🙏 राधे राधे 🙏

System Admin

1. What is system administration?
    - System administration is the process of maintaining and managing a computer system.
    - This includes the hardware, software, and network resources that make up a system.
    - System administrators are responsible for ensuring the system is available and functioning correctly, and they may also be responsible for providing training and support to users.
2. What are the skills of a system administrator?
    - They should be able to manage and configure networks, servers, and storage systems, and they should also be able to troubleshoot and resolve issues that may arise.
    - Additionally, system administrators should have strong communication and customer service skills to interact with users and other IT staff.
3. What is the role of a system administrator?
    - The sysadmin's responsibilities include ensuring that system hardware, software, and related procedures adhere to organizational values and that the system's availability, performance, and security are continuously maintained.
    - In larger organizations, system administrators typically work in teams responsible for different areas of the network, such as storage, security, or email.

Windows Admin

1. What do you know about the active directory in the system administration?
    - When talking about network security, one thing that matters is the centralized control of everything that the active directory can assure.
    - The information and settings related to the development are stored in the central database.
    - For example, The database might list 100 user accounts with details like each person's job title, phone number, and password.
2. What is group policy?
    - administrators can use group policy to control the working environment of users and computer accounts in an active directory.
    - It provides a central place for administrators to manage and configure operating systems, applications, and user settings. Using it properly enables you to increase the security of users' computers and help defend against insider and external threats.
3. What do forest, trees, and domain mean?
    - domain:

        - A domain is a logical group of network objects like computers, users, and devices with the same active directory database.
    - tree:
        - A tree is a collection of domains within a Microsoft active directory network in which each domain has exactly one parent, leading to a hierarchical tree structure.
    - forest:
        - A forest is a group of active directory trees.

4. What do you know about WINS servers?

    - WINS stands for Windows Internet Name Service.
    - This will allow the users to access resources by a computer name rather than an IP address.

5. What, according to you, could be the personal characteristics of a person administering a system?

    - System administrators face a variety of challenges. They are the problem solvers and coordinators. They understand a computer's software, hardware, and networks in-depth. Thus, they can instruct employees regarding technical issues. Their primary task is to monitor the system. They are able to keep track of the server performance and creative designs for computer systems and quickly arrange for replacement in case of any hardware failure.

6. Can you differentiate between firewall and antivirus?

    - Antivirus:
        - We use antivirus to protect the system from computer viruses.
        - When using your system, it actively monitors for any virus threats from different sources. If it finds any virus threats, it tries to clean or quarantine the virus and keeps your system and data safe.
    - Firewall:
        - a firewall protects your system from outside/intruder/hacker attacks.
        - firewall on your pc to protect yourself from unauthorized access.
        - It is either available in software or hardware form. If you have a single PC, the software firewall can do the work, but when you want to protect a large corporation, you have to install a hardware firewall to protect their system from such attacks.

7. What is a domain controller(DC)?

    - A domain controller (DC) is a windows-based computer system that is used for storing user account data in a central database.
    - The system administrator allows or denies users access to system resources, such as printers, documents, folders, network locations, etc.

8. what is the difference between FAT and NTFS?

FAT:

- There is no security when the user logs in locally.
- It usually supports file names with only 8 characters and does not support file compression.
- The partition and file size can be up to 4 GB, and there is no such security permission for file and folder levels.
- It doesn't support bad cluster mapping, so it is not very reliable.

NTFS:

- There is security for both the local and the remote users.
- It usually supports file names that have 255 characters.
- It supports file compression, and the partition size can be up to 16 exabytes.
- There is security for file and folder levels.
- It supports bad cluster mapping and transaction logging and is highly reliable.

9. Can you tell me what is loopback address and in what sense is it useful?

    - It is an address that sends outgoing signals back to the same computer for testing purposes.
    - It is managed entirely within the operating system so the client and the server process on a single system and can communicate. It is not physically connected to a network. It is useful because the loopback provides IT professionals with an interface to test the IP software without worrying about broken or corrupted drives or hardware.

10. What do you know about proxy servers?

    - It acts as the gateway between a local network (e.g., computers in a company) and a large-scale network (for ex: the internet).
    - By using this server, there is an increase in performance and security as it can be used to prevent employees from browsing inappropriate and distracting sites.

11. Can you tell us about the windows registry?

    - It is the collection of databases of configuration settings.
    - It stores important information like the location of programs, files, etc. If you don't understand what you are doing, you should not edit the Windows registry, or it will cause problems with the installed applications or the operating system.

12. What is the Sysvol Folder?

    - We can say that it is a type of shared folder that stores group policy information, or we can say that it contains public files of the domain controllers, and the domain users can access it.

13. What is the difference between a workgroup and a domain?

    - Workgroup:
        - a particular system has a collection of systems having their own rules and local users' logins.
        - Workgroups are like P2P networks

- domain:
  - The centralized authentication server, which is a collection of systems, tells what the rules are.
  - domains are like standard client/server relationships.

