about_Token_Privileges

by Thorsten Butz

PSCONF.EU

MALMÖ 25

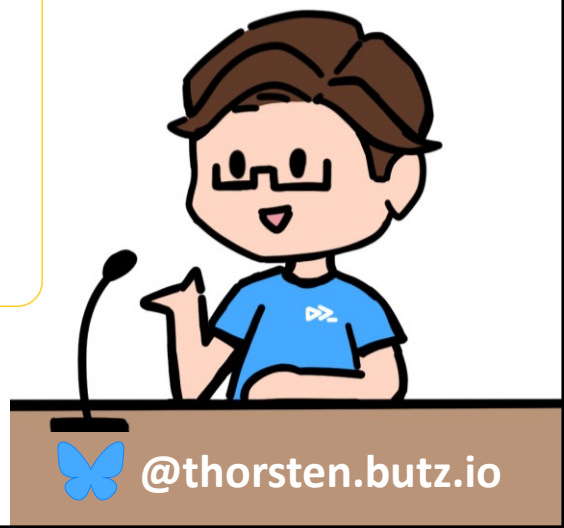
Chocolatey

Jane Street

IRONMAN SOFTWARE

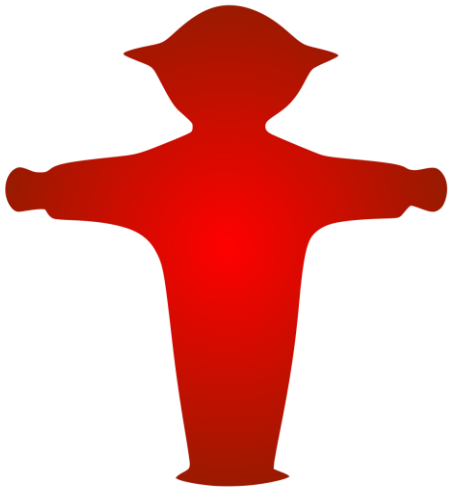
KNOWLEDGE FACTORY

SynEdgy



@thorsten.butz.io

```
# > whoami.exe /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```



User Account Control

Do you want to allow this app to make changes to your device?

Terminal

Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer

Show more details

