JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTERS OF IT SECURITY & AUDIT

1ST YEAR 2nd SEMESTER 2018/2019 ACADEMIC YEAR

KISUMU LEARNING CENTER

COURSE CODE: IIT 5123

COURSE TITLE: ADVANCED NETWORK AND SECURE COMMUNICATION

EXAM VENUE: **STREAM: IT SECURITY & AUDIT**

DATE: **EXAM SESSION: 2 HOURS**

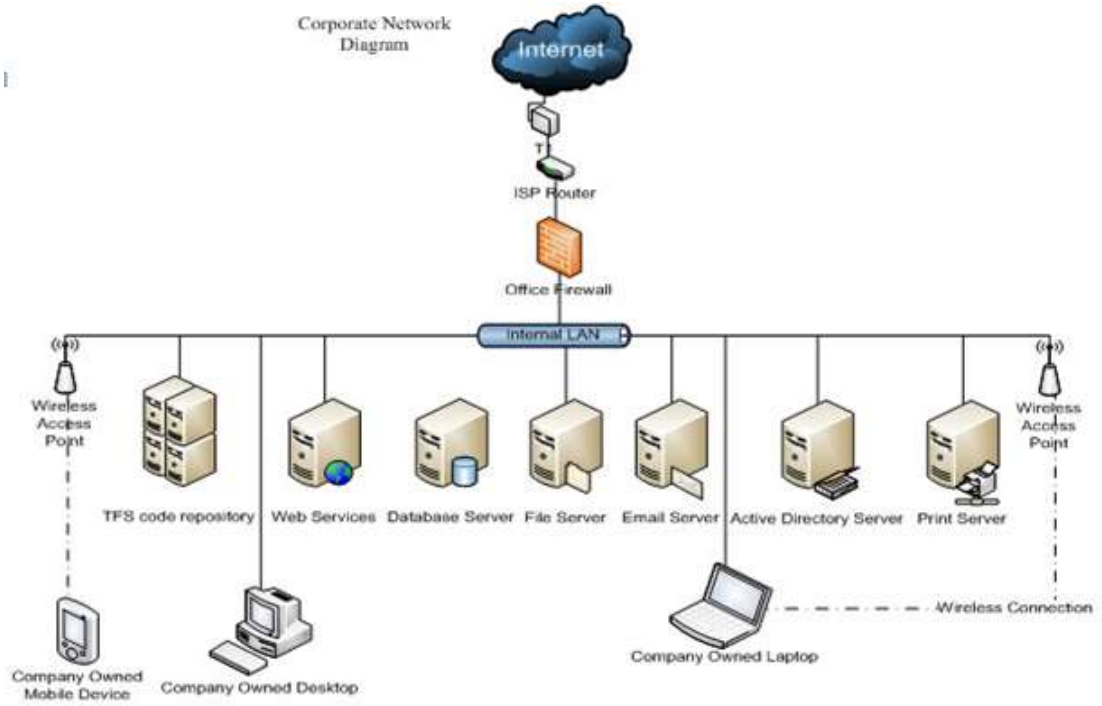
TIME:

INSTRUCTIONS

1. **Answer QUESTION ONE and ANY OTHER TWO 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 1 [20 marks] Case Study

KIS Technologies (KIS-Tech) is an organization that specializes in Web site and Web content design for all types of businesses. KIS-Tec's mission is to provide top KIS Technologies that will increase consumer generated revenue to KIS-Tec's customer Web sites. KIS-Tec's database contains over 250,000 proprietary images and graphical designs that will enhance most Website's appeal to a target demographic. KIS Technologies has several mission critical business processes. First is the use of the repository of Web site templates, custom written scripts and/or custom applications. This repository is stored in a Microsoft Visual Studio Team Foundation Service (TFS) server. This application is used to monitor the project development lifecycle of custom Visual Studio applications from inception to deployment, including the quality assurance testing phase. Other critical business processes are KIS-Tech's accounting, payroll and Marketing operations all of which are supported by IT assets. There are strict technology-based access controls associated with each of these systems to ensure that only authorized personnel can access them. Corporate and remote offices have the following services that are accessible for employees. From corporate owned computer or mobile device employees can access VPN, Outlook Web Access for email, or Active Sync for Exchange server. On any computer in the world employees can access Outlook Web Access for email. Customers are only allowed to access to the Corporate Web site. There is a published corporate security manual that covers the following security practices. Username standard including having a separate account for any elevated privileges. Password length, complexity, rotation and history requirements.



a) Using the preceding narrative and logical diagram above briefly discuss the problems this company might be experiencing based on your assessment. **(5 Marks)**

b) Draw a logical design of the improved network that is scalable considering opportunities for future growth. This network should address organization's security needs with the available resources. **(7marks)**

c) Identify and discuss the security measures you would add to this proposed network. Be specific on the type of security controls you would put in place to address threats in the network. Think in terms of network layer, layer 3, layer 2, within subnets, etc. **(8 marks)**

