

Forum:[Hack Forums](#)

Thread: [i wanna bypass uac](#)

Centsicles - July 29, 2024, 11:38 am

How do i bypass uac,its been going on for a decade,its super annoying had this for my whole life.I dont have access to bios aswell,please help (also i dont have a usb stick and i can access cmd but it needs admin for certain command's,e.g changing admin password)

DramaKing - July 29, 2024, 11:57 am

(Jul 29, 2024 11:38 AM)Centsicles Wrote: [\[CITE\]](#) How do i bypass uac,its been going on for a decade,its super annoying had this for my whole life.I dont have access to bios aswell,please help (also i dont have a usb stick and i can access cmd but it needs admin for certain command's,e.g changing admin password)

Access the BIOS?? With a remote access software program????? You really don't know anything about what you're trying to do, I take it. Well, there's lots of guides on how to turn off UAC in Windows settings; it's easy to find.

<https://www.howtogeek.com/247/disable-user-account-control-uac-the-easy-way-on-windows/>

Malware will be easily able to escalate in your system, but that's up to you.

Byte Wizard - July 29, 2024, 12:08 pm

(Jul 29, 2024 11:38 AM)Centsicles Wrote: [\[CITE\]](#) How do i bypass uac,its been going on for a decade,its super annoying had this for my whole life.I dont have access to bios aswell,please help (also i dont have a usb stick and i can access cmd but it needs admin for certain command's,e.g changing admin password)

On your PC or remote client PC?

You can never access BIOS on a remote client

If its on your PC that you own and can use you can turn off UAC in settings under "User Account Control"

Click windows key and search that

Then turn it off if you need to

globalroot - July 29, 2024, 10:55 pm

I think he means BIOS admin password, not UAC.

Why you can't access BIOS?

Centsicles - July 30, 2024, 4:48 am

(Jul 29, 2024 11:57 AM)DramaKing Wrote: [\[CITE\]](#) Access the BIOS?? With a remote access software program????? You really don't know anything about what you're trying to do, I take it. Well, there's lots of guides on how to turn off UAC in Windows settings; it's easy to find. Malware will be easily able to escalate in your system, but that's up to you.

i clicked the how to geek link,i went into change user account control settings,and i opened it,it needed admin password

(Jul 29, 2024 12:08 PM)Byte Wizard Wrote: [\[CITE\]](#) On your PC or remote client PC?

You can never access BIOS on a remote client

If its on your PC that you own and can use you can turn off UAC in settings under "User Account Control"

Click windows key and search that

Then turn it off if you need to

its on my own pc,i did what you said,and it came up with a admin password prompt

(Jul 29, 2024 10:55 PM)globalroot Wrote: [\[CITE\]](#) I think he means BIOS admin password, not UAC.
Why you can't access BIOS?

its password protected,and i want to bypass uac,i just said that bios is blocked for some random extra information.Preferably i'd like to know how to bypass both.

globalroot - July 30, 2024, 8:11 am

(Jul 30, 2024 04:48 AM)Centsicles Wrote: [\[CITE\]](#)

i clicked the how to geek link,i went into change user account control settings,and i opened it,it needed admin password

its on my own pc,i did what you said,and it came up with a admin password prompt

its password protected,and i want to bypass uac,i just said that bios is blocked for some random extra information.Preferably i'd like to know how to bypass both.

<https://bios-pw.org/>

Centsicles - July 30, 2024, 1:45 pm

i dont exactly know what to do i have hewett packard btw

DramaKing - July 30, 2024, 7:40 pm

(Jul 29, 2024 10:55 PM)globalroot Wrote: [\[CITE\]](#) I think he means BIOS admin password, not UAC.
Why you can't access BIOS?

Clearly the main question is UAC. He hasn't been able to access the BIOS his whole life, and he needs admin for certain cmd commands like changing the admin password?

So your personal computer that you own only has a limited user account? Clear the CMOS according to the directions for your computer model and use chntpw by booting SystemRescue or following this guide: <http://www.chntpw.com/guide/>. A UAC bypass code block is most likely going to get detected by antivirus, which you probably can't disable as a limited user.

