**ITCS318**
**MIDTERM SUMMATIVE EXAM PRACTICE**
**By Avin Nicolo R. Robles**

**TEST I. IDENTIFICATION**
**Instruction: Provide the correct answer.**

1.) Group of criminals that break into computers or networks to gain access for various reasons.

2.) Hired by Organizations, these hackers break into the networks or computer systems to discover weaknesses in order to improve the security of these systems.

3.) These attackers may find a vulnerability and report it to the owners of the system if that action coincides with their agenda.

4.) These attackers are unethical criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks.

5.) One of the most famous hackers in the world. He is known for his expertise in social engineering and hacking, which he used to gain unauthorized access to computer systems and networks.

6.) The most infamous Philippine hacker, created the ILOVEYOU virus, a malware that copied itself to all addresses in a computer's Windows-based email service, in 2000. The virus spread worldwide and caused billions in damages

7.) The creator of Linux. He is an Open-Source Software Pioneer.

8.) Teenagers or hobbyists mostly limited to pranks and vandalism, have little or no skill, often using existing tools or instructions found on the Internet to launch attacks.

9.) Grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.

10.) Grey hat hackers who rally and protest against different political and social ideas. Hacktivists publicly protest against organizations or governments by posting articles, videos, leaking sensitive information, and performing distributed denial of service (DDoS) attacks.

11.) These are black hat hackers who are either self-employed or working for large cybercrime organizations. Each year, cyber criminals are responsible for stealing billions of dollars from consumers and businesses.

12.) Depending on a person’s perspective, these are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking

13.) These specialists possess the insight to recognize the influence of data and harness that power to build great organizations, provide services and protect people from cyberattacks.

14.) It is the possibility that a harmful event, such as an attack, will occur.

15.) It is a weakness that makes a target susceptible to an attack.

16.) Used by criminals, these tools work by monitoring and recording all information coming across a network.

17.) It interferes with an established network communication by constructing packets to appear as if they are part of a communication.

18.) Also known as the Data Privacy Act of 2012 (DPA), aims to protect personal data in information and communications systems both in the government and the private sector.

19.) An entry-level certification that requires 2 years' experience working in network security.

20.) This role aims to protect an organization's information assets. It is entire set of components necessary to use information as a resource in the organization

21.) It is a three-dimensional security model which has now become a standard security model for many of the currently operating information systems. This comprises one dimension

22.) This measures the value of information.

23.) The characteristic of information whereby only those with sufficient privileges may access certain information.

24.) The quality or state of being whole, complete, and uncorrupted.

25.) The characteristic of information that enables user access to information in a required format, without interference or obstruction.

26.) An expansion where an information system possesses the characteristic of ID when it is able to recognize individual users.

27.) Occurs when a control proves that a user possesses the identity that he or she claims.

28.) Occurs after authentication. It assures that the user has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset.

29.) Information collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected.

30.) Exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process.

31.) Impossible to obtain perfect security—it is a process, not an absolute.

32.) No hard and fast rules nor many universally accepted complete solutions. No manual for implementing security through entire system.

33.) Dealing with technology designed to operate at high levels of performance. Specific conditions cause virtually all actions that occur in computer systems.

34.) An extension of the basic model discussed earlier in this chapter. These are activities necessary to support the design, creation, and implementation of information security strategies. An example of this is Incident Response Planning.

35.) The set of organizational guidelines that dictates certain behavior within the organization. A category of law is Enterprise information security policy (EISP).

36.) InfoSec operations that are specifically managed as separate entities.

37.) Executed through **risk management activities.** An example is Risk assessment and control.

38.) This area of InfoSec includes security personnel and the security of personnel, as well as aspects of a SETA program

39.) Identifying and controlling the resources applied to the project. Measuring progress. Adjusting the process as progress is made.

40.) German code machine during the 1930s that almost won the war by means of encrypting messages.

**TEST II. ESSAY**

**Instruction: Provide one (1) paragraph that proves your point.**

1.) What is your take regarding the difference between a Cyber Criminal and Cybersecurity Specialist?

2.) Explain the importance of Information Assurance and Security.

3.) Who truly owns your data?

4.) In regards to protecting the Organization, Will Your Future be in Cybersecurity?

5.) What is Information Security? Why is it important?

6.) Justify your answer: Should everyone have an access button?

7.) Justify your answer again: Should information be kept in a vault at all times?

8.) Explain this statement: What works for one company may fail in another.

9.) Explain: In the early 1990s, why was security treated as a low priority?

10.) Explain: **Information security is no longer the sole responsibility of a discrete group of people in the company.**