Botball 2023: Learning to be an Ethical Hacker Instructor Notes

Hello fellow instructor! This year's Botball theme is Cybersecurity and Ethical Hacking. As a part of the theme, **we are providing materials that you may use to educate your students on the cybersecurity concepts touched on in the backstory, game board, and rules.** These materials include slides, an outline of an example presentation, and additional recommendations on resources or how you may engage your students.

These instructor notes are meant to provide a guide to what a presentation on the material *may* look like, but are by no means the only way to present them!

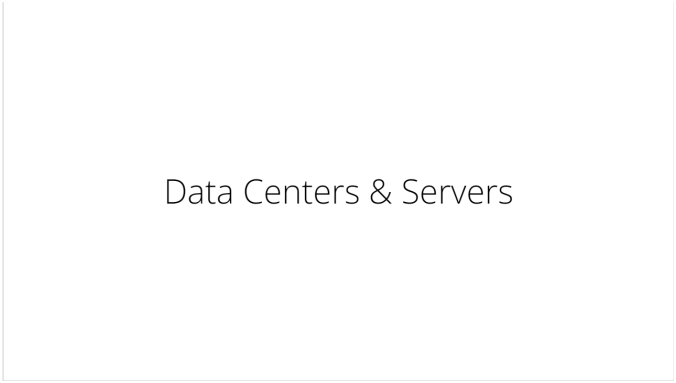
Introduction

Slide 1: Botball 2023

Goal	*Introduce the point of the presentation - namely, to educate students on cybersecurity topics by tying them into the game pieces used on the Botball board.*
Transcript	This year's Botball theme is cybersecurity. While hacking to many of you may be left to cool scenes in action movies, there are plenty of people doing the same work every day! Today, we'll talk about the Botball game board pieces, and a bit about what each of them mean.

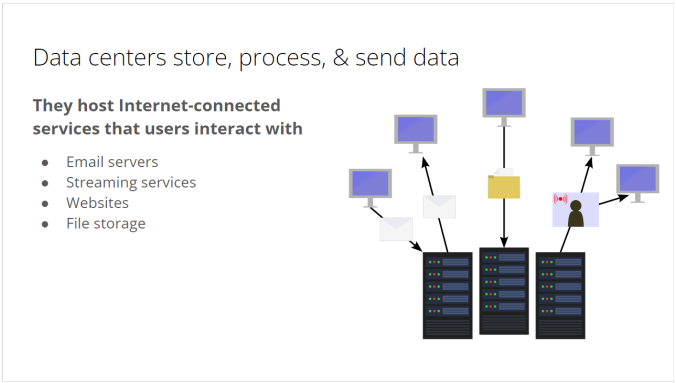
Data Centers & Servers

Slide 2: Data Centers & Servers



Goal	*Introduce the concept of "Data Centers & Servers".*
Transcript	We begin with the data center. Botgal recently started a new job as a cybersecurity engineer here. But what *is* a data center, and what are Botgal's responsibilities?
Further Engagement	*To engage your students, you could ask students to brainstorm what are some things Botgal may be responsible for. If your students can't come up with much, that's okay! We'll be covering those topics during the presentation.*

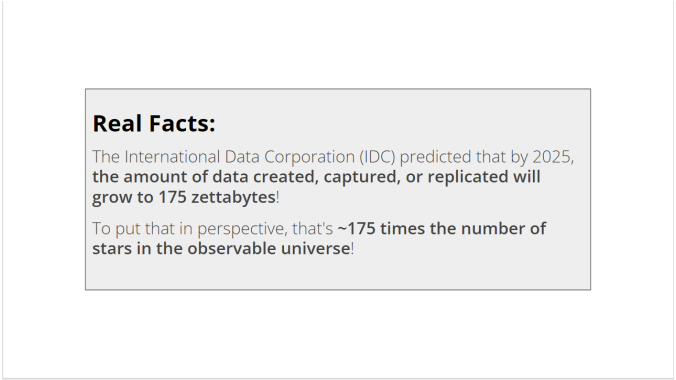
Slide 3: Data centers store, process, & send data



Goal	*Define **data centers**.*

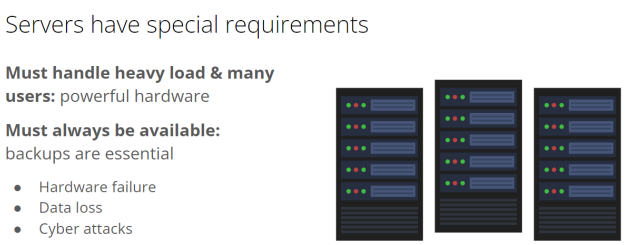
Transcript	**Data centers** are places responsible for storing, processing, and sending data. They are made up of hundreds, or sometimes thousand, of servers. These servers host Internet-connected services for users (like you!) to interact with. This includes email servers, streaming services, websites, file storage, and more.
Further Engagement	*To engage your students, you could ask for a couple more examples of Internet-connected services they may use on a daily basis (e.g. Gmail, Netflix, etc.).*
Additional Resources	*For more information about servers, we recommend these resources:* ● *What is a Server? (Deep Dive)*

Slide 4: Real Facts



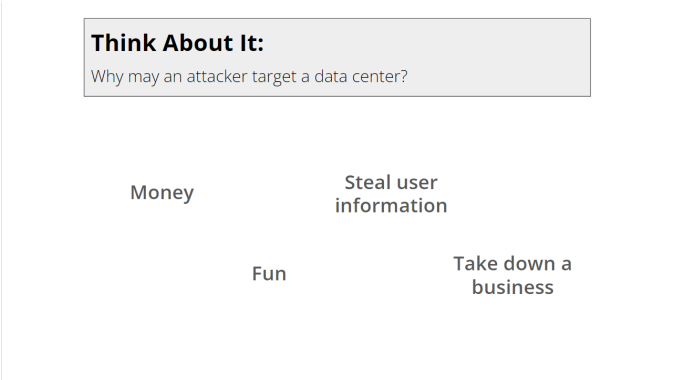
Goal	*Attempt to give a sense of scale to the amount of data passing through data centers.*
Transcript	But why do we care about data centers and their servers? Data! There's a crazy amount of data that makes its way through data centers. To give some perspective, the International Data Corporation, or IDC, made a prediction that by 2025, there would be 175 zettabytes of data create, captured, or replicated per year. That's ~175 times the number of stars in the observable universe!
Further Engagement	*To engage your students, you could add an animation to the slide and first ask students to guess the amount of data passed through.*

Slide 5: Servers have special requirements



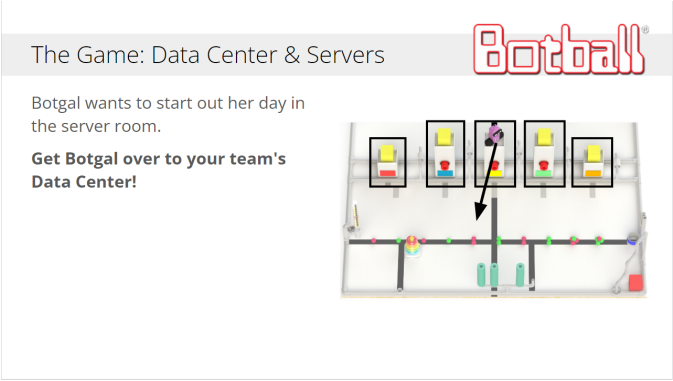
Goal	*Define **servers** and make it clear what sets them apart from your everyday desktop or laptop.*
Transcript	Not only do servers have to handle this heavy load of data, but their services need to stay up at all times! Imagine if your email service (e.g. Gmail, Outlook, Yahoo, etc.) went down – you wouldn't be a happy customer, right? To deal with these requirements, servers have powerful hardware – oftentimes much, much more powerful than anything you have at home. Server admins and cybersecurity engineers may also work together to come up with plans for emergency scenarios. This may include making regular backups of all data on the server, purchasing spare parts, and more.
Further Engagement	*To engage your students, you could start out by asking them what hardware they have in their computer (e.g. storage, graphics cards, etc.).*