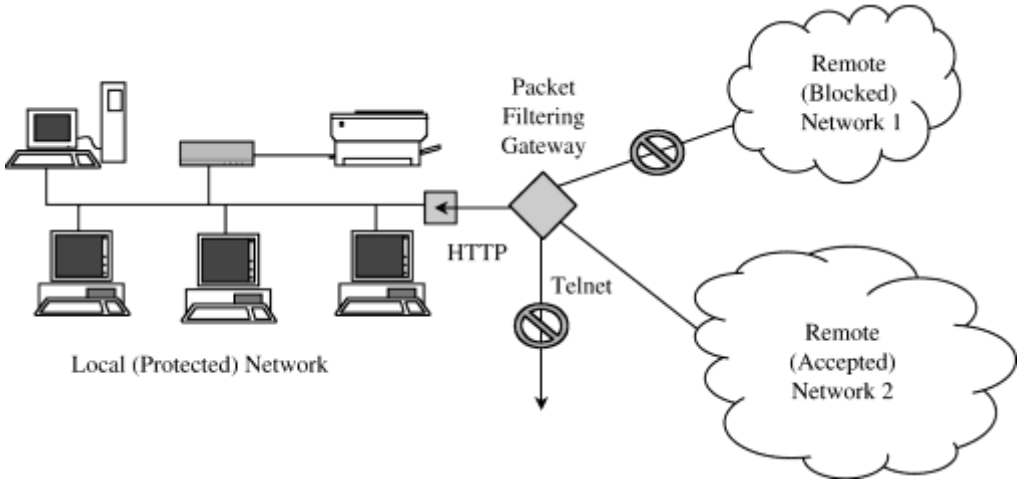
Question 2 [20 marks]

The cybersecurity landscape is changing rapidly, making current and actionable guidance on the latest trends more important than ever. You have been asked to conduct a survey on the company's cybersecurity landscape.

a) Discuss the key areas you may want to explore **(4 marks)**

b) Identify any 6 questions you would include in your survey. Justify the inclusion of each question in the survey **(6 marks)**

c) The figure below represents access control at the gateway. Explain how this takes place and identify the layer (TCP/IP model) where this occurs. **(5 marks)**



d) What any five functions can a professional code of conduct serve to fulfill? **(5 marks)**

Question 3 [20 marks]

a) The figure below represents a model for network security. This general model shows that there are four basic tasks in designing a particular security service. Identify and briefly discuss the four basic tasks that should be performed according to the diagram shown below. **(9 marks)**

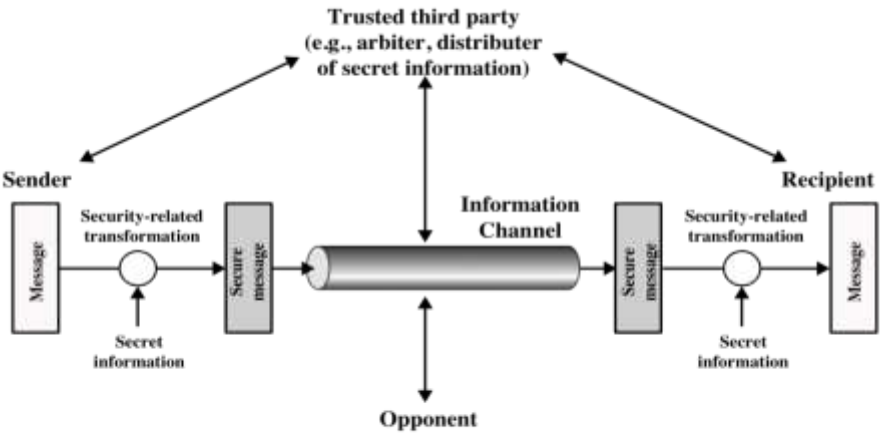


Figure 1.2 Model for Network Security

b) An enterprise can run a secure, private IP network by disallowing links to untrusted sites, encrypting packets that leave the premises and authenticating packets that enter the premises. By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security-ignorant applications.

i) IP-level security encompasses three functional areas: Discuss **(3 marks)**

ii) Identify any four services provided by IPSec **(4 marks)**

c) Identify any four services provided by IPSec **(4 marks)**

Question 4 [20 marks]

Many Universities offering degree programs in computer security in Kenya today are faced with challenges of limited resources, lack of skilled lecturers, limited time devoted to developing labs for teaching, limited administrative support due misunderstanding of the skill requirements and deliberate abuse of security tools in the labs. You have completed your master's degree in IT Security and Audit at JOOUST and have been offered a job as an assistant lecturer in the department of computer science and software engineering. You have been requested by the head of department to design an educational computer security lab to answer the challenges above. The lab should allow staff and students to analyze and study vulnerabilities of corporate network and firewall configuration. This lab should allow students and staff to study/assess latest computer security technologies and serve as a platform for security projects that would be difficult to implement in the current computer labs.

a) Identify the problem – You must define the problem in detail to justify your assessment.

(3 Marks)

b) Draw a logical design of the improved network that is scalable considering opportunities for growth. This network should address organization's security needs with the available resources. **(7 marks)**

c) Identify and discuss the security measures you would add to this proposed network. Be specific on the type of security controls you would put in place to address threats in the network. **(10 marks)**

Question 5 [20 marks]

Kenya's decentralization is among the most rapid and ambitious devolution according to the World Bank. Functions and funds have been transferred to the new counties. Significant power and resources have been devolved to the 47 counties. Security professionals now need to focus on establishing IT security situational awareness to improve the state of IT security across all the 47 counties. As a graduate of IT Security and Audit, you have been awarded a consultancy job to design and develop an assessment plan for security and privacy controls for the county governments. Your proposal must be supported with relevant ICT Authority standards and security guidelines. Your plan should articulate how to conduct security control assessments and privacy control assessments that support organizational/county/business risk management processes and should be aligned with the stated risk tolerance of these institutions.

a) Identify the problems **(5marks)**

b) Discuss the proposed security assessment plan – include any diagram or flow chart where applicable. **(15 marks)**