Assignment-2 Linux

1.In Linux FHS (Filesystem Hierarchy Standard) what is the /?

In Linux FHS, the / (forward slash) represents the root directory of the file system. It is the top-level directory in the hierarchy, from which all other directories and files stem. The root directory contains all other directories and files in the file system and serves as the starting point for all directory paths in Linux.

2. What is stored in each of the following paths?

/bin, /sbin, /usr/bin and /usr/sbin

/etc

/home

/var

/tmp

/bin: Essential executable files for system operation.

/sbin: Essential executable files for system administration tasks.

/usr/bin: User-level applications.

/usr/sbin: System administration applications.

/etc: System configuration files.

/home: User home directories.

/var: Variable data files used by the system and its services.

/tmp: Temporary files created by various programs and services.

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

/tmp is a temporary storage directory.

It is publicly accessible.

It does not have subdirectories.

It is world-writable.

4.What kind of information one can find in /proc?

System information, including hardware configuration.

Process information, including process ID and memory usage.

System configuration, including network settings and kernel parameters.

Performance statistics, including CPU usage and memory usage.

Filesystem information, including filesystem type and usage statistics.

5. What makes /proc different from other filesystems?

/proc is a virtual filesystem.

Data in /proc is dynamically generated and updated.

/proc provides a file-based interface to system information.

Data in /proc is non-persistent and stored in memory.

/proc is specific to the Linux kernel.

6.True or False? only root can create files in /proc.False.

False. Any user or program can create files in the /proc directory.

7. What can be found in /proc/cmdline?

The /proc/cmdline file contains the command-line arguments that were passed to the Linux kernel at boot time, including the kernel version, boot options, hardware parameters, and init system.

8. In which path can you find the system devices (e.g. block storage)?

System devices, including block storage devices, can be found in the /dev directory as device files that provide an interface for interacting with the device driver and accessing the device's functionality.

Permissions

9. How to change the permissions of a file?

You can change the permissions of a file in Linux using the chmod command followed by the desired permission mode, which can be specified in either numeric or symbolic representation. The chmod command modifies the read, write, and execute permissions for the owner, group, and other users on the file.

10. What does the following permissions mean:

777

644

750

The file permissions 777 mean that the file has read, write, and execute permissions for the owner, group, and other users.

The file permissions 644 mean that the file has read and write permissions for the owner, and read-only permissions for the group and other users.

The file permissions 750 mean that the file has read, write, and execute permissions for the owner, read and execute permissions for the group, and no permissions for other users. It's important to use appropriate file permissions to ensure proper security and functionality.

11.What this command does? chmod +x some\_file.

The chmod +x some\_file command makes the file "some\_file" executable, allowing it to be run as a program or script.

12.Explain what is setgid and setuid?

setgid: When set on a directory, new files or directories created within that directory inherit the group ownership of the parent directory. This is useful for facilitating collaboration among users.

setuid: When set on an executable file, the program is executed with the privileges of the file owner. This is useful for allowing non-privileged users to execute privileged programs.

13. What is the purpose of sticky bit?

The purpose of the sticky bit is to restrict the deletion or renaming of files or directories within a shared directory, and to maintain the integrity of the shared directory by preventing accidental deletion or modification of shared files.

14. What the following commands do?

chmod

chown

Chgrp

chmod: Changes file or directory permissions.

chown: Changes file or directory ownership.

chgrp: Changes file or directory group ownership.

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

sudo is a command that allows users to run commands with elevated privileges, usually as the root user. To set up sudo, you need to install the sudo package if it is not already installed, edit the /etc/sudoers file to grant sudo access to users, and save the changes. Once set up, users can run a command with elevated privileges by prefixing the command with sudo.

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

True. To install packages on a system, administrative privileges are required. This can be achieved either by being the root user or by using the sudo command.

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

ACLs (Access Control Lists) are a security mechanism used to control access to resources. They provide a more granular level of control over who can access and modify resources by allowing administrators to set permissions for individual users or groups. ACLs are useful in environments where multiple users need varying levels of access to resources or in situations where compliance regulations require additional layers of security.

