Important Instructions:

Objective:

This assessment is designed to evaluate your understanding of Linux system administration concepts through multiple-choice questions (MCQ) and scenario-based questions.

Assessment Structure:

- **MCQ Section**:
  - Total Questions: 30
  - Marks per Question: 2
  - Total Marks: 60
- **Scenario-Based Questions**:
  - Total Questions: 7
  - Marks per Question: Varies
  - Total Marks: 40 (4 questions out of 7)

Assessment Format:

- **MCQ Section**:
  - The MCQ section will be conducted on Quizizz platform. Link:
  - Access link will be provided during the assessment session.
  - Answer all questions within the stipulated time.
- **Scenario-Based Questions**:
  - Attempt any 4 out of 7 scenario-based questions.
  - Write your responses in a document or PDF format.
  - Include your name and registration number on the document.
  - Upload the document to the provided Google Form link:

Time Allocation:

- Total Time: 90 Minutes
  - MCQ Section: 30 Minutes
  - Scenario-Based Questions: 40 Minutes
  - Document preparation and uploading: 20 Minutes

Instructions:

1. **MCQ Section**:
   - Access the Quizizz link provided.
   - Answer all 30 multiple-choice questions within 30 minutes.

- Ensure you submit your responses before the time elapses.

2. **Scenario-Based Questions**:
   - Choose any 4 out of 7 scenario-based questions.
   - Read each scenario carefully and provide concise and accurate responses.
   - Write your responses in a document or PDF format.
   - Include your name and registration number at the top of the document.
   - Ensure your answers are well-organized and clearly written.
   - Upload the document to the provided Google Form link within last 20 minutes.
3. **Submission**:
   - Submit the document containing your responses to the scenario-based questions via the provided Google Form link.
   - Ensure the document is uploaded before the end of the assessment.
4. **Note**:
   - Follow the assessment guidelines carefully.
   - Manage your time efficiently to attempt all sections within the allocated time.
   - Contact the invigilator in case of any technical issues or clarifications.

Best of Luck!

Set A

Task 1: Log on to host1 as user1 and execute the logname, whoami, who, and w commands one at a time. Verify the identity of user1 by comparing the output of these commands. The output should show user1 as the user logged on and running these commands. Execute the id and groups commands and verify the identity of user1 by comparing the output of these commands. Identify the additional information that the id command provides but not the groups command. Record your results in a text file created with the vi editor in user1's home directory.

Task 2: Create sets of empty practice files to use in this lab. If you do not immediately recognize the intended shell expansion shortcut, then use the solution to learn and practice. Use shell tab completion to locate file path names. Create 12 files with tv_seasonX_episodeY.ogg names in the /home/student directory. Replace X with the season number and Y with that season's episode, for two seasons of six episodes each.

Task 3: Create a user account called user4000 with UID 4000, GID 5000, and home directory located in /usr. GID 5000 should be assigned to group lnxgrp. Assign this user a password and establish password aging attributes so that this user cannot change their password within 4 days after setting it, with a password validity of 30 days. This user should get warning messages for changing password for 7 days before their account is locked. This account needs to expire on the 20th of December, 2016.

Task 4: Collaborative Project Setup

Scenario:

Your company is launching a new product that requires close collaboration between the Marketing and Development teams. You, as the system administrator, need to ensure that

both teams have the necessary permissions to collaborate effectively without compromising security.

Characters:

- Neha (Marketing)
- Raj (Development)
- Marketing Group: marketing_team
- Development Group: development_team

Tasks:

A. Create user accounts for Neha and Raj.
B. Create groups for each department: marketing_team and development_team.
C. Add Neha to the marketing_team group and Raj to the development_team group.
D. Create a shared directory /projects/new_product where both groups can read and write files, but cannot delete files created by others.
E. Ensure the permissions are set so that new files created in /projects/new_product inherit the group of the directory.

