Cybersecurity Lab Project: Monitoring Resource Utilization and Detecting Unauthorized Privilege Escalation

Objective

This lab project focused on two critical aspects of cybersecurity monitoring within a Windows environment:
1. **Analyzing Resource Utilization** to detect abnormal system behavior that may indicate malicious activity.
2. **Detecting Unauthorized User Privilege Escalation** by enabling auditing and monitoring event logs for suspicious account modifications.

Exercise 1: Analyze Resource Utilization

Goal: Learn to monitor system performance to identify potential threats.

- Resource utilization on a Windows device was monitored to detect unusual spikes in CPU, memory, and network usage.
- Windows built-in tools such as **Task Manager** and **Resource Monitor** were highlighted for real-time tracking.
- Security specialists use these tools to correlate unusual activity with possible attacks such as denial of service, malware, or privilege escalation.

Exercise 2: Detecting Unauthorized User Privilege Escalation

Goal: Learn to detect unauthorized changes in account privileges using auditing and Event Viewer.

1. **Audit Policy Configuration:**
2. Security Group Management auditing was enabled to track group membership changes.
3. This ensures that events are logged whenever a user is added to or removed from privileged groups.

Audit Security Group Management

1. **Creating a New User Account:**
2. A new user, *Jeremiah ACI*, was created in the Marketing Organizational Unit (OU).
3. User details and login configuration were completed.

New Object User Active Directory Users

1. **Privilege Escalation Detected:**
2. The user *Jeremiah* was added to the **Domain Admins** group.

3. Event Viewer captured Event **4728** (a member was added to a security-enabled group).
4. Logs clearly show the addition of Jeremiah to the Domain Admins group.

Event Viewer 4728 Event Details

1. **Event Correlation:**
2. Event **4737** captured changes to security-enabled groups.
3. The subject account responsible for the action was identified (Administrator).

Event 4737

Key Learning Outcomes

After completing the lab, the following skills were achieved: - Ability to **monitor resource utilization** using native Windows tools. - Enable and configure **User Privilege Monitoring** through group policy. - **Generate and analyze auditing logs** in Event Viewer. - **Detect unauthorized privilege escalation**, identifying both the suspicious account and the administrator account responsible.

Conclusion

This lab demonstrated how a cybersecurity analyst can: - Track resource utilization for anomalies. - Configure auditing to monitor privileged accounts. - Detect and investigate unauthorized changes to security groups.

By applying these methods, security professionals can proactively identify insider threats, compromised accounts, and potential privilege escalation attacks within Active Directory environments.