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 file creation may fail, including insufficient permissions to create the file in the directory or file system, a file with the same name already exists, and insufficient disk space on the file system or device. Other potential reasons include issues with file system or disk errors, restrictions set by the operating system, or issues with the application being used to create the file.

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

The command "chmod -x $(which chmod)" removes the execute permission from the chmod command, making it impossible to change file permissions using the chmod command in the future. To fix this, the user can either use a different system to run the chmod command with the correct permissions, use sudo to temporarily elevate privileges and change the permissions back, or contact their system administrator or IT department for assistance.

Scenarios

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

There are several ways to copy a file to a remote Linux host, including SCP, SFTP, and Rsync. SCP allows files to be securely copied between a local and remote host over an encrypted connection using a command-line utility. SFTP is a secure file transfer protocol that allows files to be transferred between hosts using an SFTP client. Rsync is a command-line utility that allows files to be efficiently copied between hosts, using compression to reduce the amount of data transferred. The method used will depend on the user's preferences and requirements.

21. How to generate a random string?

Using a built-in function: Many programming languages provide built-in functions to generate random strings. These functions usually take the length of the string as an argument and return a string consisting of random characters.

Using a third-party library: If your programming language doesn't provide a built-in function for generating random strings, you can use a third-party library that provides this functionality.

Rolling your own: If you want more control over the random string generation process, you can implement your own algorithm that generates a random string by selecting characters from a set of possible characters.

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

Import the random and string modules.

Define a function that takes a length argument.

Define a variable letters that contains the set of characters to choose from using string.ascii\_letters and string.digits.

Use a loop and the random.choice() function to randomly select characters from the letters set and append them to a result string.

Return the result string.

Call the function with an argument of 7 to generate a random string of 7 characters.

Systemd

23. What is systemd?

systemd is a system and service manager for Linux-based operating systems.

It manages the startup and shutdown of system services and maintains system state and configuration.

systemd replaces the traditional System V init system and introduces new features like parallel startup of services, socket and D-Bus activation, user sessions, and container integration.

It includes a built-in logging system called the Journal, which provides centralized logging and easy aggregation and analysis of system logs.

systemd has become the default system and service manager in many popular Linux distributions.

24.How to start or stop a service?

Determine the name of the service you want to start or stop.

Depending on your specific operating system and service manager, use the appropriate command to start or stop the service.

If using systemd: use systemctl start [service] to start and systemctl stop [service] to stop the service.

If using SysVinit: use service [service] start to start and service [service] stop to stop the service.

If using Upstart: use initctl start [service] to start and initctl stop [service] to stop the service.

Replace [service] with the name of the service you want to start or stop.

Note that the specific commands and service names may vary depending on your system configuration.

25.How to check the status of a service?

Determine the name of the service you want to check the status of.

Depending on your specific operating system and service manager, use the appropriate command to check the status of the service.

If using systemd: use systemctl status [service] to check the status of the service.

If using SysVinit: use service [service] status to check the status of the service.

If using Upstart: use initctl status [service] to check the status of the service.

Replace [service] with the name of the service you want to check the status of.

The output of the status command will show you whether the service is running or stopped, as well as any errors or warnings that may be related to the service.

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

Determine the name of the service you want to view logs for.

Use the journalctl command with the -u option followed by the name of the service to display the logs. For example, journalctl -u [service].service.

You can also use additional options to customize the output of the logs, such as -f to follow the logs in real-time or -n to limit the number of log entries displayed.

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

Determine the process or application you want to run as a service and its command or script.

Create a service unit file that specifies the details of the service, such as the command to start the process and any necessary configuration options.

Save the unit file in the appropriate directory for your system's service manager.

Reload the service manager to recognize the new service unit file.

Start the service using the appropriate command for your system.

Top of Form

28. Troubleshooting and Debugging.

Understand the problem and its symptoms before attempting to fix it.