Slide 6: Think About It



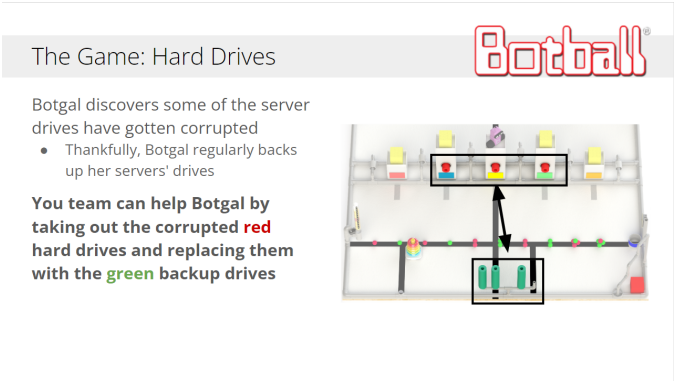
Goal	*Engage students - get them to think about why data centers may be a special target for attackers.*
Transcript	Knowing what we know, what are some reasons attackers may attack a data center?

Slide 7: The Game: Data Center & Servers



Goal	*Tie what we learned about data centers & servers into the game board.*
Transcript	On the game board, we have 5 server racks in the middle. Botgal is in the middle rack a needs to be moved to the server room.

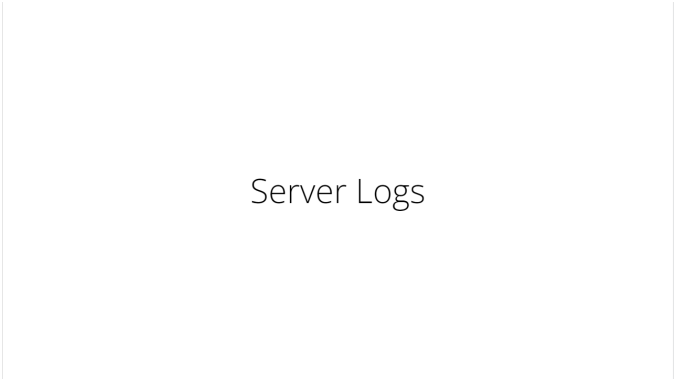
Slide 8: The Game: Hard Drives



Goal	*Tie what we learned about hard drive backups into the game board.*
Transcript	On the game board, the 3 center servers each have a red pool noodle representing a corrupted hard drive. As cyber security engineers, we may need to assist with developing recovery plans in the event of hardware failure or cyberattacks.

Server Logs

Slide 9: Server Logs

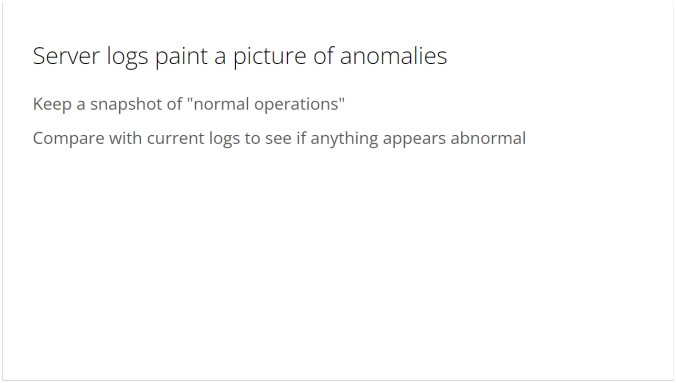


Goal	*Introduce the concept of "Server Logs".*
Transcript	Another important task for cybersecurity engineers in a data center is monitoring "server logs". In this section, we'll talk about what those are and why we should care about them.

Slide 10: Server logs store information about server usage

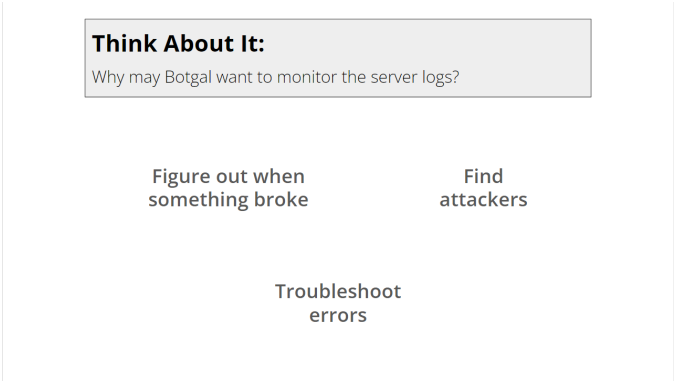
Goal	*Define **server logs**.*
Transcript	Server logs are files that record every action taken on a server. This includes who logged in, when they logged in, what they did on the system, and more.

Slide 11: Server logs paint a picture of anomalies



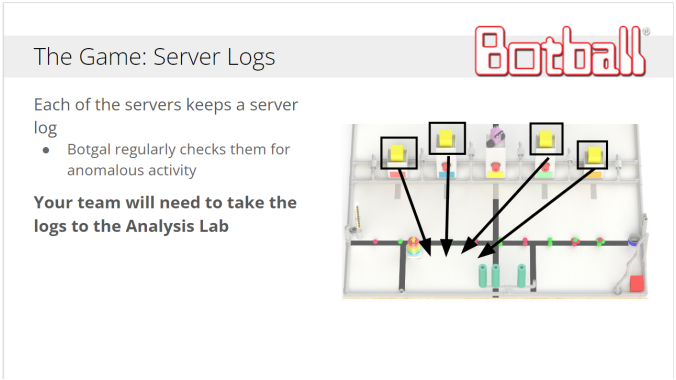
Goal	*Describe the point of server logs.*
Transcript	Under normal operations, these server logs paint a picture of what is normal. If Botgal is constantly monitoring the server logs and comparing them to what should be normal, she can quickly identify when something is wrong!

Slide 12: Think About It



Goal	*Drive in the point of why we care about quickly identifying when something is "wrong".*
Transcript	So why would Botgal want to identify when something is abnormal? Why would we want to know these things quickly?

Slide 13: The Game: Server Logs



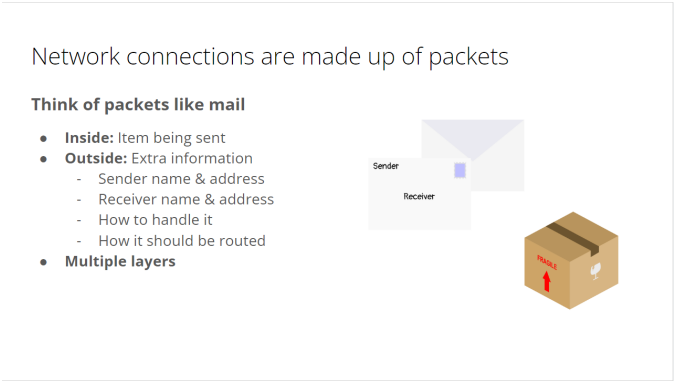
Goal	*Tie together what we learned about server logs with the game board.*
Transcript	Botgal luckily set up the servers and its services to log. On the game board, the server logs are the yellow cubes on top of the four most outer servers. You'll have to take them to the Analysis Lab for her to complete her analysis.