Task 5: Setting Default File Permissions and umask

Scenario:

You need to ensure that new files created in a specific directory inherit a set of default permissions. Understanding how to set umask and default permissions ensures consistency and security in file management.

Tasks:

A. Create a directory named project_files in your home directory (/home/user).
B. Set default permissions (umask) so that new files created within project_files have read and write permissions for the owner and read-only permissions for others.
C. Create a new file named draft.txt within project_files and verify its permissions.
D. Explain how umask values (umask) are calculated and applied to new file creations in Linux.
E. Demonstrate how to change the umask temporarily and permanently, and explain the differences.

Task 6: Process Monitoring and Management Basics

Scenario:

As a system administrator, understanding how to monitor and manage Linux processes is essential for maintaining system performance and stability.

Tasks:

A. Use the ps command to list all running processes on your Linux system.
B. Identify the PID (Process ID) and PPID (Parent Process ID) of a specific process.
C. Use top or htop to monitor real-time CPU and memory usage.
D. Kill a process using its PID.
E. Verify that the process has been terminated.

Task 7: Creating and Managing User Accounts

Scenario:

As a system administrator, you need to create and manage user accounts on a Linux server to ensure secure access and effective resource management.

Tasks:

A. Create a new user account named sales_user with a home directory /home/sales_user.
B. Assign a default shell (/bin/bash) and set a password for sales_user.
C. Verify the creation of sales_user using grep command in /etc/passwd.
D. Modify the user account properties (passwd, usermod) to enforce password expiry in 90 days.
E. Explain the steps involved in deleting sales_user account and its home directory (userdel, rm -r).

Set B

Task 1: Log on to host1 as root and execute the date and timedatectl commands to check the current system date and time. Identify the differences between the two outputs. Use timedatectl and change the system date to a date in January of the following year. Issue the date command and change the system time to one hour ahead of the current time. Observe the new date and time with both commands. Reset the date and time back to the current actual time using either the date or the timedatectl command.

Task 2: Log on to host1 as root and execute the uptime command. Identify the amount of time the system has been up for and the number of users currently logged on. Run the wc command and show how many lines, words, and bytes are in the /etc/profile file

Task 3: Create a directory called project_plans in the Documents directory. The Documents directory is placed in the student user's home directory. Create two empty files in the project_plans directory called season1_project_plan.odf and season2_project_plan.odf

Task 4: Modify the GID from 5000 to 6000 for the lnxgrp group. Add users user1 and user2new as members, and user3 as the group administrator. Assign a group password and use the newgrp command as user4 to validate that the password is working. Change this group's name to dbagrp and verify.

Task 5: Managing Team Collaboration and Permissions

Scenario:

You are the system administrator for a company that has recently started a new project requiring collaboration between two departments: Sales and Engineering. You need to create user accounts for the new team members, set up appropriate groups, and ensure secure and efficient file sharing between the departments.

Characters:

- Ravi (Sales)
- Priya (Engineering)
- Sales Group: sales_team
- Engineering Group: engineering_team

Tasks:

A. Create user accounts for the new team members: ravi and priya.
B. Create groups for each department: sales_team and engineering_team.
C. Add ravi to the sales_team group and priya to the engineering_team group.

D. Create a shared directory /shared_project where both sales_team and engineering_team can read and write files but cannot delete files created by other users.
E. Ensure the permissions are set so that new files created in /shared_project inherit the group of the directory.

Task 6: Managing Special Permissions with setuid, setgid, and SGID

Scenario:

You are configuring executable files and directories with special permissions (setuid, setgid, and SGID). Understanding their usage ensures secure execution and effective group management in Linux.

Tasks:

A. Create a shell script named admin_script.sh in /usr/local/bin that requires superuser privileges.
B. Set the setuid bit on admin_script.sh so that it runs with root permissions.
C. Test the execution of admin_script.sh by a regular user and verify its effective permissions.
D. Create a directory named shared_data in /opt and assign ownership to admin user and data group.
E. Set the setgid bit on shared_data to ensure files created within inherit the group ownership of data.

