Q1: How would you find all files larger than 100MB in a directory and its subdirectories?

Answer: Use the find command: **find /path/to/directory -type f -size +100M**

Q7: How do you identify a process consuming high CPU?

Answer:

○ Sort by CPU usage by **pressing Shift + P.**

Q8: How do you monitor disk I/O in real-time?

Answer**: iostat -x 2**

Q10: How do you list all services and their statuses?

**Answer: systemctl list-units --type=service**

Q12: How do you check for unauthorized access attempts on your server?

**Answer: sudo cat /var/log/auth.log | grep "Failed password"**

Q16: How do you change the default shell for a user?

**Answer: sudo usermod -s /bin/ username**

**Verify with: cat /etc/passwd | grep username**

Q20: How do you find the top 10 largest files in a directory?

Answer**: find /path/to/dir -type f -exec du -h {} + | sort -rh | head -n 10**

Q21: How do you back up a directory using rsync?

Answer: **rsync -av /source/directory /destination/directory**

Q25: How do you check which kernel modules are currently loaded?

Answer: **lsmod**

Q27: How do you lock a user account?

**Answer: sudo passwd -l username**

Q34: How do you restart a Kubernetes pod?

**Answer: kubectl rollout restart deployment <deployment\_name>**

Q37: How do you check the open ports on a Linux server?

**Answer: sudo netstat -tuln**

**Or using ss: ss -tuln**

Q40: How do you remove a package along with its configuration files in Debian/Ubuntu?

**Answer: sudo apt-get purge <package\_name**>

Q41: How do you check for disk usage by each directory in the current path?

**Answer: du -sh \***

Q43: How do you find out which process is using the most memory?

**Answer: ps aux --sort=-%mem | head**

Q44: How do you monitor live network traffic on an interface?

Answer: **sudo tcpdump -i eth0**

Q48: How do you prevent a user from logging in via SSH?

● Answer: **Add the user to /etc/ssh/sshd\_config: DenyUsers username**

**Restart the SSH service: sudo systemctl restart sshd**

Q49: How do you find specific error messages in a log file?

**Answer: grep "ERROR" /var/log/syslog**

Q50: How do you monitor a log file in real-time?

Answer: **tail -f /var/log/syslog**

Q52: How do you remove a kernel module?

**Answer: sudo rmmod <module\_name>**

Q55: Write a script to print the number of files in a directory.

**Answer: #!/bin/**

**DIR=$1**

**if [ -d "$DIR" ]; then**

**echo "Number of files in $DIR: $(ls -1 $DIR | wc -l)"**

**else**

**echo "$DIR is not a directory."**

**fi**

Q56: How do you test if a specific port on a remote server is open?

**Answer: nc -zv <server\_ip> <port>**

Q58: How do you check which services are enabled to start at boot?

**Answer: systemctl list-unit-files --type=service | grep enabled**

Q59: How do you stop a service and ensure it doesn’t start at boot?

**Answer: sudo systemctl stop <service\_name>**

**sudo systemctl disable <service\_name>**

Q60: How do you check memory usage in Linux?

Answer**: free -m**

Q61: How do you identify zombie processes?

Answer: **ps aux | grep 'Z'**

Q62: Write a script to monitor disk usage and send an email alert if usage exceeds **80%.**

**Answer: #!/bin/**

**THRESHOLD=80**

**USAGE=$(df -h / | grep -v Filesystem | awk '{print $5}' | sed 's/%//')**

**if [ "$USAGE" -gt "$THRESHOLD" ]; then**

**echo "Disk usage is at ${USAGE}% on $(hostname)" | mail -s "Disk Usage Alert" user@example.com**

**fi**

Q66: How do you check for failed login attempts?

Answer**: sudo grep "Failed password" /var/log/auth.log**

Q67: How do you restrict a user to their home directory using SSH?

**● Answer: Edit /etc/ssh/sshd\_config: Match User username**

**ChrootDirectory /home/username**

**AllowTCPForwarding no**

**X11Forwarding no**

**Restart the SSH service: sudo systemctl restart sshd**

Q69: How do you schedule a daily backup with cron?

● Answer: **Edit the cron jobs: crontab -e**

**Add the job: 0 2 \* \* \* tar -czf /backup/$(date +\%F).tar.gz /data**

Q74: How do you update all installed packages on a CentOS system?

