Muhammad Izham Bin Norhamadi
B032020039

Lab 10

1.1 Assigning or set privileges and permissions to an object (files or folders) is very important. Why?

Managing privileges and permission will ensure that data is secured and only authorized users can access it

2.1 What is the use of Group Policy?

Group Policy is a hierarchical infrastructure that allows a network administrator to implement specific configurations for users and computers

3.1 Explain the differences of all level in UAC settings

1) Always Notify - Notify users of any changes by apps or users

2) Notify me only when programs try to make changes - Only notify user when an app is trying to make any changes

3) Notify me only when programs try to make changes - Notify users about app without dimming the desktop

4) Never notify - Will not notify user of changes by apps and users

3.2 Explain User Account Control (UAC)

UAC is a mandatory access control enforcement feature from Windows that aims to to improve security of Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation

3.3 What were its design goals?

It aims to to improve security of Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation

3.4 How secure is UAC?

UAC is very secured in granting and elevating softwares

3.5 What are its strengths?

1) Prevents unauthorized changes to PC

2) Adjustable level of access

3.6 What are its weaknesses?

1) Can be intrusive

2) Too process specific

4. Best Practices for Access Control

4.1 Write a short summary of that breach

Separation of Duties

There is a risk of misappropriation of assets, which involves third parties or employees in an organization who abuse their position to steal from it through fraudulent activity. Inadequate segregations of duties could make fraud prevention, detection and investigation difficult, which could possibly lead to misstated financial statements, regulatory punishments, damage to the company's reputation and reduced investor trust.

Job Rotation

As an employee learns additional roles in the organization and the procedures associated with those roles, that employee is more likely to discover vulnerabilities to be exploited. As employees transition through multiple roles and are assigned new duties, they are likely to be granted additional system privileges. Left unchecked, they will almost certainly accumulate more privileges than they need to perform their current duties.

Least Privilege

Employee might be tempted to elevate their privilege or bypassing UAC such as using applications that is set to auto-elevate, allowing them to elevate privilege when necessary. Compromise of authorized applications is a common privilege escalation attack vector.

Implicit Deny

Same as least privilege, employee may be tempted to find ways to grand themselves permission to an object.

4.2 Rank these four best practices from most effective to least effective. Give an explanation of your rankings.

1. Implicit Deny
   Implicit Deny is a common and the best access control practice especially in network security granted access and access requests can easily be monitored, any anomalies on the network will be denied automatically.

2. Least Privilege
   Least Privilege is good for an employee to do their work using the bare minimum permissions given but it is time consuming to make sure that an employee has the bare minimum permission.

3. Separation of Duties
   Separation of Duties is good for preventing frauds in business makes tracing frauds activities harder to track.

4. Job rotation
   Job rotation can limit the amount of time an employee to configure system settings but assigning employee to multiple different roles may indirectly grant them additional system privileges that are not required to do their job.