Task 7: Monitoring System Resources and Process Activity

Scenario:

As a system administrator, you need to monitor system resources and analyze process activity to ensure optimal performance and troubleshoot any issues.

Tasks:

A. Use the top command to display real-time information about CPU and memory usage.
B. Identify the top three processes consuming the most CPU and memory.
C. Use ps command options (ps aux) to list all processes and their details.

D. Filter and display only the processes owned by a specific user (username).
E. Analyze the output of top and ps commands to identify any processes causing high resource utilization.

Set C

Task 1: Implementing Sticky Bit and Special Permissions

Scenario:

You are configuring a shared directory where multiple users will upload files. Understanding and applying special permissions like the sticky bit is crucial to ensure file integrity and prevent unauthorized deletion.

Tasks:

A. Create a directory named uploads in the root (/) directory.
B. Set permissions so that all users can read and write files within uploads, but only the file owner can delete their own files.
C. Apply the sticky bit to uploads to enforce the above permissions.
D. Create user accounts user1 and user2.
E. Test the permissions by having user1 upload a file and verifying user2 cannot delete it.

Task 2: Managing Process Priorities with nice and renice

Scenario:

You need to manage process priorities to optimize system performance and resource allocation using nice and renice commands.

Tasks:

A. Use ps command to list all running processes and identify the PID of a specific process.
B. Launch a CPU-intensive process with increased priority using nice command (nice -n -10 ./cpu_intensive_process).
C. Verify the priority of the process using ps -o pid,ni,args to confirm the adjusted nice value.
D. Use renice command to change the priority of an existing process (renice +5 -p PID).

E. Monitor the CPU utilization and scheduling priority of adjusted processes using top or ps commands.

Task 3: Managing Group Memberships

Scenario:

You need to manage group memberships and permissions on a Linux server to facilitate collaboration and resource sharing among users.

Tasks:

A. Create a new group named finance_team using groupadd command.
B. Add users user1, user2, and user3 to finance_team group using usermod -aG.
C. Verify group memberships of user1 using id command and explain the output.
D. Modify group properties (groupmod) to set a unique Group ID (GID) for finance_team.
E. Remove user3 from finance_team group and verify using id command.

Task 4: Create a two-level directory hierarchy with a single command to organize the mystery book chapters. Create the my_bestseller subdirectory under the Documents directory, and create the chapters subdirectory under the new my_bestseller directory. Create three more subdirectories directly under the my_bestseller directory with a single command. Name these subdirectories editor, changes, and vacation. You do not need to use the mkdir -p command to create parents because the my_bestseller parent directory exists.

Task 5: Open two terminal sessions on host1 as root. Run the system-config-users command on one of the terminals. Run a command on the other terminal to determine the PID and the nice value of the system-config-users command. Stop system-config-users on the first terminal and re-run it at a lower priority of +8. Confirm the new nice value of the process by running the appropriate command on the second terminal. Execute the renice command on the second terminal and increase the priority of the system-config-users process to –10, and validate.

Task 6: Setting Password Policies and Restrictions

Scenario:

You need to enforce password policies and restrictions for user accounts on a Linux server to enhance security and compliance.

Tasks:

A. Review existing password policies (/etc/login.defs) and identify default settings for password length, complexity, and expiration.

B. Modify password policy settings (chage, passwd) to enforce minimum password length of 8 characters and require complexity (letters, numbers, symbols).
C. Force password change (passwd -e) for user user1 to ensure compliance with updated password policies.
D. Implement password aging (chage) to enforce password expiry in 90 days for user2.
E. Verify password policies and aging settings (chage -l user1, chage -l user2) for user1 and user2.

Task 7: Utilizing apropos Command

Scenario:

You need to efficiently search and locate relevant command descriptions and manuals using apropos command in Red Hat Enterprise Linux.

