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 SECURITY AND AUDIT

(KISUMU L.CENTRE)

COURSE CODE: IIT 5123

COURSE TITLE: ADVANCED NETWORK SECURITY AND SECURE NETWORK COMMUNICATIONS

DATE: 14/8/2013 **TIME: 9.00-11.00 AM**

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.**

IIT5123	Advanced Network Security And Secure Network Communications	
Lecture Hrs	28	
Practical Hrs	14	
Course Objective	-Understand Network security concern -Learn about network first line of defense e.g routers, switches, firewall etc -Design a Secure network incorporating firewall, DMZ -Plan and Install Secure Network in the Lab or using network simulator (CISCO packet tracer) -Learn about advance security tools -Test and evaluate network for security weaknesses and network defense mechanism Learn how to configure switches, routers and firewalls using packet tracer	
Course Content	Advances in network environment security: firewalls, proxy servers, and other enterprise resources considerations for planning network connectivity and security. Planning and installing secure web servers, FTP server, Samba server, DNS server and messaging servers in a lab environment; implementing appropriate updates, bug fixes and patches to ensure network protection to the desired standards and best practices. Working with advance security tools: network scanning, web application penetration testing, log management, DLP, file integrity management etc. Test and evaluate network for security weaknesses and network defense mechanism using pen-test.	
Learning & Teaching Methodologies	Lectures, Tutorials, Lab sessions and presentations by students on specific tasks	
Instructional Materials/Equipments	Classroom and Computer Laboratory	
Course Assessment	Type	Weighting (%)
	Assignments	20
	Continuous Assessment	20
	Examination	60
	Total	100
Recommended Reading	1 Network + Guide to Network 5th Ed, 2006 Tamaran Dean 2 Network Protocols Handbook 2nd Ed, 2004 Javvin Technologies 3 http://wwwin.cisco.com/cpress/cc/td/cpress/design 4 Internet journal and publications (as appropriate)	

QUESTION ONE (20 MARKS)-COMPULSORY

a) While authentication, authorization, and encryption do not encompass all facets of information security management, they are the three main areas of concern. Briefly discuss each. 6 Marks

b) Discuss secure socket layer protocol (SSL) 4 Marks

c) Explain the 4 key steps you would undertake to ensure the security of any public Web server. 4 Marks

d) Identify 3 key factors an organizations planning for the development of a Web server should consider in order to address and implement security of the Web server. Briefly discuss each 6 Marks

QUESTION TWO (20 MARKS)

a) 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 than will deny packets from subnets 4, 5 and 6. **[5 Marks]**

Subnet number	*Subnet address*
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

b) 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 ***D***e***M***ilitarized ***Z***one 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

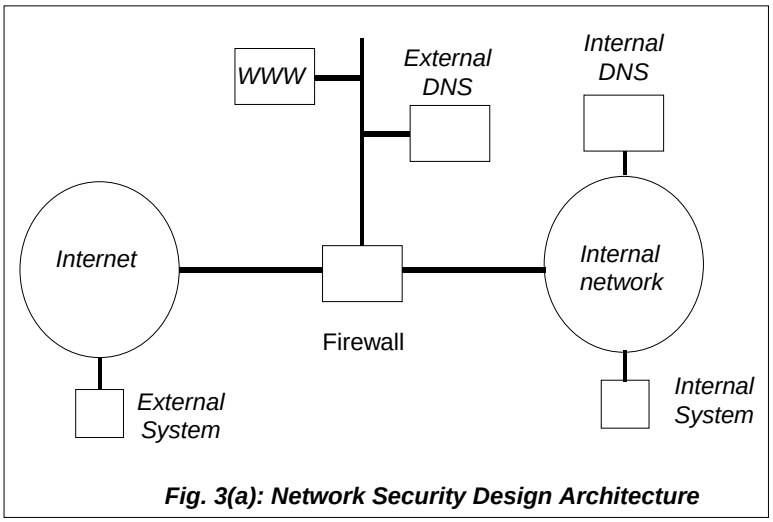

Fig. 3(a): Network Security Design Architecture

c) Organizations now need to be on constant guard against data being lost or stolen. According to KPMG's "Data Loss Barometer," in 2009 alone, more than 113.6 million people were affected by data loss. Discuss; consider the following: causes of data loss, cost of data loss, threat vectors and data loss prevention. 5 Marks

QUESTION THREE (20 MARKS)

a) There are several different types of security testing techniques/tools. Identify any three and briefly discuss each. 6 Marks

b) Discuss the four components of penetration testing. 6 Marks

c) What is a proxy firewall and how is it different from a network (or transparent) firewall? 4 Marks

d) Where would you place a web server in an organization assuming that you can use a network firewall and why? 4 Marks

QUESTION FOUR (20 MARKS)

a) A Router, firewall and a switch acts as frontline gatekeepers in a network environment. Discuss each device's vulnerability and the recommended countermeasures. 12 Marks

b) Discuss the following terms as they relate to data or network security: Confidentiality, Integrity and Availability. 8 Marks

QUESTION FIVE (20 MARKS)

a) In your organization, there are a number of services and applications. As an expert you are tasked to design and implement a scalable secure network. Give a diagrammatical representation of your design explaining the roles and functions of the network devices included in your design. The organization has the following services: E-mail server, Web, DNS servers, SQL servers, Intranet server, user workstations and File server. Your design should include firewall, routers and switches as appropriate. 20 Marks