Break the problem down into smaller parts to isolate the source of the problem.

Test potential solutions carefully and methodically.

Keep track of any changes made to the system during testing.

Collaborate with others if necessary to gain insights and expertise.

29.Where system logs are located?

The location of system logs can vary depending on the operating system and the logging system being used. Here are some common locations:

On Linux systems, system logs are typically located in the /var/log directory. For example, the syslog file contains messages from the system logger, and the auth.log file contains messages related to authentication and authorization.

On macOS systems, system logs are located in the /var/log directory as well. The system.log file contains messages from the system logger, and the authd.log file contains messages related to authentication and authorization.

On Windows systems, system logs are located in the Event Viewer. You can access the Event Viewer by searching for it in the Start menu or by running the eventvwr command in the Command Prompt.

It's worth noting that different applications and services may also have their own logs, which may be located in different directories or files. It's a good idea to consult the documentation for the specific application or service to determine the location of its logs.

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

To follow a file's content as it's being appended without opening the file every time, use the tail -f <filename> command in the terminal. This will display the last 10 lines of the file and continuously display any new lines appended to the file in real-time. You can exit the command using Ctrl+C. Use the -n option to specify the number of lines to display.

To follow a file's content as it's being appended without opening the file every time, use the **tail -f <filename>** command in the terminal. This will display the last 10 lines of the file and continuously display any new lines appended to the file in real-time. You can exit the command using **Ctrl+C**. Use the **-n** option to specify the number of lines to display.

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

Some commonly used tools for troubleshooting and debugging network issues in Linux are ping, traceroute, netstat, tcpdump, wireshark, and dig.

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

Some commonly used tools for troubleshooting and debugging disk and file system issues in Linux are fsck, smartctl, lsof, mount, and df.

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

Some commonly used tools for troubleshooting and debugging process issues in Linux are ps, top, kill, strace, and lsof.

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

Some commonly used tools for debugging CPU related issues in Linux are top, htop, mpstat, iostat, perf, and sar.

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

Verify that the system is indeed slow by checking system resource utilization, using tools like top, htop, or sar.

Check the system logs for any error messages or warnings that could indicate a problem.

Check the network connectivity using tools like ping, traceroute, or netstat, in case the issue is network-related.

Check disk and file system usage and performance using tools like df, du, or iostat.

Check running processes and services using tools like ps or systemctl, to identify any processes that are using excessive resources.

If the issue is related to a specific application, try restarting the application or checking its logs for errors.

If all else fails, consider hardware troubleshooting and diagnostics.

36.Explain iostat output

The output of iostat includes the following columns:

Device: The name of the device or partition being monitored.

tps: The number of I/O transactions per second that have been issued to the device.

kB\_read/s: The amount of data in kilobytes that has been read from the device per second.

kB\_wrtn/s: The amount of data in kilobytes that has been written to the device per second.

kB\_read: The total amount of data in kilobytes that has been read from the device since the system was started.

kB\_wrtn: The total amount of data in kilobytes that has been written to the device since the system was started.

%util: The percentage of time that the device is busy handling I/O requests.

37.How to debug binaries?

Using gdb: gdb is a command-line tool that can be used to debug binaries. It allows you to step through the code, set breakpoints, examine variables and memory, and more.

Using strace: strace is a tool that can be used to trace system calls and signals made by a process. It can be used to identify issues such as file access errors, network connectivity issues, and more.

Using ltrace: ltrace is a tool that can be used to trace library calls made by a process. It can be used to identify issues related to shared libraries or missing dependencies.

Using valgrind: valgrind is a tool that can be used to detect memory leaks and other memory-related issues in a binary.

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

CPU load refers to the number of processes that are waiting to be executed or waiting for I/O resources. It is typically expressed as a decimal value, with a load of 1.0 indicating that the system is fully utilized.

CPU utilization, on the other hand, refers to the percentage of time that the CPU is busy handling tasks. It is typically expressed as a percentage value.

39.How you measure time execution of a program?

