ITBU 443: Threats and Counter Measures, Homework 08

Chapter 08, *Computer Security, Principles and Practices*

Readings

Read chapter 08 in the *Computer Security, Principles and Practices* book.

Discussion Questions

Answer the discussion questions in writing.

1. List the four broad types of intruders. Give a real life example of an APT.
2. Name some tasks (behaviors) that intruders may perform.
3. Describe the three components of an IDS.
4. Briefly discuss the two approaches to detecting intrusions. This is a important question and you will see this again.
5. What are four kinds of data sources for IDS systems?
6. How does a NIDS differ from an HIDS?
7. What are the two threats (according to the book) that confront protective systems, such as IDSs and firewalls?
8. What s a *honeypot*? In general terms, what is the purpose of a honeypot?
9. Review Snort at `https://www.snort.org/`. Describe the feature that you think is most significant.
10. What are some of the locations for NIDS sensors?