Task - 13

[Bhumireddy Thanmaye 21BCI0013](mailto:bhumireddy.thanmaye2021@vitstudent.ac.in)

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.

**Local Security Authority Subsystem Service (LSASS)** is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system. It verifies users logging on to a Windows computer or server, handles password changes, and creates access tokens.

The Local Security Policy application contains an Audit Policy section and an Advance Audit Policy Configuration section. Both sections allow for security auditing, but the Advanced Audit Policy Configuration section allows for more granular audit controls.The Advanced Audit Policy Configuration section has 10 sections:

* Account Logon

Allows you to audit credential validation, account logon events, Kerberos authentication events, and Kerberos ticketing events.

* Account Management

Allows you to audit changes to user accounts, groups, and computer accounts.

* Detailed Tracking

Allows you to audit DPAPI, process creation, process termination, and RPC events.

* DS Access

Allows you to audit Directory Service access, changes, and replication.

* Logon/Logoff

Allows you to audit account lockouts, IPSec events, logons, and logoffs.

* Object Access

Allows you to audit file shares, certification services, the registry, kernel object access, and many other objects.

* Policy Change

Allows you to audit changes in the authentication policy, authorization policy, and other policy change events.

* Privilege Use

Allows you to audit the use of user privileges.

* System

Allows you to audit the IPSec driver, security state changes, system integrity, and other system events.

* Global Object Access Auditing

Allows you to audit registry and file system changes