**Lesson 2.2 – Server Vulnerabilities**

**\*\*Instructions:** Please change the text color of your responses to red text. Please organize the endings to each page.

**Activity 2.2.1 – More on Malware**

**\*\*Ethical hackers are in high demand. They have many career choices, and they are some of the highest paid professionals working today. The TechRepublic website estimates that there will be 1.8 million cybersecurity job openings by the year 2022 and there will be jobs all over the world.**

1. What do you think the goal was? Do you think a malware that requires someone to pass it on (as in an email) is more or less malicious than a direct attack on a system? (Step #1)
2. One could argue that the DDoS attack on social media accounts had a positive, ethical goal - to shut down terrorist activities by eliminating their ability to communicate. Do you think this would make the attacker a black-hat (criminal) hacker, white-hat (ethical) hacker, or somewhere between? (Step #1 part #2)
3. Snipping Tool image of Motivation and Goals Question – Matching (After Step #1)
4. Integrity and Ethics (Step #2)
   1. Is a retaliation attack a black-hat, white-hat, or gray-hat attack?
   2. What do you suppose is the motivation of Company B? What is the goal?
   3. Are either company’s actions ethical?
   4. Should Company B face legal consequences?
5. Types of Malware

|  |  |
| --- | --- |
| Botnet |  |
| Keylogger |  |
| Man-in-the-Middle |  |
| Ransomware |  |
| Rootkit |  |
| Programming Errors |  |

1. Summarize how each DDoS attack works

|  |  |
| --- | --- |
| Ping flood |  |
| Ping of death |  |
| Smurf attack |  |
| Mailbomb |  |
| Teardrop |  |

1. Figure #4 in Detail (Step #5)
   1. How can an encrypted connection in step 1 help secure the end user against a man-in-the-middle attack?
   2. How could latency, a delay in the transfer of data between steps 1 and 4, play a part in detecting a man-in-the-middle attack?
2. Research the large-scale ransomware attack called WannaCry (Step #6)
   1. What is the motivation of the attack?
   2. How did the attack spread?
   3. How did a Microsoft security update from April 017 affect the attack?
3. Snipping Tool image of Programming Errors – Matching (After Step #6 – Programming Errors)
4. Ethical Scenario: Cyber Warfare
   1. At what point is it acceptable, if at all, to engage in cyber warfare with an adversary of the state?
   2. Whose responsibility is it to protect private citizens and organizations from being attacked in a cyber war?

**CONCLUSION**

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?