Network Connections

Slide 14: Network Connections

Goal	*Introduce the concept of "Network Connections".*
Transcript	Botgal's work at the datacenter requires her to monitor and understand what's going on in the network.
Additional Resources	*Note that we do not go very in-depth into networking concepts in these slides. In fact, we abstract away some of the information to simplify the basic information we're trying to get across. For more information on introduction to networking concepts, check out these resources:* ● *What is a Protocol? (Deepdive)* ● *Computer Networking (Deepdive)*

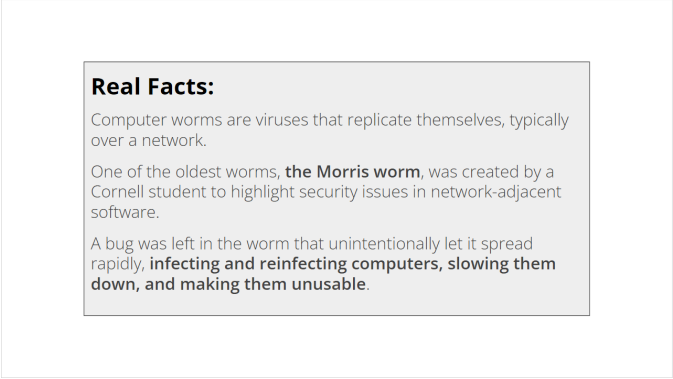
Slide 15: Network connections are made up of packets



Goal	*Give a very high-level view of how networking works.*

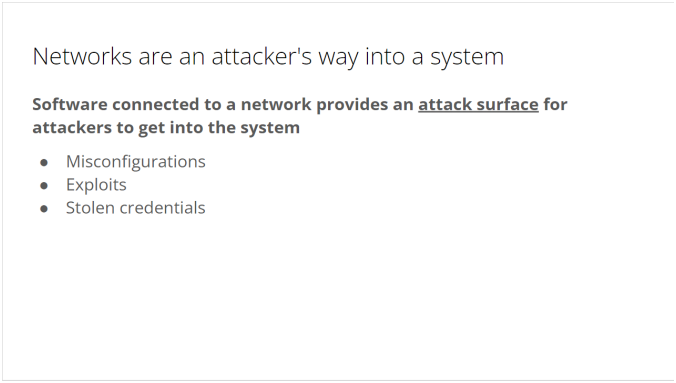
Transcript	At its very basis, computer networking works similar to the mail system: information is packaged up in a container with additional information, such as sender/receiver addresses, handling information, and more.
Additional Resources	*Again, this is abstracted to get to the concepts relevant to what is on the game board. On the game board, students need to sort through packets coming through the network connection. There are many resources to learn deeper networking concepts.*

Slide 16: Real Facts



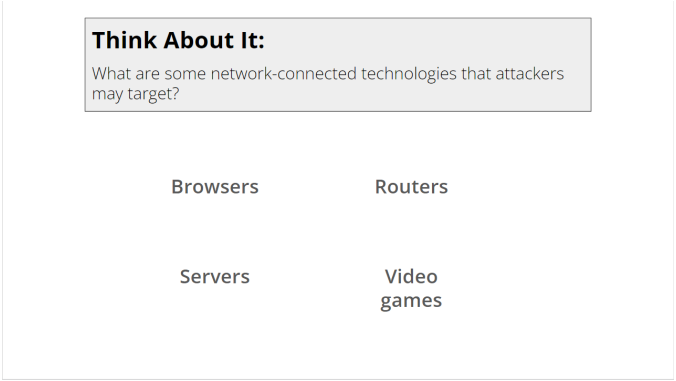
Goal	*Highlight how exposure to a network provides an attack surface for attackers to leverage.*
Transcript	One thing that's important in cybersecurity is the idea of an "attack surface". These are the ways that an attacker may have access to get into a system. Computer networks provide a ripe opportunity for attackers. Malware is one good real-life example. Computer worms, such as the Morris worm, would infect devices by targeting the software connected to the network. The Morris worm did an extraordinary amount of damage, spreading exponentially, and making computers unusable.

Slide 17: Networks are an attacker's way into the system



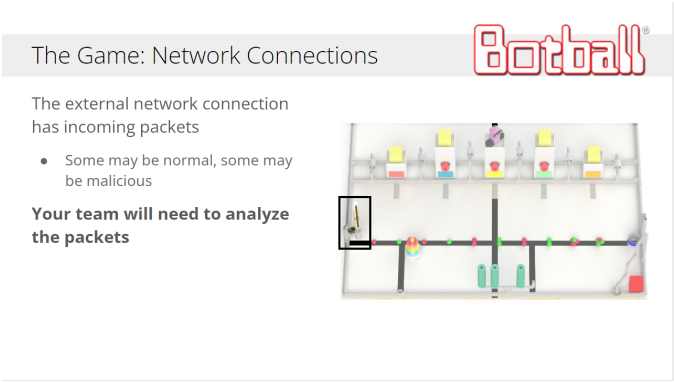
Goal	*Use a real-life example from the prior slide to drive the point that networks provide an attack surface cyber security engineers need to be aware of.*
Transcript	Cybersecurity engineers need to scrutinize each and every entry point from a network into a computer system to minimize the attack surface as much as possible.

Slide 18: Think About It



Goal	*Engage students to get them to think about examples of attack surfaces.*
Transcript	If we wanted to do the same, what are some examples of some network-connected entry points into a system or network?

Slide 19: The Game: Computer Networks



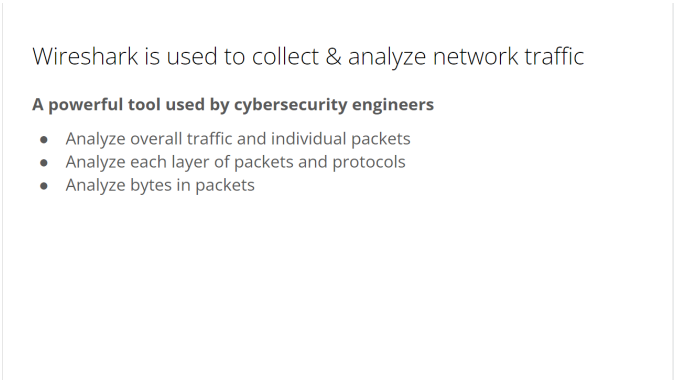
Goal	*Tie together what we learned about network connections with the game board.*
Transcript	In Botgal's data center, there's a constant flow of **incoming network connections**, represented by the **ping pong balls** inside the ping pong ball dropper. Red ping pongs are malicious network connections, and yellow ping pongs are benign. Botgal may want to do something about the malicious network connections. See if you can grab the red ping pong for her!

Wireshark

Slide 20: Wireshark

Goal	*Introduce the concept of "Wireshark".*
Transcript	Cybersecurity engineers need a way to do deeper analysis on traffic. We'll talk about a powerful tool called "Wireshark" that people like Botgal use to examine network traffic.

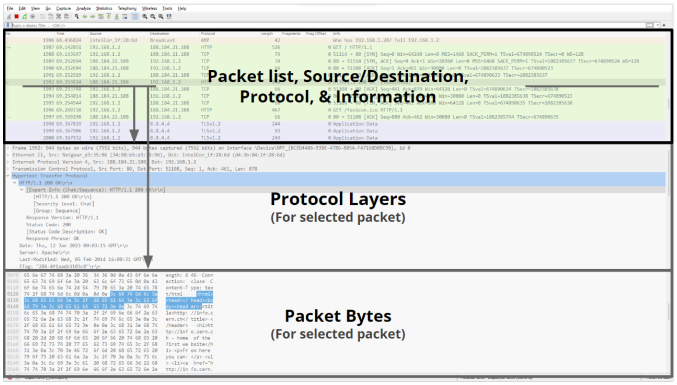
Slide 21: Wireshark is used to collect & analyze network traffic



Goal	*Define **Wireshark**.* *The next slide will have a screenshot of Wireshark to make it a bit more clear on what we talk about in this slide.*
Transcript	**Wireshark** is a powerful network analysis tool used by cybersecurity engineers and many others.

