Scripts

<https://sushant747.gitbooks.io/total-oscp-guide/content/privilege_escalation_windows.html>

Powershell script for unquoted Service Paths

Get-WmiObject win32\_service | select Name,PathName,StartMode,StartName | where {$\_.StartMode -ne "Disabled" -and $\_.StartName -eq "LocalSystem" -and $\_.PathName -notmatch "`"" -and $\_.PathName -notmatch "C:\\Windows"} | Format-List

https://offsec.blog/hidden-danger-how-to-identify-and-mitigate-insecure-windows-services/

**AlwaysInstallElevated**

reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated

reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated

<https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation>

<https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/dll-hijacking>

process monitor (procmon) from SIS internals

[procmon](https://docs.microsoft.com/en-us/sysinternals/downloads/procmon) from sysinternals, **setting** the **following 2 filters**:

<https://juggernaut-sec.com/dll-hijacking/#Windows_10_Phantom_DLL_Hijacking_-_WptsExtensionsdll>

The system directory. Use the [**GetSystemDirectory**](https://docs.microsoft.com/en-us/windows/desktop/api/sysinfoapi/nf-sysinfoapi-getsystemdirectorya) function to get the path of this directory.(C:\Windows\System32)

<https://fuzzysecurity.com/tutorials/16.html>

https://delinea.com/blog/windows-privilege-escalation

<https://www.base64decode.org/>

<https://grimhacker.com/2015/04/10/gp3finder-group-policy-preference-password-finder/>

https://infosecwriteups.com/ikeext-dll-hijacking-3aefe4dde7f5

Afbeelding met tekst, elektronica, schermopname, software

Automatisch gegenereerde beschrijving