Interview questions for Linux

1. What is the difference between Linux and Unix?

- Answer: Linux is an open-source operating system modelled on Unix, which is a proprietary OS. Linux is community-driven, while Unix is mostly vendor-specific like AIX or Solaris.

2. Explain the Linux file system hierarchy.

- Answer: The Linux file system follows a tree structure starting at / (root). Common directories include /home (user files), /bin (essential binaries), /etc (config files), /var (variable data), and /tmp (temporary files).

3. How do you check the current kernel version in Linux?

- Answer: uname -r

4. What are symbolic links, and how are they created?

- **Answer**: A symbolic link (symlink) is a shortcut that points to another file or directory. It's created using: **ln -s target link_name**

Commands

5. How do you find a specific word in a file or directory using a command?

- **Answer**: Use grep.

6. Explain the difference between find and locate.

- **Answer**:
    - find searches in real-time and can search by various criteria (name, size, date).
    - locate uses a pre-built database for faster searches but may not reflect recent changes.

7. What does the chmod command do? Explain file permissions in Linux.

- **Answer**: chmod changes file or directory permissions. Permissions include:
    - **r** (read), **w** (write), **x** (execute).

8. How do you check disk usage and free space on Linux?

- **Answer**: Use the following commands:
    - Disk usage: du -h

- Free space: df -h

9. Explain the use of grep, awk, and sed.

- **Answer**:
  - grep: Searches for patterns in text.
  - awk: Processes and analyzes text (fields and columns).
  - sed: Performs text transformation or substitution.

Networking

10. How do you check network connectivity using Linux commands?

- **Answer**: Use ping: ping -c 4 google.com

11. What does the netstat command do?

- **Answer**: It displays network connections, routing tables, and interface statistics.

12. How do you check the IP address of a Linux machine?

- **Answer**: Use the **ip addr show** or **ifconfig**

13. What is the difference between TCP and UDP?

- **Answer**:
  - **TCP**: Connection-oriented, reliable (e.g., HTTP, FTP).
  - **UDP**: Connectionless, faster but less reliable (e.g., DNS, video streaming).

14. How do you troubleshoot network connectivity issues?

- **Answer**: Steps include:
  - Check IP configuration: ip addr or ifconfig.
  - Check default gateway: ip route show.
  - Test DNS resolution: ping or dig.
  - Check firewall rules: iptables -L or ufw status.

15. What is the purpose of the /etc/hosts file?

- **Answer**: It maps hostnames to IP addresses locally before querying DNS.

16. What is a subnet mask, and why is it used?

- **Answer**: A subnet mask divides an IP address into a network and host portion. It determines which part of the IP address identifies the network and which part identifies the device in that network. For example, a subnet mask of 255.255.255.0 allows 256 IP addresses, with 254 usable for hosts.

17. What is the difference between a private and public IP address?

- **Answer**:
    - **Private IP**: Used within internal networks and not routable on the internet (e.g., 192.168.x.x, 10.x.x.x).
    - **Public IP**: Routable on the internet and used for external communications.

18. What is NAT, and how does it work?

- **Answer**: NAT (Network Address Translation) allows multiple devices on a private network to share a single public IP address for accessing the internet. It translates private IP addresses to a public one at the router level.

19. What is DNS, and how does it work?

- **Answer**: DNS (Domain Name System) resolves human-readable domain names (e.g., example.com) into IP addresses (e.g., 93.184.216.34). It works by querying DNS servers in a hierarchical manner, starting from the root server, then the TLD server, and finally the authoritative server.

20. What is the difference between IPv4 and IPv6?

- **Answer**:
    - **IPv4**: 32-bit addressing, supports ~4.3 billion addresses (e.g., 192.168.0.1).
    - **IPv6**: 128-bit addressing, supports a vastly larger address space, and includes features like built-in security (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

21. What is a firewall, and how does it work in Linux?

- **Answer**: A firewall controls incoming and outgoing traffic based on predefined rules. In Linux, tools like iptables or ufw are used to set firewall rules.

22. What is SSH, and how does it enhance security?

- **Answer**: SSH (Secure Shell) is a protocol for secure remote access to servers. It uses encryption to protect data and authentication mechanisms like password-based or key-based access.

23. How does a VPN work?

- **Answer**: A VPN (Virtual Private Network) creates an encrypted tunnel between a user's device and a remote server, ensuring secure data transmission and masking the user's IP address.

24. What is a VLAN, and why is it used?

- **Answer**: A VLAN (Virtual Local Area Network) divides a physical network into multiple logical networks, isolating traffic for better performance, security, and organization.

25. What are the differences between a router and a switch?

- **Answer**:
    - **Router**: Connects different networks and directs traffic between them.
    - **Switch**: Connects devices within the same network, forwarding traffic based on MAC addresses.

26. What is MTU, and how does it impact network performance?

- **Answer**: MTU (Maximum Transmission Unit) is the largest size of a data packet that can be sent in one frame. A mismatch in MTU can cause fragmentation or performance issues.

27. What is port forwarding, and when is it used?

- **Answer**: Port forwarding redirects incoming traffic from a specific port on a router to a device in a private network. It is used for hosting servers or accessing internal devices from outside the network.

28. What is the difference between HTTP and HTTPS?

- **Answer**:
    - **HTTP**: Transmits data in plaintext.
    - **HTTPS**: Uses SSL/TLS to encrypt data, ensuring secure communication.

29. How do you monitor network traffic on a Linux system?

- **Answer**: Use tools like tcpdump, wireshark, or nload to capture and analyze network packets.

30. What are common steps to troubleshoot network issues in Linux?

- **Answer**:
    1. Check the network interface status: ip link.
    2. Verify IP configuration: ip addr.
    3. Test connectivity: ping.
    4. Check routes: ip route.
    5. Investigate DNS resolution: dig or nslookup.
    6. Check firewall rules: iptables -L.