Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
BACHELOR OF INFORMATICS AND COMPUTER SCIENCE
BACHELOR OF COMPUTER NETWORKS AND CYBER SECURITY
END OF SEMESTER EXAMINATION
ICS3206 & CNS3205: SERVER ADMINISTRATION

DATE: 7th December 2023 Time: 13.00 - 15.00

Instructions

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

Question One [30 Marks]

A. Secure Socket Shell (ssh) is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network. Explain SSH port forwarding as used in most systems. **[2 Marks]**

B. Explain four differences between ssh & Telnet. **[6 Marks]**

C. Briefly, discuss how to disable the root login in Linux server. **[3 Marks]**

D. Understanding how to run a native text editor on a Linux system is very important mainly for these two reasons: security and working on a remote server. Using any appropriate examples, discuss these reasons. **[6 Marks]**

E. Explain any two differences between Git and GitHub. **[4 Marks]**

F. Using a diagram, explain the Linux filesystem. **[5 Marks]**

G. Discuss any three the main features of a Linux filesystem. **[3 Marks]**

H. Write a command that shows the version of the Linux kernel that a user is currently using. **[1 Mark]**

Question Two [15 Marks]

A. Consider a file with the following permissions: -rw-r-xrw- readme.txt. Show by use of commands how you can modify the permissions using both the symbolic and numeric/absolute modes such that all the users in the system have read, write and execute permissions. **[6 Marks]**

B. Explain why it is possible for sudo to let a standard user account run commands as root. **[2 Marks]**

C. Write the answer that best describe activity explain below regarding users and groups management in Linux: **[3 Marks]**

I. The name of the file in which details of user accounts are stored.

II. The name of the file that stores salted/hashed versions of user passwords for authentication.

III. A command can be used to change password policies such as minimum and maximum password age.

D. Explain any four process states in Linux. **[4 Marks]**

Question Three [15 Marks]

A. Use diagrams to illustrate the difference in implementation between the hosted and the bare-metal hypervisors. **10 Marks]**

B. Figure1 shows the /var/log/Syslog directory in the Linux file system. Explain the output as shown in the figure. **[5 Marks]**

```
ubuntu@ip-10-111-10-49:/var/log$ cat syslog
Mar 18 06:33:28 ip-10-111-10-49 systemd[1]: Starting Daily apt upgrade and clean activities...
Mar 18 06:33:30 ip-10-111-10-49 systemd[1]: Started Daily apt upgrade and clean activities.
Mar 18 06:35:30 ip-10-111-10-49 systemd[1]: Created slice User Slice of ubuntu.
Mar 18 06:35:30 ip-10-111-10-49 systemd[1]: Starting User Manager for UID 1000...
Mar 18 06:35:30 ip-10-111-10-49 systemd[1]: Started Session 251 of user ubuntu.
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Listening on GnuPG cryptographic agent and passphrase cache.
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Listening on GnuPG cryptographic agent and passphrase cache (re
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Listening on GnuPG cryptographic agent and passphrase cache (ac
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Reached target Paths.
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Listening on GnuPG network certificate management daemon.
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Reached target Timers.
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Listening on REST API socket for snapd user session agent.
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Reached target Sockets.
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Reached target Basic System.
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Reached target Default.
Mar 18 06:35:30 ip-10-111-10-49 systemd[31311]: Startup finished in 18ms.
Mar 18 06:35:30 ip-10-111-10-49 systemd[1]: Started User Manager for UID 1000.
Mar 18 06:36:05 ip-10-111-10-49 systemd-networkd[876]: eth0: Configured
Mar 18 06:36:05 ip-10-111-10-49 systemd-timesyncd[565]: Network configuration changed, trying to establish conn
Mar 18 06:36:05 ip-10-111-10-49 systemd-timesyncd[565]: Synchronized to time server 91.189.89.198:123 (ntp.ubun
```

Question Four [15 Marks]

A. Server hardening is a system hardening process that aims to protect and secure a server infrastructure against cyberattacks by reducing its attack surface. An attack surface consists of all possible points of a system where an unauthorised attacker can attempt to enter. Explain any five ways to secure remote servers with multiple sysadmins enabled. **[10 Marks]**

B. Red Hat Package Manager (RPM) is a free software tool used by many Linux distributions for installing, upgrading, and removing packages on Linux distributions. Explain the two main types of RPM packages. **[5 Marks]**

Question Five [15 Marks]

A. Using examples, discuss the process of registering a domain. **[5 Marks]**

B. Regarding the performance of web servers, discuss any five comparisons between the Nginx and Apache web servers. Use examples where possible. **[10 Marks]**