

Cybersecurity Notebook 2020 - 2021

Unit 2

Name:

Table of Contents

**Unit 2**

[Unit 2.1.1](#hqu2n5sbfd43) **Confidentiality, Integrity, and Availability**

[Unit 2.1.2](#sd0a67cszf3b) **Passive Analysis**

[Unit 2.1.3](#jbiymkxlsown) **E-Commerce Architecture**

[Unit 2.2.1](#75tlkvk5dti4) **More on Malware**

[Unit 2.2.2](#rja648psz27n) **Server Vulnerabilities**

[Unit 2.2.3](#ritqvc36s1jp) **Server Analysis**

[Unit 2.2.4](#nr4zns9x68ko) **Secure the Server**

[Unit 2.3.1](#ycl9lt7fqq2l) **Securing E-Commerce Data**

[Unit 2.3.2](#9c4dqm3eq35e) **Stopping the Spread of Malware**

[Unit 2.3.3](#o9j9vm5qfiuq) **Server Attacks**

[Unit 2.3.4](#fae1u3vkg09v)**Find the Exploits**

[Unit 2.4.1](#mjpamfa9gor3) **E-Commerce Enrichment**

**Cybercase**

****

## E-Commerce Site Security

Bikes, Boards, and Beyond, a local retail shop, sells outdoor active gear, from skateboards and scooters to snowshoes and skiing equipment. The shop wants to grow its business and has decided to start an online shopping site to reach customers nationwide.

They have almost everything ready: a product database, a beautiful website design, extra inventory in their storage room, and a reliable shipping system in place. They have even decided, as part of their business expansion, to use an electronic system to track and manage in-store tasks and activities. They purchased digital scanners to track inventory in stock in the storerooms and on the shelves, new computers to process in-store orders and returns, and a badge scanning device to swipe employees in and out of the store to track their work hours.

Before Bikes, Boards, and Beyond goes live with their online shopping site, they need to test their website and ensure it is secure. Funneling their business through the world wide web could put the store's information and the information of their customers at risk. Therefore, the store has hired you and your cyber team to confirm that their site is secure and ready for, what they hope will be, high e-commerce traffic.

How will you secure their data? Do some data require more security and protection than others? What are some vulnerabilities that could threaten the security of the e-commerce site? How can you design a secure system, while ensuring the accessibility of the website to the customers and the store's internal data to its employees?

The activities and projects in this unit will arm you with the skills and knowledge necessary to help you secure the e-commerce site and protect it from future cybersecurity threats.

**Unit 2.1.1**

**Goals**

* Learn about data confidentiality, integrity, and availability.
* Define the Internet of Things
* Protect against about website tracking

**Self-Assessment:**

1. What types of architectural considerations should e-commerce sites consider to ensure the protection of their digital resources?

Making sure the site is compliant, using proper ecommerce guidelines, Trademarks.

1. What is the CIA triad?
2. How does passive analysis differ from active analysis?
3. What is the difference between black-, white-, and gray-hat hacking?
4. What is the goal of pen test?
5. Describe some exploits that a malicious user can execute in a browser.

#3 Notebook

1. Any personal information that is sent through the site. Including names, bank info, addresses, etc.
2. Don't give out your information unless it's a trusted website, and be cautious about what information you put in.

#4 Answer Questions - Notebook

1. What is the CIA Triad?

A Security model that represents Cyber Security. Which stands for Confidentiality, Integrity, and Availability.

1. Define the Confidentiality component of CIA and list some ways of protecting it.

Confidentiality is protecting from unauthorized usage of data, you can protect your data by using encryption.

1. Define the Integrity component of CIA and list some ways of protecting it.

Integrity is making sure data isn’t tampered with a good way of making sure that data isn’t tampered with is using confidentiality, making sure there’s no unauthorized access to data.

1. Define the Availability component of CIA and list some ways of protecting it.

Availability is making sure data is able to be accessed by authorized users at all times, protecting availability is as simplistic as keeping the networks up with good connection and rapid recovery system.

1. Why is the CIA Triad important to Bikes, Boards, and Beyond as they launch their new website?

As with any business, they should be concerned about trying to create a balanced system using CIA.

#6 Use Google Draw or another tool and place in the notebook

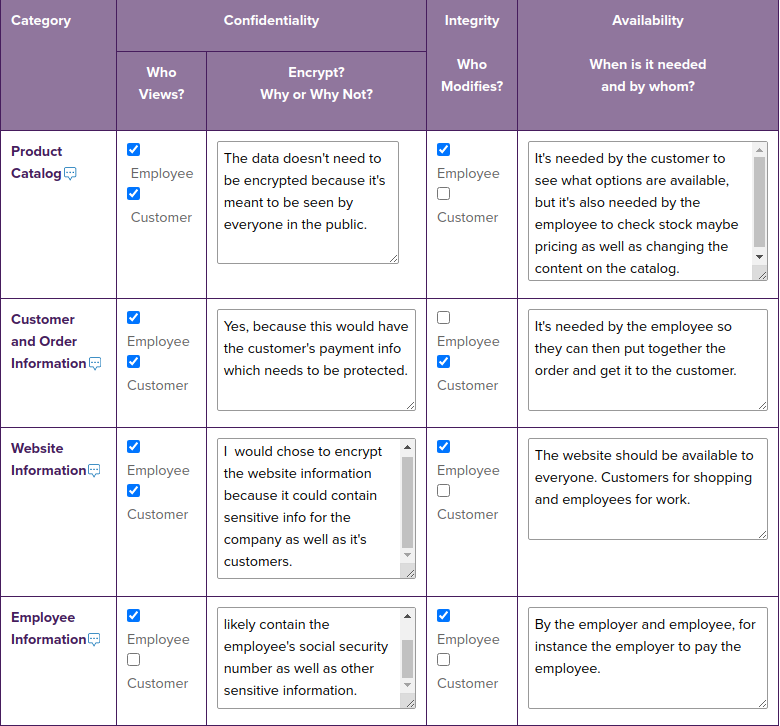
#7 Notebook

1. Confidentiality – Social Security number
2. Availability – Family Calendar
3. Integrity – Personal Health Records
4. Availability – Online shopping catalog

