ITBU 313: Introduction to Cyber Security, Homework 06

Chapter 18, *Computer Security, Principles and Practices*

Readings

Read chapter 18 in the *Computer Security, Principles and Practices* book.

Discussion Questions

Answer the discussion questions in writing.

1. List five benefits of securty auditing.
2. What is a security audit? What is a security audit trail? Be specific.
3. What is the difference between audit functions and alarm functions?
4. List seven areas that a security policy might monitor.
5. The book mentions a couple of areas that constitute a large percentage of reported vulnerabilities. Name two of these areas.
6. How would you gain an understanding of a baseline of log entries? What does the book suggest as "the most effective way" to understand log data.
7. What is involved in an audit trail review after an event?
8. Define *baselining*.
9. Suppose you are interviewing for a cybersecurity position. The hiring manager asks you about SiEM. How would you answer his question?
10. Explain the difference between an audit review and an audit analysis.
11. (Not in book.) If you are using Windows, invoke the `Event Viewer`. Navigate to `Windows Logs`. What do you see? Examine each of the subcategories (Application, Security, Setup, etc.). Examine any Errors that you see.