**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 2.2.2 – Server Vulnerabilities**

**\*\*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. Screenshot of the Directory (Direction #3 Step D)
2. Document the directory structure within the inetpub folder listing the following in particular; you will need them later in this activity: (After Step #7)
   1. The names of subfolders and files in inetpub
   2. The names of the files in wwwroot
3. Explain how the contents of the hidden\_directory1 folder relate to the screenshot you took in step 3d.
4. Explain why hidden\_directory2 caused an error in step 3.
5. Document the two addresses you crafted and the result of trying each one. Were they successful or did they cause an error? (Step #9)
6. Record what you see (After Step #12)
   1. Are there sub-directories? If so, can you navigate into them?
   2. What files can you see? Record their type(s).
   3. Save a screenshot of your browser as evidence of your ability to access the log file directory.
   4. Browsers cannot display log files, but the files can be downloaded. Download and open a log file.
   5. In one of the log files, there’s information that would be very valuable to a malicious hacker. What is the file and what does it contain?
   6. Save a screenshot as evidence of your ability to access the log file.
7. What does this tell you about the web server? (After Step #16)
8. Save a screenshot of the result as evidence. (After Step #16)
9. Find and save a screenshot of any malicious content as evidence. (After Step #18)

**OPTIONAL EXTENSION – COMPLETE OPTIONAL EXTENSION**

1. Complete the Option Extension
   1. Describe each vulnerability and predict the consequence of an attacker exploiting it.

**CONCLUSION**

1. 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:
   1. What is dangerous about allowing users to explore the directory structure of a web server?
   2. How can an attacker use the knowledge of the location of a log file to their advantage?
   3. How should a security professional deal with non-essential services running on a web server?