Botball 2023

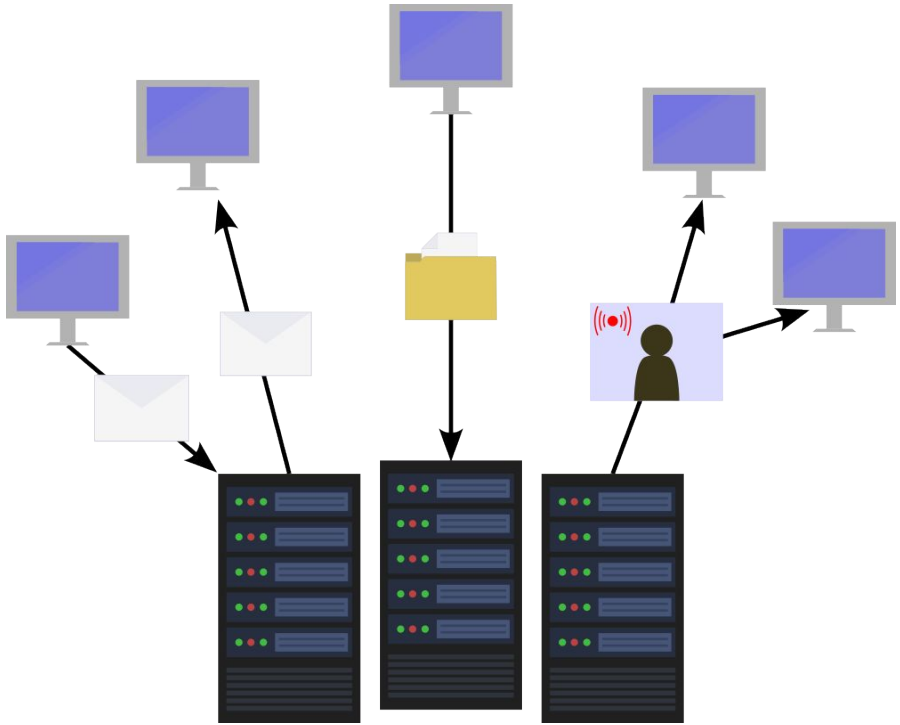
Learning to be an Ethical Hacker

Data Centers & Servers

Data centers store, process, & send data

They host Internet-connected services that users interact with

- Email servers
- Streaming services
- Websites
- File storage



Real Facts:

The International Data Corporation (IDC) predicted that by 2025, **the amount of data created, captured, or replicated will grow to 175 zettabytes**!

To put that in perspective, that's **~175 times the number of stars in the observable universe**!

Servers have special requirements

Must handle heavy load & many users: powerful hardware

Must always be available: backups are essential

- Hardware failure
- Data loss
- Cyber attacks

Think About It:

Why may an attacker target a data center?

Money

Steal user information

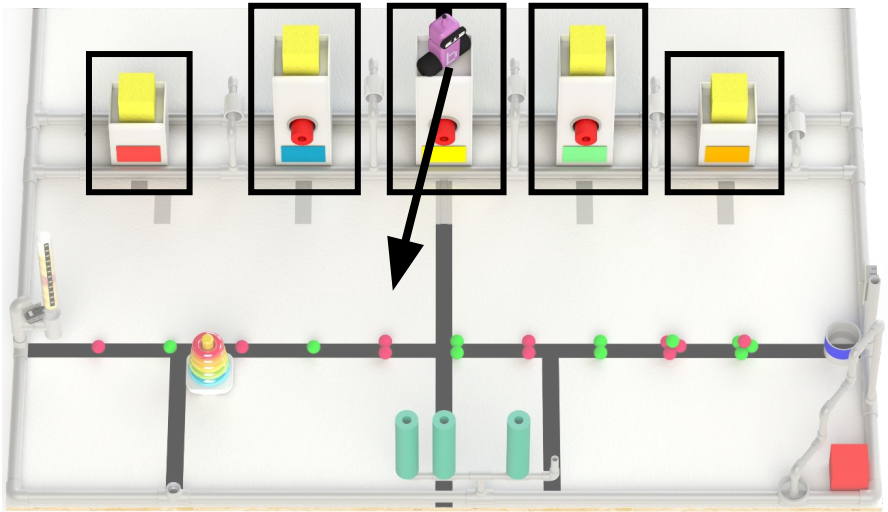
Fun

Take down a business

The Game: Data Center & Servers

Botgal wants to start out her day in the server room.

Get Botgal over to your team's Data Center!