14. What can you tell us about the lightweight directory access protocol (LDAP)?

    - The LDAP (lightweight directory access protocol) is used to name the object in an AD (Active Directory) and makes it widely accessible for management and query applications. It is most commonly used to provide a central place to store the usernames and passwords.

15. What do you know about the PPP protocol?

    - PPP protocol stands for point-to-point protocol. This protocol helps us communicate between the two computers (routers).
    - The two derivatives of the point-to-point protocol are:
      - Point-to-point protocol over Ethernet
      - Point-to-point protocol over ATM

16. What is IP Spoofing, and what can we do to prevent it?

    - It is a type of mechanism that is used by attackers to get authorized access to the system. The intruder sends the message to the computer with an IP address from a trusted source/host.
    - We can prevent it by filtering packets using special routers and firewalls that allow packets with recognized formats to enter the network.

17. What is garbage collection?

    - The memory that is occupied and is no longer in use is called garbage collection.

18. Tell us something about frame relay.

    - In the OSI model, it operates at the physical and data link layer and is a high-speed data communication technology. It uses frames for the transmission of data in the network.

19. What is DNS?

    - The DNS stands for the domain name system. The IP addresses are constantly changing, so the DNS makes the IP address into human-friendly names so humans can remember them much more easily.

20. Can you tell the difference between the domain admin groups and the Enterprise admin groups in the ad (active directory)?

    - Domain admin groups:
      - The members of the domain admin group have complete control of the domain.
    - Enterprise admin group:
      - The members of the enterprise admin group have complete control of the domains in the forest.

21. What will be your daily routine if you are a system administrator?

- software installation and updates, providing system access control, creating backups, data recovery, etc.

22. Describe the concept of DHCP?

- DHCP refers to dynamic host configuration protocol. This protocol is used to assign the IP address to the computers.
- So when we use the DHCP protocol, its IP address is changed whenever a computer is connected to a network.

23. Key Differences Between Hub and Switch

- A hub is a networking device that connects multiple PCs to a single network, whereas a Switch connects multiple devices on a single computer network.
- A hub operates on the OSI physical layer, whereas a switch operates on the OSI data link layer.
- The hub uses a half-duplex cable, whereas the switch uses a full-duplex cable.
- The switch is an active device, whereas the hub is a passive device.
- The switch employs the Spanning Tree Protocol to avoid switching loops. On the other hand, the hub cannot avoid switching loops.
- The hub's data transmission speed is quite slow compared to a switch.

24. What do you know about HTTPS, and what port does it use?

- The HTTPS uses the SSL certificates to confirm that the server you are connecting to is the one it says.
- The HTTPS traffic goes over TCP port 443.

25. What can you tell us about TCP?

- The TCP refers to Transmission Control Protocol and is a massively used protocol (for ex: HTTP, FTP & SSH).
- TCP is that it establishes the connection on both ends before any data starts to flow.
- The TCP always needs confirmation from the other side that the message is received or not.

26. What do you know about UDP?

- We can call the UDP the twin of the TCP. The UDP stands for User Datagram Protocol.
- The UDP doesn't care if somebody is listening on the other end or not, and it is called the connectionless protocol.Whereas, when we talk about the TCP, it makes everybody stay on the same page.
- The transmission speed on a UDP is faster than the transmission speed of TCP.

27. What can you tell us about port forwarding?

- When we want to communicate with the inside of a secured network, there is the use of a port forwarding table within the router or other connection management device that will allow the specific traffic to be automatically forwarded to a particular destination. It probably does not allow access to the server from outside directly into your network.

28. Can you differentiate between a PowerShell and a Command prompt?

- CMD is the command line for Microsoft Windows operating system, with command-based features.
- Powershell is a task-based command-line interface, specifically designed for system admins and is based on the . Net Framework.

29. What are ARP and EFS?

- ARP:
  - ARP refers to the address resolution protocol that allows the DNS to be linked to MAC addresses; the mapping of the human-friendly URLs to IP addresses is allowed by standard DNS. At the same time, the address resolution protocol allows the mapping of IP addresses to mac addresses. In this manner, the system goes from a regular domain name to an actual piece of hardware.
- EFS:
  - it refers to the encrypted file system. The encrypted files tied to the specific user become difficult when trying to decrypt a file without the user's assistance. There can also be a case when the user forgets their password or loses their password in such case. It becomes almost impossible to decrypt the file as the decryption process is tied to the user's login and password. It can only occur on NTFS formatted partitions. For a larger purpose, the better alternative is a Bitlocker.

30. What is an id?

- IDs stand for an intrusion detection system
  - HIDS (Host intrusion detection system)
  - NIDS (Network intrusion detection system)

31. What is Telnet?

- It is one of the application protocols that allow the connection on any port and is a very small and versatile utility.
- It allows the admin to connect to the remote devices. In case telnet transfers data in the form of text. On a remote host, the telnet provides access to a command-line interface because of security concerns when we use the telnet over an open network source such as the internet.