To continue, enter an admin username and password.

Terminal will also be installed for the administrator.

User name

User name

Password

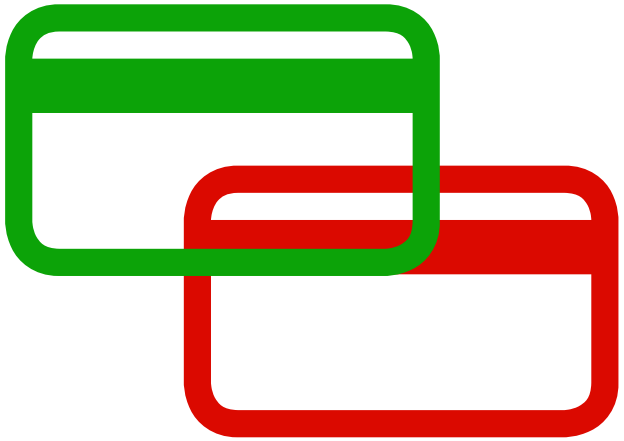
Password

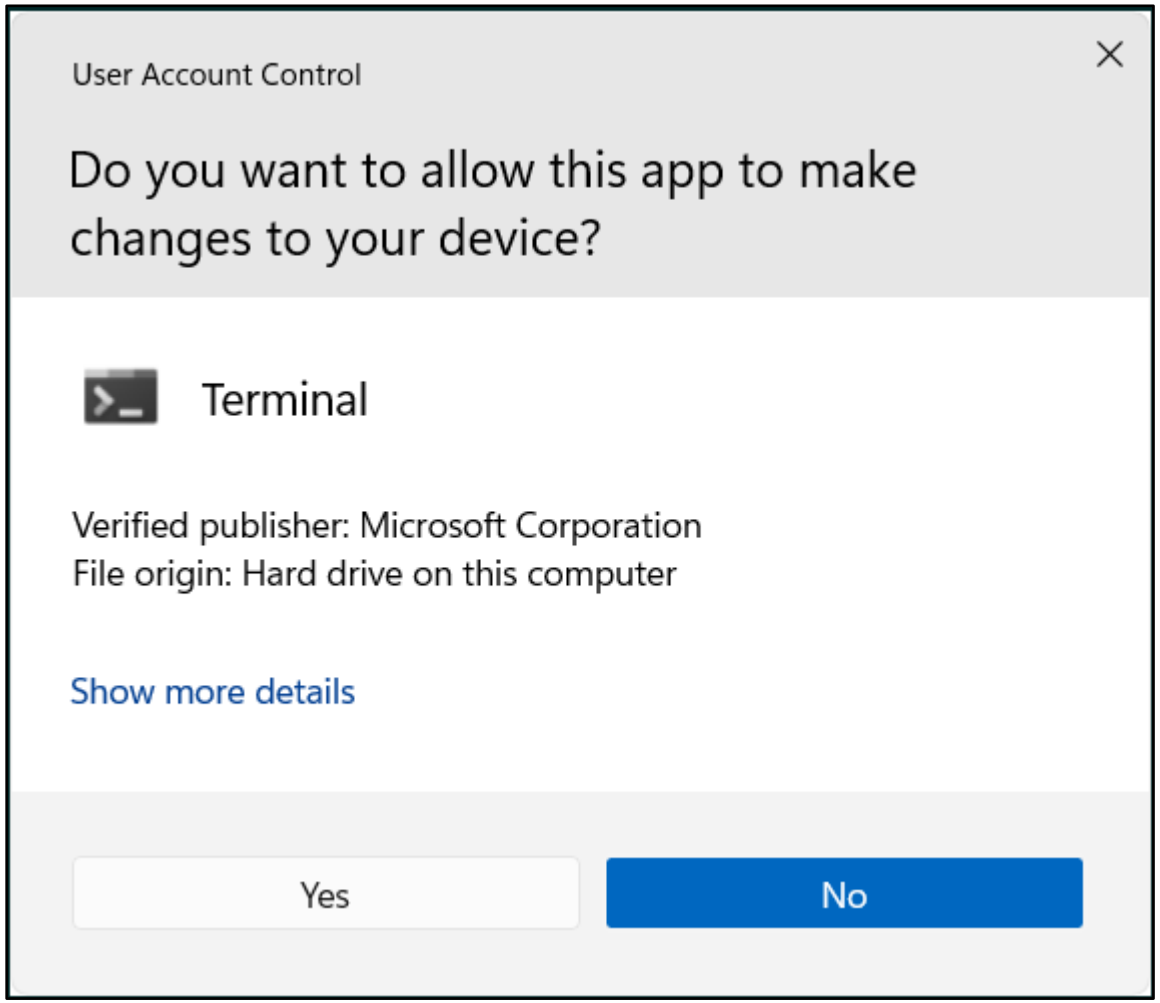
Domain: CONTOSO

Yes

No

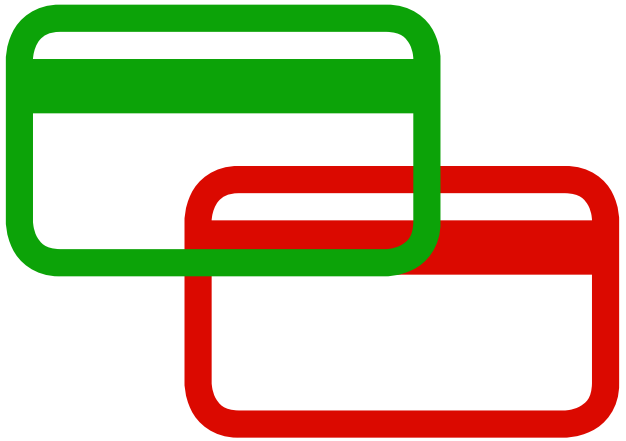
Windows Vista: User Account Control





"Protected Admin"

Vista: Split token login

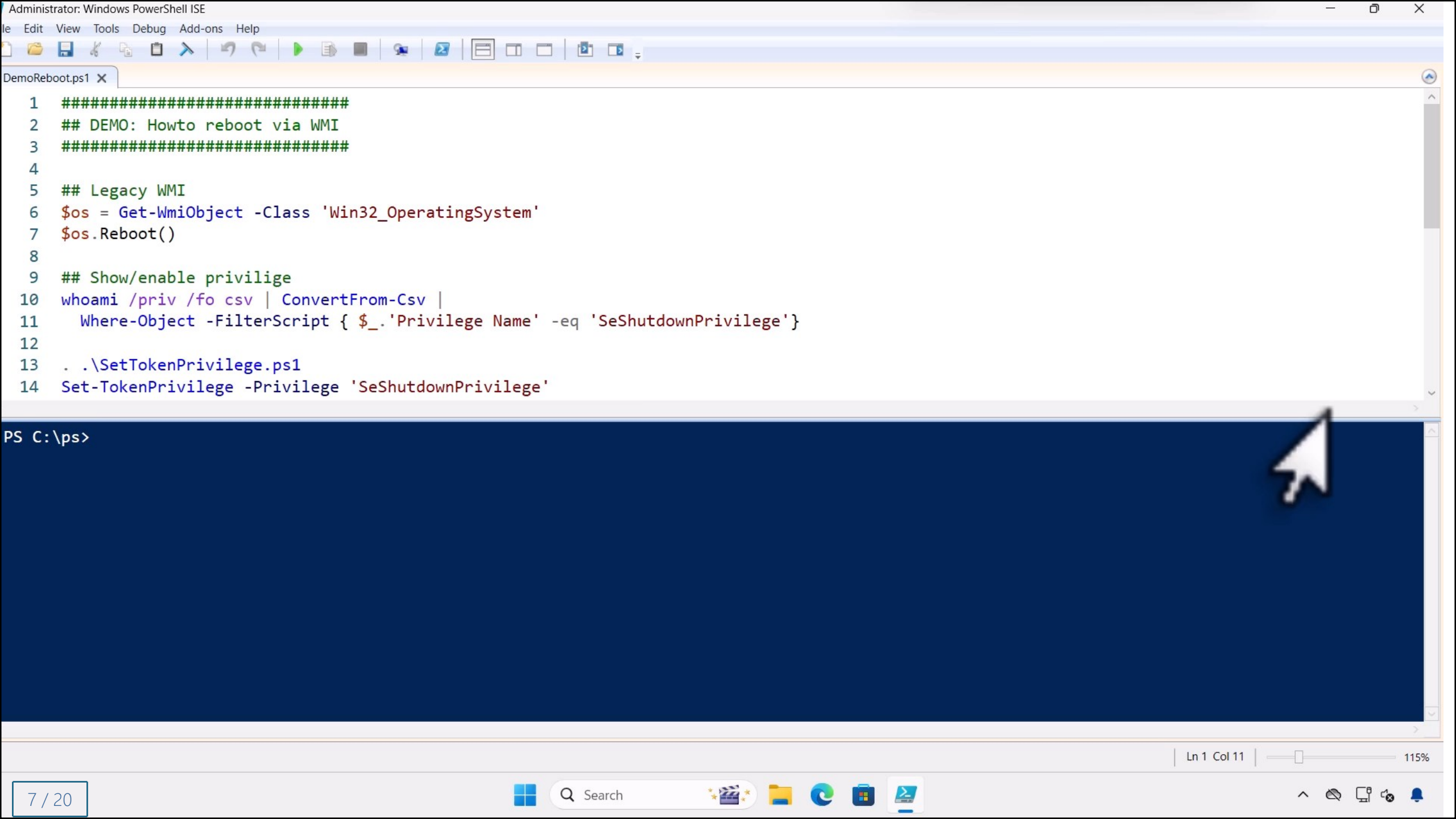


Mark Russinovich

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
```

