Primary Access Token Manipulation

Exercise 1: Understanding Tokens

Objective:

Familiarize users with access tokens and their components.

Software:

- Process Explorer

Steps:

1. View Current Token Privileges

1. Open Command Prompt (CMD) as an administrator (Keep this open for the next exercise).
2. Run the following command:

   ```
   whoami /all
   ```

3. Observe and document the privileges listed under "Privileges Information".
   - **Example:** SeDebugPrivilege
   - **Explanation:** SeDebugPrivilege gives a user the ability to debug any process that belongs to another account. This is mostly employed by system administrators and developers.

2. Explore Tokens

1. Open the Process Explorer software as the system administrator.
2. Find out the process in the list that corresponds to the CMD that you have opened.

3. Click on ‘cmd’, then right-click on the process and click on ‘Properties’.
4. To see the token information, go to the “Security” tab.
5. Identify and document the following components of the token: Identify and document the following components of the token:
    - **User SID**: Security Identifier of the user. (**Usually at the top)**
    - **Group SIDs**: Security Identifiers of the groups that the user is a member of. (**You will need to click the row you want to display this SID)**
    - **Privileges**: List of privileges which are granted to the token.

3. Analyze Token Components

1. Research the significance of each token component.
    - **Example Privilege: SeDebugPrivilege**
        - **What it enables**: Allows debugging of processes, which can be critical for troubleshooting and system management.
2. Document the findings in detail, explaining the role and impact of each privilege and component.