



**JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY SCHOOL OF
INFORMATICS AND INNOVATION SYSTEMS**

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE

COMPUTER SECURITY AND FORENSIC

2ND YEAR 2ND SEMESTER 2013/2014 ACADEMIC YEAR

MAIN

COURSE CODE: IIT 3227

COURSE TITLE: COMPUTER SYSTEMS AND NETWORKING LAB

EXAM VENUE: CL I

STREAM: (BSc. Computer Security and Forensic)

DATE: 17/04/14

EXAM SESSION: 9.00 – 11.00 AM

TIME: 2.00 HOURS

Instructions:

- 1. Answer question 1 (Compulsory) and ANY other 2 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 30 MARKS (COMPULSORY)

- a) i) Briefly define Intrusion detection systems (IDS) [2 Marks]
- ii) How are IDS different from firewalls? [3 Marks]
- iii) In a networking environment, is it possible to have both firewall and network intrusion detection systems (NIDS)? Depending on your answer briefly explain how you would configure your network given the two network security systems. [5 Marks]
- b) In planning and designing network security, access controls lists (ACLs) are one of the tools commonly used. Consider the IP address ranges for six subnets on network 130.10.0.0 in Fig. Q2. Design a single standard deny access list that will deny packets from subnets 4, 5 and 6. [6 Marks]

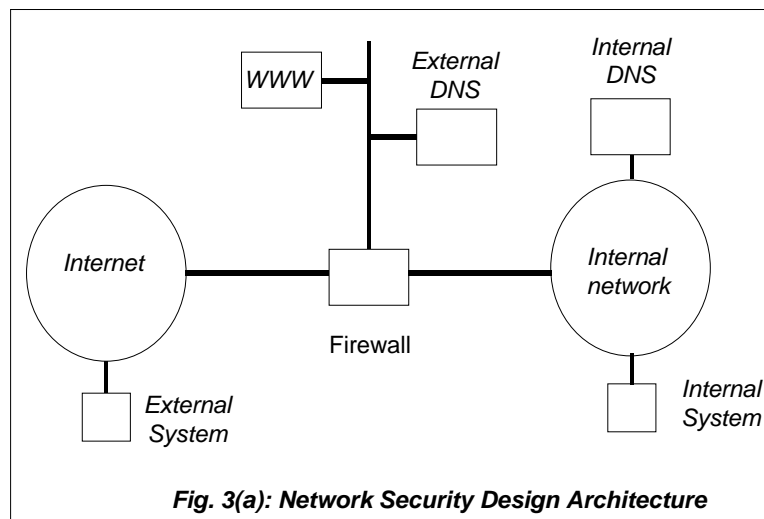
<i>Subnet number</i>	<i>Subnet address</i>
1	130.10.32.0
2	130.10.64.0
3	130.10.96.0
4	130.10.128.0
5	130.10.160.0
6	130.10.192.0

Fig. Q2. IP Address Ranges for Six Subnets on 130.10.0.0

- c) A Router, firewall and a switch acts as frontline gatekeepers in a network environment. Discuss each device's vulnerability and the recommended countermeasures. [9 Marks]

QUESTION TWO (20 MARKS)

- a) Fig. 3 below shows a sample, familiar network security design architecture (or small variations from it) that is in widespread use throughout the world for a variety of organizations. A Web Server (WWW) for sending static Web pages to potential customers and a DNS server are often located in a *DeMilitarized Zone* DMZ.
- i). Identify the function and importance of a DNS server. [4 Marks]
- ii). Briefly discuss why a *Split DNS* arrangement is preferred here. [4 Marks]
- iii). Give your understanding of a Demilitarized Zone (DMZ). [2 Marks]



b) Define a network load balancer and explain its role in a network environment [3 Marks]

c) You are hired as network administrator; you realize that the organization has an exposed server that provides public access to a critical service, such as a web or email server. Briefly explain what you would do rectify or correct the position [4 Marks]

d) Briefly explain the functions of a proxy server in a network environment. [3 Marks]

QUESTION THREE (20 MARKS)

a) Differentiate the following: [9 Marks]

- i) VLAN and Subnetwork
- ii) DHCP and HTTP
- iii) VPN and SSL

b) Explain the concept of Network address translation (NAT) and identify its important security aspect. [4 Marks]

c) Most organizations deploy, at a minimum, two firewalls. Identify their placement and briefly explain each firewall's functions. [7 Marks]

QUESTION FOUR (20 MARKS)

a) Draw and explain a basic secure organizational network encompassing a router, firewall, proxy server, switch, VLANs [8 Marks]

b) Briefly explain how IPSEC and VPN can be implemented to connect an organization and its branches in different geographical locations. [7 Marks]

c) Identify and differentiate the two types of ACL [3 Marks]

d) Explain the operational principle of CSMA/CA [2 Marks]

QUESTION FIVE (20 MARKS)

- a) Explain using labeled diagrams how a Honeypot works. [4 Marks]
- b) Wireless networks suffer a number of limitations; state at least three of its limitations and briefly explain each. [6 Marks]
- c) Name the four major types of firewalls; identify their levels of operation within the OSI layer model. [4 Marks]
- d) Explain network security. What are the types of security features used in client server types of network? [6 Marks]