BITS3353 NETWORK SECURITY ADMINISTRATION AND MANAGEMENT:
LAB WEEK 1

NAME: Muhammad Izham Bin Norhamadi
MATRIX NO: B032020039

Overview of Network Security Administration and Management
Instructions:
1. Solve the below given question after watching the given YouTube Video's URLs below. The answer may in this videos.
2. Submit your answer via ULearn before 6pm (16/10/2020)

URL's:
Defences Against Attacks
https://www.youtube.com/watch?v=nXFgPGOPgaM
INFORMATION SYSTEM - COMPUTER SECURITY
https://www.youtube.com/watch?v=UJEwjGB1lk0
The "C.I.A." security concepts.
https://www.youtube.com/watch?v=432IHWNMqJE
Intro to Computer security
https://www.youtube.com/watch?v=ni-ByB4XGmI
Computer Security Terminology
https://www.youtube.com/watch?v=hWIgXS9utLM

1. Define Information Security as well as highlight TWO(2) benefit of it to the user.
   - The state of being protected against unauthorized use of information, especially electronic data, or the measures taken to achieve this.

2. Explain on CIA and why we need to more concern on CIA.
   - CIA stands for Confidentility, Integrity, and Availability. The CIA triad is vital to information security since it enhances security posture, helps organizations stay compliant with complex regulations and ensures business continuity. In terms of our daily life, CIA protects our sensitive and private information sent online from unauthorized access.

   Tips: Give the definition and highlight the importance of CIA in our daily life.

3. List FIVE(5) computer security terminology and explain on ALL of it.
   - Asset
     Assets are items of value such as property and equipment in which an organization or company owns in order to operate. On the other hand digital asset is any data, device or other component of an organization's systems that is valuable often because it contains sensitive data or required for the organization to operate.

   - Threat
     Threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information.

   - Vulnerability
     Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

- Exploit
  An exploit is a program, or piece of code designed to find and take advantage of security flaw or vulnerability in an application or computer system, typically for malicious purposes.

- Risk
  Risk is anything on the computer that may damage, steal data, or allow someone else to access the computer without consent or knowledge, resulting in loss or exposure of data.

4. Define firewall as well as highlight TWO(2) benefit of it to the user.
Firewall is a network security device that monitors incoming and outgoing traffic and decides whether to allow or block specific traffic based on defined set of security rules.

Benefits to the user:-

1- Acting as a defence from malicious network activity by isolating individual network endpoints from one another.
2- Allows user to monitor and control specific network behaviour of individuals applications on the system.

5. Incase you get attacked by CyberAttacker. What steps might be taken to defense against attacks?

1- Identify the type of the attack, threats, vulnerabilities and damage on the system
2- Scan the system for any malware with antivirus software and remove them
3- Recover and move sensitive data to another drive storage
4- Strengthen security by keeping softwares up-to-date, limiting network traffic for applications and formatting drives.