



THE MOMBASA POLYTECHNIC UNIVERSITY COLLEGE

(A Constituent College of JKUAT)

(A Centre of Excellence)

Faculty of Engineering & Technology

**DEPARTMENT OF COMPUTER SCIENCE & INFORMATION
TECHNOLOGY**

**UNIVERSITY EXAMINATION FOR:
BACHELOR OF TECHNOLOGY IN INFORMATION TECHNOLOGY
(BTech. IT 11M)**

EIT 4209: NETWORK SYSTEM ADMINISTRATION

END OF SEMESTER EXAMINATION

SERIES: DECEMBER 2012

TIME: 2 HOURS

Instructions to Candidates:

You should have the following for this examination

- *Answer Booklet*

This paper consist of **FIVE** questions

Answer question **ONE (COMPULSORY)** and any other **TWO** questions

Maximum marks for each part of a question are as shown

This paper consists of **THREE** printed pages

Question One (Compulsory)

a) Explain the following terms:

- (i) Network Analyser
- (ii) Active Directory
- (iii) System Administrator

(6 marks)

b) State any **FOUR** reasons why network administrators use network analysers.

(4 marks)

c) Explain the difference between the following terms:

- (i) "Client" and "Server"
- (ii) "Domain" and "Workgroup"

- (iii) “Firewall” and “Intrusion Detection System”
- (iv) “Administrator User Account” and “Guest User Account”
- (v) “File Transfer Protocol (FTP)” and “Hypertext Transfer Protocol (HTTP)” **(20 marks)**

Question Two

a) Administrative tools enable network administrators to add, search and change computer and network settings and active. Directories objects. Explain any **FIVE** such tools used in Microsoft server 2003/2008. **(10 marks)**

b) Consider the scenario and answer the question that follow:

You go to your main access switch, or border router, and configure one of the unused port mirroring. You plug in your laptop, fire up your network analyzer, and see thousands of User Datagram Protocol (UDP) packets destined for port 1434 with various apparently random, Internet Protocol (IP) addresses. You immediately apply access filters to block these packets from entering or existing your network until you do more investigating. A quick search on the Internet holds the answer. The date is December 13, 2012 and you have just been hit with the SQL slammer worm.

- (i) Explain the term “SQL Slammer worm” **(1 marks)**
- (ii) Explain the term “User Datagram Protocol” **(1 marks)**
- (iii) Explain any other **FOUR** methods that could be used to detect sniffers on the network. **(8 marks)**

Question Three

a) Working with groups instead of individual users helps simplify network maintenance and administration. Explain the following types of groups in Active Directory:

- (i) Security groups
- (ii) Distribution groups **(4 mars)**

b) Describe the following types of groups:

- (i) Global group
- (ii) Universal group
- (iii) Domain local groups **(6 marks)**

c) Describe any **FIVE** types of servers you are likely to find in large organizations, stating their functions. **(10 marks)**

Question Four

a) Explain the difference between the following terms:

- (i) “Risk” and “Penetration”
- (ii) “Threat” and “Penetration” **(8 marks)**

b) Every organization should monitor its systems for possible unauthorized intrusion and other attacks. This needs to be part of the daily routine of every organization’s IT unit, as it is essential to safeguarding a company’s information assets.

- (i) Identify any **FOUR** valuable information assets that any MPUC must safeguard. **(4 marks)**
- (ii) Explain the term “Intrusion” **(2 marks)**
- (iii) Explain the term “Attack” **(2 marks)**

c) State **FOUR** characteristics of a client-server system. **(4 marks)**

Question Five

- a) As our computing infrastructures have grown more network-centre and much of our lives revolve around networked computers. Attackers have devised very clever means for undermining computer communications. Therefore, various techniques exist for gaining access to computing resources using networked-based attacks. Critically discuss any **TWO** types of attacks, and recommend defenses against both attacks. **(4 marks)**
- b) State any **THREE** advantages and disadvantages of client-server system. **(6 marks)**
- c) Explain the difference between the following terms:
(i) “Desktop Operating System” and “Network Operating System”
(ii) “Local User Account” and “Domain User Account” **(8 marks)**
- d) Explain any **TWO** components of a client server architecture. **(2 marks)**