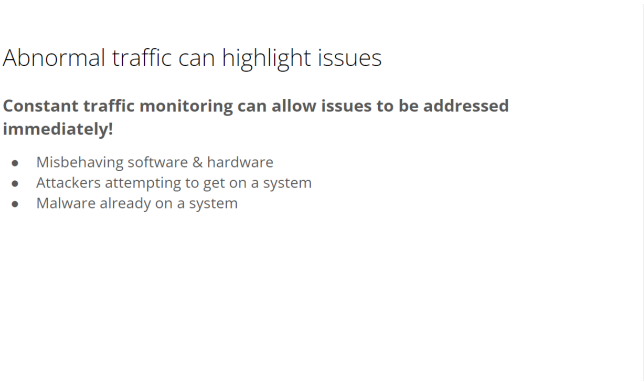
	Somebody using Wireshark can analyze the overall flow of traffic, the individual packets, protocol information, and the bytes making them up.

Slide 22: View of Wireshark in Use



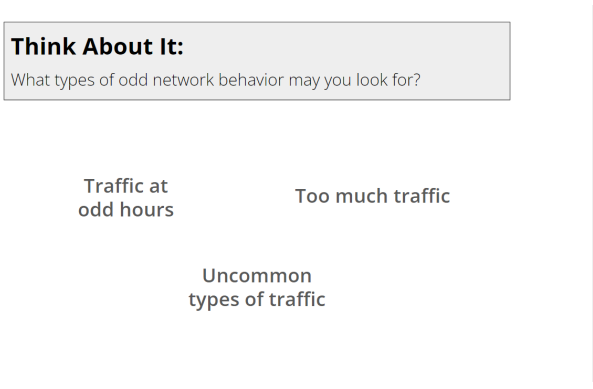
Goal	*Show what Wireshark looks like to students. Note that it's a complicated tool, especially when a lot of networking concepts were abstracted away, but it can give students an idea of how it allows security engineers to "unpack" the network traffic and analyze it in-depth.*
Transcript	Wireshark looks complicated, but a cybersecurity engineer can navigate it with ease! The top box shows a list of each packet in the network traffic. In our Botball gameboard, each of these would be a ping pong ball. The middle box breaks down a selected packets in a number of protocol layers. Remember - network traffic is like mail and the data to send may be packaged in a number of layers. The bottom box displays the packet as bytes to make it easier for an analyst to skim the contents.
Further Engagement	*To engage your students, you could download Wireshark and examine a number of example PCAPs (Packet Capture) files of network traffic.* • *https://wiki.wireshark.org/SampleCaptures*

Slide 23: Abnormal traffic can highlight issues



Goal	*Get to the point that traffic monitoring and tools like Wireshark are powerful to cyber security engineers.* *We will talk a bit about what "issues" may look like in network traffic on the next slide.*
Transcript	With constant monitoring, engineers establish a baseline of what their network traffic *should* look like. If anything appears different, then engineers can further investigate (with tools such as Wireshark!) to determine if it *is* a problem and address immediately.

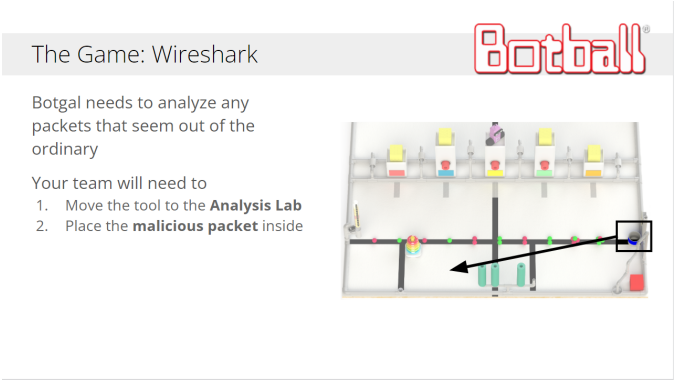
Slide 24: Think About It



Goal	*Get students to think about what "abnormal traffic" looks like.*

Transcript	So Botgal's established a baseline of what her network traffic *should* look like. What are some things that may seem "abnormal" as she's observing network traffic?

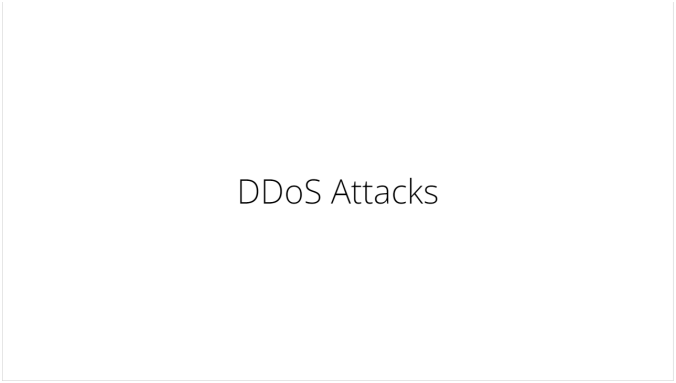
Slide 25: The Game: Wireshark



Goal	*Tie in what we've learned about Wireshark to the Botball gameboard.*
Transcript	Botgal needs to analyze malicious network traffic. She can move the **Wireshark** tool, represented by the **3" coupler** to the Analysis lab. Once she has access to Wireshark, she can place the suspected malicious network connection in to give it a look.

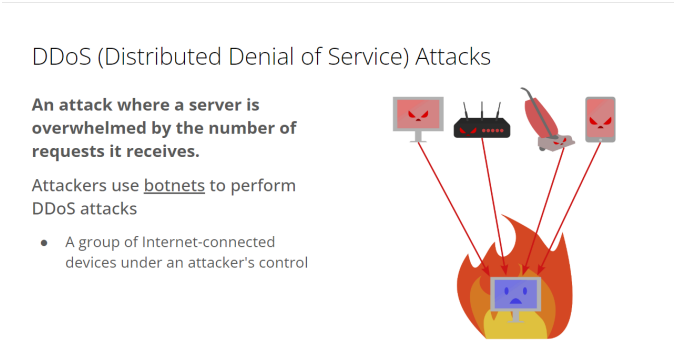
DDoS Attacks

Slide 26: DDoS Attacks



Goal	*Introduce the concept of "DDoS attacks".*
Transcript	Sometimes we may not be dealing with just one malicious network connection, but *thousands* of them! Why would attackers do this, and what should cybersecurity engineers do in this situation?

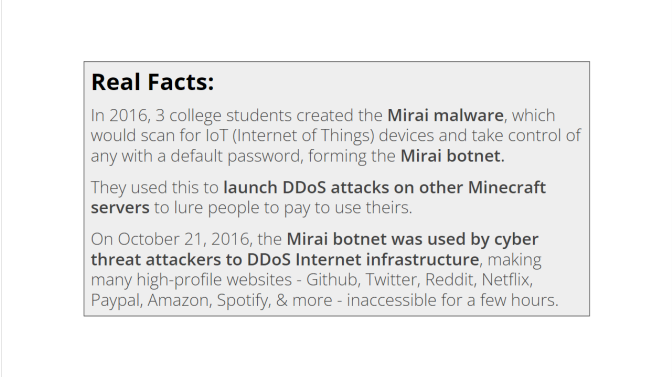
Slide 27: DDoS (Distributed Denial of Service) Attacks



Goal	*Define **DDoS (Distrubuted Denial of Service) attacks** and **botnets**.*
Transcript	**DDoS, or Distributed Denial of Service, attacks** are attacks in which attackers flood a network with thousands or millions of requests at once. This may overwhelm the target network, servers, and software services, causing them to fail and become unavailable.

	Attackers will oftentimes use **botnets** to accomplish this. A **botnet** is a group of devices around the Internet that an attacker has gained control over - either by hacking or using default passwords. An attacker can send commands to the devices under their control to have them flood a target with many network connections!