Tasks:

A. Use apropos file permissions command to search for commands related to file permissions management.
B. Identify and explain at least three commands (chmod, chown, chgrp) listed in apropos file permissions output.
C. Explore additional options (-r, -e) available in apropos command to refine search results based on command names and descriptions.
D. Compare the search results obtained from apropos file permissions with similar search using man -k command. Highlight differences in search scope and results.
E. Demonstrate how to access detailed documentation for chmod command using man command after finding it through apropos search.

Set D

Task 1: Understanding File Ownership and Permissions

Scenario:

You are tasked with managing file permissions on a Linux server used by multiple departments. Understanding how ownership and permissions work is crucial for ensuring data security and accessibility.

Tasks:

A. Create a file named confidential.txt in your home directory (/home/user) with sensitive information.
B. Set the permissions so that only your user (user) can read and write to confidential.txt.
C. Create a new user account named guest.
D. Allow guest to read the contents of confidential.txt without modifying it.
E. Verify the permissions of confidential.txt and explain the output.

Task 2: Analyzing Process Dependencies with pstree

Scenario:

You need to visualize and analyze process dependencies and hierarchies using pstree command in Linux.

Tasks:

A. Use pstree command without options to display a hierarchical tree of all processes.
B. Limit the output of pstree to a specific process and its child processes (pstree -p PID).
C. Display process command-line arguments (pstree -a) to identify executed commands within process hierarchies.
D. Analyze process relationships and dependencies using pstree -c and pstree -h options.
E. Compare pstree output with ps or top command results to understand process relationships.

Task 3: Setting and Managing File Permissions

Scenario:

You need to configure file permissions for sensitive data files on a Linux server to restrict access based on user roles and requirements.

Tasks:

A. Create a directory named sensitive_data in /home/user with read and write permissions for the owner (user) only.
B. Add a new user manager to the system and grant read-only access to sensitive_data directory.
C. Ensure no other users can access or modify files within sensitive_data.
D. Use ls -l command to verify and explain the permissions set for sensitive_data.

Task 4: Accessing Red Hat Documentation Portal

Scenario:

You need to access comprehensive Red Hat Enterprise Linux documentation and resources online to find solutions and troubleshooting tips.

Tasks:

A. Open a web browser and navigate to the official Red Hat documentation portal (https://access.redhat.com/documentation).
B. Explore different categories (e.g., Installation, Administration, Security) available in Red Hat documentation.
C. Search for troubleshooting steps related to network configuration issues using the search functionality on Red Hat documentation portal.
D. Identify and bookmark relevant articles or guides that provide solutions to common Linux administration tasks or issues.
E. Discuss the advantages of using official Red Hat documentation portal for accessing up-to-date information and community resources.

Task 5: Create sets of empty practice files to use in this lab. If you do not immediately recognize the intended shell expansion shortcut, then use the solution to learn and practice. Use shell tab completion to locate file path names. Create 12 files with tv_seasonX_episodeY.ogg names in the /home/student directory. Replace X with the season number and Y with that season's episode, for two seasons of six episodes each.

Task 6: Log on to host1 as root and create directory /shared_dir1. Create a group called shared_grp and assign user1000 and user2000 to it (create these users if they do not already

exist). Set up appropriate ownership, group membership, and permissions on the directory to support group collaboration.

Task 7: File and Directory Management

Scenario:

You are tasked with familiarizing yourself with basic file and directory management commands in Linux.

Tasks:

A. Create a directory named lab_files in your home directory (/home/user).
B. Navigate into lab_files directory and create three subdirectories named docs, images, and code.
C. Create a file named notes.txt inside docs directory. Add some sample text using a command-line text editor (nano or vim).
D. Use cp command to create a copy of notes.txt in code directory named notes_backup.txt.
E. Rename notes.txt to important_notes.txt using mv command.
F. Use ls command to list the contents of lab_files/docs directory.
G. Display detailed information about important_notes.txt using ls -l command.
H. View the contents of important_notes.txt file using cat or less command.

