Assignment-2 Linux

Format:Lab Session

Time:90 mins

Instruction:

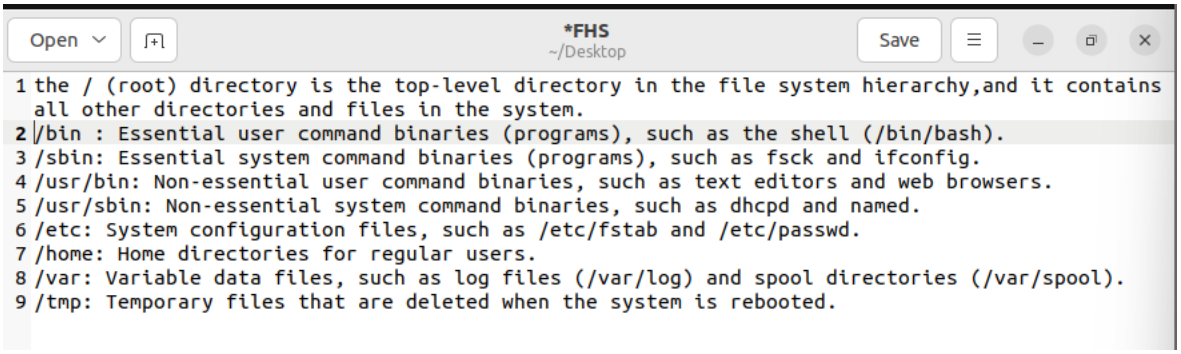
1.Complete the assignment and also upload the solutions in your Git repo

2.Take screenshot of the solution and paste it in word document

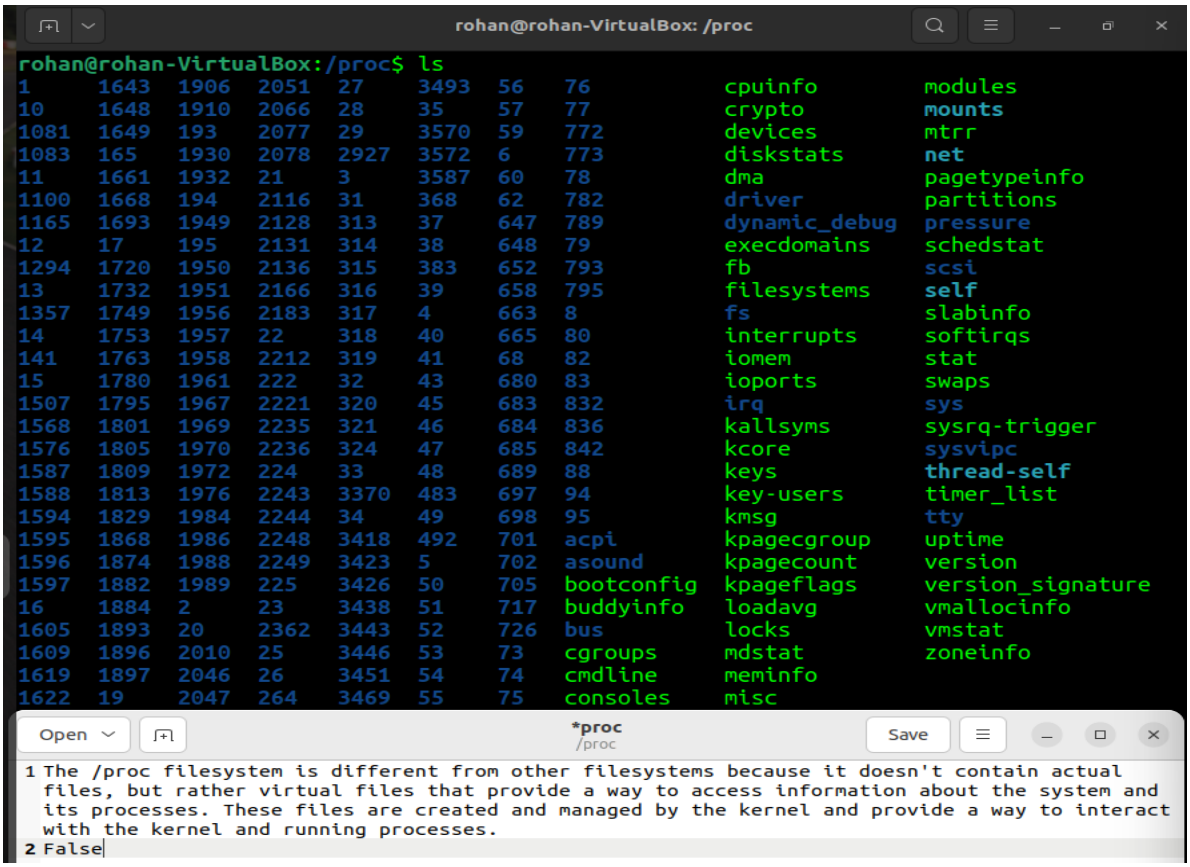
3.Convert the word doc into pdf before uploading.

