MAKERERE UNIVERSITY BUSINESS SCHOOL

FINAL EXAMINATION FOR THE DEGREE OF BACHELOR OF BUSINESS COMPUTING OF MAKERERE UNIVERSITY, ACADEMIC YEAR 2026/2027

COURSE NAME: SYSTEMS AND NETWORK ADMINISTRATION
YEAR OF STUDY: THREE **COURSE CODE**: BUC3129
DATE: WEDNESDAY, 13TH NOVEMBER 2026 **TIME**: 8:00AM-5:00PM
MODE OF ASSESSMENT: TAKEHOME **SEMESTER**: ONE

INSTRUCTIONS:

- This paper is the **take-home component** of the BUC3129 Systems and Network Administration final examination. The final examination has two components, and both are compulsory:

Component	Format	Date	Weight
Take-home group capstone project (this paper)	Group practical project, written report, presentation and individual oral defence. Marked out of 60.	Issued Wednesday, 4th November 2026. Submit before 17:00hrs on Friday, 13th November 2026.	60%
Theory sit-in examination	Individual, closed-book written examination of two (2) hours covering the whole course.	Monday, 30th November 2026. Time and venue as per the examinations timetable.	40%
Total			100%

- This is a take-home examination and is accessible from **Wednesday, 4th November 2026**. All deliverables must be submitted on the Makerere University Business School E-learning platform (MUBSEP) **before 17:00hrs on Friday, 13th November 2026**. Late submissions will not be accepted.
- Do the project in your class groups (the same groups used for Coursework Two). Every member must contribute, must hold a defined role (see Section D), and must be ready to answer questions on **any** task when chosen randomly during the presentation and defence.
- Use **Ubuntu Server, the current stable Long Term Support (LTS) release (24.04 LTS or newer, 64-bit)**, installed as a virtual machine in **Oracle VirtualBox** (recommended) or another hypervisor of your choice such as VMware Workstation Player, Hyper-V or

KVM. A group that chooses a different Linux distribution or Unix-like operating system must state and justify the choice in the report and is responsible for using equivalent tools.

- The server must be administered from the command line. Do **not** install a desktop environment on the server. A second machine (your host computer or a second virtual machine) acts as the administrator's workstation.
- Installation media and software used must be free and legally obtained. Ubuntu Server images are available free of charge from the official Ubuntu website.
- For the final submission, upload: (i) the **PDF Report**; (ii) one ZIP file titled **GroupNumber_BUC3129_Evidence.zip** containing your scripts, configuration files and command logs; (iii) a text file containing the **link to the exported virtual machine and its SHA-256 checksum** (Task 10); and (iv) a separate one-page **credentials sheet**. The PDF Report must have a cover page indicating the company name, group number and all members, including their Student and Registration numbers and the role each member held.
- Every screenshot must show your group's server hostname or a group member's account name (for example, in the command prompt). Screenshots that could belong to any group score nothing.
- **Never** include passwords in the report. Submit them only on the separate credentials sheet. In the field, documentation is shared widely and credentials are not.
- Explain what you did and why. Do not paste long lists of commands into the body of the report; put full command logs and scripts in the Evidence ZIP and refer to them.
- Avoid copying and pasting, or any other kind of plagiarism and cheating. All groups are required to check for plagiarism via Turnitin before uploading the final report on MUBSEP. **Plagiarism and AI level MUST be below 15%.**
- The report **SHOULD NOT** be less than 15 pages and **NOT MORE** than 25 pages, excluding the cover page and appendices.
- Each member **MUST** complete the Self and Peer Evaluation of this Group Project via the Attendance Tracker on MUBSEP before the final deadline. A member whose name appears against no task, or who does not attend the defence, cannot score in this examination.
- Work only inside virtual machines. Take a snapshot before every significant change; a snapshot is your rollback plan. Lost work is not an accepted reason for late submission.
- All organisations, names and records in this paper are fictitious and were created for teaching. Any resemblance to a real organisation or person is coincidental.

Allocation of Marks

Section	Component	Max. Marks
A	Practical Linux administration tasks (Tasks 1 to 10)	40
B	Administration report and runbook	8
C	Group presentation and live demonstration	6
C	Individual oral defence (awarded to each member individually)	6
	Total (contributes 60% of the final examination)	**60**

TAKE-HOME EXAM PROJECT (60 MARKS):

BACKGROUND: WHY LINUX SYSTEM ADMINISTRATION

In Coursework Two your group operated as a small IT support company and built, secured and handed over a Windows Server environment for a client. This take-home examination builds directly on that work. The same company now takes on a new client whose servers will run Linux, and you will set up, configure, secure and administer a properly working Linux server from first installation to final handover.