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same sessio Disabled
```


Administrator: Windows PowerShell ISE
le Edit View Tools Debug Add-ons Help
DemoReboot.ps1
1 ##############################
2 ## DEMO: Howto reboot via WMI
3 ##############################
4
5 ## Legacy WMI
6 $os = Get-WmiObject -Class 'Win32_OperatingSystem'
7 $os.Reboot()
8
9 ## Show/enable privilige
10 whoami /priv /fo csv | ConvertFrom-Csv |
11 Where-Object -FilterScript { $_.'Privilege Name' -eq 'SeShutdownPrivilege'}
12
13 . .\SetTokenPrivilege.ps1
14 Set-TokenPrivilege -Privilege 'SeShutdownPrivilege'
PS C:\ps>
Ln 1 Col 11
115%
Search

Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

DemoReboot.ps1

```powershell
##############################
## DEMO: Howto reboot via WMI
##############################

## Legacy WMI
$os = Get-WmiObject -Class 'Win32_OperatingSystem'
$os.Reboot()

## Show/enable privilige
whoami /priv /fo csv | ConvertFrom-Csv |
  Where-Object -FilterScript { $_.'Privilege Name' -eq 'SeShutdownPrivilege'}

. .\SetTokenPrivilege.ps1
Set-TokenPrivilege -Privilege 'SeShutdownPrivilege'
```

```
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : WMIMethodException


PS C:\ps> whoami /priv /fo csv | ConvertFrom-Csv |
  Where-Object -FilterScript { $_.'Privilege Name' -eq 'SeShutdownPrivilege'}

Privilege Name      Description          State
--------------      -----------          -----
SeShutdownPrivilege Shut down the system Disabled



PS C:\ps>
```

Ln 20 Col 11 115%

Search

Lee Holmes


```
## Taken from P/Invoke.NET with minor adjustments.
$definition = @'
using System;
using System.Runtime.InteropServices;
public class AdjPriv {
    [DllImport("advapi32.dll", ExactSpelling = true, SetLastError = true)]
    internal static extern bool AdjustTokenPrivileges(IntPtr htok, bool disall,
        ref TokPriv1Luid newst, int len, IntPtr prev, IntPtr relen);

    [DllImport("advapi32.dll", ExactSpelling = true, SetLastError = true)]
    internal static extern bool OpenProcessToken(IntPtr h, int acc, ref IntPtr phtok);

