JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE IN HEALTH INFORMATICS

2ND YEAR 2ND SEMESTER 2017/ 2018 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE: IIT 5122

COURSE TITLE: FIREWALL FUNDAMENTALS

EXAM VENUE:

DATE: **STREAM: MSC IT SECURITY AND AUDIT**

TIME: 2 HOURS **EXAM SESSION:**

INSTRUCTIONS:

1. **Answer any three (3) 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) Explain the meaning of firewall as used in IT security and name at least two examples of commonly used firewalls in the industry. (4 marks)

b) The OSI network model is used to describe what tasks a protocol suite performs as you explore how data moves from the user interface of a transmitter down to the lowest layer and up the layer of the receiving device to the user interface.

Required:

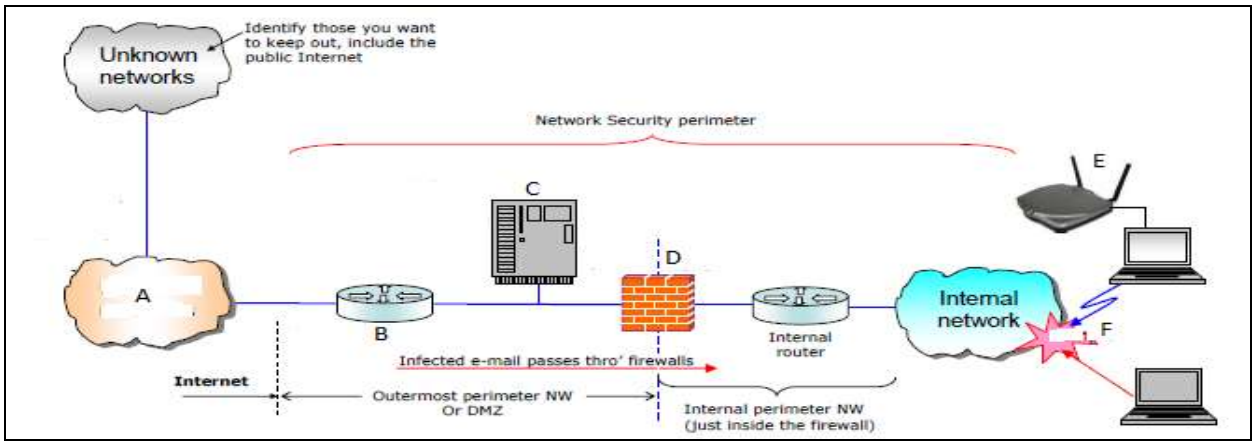
i. Draw and label all the layers of the OSI network model. (2 marks)
ii. Explain the role of each layer. (3.5 marks)
iii. State two protocols used in each layer (3.5 marks)

c) Explain how a deeper understanding of the OSI network model would help a network security administrator to effectively deploy a firewall on the LAN that is connected to the internet. (2 marks)

d) Discuss the five steps of data encapsulation in TCP/IP model. (5 marks)

QUESTION TWO (20 MARKS)

a) The figure below represents computer network of an organization. Study it carefully then answer the questions that follow.



Required:

i. State the parts labeled A, B, C, D, E and F. (6 marks)
ii. Explain at least two (2) roles of part B (4 marks)
iii. State any three network services that can be found in part C. (3 marks)
iv. Explain the problem at the part labeled F (2 marks)

v. Explain the probable cause of the problem in (iv) above (3 marks)
vi. Explain the main function of the part labeled D. (2 marks)

QUESTION THREE (20 MARKS)

a) A firewall's actions on traffic is usually determined by its policies, rules and filters.
Required
   i. Differentiate between firewall policy and firewall rule (4 marks)
   ii. Explain the three main actions a firewall can take on data traffic based on its rules. (6 marks)

b) When configuring a firewall to do its job, a filter defines some specific pattern for which a firewall seeks a match. Discuss the following types of filters. (4 marks)
   i. Exclusionary filter
   ii. Inclusionary filter

c) State the order in which you would apply these filters in the networks of the following types of organizations. Give sound security and experiential reasons for your answer. (6 marks)
   i. Public University
   ii. Commercial bank

QUESTION FOUR (20 MARKS)

a) The firewall of Lake International Research Centre- an NGO conducting VMMC and VCT services in Western Kenya Region was deployed ten years ago and since then, three newer versions have been released. Since the firewall has been very stable, the ICT Manager does not want to change it.
   i. Do you think he should install a different firewall? Give valid reasons for your answer. (3 marks)
   ii. In case he cannot buy a new version of the firewall, what advice can you give him to help improve the security of his network? (2 marks)

b) There are many threats in an organization that a firewall can prevent while there are others a firewall cannot prevent.
Required
   i. List any four logical threats a firewall can prevent. (2 marks)
   ii. List any four logical threats a firewall cannot prevent. (2 marks)

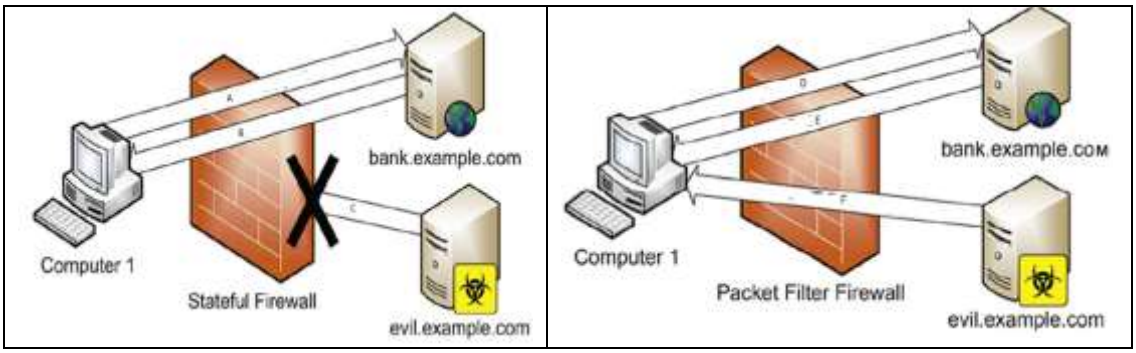
c) Discuss any three logical vulnerabilities that a firewall can be prone to, and how they can be controlled. (6 marks)

d) The understanding of sockets is very important in network security.
   i. Explain the meaning of network socket. (2 marks)
   ii. List the information that constitutes network socket. (3 marks)

QUESTION FIVE (20 MARKS)

a) Discus the following security protocols used in securing network communication and resources. For each protocol, state the port number it uses. (6 marks)
   i. VPN
   ii. HTTPS
   iii. SSH

b) The figures below represent security actions of a stateful inspection firewall and Packet filter firewall on a computer network. Study them carefully then answer the questions that follow.



Required:
   i. State and explain he activities labeled A, B, C, D, E and F. (3 marks)
   ii. Explain the difference between activity C and activity F, giving the technical reason behind this difference. (3 marks)

c) Discuss the following types of firewalls and describe the ideal circumstances under which each one of them may be deployed, considering the strengths and weaknesses of each. (8 marks)
   i. Packet-filtering Firewalls
   ii. Circuit-level firewalls
   iii. Application Gateway Firewalls
   iv. Proxy Servers