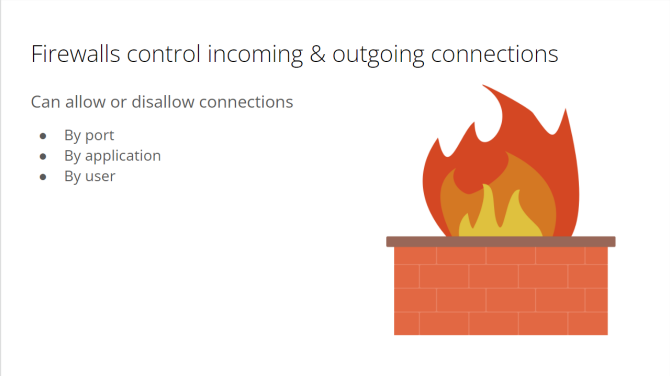
Slide 28: Real Facts



Goal	*Highlight how DDoS attacks affect people in real life.*
Transcript	With more and more devices being connected to the Internet, DDoS attacks have become more prevalent. Everyday devices with Internet access, such as a vacuum cleaner, are called **Internet-of-Things (IoT) devices**. These Internet-connected systems are simple and rarely are secure. In 2016, 3 college-age students ran a Minecraft server. In a ploy to make more money, they set out with the goal of taking down other Minecraft servers to drive users to pay for their server. To do this, they needed a botnet to DDoS and take down the servers. They created the Mirai malware, which would scan the Internet for IoT devices, and would attempt to gain access by trying a number of default credentials. Surprisingly, it was overly successful, taking over hundreds of thousands of devices. Unfortunately, the source code for Mirai was stolen by cyber threat actors. It was redirected at Internet infrastructure, making many high-profile websites and services inaccessible for hours.

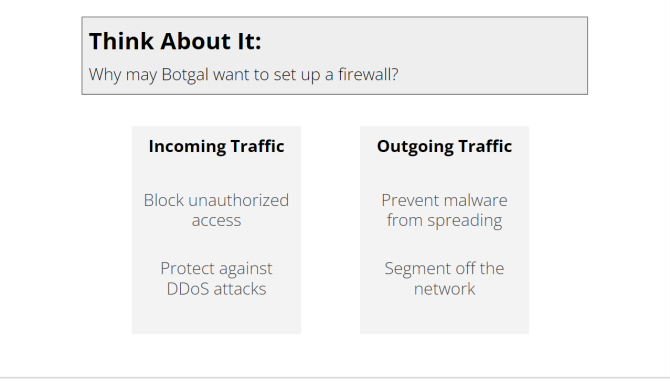
Further Engagement	*To engage students, you could ask them to list out different Internet-connected devices.*
Additional Resources	• *How a Dorm Room Minecraft Scam Brought Down the Internet* • *The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the Internet*

Slide 29: Firewalls control incoming & outgoing connections



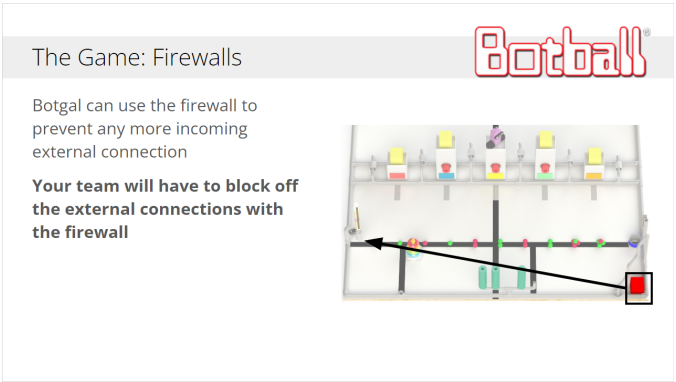
Goal	*Define **firewalls** and explain how they can help manage network-based attacks.*
Transcript	So how do we defend our network against attacks? **Firewalls** provide us one tool to protect our networks. **Firewalls** enable network connections to be allowed or disallowed depending on a number of features - port, application, and more.

Slide 30: Think About It



Goal	*Engage students to think a bit more about the purpose and usefulness of firewalls.*
Transcript	What may be some ways Botgal could use a firewall to protect her network?

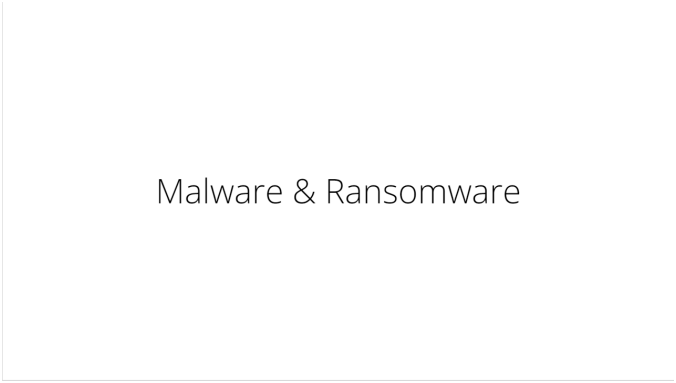
Slide 31: The Game: Firewalls



Goal	*Tie in what we learned about DDoS attacks and firewalls to the gameboard.*
Transcript	Botgal wants to set up a **firewall**, represented by **the red cube**, to protect the data center. You'll need to help her move it under the ping pong ball dropper to prevent additional incoming network connections.

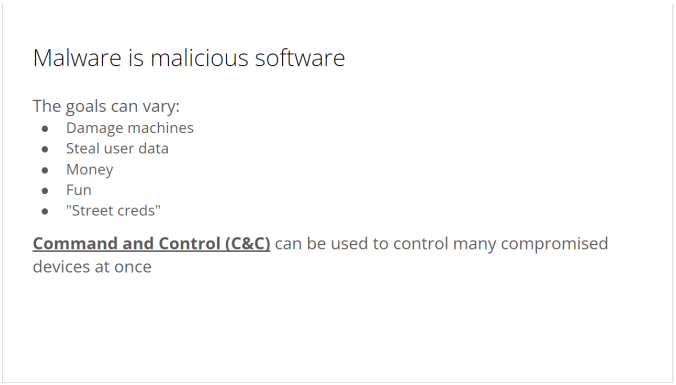
Malware & Ransomware

Slide 32: Malware & Ransomware



Goal	*Introduce the concepts of "malware and ransomware".*
Transcript	On occasion, attackers manage to get onto our system. Malware is one way attackers can do this.

Slide 33: Malware is malicious software



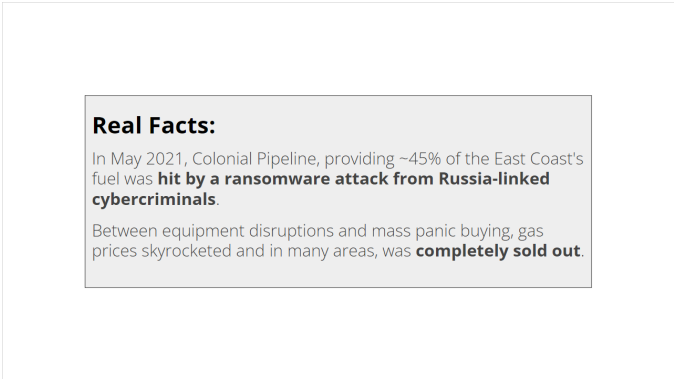
Goal	*Define **malware** and **C&C (Command & Control)**.*
Transcript	**Malware** or "malicious software" is software that affects your computer in a negative manner. It might: ● Slow down or break your system ● Steal user information like credentials, banking details, etc. Malware may use **Command & Control (C&C)** which allows attackers to remote control and issue commands to malware

	installed across many systems. This is how attackers manage botnets!

