Interview Questions:

1. What is server hardening?

Reducing a server's attack surface by disabling unnecessary services, closing unused ports, enforcing strong authentication, and applying security patches.

2. What is UFW and how does it work?

- **UFW (Uncomplicated Firewall):** a simple frontend for iptables.
- Controls incoming/outgoing traffic via rules.
- Example: ufw allow 22/tcp, ufw enable.

3. Why disable root login in SSH?

- Prevents direct access to the most privileged account.
- Forces login with normal user + sudo (leaves logs).
- Reduces brute-force attack risk on root.

4. What is fail2ban used for?

- Monitors log files for failed login attempts.
- Blocks attacker IPs using firewall rules.
- Protects against brute-force (SSH, web, etc.).

5. How do you check for open ports on Linux?

- ss -tuln (modern).
- netstat -tuln (legacy).
- lsof -i (processes using ports).
- nmap localhost (scan externally).

6. What is key-based authentication?

- Uses **public/private key pair** for SSH.
- Public key on server, private key stays with user.
- Stronger than passwords, resistant to brute-force.

7. What are system services and how to manage them?

- Background processes (daemons) like SSH, Apache.
- Managed by systemd.
- Commands: systemctl start|stop|enable|status <service>.

8. How do you secure SSH?

- Disable root login.
- Use key-based authentication.
- Restrict users/groups.
- Allow only trusted IPs via firewall.
- Enable fail2ban + logging.

9. Why is patch management important?

- Fixes known vulnerabilities quickly.
- Reduces risk of exploitation.
- Ensures compliance, stability, and security.

10. How can you audit server security?

- Review logs (/var/log/).
- Check running services and open ports.
- Verify firewall rules.
- Test SSH configuration.

- Run vulnerability scans (Lynis, Nessus, OpenVAS).
- Ensure system is up to date.