...
```

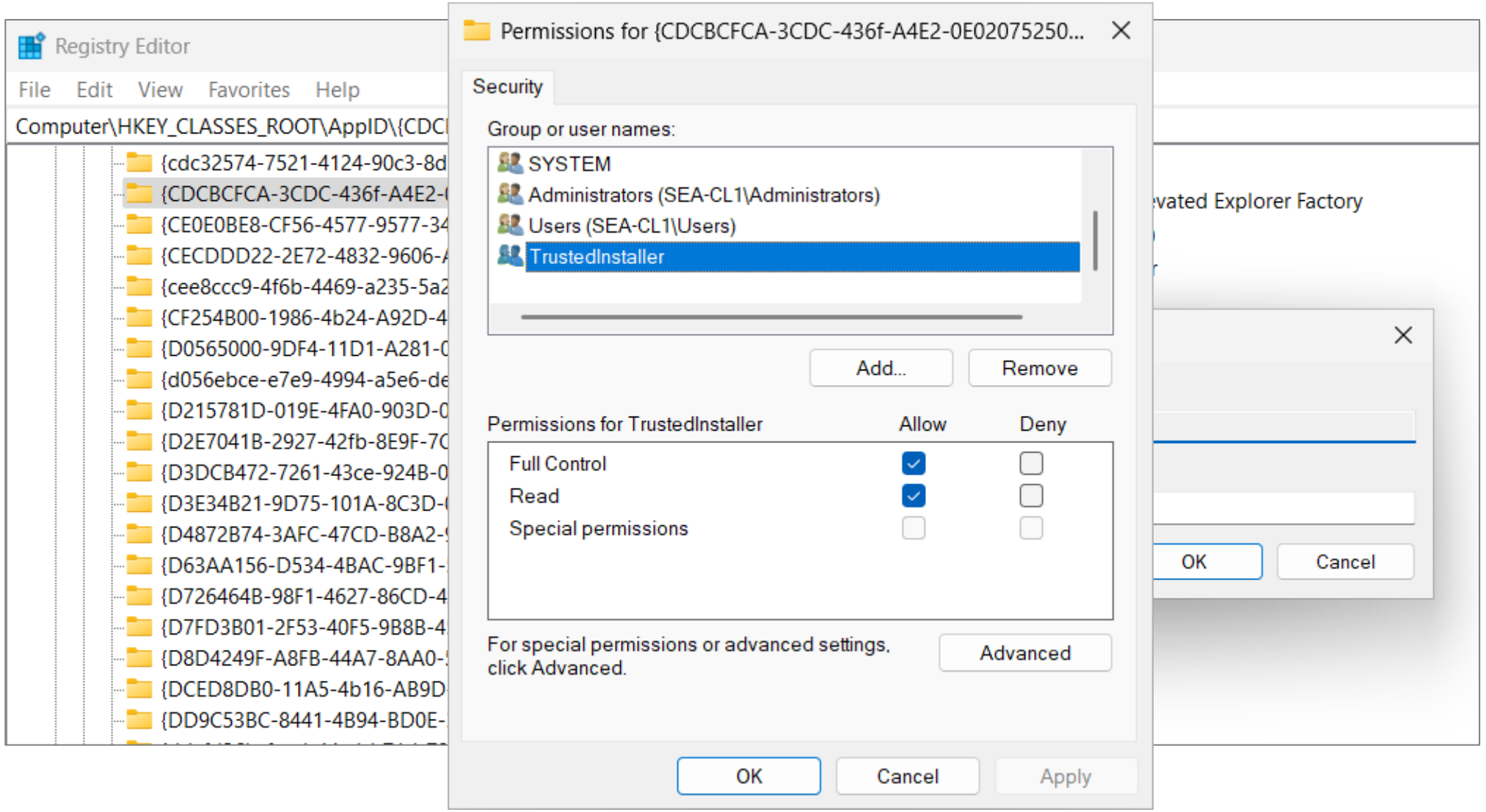
https://www.leeholmes.com/adjusting-token-privileges-in-powershell/

Token privileges: a 2nd step authorization

"A privilege is the right of an account, such as a user or group account, to perform