University of Colombo, Sri Lanka

University of Colombo School of Computing

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2024 — 3rd Year Examination — Semester 5

IT5406 — Systems & Network Administration

Structured Question Paper

(2 Hours)

To be completed by the candidate							
Index Number							

Important Instructions

- The duration of the paper is **2 hours**.
- The medium of instructions and questions is English. Students should answer in the medium of English language only.
- This paper has **4 questions** on **11 pages**. Answer **all** questions.
- All questions carry **equal** marks.
- Write your answers **only on the space provided** on this question paper.
- Do not tear off any part of this question paper. Under no circumstances may this paper (or any part of this paper), used or unused, be removed from the Examination Hall by a candidate.
- Note that questions appear on both sides of the paper. If a page or part of a page is not printed, please inform the supervisor/invigilator immediately.
- Any electronic device capable of storing and retrieving text, including electronic dictionaries, smartwatches, and mobile phones, is not allowed.
- Calculators are **not allowed**.
- *All Rights Reserved.* This question paper can NOT be used without proper permission from the University of Colombo School of Computing.

To be completed by the examiners

1	
2	
3	
4	
Total	

Index Number □□□□□□□

1. (a). Write down **three (03)** important questions you should answer before adopting a Linux distribution.

[3 marks]

Is this distribution going to be around in five years?, Is this distribution going to stay on top of the latest security patches?, Does this distribution have an active community and sufficient documentation?, If I have problems, will the vendor talk to me, and how much will that cost?, Reference book page 08

(b). Write down **three (03)** Red Hat Package Management System based Linux distributions.

[3 marks]

Red Hat Enterprise , CentOS, Fedora, Oracle Linux , SUSE Linux Enterprise, openSUSE, reference page 9.

(c). What is the purpose of a "man page"?

[2 marks]

Man pages are concise descriptions of individual commands, drivers, file formats, or library routines. (reference page 14)

(d). Write down a Linux command that allows you to determine if a software is already installed or not.

[2 marks]

which, locate, (reference page 21)

Index Number

(e). Briefly describe the role of a **Security Operations Engineer**.

[3 marks]

Security operations engineers focus on the practical, day-to-day side of an information security program. These folks install and operate tools that search for vulnerabilities and monitor for attacks on the network. They also participate in attack simulations to gauge the effectiveness of their prevention and detection techniques.

Reference page 27.

(f). Explain the given GRUB commands, using a single sentence.

[1 marks]

boot

Boots the system from the specified kernel image

[1 marks]

linux

Loads a Linux kernel

[1 marks]

search

Searches devices by file, filesystem label, or UUID

Index Number □□□□□□□

(g). Briefly describe the **Single-user Mode** in a Linux system.

[3 marks]

Single-user mode, in which only a minimal set of filesystems is mounted, no services are running, and a root shell is started on the console

Reference page 41.

(h). Write down **three (03)** configurations found in a unit with respect to a service in **systemd**.

[6 marks]

the unit file specifies the location of the executable file for the daemon, tells systemd how to start and stop the service, and identifies any other units that the service depends on.

Reference page 45.

Index Number | | | | | | | |

2. (a). i. What is the Linux utility command that can be used to set a network interface's media-specific parameters such as link speed?

[1 marks]

ethtool Reference Page 421

ii. Write down the Linux command that can be used to set the network interface **eth0** to **100 Mbps full duplex**.

[3 marks]

sudo ethtool -s eth0 speed 100 duplex full
Reference Page 422

iii. Write down the Linux command that can be used to ignore ICMP ping messages.

[3 marks]

sudo cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
Reference Page 422

iv. A time value measured in milliseconds can be found in the output of a ping command. Explain what is that measurement and how it is useful.

[3 marks]

round trip travel time
The round trip time reported by ping can afford insight into the overall performance of a path through a network
Reference Page 430

(b). Explain why it is not recommended to use Linux, UNIX, or Windows systems as firewalls?

[3 marks]

Because of the insecurity inherent in running a full-fledged, general-purpose oper- ating system
Reference page 440

Index Number

(c). Network troubleshooting is an essential skill a System and Network Administrator should have. Write down **four (04)** basic principles to follow when troubleshooting a system or network.