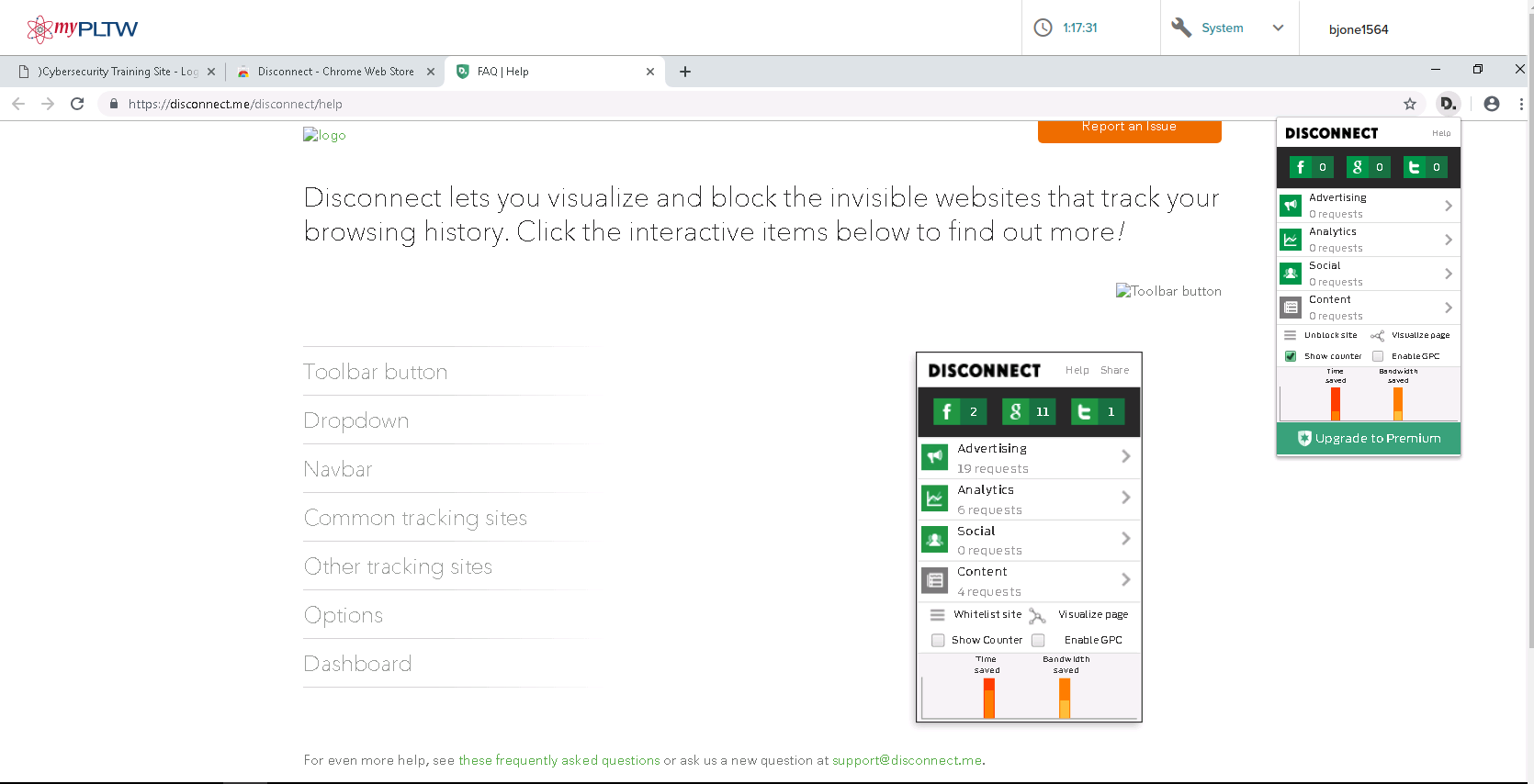
#8 Notebook

The reason I picked the specific triads for each is because of how each is described, confidentiality is for things that are more sensitive and shouldn't be given out often such as a social security number. Availability is for things that should be easily accessed and don't need much security as well as won't cause problems if it got leaked, such as a family calendar or a shopping catalog. Integrity is used for things that are important and shouldn't be tampered with, but can be seen by others with little to no consequence, such as flight times and hospital data such as dosage for medication or the schedule for surgeries.

#11 Screenshot of completed matrix

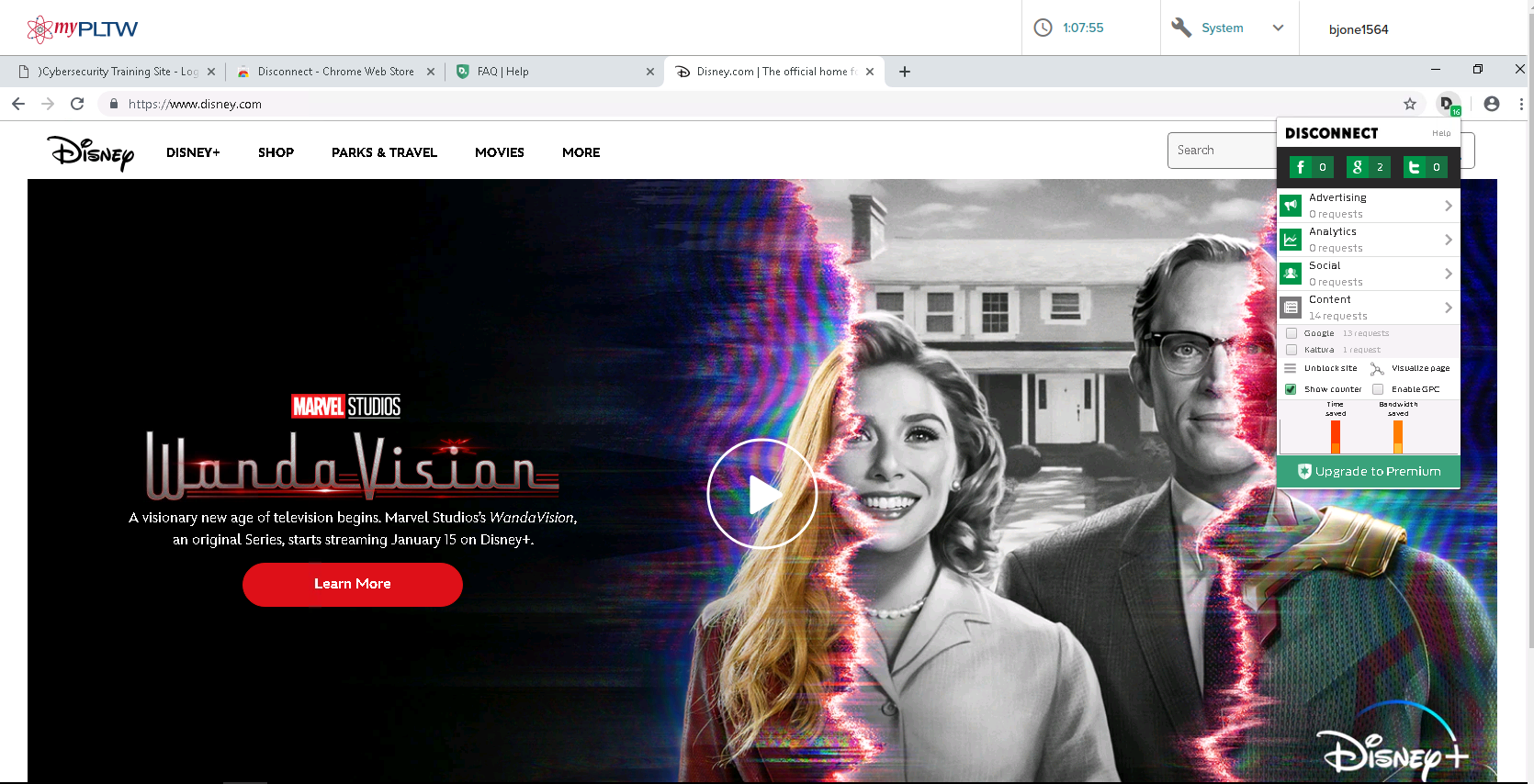


#18 Screenshot of Disconnect



#20 Screenshot and Notebook answers

My browser accessed two additional sites, Google and Kaltura.



#22 Notebook

1. I take precautions when browsing the internet on my personal devices. While I can't say I'm not completely safe when it comes to cyber-attacks, I do feel that I am safe to the point that I am not worried about being a victim of a cyber-attack.
2. I think on standards of personal devices availability should be a priority. But for something like school computers, I think there should be a fair amount of integrity as well as confidentiality. There's content that needs to be accessed by certain people on the school computers, things that should be seen but not shared with everyone. Sensitive info that needs to be accessed but not necessarily available.

Conclusion Questions

* Research an IoT device as directed by your teacher. Prepare to discuss its pros and cons, functionally and ethically. You can draw this table in your notebook to help you organize your work.

|  |  |  |
| --- | --- | --- |
|  | * **Pros** | * **Cons** |
| * Functionally | * Easier use of technology and other products as well as remote use. | * Requires constant monitoring, as well as possibility for actions not wanted by the user. |
| * Ethically | * Can help with people who have disabilities, help increase quality of life. | * Some devices constantly listen to conversations that could have potentially sensitive information in it, sending data to the companies that run these devices. Possibility for cyber- attacks and leak information to the public. |

* Refer to the table you completed in the previous section for the Bikes, Boards, and Beyond system. Summarize the security considerations that you would suggest to ensure the information architecture meets the CIA Triad model.