Answer: sudo yum update

Q79: How do you kill all processes owned by a specific user?

Answer: **sudo pkill -u <username>**

Q81: How do you monitor real-time I/O usage per process?

Answer: **iotop**

Q83: Write a script to automate user creation and password assignment.

**Answer: #!/bin/**

**USER=$1**

**PASS=$2**

**sudo useradd -m $USER**

**echo "$USER:$PASS" | sudo chpasswd**

**echo "User $USER created with the given password."**

Q86: How do you disable root login over SSH?

● Answer: **Edit the SSH configuration file: sudo vi /etc/ssh/sshd\_config**

**Update or add:**

**perl PermitRootLogin no**

**Restart the SSH service: sudo systemctl restart sshd**

Q87: How do you configure a Linux firewall to allow only HTTP and SSH traffic?

**Answer: sudo ufw allow ssh**

**sudo ufw allow http**

**sudo ufw enable**

Q88: How do you schedule a weekly backup of the /home directory?

● Answer: **Create a backup script: vi /usr/local/bin/backup.sh**

**Add: #!/bin/**

**tar -czf /backup/home\_$(date +%F).tar.gz /home**

**Make the script executable: chmod +x /usr/local/bin/backup.sh**

**Add to cron:**

**crontab -e**

Q93: How do you blacklist a kernel module?

● Answer: **Add the module name to /etc/modprobe.d/blacklist.conf:**

**echo "blacklist <module\_name>" | sudo tee -a /etc/modprobe.d/blacklist.conf**

**Regenerate the initramfs: sudo dracut -f**

Q99: How do you check the status of Kubernetes pods?

Answer: **kubectl get pods**

Q105: How do you monitor memory usage for a specific process?

Answer: **pmap <PID> | grep total**

Q106: How do you find the top 5 CPU-consuming processes?

Answer: **ps -eo pid,ppid,cmd,%mem,%cpu --sort=-%cpu | head -n 5**

Q109: How do you display disk usage for a specific directory in a human-readable format?

Answer: **du -sh /path/to/directory**

Q111: How do you enforce password expiration for a user?

Answer: **sudo chage -M 30 username**

Q112: How do you set up a firewall rule to block all incoming traffic except SSH?

Answer: **sudo ufw default deny incoming**

**sudo ufw allow ssh**

**sudo ufw enable**

Q113: How do you compress and back up a MySQL database?

Answer:

**mysqldump -u root -p database\_name | gzip > database\_backup.sql.gz**

Q125: How do you display the currently logged-in users?

Answer: **who**

Q127: How do you troubleshoot if a specific port is not accessible on a server?

● Answer: **Check if the service is running: sudo systemctl status <service\_name>**

**Verify if the port is open: sudo netstat -tuln | grep <port>**

**Check firewall rules: sudo ufw status**

**Test connectivity using telnet or nc: telnet <server\_ip> <port>**

**Inspect logs for errors in /var/log.**

Q129: How do you restart a service automatically if it crashes?

● Answer**: Create a systemd service file or edit an existing one: sudo vi /etc/systemd/system/<service\_name>.service**

**Add the following lines under [Service]: makefile Restart=always**

**RestartSec=5**

**Reload systemd and enable the service: sudo systemctl daemon-reload**

**sudo systemctl enable <service\_name>**

Q130: How do you check all processes owned by a specific user?

Answer**: ps -u <username>**

**Q133:** Write a script to check if a website is reachable.

**Answer: #!/bin/**

**WEBSITE=$1**

**if curl -Is $WEBSITE | grep "200 OK"; then**

**echo "$WEBSITE is reachable."**

**else**

**echo "$WEBSITE is not reachable."**

**fi**

Q134: Write a script to back up a directory and log the output.

**Answer: #!/bin/**

**DIR=$1**

**BACKUP\_DIR="/backup/$(date +%F)"**

**mkdir -p $BACKUP\_DIR**

**tar -czf $BACKUP\_DIR/backup.tar.gz $DIR > /var/log/backup.log 2>&1**

**echo "Backup completed. Log available at /var/log/backup.log."**

Q137**: How do you enable auditing on a file?**

**● Answer: Install auditd if not already available: sudo apt install auditd**

**Add a rule: sudo auditctl -w /path/to/file -p rwxa -k file\_audit**

**Check logs: sudo ausearch -k file\_audit**

Q138: How do you enable password-based SSH authentication?

