JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF INFORMATION SYSTEMS AND TECHNOLOGY

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF COMPUTER SECURITY & FORENSIC

3RD YEAR 2nd SEMESTER 2019/2020 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB1302

COURSE TITLE: ENTERPRISE SYSTEMS MANAGEMENT & SECURITY

EXAM VENUE: STREAM: BSC COMPUTER SECURITY & FORENSIC

DATE:1/12/20 **EXAM SESSION: 9-12 NOON**
TIME: 3 HRS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions.**
2. **Candidates are advised to write on the text editor provided, or to write on a foolscap, scan and upload alongside the question.**
3. **Candidates must ensure that they submit their work by clicking 'FINISH AND SUBMIT ATTEMPT' button at the end.**

QUESTION ONE (30 MKS)

a) Describe the significance of the following technologies as used in enterprise security

i) High-performance computing (2 mks)

ii)Information security (2 mks)

iii) Salting (2 mks)

iv) RAID (2 mks)

b) Describe any **FOUR** reasons for the deployment of Lightweight Directory Access Protocol (LDAP) directory. (4 mks)

c) Default Linux installations (un-patched and unsecured) have been vulnerable to a number of attacks.

i) Discuss any **FOUR** of these vulnerabilities. (4 mks)

ii) Discuss any **FOUR** remedies to the vulnerabilities in (i) above. (4 mks)

d) MD5 algorithm is prone to two main types of attack: dictionary attacks and rainbow tables. Explain how these attacks are carried out. (4 mks)

e) With growing use of internet and exponential growth in amount of data to be stored and processed (known as "big data"), the size of data centers has greatly increased. This, however, has resulted in significant increase in the power consumption of the data centers. In recent years, researchers have proposed several techniques for managing power consumption in data centers. Discuss **FOUR** of these techniques. (4 mks)

f) Explain why an organization may opt to invest in SAN technology. (2 mks)

QUESTION TWO (20 MKS)

a) The application of security policies for computer systems into mechanisms of access control is a vast and varied field within computer security. The fundamental goal of any access control mechanism is to provide a verifiable system for guaranteeing the protection of information from unauthorized and inappropriate access as outlined in one or more security policies. Describe the following access control models:

i) Mandatory Access Control (MAC) (3 mks)

ii) Discretionary Access Control (DAC) (3 mks)

iii) Role-Based Access Control (RBAC) (4 mks)

b) Briefly discuss the following algorithms:

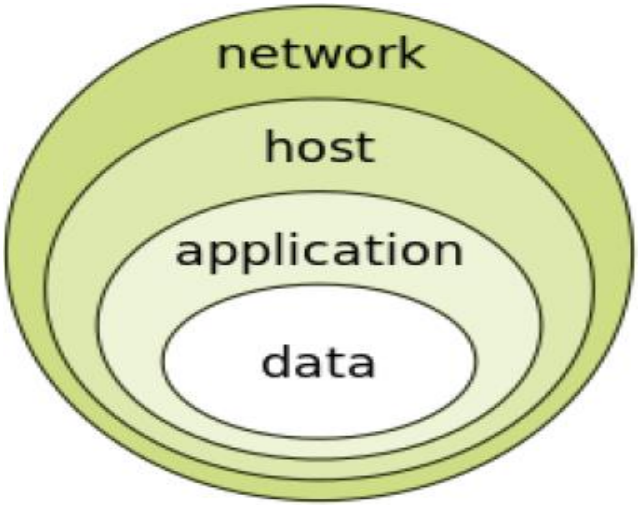
i) Blowfish (3 mks)

ii)MD5 (3 mks)

c) The World Wide Web is one of the most important ways for your organization to publish information, interact with Internet users, and establish an e-commerce business presence. However, if you are not rigorous in securely configuring and operating a public Web site, you leave yourself and your organization vulnerable to a variety of security problems. Discuss any **FOUR** ways of securing public web servers. (4 mks)

QUESTION THREE (20 MKS)

a) Study the diagram below carefully and use it to answer the questions that follow.



i) Describe the phenomenon depicted in the diagram above. (9 mks)

ii) Donn Parker defines the **SIX** main elements of the Information Security known as Parkerian hexad. These elements are employed to implement the dictates of the phenomenon in (i) above. Discuss these elements. (6mks)

b) Whereas DNS focuses on simplification by using workstation names instead of addresses, the Network Information Service (NIS) focuses on simplifying network administration by providing centralized control over a variety of network information. Briefly describe the NIS architecture. (5 mks)

QUESTION FOUR (20 MKS)

a) Controls are ways of protecting the information system attributes such as confidentiality, integrity and availability. Under ISO/IEC 27001:2005, 133 controls have been listed, which are cut down to 113 in ISO/IEC 27001:2013. Explain the following controls as applied in these specifications:

i) Administrative or procedural controls (4 mks)

ii) Logical controls (4 mks)

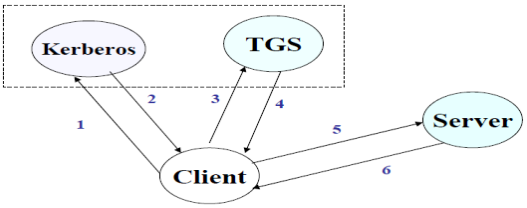
iii) Physical controls (4 mks)

b) ACL which stands for Access Control List, a list of permissions attached to an object that dictates who can access what and the level of this access, which is more commonly

known as authorization. Compare and contrast Windows and Linux operating systems in terms of ACLs. (8 mks)

QUESTION FIVE (20 MKS)

Consider the following authentication scheme.



i) Briefly describe the basics of this Kerberos authentication. (5 mks)

ii) Discuss the **THREE** phases of Kerberos authentication (6 mks)

iii) The three phases of authentication in (ii) are achieved via **TWO** authentication protocols. Explain the functionalities achieved by these protocols, indicating clearly the phase that each of these protocols operate in. (4 mks)

iv) Kerberos requires the workstations to be synchronized. Explain how this is implemented. (5 mks)