JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE INFORMATION TECHNOLOGY SECURITY& AUDIT

2ND YEAR 1st SEMESTER 2024/2025 ACADEMIC YEAR

KISUMU CAMPUS

MAIN PAPER

COURSE CODE: ICM 1107

COURSE TITLE: FIREWALL FUNDAMENTALS

EXAM VENUE: **STREAM:**

DATE: **EXAM SESSION:**

TIME: 3.00 HOURS

INSTRUCTIONS:

1. **Answer ANY three questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION ONE (20 MARKS)

a) Your company is deciding between implementing an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS). What key difference would you highlight to help them make an informed decision? **(2 marks)**

b) You're setting up a firewall for a medium-sized company. Explain how you would implement and utilize logging, and why it's crucial for the organization's security. Provide at least three specific benefits of proper logging in this context. **(6marks)**

c) As a Network security consultant, you're recommending the implementation of a honeypot to a client. Describe four specific ways this honeypot would enhance their network security, using real-world examples. **(4marks)**

d) A colleague believes that installing a firewall will solve all of the company's security issues. Explain three important security functions that a typical firewall cannot perform, and suggest alternative solutions for each.

(6marks)

e) You're creating a security awareness training for non-technical staff. How would you explain the difference between a worm and a virus in a way that highlights their distinct behaviors and potential impacts on the organization? **(2marks)**

QUESTION TWO (20 MARKS)

a) You've been tasked with improving security for a company that has both on-premises and cloud-based infrastructure. Recommend three technical controls for the network environment and three for individual host systems. Justify each recommendation. **(6marks)**

b) You're required to configure a new firewall for your organization. What are the three main options for defining rules in the firewall policy? Provide a brief example of when each option might be most appropriate. **(6marks)**

c) Your manager is considering removing the company's firewall since they've just implemented a VPN solution. Explain why this would be a mistake, highlighting the continued importance of firewalls even with VPN usage.

(4marks)

QUESTION THREE (20 MARKS)

a) You're the IT security manager for a large corporation that's upgrading its firewall infrastructure. The CEO has asked you to justify the investment in a modern, modular firewall system. Prepare a brief explanation of six add-on modules or advanced functions that modern firewalls can perform beyond basic packet filtering. For each module or function, provide a specific example of how it would

enhance the company's security posture or operational efficiency.

(12marks)

b) A small but rapidly growing e-commerce startup has hired you as a security consultant to advise on securing their network setup. They're particularly concerned about insider threats and physical security risks. Propose two administrative and two physical control measures that would be most effective for their situation. For each measure, explain why it's important and how it addresses a specific risk the startup might face.

(6marks)

c) Many security experts advocate for a specific approach when handling firewall filters and rules. Identify this preferred approach and explain why it's considered best practice. How would you implement this approach in your organization's firewall configuration?

(2marks)

QUESTION FOUR (20 MARKS)

a. As an IT consultant, you've been hired to improve the network security of a mid-sized e-commerce company. They've asked you to recommend and explain the functions of five different network security devices that would enhance their overall security posture. For each device you recommend, provide a brief explanation of its primary function and how it would address a specific security concern for the e-commerce platform.

(10marks)

b. You're a cybersecurity consultant tasked with recommending a firewall solution for three different clients:

- A small business with basic network security needs
- A medium-sized company handling sensitive financial transactions
- A large enterprise with complex application requirements

For each client, recommend either a Packet-filtering firewall, Session layer firewall, or Application layer firewall. Justify your choice by explaining how the specific features of each firewall type align with the client's needs and potential security challenges. **(6 marks)**

c. You're conducting a security audit for a steel manufacturing company that believes their network is secure because they have "a firewall." To help them understand the full scope of firewall functionality, describe four critical functions that their firewall should be performing. For each function: Explain what the function does

(4marks)

QUESTION FIVE (20 MARKS)

a) your company – a small business company recently moved into a new building with Internet access but no DHCP service or budget to purchase a firewall to protect your network You have 100 computers and 10 servers, couple of printers and network devices to connect your LAN. Your task as network administrator is to implement a DHCP server, a firewall router but to your surprise you do not have access to the router or any money to spend on a dedicated appliance. So what are your options – of course you go the open source way. In this project you have discovered that you can use IPCop software-based firewall to protect your network. In your solution describe how best to accomplish this task

(10Marks)

b) You're a security specialist hired to secure network infrastructure for a medium enterprise company – you're tasked with installing a Universal Threat Management (UTM) appliance – however, the organization has limited funds for purchasing a commercial UTM. After doing your research on the web – you learned that you can use integrated Shorewall firewall, Squid proxy server and Dansguardian to accomplish the task. The company requires four network zones: LAN, DMZ, Wireless and of course the Internet. In your solution describe how best to accomplish this task.

(**10Marks)**