0204677 Lim Zhe Yuan **DCS22104 Fundamentals of Security in Ethical Hacking**

Section A

1.

	Non-malicious programs	**Malicious programs**
Harmless	Spreadsheet, Text editor	Trojan, Spyware
Catastrophic/ Harmful	Video call application, Internet relay chat (IRC)	Worm, Ransomware

2. Data
3. CIA requirements:
   C – Confidentiality: Company information and assets can only allow authorized personnel to access.
   I - Integrity: Company data should be able to be manipulated to ensure the authenticity of data.
   A - Availability: Company information should be accessible and usable at all times
4. -Port numbers
   -Service names
   -Service states
   -Operating system information
   -Network routes

Section B

1. - Insiders have more knowledge of the inner workings of an organization than outsiders. This allows attackers to plan their attacks in advance so that they can bypass the security defence set by an organization through extortion of an insider.
   - Insiders have the privilege to access company assets that cannot be accessed by outsiders without any limitation. This allow attackers to borrow an insider's identity to perform the attack in an area that they are normally unauthorized to be in.
   - Insiders holds more company secrets than outsiders. This allows attackers to hold the information as hostage and convince organizations to do anything that they say.

2. Hazard analysis refers to the observation and monitoring of system states based on design constraints. In a hazard analysis, both black box and white box testing is used to test the input handling, validation capabilities, and exception handling of a system. Black box testing refers to a testing method that uses human logical values as input, while black box testing refers to a testing method that uses actual data values to compare the actual outcomes with human-expected outcomes. Normally, tools such as debuggers aid in this process, such as JTest for Java applications, Mocha for JavaScript applications, C++ Unit Testing Framework for C++ applications and PHPUnit for PHP applications. Flow controls are also part of a hazard analysis. They ensure that data, exceptions, page redirections are sanitized properly before being processed and executed for the user. Storage of data in volatile and non-volatile memory is also managed so that data are stored properly and does not leak out during runtime.

3. -Malwares are malicious software that contains an executable file
   -Malwares can spread anywhere where sharing occurs

-Malwares are able to modify hidden and read-only files

4. -System settings and configurations may be reset. Users might be confused and have difficulties using the system if they notice the system settings are not what they personalized as.
   -System data may be deleted unexpectedly. Data that holds some importance to users may be wiped off and become irreversible, making users lose work that they put time and effort in.

Section C

1. use auxiliary/scanner/ssh/ssh_version
   set RHOSTS 192.168.3.34
   set THREADS 255
   set TIMEOUT 60
   show options
   service ssh status

2. Social engineering attack is a method of attack that takes advantage of weaknesses in human psychological traits.
3. -Voice phishing. This attack uses voice with a convincing tone to trick and manipulate victims into doing what they want.
   -Photography. This attack captures and records photos and images of a victim's computer or victim's background without their consent and permission.
   -Videography. This attack captures and records videos of a victim's computer or victim's background without their consent and permission.
   -Space and time invasion. This attack is a method where the victim is distracted by an attacker using either aspects of location or time, so that the attacker or their helper may have a window of opportunity to perform the attack without the victim knowing it.

Section D

1. -Learn from the security breach incident. This is done to enforce security defenses and prevent similar security breaches from happening in the future.
   -Analyze the severity of the damage caused by the breach. This is done to reconsider about whether to continue using the damaged infrastructure or replace it with a new one.
   -Setup a network logger. This is done to monitor network traffic in case of future attacks from the attacker.
   -Perform software patches. This is done to fix up any security loopholes in a software.
   -Report to local authority or Interpol about the security breach. This is done to enlist more capable individuals to investigate the security breach.
2. -One-Time Password (OTP). It is an authentication method that is generated for a short period of time before expiring.
   -Synchronous Token. It is an authentication token where a timestamp is embedded within the token for comparison between the current date and time.

-Continuous Authentication. It is an authentication method where users are prompted continuously to verify their legitimacy during a session.
-Challenge Response Authentication. It is an authentication method where a set of questions are provided for users to give answers to, such as a CAPTCHA.
-Response Generating Authentication. It is an authentication method that contains interactive features, such as image selections, puzzle solving, voice identification, or many more.