Task-12

Vidit Sharma
21BCY10055

Date- 12/09/2023

Local Security Policy-

The local security policy of a system is a set of information about the security of a local computer. Local Security Policy refers to a set of rules, settings, and configurations that control the security of a computer system at the local level, typically on an individual device or computer within a network. It is a component of the Windows operating system (often called Local Security Policy Management Console) and is used to define security settings specific to that particular computer.

The local security policy information includes the following:

- The domains trusted to authenticate logon attempts.
- Which user accounts may access the system and how. For example, interactively, through a network, or as a service.
- The rights and privileges assigned to accounts.
- The security auditing policy.

Local Security Policy settings can include:

- Account Policies: These settings manage user account security, including password policies, account lockout policies, and more.
- Local Policies: These settings control security options such as user rights assignments, audit policies, and security options for the device.
- Security Options: These are configurations that control various aspects of system security, such as network security, user authentication, and behavior of certain Windows features.
- Advanced Audit Policy Configuration: These settings provide more detailed control over auditing and logging of security events.

Local Security Policy is often used in standalone computers or devices that are not part of a centralized domain, as opposed to Group Policy, which is used in domain-based networks to manage security policies across multiple computers. Administrators can use Local Security Policy to define security standards, access controls, and audit settings to ensure the security of a single computer or a smaller network.