ITBU 443: Threats and Counter Measures, Homework 07

Chapter 07, *Computer Security, Principles and Practices*

Readings

Read chapter 07 in the *Computer Security, Principles and Practices* book.

Discussion Questions

Answer the discussion questions in writing.

1. What is a *denial of service* attack?

2. What are some of the computing resources that a DoS attack impairs?

3. How does a "classic" DoS attack occur?

4. Describe the TCP *three way handshake*. Why does TCP use this method?

5. What is the ICMP protocol used for? What common command is used for ICMP? How would you implement this kind of flooding attack? (Note: I an asking you to write some very simple pseudo-code.)

6. What is a *distributed denial of service* attack? How does it differ from a DoS attack?

7. How does a *reflection attach* work? Be specific.

8. How does an *amplification attach* work? Be specific.

9. List several methods an administrator could use to minimize a DoS attack. What additional methods would minimize a DDoS.

10. What is the origin of the term *slashdotted*? You may be interested in reading `https://slashdot.org/`. I have made a habit of looking through it on a daily basis.