various system-related operations on the local computer, such as shutting down the system, loading device drivers, or changing the system time."

https://learn.microsoft.com/en-us/windows/win32/secauthz/privileges

Run explorer.exe as administrator



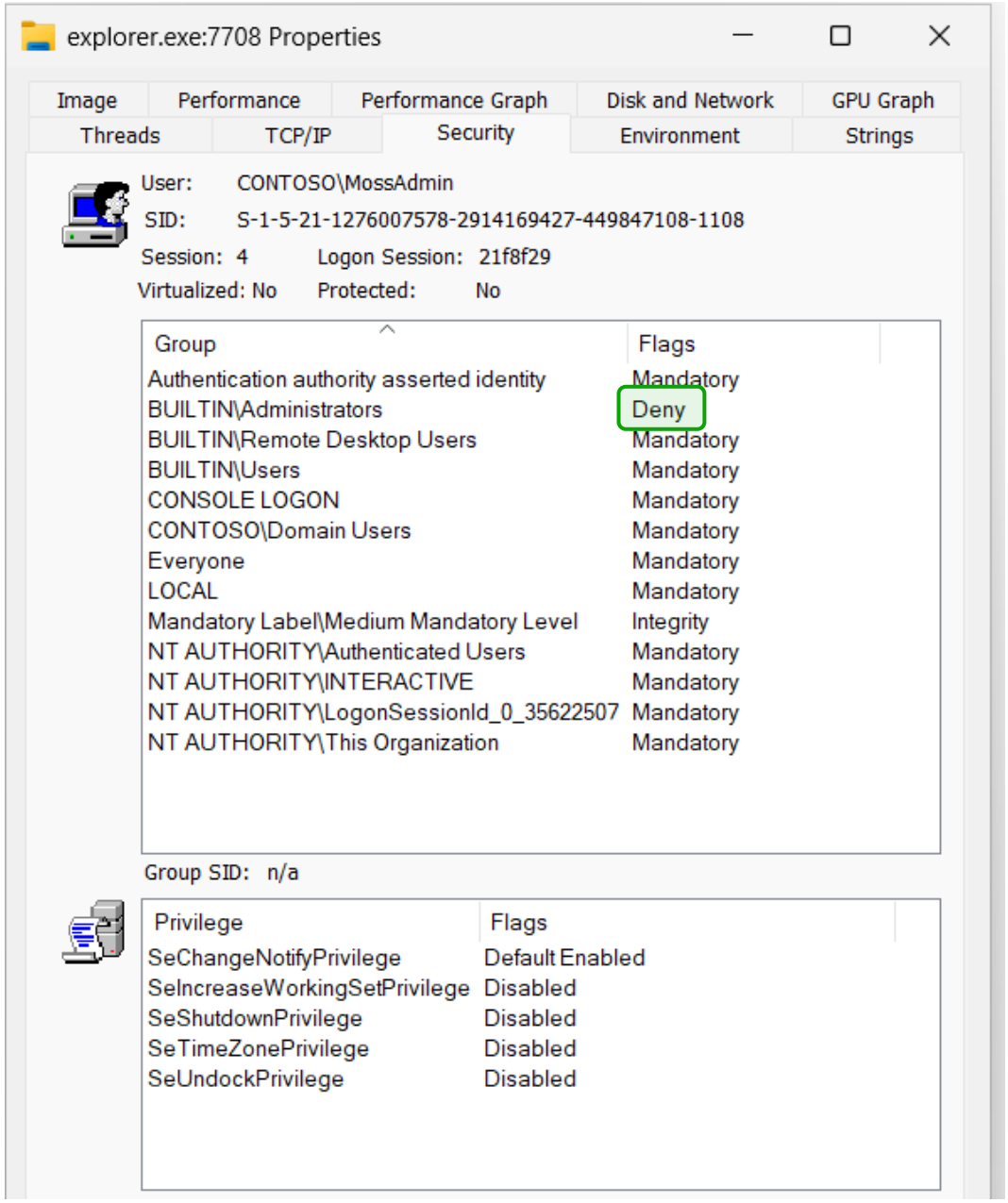
Bypassing Set-ACL

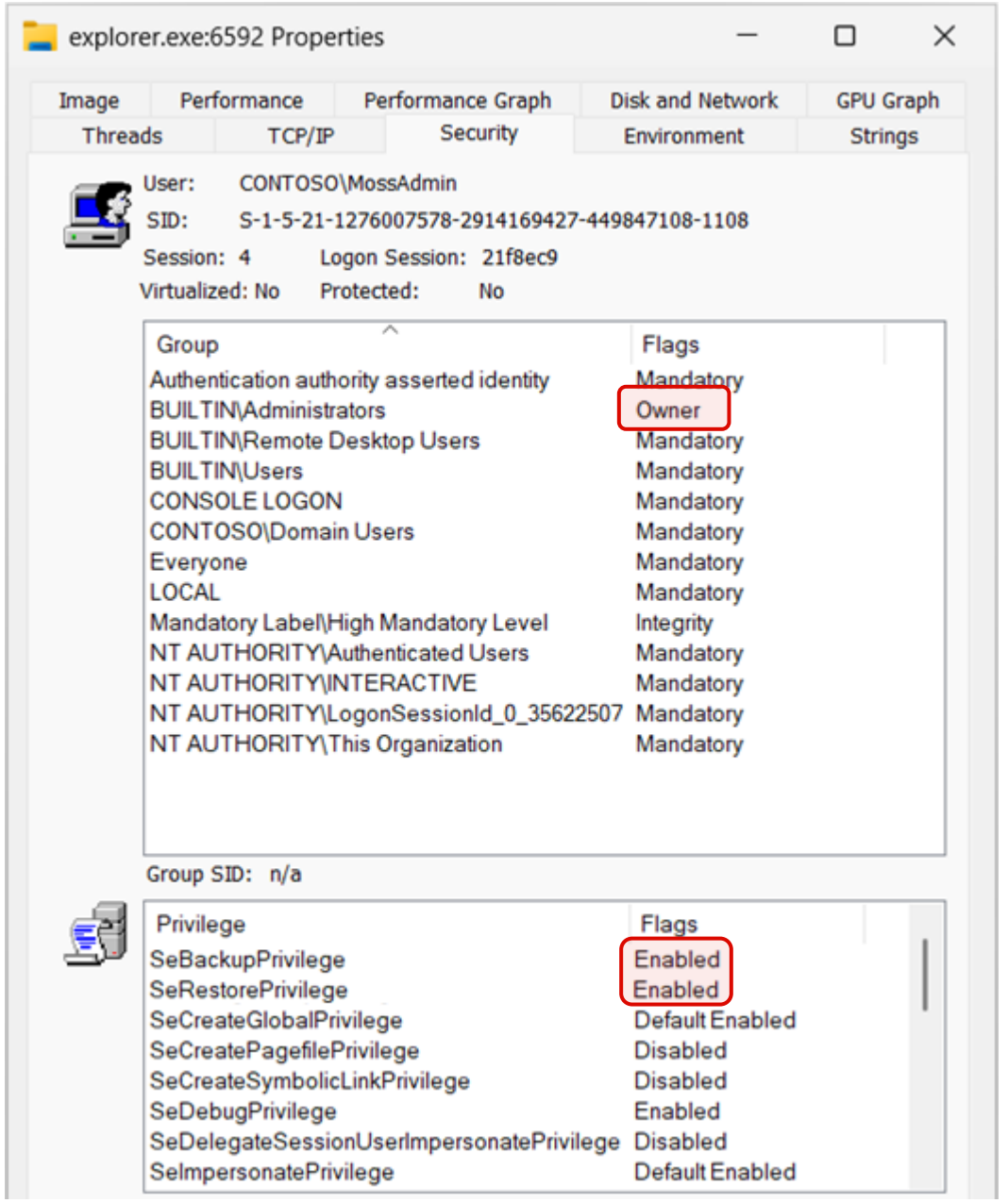
```powershell
## Enable SeTakeOwnership privilige
. .\SetTokenPrivilege.ps1
Set-TokenPrivilege -Privilege 'SeTakeOwnershipPrivilege' -ProcessId $pid