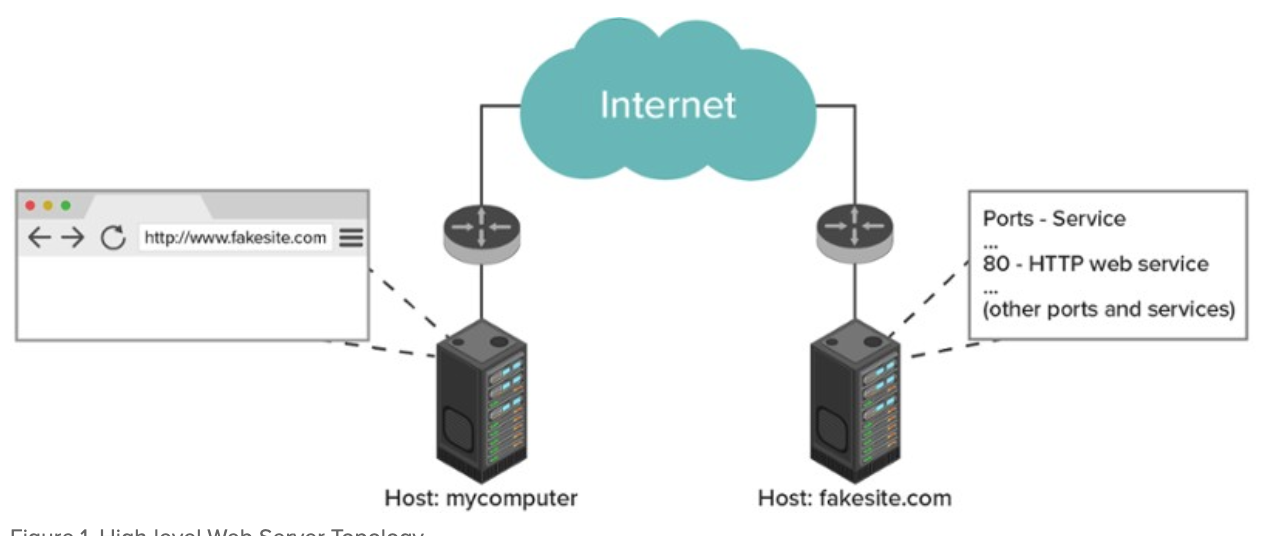
**Unit 2.1.2**

**Goals**

* Identify website ownership
* Observe website traffic
* Learn about domain names and the domain name service
* Identify ports and their services

**Resources for 2.1.2**

* [IANA Service Names and Port Numbers](https://lms-content.pltw.org/curriculum/HS/CS/SEC/Student/unit2/IANA_service-names-port-numbers.csv)
* [Login in for AWS - Follow directions from teacher on using](http://www.awseducate.com/signin/SiteLogin)



#15 Notebook

#16 Screenshot

#23 Notebook

#26 Notebook

#27 Notebook

#28 Notebook

#30 Screenshot & Notebook

#31 Notebook

#32 Screenshot

#34 Screenshot

#36 - Screenshot

#37 Notebook

#39 Notebook

Conclusion Questions

* Work through the following scenario: suppose you are the victim of a malware attack and you suspect a spoofed website is the problem. Summarize how each tool could help you in your investigation of the website.
  + whois
  + nslookup
  + traceroute
  + netstat

**Unit 2.1.3**

**Goals**

* Collaborate with a cybersecurity team.
* Create network topologies.
* Reflect on your cyber team experience

**2.1.3 Rubric**

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** | **Basic** | **Proficient** | **Advanced** |
| Asset Identification  LO 9.1: Identify the components (software, hardware, protocols) that allow computers to network and communicate.  LO 10.3: Design the correct level of protection by implementing the appropriate safeguards. | The student identified some of the data elements and their security components related to the CIA Triad (from A2.1.1). | The student identified most of the data elements and their security components related to the CIA Triad (from A2.1.1) | The student identified all of the data elements and their security components related to the CIA Triad (from A2.1.1) |
| The student identified no more than a few of the hardware needed for the network. | The student identified most of the hardware needed for the network. | The student identified all of the hardware needed for the network. |
| Risk Protection  LO 8.2: Identify user actions that strengthen the security of information stored on a computer.  LO 10.3: Design the correct level of protection by implementing the appropriate safeguards. | The student identified no more than a few of the encryption requirements for the data. | The student identified most of the encryption requirements for the data. | The student identified all of the encryption requirements for the data. |
| Documentation  LO 15.2: Recognize documentation as an indispensable part of the security process. | The student created an inadequate or inaccurate network topology diagram. | The student created an adequate but slightly inaccurate network topology diagram. | The student created a thorough and accurate network topology diagram. |
| The student created minimal to no documentation explaining their protection measures and choice of network topology. | The student created adequate documentation explaining their protection measures and choice of network topology. | The student created thorough documentation explaining their protection measures and choice of network topology. |
| Collaboration  LO 14.2: Collaborate effectively as part of a team  LO 14.3: Apply project management strategies effectively as part of a team. | The student is inconsistently engaged and inadequately contributes to the team’s work. | The student is consistently engaged and adequately contributes to the team’s work. | The student is consistently engaged and substantially contributes to the team’s work. |
| The student rarely provides constructive feedback to others and does not encourage or incorporate input from others. | The student occasionally provides constructive feedback to others and consistently encourages and incorporates input from others. | The student consistently provides constructive feedback to others and consistently encourages and incorporates input from others. |
| Presentation (Optional)  LO 2.2: Engage stakeholder in a problem and use their perspectives to shape the course of your development.  LO 15.1: Communicate ideas, processes, and products to optimize audience perception and understanding. | The student rarely participates in the presentation. | The student occasionally participates in the presentation. | The student substantially participates in the presentation. |
| The presenter is unclear, presents some of the necessary information, and does not stay on topic. | The presenter is clear, presents most or all of the necessary information, but does not stay on topic. | The presenter is clear, presents all of the necessary information, and stays on topic. |
| The presenter rarely uses appropriate body language, voice modulation, and eye contact. | The presenter occasionally uses appropriate body language, voice modulation, and eye contact. | The presenter consistently uses appropriate body language, voice modulation, and eye contact. |

### **Comments**

#4 Notebook - Screenshot of Topology (or insert Google Draw into notebook)

Most servers are not connected directly to the internet seeing as how they are the ones that mostly make up the internet. But the closest (at least what I found) thing is a Star Topology Network.