Slide 34: Ransomware: Your data is the hostage

Goal	*Define **ransomware**.*
Transcript	One particular common flavor of malware nowadays is **ransomware**. **Ransomware** encrypts your files and data, demanding money in exchange for your files back. Hospitals, critical infrastructure, & large corporations are common targets of ransomware, as they're oftentimes willing to pay to regain access as quickly as possible.

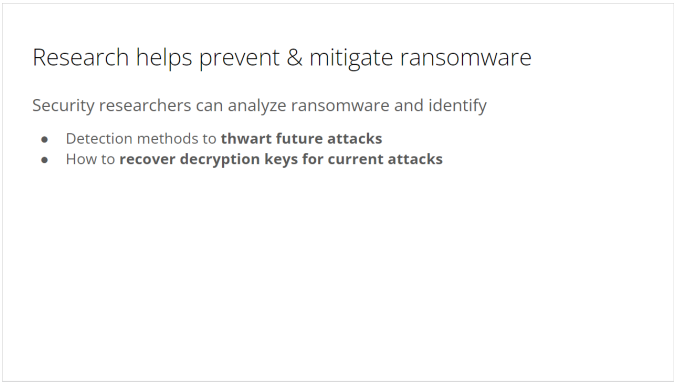
Slide 35: Real Facts



Goal	*Talk about real events in which malware, specifically ransomware, has affected people's day-to-day lives.*

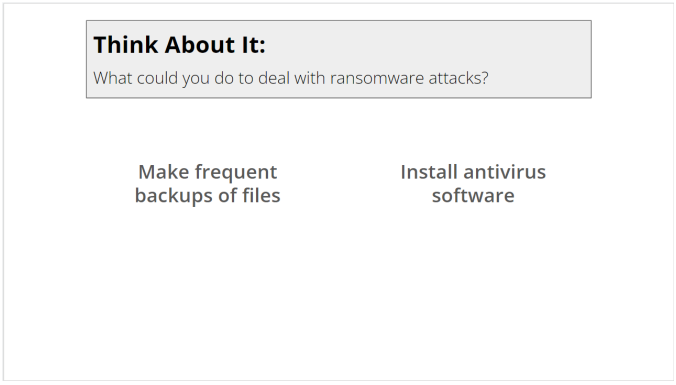
Transcript	One such recent target was Colonial Pipeline, a company supporting critical infrastructure on the east coast, serving ~45% of its fuel. The ransomware attack made fuel harder to find, causing people to panic-buy gas, and make it even harder to find.

Slide 36: Researchers help prevent & mitigate ransomware



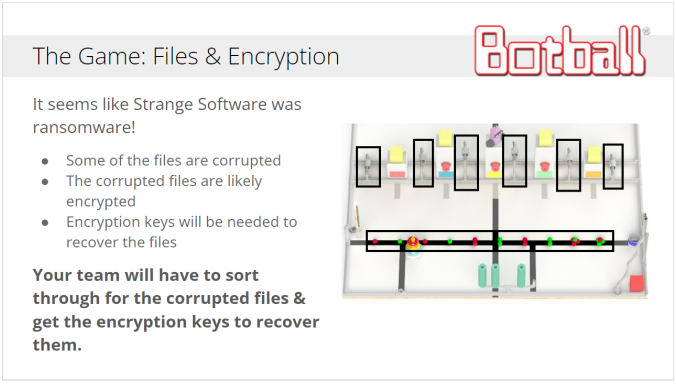
Goal	*Describe how security researchers and engineers help fight against ransomware.*
Transcript	Security researchers analyze ransomware to understand a number of things - 1. How to identify the ransomware: This will allow us to update antivirus to quickly detect and remove or alert at the first sight of an infection. 2. How the ransomware encrypts files: This allows researchers to provide victims with information on how to decrypt the files without paying the ransom. This work is valuable to prevent more victims from funding the attackers!

Slide 37: Think About It



Goal	*Engage students to think about ways to combat ransomware.*
Transcript	Knowing what we know now, what ways may we be able to protect ourselves from ransomware?

Slide 38: The Game: Files & Encryption

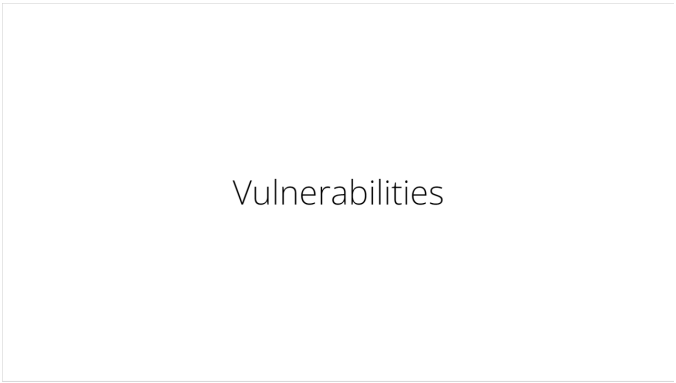


Goal	*Tie together what we covered on malware & ransomware with the game board.*
Transcript	After some searching on the server, Botgal identifies some malware. Furthermore, it's ransomware that encrypted some of the files on the system! Botgal needs to sort through the **files**, represented as **poms** on the board, to grab the **red corrupted/encrypted ones**. She also needs help recovering the **encryption keys**, represented as the PVC slides at the center of the board.

	Once you have done these, she should be able to recover all the corrupted files on the server!

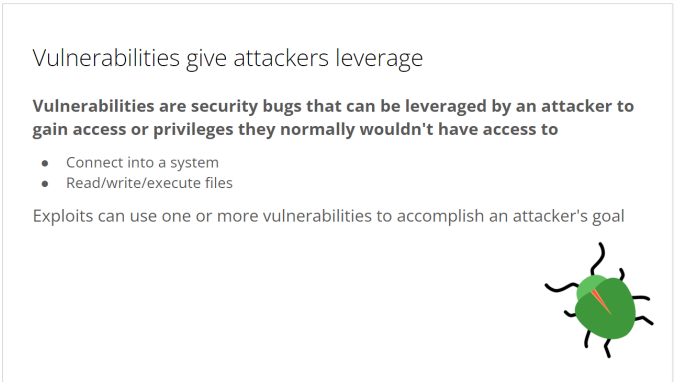
Vulnerabilities

Slide 39: Vulnerabilities



Goal	*Introduce "Vulnerabilities".*
Transcript	But how do attackers get onto a system? Sometimes they're able to guess a username & password. Sometimes they're able to trick users into downloading malware. But sometimes, they're able to use vulnerabilities to gain power on a system.
Additional Resources	• *What is a Security Vulnerability?* • *Understand Security Risk vs Security Vulnerability*

Slide 40: Vulnerabilities give attackers leverage



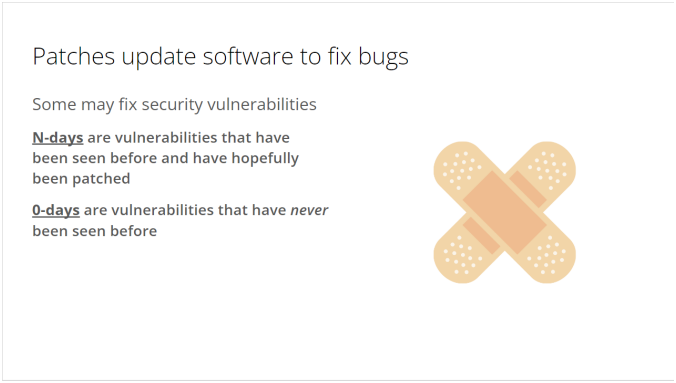
Goal	*Define **vulnerabilities**.*

Transcript	**Vulnerabilities** are security bugs that attackers can use to give them more power on a system than was intended. This could include: ● Gaining access into a system ● Reading/writing/executing files or memory ● Gaining more powerful privileges The key is that the type or level of access (or the access in general) was not intended for the attacker.