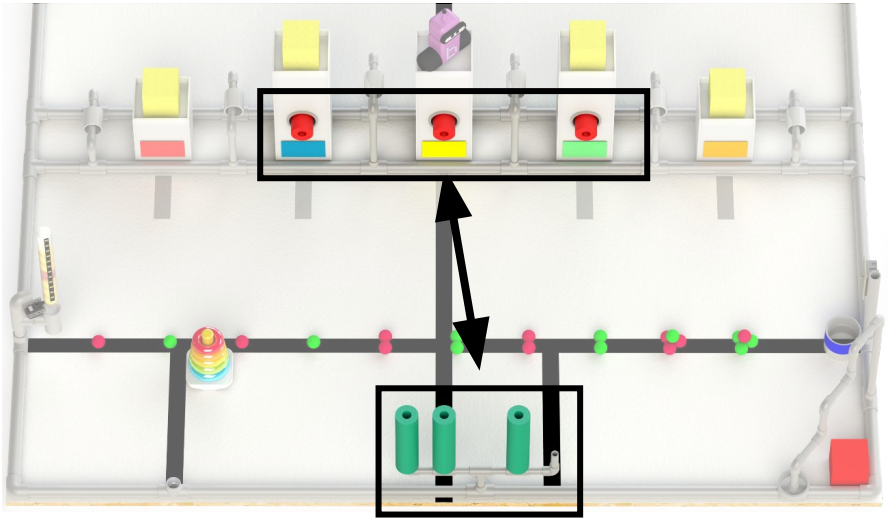


The Game: Hard Drives

Botgal discovers some of the server drives have gotten corrupted

- Thankfully, Botgal regularly backs up her servers' drives

You team can help Botgal by taking out the corrupted red hard drives and replacing them with the green backup drives

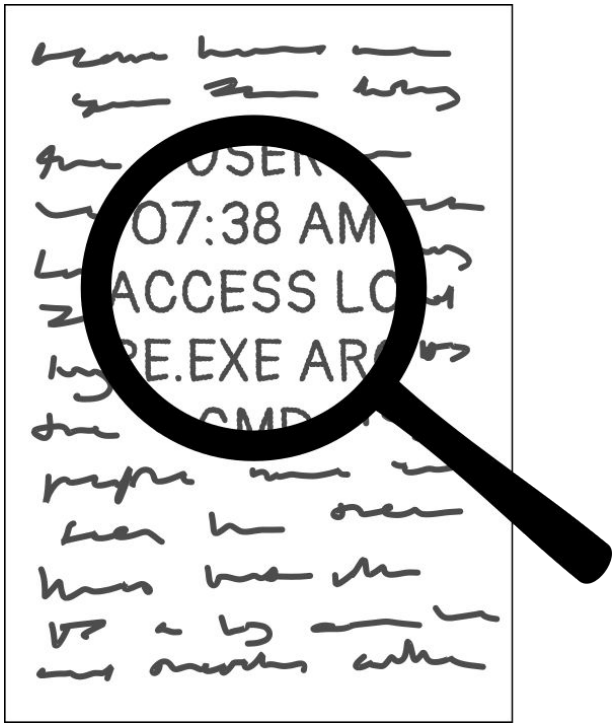


Server Logs

Server logs store information about server usage

This may include:

- Who connected to the server
- What a user did on the server
- What files were accessed
- What software was installed
- When actions occurred
- Software-specific information



Server logs paint a picture of anomalies

Keep a snapshot of "normal operations"

Compare with current logs to see if anything appears abnormal

Think About It:

Why may Botgal want to monitor the server logs?