Using the time command: The time command can be used to measure the execution time of a program. Simply precede the command with the time command, and it will display the total execution time, as well as CPU usage and other statistics.

Using the date command: The date command can be used to measure the execution time of a program by capturing the system time before and after the program execution and calculating the difference.

Using profiling tools: Profiling tools such as perf, gprof, or Valgrind can be used to measure the execution time of a program and identify performance bottlenecks.

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?

To kill a process that is writing to a file, you can follow these steps in Linux: Identify the process ID (PID) of the process writing to the file using the lsof command. For example: lsof /path/to/file Use the PID to send a signal to the process using the kill command. For example: kill PID If the process does not respond to the kill command, you can use the kill -9 command to force the process to terminate. For example: kill -9 PID

Kernal

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

The main function of the kernel is to act as an intermediary between the hardware and the software, managing hardware resources and providing services to software applications. The kernel also handles tasks such as process management, memory management, device drivers, file system management, and security.

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

uname -r command

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

A kernel module can be used to add support for new hardware, file systems, or network protocols, or to provide new system services and functions.

To load a new kernel module, follow these steps:

1.Check if the module is already installed: Run the command lsmod to list all the currently loaded modules on your system. You can check if the module you want to load is already present.

2.Install the module if needed: If the module is not installed, you need to install it using the package manager for your Linux distribution.

3.Load the module: Use the modprobe command to load the module into the kernel. For example, to load the nvidia module.

4.Verify the module is loaded: Run the lsmod command again to verify that the module has been loaded.

44.Explain user space vs. kernel space

Kernel SpaceUser Space

Kernels and OS core execute here.Normal program and applications softwares run here.

Its the core space of OS.It's a form of sand-boxing that restricts user processes to access OS kernel.

It has full access to all memory and machine hardware.It has limited access to memory and access kernel through system calls only.

It contains the page table for process, kernel data structure, threads, and kernel code etc. It contains the program code, data, stacks, and heap of the process.

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

During the compilation phase, you can customize the kernel configuration by selecting which features and modules to include or exclude. This is typically done using a configuration tool such as make menuconfig, make xconfig, or make defconfig. These tools allow you to enable or disable various kernel features, drivers, and subsystems, and to fine-tune the kernel's behavior and performance.

46.Where can you find kernel's configuration?

the kernel configuration is stored in a file called .config in the root directory of the kernel source tree. This file contains a list of configuration options and settings that were selected during the kernel compilation process.

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

On Linux, boot loader configuration files are typically located in the /boot directory and named grub.cfg or menu.lst. This file contains boot loader configuration information, such as command line options and parameters passed to the kernel at boot time.

48.How to list kernel's runtime parameters?

sysctl -a

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

Running sysctl -a as a normal user will only show kernel parameters that are readable by non-privileged users. Many kernel parameters require root privileges to read or modify. So running sysctl -a as a regular user may not show all parameters or their current values.

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

To enable IPv4 forwarding in the kernel, you can use the sysctl command to modify the net.ipv4.ip forward parameter.

Here are the steps to enable IPv4 forwarding in the kernel:

Open a terminal or command prompt as root or with sudo privileges.

Check the current value of the net.ipv4.ip forward parameter by running sysctl net.ipv4.ip\_forward

To enable IPv4 forwarding, set the value of the net.ipv4.ip\_forward parameter to 1 by running the following command sysctl -w net.ipv4.ip\_forward=1

Check if the value of the net.ipv4.ip\_forward parameter was changed to 1 by running the following command

sysctl net.ipv4.ip\_forward

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

When you run sysctl commands to change kernel parameters, the changes take effect immediately and affect the real-time behavior of your system.

The sysctl command uses the sysctl() system call to communicate with the kernel and change the value of specified kernel parameters. The kernel then updates the appropriate data structures and applies the new settings immediately.

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

•Identify the kernel parameter that you want to modify and its current value. You can use the sysctl command to view the current values of kernel parameters.

