(Knowledge for Development)

KIBABII UNIVERSITY

UNIVERSITY EXAMINATIONS
2019/2020 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS
YEAR THREE SEMESTER ONE EXAMINATIONS

FOR THE DEGREE OF
BACHELOR OF SCIENCE COMPUTER SCIENCE

COURSE CODE: CSC 373E

COURSE TITLE: NETWORK AND SYSTEM ADMINISTRATION

DATE: 16/02/2021 **TIME: 08.00 A.M – 10.00 A.M**

INSTRUCTIONS TO CANDIDATES

ANSWER **QUESTIONS ONE** AND **ANY OTHER TWO.**

QUESTION ONE [COMPULSORY] [30 MARKS]

a) Define a human-computer system in the context of system administration. **[2 marks]**

b) Outline the challenges of system administration. **[5 marks]**

c) What is a Multi Router Traffic Grapher (MRTG) and how does it assist the system administrator. **[3 marks]**

d) Explain how the following tools can make the job of a network/system administrator easier?

  i) Ghosting tools **[2 marks]**

  ii) DHCP tool **[2 marks]**

e) A user contacts you and reports that their Windows 2000 workstation is having trouble connecting to the Web. You run the ipconfig command on the computer and you find that the computer is not referencing the correct primary DNS server. What must you do to remedy this? **[3 marks]**

f) Upon examining bandwidth utilization graph, a network administrator discovers a great difference for the graph oscillation for both the inbound and the outbound traffic. He then checked the firewall log file size and noticed that it was about 9 times multiple of the usual size. He then decides to use Ethereal to be able to quickly detect the cause of the problem and notice that there was a high percentage of ICMP traffic passing through the network. The source address of the traffic was one of the notebooks IP addresses that were connected to the LAN, and the destinations were external consecutive ranges of IP addresses "contiguous blocks of IP addresses". At this point he succeeded in isolating the problem as the known worm "W32.Welchia.Worm", one of its payload is to scan for active machines to infect by sending an ICMP echo request (or PING), resulting in increased ICMP traffic, localized network latency and widespread denial of service.

  i). Outline the solution that the network administrator would apply to this problem. **[2 marks]**

  ii). State the THREE network monitoring strategies applied by the network administrator to detect the warm and for each state the tool used or may have been used in the scenario **[6 marks]**

g) Identify and explain the three main components in a human–computer system. **[5 marks]**

QUESTION TWO [20 MARKS]

a) Explain why it is important to perform backups on a regular basis. **[2 marks]**

b) Distinguish between full, differential and incremental backups. **[6 marks]**

c) As a system administrator describe TWO backup/restore policy you may use. **[4 marks]**

d) State any EIGHT things you need to take into consideration when planning an upgrade from one network operating system to another? **[8 marks]**

QUESTION THREE [20 MARKS]

A company, example.org, has a webserver (ws.example.org) and several workers, each of which have a desktop computer. The company's network has the following hostnames and IP addresses:

Hostname	**IP Address**
router.example.org	192.168.223.1
ws.example.org	192:168.223.5
desktop1.example.org	192.168.223.8
desktop2.example.org	192.168.223.9

In the beginning, the company wanted to make sure that their webserver was accessible to potential customers over the Internet. To accomplish this, they purchased a leased line (or other permanent connection), put a router on their premises, and then hooked their webserver up to the Internet. Then their problems started. The first thing they noticed was that their webserver received lots of traffic, but much of that traffic was not to the web server process itself. They also noticed slowdowns on their server, and they found processes running on it that the System Administrators were not familiar with. Furthermore, they noticed that their desktop systems suddenly got slower and started behaving erratically.

a) Explain the probable course of this problem. **[6 marks]**

port scanning. The Internet connection they had installed had become a gateway for attackers to learn about their systems, and then to attack known vulnerabilities on those systems. One of the commonly used network scanning tools is nmap. It scans by initiating a TCP connection to a particular port. If a host responds with a packet acknowledgement, then nmap knows that a service is running a service on that port. If a host responds with a port unreachable, then nmap knows that the host is alive, but that the service may not be available. In general, network scanning tools use various strategies to hide their work. For example, most tools are not so naive as to sequentially scan IP addresses and ports, which would make them very vulnerable to detection. Instead, they have various timers and randomizers that attempt to bypass any detection mechanisms. Once the attackers found vulnerable services on the machines, they would then use known attacks to get in.

b) The System Administrators were not happy with the situation, though: while the only system that needed to be accessible to the Internet was the web server, internal systems were also visible to the Internet. They needed to somehow stop that access. After some searching, they found some layer 3 and layer 4 firewall products to solve their problems.

i. Identify an appropriate layer 3 firewall that the System admin may use and explain how it can be used to protect the internal systems (i.e., the desktop systems). **[4 marks]**

ii. Explain how the layer 4 firewall would help the system administrator to do port filtering. Hence state to rule sets that the system administrator would set to restrict network traffic to just the web server **[4 marks]**

c) The users then called with a request: since the company's web server was such a vital resource, the users thought they should use the Internet, too. After all, they needed to find product information from other companies, and by looking on the Internet, they were able to research others' products faster. The system administrators discussed the problem, and determined that a safe firewall rule would allow the internal desktops to talk to a web server on the Internet, but not allow any other traffic. Thus, they came up with a set of rules like this:

- allow desktop*.example.org to send to anyone on destination port 80
- allow anyone to send to desktop*.example.org, but only if the source port is port 80

This almost worked, but there is one problem: An attacker can simply use port 80 as the source port and now scan the network.

Explain how the TCP 3-way handshake may be used to address this problem?

Other than the TCP three-way handshake solution, state two other firewalls that can be used to address this problem? **[6 marks]**

QUESTION FOUR [20 MARKS]

a) A critical skill for any network/system administrator that supports a network environment is IP subnetting. Outline FOUR reasons to explain why subnetting is important? **[8 marks]**

b) You are the network administrator for the XYZ Company; you would like to subnet the company's network (198.168.168.0) so that there are five separate subnets with 25 hosts each. Complete the table below to show how you will create the subnets. Include extra subnets that you may create. **[12 marks]**

subnet	Network address	Host addresses	Broadcast address
Subnet mask: 255.255.255.**224**			

QUESTION FIVE [20 Marks]

a) Differentiate the following terminologies as used in internetworking.

   i. IPv4 and IPv6 **[2 marks]**

   ii. Static and dynamic addressing **[2 marks]**

   iii. Private and public addresses **[2 marks]**

b) Describe the concept of Multiprotocol Label Switching (MPLS) as used in telecommunication networks. **[4 marks]**

c) Discuss analog/digital data and analog/digital signals as used in data transmission. **[3 marks]**

d) Discuss any seven (7) network monitoring tools deemed necessary for computer networks troubleshooting today. **[7 marks]**