Figure out when something broke

Find attackers

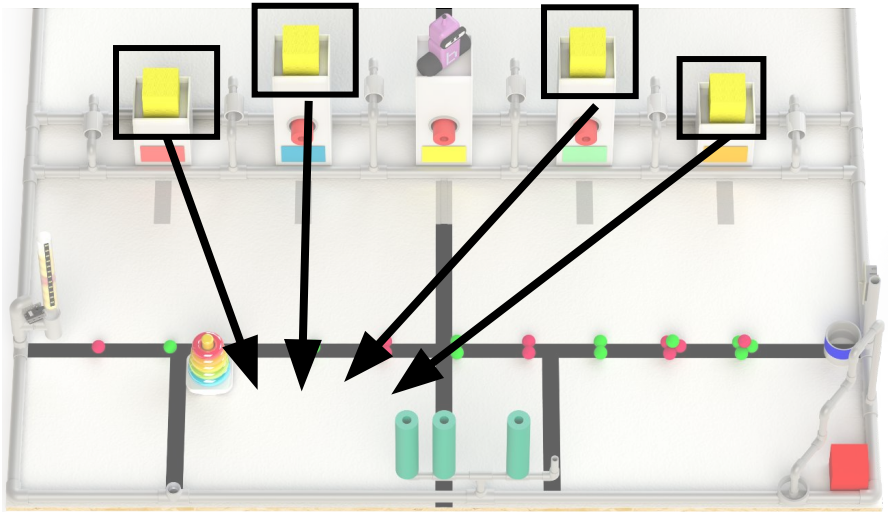
Troubleshoot errors

The Game: Server Logs

Each of the servers keeps a server log

- Botgal regularly checks them for anomalous activity

Your team will need to take the logs to the Analysis Lab

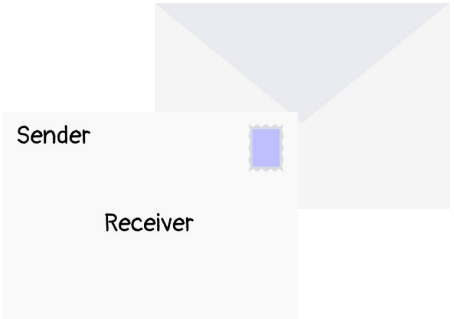


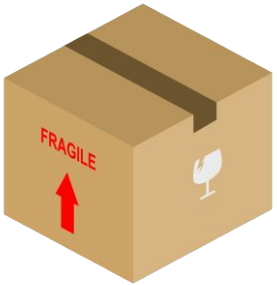
Network Connections

Network connections are made up of packets

Think of packets like mail

- **Inside:** Item being sent
- **Outside:** Extra information
  - Sender name & address
  - Receiver name & address
  - How to handle it
  - How it should be routed
- **Multiple layers**





Real Facts:

Computer worms are viruses that replicate themselves, typically over a network.

One of the oldest worms, **the Morris worm**, was created by a Cornell student to highlight security issues in network-adjacent software.

A bug was left in the worm that unintentionally let it spread rapidly, **infecting and reinfecting computers, slowing them down, and making them unusable**.

Networks are an attacker's way into a system

Software connected to a network provides an attack surface for attackers to get into the system

- Misconfigurations
- Exploits
- Stolen credentials

Think About It:

What are some network-connected technologies that attackers may target?