[6 marks]

Make one change at a time, Back out any changes that have an undesired effect, Document the situation as it was before you got involved, and document every change you make along the way, Start at one end of a system or network and work through the system's critical components until you reach the problem, use the layers of the network to negotiate the problem
Reference Page 428

(d). List **three (03)** core features of a Virtual Private Cloud (VPC) in cloud networking.

[6 marks]

An IPV4 private address space, Subnets to segment the VPC address space into smaller subnetworks, Routing tables, Security groups, Network Access Control Lists
Reference page 448

Index Number □□□□□□□

3. (a). Write down the **three (03)** most commonly used cloud service categories and explain how each one is different from the others.

[12 marks]

Infrastructure-as-a-Service (IaaS),

users request raw compute, memory, network, and storage resources. These are typically delivered in the form of virtual private servers, aka VPSs. Under IaaS, users are re- sponsible for managing everything above the hardware: operating systems, networking, storage systems, and their own software.

Platform-as-a-Service (PaaS),

developers submit their custom applications packaged in a format specified by the vendor. The vendor then runs the code on the user's behalf. In this model, users are respon- sible for their own code, while the vendor manages the OS and network.

Software-as-a-Service (SaaS)

the vendor hosts and manages software and users pay some form of subscription fee for access. Users maintain neither the operating system nor the applica- tion. Almost any hosted web application (think WordPress) falls into the SaaS category.

Reference page 276, 277

Index Number □□□□□□□

(b). Cloud providers maintain data centers around the world. They use "Regions" and "Availability zones" as standard terms to describe geography-related features. Describe each term and explain the difference using examples.

[10 marks]

A "region" is a location in which a cloud provider maintains data centers. In most cases, regions are named after the territory of intended service even though the data centers themselves are more concentrated. For example, Amazon's us-east-1 region is served by data centers in north Virginia.3

Some providers also have "availability zones" (or simply "zones") which are col- lections of data centers within a region. Zones within a region are peered through high-bandwidth, low-latency, redundant circuits, so inter-zone communication is fast, though not necessarily cheap. Anecdotally, we've experienced inter-zone latency of less than 1ms.

Reference page 278

(c). Write down **three (03)** cloud service providers.

[3 marks]

Amazon Web Services, Google Cloud Platform, DigitalOcean, etc.

Reference page 273

Index Number □□□□□□□

4. (a). What is a privileged network port?

[3 marks]

A network port that can only be opened by root user and those numbered below 1024.

(b). In a Linux system `/etc/shadow` file contains user passwords. However, the file is owned by the user root and assigned group is also root. Explain how Linux system has made regular users to change their own password without superuser privileges.

[5 marks]

When the kernel runs an executable file that has its "setuid" or "setgid" permission bits set, it changes the effective UID or GID of the resulting process to the UID or GID of the file containing the program image rather than the UID and GID of the user that ran the command.

Regular users need a setuid passwd command to mediate their access.

Page number 250, 68.

(c). Explain the niceness of a Linux process using the nice values.

[5 marks]

nice manages only CPU scheduling priority. A high niceness means a low priority for your process: you are going to be nice. A low or negative value means high priority: you are not very nice.

Reference page 102

Index Number □□□□□□□

(d). Explain the schedule of the linux cron configuration given below.

```
*/30 4,16 * * 1,3,5 /usr/bin/backup_script
```

[5 marks]

every 30 minutes
4 a.m. and 4 p.m.
any day of month
every month
on weekdays mon, wed, and fri
Reference page 110

(e). Explain the following log rotation configuration.

```
/var/log/sssd/*.log {
 weekly
 missingok
 notifempty
 rotate 2
 compress
```

[5 marks]

weekly run
if log file missing, that's fine
don't rotate if empty
keep only 2 files
compress rotated files
Reference page 320

Index Number

(f). What is the Linux utility command that can be used to display every system call that a process makes and every signal it receives?

[2 marks]

strace Reference page 105

****