Bailey Metz

Csilla Farkas

CSCE 522

30 August 2018

Question 1: **Distinguish between vulnerability, threat, and control.**

Vulnerabilities are weaknesses in a security system that are open to exploits or unnecessary access by a known or unknown source in order to cause loss or harm.   
  
Threats are sets of circumstances that have the potential to cause loss or harm.

Control removes vulnerabilities and makes systems safe and secure from the possibility of threats and exploits.

*“A threat is blocked by control of a vulnerability”*

Question 4**: List at least three kinds of damage a company could suffer  
when the integrity of a program or company data is compromised.**

A company can suffer financially when attackers steal financial information for personal gain. A company could also suffer from shame and embarrassment if private or personal information is suddenly displayed publicly. An example of this could be a board member of a CEO having an affair with another company employee. Finally, a company or organization could suffer fatalities if the private information falls into the wrong hands. For example, if a country’s military information is somehow leaked to an enemy, this could lead to that enemy’s military forces planning an unfair attack to assassinate their enemies.

Question 9**: On your personal computer, who can install programs? Who can change operating system data? Who can replace portions of the operating system? Can any of these actions be performed remotely?**

On my computer, only users with administrative access can install/uninstall programs. Only users with root access can change operating system data or replace portions of the operating system. This is a very difficult thing to do remotely, but can be done so. It is possible to access a computer remotely through secure shell (SSH) or other various programs (but these require the user to enter their authorization credentials or click on a certain link unless the attacker has already acquired these credentials [typically a username and password]). By the same token, an attacker could gain access to a computer remotely using various techniques such as vishing, phishing, malware, ransomware, etc. In these circumstances, an attacker can usually gain complete access to a computer from a remote location.