1. In Linux FHS (Filesystem Hierarchy Standard) what is the /?
2. What is stored in each of the following paths?
   /bin, /sbin, /usr/bin and /usr/sbin
   /etc
   /home
   /var
   /tmp

3. What is special about the /tmp directory when compared to other directories



4. What kind of information one can find in /proc?
5. What makes /proc different from other filesystems?
6. True or False? only root can create files in /proc
7. What can be found in /proc/cmdline?



8. In which path can you find the system devices (e.g. block storage)?
   System devices (e.g. block storage) can be found in the /dev directory. This directory contains device files that represent physical and logical devices attached to the system, such as hard drives, USB drives, and network interfaces.

Permissions

9. How to change the permissions of a file?
   chmod 755 <file name>
10. What does the following permissions mean?:
    777: **full (read, write, and execute) permissions for all**
    644: **read and write permissions, but not execute**
    750: **full (read, write, and execute) permissions for owener not for users**
11. What this command does? chmod +x some_file
    The command chmod +x some_file adds the execute permission to the file some_file. This makes it possible to execute the file as a

program, either by running it directly (./some_file) or by including it in a script.

12. Explain what is setgid and setuid

setgid and setuid are special permissions that can be applied to executable files. When a file is setgid, it means that any user who runs the file will be given the same group ownership as the file's group owner. When a file is setuid, it means that any user who runs the file will be given the same user ownership as the file's owner.

13. What is the purpose of sticky bit?

The purpose of the sticky bit is to prevent users from deleting or renaming files that they don't own in a shared directory. When the sticky bit is set on a directory, only the owner of a file can delete or rename it, even if other users have write permissions on the directory.

14. What the following commands do?

Chmod: **is used to change the permissions of a file or directory**

Chown: **command is used to change the ownership of a file or directory**

Chgrp: **command is used to change the group ownership of a file or directory.**

15. What is sudo? How do you set it up?

sudo is a command that allows users to run commands as another user, typically the root user, without having to log in as that user. To set up sudo, you need to add the user to the sudo group and edit the sudoers file to grant the user the appropriate permissions.

16. True or False? In order to install packages on the system one must be the root user or use the sudo command

True, in order to install packages on the system, you need to be the root user or use the sudo command to gain temporary root access.

17. Explain what are ACLs. For what use cases would you recommend to use them?

ACLs (Access Control Lists) are a way of providing more fine-grained control over file and directory permissions. They allow you to set permissions for specific users or groups beyond the standard owner, group, and others. ACLs are useful for scenarios where you need to

provide access to a file or directory for a specific user or group without changing the overall ownership or permissions of the file or directory.

18. You try to create a file but it fails. Name at least three different reason as to why it could happen

    There are several reasons why creating a file could fail in Linux:Insufficient permissions: If you don't have the necessary permissions to create a file in a particular directory, the operation will fail.

    Disk space: If the disk is full or there isn't enough space

19. A user accidentally executed the following chmod -x $(which chmod). How to fix it?

Scenarios

20. You would like to copy a file to a remote Linux host. How would you do?

    scp /path/to/local/file username@remotehost:/path/to/remote/directory/

21. How to generate a random string?

    openssl rand -hex 4

22. How to generate a random string of 7 characters?

    openssl rand -base64 5|cut -c1-7

Systemd

23. What is systemd?

    Systemd is a system and service manager for Linux operating systems. It is responsible for managing the system's startup and shutdown processes, as well as the management of services, sockets, and other system resources. Systemd is now widely adopted by most modern Linux distributions as the default init system.

