Strathmore
UNIVERSITY

**STRATHMORE UNIVERSITY**
**FACULTY OF INFORMATION TECHNOLOGY**
**BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBERSECURITY**
**END OF SEMESTER EXAMINATION**
**CNS 2106 – NETWORK PROGRAMMING**

DATE: 30th November, 2022 Time: 2 Hours

**Instructions**
1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

**QUESTION ONE**

a. State the use of the following Linux text processing tools or utilities: grep, sed, cut, awk [**4 Marks**]

b. What are the four **tables** maintained by the Linux kernel for processing incoming and outgoing packets? [**2 Marks**]

c. Give the full file path for the following services on a Linux system
   i. Where manual IP addresses are configured [**1 Mark**]
   ii. Where the SSH public key is stored on a remote server? [**1 Mark**]
   iii. Where an additional DNS server IP addresses can be defined for a network that uses DHCP [**1 Mark**]
   iv. Where static mapping between names and IP addresses is achieved [**1 Mark**]

d. Give the full file path used for recording logs for the following services on a Linux system
   i. Apache2 web server [**1 Mark**]
   ii. Exim4 email server [**1 Mark**]
   iii. Bind9 DNS server [**1 Mark**]
   iv. System authentication [**1 Mark**]

e. A Site Reliability Engineer noted a disturbing pattern with one of the cloud systems she was administering. The server would shut down every week on Saturday at 01H00. With respect to CRON explain with an example of an entry that may have been left on the server. [**3 Marks**]

f. Write sample commands that will achieve the following
   i. Change the owner (user) of a file from jane to john [**1 Mark**]
   ii. Change the owner of a directory and all its files from luke to lisa [**1 Mark**]
   iii. Grant read and write permission to user and group, and no permission to others [**1 Mark**]

g. Simple Network Management Protocol (SNMP) is implemented by open source software such as Cacti and Nagios.
   i. Describe the configuration settings that are required on a Nagios core server as well as on a remote monitored server. [**5 Marks**]

   ii. Describe the interaction between a Nagios core server and a monitored remote server. You answer should include three system conditions (object) that can be monitored. [**5 Marks**]

**(Total: 30 Marks)**

**QUESTION TWO**

a. When configuring access control for SSH, what does the following directives mean:
   i. PermitRootLogin yes. [**1 Mark**]
   ii. Allowusers <username> [**1 Mark**]

b. Explain why it is recommended to only permit remote SSH login with Public Key authentication. Give an example of problems with use of passwords for SSH authentication. [**4 Marks**]

c. HTTP server application such as Apache2 support authentication and access control with use of IP address, as well as user-names with passwords.
   i. Describe how authentication and access control can be configured based on both IP address and user-names with passwords. [**3 Marks**]

   ii. Describe an application scenario where IP address authentication can be used for HTTP. [**2 Marks**]

   iii. Describe an application scenario where both IP address and user-names with password authentication can be used. [**2 Marks**]

d. Name two Linux files that are used for holding login credentials for system users. [**2 Marks**]

**(Total: 15 Marks)**

**QUESTION THREE**

a. In IPTables, what is meant by a chain policy? [**1 Mark**]

b. What do the following IPTables commands achieve; iptables –L, iptables –F, iptables –N, iptables -X [**2 Marks**]

c. In IPTables, which part of a packet is examined in order to figure out whether or not the condition part of a rule is satisfied? Name any two parts. [**2 Marks**]

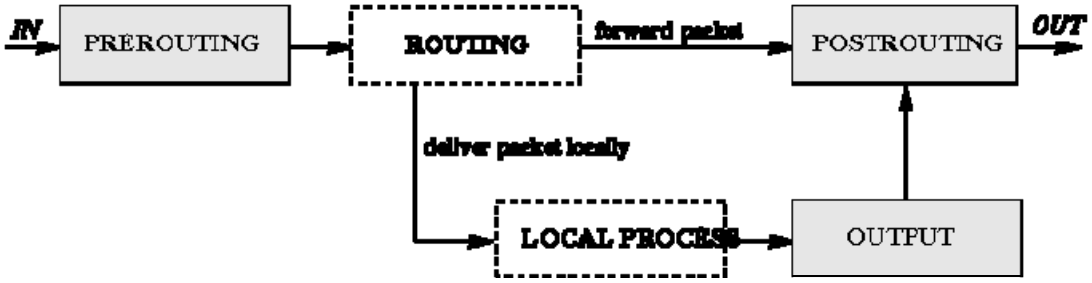
d. As a packet is being processed by a chain of rules, what happens to the packet if it does not satisfy the conditions in any of the rules? [**2 Marks**]

e. How does an iptables based firewall decide which packets to subject to the INPUT chain of rules, which to the FORWARD chain of rules, and which to the OUTPUT chain of rules? [**3 Marks**]

f. State the difference between –J DROP and –J REJECT actions of an IPTables rule when used to deny access to an IP packet. [**1 Mark**]

g. Draw the internal structure of the IPTables **nat** table and explain the processing of packets in a router (or gateway) that implements Network Address Translation. Hint: Show and explain use of PREROUTING and other chains of the **nat** table. [**4 Marks**]

***Solution***




**(Total: 15 Marks)**

**QUESTION FOUR**

a. BASH is a popular language used for Network Programming.

i. Give the first line of a BASH file [**1 Mark**]

ii. Write a sample BASH **For Loop** [**2 Marks**]

iii. Write a sample BASH **if** conditional block [**2 Marks**]

iv. Declare and initialise a BASH array named **week** whose elements are the days of the week [**2 Marks**]

v. What are BASH operators for the following other programming language operators <, >, != [**3 Marks**]

b. Write a Linux command that will assign an **extra (alias)** IP address (10.20.113.45/24) to the network card eth0 [**3 Marks**]

c. The administrator of a Linux system wants to use CRON to provide a daily custom message that is displayed to all users when the login to the terminal e.g. via SSH. In which system file should the message be written? [**2 Mark**]

**(Total: 15 Marks)**

**QUESTION FIVE**

a. You are required to design a small Internet Service Provider (ISP) network that will achieve the following.
   i. Utilise one public IP address to provide Internet access to 20 users
   ii. Measure internet usage by user
   iii. Block internet access for users who reach a 10 Gb data allowance in a month
   iv. Send an SMS at 00H30 everyday notifying each user of their day's usage and quota balance
   v. Send an SMS to alert the ISP's network engineer whenever there is a problem with the network e.g. failure of the uplink or key services required by the users

   Draw a diagram of the ISP network that shows the full architecture, and use the architecture to explain how you will meet the requirements above. Note: number your answers accordingly.

[**15 Marks**]

**(Total: 15 Marks)**