Browsers

Routers

Servers

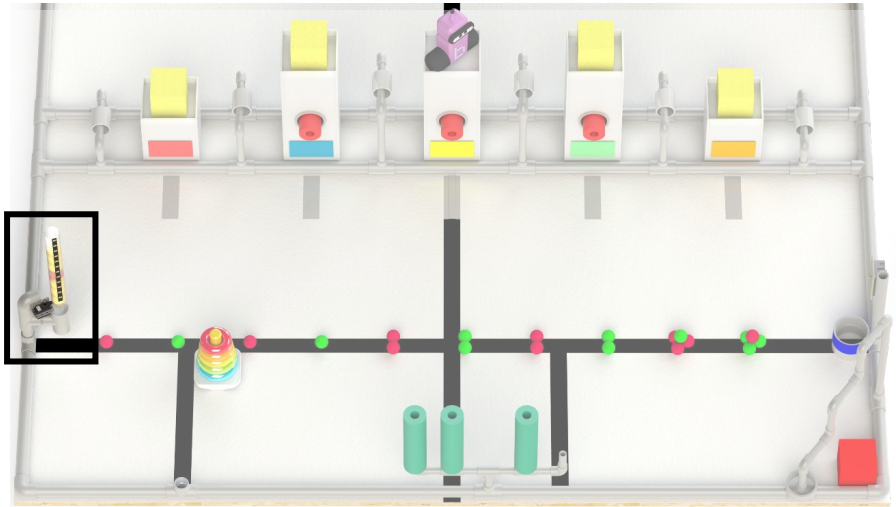
Video games

The Game: Network Connections

The external network connection has incoming packets

- Some may be normal, some may be malicious

Your team will need to analyze the packets

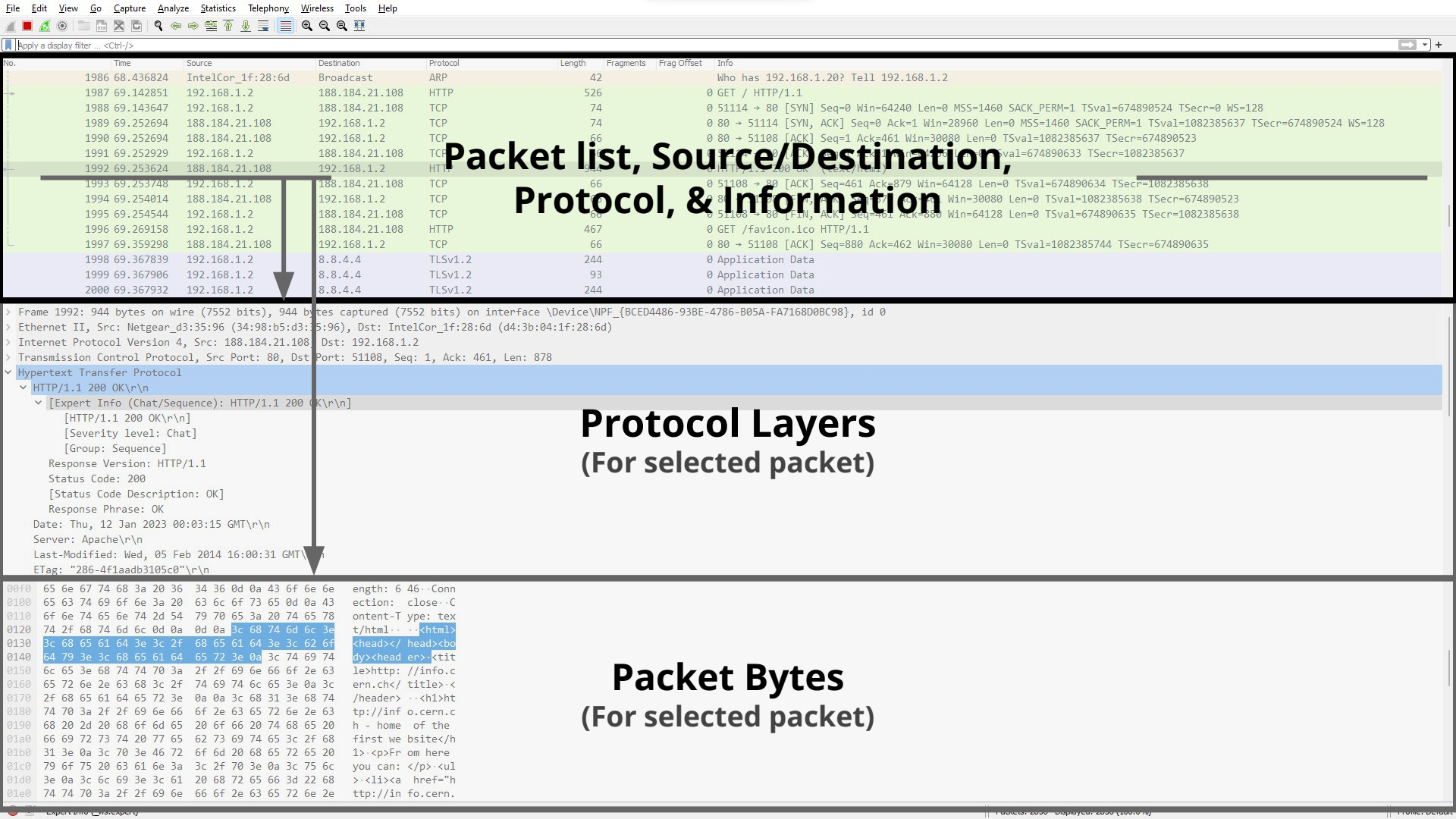


Wireshark

Wireshark is used to collect & analyze network traffic

A powerful tool used by cybersecurity engineers

- Analyze overall traffic and individual packets
- Analyze each layer of packets and protocols
- Analyze bytes in packets


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Fragments Frag Offset Info
1986 68.436824 IntelCor_1f:28:6d Broadcast ARP 42 Who has 192.168.1.20? Tell 192.168.1.2
1987 69.142851 192.168.1.2 188.184.21.108 HTTP 526 0 GET / HTTP/1.1
1988 69.143647 192.168.1.2 188.184.21.108 TCP 74 0 51114 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=674890524 TSecr=0 WS=128
1989 69.252694 188.184.21.108 192.168.1.2 TCP 74 0 80 → 51114 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1082385637 TSecr=674890524 WS=128
1990 69.252694 188.184.21.108 192.168.1.2 TCP 66 0 80 → 51108 [ACK] Seq=1 Ack=461 Win=30080 Len=0 TSval=1082385637 TSecr=674890523
1991 69.252929 192.168.1.2 188.184.21.108 TCP 66 0 51108 → 80 [ACK] Seq=461 Ack=879 Win=64128 Len=0 TSval=674890633 TSecr=1082385637
1992 69.253624 188.184.21.108 192.168.1.2 HTTP 944 0 HTTP/1.1 200 OK (text/html)
1993 69.253748 192.168.1.2 188.184.21.108 TCP 66 0 51108 → 80 [ACK] Seq=461 Ack=879 Win=64128 Len=0 TSval=674890634 TSecr=1082385638
1994 69.254014 188.184.21.108 192.168.1.2 TCP 66 0 80 → 51108 [FIN, ACK] Seq=879 Ack=461 Win=30080 Len=0 TSval=1082385638 TSecr=674890523
1995 69.254544 192.168.1.2 188.184.21.108 TCP 66 0 51108 → 80 [FIN, ACK] Seq=461 Ack=880 Win=64128 Len=0 TSval=674890635 TSecr=1082385638
1996 69.269158 192.168.1.2 188.184.21.108 HTTP 467 0 GET /favicon.ico HTTP/1.1
1997 69.359298 188.184.21.108 192.168.1.2 TCP 66 0 80 → 51108 [ACK] Seq=880 Ack=462 Win=30080 Len=0 TSval=1082385744 TSecr=674890635
