspect SSL traffic
- Integrated IPS and IDS are deployed separately in traditional firewalls



FW Example

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

Outbound
- Block everything going outbound (break internet)



6

Lab !!

(it's not packet tracer, i swear)

Any Questions?

Please ask! We are here to help :D

Homework (Due 9/6 @5:00 AM)

https://jessh.zip/ccdcfallhw1