68

(Knowledge for Development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS

2021/2022 ACADEMIC YEAR

END OF SEMESTER EXAMINATION

YEAR THREE SEMESTER TWO EXAMINATION

FOR THE DEGREE OF BACHELORS OF SCIENCE (INFORMATION TECHNOLOGY)

COURSE CODE: BIT 325

COURSE TITLE: INFORMATION ASSURANCE AND SECURITY II

DATE: ~~31~~ 5th/08/ 2022 TIME: 2.00 P.M- 4.00 P.M

INSTRUCTIONS

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE (COMPULSORY) [30 MARKS]

a. Define Threat as used in information assurance and security. **[2 Marks]**

b. Give the difference between Bots and worms. **[4 Marks]**

c. Discuss Adware and Rootkits. **[4 Marks]**

d. State the distinction between Theft of intellectual property and Identity theft. **[4 Marks]**

e. Social Engineering is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer. Explain two ways to control social engineering. **[2 Marks]**

f. As an ICT security expert explain how Technology with weak security can be controlled

[2 Marks]

g. BYOD means bring your own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.briefly explain some of the security threats posed by BYOD.

[2 Marks]

h. Mobile malware is a type of software used specifically on mobile devices for malicious purposes Illustrate why mobile malware attacks are very likely to be one of the most pertinent cyber security threats. **[2 Marks]**

i. State and explain two hardware vulnerabilities and two firmware vulnerabilities [2 Marks].

j. Define Steganography as used in cryptography. **[2 Marks]**

k. Differentiate between Symmetric and Asymmetric encryption. **[2 Marks]**

l. Lack of focus on cyber security can damage your business in range of ways explain at least three impacts of cybercrime. **[2 Marks]**

QUESTION TWO [20 MARKS]

a. Define malware as used in information assurance and security. **[2 Marks]**

b. As cyber-attacks continue to become more and more sophisticated, attacks are likely to take place in newer digital spheres. In particular, we expect to see cybercriminals exploring ways to attack the 5G-to-WI-Fi handover. Explain. **[4 Marks]**

c. What is the difference between Network Security and Internet Security? **[2 Marks]**

d. Explain the following techniques of Steganography. **[6 Marks]**

i. Character marking

ii. Invisible ink

iii. Pin punctures

e. Passive attacks are of two types, state and explain. **[4 Marks]**

f. Define Cyber defense as used in information assurance and security **[2 Marks]**

QUESTION THREE [20 MARKS]

a. Discuss Malware on the basis of Infection Method and Malware on the basis of Action citing two examples on each. **[4 Marks]**

b. Explain why Internet of Things (IoT) Devices are Computer Security Threats to prepare for. **[4 Marks]**

c. One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security give some of the mechanisms used **[3 Marks]**

d. There are three simple steps you can take to increase security and reduce risk of cybercrime discuss these three simple steps. **[3 Marks]**

e. Cyber defense covers a wide range of activities that are essential in enabling your business to protect itself against attack and respond to a rapidly evolving threat landscape. Explain at least four of these activities. **[4 Marks]**

f. What is the function of Data loss prevention (DLP). **[2 Marks]**

QUESTION FOUR [20 MARKS]

a. Discuss Disruption, Distortion and Deterioration as Major Trends for Computer Security Threats. **[6 Marks]**

b. Explain how Deep fakes is produced. **[2 Marks]**

c. There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst, illustrate at least four types cryptanalytic attacks. **[2 Marks]**

d. With aid of a well labeled diagram explain the four general categories of attack under Security Attacks. **[8 Marks]**

e. What do you understand by the term Insider threats. **[2 Marks]**

QUESTION FIVE [20 MARKS]

a. Strengthening your cyber security means being proactive and staying one step ahead of cybercriminals. This starts with identifying which threats are most likely to impact companies explain Phishing Attacks and Cloud Jacking as Computer Security Threats to prepare for. **[4 Marks]**

b. To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. Explain the three aspects of information security to consider. **[3 Marks]**

c. Cryptographic systems are generally classified along 3 independent dimensions, discuss these independent dimensions. **[6 Marks]**

d. Active attacks involve some modification of the data stream or the creation of a false stream, these attacks can be classified in to four categories, explain these categories. **[4 Marks]**

e. Databases require best practices to secure the data within them, Illustrate the steps involved to ensure sensitive information stays protected. **[3 Marks]**