Slide 41: Real Facts

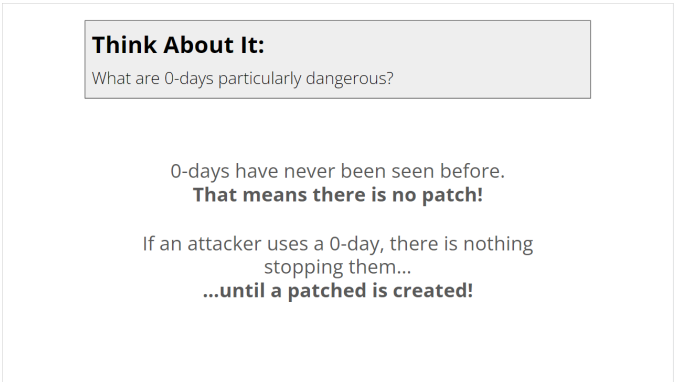
Goal	*Depict real life events affected by vulnerabilities.*
Transcript	Vulnerabilities can have massive impact into people's day-to-day lives. Microsoft Exchange, an email service used by companies, businesses, & individual users the world over, was found to have several high-impact vulnerabilities giving attackers control of the system. While patches for these vulnerabilities have rolled out, they've rolled out slowly, with administrators applying them even slower. The result? Attackers took advantage of this to hack into these unpatched email servers.

Slide 42: Patches update software to fix bugs



Goal	*Describe a way to deal with vulnerabilities.*
Transcript	**Patches** are software updates that address software bugs. Ideally, they also fix vulnerabilities, preventing attackers from being able to leverage them. **N-days** are vulnerabilities that are known and have been reported before. **0-days**, on the other hand, are vulnerabilities that have *never* been seen before in the wild.

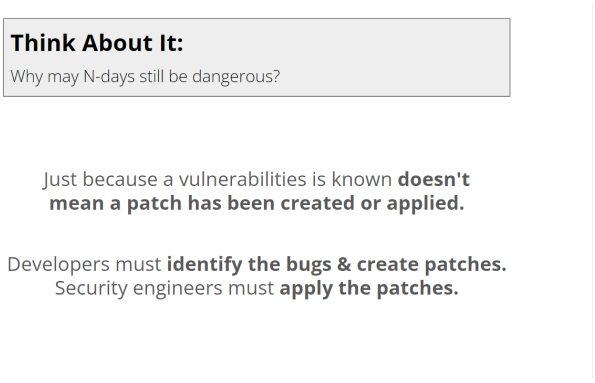
Slide 43: Think About It (0-Days)



Goal	*Engage students to think about the danger of 0-days.*
Transcript	Why may 0-days be particularly dangerous? <Get student answers>

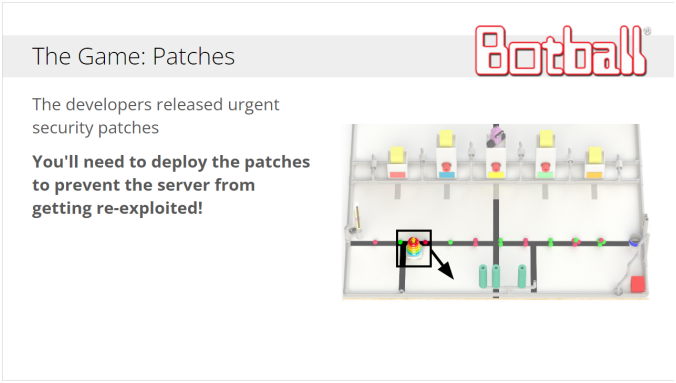
	Well, 0-days have never been seen before. That means there's no patch or any official form of defense against them!

Slide 44: Think About It (N-Days)



Goal	*Engage students to think about the danger of N-days.*
Transcript	And why may *N-days* still be dangerous as well? <Get student answers> Just because a vulnerability is known doesn't mean a patch has been created for it. Similarly, even if a patch exists, it doesn't mean it has been applied. N-days require the cooperation of developers and cybersecurity engineers/admins to create and apply patches.

Slide 45: The Game: Patches

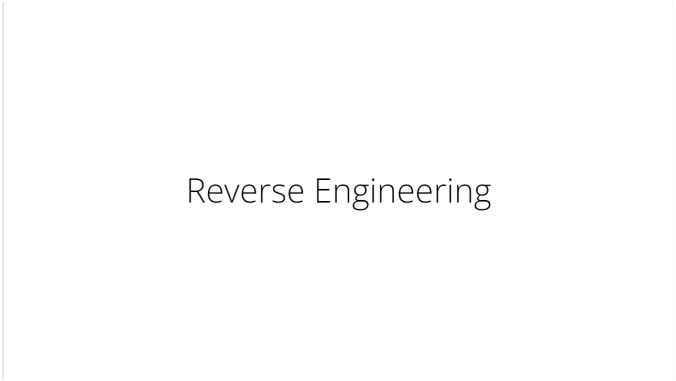


Goal	*Tie what we learned about vulnerabilities and patches to the game.*

Transcript	Botgal has identified a vulnerability she believes an attacker used to get into the server. **Patches**, represented by the **ring stand**, need to be applied by moving the rings and stacking them in the **Server Room**.

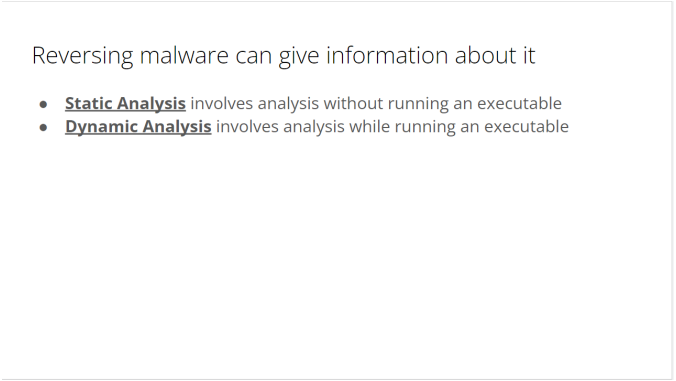
Reverse Engineering

Slide 46: Reverse Engineering



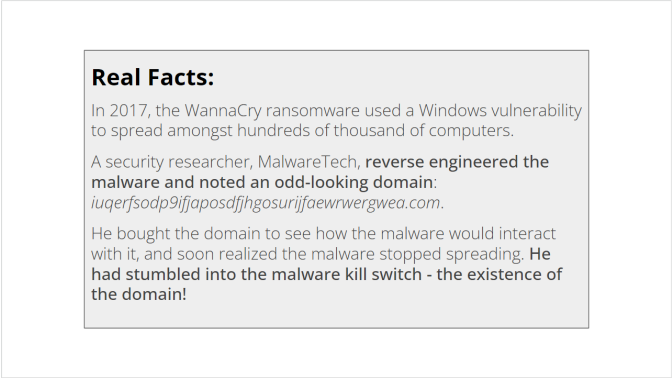
Goal	*Introduce "Reverse Engineering".*
Transcript	Once we've properly defended the network and patched the vulnerabilities on the server, we need to turn our attention to reverse engineering the malware.