**● Answer: Edit /etc/ssh/sshd\_config: PasswordAuthentication yes**

**Restart the SSH service: sudo systemctl restart sshd**

Q152: How do you capture network packets on a specific interface?

**Answer: sudo tcpdump -i eth0**

Q153: How do you list all active and inactive services?

Answer: **systemctl list-units --type=service**

Q154: How do you view the startup services and their statuses?

Answer: **sudo systemctl list-unit-files --type=service**

Q157: Write a script to count the number of users currently logged in.

**Answer: #!/bin/**

**echo "Number of logged-in users: $(who | wc -l)"**

Q167: How do you enable IP forwarding temporarily?

Answer: **sudo sysctl -w net.ipv4.ip\_forward=1**

Q180: How do you view the system logs of a specific service?

**Answer: journalctl -u <service\_name>**

Q183: Write a script to monitor a directory and log changes.

Answer: #!/bin/

inotifywait -m /path/to/directory -e create -e delete -e modify |

while read path action file; do

echo "[$(date)] $file was $action in $path" >> /var/log/dir\_changes.log

done

Q184: Write a script to send an email alert if a service is down.

**Answer: #!/bin/**

**SERVICE=nginx**

**if ! systemctl is-active --quiet $SERVICE; then**

**echo "$SERVICE is down on $(hostname)" | mail -s "Service Alert" admin@example.com**

**fi**

Q187: How do you configure SSH key-based authentication?

● Answer: **Generate a key pair: ssh-keygen -t rsa**

**Copy the public key to the remote server: ssh-copy-id user@remote\_server**

**Verify login: ssh user@remote\_server**

**Q188: How do you block an IP address using iptables?**

**Answer: sudo iptables -A INPUT -s <IP\_ADDRESS> -j DROP**

Q207: Write a script to find the largest file in a directory.

**Answer: #!/bin/**

**find $1 -type f -exec du -h {} + | sort -rh | head -n 1**

**Answer: sudo passwd -l <username>**

Q217: How do you view active IRQs in Linux?

**Answer: cat /proc/interrupts**

Q225: How do you display system architecture?

**Answer: uname -m**

Q226: How do you display the last reboot time of the system?

Answer: **who -b**

Q233: How do you configure a Linux server as a router?

● Answer: **Enable IP forwarding: sudo sysctl -w net.ipv4.ip\_forward=1**

**Make it persistent: echo "net.ipv4.ip\_forward=1" | sudo tee -a /etc/sysctl.conf**

**Add routing rules using iptables: sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**

Q234: How do you capture only HTTP traffic using tcpdump?

**Answer: sudo tcpdump -i eth0 port 80**

Q235: How do you set a process to run at a specific nice level permanently?

● Answer: **Use nice while starting the process: nice -n 10 <command>**

**Use renice for running processes: renice 10 -p <PID>**

Q236: How do you restart all failed services?

Answer: **sudo systemctl list-units --failed | awk '{print $1}' | xargs sudo systemctl restart**

Q237: How do you monitor real-time system statistics?

Answer: Use the dstat command: **dstat**

● It provides real-time statistics for CPU, memory, disk I/O, and more.

Q238: How do you monitor user activity on a Linux system?

Answer: **Use the w command: w**

● It shows logged-in users and their activity.

Q239: Write a script to list all files modified in the last 2 days.

**Answer: #!/bin/**

**find $1 -type f -mtime -2**

Q243: How do you list all open files by a specific process?

Answer**: lsof -p <PID>**

Q244: How do you block specific IP ranges using iptables?

Answer**: sudo iptables -A INPUT -m iprange --src-range 192.168.1.0-192.168.1.255 -j DROP**

Q247: How do you filter logs for a specific date range?

Answer: **awk '/2025-01-20/,/2025-01-21/' /var/log/syslog**

Q248: How do you monitor changes to a log file?

Answer**: Use tail with -f: tail -f /var/log/syslog**

Q249: How do you list all currently loaded kernel modules with their sizes?

Answer: **lsmod**

Q250: How do you remove a kernel module that’s in use?

● Answer: Identify dependent processes: **lsmod | grep <module\_name>**

**Stop dependent processes or unload dependencies first: sudo modprobe -r <module\_name>**