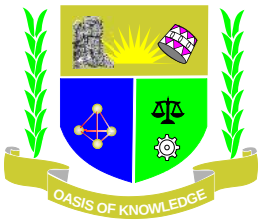

JARAMOGI OGINGA ODINGA UNIVERSITY

OF SCIENCE & TECHNOLOGY

UNIVERSITY EXAMINATIONS 2012/2013

1ST YEAR 2ND SEMESTER EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

(KISUMU L.CENTRE)

COURSE CODE: IIT 5122

COURSE TITLE: FIREWALL FUNDAMENTALS

DATE: 13/8/2013 **TIME: 2.00-5.00 PM**

DURATION: 3 HOURS

INSTRUCTIONS

1. **This paper consists of 5 Questions.**
2. **Answer Question 1 (Compulsory) and any other 2 questions.**
3. **Write your answers on the answer booklet provided.**

Question one 20marks

a) Name and explain **three** (3) types of firewalls 3mks
b) Name and explain **four** (4) functions of firewalls in a network. 4mks
c) Identify and explain **four** (4) limitations of firewalls. 4mks
d) Using diagrams, explain **three** (3) types of firewall architecture. 9mks

Question two 20marks

a) Name two distinct tables in Iptables. 2mks
b) Describe the differences in attacks bellow between Ipv4 and Ipv6.
c) In your own judgment (giving reasons) indicate the level of difficulty for the attack to succeed in Ipv4 vs Ipv6.
   i) Reconnaissance. 2mks
   ii) Unauthorized access. 2mks
   iii) Header manipulation and fragmentation. 2mks
   iv) Layer 3 and Layer 4 spoofing. 2mks
   v) Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) attacks. 2mks
   vi) Broadcast amplification attacks (smurf) 2mks
   vii) Routing attacks 2mks
   viii) Viruses and worms 2mks
   ix) Transition, translation, and tunneling mechanisms. 2mks

Question three 20marks

a) With an example, describe when it's best to perform firewall filter based on:-

i) IP addresses. 2mks
ii) Domain Names 2mks
iii) Protocols 2mks
iv) Ports 2mks
v) Specific words and phrases(sniff) 2mks

b) With an example, describe the weaknesses of filtering based on:-

i) IP addresses. 2mks

ii) Domain Names 2mks

iii) Protocols 2mks

iv) Ports 2mks

v) Specific words and phrases(sniff) 2mks

Question Four 20marks

You are the sole proprietor of an e-commerce start-up company.

You have an internal and an external emailing system, in addition to the web-servers that customers use to make orders online.

i) Name and give a brief explanation of **three** (3) firewall architectures. 3mks

ii) Of the **three** (3) firewall architectures that you have named above, which architecture will be best suited for your start-up company? Give a brief explanation 2mks

iii) Draw and label a diagram that represents your architecture of choice. 5mks.

iv) Name and explain **four** (4) firewall performance attributes 4mks

v) Name and explain **three** (3) firewall components that you would consider. 3mks

vi) Give **three** (3) importance of factoring in firewall performance attributes when shopping for a firewall for your start-up company. 3mks

Question Five 20marks

a) Name and explain the **three** (3) zones in a DMZ network. 3mks

b) Considering an e-commerce application similar to Question D above, draw and label **three** (3) zones in Question 1 above. 6 mks

c) Name and explain **five** (5) considerations to take into account as you determine the requirements for a firewall. 5 mks

d) Name and describe **five** (5) types of intrusion that firewalls can help prevent. 5mks

e) What is the advantage of a packet sniffer? 1mk