Slide 47: Reversing malware can give information about it



Goal	*Define **reverse engineering**.*
Transcript	**Reverse engineering** utilizes tools to understand how a binary or software works. We do this when we do not have source code, but still need to understand how something works. Two different approaches: ● Static analysis - analyze behavior without running ● Dynamic analysis - analyze behavior while running

Slide 48: Real Facts

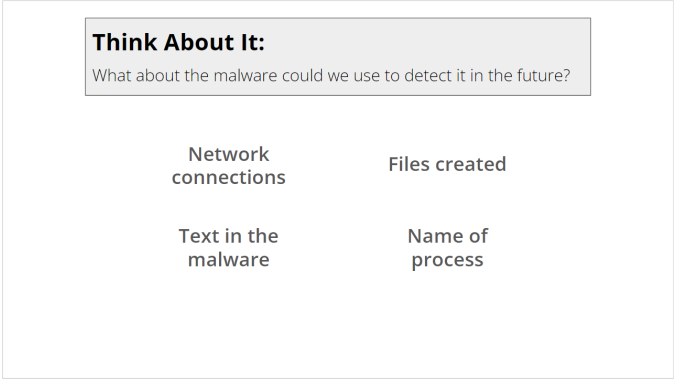


Goal	*Give a real-life example of how reverse engineering malware allowed it to be quickly neutralized.*
Transcript	Reverse engineering is an important skill for any cybersecurity engineer. The WannaCry malware spread rapidly and deeply affected many systems. One security researcher, MalwareTech, reverse engineered a malware sample and noticed a strange domain name embedded in it. Curious, he investigated it and noticed that it was not currently owned by anyone. Expecting the domain to deal with C&C, he purchased it, and quickly realized all WannaCry copies stopped spreading - it turned out that the existence of the domain was the malware kill switch!
Additional Resources	• How to Accidentally Stop a Global Cyber Attacks

Slide 49: Reverse engineering malware for defense

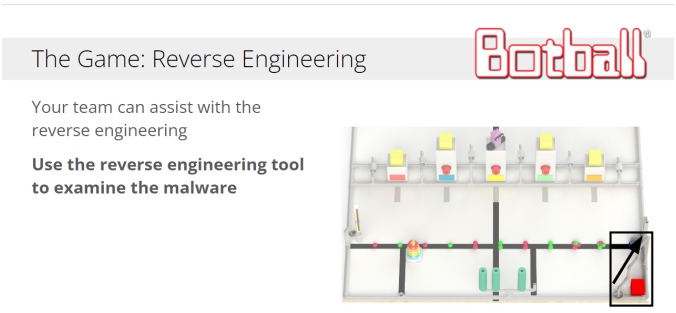
Goal	*Talk about some specifics on how reverse engineering helps defend against malware.*
Transcript	Reverse engineering can also help prevent or mitigate future infections of a system. Certain properties of malware can be watched out for in the future, triggering alerts and action if detected. That means malware can be identified and removed before damage is done. At a high-level, this is how antivirus works!

Slide 50: Think About It



Goal	*Engage students to think about how we can identify malware.*
Transcript	What are some examples of properties we could use to detect malware?

Slide 51: The Game: Reverse Engineering

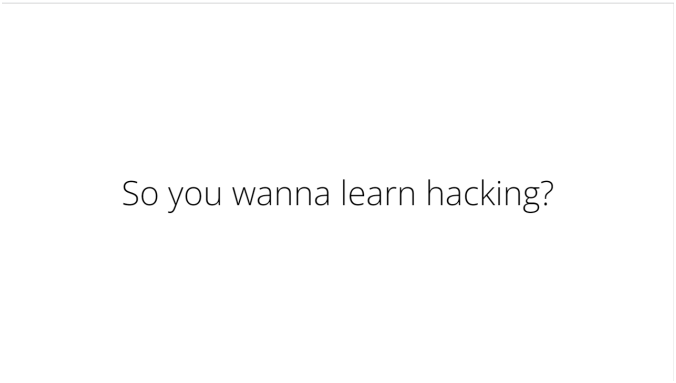


Goal	*Tie what we learned about reverse engineering to the gameboard.*

Transcript	Botgal needs help analyzing the malware. You'll have to use the **reverse engineering tool** in the corner, moving the ring up to a higher to perform more analysis.

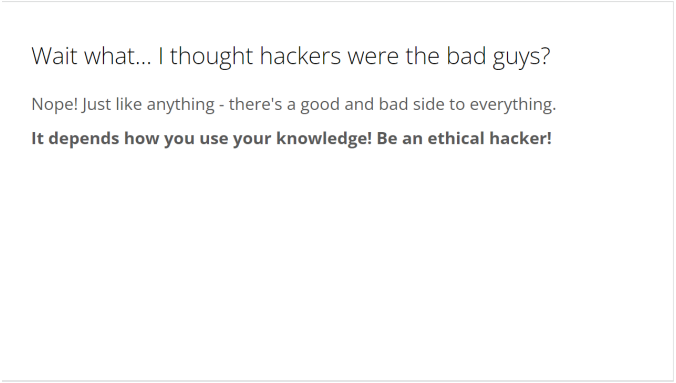
So you wanna learn hacking?

Slide 52: So you wanna learn hacking?



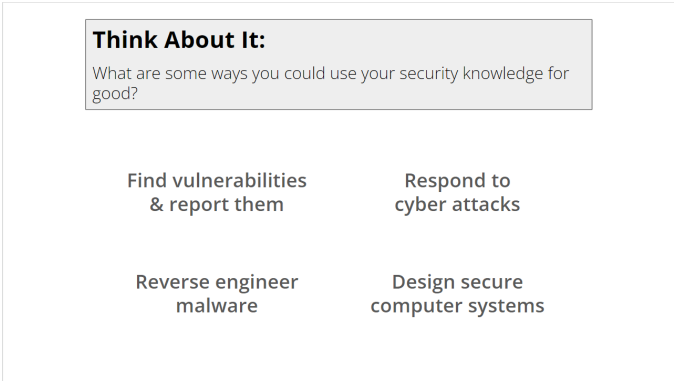
Goal	*Provide additional thoughts and resources for students interested in learning more about security.*
Transcript	So now that we've learned a bit about cybersecurity, do you want to learn more about hacking?

Slide 53: Wait…I thought hackers were the bad guys?



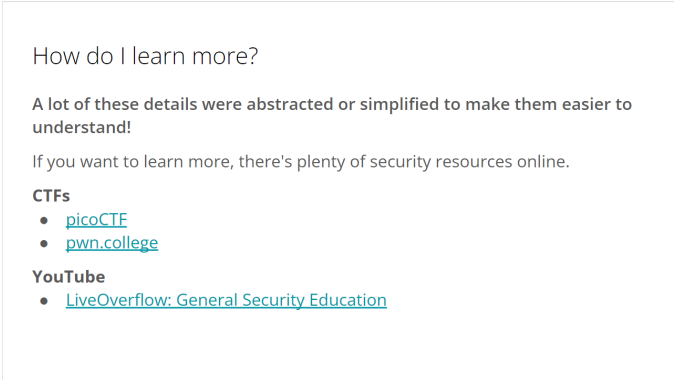
Goal	*Dispel negative associations with "hackers" and "hacking".*
Transcript	"Hackers" and "hacking" are just people that are able to understand and perform a lot of the same skills that Botgal has. Just like everything else, there's a good and bad side to it. It all depends on what you do with your skills!

Slide 54: Think About It



Goal	*Encourage students to thing about positive things they can do with "hacker skills".*
Transcript	What are some things you could do to use your "hacker knowledge" for good?

Slide 55: How do I learn more?



Goal	*Provide additional resources.*
Transcript	So now your interest is piqued in hacking, how do you learn more? The Internet is by far the best resource! Search whatever you'd like to learn, and there's likely tons of writeups, videos, and practice material. Specifically, CTFs, or Capture The Flags, are hacking competitions geared to train your skills and increase your knowledge. picoCTF and pwn.college are two such beginner-friendly sites.

Additional Resources	• *A Deeper Look at Hacking Laws* • *Play CTF! A Great Way to Learn Hacking - Fsec 2017* • *How To Learn Hacking With CTFs*