**SAMEER CHAUHAN 21BCE0999 TASK-11 12-09-23 TUESDAY**

**AIM-Documentation on local Security policy**

Local security policy- typically refers to the security settings and configurations that are applied to an individual computer or device within a network. These policies are used to enforce security measures at the local level to protect the device and its data. The specific configuration options and settings may vary depending on the operating system you're using, such as Windows or Linux.

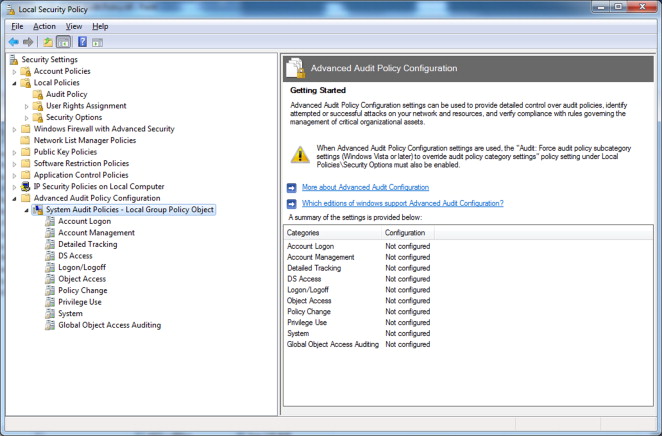
1- **User Account Controls (UAC):** On Windows systems, UAC is a local security policy that controls how applications can execute with administrative privileges. It prompts the user for consent or credentials when attempting to perform actions that require administrative access.

2- **Password Policies:** Local security policies often include settings related to password complexity, length, expiration, and lockout policies. These policies help ensure strong and secure user passwords.

3- **Account Lockout Policies:** These policies determine how many failed login attempts are allowed before an account is locked and for how long. They help prevent brute-force attacks.

4- **Firewall Rules:** Configuring local firewall rules to control incoming and outgoing network traffic is a key part of local security policy. This helps protect the device from unauthorized network access.

5- **File and Folder Permissions:** Local security policy defines who can access, modify, and delete files and folders on the system. Setting appropriate permissions is crucial for data security.



As we can see local security policy in some pc this option is not available by default so we have to manually download it by giving some command in command prompt.

The role of local security policies in Q Radar can be understood in the following ways:

1-**Source of Log Data**: Q Radar relies on log and event data generated by various systems and devices within an organization's network. Local security policies on these systems determine what events are logged and in what format. For example, Windows Event Logs, Linux audit logs, firewall logs, and antivirus logs are all influenced by local security policies. Q Radar collects and analyses these logs to identify potential security threats.

**2-Data Normalization:** Q Radar normalizes log data from diverse sources to create a unified view of security events. Local security policies can impact the format, structure, and content of log data. Q Radar's parsing and normalization processes may need to account for these variations to ensure accurate analysis.

3- **User Activity and Access Control**: Local security policies play a crucial role in defining user access controls, authentication, and authorization settings. Q Radar relies on this information to track user activities and identify potential security violations. For instance, if an unauthorized user attempts to access a resource, this information will be logged by the local security policy and forwarded to Q Radar for analysis.

4- **System Alerts and Notifications**: Security policies may dictate how system alerts and notifications are generated. Q Radar can integrate with these alerts and use them to trigger further investigations or responses. For example, an intrusion detection system (IDS) may generate alerts based on local security policies, and Q Radar can correlate these alerts with other events to identify potential attacks.

5- **Asset Identification and Classification**: Local security policies can impact how systems and assets are identified and classified. Q Radar relies on accurate asset information to categorize and prioritize security events. If an asset's security settings change due to a local policy update, Q Radar must reflect those changes in its asset database.