1998 69.367839 192.168.1.2 8.8.4.4 TLSv1.2 244 0 Application Data
1999 69.367906 192.168.1.2 8.8.4.4 TLSv1.2 93 0 Application Data
2000 69.367932 192.168.1.2 8.8.4.4 TLSv1.2 244 0 Application Data
Packet list, Source/Destination, Protocol, & Information
Frame 1992: 944 bytes on wire (7552 bits), 944 bytes captured (7552 bits) on interface \Device\NPF_{BCED4486-93BE-4786-B05A-FA7168D0BC98}, id 0
Ethernet II, Src: Netgear_d3:35:96 (34:98:b5:d3:35:96), Dst: IntelCor_1f:28:6d (d4:3b:04:1f:28:6d)
Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.1.2
Transmission Control Protocol, Src Port: 80, Dst Port: 51108, Seq: 1, Ack: 461, Len: 878
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Thu, 12 Jan 2023 00:03:15 GMT\r\n
Server: Apache\r\n
Last-Modified: Wed, 05 Feb 2014 16:00:31 GMT\r\n
ETag: "286-4f1aadb3105c0"\r\n
Protocol Layers
(For selected packet)
00f0 65 6e 67 74 68 3a 20 36 34 36 0d 0a 43 6f 6e 6e ength: 6 46··Conn
0100 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 43 ection: close··C
0110 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 ontent-T ype: tex
0120 74 2f 68 74 6d 6c 0d 0a 0d 0a 3c 68 74 6d 6c 3e t/html·· ··<html>
0130 3c 68 65 61 64 3e 3c 2f 68 65 61 64 3e 3c 62 6f <head></ head><bo
0140 64 79 3e 3c 68 65 61 64 65 72 3e 0a 3c 74 69 74 dy><head er>·<tit
0150 6c 65 3e 68 74 74 70 3a 2f 2f 69 6e 66 6f 2e 63 le>http: //info.c
0160 65 72 6e 2e 63 68 3c 2f 74 69 74 6c 65 3e 0a 3c ern.ch</ title>·<
0170 2f 68 65 61 64 65 72 3e 0a 0a 3c 68 31 3e 68 74 /header> ··<h1>ht
0180 74 70 3a 2f 2f 69 6e 66 6f 2e 63 65 72 6e 2e 63 tp://inf o.cern.c
0190 68 20 2d 20 68 6f 6d 65 20 6f 66 20 74 68 65 20 h - home of the
01a0 66 69 72 73 74 20 77 65 62 73 69 74 65 3c 2f 68 first we bsite</h
01b0 31 3e 0a 3c 70 3e 46 72 6f 6d 20 68 65 72 65 20 1>· Fr om here
01c0 79 6f 75 20 63 61 6e 3a 3c 2f 70 3e 0a 3c 75 6c you can: ·<ul
01d0 3e 0a 3c 6c 69 3e 3c 61 20 68 72 65 66 3d 22 68 >·
<a href="h
01e0 74 74 70 3a 2f 2f 69 6e 66 6f 2e 63 65 72 6e 2e ttp://in fo.cern.
Packet Bytes
(For selected packet)

