Primary Access Token Manipulation

Exercise 2: Stealing Tokens from a Vulnerable Application

Objective:

Practice stealing tokens from an application.

Software:

- Process Explorer
- Incognito

Steps:

1. Identify the Vulnerable Application

1. Open Process Explorer as an administrator.
2. Use Process Explorer to identify processes running with elevated privileges (e.g., Command Prompt (CMD) running as admin, you can use the same one from the previous exercise).

2. Steal the Token

1. Don't open the files. Go to the "Exercise 2" folder, right click anywhere and click "Command Prompt (Administrator)"
2. Use the tool 'Incognito' installed in the VM to list available tokens:

   ```
   incognito list_tokens -u
   ```

3. Identify the token you want to steal, typically one with elevated privileges (e.g., NT AUTHORITY\SYSTEM).

3. Time to Use the Token

1. Execute the following command to open a Command Prompt (CMD) with SYSTEM privileges (PossibleShell.exe is just opening a command prompt. In an actual scenario this would be a reverse shell exe encoded from a metasploit module):

   ```
   incognito execute -c "NT AUTHORITY\SYSTEM" PossibleShell.exe
   ```

2. Verify the elevated privileges by running the command:

   ```
   whoami
   ```

3. Document the impact of gaining elevated privileges, such as:
   - Access to restricted files or directories.
   - Ability to modify system settings.
   - Execution of administrative commands.