SET E

1. You need to organize and manage a directory structure for a new project. Perform the following tasks:

A. Create a directory structure /projects/alpha/{src,bin,doc}.
B. Move all .c files from /tmp/code/ to /projects/alpha/src/.
C. Find all .log files in /var/log that are older than 30 days and delete them.
D. Create a hard link to /projects/alpha/src/main.c in /projects/alpha/bin/.
E. Create a symbolic link named project_docs in your home directory that points to /projects/alpha/doc.

2. You need to set up user accounts and groups for a new department. Perform the following tasks:

A. Create a group named devops.
B. Add users alice, bob, and charlie with the home directory /home/devops/ and default shell /bin/bash.
C. Add alice and bob to the devops group.
D. Create a shared directory /srv/devops/ and set the appropriate permissions so that only members of the devops group can read, write, and execute.
E. Use chage to set a password expiration of 90 days for the user charlie. If you are not familiar to chage then do it in another way.

3. You need to manage permissions and access for a team working on a critical project. Perform the following tasks:

A. Create a group named `critical_project`.
B. Add users `john`, `doe`, and `jane` with the home directory `/home/critical/` and default shell `/bin/bash`.
C. Add `john` and `jane` to the `critical_project` group.
D. Create a directory `/srv/critical_project/` and set permissions so that only the `critical_project` group has full access.
E. Give read access to the user `auditor` on `/srv/critical_project/`.

4. You need to set up user accounts and groups for a development team. Perform the following tasks:

A. Create a group named `developers`.
B. Add users `alice`, `bob`, and `charlie` with the home directory `/home/developers/` and default shell `/bin/bash`.
C. Add `alice` and `bob` to the `developers` group.
D. Create a shared directory `/srv/developers/` and set permissions so only the `developers` group has full access.
E. Set a password expiration policy of 60 days for all users in the `developers` group.

5. You need to ensure the smooth operation of a critical application named `app_service` on a Linux server. Perform the following tasks to monitor and manage its processes effectively.

A. Identify the process ID (PID) of `app_service`.
B. Monitor the CPU and memory usage of `app_service` in real-time.
C. Log the CPU and memory usage of `app_service` every minute to `/var/log/app_service_usage.log`.
D. Change the priority of the `app_service` process to a higher priority (lower nice value).
E. Ensure that the priority change persists across reboots.

6. You are a system administrator for a company called SecureFiles Inc. You need to manage file and directory permissions to ensure proper access control and security. Perform the following tasks related to file-system permissions and ownership.

Tasks:

A. List the permissions of the file `/srv/data/report.txt`.
B. Explain what the current permissions mean for the owner, group, and others.
C. List the permissions of the directory `/srv/data/` and interpret what they mean for accessing files within this directory.
D. Change the permissions of `/srv/data/report.txt` to `rw-r-----`.
E. Change the ownership of `/srv/data/report.txt` to user `john` and group `data_team`.
F. Set the permissions of the directory `/srv/data/` so that the owner has full access, the group has read and execute access, and others have no access.
G. Configure the default permissions for new files created by user `jane` to be `rw-r-----`.
H. Explain the effect of the `umask` setting in achieving the above default permissions.

7. You have been hired as a system administrator for TechSolutions Inc. Your tasks involve managing user and group accounts on the company's Linux servers to ensure secure and organized access. Perform the following tasks related to user and group management.

Tasks:

A. Create a new user named mike with the home directory /home/mike/ and default shell /bin/bash.
B. Set a password for the user mike.
C. Delete the user mike and remove their home directory.
D. Create a group named project_team.
E. Add users mike and jane to the project_team group.
F. Modify the project_team group to include the user developer.
G. Delete the group old_team.
H. Set a password expiration policy of 30 days for all users.
I. Lock the user account suspended_user.
J. Unlock the user account inactive_user.