Abnormal traffic can highlight issues

Constant traffic monitoring can allow issues to be addressed immediately!

- Misbehaving software & hardware
- Attackers attempting to get on a system
- Malware already on a system

Think About It:

What types of odd network behavior may you look for?

Traffic at odd hours

Too much traffic

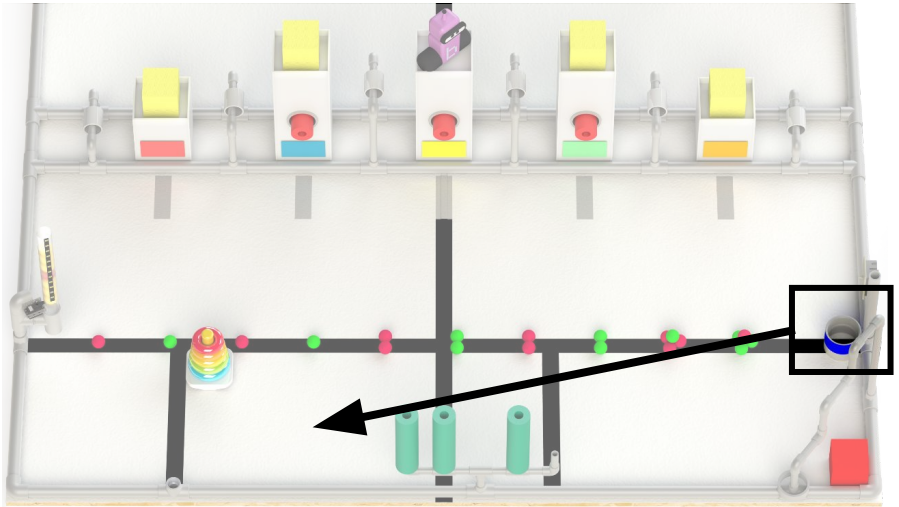
Uncommon types of traffic

The Game: Wireshark

Botgal needs to analyze any packets that seem out of the ordinary

Your team will need to

1. Move the tool to the **Analysis Lab**
2. Place the **malicious packet** inside



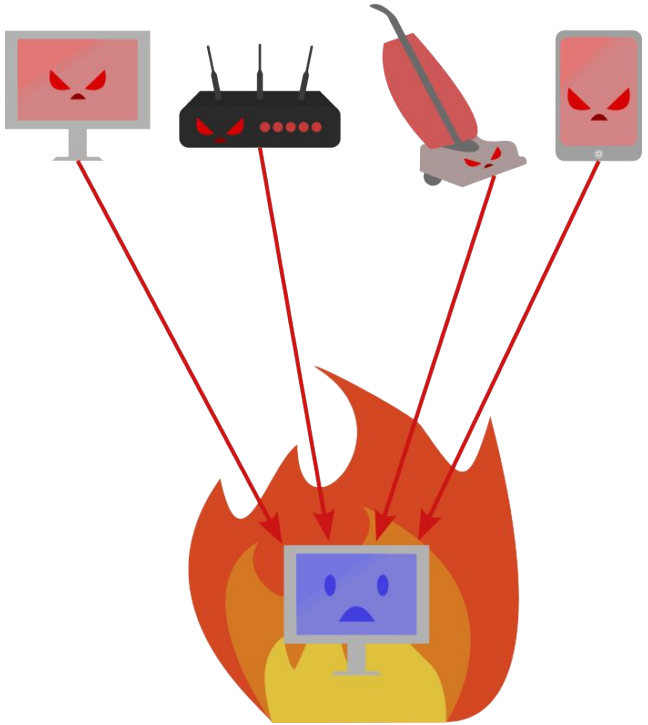
DDoS Attacks

DDoS (Distributed Denial of Service) Attacks

An attack where a server is overwhelmed by the number of requests it receives.

Attackers use botnets to perform DDoS attacks

- A group of Internet-connected devices under an attacker's control



Real Facts:

In 2016, 3 college students created the **Mirai malware**, which would scan for IoT (Internet of Things) devices and take control of any with a default password, forming the **Mirai botnet.**

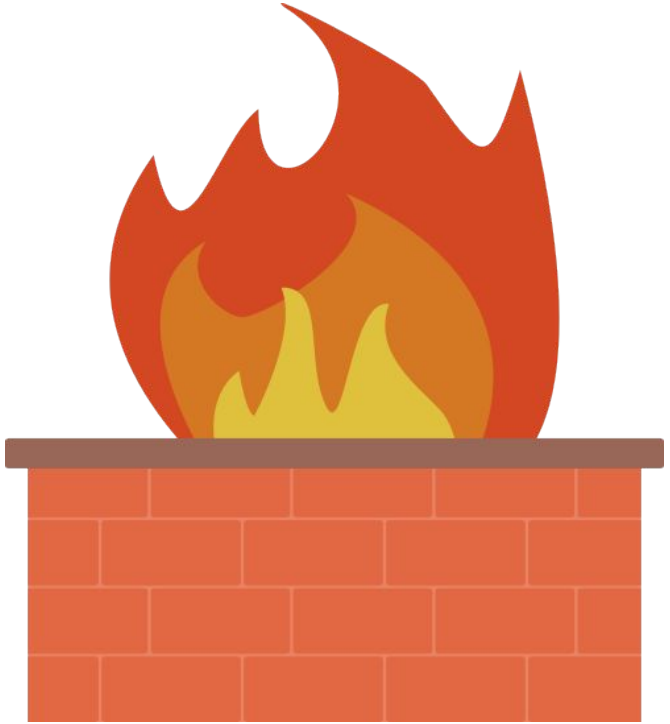
They used this to **launch DDoS attacks on other Minecraft servers** to lure people to pay to use theirs.

On October 21, 2016, the **Mirai botnet was used by cyber threat attackers to DDoS Internet infrastructure**, making many high-profile websites - Github, Twitter, Reddit, Netflix, Paypal, Amazon, Spotify, & more - inaccessible for a few hours.

Firewalls control incoming & outgoing connections

Can allow or disallow connections

- By port
- By application
- By user



Think About It:

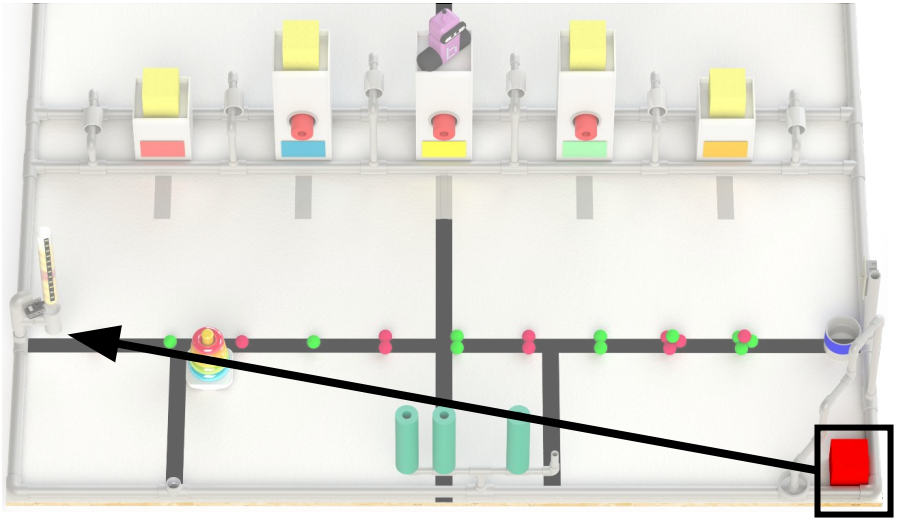
Why may Botgal want to set up a firewall?

