Name :- M Om Nivas Reg no : 21BCE9706

E-mail :- omnivas.21bce9706@vitapstudent.ac.in

Task – 13

LOCAL SECURITY POLICY :-

The local security policy of a system is a set of information about the security of a local 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.

The *Local Security Authority* (LSA) stores the local policy information in a set of LSA Policy Objects.

Local Security Policy, often referred to as Local Security Policy Settings or Local Security Policies, is a feature in Microsoft Windows operating systems that allows administrators to configure and manage security settings for a single computer or a local system. These policies are designed to enhance the security of the system by controlling various aspects of user access, permissions, and authentication.

Local Security Policy includes a wide range of settings and configurations that can be customized to meet specific security requirements. Some common aspects that can be controlled through Local Security Policy include:

- User Rights Assignment: This allows administrators to specify which users or groups have particular rights on the system, such as the right to log on locally, shut down the system, or change system time.
- Security Options: These settings define system-wide security configurations, such as password policies, account lockout policies, and auditing settings.
- Audit Policy: Administrators can configure what types of events are audited on the system, including login attempts, file access, and other security-related activities.
- Local Policies: This section covers various security-related policies, such as password policies (e.g., minimum password length, password complexity requirements), user account control settings, and more.

- Software Restriction Policies: These policies help control which software can run on the system, reducing the risk of running malicious programs.
- Advanced Audit Policy Configuration: Provides granular control over auditing settings, allowing administrators to specify exactly what events to audit and where the audit logs are stored.

Local Security Policy is typically used on stand-alone computers or computers that are not part of a domain. For larger network environments or domains, security policies are usually managed through Group Policy, which allows administrators to enforce policies across multiple computers and users.

To access Local Security Policy on a Windows computer, you can use the "Local Security Policy" administrative tool, which can be found in the Windows Administrative Tools or by running the "secpol.msc" command.

It's important to note that configuring security policies incorrectly can lead to security vulnerabilities or unintended consequences, so it's essential to have a good understanding of the policies and their implications before making changes.

END