Linux is one of the most widely used operating systems in the world. First released by Linus Torvalds in 1991 as a free and open-source kernel, it now runs most of the internet's web servers, the majority of workloads on public cloud platforms such as Amazon Web Services, Microsoft Azure and Google Cloud, the core infrastructure of many banks, telecommunication companies and mobile money platforms, and every one of the world's 500 fastest supercomputers on the TOP500 list since November 2017. The Android operating system on most smartphones is itself built on the Linux kernel. Organisations choose Linux because it carries no licence fees, is stable and secure, runs well on modest hardware, and can be managed remotely and automated entirely from the command line.

A Linux system administrator is responsible for installing and configuring servers, connecting them to the network, managing users, groups and file permissions, adding and managing storage, installing and updating software with a package manager, controlling services and processes, scheduling routine jobs such as backups, reading system logs, and hardening the server against attack. These are the same domains examined in industry certifications such as the Linux Foundation Certified System Administrator (LFCS) and CompTIA Linux+, and they are the focus of this project.

Ubuntu Server, published by Canonical, is one of the most widely deployed Linux distributions on servers and in the cloud. A new Long Term Support (LTS) release is

published every two years and receives at least five years of free security updates, which is why LTS releases are the standard choice for production servers. It uses the APT package manager, systemd for services, Netplan for network configuration and the Uncomplicated Firewall (UFW) front-end, all of which you will meet in this project.

SCENARIO:

Mpanga Valley Coffee Exporters Ltd is a medium-sized coffee processing and export company with its head office in Mukono and a buying centre in Mubende. It has about thirty staff in four departments: Management, Finance, Operations and Sales. Today the company keeps its files on an old desktop computer in the accounts office that everybody shares through one user account. There is no backup, no control over who can open the payroll and export contract files, and the machine is infected by malware every few months.

The Board has approved a move to an open-source Linux server so that the money saved on licences can be spent on a proper backup drive. Your company has been contracted to build the first server, prove that it works, and hand it over with documentation that the company's new junior IT officer can follow. The Managing Director has sent your company the following work order. Treat it as a real client request.

> *"We want one server that all our staff can use from their desks, and we want it set up the professional way. Every staff member must have their own login, and only your IT people should be able to make changes to the server. Our Finance files, especially payroll, must be seen only by Finance, and I must be able to read them but not change them. Sales and Operations need their own folders, and everybody needs one shared folder for notices and forms, where nobody can delete what a colleague has put there. Last month we lost three years of buyer records when the old computer's disk failed, so the files must be kept on storage that we can grow when it fills up, and they must be backed up every night without anybody remembering to do it. I want a simple internal web page staff can open to know the server is working. Our former accountant, Joan Akello, has left the company; her files must be kept but she must never be able to log in again. Finally, I am told that servers on the internet are attacked every day. Make sure ours is locked down, and that you can tell me who tried to get in."*

Several technical requirements are hidden in the work order. Section 2 of your report must restate each of them in technical language and show which task meets it.

Client Information

Use the following details exactly as given. Replace **NN** with your two-digit group number (for example, Group 7 uses 07 and 107).

Item	Value
Server hostname	gNN-srv01 (for example, g07-srv01)
Company directory on the server	/srv/mpanga
Network adapter 1	NAT (for internet access and software updates)
Network adapter 2	Host-only network 192.168.56.0/24 (VirtualBox default, or your hypervisor's equivalent)
Server static address on adapter 2	192.168.56.1NN/24 (for example, 192.168.56.107 for Group 7)
Time zone	Africa/Kampala
Minimum virtual machine size	2 vCPUs, 2 GB RAM, 25 GB system disk

Staff member	Position	Department	Username
Grace Namuli	Managing Director	Management	gnamuli
Daniel Okello	Finance Manager	Finance	dokello
Sarah Atim	Accounts Assistant	Finance	satim
Brian Mugisha	Operations Manager	Operations	bmugisha
Ruth Nakato	Sales Officer	Sales	rnakato
Isaac Wasswa	Sales Officer	Sales	iwasswa
Joan Akello	Former Accountant (has left)	Finance	jakello

REQUIRED

As the IT support company contracted by Mpanga Valley Coffee Exporters Ltd, set up, configure and administer a working Linux server that meets the work order. Each task below tells you **what must exist when you have finished**, not which commands to type. Researching the right tool is part of the task. Record every command you run (your shell history or a session log) and include it in the Evidence ZIP.