24. How to start or stop a service?

    sudo systemctl start <service-name>

    sudo systemctl stop <service-name>

25. How to check the status of a service?

    sudo systemctl status <service-name>

26. On a system which uses systemd, how would you display the logs?

sudo journalctl -u sshd

27. Describe how to make a certain process/app a service

[Unit]
Description=My Python Script

[Service]
ExecStart=/usr/bin/python /path/to/my/script.py
Restart=always

[Install]
WantedBy=multi-user.target

28. Troubleshooting and Debugging

Troubleshooting and debugging can involve a variety of techniques, depending on the specific issue you are trying to resolve. Some general strategies include reviewing system and application logs, testing network connectivity and performance, using diagnostic tools like ping and traceroute, and analyzing system resource usage.

29. Where system logs are located?

System logs are typically located in the /var/log directory on Linux and Unix systems. The specific log files may vary depending on the system and applications installed, but common logs include syslog, auth.log, and messages.

30. How to follow file's content as it being appended without opening the file every time?

sudo tail -f /var/log/syslog

31. What are you using for troubleshooting and debugging network issues?

For troubleshooting and debugging network issues, there are many tools and utilities available, including ping, traceroute, netstat, tcpdump, and Wireshark. These tools can be used to test network connectivity, identify network errors, and analyze network traffic.

32. What are you using for troubleshooting and debugging disk & file system issues?

For troubleshooting and debugging disk and file system issues, there are several tools and commands available, including fsck, df, du, and

lsblk. These tools can be used to check and repair file system errors, monitor disk usage, and view disk and partition information

33. What are you using for troubleshooting and debugging process issues?

For troubleshooting and debugging process issues, you can use tools like ps, top, htop, and lsof. These tools can be used to view running processes, monitor system resource usage, and identify process-specific issues like file locks or memory leaks.

34. What are you using for debugging CPU related issues?

For debugging CPU-related issues, you can use performance monitoring tools like top, htop, vmstat, iostat, and sar. These tools can be used to view CPU usage, monitor system resource usage, and identify processes that are using excessive CPU resources

35. You get a call from someone claiming "my system is SLOW". What do you do?

When someone reports that their system is slow, you should start by gathering more information about the system and the specific issue they are experiencing. You can ask questions to determine when the system started running slow, what specific tasks are slow, and whether any error messages or warnings have been displayed. You can also check system resource usage and review system logs to look for potential issues.

36. Explain iostat output

The iostat command is a performance monitoring

37. How to debug binaries?

To debug binaries, you can use tools like gdb (GNU Debugger) or strace. gdb allows you to inspect and manipulate the state of a running process or binary, while strace allows you to trace system calls and signals made by a process or binary.

38. What is the difference between CPU load and utilization?

CPU load and CPU utilization are related concepts but have different meanings. CPU load refers to the amount of work that is waiting to be processed by the CPU, while CPU utilization refers to the percentage of time that the CPU is actively processing work. CPU load is typically measured as a decimal value between 0 and 1, where 1

represents a fully utilized CPU, while CPU utilization is typically measured as a percentage of total CPU capacity.

39. How you measure time execution of a program?

time ls

Scenarios

40. You have a process writing to a file. You don't know which process exactly, you just know the path of the file. You would like to kill the process as it's no longer needed. How would you achieve it?

lsof /path/to/file
kill <pid>
pkill <process_name>

Kernel

41. What is a kernel, and what does it do?

The kernel is the core component of an operating system. It is responsible for managing system resources and providing a layer of abstraction between software and hardware. The kernel controls access to the computer's hardware and provides services such as process scheduling, memory management, and file system access.

42. How do you find out which Kernel version your system is using?

uname -r

43. What is a Linux kernel module and how do you load a new module?

sudo modprobe <module_name>

44. Explain user space vs. kernel space

User space and kernel space are two distinct areas of memory in an operating system. User space is where applications and user-level processes run, while kernel space is where the operating system's kernel and device drivers run. Access to kernel space is restricted to privileged users or processes, while user space can be accessed by any user-level process.