Customer information

#8 Notebook - Be detailed with explanation

#10 Notebook

Career Exploration - Notebook with citations

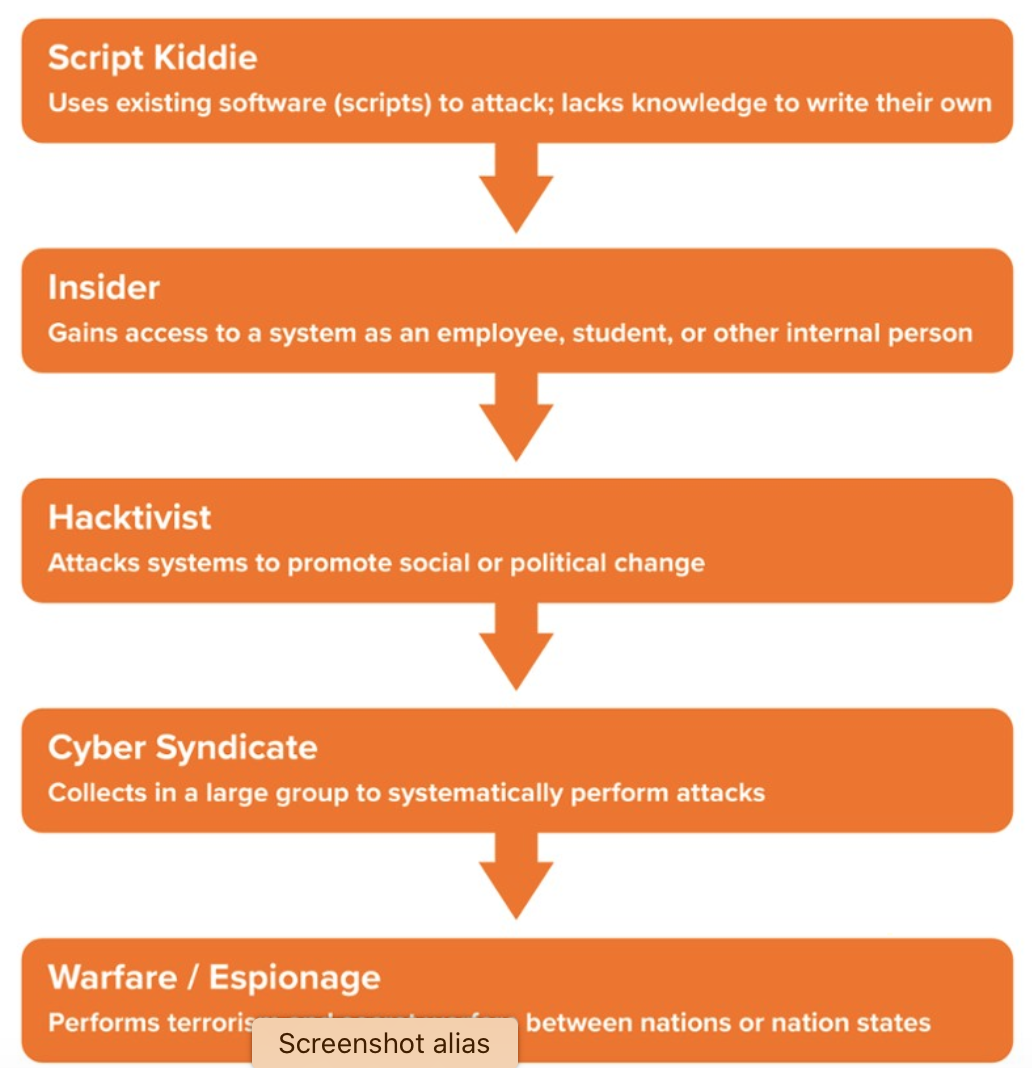
Conclusion Questions

* Compare your design to another team’s design. Is there anything you’d like to improve or would recommend to the other team to modify? Explain your thoughts.
* Is there such a thing as “too much security”? Why or why not?

**Unit 2.2.1**

**Goals**

* Define malware.
* Learn malware types and levels of sophistication.
* Learn motivations of malicious users.

****

#1 Notebook- Attack one & Attack two

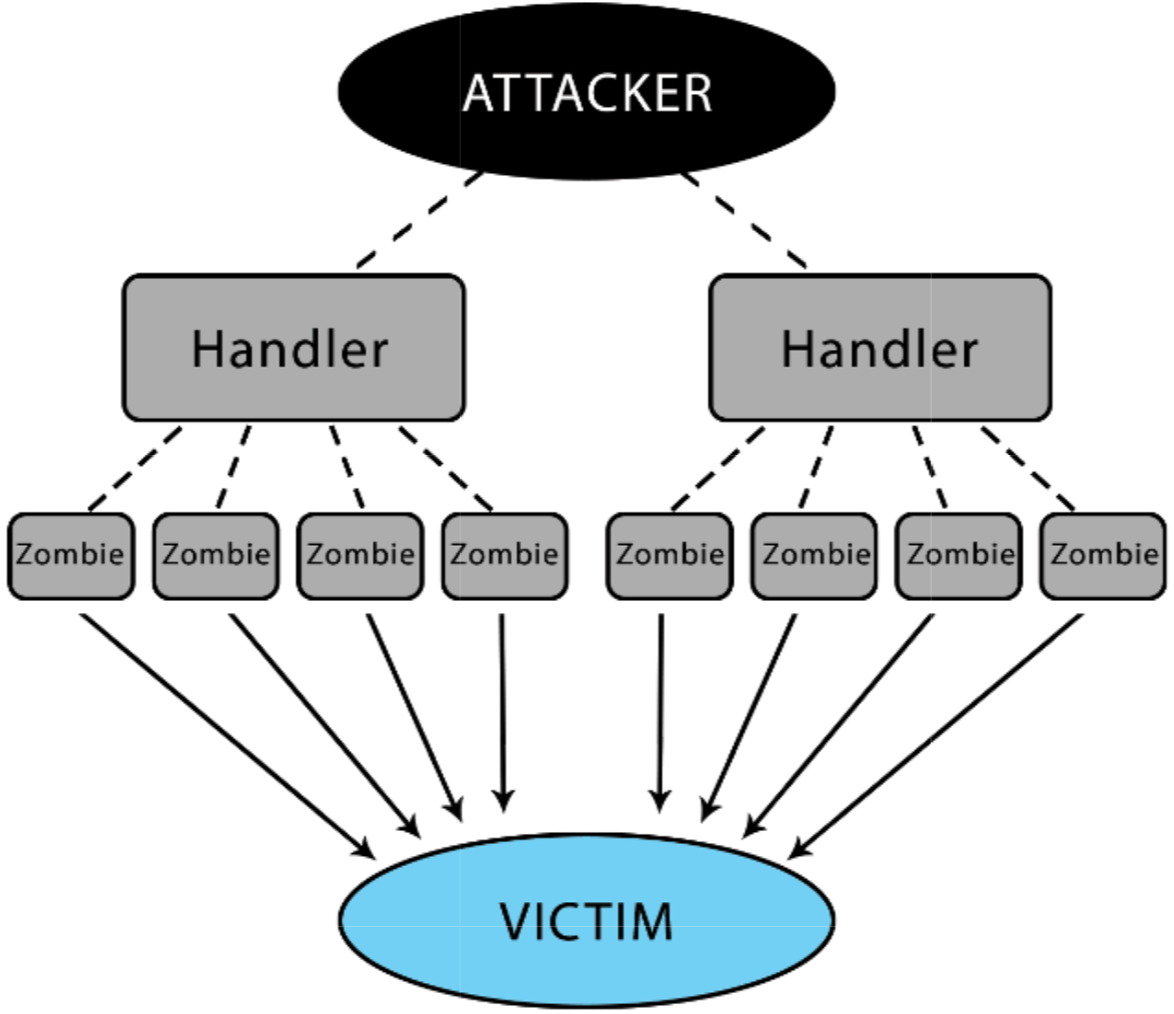
1. The goal must have been to make the user unable to use their computer seeing as they used the malware to shut down all system operations. I feel that most malware does need some way to be passed on, however not all malware does. I would say this is a more malicious attack because it secretly takes out the user’s computer rather than make an attack that could possibly be stopped.
2. I feel that the hacker (unless done by the government) would definitely be unauthorized, however I do think that he would be partially authorized because of his goal from DDoSing.

#2 Notebook - All four questions

1. Retaliation would be considered an Authorized attack.
2. Company B is trying to protect their information from the attackers, by attakcing them back.
3. I would say that Company B is trying to be ethical, but there are better ways through legal proceedings to reclaim their stolen information.
4. While the attack was in good faith, I am not entirely sure if company B should face legal proceedings or not. They still launched a cyber attack, but the purpose behind it was for good. I could see them going into court, but the overall rule could turn out as innocent.

#3 Notebook - All six types - Don’t just write what is on the page and be specific. Go back to 1.2.1

1. Virus: software spread by people.
2. Worm: Virus, but doesn’t require humans to spread.
3. Backdoor: malicious software that bypasses restricted access.
4. Spyware: Software that secretly collects information about the user.
5. Trojan Horse: A program that once opened launches an attack on the user.
6. Ransomware: A program in which the attacker takes control over your computer or steals information and won’t return it until a fee is payed.



