JARAMOGI OGINGA ODINGA UNIVERSITY

OF SCIENCE & TECHNOLOGY

UNIVERSITY EXAMINATIONS 2012/2013

1ST YEAR 1ST SEMESTER EXAMINATION FOR THE DEGREE

OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

(KISUMU L.CENTRE)

COURSE CODE: IIT 5111

COURSE TITLE: COMPUTER OPERATING SYSTEM &

VIRTUALIZATIONS

DATE: 12/8/2013   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.

SECTION A

(20 Marks)

Q1 True/False, Multiple choice and Explanation   (One Mark Each)

1) An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

   A. Evidence collected through personal observation
   B. Evidence collected through systems logs provided by the organization's security administration
   C. Evidence collected through surveys collected from internal staff
   D. Evidence collected through transaction reports provided by the organization's IT administration

2) Your company has a domain controller named Server1 that runs Windows Server 2008 R2. Server1 has the DNS Server role installed. You need to configure the DNS server to resolve IP addresses to host names. Which record should you create?

   A. Pointer (PTR)
   B. Host Info (HINFO)
   C. Service Location (SRV)
   D. Canonical Name (CNAME)

3) You are employed as an enterprise administrator at Company.com. The Company.com network consists of a single Active Directory domain named Company.com. All servers on the Company.com network run Windows Server 2008.

   Company.com contains a server named Company-SR10 that runs the Web Server (IIS) role. Company-SR10 is hosting a public website. During a routine monitoring you notice high traffic volume on the public website. You need to get the source of the high traffic volume.

   What should you do?

   A. The best option is to enable website logging to filter the logs for the source IP address, in the IIS server manager.
   B. The best option is to view the source IP address of the traffic by install a third-party traffic analysis software.
   C. The best option is to run the net session - at command on Company-SR10.
   D. The best option is to run the net stat/all command to view the traffic statistics

4) Why does the IS auditor often review the system logs?

   A. To get evidence of password spoofing.

B. To get evidence of data copy activities
C. To determine the existence of unauthorized access to data by a user or program
D. To get evidence of password sharing

5) An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

A. cold site.
B. warm site.
C. dial-up site.
D. duplicate processing facility.

6) What influences decisions regarding criticality of assets?

A. The business criticality of the data to be protected
B. Internal corporate politics
C. The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole
D. The business impact analysis

7) A critical function of a firewall is to act as a:

A. special router that connects the Internet to a LAN.
B. device for preventing authorized users from accessing the LAN.
C. server used to connect authorized users to private trusted network resources.
D. proxy server to increase the speed of access to authorized users.

8) Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing. True or false?

A. True
B. False

9) Briefly describe the protocols that are used on the WAN.

A. X.25,
B. ISDN,
C. ATM, Frame Relay
D. X.500

10) Your company has an IPv4 Ethernet network. A router named R1 connects your segment to the Internet. A router named R2 joins your subnet with a segment named Private1. The Private1 segment has a network address of 10.128.4.0/26. Your computer named WKS1 requires access to servers on the Private1 network. The WKS1 computer configuration is as shown in the following table.

Network	Addresses
IPv4 Address	10.128.64.113
Subnet mask	255.255.252.0
Default Gateway	10.128.64.1

he routers are configured as shown in the following table.

Router ID	Addresses
R1 – interface 1	10.128.64.1
R1 – interface 2 (To Internet)	131.107.108.37
R2 – interface 1	10.128.64.10
R2 – interface 2	10.128.4.1

WKS1 is unable to connect to the Private1 network by using the current configuration. You need to add a persistent route for the Private1 network to the routing table on WKS1. Which command should you run on WKS1?

A. Route add -p 10.128.4.0/22 10.128.4.1
B. Route add -p 10.128.4.0/26 10.128.64.10
C. Route add -p 10.128.4.0 mask 255.255.255.192 10.128.64.1
D. Route add -p 10.128.64.10 mask 255.255.255.192 10.128.4.0

11) Grid computing harnesses far-flung computers together by way of the Internet or a virtual private network to share CPU power, databases, and database storage.

A) True
B) False

12) Risk assessment consists of the identification of risks or threats, the implementation of security measures, and the monitoring of those measures for effectiveness.

A) True
B) False

13) Risk management is the process of evaluating IT assets, their importance to the organization, and their susceptibility to threats, to measure the risk exposure of these assets.

A) True
B) False

14) Intrusion-detection software looks for people on the network who should not be there or who are acting suspiciously.

   A) True
   B) False

15) If you act legally, you are also acting ethically.

   A) True
   B) False

16) Identity theft occurs when someone forges your identity for fraudulent purposes.

   A) True
   B) False

17) Making backup copies of information is critically important.

   A) True
   B) False

18) Public key encryption utilizes two keys—only a person with both keys can decrypt a message or file.

   A) True
   B) False

19) The most successful companies place the highest value on information.

   A) True
   B) False

20) Disaster recovery plans specify how an IT system or information can be recovered in the event of a catastrophe.