## Define RegKeys (Since Set-ACL does not work here, we use the .NET API)
$baseKey = [Microsoft.Win32.Registry]::ClassesRoot ## 'HKEY_CLASSES_ROOT'
$subKey = 'AppID\{CDCBCFCA-3CDC-436f-A4E2-0E02075250C2}'
$me = [System.Security.Principal.NTAccount]::new("$env:USERDOMAIN\$env:USERNAME")

## Creating the required RegistryKey object (Microsoft.Win32.RegistryKey)
$regKey = $baseKey.OpenSubKey(
    $subKey,
    [Microsoft.Win32.RegistryKeyPermissionCheck]::ReadWriteSubTree,
    [System.Security.AccessControl.RegistryRights]::TakeOwnership
)

## Getting the current ACL
$acl = $regKey.GetAccessControl()
$acl.owner
$acl.Sddl
```

Take control

```powershell
## Let the calling account become the owner
$acl.SetOwner($me)
$regKey.SetAccessControl($acl)

## Define new rule: Allow "me" to have full control
$rule = [System.Security.AccessControl.RegistryAccessRule]::new(
    $me,
    [System.Security.AccessControl.RegistryRights]::FullControl ,
    [System.Security.AccessControl.InheritanceFlags]'ObjectInherit,ContainerInherit',
    [System.Security.AccessControl.PropagationFlags]::None ,
    [System.Security.AccessControl.AccessControlType]::Allow
)
$acl.AddAccessRule($rule)
$regKey.SetAccessControl( $acl )