Incoming Traffic	Outgoing Traffic
Block unauthorized access	Prevent malware from spreading
Protect against DDoS attacks	Segment off the network

The Game: Firewalls

Botgal can use the firewall to prevent any more incoming external connection

Your team will have to block off the external connections with the firewall



Malware & Ransomware

Malware is malicious software

The goals can vary:

- Damage machines
- Steal user data
- Money
- Fun
- "Street creds"

Command and Control (C&C) can be used to control many compromised devices at once

Ransomware: Your data is the hostage

It has become a common type of malware where **attackers encrypt your data and will only decrypt it for money**.

Hospitals are sadly a common target for ransomware attackers.

Real Facts:

In May 2021, Colonial Pipeline, providing ~45% of the East Coast's fuel was **hit by a ransomware attack from Russia-linked cybercriminals**.

Between equipment disruptions and mass panic buying, gas prices skyrocketed and in many areas, was **completely sold out**.

Research helps prevent & mitigate ransomware

Security researchers can analyze ransomware and identify

- Detection methods to **thwart future attacks**
- How to **recover decryption keys for current attacks**

Think About It:

What could you do to deal with ransomware attacks?

Make frequent backups of files

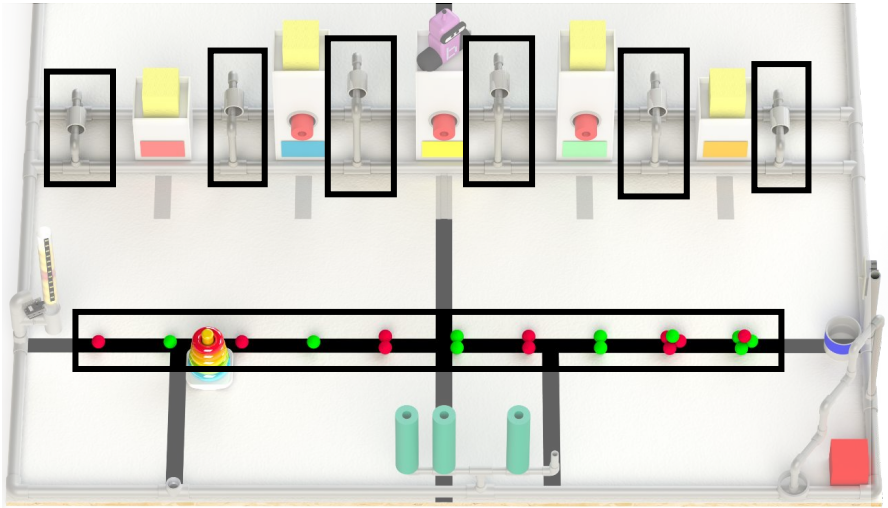
Install antivirus software

The Game: Files & Encryption

It seems like Strange Software was ransomware!

- Some of the files are corrupted
- The corrupted files are likely encrypted
- Encryption keys will be needed to recover the files

Your team will have to sort through for the corrupted files & get the encryption keys to recover them.



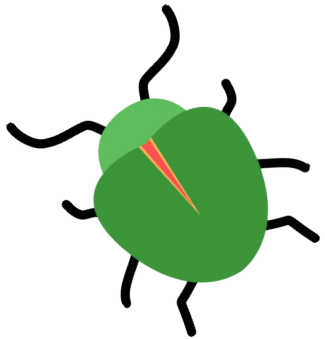
Vulnerabilities

Vulnerabilities give attackers leverage

Vulnerabilities are security bugs that can be leveraged by an attacker to gain access or privileges they normally wouldn't have access to

- Connect into a system
- Read/write/execute files

Exploits can use one or more vulnerabilities to accomplish an attacker's goal



Real Facts:

Since 2021, dozens of security vulnerabilities have been reported in Microsoft Exchange. **Patches for these vulnerabilities have rolled out slowly, and server administrators have additionally been slow on applying them.**

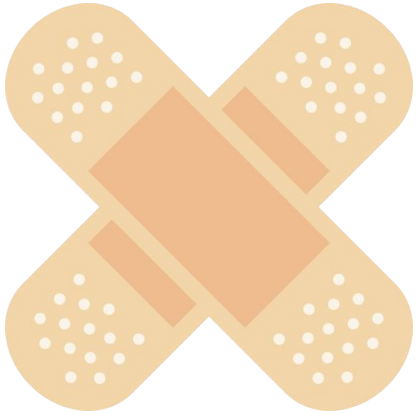
Attackers have taken advantage of this to **hack these email servers**, even **using the exploits in their ransomware** as an entry point into the system.

Patches update software to fix bugs

Some may fix security vulnerabilities

N-days are vulnerabilities that have been seen before and have hopefully been patched

0-days are vulnerabilities that have *never* been seen before



Think About It:

What are 0-days particularly dangerous?

0-days have never been seen before.
That means there is no patch!