   A) True
   B) False

SECTION B

Q2 Hypervirtualization

a) Briefly explain the term virtualization and why is it important in modern network infrastructure. (**2 Marks**)

b) Briefly describe terms: (**18 Marks**)
   i) Virtualization,
   ii) Hypervisor,
   iii) High Performance Computing,
   iv) On-demand Computing,
   v) Virtualized System Environment
   vi) Cluster Computing
   vii) Cloud Virtualization

Q3

a) You're an Information Security Consultant working Kisumu City, you have been contracted to deploy multiple servers and firewalls to protect the LAN – however, the company that have contracting you have very limited funds. How would you go about accomplishing this task?
(**5 Marks**)

c) You're tasked with deploying Bind9 DNS server for company with domain name: **example.com**.

   i) Describe the critical stages required to deploy a fully working DNS server with a capability to also function as MX mail server. (**7 Marks**)

   ii) Write down the commands required to test its functionality as a server, and as a mail server. (**2 Marks**)

d) What's LDAP and why is it very important in a enterprise network infrastructure. Draw a schematic diagram to present **example.com** domain with two OUs i.e., IT and Sales
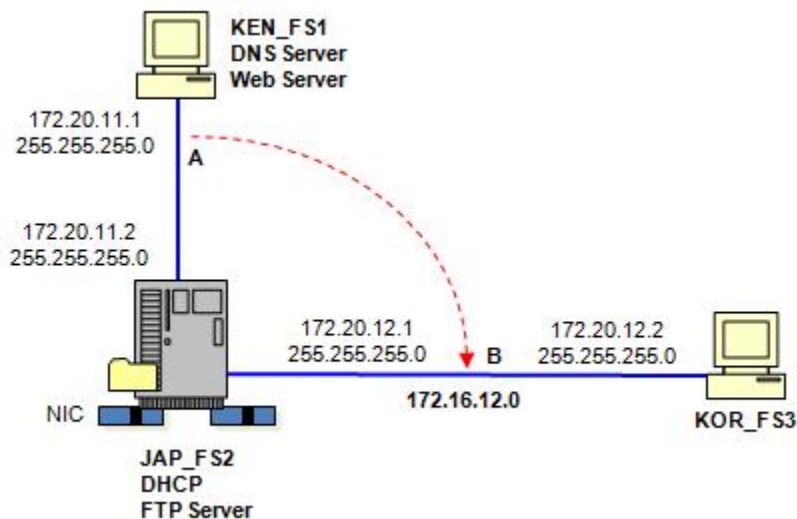(**6 Marks**)

Q4 Active Directory

a) What is a messaging server and why is it important to have it in an organization? (**4 Marks**)

b) Given an option to choose between MS Exchange server and Postfix mail server, which one would choose and why? (**Hint:** Cost versus open source). (**4 Marks**)

c) You're tasked with deploying MS Exchange messaging server 2010, describe key requirements needed to successfully deploy working server. (**12 Marks**)

Q5

You're a consultant for an Intercontinental Software which is an international company involved in creating applications for the Textile Manufacturing industry and wants to setup a number of software development teams. The company has offices in three countries – Canada, Japan, and Australia (Kenya, Japan, and Korea) – and would like to have individuals from each office on each team.

You have been hired to connect and configure Intercontinental Software's TCP/IP networks so that users in each location can communicate with those in any other location. In order to share information quickly with the other locations, the server in the Kenya head office will be set up as a Web Server and you will set up a default home page for the company. For the purpose of conveniently sharing files, the server in Japan will be set up as the corporate FTP server.

A diagram of the network is shown below with relevant information. (**Note**: the company is using leased T1 lines between all locations. Consider each connection as a direct connection between the servers.)

a) Through step-by-step write the critical steps required to accomplish this task using the following set criteria: (**20 Marks**)

Project Objectives
The objectives of this project are:
- Install and configure the DHCP Server services and DHCP clients
- Install and configure the DNS Server services
- Manage the DNS database and DNS topology
- Install and configure IP routing
- Install and configure Internet Information Services (IIS)
- Enable and block HTTP and FTP services using IPSec policies

Project Specifications

1. All servers must be members of the ICSOFTWARE workgroup.

Canada, Japan, and Australia (Kenya, Japan, and Korea)
2. DHCP must be configured on JAP_FS2 to supply IP lease assignment to KOR_FS3. JAP_FS1 must be configured with static IP address and KOR_FS3 must receive the same IP address each time it boots up.

3. All servers need to be able to communicate with each other. Since some servers are on different subnets, you need to configure static IP routes to facilitate this; however, IP routing can be used on the JAP_FS2 server. (Dynamic routing protocols are not to be used.) (**Note:** Static routes can be setup using either ROUTE.EXE command-line utility or the Routing and Remote Access MMC program. It is significantly easier to create static routes with the GUI program than with the ROUTE utility.)

4. The DNS Services must be installed and configured on KEN_FS1 and must provide DNS services to all other servers. A DNS domain name of **ICSoftware.com** must be created. Name resolution to IP address and IP address resolution to host name is required.

5. KEN_FS1 is to serve as the corporate Web server and requires the installation of IIS. You must also configure a simple home page with the words "Welcome to Intercontinental Software" that all servers will be able to view through a Web browser using the site's URL. FTP services on KEN_FS1 must be blocked using an IPSec Blocking Policy.

6. JAP_FS1 is to provide corporate FTP server and also requires the installation of IIS. You must create a simple text file and place it in the root directory of FTP Server. WWW services on JAP_FS1 must be blocked using an IPSec Blocking Policy.