Ans 1. Account Lockout Policy

1. The Account lockout threshold policy setting determines the number of failed sign-in attempts that will cause a user account to be locked.
2. A locked account cannot be used until you reset it or until the number of minutes specified by the Account lockout duration policy setting expires.
3. You can set a value from 1 through 999 failed sign-in attempts, or you can specify that the account will never be locked by setting the value to 0.
4. If Account lockout threshold is set to a number greater than zero, Account lockout duration must be greater than or equal to the value of Reset account lockout counter after.
5. Brute force password attacks can be automated to try thousands or even millions of password combinations for any or all user accounts. Limiting the number of failed sign-ins that can be performed nearly eliminates the effectiveness of such attacks.

Ans 2. Group Policy

1. Group Policy is an infrastructure that allows you to specify managed configurations for users and computers through Group Policy settings and Group Policy Preferences.
2. To configure Group Policy settings that affect only a local computer or user, you can use the Local Group Policy Editor.
3. You can manage Group Policy settings and Group Policy Preferences in an Active Directory Domain Services (AD DS) environment through the Group Policy Management Console (GPMC).
4. Group Policy management tools also are included in the Remote Server Administration Tools pack to provide a way for you to administer Group Policy settings from your desktop.
5. By carefully planning, designing, testing, and deploying a solution based on your organization’s business requirements, you can provide the standardized functionality, security, and management control that your organization needs.
6. By using Group Policy, you can significantly reduce your organization’s total cost of ownership.

Ans 3. AppLocker

1. It’s a malware world out there. New malware strains pop up throughout the world today like weeds on a warm spring day.
2. Microsoft AppLocker provides out-of-the-box application whitelisting (AWL) capabilities that prevents users from running possibly dangerous applications.
3. Ultimately, when you use Windows AppLocker to whitelist applications, you are specifying the exact applications and .exe files that users may open.
4. Opposed to AppLocker, PolicyPak is designed to accelerate the whitelisting process. In other words, Windows Administrators have much more time to work on critical infrastructure tasks.
5. Unlike AppLocker, PolicyPak works with the Windows Professional edition of Windows 7 and later. Whitelisting benefits aren’t limited to just a few select operating systems.

Ans 4. Group Policy Objects / Objectives (GPO)

1. A Group Policy Object (GPO) is a virtual collection of policy settings. A GPO has a unique name, such as a GUID.
2. Group Policy settings are contained in a GPO. A GPO can represent policy settings in the file system and in the Active Directory.
3. GPO settings are evaluated by clients using the hierarchical nature of Active Directory.
4. To create Group Policy, an administrator can use the Group Policy Object Editor, which can be a stand-alone tool.
5. It is recommended that you use the Group Policy Object Editor as an extension to an Active Directory-related MMC snap-in because this will allow you to browse the Active Directory for the correct Active Directory container and define Group Policy based on the selected scope of management (SOM).
6. Examples of Active Directory-related snap-ins include the Active Directory Users and Computers snap-in and the Active Directory Sites and Services snap-in.
7. Policy settings are divided into 2:
   1. Settings that affect computer
   2. Settings that affect user
8. Computer-related policies specify system behavior, application settings, security settings, assigned applications, and computer startup and shutdown scripts.
9. User-related policies specify system behavior, application settings, security settings, assigned and published applications, user logon and logoff scripts, and folder redirection.
10. Be aware that computer-related settings override user-related settings.