DDoS Example

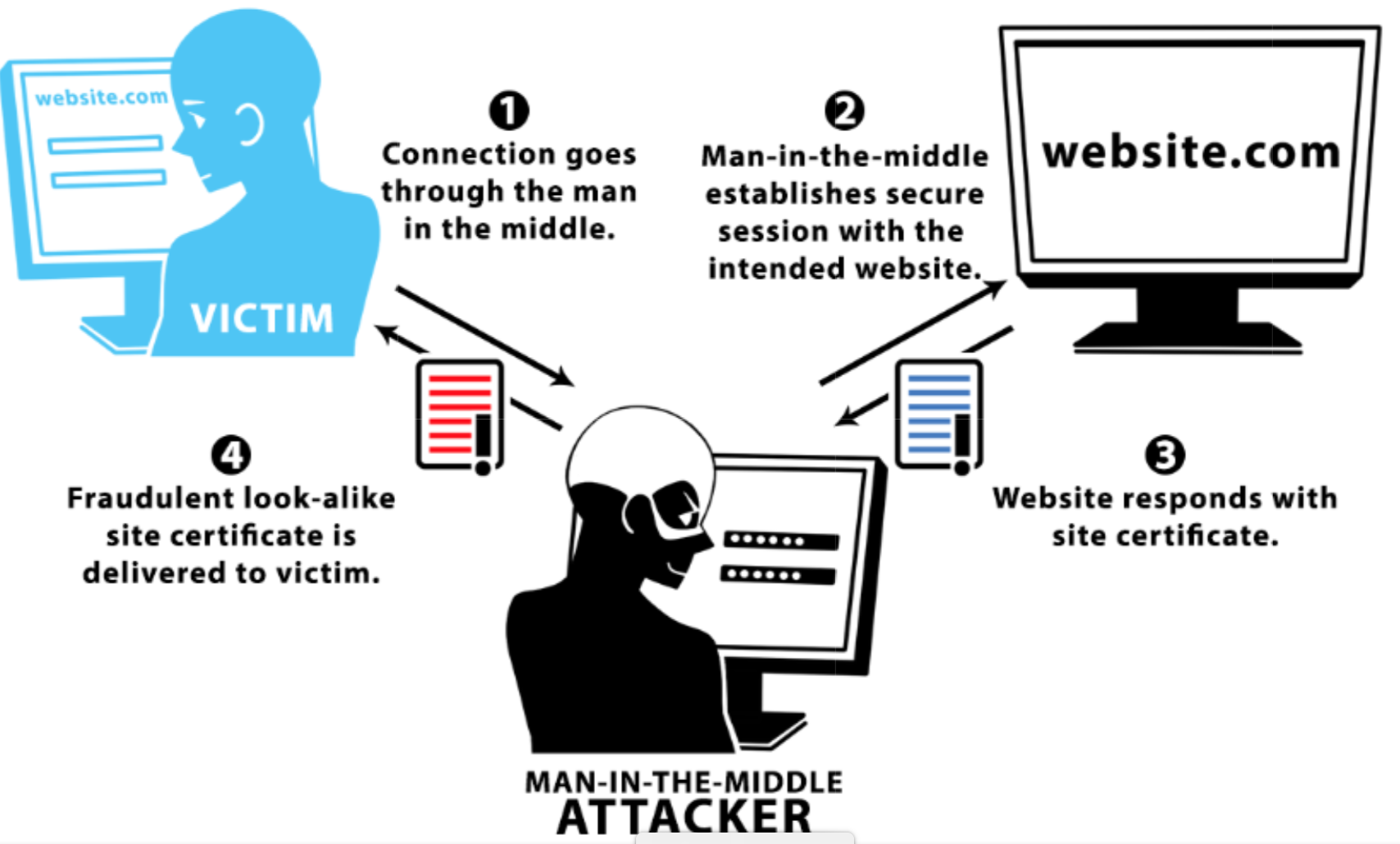
#4 Notebook - All five and be specific.

Ping Flood: The attacker overwhelms the target’s device by flooding the device with pings.

Ping of Death: The attacker sends a malformed or malicious ping in attempt.

Smurf attack: Large numbers of packets with the victims source IP are broadcast to computer networks.

Mail Bomb: The attacker uses bots to automatically subscribe the victim to message subscriptions, to which they are then bombarded with emails, the intention being to make the email unusable or cause network downtime.



#5 Notebook

Encryption can prevent the MitM from reading your network messages being sent to the intended site.

Latency could be a part of the attack because the attacker has to send info that is similar looking to the website that is being accessed. If his network connection is slow then it could cause latency as well.

#6 Notebook -all three

STUXNET Activity - For some extra credit you may complete the STUXNET activity listed at an optional extension in Rootkit section.

Conclusion Questions

* Many different vulnerabilities can affect systems in many different ways. As security specialists gain the upper hand on malicious users, new malware is discovered, and new attacks occur. Staying ahead of this cybersecurity “game” can be challenging, but it can also be exciting and rewarding. What aspects of detecting and fighting malware appeals to you the most?

**Unit 2.2.2**

**Goals**

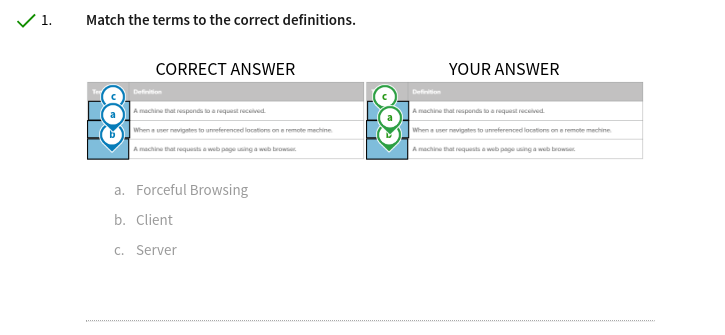
* Learn how web servers organize files.
* Investigate a web server for directory browsing and log file location vulnerabilities.
* Use anonymous FTP to update a web server.

#3 Notebook & Screenshot

myotherfile.txt



#4 Screenshot of the completed chart



#7 Notebook

Custerr

Ftp root

Hidden\_directory1

History

Logs

Mailroot

Temp

>Wwwroot

|iisstart.htm

|iisstart.png

|web.config

Index.html

Web.config

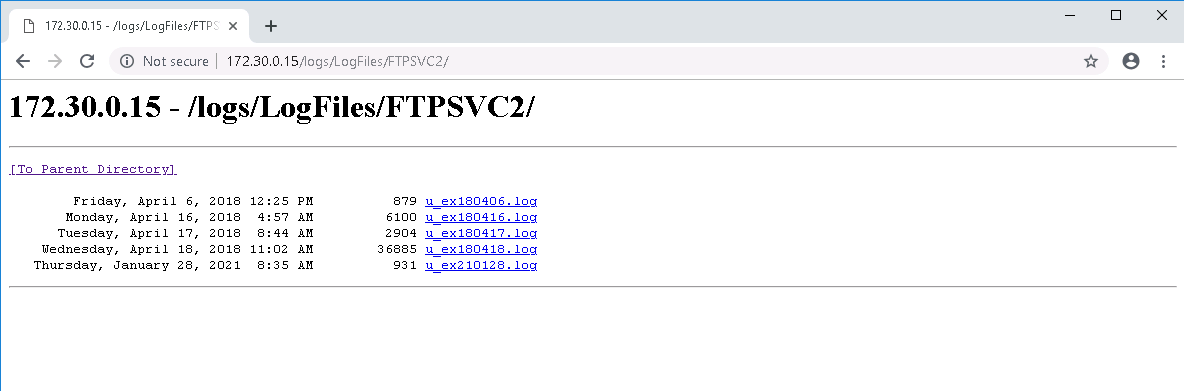
#9 Notebook

172.30.0.15/www root/iisstart.htm - didn’t work.

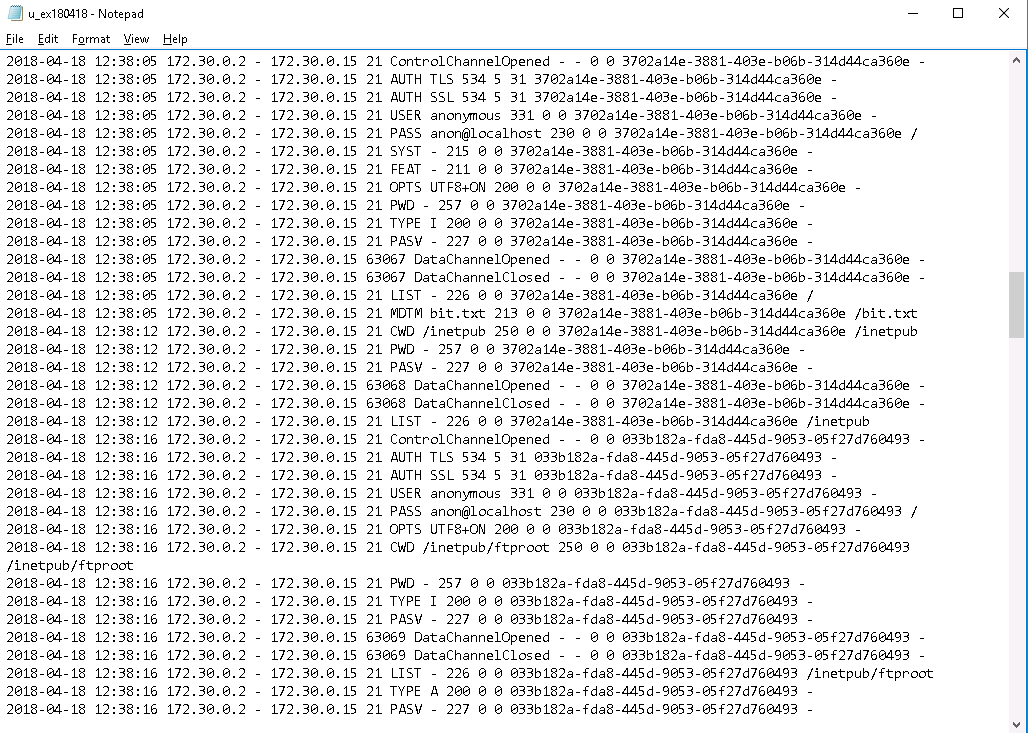
172.30.0.15/index.html - didn’t work.

