CIS4367 **Brandon Thompson**
Prof. Elibol Due Date: 4/16/2020

Homework 19

PROBLEM #1:

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

SOLUTION:

1. How do you segment a network to keep certain traffic from reaching specific areas.

   Segmenting the network is crucial to stopping the spread of malicious code or denying access to a portion of the network from an attacker.

2. What are VLANs and how do they work?

   VLANs are used very often in large networks.

3. How do you configure a firewall?

   Without proper firewall configuration, they are not a worthwhile investment.

4. Is intrusion detection necessary on a home PC?

   Home PCs store a lot of personal data, is a higher level of defense necessary for them?

5. Do wireless networks have different security risks than wired networks?

   Wireless networks are very common, knowing the differences in the security issues is paramount to defending them.

6. If I notice my system is compromised what is the best way to assess and mitigate the damage that can be done?

   How do you monitor changes in an infected system to know what type of information the attacker is trying to retrieve.

7. How do you configure an IDS?

   Intrusion detection systems need proper configuration to be of optimal use.

PROBLEM #2:

Prepare a one-paragraph objective summary of the main ideas in this chapter (Chapter 8).

SOLUTION:

This chapter focuses on intrusion detection, how do you determine when a unwanted user id trespassing in the network. This could be in the form of an unauthorized logon, elevated privileges or unauthorized actions. Intruders have different levels of skill, from 'Apprentice' to 'Master' that determines the technical skill of the attacker and how difficult it will be to defend against. Most attacks follow a basic methodology of: gather information, initial access, privilege escalation, gather information, maintain access, cover tracks. Intrusion detection systems will try to stop this from happening by matching patterns of authorized users against the attackers behavior. If attackers are not careful, they could get trapped in a 'honeypot' that will divert them from critical systems and collect information about their activity. Administrators can monitor suspicious activity through the IDS rules to look for specific, unauthorized actions.