If an attacker uses a 0-day, there is nothing stopping them...
...until a patched is created!

Think About It:

Why may N-days still be dangerous?

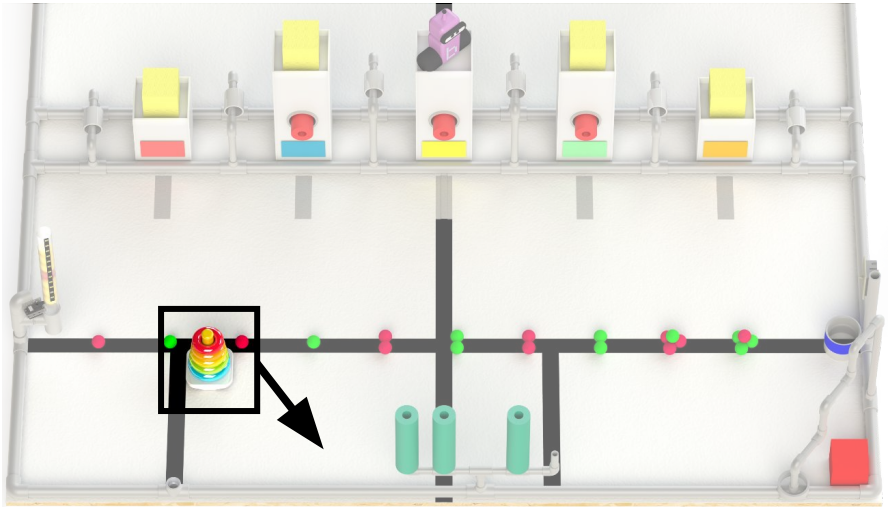
Just because a vulnerabilities is known **doesn't mean a patch has been created or applied.**

Developers must **identify the bugs & create patches.**
Security engineers must **apply the patches.**

The Game: Patches

The developers released urgent security patches

You'll need to deploy the patches to prevent the server from getting re-exploited!



Reverse Engineering

Reversing malware can give information about it

- **Static Analysis** involves analysis without running an executable
- **Dynamic Analysis** involves analysis while running an executable

Real Facts:

In 2017, the WannaCry ransomware used a Windows vulnerability to spread amongst hundreds of thousand of computers.

A security researcher, MalwareTech, **reverse engineered the malware and noted an odd-looking domain**: *iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com*.

He bought the domain to see how the malware would interact with it, and soon realized the malware stopped spreading. **He had stumbled into the malware kill switch - the existence of the domain!**

Reverse engineering malware for defense

1. Understand how the malware works
2. Note properties specific to the malware
3. Look for those properties in the future to alert on

This is how antivirus software detects viruses!

Think About It:

What about the malware could we use to detect it in the future?

Network connections

Files created

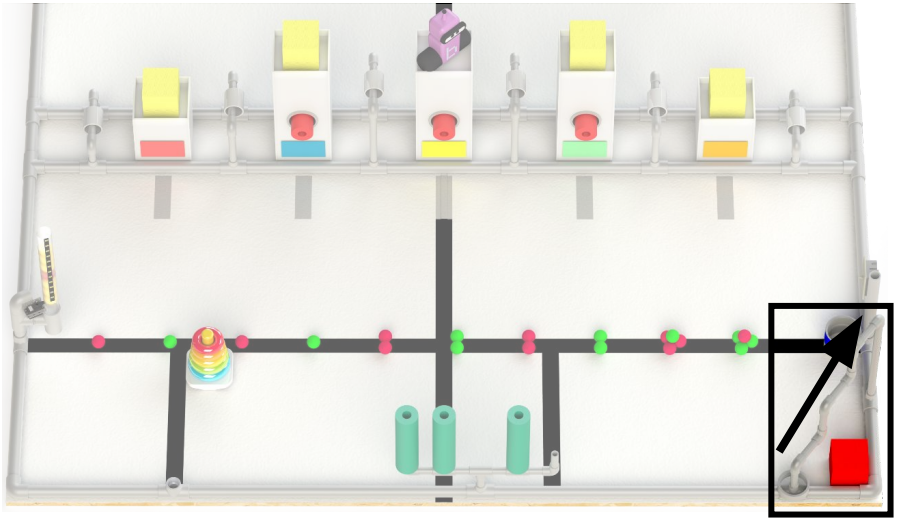
Text in the malware

Name of process

The Game: Reverse Engineering

Your team can assist with the reverse engineering

Use the reverse engineering tool to examine the malware



So you wanna learn hacking?

Wait what... I thought hackers were the bad guys?

Nope! Just like anything - there's a good and bad side to everything.

It depends how you use your knowledge! Be an ethical hacker!

Think About It:

What are some ways you could use your security knowledge for good?

Find vulnerabilities & report them

Respond to cyber attacks

Reverse engineer malware

Design secure computer systems

How do I learn more?

A lot of these details were abstracted or simplified to make them easier to understand!

If you want to learn more, there's plenty of security resources online.

CTFs

- picoCTF
- pwn.college

YouTube

- LiveOverflow: General Security Education