SPECIFY TYPE OF EXAMINATION

FIRST ATTEMPT □
FIRST RESIT □
SECOND RESIT □
RE-TAKE □

JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREES OF BACHELOR OF COMPUTER SECURITY AND FORENSICS

2ND YEAR 2ND SEMESTER 2022/2023 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1202

COURSE TITLE: COMPUTER AND NETWORK SECURITY

DATE: 18TH DECEMBER, 2022 **TIME: 9.00-11.00 NOON**

TIME: 2 HOURS

Instructions:

1. **This paper contains FIVE questions**
2. **Question one is compulsory**
3. **Answer any other two questions**

Question 1 (30 marks)

a) When securing the network, you are required to secure both the hardware as well as the software. Briefly highlight the three types of resources to consider when protecting hardware. (3 marks)

b) Network system administrators must be able to find ways to restrict access to the company network or sections of the network from both the "bad Internet" outside and from unscrupulous inside users. Such security mechanisms are based on a firewall.

   i) What are the two basic security functions? (2 marks)

   ii) The accept/deny policy used in firewalls is based on an organization's security policy. Briefly discuss the two commonly used firewall policies that are derived by consolidating the organization's security policies. (4 marks)

c) Briefly enumerate any THREE factors that have led to an increase in the security threats on computer systems. (3 marks)

d) Enumerate the THREE main motives behind a distributed denial-of-service attack. (3 marks)

e) List the THREE main subsects of hackers based on the hacking philosophies (3 marks)

f) Briefly mention TWO reasons why security policies are important in the security plan of a system. (2 marks)

g) In dealing with business information system disasters, the strategies involve quick and timely response to the disaster prevention system (DPS) signals with directed action. Highlight the two essential steps in disaster response. (2 marks)

h) List the three general forms that authentication can take. (3 marks)

i) Disaster planning is an ongoing process that never ends. This means that for your company to remain in business and remain competitive, the disaster recovery plan must be in place and must keep changing to meet the developing new technologies. Highlight the THREE aspects that you need to consider to ensure that the plan is always up-to-date. (3 marks)

j) The prime object of authorization is system security achieved through the controlled access to the system resources. Enumerate the TWO authorization principles that can be applied in ensuring that only authorized users can access resources. (2 marks)

Question 2 (20 marks)

a) Paul Brooke lists the FIVE steps necessary for a good authentication policy. Highlight these steps. (5 marks)

b) Enumerate THREE personal motives that may drive the actions of a hacker. (3 marks)

c) Explain clearly what the term "social engineering" means. (2 marks)

d) One of the system administrator's biggest problems, which can soon turn into a nightmare if it is not well handled, is controlling access of who gets in and out of the system and who uses what resources, when, and in what amounts. With the aid of a suitable diagram, briefly discuss the four elements of access control. (6 marks)

e) List the four essential components of a cryptographic system. (4 marks)

Question 3 (20 marks)

a) Generally, authentication requires the presentation of credentials or items of value to really prove the claim of who you are. The items of value or credential are based on four unique factors. Discuss the them. (8 marks)

b) List any two bodies or organizations behind the formulation, development, and maintenance of security standards at the international level and at the multinational level respectively. (4 marks)

c) Seasoned hackers plan their attacks well in advance, and their attacks do not affect unmarked members of the system. To get to this kind of precision, they usually use specific attack patterns of topologies. The attack pattern, the topology, is affected by the FOUR factors. Discuss them (8 marks)

Question 4 (20 marks)

a) Computer network security is made up of three principles: prevention, detection, and response. Intrusion detection is a technique of detecting unauthorized access to a computer system or a computer network while intrusion prevention is the art of preventing unauthorized access of a system's resources.
   i) Describe the steps in the system intrusion process. (6 marks)
   ii) Discuss the two preplanned defensive measures that must be included in an organization to ensure a good response to a system intrusion. (4 marks)

b) As Kruse puts it, when dealing with computer forensics, the only thing to be sure of is uncertainty. So the investigator should be prepared for difficulties in searching for bits of evidence data in a haystack. The evidence sought for usually falls into five categories. Discuss them. (10 marks)

Question 5 (20 marks)

a) Computer Gateway Interface (CGI) scripts are popular as they allow the web server to be dynamic and interactive with the client browser as the server receives and accepts user input and responds to them in a measured and relevant way to satisfy the user. However, CGI scripts present security problems to the cyberspace in several ways. Briefly discuss the five main ways that they present security problems. (10 marks)

b) Both the International Convention of Cyber Crimes and the European Convention on Cyber Crimes have outlined a comprehensive list of what constitutes cybercrimes. Enumerate any FOUR of these crimes (4 marks)

c) Briefly highlight the SIX factors that govern a quick disaster response. (6 marks)