Ans 5. File System

1. In computing, file system or filesystem (often abbreviated to fs) is a method and data structure that the operating system uses to control how data is stored and retrieved.
2. Without a file system, data placed in a storage medium would be one large body of data with no way to tell where one piece of data stopped and the next began, or where any piece of data was located when it was time to retrieve it. By separating the data into pieces and giving each piece a name, the data is easily isolated and identified.
3. Taking its name from the way a paper-based data management system is named, each group of data is called a "file."
4. The structure and logic rules used to manage the groups of data and their names is called a "file system."
5. Examples of File System:
   1. FAT: FAT is a type of file system, which is developed for hard drives. It stands for file allocation table and was first introduced in 1977, which is used for 12 or 16 bits for each and every cluster access into the file allocation table (FAT). On hard drives and other computer systems, it helps to manage files on Microsoft operating systems. In devices like digital cameras, flash memory, and other portable devices, it is also often found that is used to store file information. It also helps to extend the life of a hard drive as it minimizes the wear and tears on the hard disc. Today, FAT is not used by later versions of Microsoft Windows like Windows XP, Vista, 7, and 10 as they use NTFS. The FAT8, FAT12, FAT32, FAT16 are all the different types of FAT (for file allocation table).
   2. GFS: A GFS is a file system, which stands for Global File System. It has the ability to make enable multiple computers to act as an integrated machine, which is first developed at the University of Minnesota. But now it is maintained by Red Hat. When the physical distance of two or more computers is high, and they are unable to send files directly with each other, a GFS file system makes them capable of sharing a group of files directly. A computer can organize its I/O to preserve file systems with the help of a global file system.
   3. HFS: HFS (Hierarchical file system) is the file system that is used on a Macintosh computer for creating a directory at the time a hard disk is formatted. Generally, its basic function is to organize or hold the files on a Macintosh hard disk. Apple is not capable of supporting to write to or format HFS disks since when OS X came on the market. Also, HFS-formatted drives are not recognized by Windows computers as HFS is a Macintosh format. With the help of WIN32 or NTFS file systems, Windows hard drives are formatted.
   4. NTFS: NTFS is the file system, which stands for NT file system and stores and retrieves files on Windows NT operating system and other versions of Windows like Windows 2000, Windows XP, Windows 7, and Windows 10. Sometimes, it is known as the New Technology File System. As compared to the FAT and HPFS file system, it provides better methods of file recovery and data protection and offers a number of improvements in terms of extendibility, security, and performance.
   5. UDF: A UDF is a file system, stands for Universal Disk Format and used first developed by OSTA (Optical Storage Technology Association) in 1995 for ensuring consistency among data written to several optical media. It is used with CD-ROMs and DVD-ROMs and is supported on all operating systems. Now, it is used in the process of CD-R's and CD-RW's, called packet writing.

Ans 6. Data Backup & Recovery

1. Backup and recovery describe the process of creating and storing copies of data that can be used to protect organizations against data loss.
2. Recovery from a backup typically involves restoring the data to the original location, or to an alternate location where it can be used in place of the lost or damaged data.
3. The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data. Backup copies allow data to be restored from an earlier point in time to help the business recover from an unplanned event.
4. Storing the copy of the data on separate medium is critical to protect against primary data loss or corruption. This additional medium can be as simple as an external drive or USB stick, or something more substantial, such as a disk storage system, cloud storage container, or tape drive. The alternate medium can be in the same location as the primary data or at a remote location. The possibility of weather-related events may justify having copies of data at remote locations.
5. For best results, backup copies are made on a consistent, regular basis to minimize the amount data lost between backups. The more time passes between backup copies, the more potential for data loss when recovering from a backup. Retaining multiple copies of data provides the insurance and flexibility to restore to a point in time not affected by data corruption or malicious attacks.

Ans 7. Service Packs

1. A service pack (SP) is a Windows update, often combining previously released updates, that helps make Windows more reliable.
2. Service packs can include security and performance improvements and support for new types of hardware. Make sure you install the latest service pack to help keep Windows up to date.
3. Service packs take about 30 minutes to install, and you'll need to restart your computer about halfway through the installation.

