CP1402/CP5631 – Network Risk Management

1. Explain the term “social engineering”. Have you ever experienced it? What happened?
   Social engineering is a strategy to gain a user’s password

   Common types of social engineering:

   a. Phishing
   b. Baiting
   c. Quid pro quo
   d. Tailgating
   e. Piggybacking
   f. Shoulder surfing

   One of my close friends has experienced someone getting her bank account password over the phone. I am not sure it was social engineering. She was applying a credit card at China CITIC bank online. After several minutes, she got a phone call from someone. A man in the call claimed that the call came from China CITIC bank, and requested her bank account password to finish the credit card application. My friend provided password without considering a lot. After 10 minutes, she thought it is very strange and log in her account to check balance. She found all her money was gone. it is about 30000 SGD.

2. What are Denial of Service (DoS) and Distributed DoS attacks? Are these serious attacks? Explain your answer.

   A DoS (denial-of-service) attack occurs when an intruder issues a flood of broadcast ping messages preventing legitimate users from accessing normal network resources.
   There are several DoS subtypes:
   - Distributed DoS (DDoS) attack – are orchestrated through several sources, called zombies
   - DRDoS (distributed reflection DoS) attack – a DDoS attack is a type of DDoS attack that is bounced off uninfected computers, called reflectors, before being directed at target

   Some are serious attacks. PDoS attack damages a device’s firmware beyond repair

   Some are not serious attacks. Friendly DoS attack – an unintentional DoS attack has no malicious intent

3. What is the different between virus and worm?

Virus – a program that replicates itself with the intent to infect more computers
Worm – a programs that runs independently and travels between computers and across networks

4. Explain Ransomware.

   Ransomware – a program that locks a user's data or computer system until a ransom is paid.

5. Explain how Pen (penetration) testing works.

   Pen (penetration) testing uses variable tools to find network vulnerabilities and attempts to exploit them

6. Device hardening refers to
   steps to secure a device from network- or software-supported attacks

7. What are the symptoms of malware? Explain

   Malware is a generalised term that refers to many kinds of malicious software.

   - Virus – a program that replicates itself with the intent to infect more computers
   - Trojan horse (Trojan) – a program that disguises itself as something useful, but actually harms your system
   - Worm – a programs that runs independently and travels between computers and across networks
   - Bot – a program that runs automatically without requiring a person to start or stop it
   - Ransomware – a program that locks a user's data or computer system until a ransom is paid

8. What are your thoughts on Bring Your Own Device (BYOD) practice? E.g., do you think it is a safe practice? explain your answer.
   BYOD (bring your own device) allows people to bring their smartphones, laptops, or other technology into a facility for the purpose of performing work or school responsibilities

   It is not a safe practice.
   A BYOD model offers convenience and flexibility, but it also creates security concerns. The following is risk.

   - Data theft. If you let your employees use their own devices unchecked, it's likely that some of the personal applications they use may not be as stringent with their security requirements. If an account they have for personal use is hacked, it could ultimately end up exposing corporate data and confidential information.

- Malware. Employees use personal devices to download various types of information and files, such as PDFs and applications. If an employee isn’t carefully distinguishing between valuable corporate data and data used for personal purposes, this could compromise security.

Task: Check Final exam sample questions file in the “Assessments” folder out. If time allowed, do them during the prac and if you have any questions, discuss them with your tutor. Note that your tutor cannot provide you with the solutions, they can only discuss with you regarding your questions.