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 BACHELOR OF SCIENCE IN SECURITY AND FORENSICS

2ND YEAR 1ST SEMESTER 2015/2016 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3216

COURSE TITLE: TCP/IP NETWORK ADMINISTRATION

EXAM VENUE: **STREAM: COMPUTER SECURITY & FORENSICS**

DATE: **EXAM SESSION:**

TIME:

INSTRUCTIONS

1. **Answer Question 1 (Compulsory) 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 [30 marks]

a) Define the following terms
    i) IP Address   **(2 marks)**
    ii) Subnet Mask   **(2 marks)**
    iii) Default Gateway   **(2 marks)**
    iv) Protocol analyzer   **(2 marks)**
    v) Packet switching   **(2 marks)**
    vi) Flow control   **(2 marks)**
    vii) Error control   **(2 marks)**
b) Discuss three categories of IPv4 addresses   **(6 marks)**
c) Discuss the TCP/IP stack.   **(8 marks)**
d) What is the key difference between TCP and UDP segment?   **(4 marks)**

Question 2 [20 marks]

a) Identify the protocols associated with the port numbers Define the following terms: **(7 marks)**
    i.   25
    ii.   21
    iii. 53
    iv. 23
    v.   80
    vi. 443
    vii. 67

b) Give three reasons why subnetting is important.   **(3 marks)**
c) Understanding Layer 3 protocols and services is critical to troubleshooting many issues. Identify three Layer 3 issues: **(6 marks)**
d) Identify four differences between IPv4 and IPv6   **(4 marks)**

Question 3 [20 marks]

a) Differentiate between routing and routed protocol. Give two examples of each   **(6 marks)**

b) Discuss any four tools available to a network administrator for monitoring network resources and reports   **(8 marks)**

c) Prefix-Notation is usually referred to as "slash" notation. The number after the slash refers to the number of one bits in the subnet mask. The subnet mask

always has contiguous 1 bits from left-to-right. Provide the dotted decimal notation for the following prefix notation.   **(6 marks)**

    i)   /9

    ii)   /27

    iii) /18

Question 4 [20 marks]

a) The network engineer gives you the following network address and subnet mask: 192.168.1.0/27   **(6 marks)**

    i)   Determine the number of subnets that can be created from this network address (show your work)

    ii) Calculate the number of assignable IP addresses for each subnet created (show your work).

d) The definition of computer security introduces *five* important things which form the heart of computer security. Identify these five.   **(5 marks)**

e) Security controls in cloud computing are similar to the security controls in any IT environment. However, because of the operational models and technologies used to enable cloud service, cloud computing may present risks that are specific to the cloud environment. The essential concept in this regard is that the enterprise loses a substantial amount of control over resources, services, and applications but must maintain accountability for security and privacy policies. The Cloud Security Alliance has identified the top cloud specific security threats, together with suggested countermeasures: Discuss the top *five* cloud security threats and their countermeasures.   **(10 marks)**

Question 5 [20 marks].

a) Differentiate between active and passive attacks. Give two examples each.   **(6 marks)**

b) IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. The principal feature of IPSec that enables it to support these varied applications is that it can encrypt and/or authenticate all traffic at the IP level. Discuss th three functional areas of IP level security.   **(6 marks)**

c) One of the most common tasks for administrators is the creation of Active Directory user objects. Windows Server 2012 includes several tools you can use to create objects. In addition, group policy allows you to control and deploy operating system settings to

computers all over your network. During the lab you added computers to the AD and set up group policies for the client computer. Briefly describe how you added a windows 7 client machine to windows server 2012. How did you configure security policy for this client machine? **(8 marks)**