## "Remove" the blocker
Rename-ItemProperty -Path "Registry::$($regKey.Name)" -Name 'RunAs' -NewName 'RunA_'
```

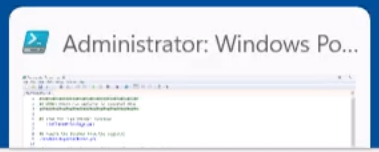
Process Explorer





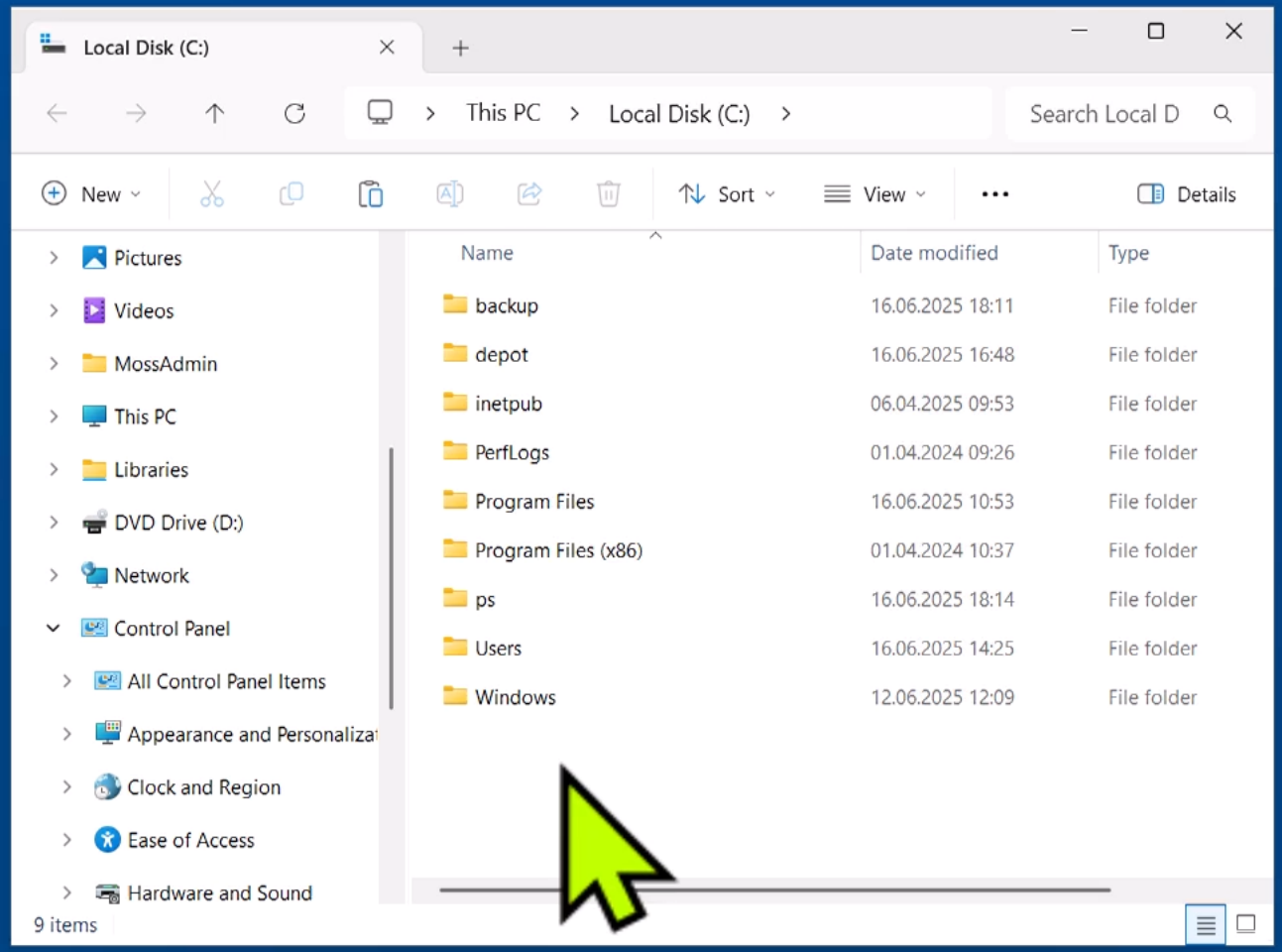
\\SEA-CL1
CONTOSO\MossAdmin

\\SEA-CL1
CONTOSO\MossAdmin



Search

\\SEA-CL1
CONTOSO\MossAdmin



Recycle Bin

Search

Holding out for a hero

```
# > robocopy /mir C:\Users\BarberJ\Desktop\ C:\backup\ /b
```

Win32 API


```
Add-Type -TypeDefinition @"
using System;
using System.IO;
using System.Runtime.InteropServices;
using Microsoft.Win32.SafeHandles;

public class BackupCopy {
    const uint GENERIC_READ = 0x80000000;
    const uint GENERIC_WRITE = 0x40000000;
    const uint FILE_FLAG_BACKUP_SEMANTICS = 0x02000000;
    const uint OPEN_EXISTING = 3;
    ...
}
"@

## Copy a single file (set overwrite to true or false)

[BackupCopy]::CopyFileWithBackupSemantics($src,$dst,$false)
```

In a nutshell

- **Token privileges** must be granted (during logon) and activated (at runtime).
- **UAC** works like a shim to enable elevated permissions while NOT activating privileges.
- You have to deal with the Win32 API and P/Invoke to utilize **NTFS backup semantics** combined with privileges like `SeBackupPrivilege` or `SeRestorePrivilege` to let processes bypass file system ACLs for reading, writing or restoring.
- **Robocopy** has built-in superpowers for everday working life.