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

3RD YEAR 1ST SEMESTER 2024/2025 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1202

COURSE TITLE: COMPUTER AND NETWORK SECURITY

DATE:16/4/2025 VENUE:CL 3 SESSION: 15.00-17.00

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)

Scenario: Global Tech Innovations (GTI)

Global Tech Innovations (GTI) is a multinational corporation with headquarters in the United States and regional offices in Europe, Asia, and Africa. GTI maintains a complex IT infrastructure that integrates on-premises data centers, cloud services, and remote offices via a global network. Recently, GTI suffered several cybersecurity incidents:

- A phishing campaign that resulted in unauthorized access to sensitive corporate data.
- Exploitation of vulnerabilities in a legacy web application that led to a data breach.
- A ransomware attack that temporarily disrupted business operations.

Additionally, GTI employs scripting to automate routine network administration tasks; however, some of these scripts are outdated and may harbor vulnerabilities. In response, GTI's security team is tasked with reviewing the company's network fundamentals, security policies, threat landscape, vulnerability management, access control and authentication practices, firewall configurations, and disaster management plans. They must propose a comprehensive strategy to strengthen the overall security posture. As a member of the security team, consider the following issues and address them comprehensively.

a) Identify and briefly describe the four fundamental components required for effective communication in a computer network. (4 marks)
b) Briefly compare centralized and distributed network models. (2 marks)
c) Based on GTI's global operations, discuss which network model (centralized, distributed or hybrid) would best suit the organization and justify your choice. (2 marks)
d) Identify and analyze two key vulnerabilities that might have been exploited during the phishing and web application breach at GTI. (4 marks)
e) Identify three possible attacker types behind the recent cybersecurity incidents at GTI and briefly discuss possible motives for each attacker type. (3 marks)
f) Considering the security incidents that have occurred at GTI, briefly discuss the likely objective(s) for each of the attacks. (3 marks)
g) Examine the role of scripting in GTI's network automation. Identify two security risks associated with outdated or insecure scripts and propose measures to mitigate these risks. (4 marks)
h) Propose two configuration strategies that could enhance the company's network security and explain how they would improve protection. (4 marks)
i) It is possible that GTI may be using traditional single-factor authentication (e.g., passwords) that are vulnerable to phishing and brute-force attacks.
    i) Recommend a better authentication system to possibly mitigate the observed risks and discuss briefly how it may be achieved. (2 mark)
    ii) Give a rationale for the recommendation above. (2 marks)

Question 2 (20 marks)

a) When securing the network, you are required to secure both the hardware as well as the software. Discuss the three types of resources to consider when protecting hardware. (6 marks)
b) Discuss two reasons why security policies are important in the security plan of a system. (4 marks)
c) 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)
d) Briefly discuss the four essential components of a cryptographic system. (4 marks)

Question 3 (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) 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)

Question 4 (20 marks)

a) 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) Discuss the two basic security functions of firewalls (4 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)
b) Whether the organization is doing an in-house design of its own firewall or buying it off the shelf, several issues must first be addressed. Discuss six of these issues. (12 marks)

Question 5 (20 marks)

a) 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)

b) Highlight briefly the five core steps to consider, as discussed by Jasma (2002), when constructing a viable, implementable and useful security policy. (5 marks)

c) Briefly enumerate any five factors that have led to an increase in the security threats on computer systems. (5 marks)