**Homework #6**

**CECS 378 – Spring 2021 Cappel**

**Due:** Wednesday, April 21th prior to class (11:59 PM)

**Homework #6 is focused on Chapter 8 and Chapter 9. There are 10 total questions all worth 10 points each (100 pts total).**

**Chapter 8 – Intrusion Detection**

1. List and briefly define four classes of intruders.
2. What are three benefits that can be provided by an IDS?
3. What is the difference between signature detection and rule-based heuristic identification?
4. Describe the types of sensors that can be used in a NIDS.
5. What is a honeypot?

**Chapter 9 – Firewalls and Intrusion Prevention Systems**

1. List four characteristics used by firewalls to control access and enforce a security policy.
2. What is the difference between a packet filtering firewall and a stateful inspection firewall?
3. What is a DMZ network and what types of systems would you expect to find on such networks?
4. How can an IPS attempt to block malicious activity?
5. Explain the strengths & weaknesses of each of the following firewall deployment scenarios in defending servers, desktop machines, & laptops against network threats.
6. A firewall at the network perimeter.
7. Firewalls on every end host machine.
8. A network perimeter firewall and firewalls on every end host machine