45. In what phases of kernel lifecycle, can you change its configuration?

The configuration of the kernel can be changed during different phases of its lifecycle. During the build process, the configuration can be modified to enable or disable certain features. Once the kernel is running, the configuration can be changed at runtime using tools such as sysctl.

46. Where can you find kernel's configuration?

The kernel configuration file can typically be found in the /boot directory on Linux systems. The filename usually begins with "config-" followed by the kernel version number.

47. Where can you find the file that contains the command passed to the boot loader to run the kernel?

The file that contains the command passed to the boot loader to run the kernel is typically located in the /boot directory and is named grub.cfg on systems that use the GRUB bootloader.

48. How to list kernel's runtime parameters?

sudo sysctl -a

49. Will running sysctl -a as a regular user vs. root, produce different result?

Yes, running sysctl -a as a regular user will produce a different result than running it as root. The non-root user will only be able to see a subset of the kernel parameters that are not restricted to privileged users.

50. You would like to enable IPv4 forwarding in the kernel, how would you do it?

sudo sysctl net.ipv4.ip_forward=1

51. How sysctl applies the changes to kernel's runtime parameters the moment you run sysctl command?

When you run the sysctl command to change a kernel runtime parameter, the change is applied immediately to the running kernel.

52. How changes to kernel runtime parameters persist? (applied even after reboot to the system for example)

Changes to kernel runtime parameters can persist in several ways, depending on the system. On many Linux systems, the parameters can be set in configuration files located in the /etc/sysctl.d/ directory. Alternatively, the parameters can be set in the /etc/sysctl.conf file. On other systems, the parameters may be set in startup scripts or other configuration files

53. Are the changes you make to kernel parameters in a container, affects also the kernel parameters of the host on which the container runs?

Changes you make to kernel parameters in a container only affect the kernel parameters of that container, not the kernel parameters of the host system. Each container has its own virtualized environment,

including its own kernel, so changes made within the container do not affect the host system.

SSH

54. What is SSH? How to check if a Linux server is running SSH?

systemctl status ssh

55. Why SSH is considered better than telnet?

SSH is considered better than telnet because it provides encrypted communication between the client and the server, whereas telnet sends all communication in plain text. This means that any sensitive information, such as passwords, can be intercepted and read by anyone who has access to the network traffic. SSH, on the other hand, encrypts all communication, making it much more secure.

56. What is stored in ~/.ssh/known_hosts?

The ~/.ssh/known_hosts file contains a list of known hosts and their public keys. When connecting to a host over SSH, the client verifies that the host's public key matches the one stored in the known_hosts file. If the key does not match, the client will warn the user that the connection may be insecure.

57. You try to ssh to a server and you get "Host key verification failed". What does it mean?

"Host key verification failed" means that the public key of the host you are trying to connect to does not match the one stored in your ~/.ssh/known_hosts file. This could be because the host's public key has changed, or because you are connecting to a different host than you intended. To fix this, you can remove the offending entry from the known_hosts file, or verify that you are connecting to the correct host.

58. What is the difference between SSH and SSL?

SSH and SSL (Secure Sockets Layer) are both protocols for secure communication over a network. SSH is primarily used for secure remote access to a computer, while SSL is used for securing web-based communication, such as HTTPS. While both protocols use encryption to provide secure communication, they are designed for different purposes and have different strengths and weaknesses.

59. What ssh-keygen is used for?

ssh-keygen is a command-line tool used to generate and manage SSH keys. SSH keys are used for authentication when connecting to a remote server over SSH. ssh-keygen can be used to generate a new key pair, view or change the passphrase on an existing key, or convert between different key formats.

60. What is SSH port forwarding?

SSH port forwarding (also known as SSH tunneling) is a technique for forwarding network traffic from one computer to another over an encrypted SSH connection. This can be useful for securely accessing services on a remote server that are not exposed to the public internet, or for accessing services that are blocked by a firewall. With SSH port forwarding, you can create a secure tunnel between your computer and the remote server, and forward traffic through that tunnel to access the desired service.