SECTION A: PRACTICAL LINUX ADMINISTRATION TASKS [40 MARKS]

Task 1: Installation and Initial Configuration [3 MARKS]

(a) Create a virtual machine that meets the minimum size in the Client Information table, with the two network adapters described, and install Ubuntu Server LTS on it with the OpenSSH server included.

(b) Set the hostname, the time zone and the clock synchronisation so that the server reports the correct local time and identifies itself correctly on the network.

(c) Bring the whole system up to date with all available updates before any other work, then take a snapshot named “baseline”.

(d) Record the release and kernel version, the CPU, memory and disk the server sees, and explain in the report why an LTS release is the right choice for this client.

Evidence required: The hypervisor settings of the virtual machine; the server's identity, time and release information; the update completing; and the snapshot list showing “baseline”.

Task 2: Network Configuration and Remote Access [4 MARKS]

(a) Configure the host-only adapter with the static address in the Client Information table, while the NAT adapter continues to obtain its address automatically. The configuration must survive a reboot.

(b) Make sure the server can resolve internet names, reach the internet through the NAT adapter, and reach the administrator's workstation through the host-only network.

(c) From the administrator's workstation, log in to the server over SSH using a group member's account. All further administration should be done this way.

(d) Identify which network services are listening on the server and on which ports, and explain each one in the report.

Evidence required: The network configuration file(s); the interface addresses and routing table after a reboot; successful name resolution and connectivity tests; an SSH session opened from the workstation; and the list of listening ports.

Task 3: Users, Groups and Administrative Rights [5 MARKS]

(a) Create one personal account for every member of your group, and make these accounts the only ones able to carry out administrative tasks. Ordinary staff must not be able to run anything as the administrator, and nobody should need to log in directly as root.

(b) Create the staff accounts in the staff table and a group for each department, with each staff member in the correct group. Every staff account must have its own private home directory.

(c) Enforce a password policy for staff accounts: a minimum length of 10 characters, a mix of character types, a maximum password age of 90 days with a warning 7 days before expiry, and a forced password change at first login.

(d) Deal with the leaver, Joan Akello, so that her account and files are kept but she can no longer log in by any method.

(e) Show that a staff member who tries to use administrative rights is refused and that the attempt is recorded.

Evidence required: The account and group listings; the administrative rights configuration; the password ageing settings of one staff account; a refused administrative attempt with the log entry it produced; and a failed login attempt by jakello.

Task 4: Storage Management **[4 MARKS]**

(a) Add a second virtual disk of at least 10 GB to the server. Configure it with logical volume management so that the company's storage can be grown later without rebuilding the server.

(b) Create one logical volume for the company's files, mounted at /srv/mpanga, and a second logical volume for backups, mounted at /backup. Leave some space in the volume group unallocated, and explain why.

(c) Both file systems must mount automatically at boot, identified in a way that does not change if disks are added or reordered.

(d) The Operations department warns that the company files will soon outgrow their space. Grow the company files volume and its file system by at least 1 GB while it is mounted and in use, without losing any data.

Evidence required: The disk, physical volume, volume group and logical volume listings; the persistent mount configuration; disk usage before and after the volume was grown; and the files still present after a reboot.

Task 5: File System Structure and Permissions **[5 MARKS]**

What must exist: a directory tree under /srv/mpanga with a directory for each of Finance, Operations, Sales and a Shared area, with the following access rules. Permissions must be assigned to groups, not to individual users, except where an exception is stated.

(a) Finance can read and write in the Finance directory. The Managing Director can read it but cannot change anything. Nobody else can even list its contents.

(b) Sales and Operations each have full access to their own directory and no access to each other's. As a stated exception, the Operations Manager must be able to read (but not change) the Sales directory without being added to the Sales group.

(c) All staff can create files in the Shared directory. New files automatically belong to the staff group, not to the creator's private group, and no user can delete or rename a file created by another user.

(d) New files created by staff must not be readable by everybody on the server by default.