#12 Notebook & Multiple Screenshots

There are sub directories that are able to be navigated, the files are type .log.

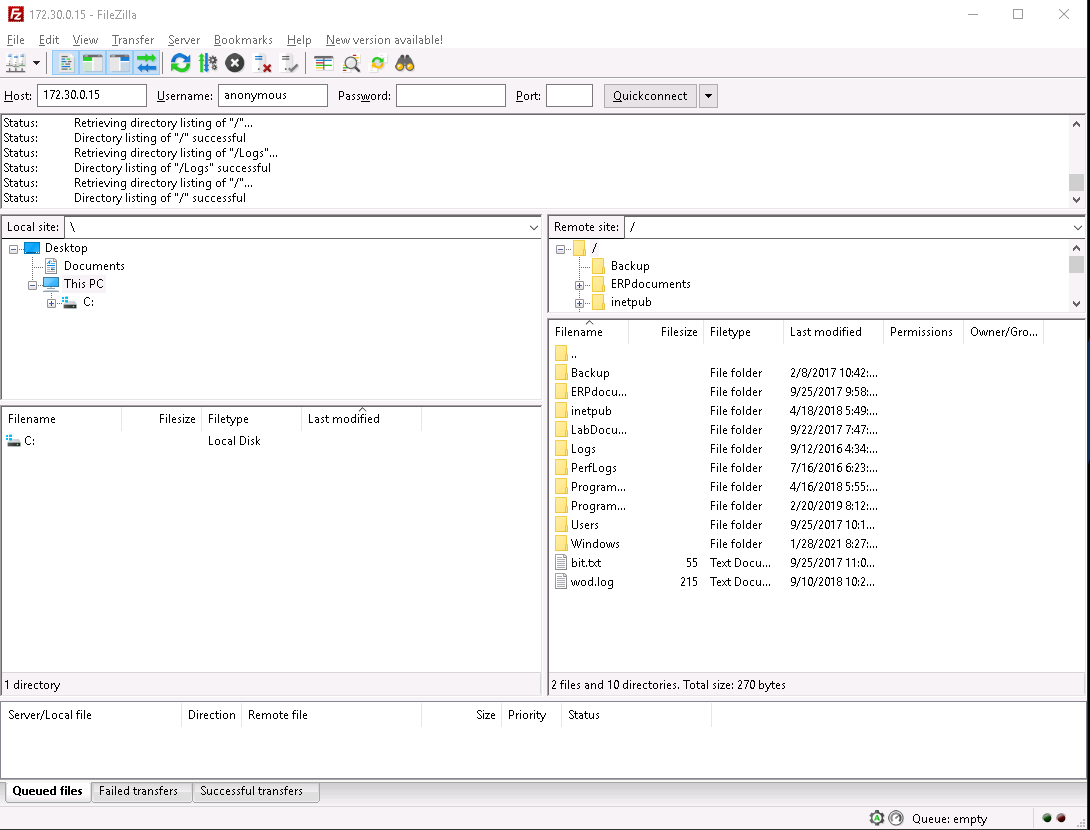


u\_ex180418.log has some sign in information for some program, including a password.

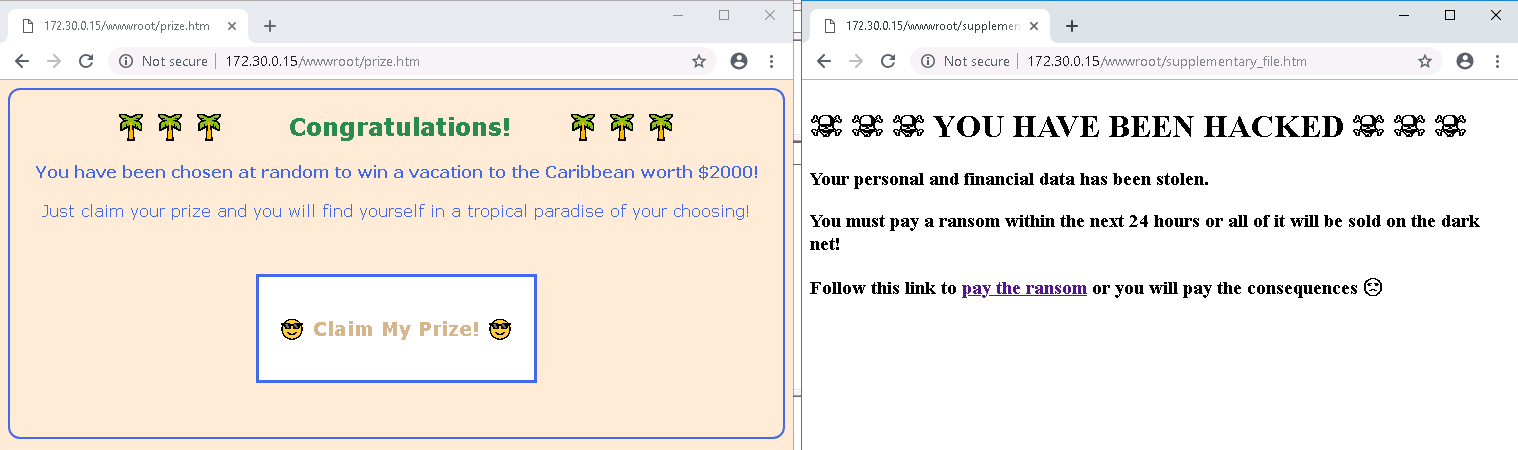


#16 Notebook & Screenshot

This shows all of the programs and files that go through the web server, I can also access all the logs as well as other program files.



#18 Screenshot



NVD Extension - Extra Credit

CVE-2001-0333: Allows remote attackers to execute arbitrary commands by encoding “..” and “\” characters twice.

CVE-2001-0335: Allows remote attackers to enumerate guest accounts in trusted domains by preceding the username with a special sequence of characters.

Conclusion Questions

* Write a summary about what you’ve learned in this activity regarding vulnerabilities and how attackers may be able to use them. Consider how an attacker might be able to combine the vulnerabilities to achieve some goal. Your summary should address the following questions:
  + What is dangerous about allowing users to explore the directory structure of a web server?
  + How can an attacker use the knowledge of the location of a log file to their advantage?
  + How should a security professional deal with non-essential services running on a web server?

**Unit 2.2.3**

**Goals**

Mitigate web server vulnerabilities including

* Directory browsing
* Default log file location
* Anonymous FTP

#10 Notebook & Screenshot

#16 Notebook & Screenshot

#17 Notebook

#30 Screenshot & Notebook

Conclusion Questions

* How does the security (or lack of security) on the host affect the security of the web server?

**Unit 2.2.4**

**Goals**

* Collaborate with a cybersecurity team.
* Mitigate web server vulnerabilities SMTP and loose-lipped errors.
* Create a report to document your remediation steps.
* Reflect on your cyber team experience.

#2 Notebook

#7 Notebook

#8 Screenshot

#9 Notebook & Screenshot

#12 Notebook - Create plan

#16 Notebook & Multiple Screenshots

Conclusion Questions

* What security trade-offs or options should an administrator consider when confronted with a potentially extraneous service, such as FTP or SMTP, running on a web server?
* What kinds of information can an attacker identify that may help them compromise a web server’s security?
* Pick two of the vulnerabilities you’ve explored in this lesson and explain how an attacker can exploit them to infect a server with malware.

