**Homework #5**

**CECS 378 – Spring 2021 Cappel**

**Due:** Wednesday, April 7th prior to class (11:59 PM)

**Homework #5 is focused on Chapter 6 and Chapter 7. There are 10 total questions all worth 10 points each (100 pts total).**

**Chapter 6 – Malicious Software**

1. What are three broad mechanisms that malware can use to propagate?
2. What are four broad categories of payloads that malware may carry?
3. What are typical phases of operation of a virus or worm?
4. Describe some malware countermeasure elements.
5. Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms discussed in this chapter could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?

**Chapter 7 – Denial-of-Service Attacks**

1. Define a *denial-of-service (DoS) attack*.
2. Define a *distributed denial-of-service (DDoS) attack*.
3. List three common *flooding attacks* and describe each.
4. Define a *reflection attack* as well as an *amplification attack*.
5. In order to implement the classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Consider an attack using ICMP echo request (ping) packets that are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker send to flood a target organization using a 0.5-Mbps link? How many per second if the attacker uses a 2-Mbps link? Or a 10-Mbps link?