(e) Prove each rule by acting as the affected users: show at least three refusals (for example, a Sales officer opening Finance, the Managing Director editing a Finance file, and one user deleting another user's file in Shared).

Evidence required: A tree view of /srv/mpanga with ownership and permissions shown; the special permission bits and access control entries you used; and each refusal with the user's name visible. A claim that it works is not proof. The refusal is the proof.

Task 6: Software and Package Management **[4 MARKS]**

(a) Install, from the official Ubuntu repositories, the tools your group needs to administer this server (at minimum a process monitor, a directory tree viewer and the access control list tools), and a web server.

(b) Publish a simple internal web page from the server, showing the company name, the server hostname and your group's members, and open it from the browser on the administrator's workstation using the server's static address.

(c) Configure the server to install security updates automatically.

(d) Remove one package you no longer need together with its configuration files, show the details (version and source repository) of one installed package, and prevent one package of your choice from being upgraded. Explain in the report when an administrator would hold a package back.

(e) Export a list of all installed packages to a file and include it in the Evidence ZIP.

Evidence required: The installations; the web page opened from the workstation with the address bar visible; the automatic update configuration; the removal, package details and held package.

Task 7: Services and Process Management **[4 MARKS]**

(a) Produce an inventory of the services running on the server. Choose three, at least one of which the client's work depends on, and state for each: what it does, whether it starts at boot, and what would stop working if it were stopped.

(b) Write a health-check script that records, with a date and time, the free space on /srv/mpanga and /backup, memory use and system load. Make the operating system run it every five minutes as a managed service, so that it starts by itself after a reboot without anybody logging in.

(c) Have one member, logged in as an ordinary staff account, start a process that uses the processor heavily. As the administrator, find it without being told what it is, identify its owner, process ID and resource use, first lower its priority, and then stop it safely.

(d) In the report, explain the difference between asking a process to stop and forcing it to stop, and when forcing it would be the wrong choice.

Evidence required: The service inventory table; the health-check script and its service and timer definitions; the health log showing entries from before and after a reboot; and the runaway process at the top of the monitor with its owner, followed by the system back to normal.

Task 8: Scheduled Backup, Restore and Logs **[4 MARKS]**

(a) Write a backup script that saves the Finance and Shared directories to /backup as a single compressed archive whose name includes the date and time, keeps only the seven most recent archives, and writes one line to a backup log every time it runs, whether it succeeds or fails.

(b) Schedule the script to run automatically every night at 01:30. Do not test a nightly job by waiting for the night: run it every few minutes first, prove it works, then change it to the real schedule, and say in the report that you did this.

(c) Delete a file from the Finance directory, then restore it from the latest archive to its original location with its original owner and permissions intact.

(d) Use the system logs to report every failed login attempt on the server over SSH, with the account name, source address and time. Configure the health log from Task 7 so that it is rotated weekly and old copies are compressed.

(e) In the report, explain why a backup kept on the same server is not a real backup, and what this client actually needs.

Evidence required: The backup script and schedule; the archives and backup log with timestamps; the deleted file and the restored file with its ownership and permissions; the failed login report; and the log rotation configuration.

Task 9: Server Security Hardening **[4 MARKS]**

(a) Set up key-based SSH login for every administrator account, then disable password logins over SSH and direct login as root over SSH. Confirm that key login still works before you close your existing session.

(b) Enable the host firewall with a default policy that refuses incoming connections. Allow SSH only from the host-only network 192.168.56.0/24, and allow the internal web page.

(c) Install and configure a service that automatically blocks an address after five failed SSH login attempts. Trigger it from the workstation, show the address blocked, and then unblock it.

(d) Show that a connection which is not allowed is refused, and list every remaining open port with the reason it is open.

Evidence required: The relevant lines of the SSH server configuration; a successful key login and a refused password login; the firewall status with its rules; the blocked and unblocked address; and the list of open ports.

Task 10: Fault Ticket and Handover **[3 MARKS]**

(a) One member deliberately changes one thing so that something built in Tasks 2 to 9 stops working and tells nobody what was changed. The member reports it in one sentence, as a user would (for example, “I cannot open the Sales folder”). The rest of the group handles it as a support ticket: log it, give it a priority, investigate, fix, test and close it. The order of the checks matters more than the answer.

(b) Shut the server down properly and export it from the hypervisor as a single appliance file named **BUC3129_GroupNN_Server.ova**. Calculate and record its SHA-256 checksum.