**Unit 2.3.1**

**Goals**

* Learn client-server architecture.
* Explore JavaScript programs.
* Recognize and mitigate cross-site scripting exploits and SQL injection exploits.

**Resources / Reminders**

1. **Become familiar with Client Server Communication Slides**
2. **Record the techniques in lessons and passwords and usernames. Record here- This will be used later**

#5 Notebook

#6 Notebook

#7 Notebook - explain why

#11 - it should look like this:



#14 Screenshot & Notebook

#15 Screenshot & Notebook

#17 Notebook

#20 Screenshot & Notebook

#26 Notebook

#29 Screenshot & Notebook

#30 Screenshot & Notebook

#31 Screenshot & Notebook

#33 Screenshot & Notebook (Pick one of the SQL injects for the screenshot.)

#36 Screenshot & Notebook

Optional Extension - Research

**Conclusion Questions**

* How can you apply the security measures presented in this activity to the Bikes, Boards, and Beyond website?
* Data cleansing is a common protection measure that companies implement today. Do you think it’s acceptable to try out XSS and SQL injection for fun thinking it won’t harm anyone? Explain your thinking.
* Update your Code of Conduct to reflect ethical decisions related to web page exploits.

**Unit 2.3.2**

**Goals**

* Learn basic network topology.
* Monitor and analyze data packets.
* Witness and mitigate a ping flood attack.

# 5 Notebook

#7 Notebook

#11 Screenshot & Notebook

#13 Notebook

#18 Notebook

#25 Notebook

#26 - 28 Notebook - write down the commands

#31 Screenshot & Notebook

#37 Notebook

#40 Notebook

**Conclusion Questions**

* What do you think is the goal of a ping flood attack? Why would someone use this type of attack vector? Think about the types of hackers on the internet (black/white/gray).
* How could an attack like a ping flood be harmful to an entire network?

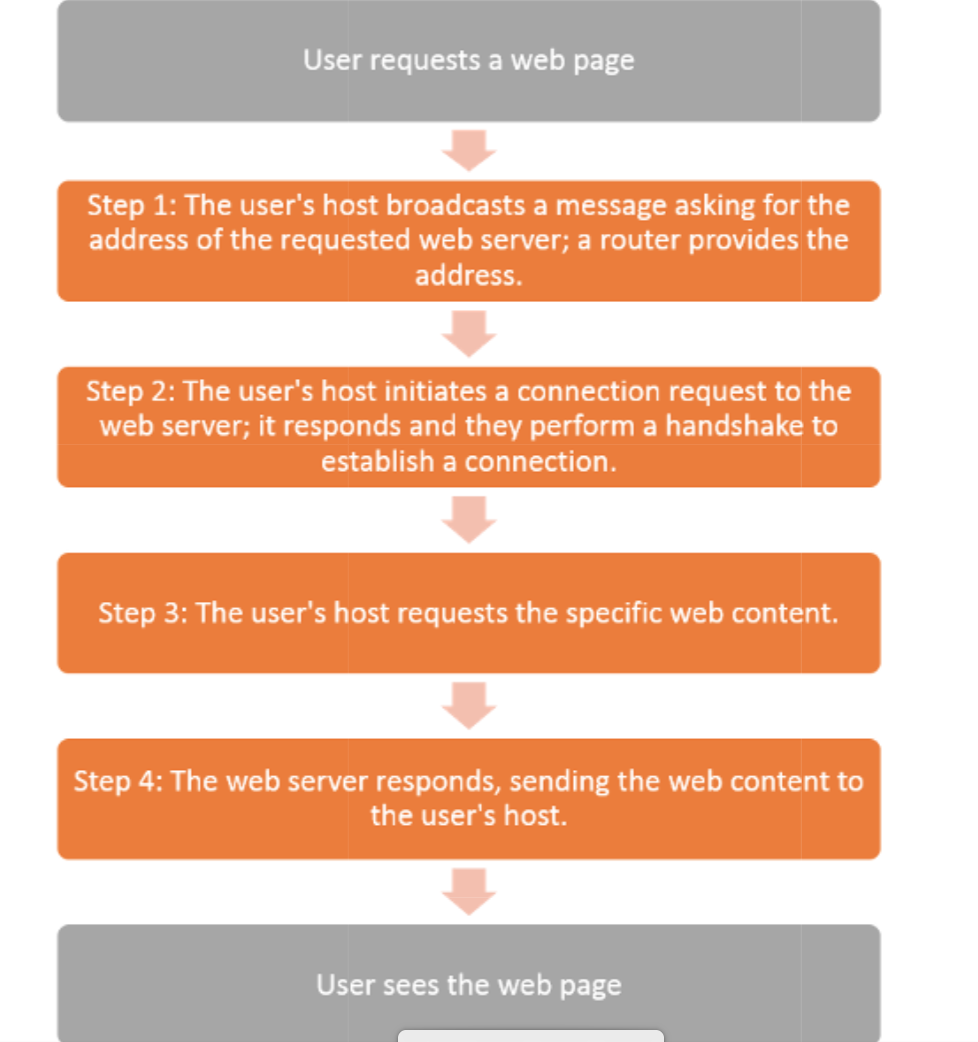
**Unit 2.3.3**

**Goals**

* Analyze packets related to broadcasting, TCP handshakes, and HTTP requests and responses.
* Witness packets involved in a brute force attack.

**Resources**

[IEEE\_regauth\_OUI.txt](https://lms-content.pltw.org/curriculum/HS/CS/SEC/Student/unit2/IEEE_regauth_OUIs.txt)



#6 Notebook

#9 Notebook

#12 Screenshot - After you apply the filter, look for Packet list Info that may answer the question. The answer in the Info column

#14 Notebook

#15 Notebook & Screenshot

#16 - Notebook

#19 - Notebook & Screenshot - Lines that show the handshake with this system.

#24 Screenshot

#25 - Notebook

#26 - Notebook

#28 Notebook & Screenshot - look for the <SCRIPT> and </SCRIPT> tags that encompass the WebFontConfig script name.

#35 Notebook

#37 - Notebook

#38 Notebook & Screenshot - Look in the filter pane on top to see the answer

Conclusion Questions

* Why would website applications encrypt or encode data that they send over the network? Be sure to include what you learned in Wireshark in your answer.
* Why would a black-hat hacker want to spoof a MAC address?
* Suppose a brute force attack was made using a computer algorithm that runs automatically. Describe how the packet capture data for this attack would look different than the data you saw in this activity.

**Unit 2.3.4**

**Goals**

* Collaborate with a cybersecurity team.
* Participate in a “training exercise” to recognize
  + - An XSS Stored attack
    - A Command Execution attack.
* Perform a penetration test on a website and document it.
* Reflect on your cyber team experience.

