**Lesson 2.2 – Server Vulnerabilities**

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

**Project 2.2.4 – Secure the Server**

1. Answer the following questions about SMTP. (After Step #2)
   1. What is its primary purpose?
   2. Is it needed for a web server? Why or why not?
2. Record the SMTP port number in your notebook. (After Step #7)
3. Save a screenshot of the result as evidence that the service is currently running. (After Step #8)
4. What can you learn about the web server from the error message displayed in your window? (After Step #9)
5. Save a screenshot as evidence of loose-lipped error messages. (After Step #9)
6. Include in your documentation: (After Step #15)
   1. The name of the service/feature that you are addressing.
   2. An explanation of how you remediated it.
   3. Save screenshots to show your remediation work.
7. Run the appropriate utility to make sure SMTP service is no longer running. (After Step #16)
   1. Save a screenshot as evidence of each resolution
8. Using the web browser on the login machine, verify that error messaging is no longer a security weakness. (After Step #17)
   1. Save a screenshot as evidence of each resolution
9. Verify that all additional remediation steps you took have addressed the vulnerabilities that you uncovered. (After Step #18)
   1. Save a screenshot as evidence of each resolution

**Conclusion**

1. 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?
2. What kinds of information can an attacker identify that may help them compromise a web server’s security?
3. 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.