•Decide on the new value that you want to set for the parameter.

•Modify the appropriate configuration file in the /etc/sysctl.d directory or add the parameter to the /etc/sysctl.conf file. To modify an existing file, you can use a text editor such as vi or nano. To create a new file, you can use the touch command. For example, to set the net.ipv4.tcp\_syncookies parameter to 0, you can create a new file called /etc/sysctl.d/99-sysctl.conf

Save the changes to the file(s).

•To apply the changes immediately, run the sysctl command with the -p

•To verify that the changes have been applied, you can run the sysctl

•Finally, reboot the system to ensure that the changes persist across reboots. After the reboot, you can use the sysctl command to verify that the changes are still in effect.

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?

No, changes made to kernel settings inside the container do not affect the kernel settings of the server on which the container is running.

Containers run on the host OS and share the same kernel with the host. However, the kernel container view is isolated from the host view, and changes to the kernel settings inside the container only affect the kernel container view.

SSH

SSH

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

SSH is a network protocol used to securely connect to a server or remote computer. To check if Linux server is running SSH you can check if SSH service is running using systemctl command or check if port 22 is open and listening by use the netstat command. You can also try connecting to the server using an SSH client to see if the connection is successful.

55.Why SSH is considered better than telnet?

SSH is considered better than Telnet because it provides a secure and encrypted connection between the client and the server, supports stronger authentication methods, is available on a wide range of platforms, and provides additional functionality beyond remote command-line access. Telnet, on the other hand, sends all data in plain text, has limited support and compatibility with modern systems, and is limited to remote command-line access.

56.What is stored in ~/.ssh/known\_hosts?

~/.ssh/known\_hosts file contains a list of host keys for SSH servers that the user has connected to previously. When a user connects to an SSH server for the first time, the server's public key is added to the known\_hosts file. On subsequent connections, the client verifies the server's identity by checking the public key against the known\_hosts file.

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

In Linux, "Host key verification failed" error message means that the public key of the remote SSH server that you are trying to connect to does not match the key stored in your ~/.ssh/known\_hosts file.

This error can occur for a few reasons:

The SSH server's key has been regenerated since you last connected to it

You are connecting to a different server with the same IP address or hostname

Your known\_hosts file has been modified or corrupted

To resolve this issue, you can either remove the old key from your known\_hosts file or update the file with the new key. When connecting to a new SSH server for the first time, you should always verify the server's key fingerprint to ensure that you are connecting to the correct server.

58.What is the difference between SSH and SSL?

SSH (Secure Shell) is primarily used for secure remote login and command execution on a server. It provides strong authentication, encryption, and integrity protection, ensuring that communications between the client and server are secure and private.

SSL (Secure Sockets Layer), now commonly referred to as TLS (Transport Layer Security), is mainly used for securing web traffic between a web server and a web client (such as a browser). SSL/TLS provides secure communication over HTTP by encrypting the data in transit and verifying the server's identity using digital certificates.

59.What ssh-keygen is used for?

ssh-keygen is a command-line utility used to generate, manage, and manipulate public and private authentication keys for SSH (Secure Shell) protocol. It allows users to create key pairs, which consist of a private key and a public key. The private key is kept on the user's local machine, while the public key is added to the remote server's authorized\_keys file. This enables the user to authenticate to the remote server securely without entering a password.

ssh-keygen can also be used to convert keys between different formats, change the passphrase used to encrypt private keys, and perform other key-related tasks. It is a versatile tool that is widely used in Linux environments for secure remote access to servers and systems.

60.What is SSH port forwarding?

SSH port forwarding (also known as SSH tunneling) is a technique used to securely tunnel traffic from one networked device to another using the SSH protocol.

SSH port forwarding works by forwarding a TCP/IP port on the local machine to a port on a remote machine over an encrypted SSH connection. This allows users to securely access remote services that may not be directly accessible from their local network. For example, users can use SSH port forwarding to access a web server running on a remote machine, even if the web server is only listening on its local loopback interface.

Top of Form