# **Project 2.3.4 Find the Exploits**

|  |  |  |  |
| --- | --- | --- | --- |
| Criteria | Basic | Proficient | Advanced |
| Asset Identification  LO 8.2: Identify user actions that strengthen the security of information stored on a computer. | The student briefly mentioned what information may have been compromised. | The student adequately described what information may have been compromised. | The student accurately and thoroughly described what information may have been compromised. |
| Risk Protection  LO 5.1: Find patterns and test hypotheses about digitally processed information to gain insight and knowledge.  LO 9.1: Identify the components (software, hardware, protocols) that allow computers to network and communicate.  LO 9.3: Identify user actions that strengthen the security of a networked system.  LO 10.4: Detect and analyze the occurrence of a cybersecurity event. | The student identified all suspicious packets and packet details for one of the three exploits captured in the pcap files. | The student identified all suspicious packets and packet details for the two of the three exploits captured in the pcap files. | The student identified all suspicious packets and packet details for the all three exploits captured in the pcap files. |
| The student correctly identified the software corrections for one of the three exploits captured in the pcap files.  *-or-*  The student correctly identified the entire script rather than the correct section of code. | The student correctly identified the software corrections for two of the three exploits captured in the pcap files.  *-or-*  The student identified the entire script rather than the correct section of code. | The student correctly identified the software corrections for all three exploits captured in the pcap files. |
| Risk Detection  LO 4.2: Apply tools with varying levels of abstraction within software, a computer, a network, and the internet.  LO 7.2: Use abstractions to manage and analyze information.  LO 9.2: Analyze the evidence of web exploitations, both from front-end application and back-end services perspective.  LO 10.2: Analyze the evidence of an attack. | The student identified few suspicious packets or packet details for any of the training section attacks:  XSS Stored  Command execution | The student identified most suspicious packets or packet details for any of the training section attacks:  XSS Stored  Command execution | The student identified all suspicious packets and packet details for both exploits training section attacks:  XSS Stored  Command execution |
| The student partially identified software corrections for the training section:  XSS Stored  Command execution | The student identified the entire script rather than the correct section of code for the training section attacks for one or both training section attacks:  XSS Stored  Command execution | The student correctly identified the software corrections for the both exploits in the training section attacks:  XSS Stored  Command execution |
| Documentation  LO 7.1: Describe the variety of abstractions used to represent data.  LO 15.2: Recognize documentation as an indispensable part of the security process. | The student created an inadequate or inaccurate network topology diagram. | The student created an adequate but slightly inaccurate network topology diagram. | The student created a thorough and accurate network topology diagram. |
| The student created minimal to no documentation explaining their protection measures and choice of network topology. | The student created adequate documentation explaining their protection measures and choice of network topology. | The student created thorough documentation explaining their protection measures and choice of network topology. |
| Collaboration  LO 13.1: Abide by professional, ethical, and legal standards when handling data or protecting data.  LO 14.1: Collaborate when processing information to gain insight and knowledge.  LO 14.2: Collaborate effectively as part of a team.  LO 14.3: Apply project management strategies effectively as part of a team.  LO 15.1: Communicate ideas, processes, and products to optimize audience perception and understanding. | The student is inconsistently engaged and inadequately contributes to the team’s work. | The student is consistently engaged and adequately contributes to the team’s work. | The student is consistently engaged and substantially contributes to the team’s work. |
| The student rarely provides constructive feedback to others and does not encourage or incorporate input from others. | The student occasionally provides constructive feedback to others and consistently encourages and incorporates input from others. | The student consistently provides constructive feedback to others and consistently encourages and incorporates input from others. |

### Comments

#7 Screenshot & Notebook

#8 Screenshot

#10 Screenshot & Notebook

#11 Screenshot

#16 - Several Screenshot & Notebook

#18 Screenshot

Conclusion Questions

* How do you think the people responsible for the web server, the web pages, and scripts could have prevented these vulnerabilities?
* Why is this series of pen testing an ethical use of hacking skills?

**Unit 2.4.1**

**Goals**

* Collaborate with a cybersecurity team.
* Create a plan of action.
* Perform a pen test of a website and document all aspects of the test.
* Create a Pen Test report.
* Reflect on your cyber team experience.

**Rubric**

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** | **Basic** | **Proficient** | **Advanced** |
| Risk Detection  LO 5.1: Find patterns and test hypotheses about digitally processed information to gain insight and knowledge.  LO 9.1: Identify the components (software, hardware, protocols) that allow computers to network and communicate.  LO 9.3: Identify user actions that strengthen the security of a networked system.  LO 10.4: Detect and analyze the occurrence of a cybersecurity event. | The student created a plan of action that addressed only a few of the steps the team expects to perform to identify, detect, protect and report the vulnerabilities. | The student created a plan of action that addressed most of the steps the team expects to perform to identify, detect, protect and report the vulnerabilities. | The student created a plan of action that addressed all of the steps the team expects to perform to identify, detect, protect and report the vulnerabilities. |
| Webserver:  The student identified the status (enabled and vulnerable, or disabled and secured) of only a few (one to three) server vulnerabilities. | Webserver:  The student identified the status (enabled and vulnerable, or disabled and secured) of most (four or five) server vulnerabilities. | Webserver:  The student identified the status (enabled and vulnerable, or disabled and secured) of all (six) server vulnerabilities. |
| Website:  The student addressed how they tested one exploit on one or both web pages of the pen test site. | Website:  The student addressed how they tested most (two or three) exploits on both web pages of the pen test site. | Website:  The student addressed how they tested all (four) exploits on both web pages of the pen test site. |
| Risk Protection  LO 4.2: Apply tools with varying levels of abstraction within software, a computer, a network, and the internet.  LO 7.2: Use abstractions to manage and analyze information.  LO 9.2: Analyze the evidence of web exploitations, from both front-end application and back-end services perspectives.  LO 10.2: Analyze the evidence of an attack. | Webserver:  The student correctly identified the configuration to secure one vulnerability found on the server. | Webserver:  The student correctly identified the configuration to secure most of the vulnerabilities found on the server. | Webserver:  The student correctly identified the configuration to secure all vulnerabilities found on the server. |
| Website:  The student correctly identified one exploit.  The student correctly identified one script that will secure the exploited web pages. | Website:  The student correctly identified most exploits.  The student correctly identified most scripts that will secure the exploited web pages. | Website:  The student correctly identified all exploits.  The student correctly identified all scripts that will secure the exploited web pages. |
| Response Plan Documentation  LO 15.2: Recognize documentation as an indispensable part of the security process. | Webserver:  The student accurately documented their test results and recommendations for one vulnerability:  Evidence of the vulnerability  Recommended configuration | Webserver:  The student accurately documented their test results and recommendations for most vulnerabilities:  Evidence of the vulnerability  Recommended configuration | Webserver:  The student accurately documented their test results and recommendations for all vulnerabilities:  Evidence of the vulnerability  Recommended configuration |
| Website:  The student accurately documented their tests results and recommendations for one exploit:  Evidence of the exploited web page  Wireshark packet with exploited URL  Recommended script | Website:  The student accurately documented their tests results and recommendations for most exploits:  Evidence of the exploited web page  Wireshark packet with exploited URL  Recommended script | Website:  The student accurately documented their tests results and recommendations for all exploits:  Evidence of the exploited web page  Wireshark packet with exploited URL  Recommended script |
| Collaboration  LO 13.1: Abide by professional, ethical, and legal standards when handling data or protecting data.  LO 14.1: Collaborate when processing information to gain insight and knowledge.  LO 14.2: Collaborate effectively as part of a team  LO 14.3: Apply project management strategies effectively as part of a team.  LO 15.1: Communicate ideas, processes, and products to optimize audience perception and understanding. | The student is inconsistently engaged and inadequately contributes to the team’s work. | The student is consistently engaged and adequately contributes to the team’s work. | The student is consistently engaged and substantially contributes to the team’s work. |
| The student rarely provides constructive feedback to others and does not encourage or incorporate input from others. | The student occasionally provides constructive feedback to others and consistently encourages and incorporates input from others. | The student consistently provides constructive feedback to others and consistently encourages and incorporates input from others. |
| Presentation (Optional)  LO 2.2: Engage stakeholder in a problem and use their perspectives to shape the course of your development.  LO 15.1: Communicate ideas, processes, and products to optimize audience perception and understanding. | The student rarely participates in the presentation. | The student occasionally participates in the presentation. | The student substantially participates in the presentation. |
| The presenter is unclear, presents some of the necessary information, and does not stay on topic. | The presenter is clear, presents most or all of the necessary information, but does not stay on topic. | The presenter is clear, presents all of the necessary information, and stays on topic. |
| The presenter rarely uses appropriate body language, voice modulation, and eye contact. | The presenter occasionally uses appropriate body language, voice modulation, and eye contact. | The presenter consistently uses appropriate body language, voice modulation, and eye contact. |

### **Comments**

#6 - #9 Notebook - Create a plan

#12 Notebook & Screenshots (Important: Copy the web addresses of the exploits)

Follow directions about creating screenshots of scripts and results

**Prepare a report based on:**

* Identify
* Detect
* Protects
* Responds

**#16 Notebook**

**Conclusion Questions**

* Why should a security analyst be able to read and analyze software such as programs written in JavaScript?
* Why is it important to plan and then document all of the steps you take in a pen test?