CIS4367.01 **Brandon Thompson**
Prof. Elibol Due Date: 3/30/20

Homework 13

PROBLEM #1:

List 7 questions, or things you don't know about keeping a computer system secure from malicious software. For each question you list, indicate why it might be important to know the answer.

SOLUTION:

- How does malicious software get onto a system.
  Knowing how malicious software gets on a system is pertinent to protecting the system.
- What should you do immediately after a system is compromised?
  This is important to reduce the spread of the infection and protect other devices on the network.
- How do you setup a firewall? Firewalls are important parts of defending a computer system from network bound attacks, the setup of the firewall is critical to the effectiveness of the firewall.
- If my data was encrypted by ransomware, what steps should I take to get my data back?
  Instead of paying the ransom to get data back, what other methods are there?
- How do you determine if a website is safe to browse or not?
  A majority of attacks can be mitigated by knowing safe browsing techniques.
- How do you detect malicious software on a computer system and what it will do to the system?
  Knowing what the side effects of malware are is important to mitigating the effects of a malicious software.
- What is the best Anti-virus available?
  The internet offers many different options for anti-virus but some are better than others.

PROBLEM #2:

Write a one paragraph objective summary of the main ideas in this chapter (6).

SOLUTION:

Malicious software is one of the most significant categories of threats to computer systems. Malware is a program that is inserted into a system with the intent of compromising confidentiality, integrity, or availability. There are many types of malicious programs, defined by their infection mechanism, triggers, and payloads. Malicious software tries to bypass the system security by changing the signature of the code. Anti-virus software tries to find malicious software either by the signature of the code or by flagging unauthorized actions.