Ans 9. Types of OS

1. Batch OS:
   1. Batch OS is the first operating system for second-generation computers. This OS does not directly interact with the computer. Instead, an operator takes up similar jobs and groups them together into a batch, and then these batches are executed one by one based on the first-come, first, serve principle.
   2. Advantages:
      1. Execution time taken for similar jobs is higher.
      2. Multiple users can share batch systems.
      3. Managing large works becomes easy in batch systems.
      4. The idle time for a single batch is very less.
   3. Disadvantages:
      1. It is hard to debug batch systems.
      2. If a job fails, then the other jobs have to wait for an unknown time till the issue is resolved.
      3. Batch systems are sometimes costly.
   4. Examples of Batch OS: payroll system, bank statements, data entry, etc.
2. Distributed OS:
   1. A distributed operating system is a recent advancement in the field of computer technology and is utilized all over the world that too with great pace.
   2. In a distributed OS, various computers are connected through a single communication channel.
   3. These independent computers have their memory unit and CPU and are known as loosely coupled systems.
   4. The system processes can be of different sizes and can perform different functions.
   5. The major benefit of such a type of operating system is that a user can access files that are not present on his system but another connected system.
   6. In addition, remote access is available to the systems connected to this network.
   7. Advantages:
      1. Failure of one system will not affect the other systems because all the computers are independent of each other.
      2. The load on the host system is reduced.
      3. The size of the network is easily scalable as many computers can be added to the network.
      4. As the workload and resources are shared therefore the calculations are performed at a higher speed.
      5. Data exchange speed is increased with the help of electronic mail.
   8. Disadvantages:
      1. The setup cost is high.
      2. Software used for such systems is highly complex.
      3. Failure of the main network will lead to the failure of the whole system.
   9. Examples of Distributed OS: LOCUS, etc.
3. Multitasking OS:
   1. The multitasking OS is also known as the time-sharing operating system as each task is given some time so that all the tasks work efficiently.
   2. This system provides access to a large number of users, and each user gets the time of CPU as they get in a single system.
   3. The tasks performed are given by a single user or by different users.
   4. The time allotted to execute one task is called a quantum, and as soon as the time to execute one task is completed, the system switches over to another task.
   5. Advantages:
      1. Each task gets equal time for execution.
      2. The idle time for the CPU will be the lowest.
      3. There are very few chances for the duplication of the software.
   6. Disadvantages:
      1. Processes with higher priority cannot be executed first as equal priority is given to each process or task.
      2. Various user data is needed to be taken care of from unauthorized access.
      3. Sometimes there is a data communication problem.
   7. Examples of Multitasking OS: UNIX, etc.
4. Network OS:
   1. Network operating systems are the systems that run on a server and manage all the networking functions.
   2. They allow sharing of various files, applications, printers, security, and other networking functions over a small network of computers like LAN or any other private network.
   3. In the network OS, all the users are aware of the configurations of every other user within the network, which is why network operating systems are also known as tightly coupled systems.
   4. Advantages:
      1. New technologies and hardware can easily upgrade the systems.
      2. Security of the system is managed over servers.
      3. Servers can be accessed remotely from different locations and systems.
      4. The centralized servers are stable.
   5. Disadvantages:
      1. Server costs are high.
      2. Regular updates and maintenance are required.
      3. Users are dependent on the central location for the maximum number of operations.
   6. Examples of Network OS: Microsoft Windows server 2008, LINUX, etc.
5. Real Time-OS:
   1. Real-Time operating systems serve real-time systems. These operating systems are useful where many events occur in a short time or certain deadlines, such as real-time simulations.
   2. Types of Real Time OS:
      1. Hard Real Time OS
      2. Soft Real Time OS
   3. Advantages:
      1. It provides more output from all the resources as there is maximum utilization of systems.
      2. It provides the best management of memory allocation.
      3. These systems are always error-free.
      4. These operating systems focus more on running applications than those in the queue.
      5. Shifting from one task to another takes very little time.
   4. Disadvantages:
      1. System resources are extremely expensive and are not so good.
      2. The algorithms used are very complex.
      3. Only limited tasks can run at a single time.
      4. In such systems, we cannot set thread priority as these systems cannot switch tasks easily.
   5. Examples of Real-Time OS: Medical imaging systems, robots, etc.
6. Mobile OS:
   1. A mobile OS is an operating system for smartphones, tablets, and PDA’s. It is a platform on which other applications can run on mobile devices.
   2. Advantages:
      1. It provides an ease to users.
   3. Disadvantages:
      1. Some of the mobile operating systems give poor battery quality to users.
      2. Some of the mobile operating systems are not user-friendly.
   4. Examples of the Mobile OS: Android OS, IOS, Symbian OS, and Windows mobile OS.

Ans 10. TELNET

1. Telnet is an application protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte-oriented data connection over the Transmission Control Protocol (TCP).
2. Telnet was developed in 1969 beginning with RFC 15, extended in RFC 855, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards. The name stands for "teletype network".
3. Telnet is a client-server protocol, based on a reliable connection-oriented transport.
4. This protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23, where a Telnet server application (telnetd) is listening.
5. Telnet, however, predates TCP/IP and was originally run over Network Control Program (NCP) protocols.

Ans 11. Proxy Server

1. A proxy server is a computer system or router that functions as a relay between client and server.
2. It helps prevent an attacker from invading a private network and is one of several tools used to build a firewall.
3. The word proxy means "to act on behalf of another," and a proxy server acts on behalf of the user.
4. All requests to the Internet go to the proxy server first, which evaluates the request and forwards it to the Internet.
5. There are two types of proxies: forward proxies (or tunnel, or gateway) and reverse proxies (used to control and protect access to a server for load-balancing, authentication, decryption or caching).