(c) Upload the file to a cloud drive, set sharing to “anyone with the link can view”, and test the link from a different account. A link that cannot be opened counts as no submission, and the link must still work on the day of marking.

Evidence required: The completed support ticket (reported problem, priority and reason, checks made in order with the result of each, root cause, fix, test, and time opened and closed); the export settings; and the checksum.

SECTION B: ADMINISTRATION REPORT AND RUNBOOK [8 MARKS]

Prepare one professional report per group, written in formal language, as the handover pack you would give the client so that the next administrator can run the server without calling you. The report shall include:

- **Cover page** with the company name, group number, all members' names, Student and Registration numbers, roles, and the server hostname.
- **Executive Summary** of one page, written so that the Managing Director, who is not technical, understands what has been delivered.
- **The Work Order Decoded:** the Managing Director's note restated as numbered technical requirements, each mapped to the task that meets it.
- **The Environment as Built:** the virtual machine, network, storage layout, directory and permission design, services and scheduled jobs, with at least one simple diagram.
- **Tasks 1 to 10:** one section per task stating what was built, the evidence, and the reasoning behind your choices.
- **Problems and Solutions:** at least five genuine problems met during the project and how you solved them.
- **Recommendations:** three things you would change if the company grew to 150 staff across both sites, with reasons.
- **References** for every source you used, in a consistent referencing style.

Appendices (required):

- **Appendix A: Administrator's Runbook**, with step-by-step instructions in plain language for five routine jobs: add a new staff member with the right access; remove a staff member who has left; restore a file deleted yesterday; check that last night's backup ran; and respond to “the disk is full”. Written so that someone who has never seen your server could follow it.
- **Appendix B:** the completed support ticket from Task 10.
- **Appendix C:** the acceptance test checklist, listing every requirement, the test, the expected result, the actual result, and pass or fail.
- **Appendix D:** the roles and task allocation table (Section D), signed by every member.

Marks in Section B are awarded for completeness and organisation, the quality of explanation and reasoning, the usefulness of the runbook, and professional presentation and referencing.

SECTION C: PRESENTATION AND DEFENCE [12 MARKS]

After the final submission, each group shall present its work to the course examiners, who will act as the Managing Director and the Board of Mpanga Valley Coffee Exporters Ltd. The presentation schedule will be communicated on MUBSEP. Prepare a short slide deck and agree in advance who presents each part.

(a) **Presentation and live demonstration (6 marks, group mark).** In about fifteen minutes, present the client's requirements, the environment as built and the most important design decisions. Then demonstrate the live server, imported from your exported appliance file, using your own acceptance test checklist. The examiners will choose which tests are run. A requirement only counts as delivered if it passes in front of the client.

(b) **Individual oral defence (6 marks, individual mark).** Each member will be questioned individually on any task, not only the tasks they led, and may be asked to carry out a short administrative action on the live server. Marks in this part are awarded to each member separately, according to how well that member explains and defends the work.

A member who does not attend the presentation and defence scores zero.

SECTION D: TEAM ROLES AND DIVIDING THE WORK

Organise your group as an IT support team. Each member must take one of the roles below; in a group of more than five, roles may be shared. Rotate the roles from Coursework Two, so that whoever led the Windows domain build does not lead the Linux installation. Every member must lead at least two tasks and assist on the others.

Role	**Main responsibilities**
Team Leader / Project Manager	Plans the work, keeps the task allocation table, approves changes together with one other member, and coordinates the report and presentation.
Systems Administrator	Installation, initial configuration, software and package management, and services.
Network Administrator	Network configuration, remote access and firewall.
Security and Access Administrator	Users, groups, administrative rights, password policy, permissions and SSH hardening.
Storage, Backup and Documentation Officer	Logical volumes, backup and restore, logs, the runbook and the acceptance test checklist.

Include the following table, completed and signed by every member, as Appendix D of the report. In the field, no change to a live server is approved by the person making it.

Task	**Led by**	**Assisted by**	**Signature**
1. Installation and initial configuration			
2. Network configuration and remote access			
3. Users, groups and administrative rights			
4. Storage management			
5. File system structure and permissions			
6. Software and package management			
7. Services and process management			
8. Scheduled backup, restore and logs			
9. Server security hardening			
10. Fault ticket and handover			
Report, runbook and presentation			

~ END ~