Also, you should post questions like this in the Windows forum or Beginner Hacking, so that people, you know, don't get the wrong idea.

I'm going to make a wild stab and suggest that this is a school computer that wasn't properly reset.

terrestrial - July 30, 2024, 7:59 pm

You cannot access your bio with software on your pc, atleast to my knowledge.

Centsicles - July 31, 2024, 2:09 am

(Jul 30, 2024 07:40 PM)DramaKing Wrote: [\[CITE\]](#) Clearly the main question is UAC. He hasn't been able to access the BIOS his whole life, and he needs admin for certain cmd commands like changing the admin password?

So your personal computer that you own only has a limited user account? Clear the CMOS according to the directions for your computer model and use chntpw by booting SystemRescue or following this guide A UAC bypass code block is most likely going to get detected by antivirus, which you probably can't disable as a limited user.

Also, you should post questions like this in the Windows forum or Beginner Hacking, so that people, you know, don't get the wrong idea.

I'm going to make a wild stab and suggest that this is a school computer that wasn't properly reset.

its my dad's laptop that he gave to me.And i dont have a usb drive,all of them belong to my dad with some private stuff

DramaKing - July 31, 2024, 5:49 am

(Jul 31, 2024 02:09 AM)Centsicles Wrote: [\[CITE\]](#) its my dad's laptop that he gave to me.And i dont have a usb drive,all of them belong to my dad with some private stuff

Sorry, forgot. So he won't let you use his administrator account to so that you can give yourself full privileges? You will need to learn some real hacks.

[Video: <https://youtu.be/uTcrbNBcoxQ?si=us9nusTnPalzBbQF>]

There's also this method from an annoying clickbait hacker. No USB drive required, just Advanced System Recovery. Actually, that is more for when you have no account that you can access. You can use the "Sticky Keys" method of replacing sethc.exe with cmd.exe. sethc.exe is owned by SYSTEM, and Windows will run it as the SYSTEM user.

[Video: <https://youtu.be/GyIEZRFX2Zk?si=ri0tinp1lqJxWx3t>]

Centsicles - July 31, 2024, 12:23 pm

(Jul 31, 2024 05:49 AM)DramaKing Wrote: [\[CITE\]](#) Sorry, forgot. So he won't let you use his administrator account to so that you can give yourself full privileges? You will need to learn some real hacks.

There's also this method from an annoying clickbait hacker. No USB drive required, just Advanced System Recovery. Actually, that is more for when you have no account that you can access. You can use the "Sticky Keys" method of replacing sethc.exe with cmd.exe. sethc.exe is owned by SYSTEM, and Windows will run it as the SYSTEM user.

what really is the point of the first video? As for the second video,i dont have a phone to watch it on while i do it,i have very and i mean very,limited hours

DramaKing - July 31, 2024, 1:49 pm

The first video is more of a subject overview while the second is a specific tutorial. If you can't remember the steps, then note them on paper. It might take you only five minutes.

Centsicles - August 3, 2024, 5:10 am

(Jul 31, 2024 01:49 PM)DramaKing Wrote: [\[CITE\]](#) The first video is more of a subject overview while the second is a specific tutorial. If you can't remember the steps, then note them on paper. It might take you only five minutes.

the problem is,my dad uses this laptop (he has an entirely different account that i cant access) what happens if he finds out? Is there any way where i can just look at the password wthout changing it?

DramaKing - August 3, 2024, 5:53 am

(Aug 3, 2024 05:10 AM)Centsicles Wrote: [\[CITE\]](#) the problem is,my dad uses this laptop (he has an entirely different account that i cant access) what happens if he finds out? Is there any way where i can just look at the password wthout changing it?

Best way to do this is to ask him if he can make you an administrator so that you won't get in trouble. But it sounds like you want to know what his password is so that there are no user changes. So what you can do is boot into the Advanced Startup Options / Advanced System Recovery as mentioned after making sure that BitLocker is not enabled. Then open a Command Prompt and enter the following commands.

Code C:

```
cd C:\Windows\System32\config  
copy SAM C:\Users\<username>\  
copy SYSTEM C:\Users\<username>\  
shutdown /r /t 0
```

Then you can download [samdump2](#) and feed it the registry hives in your home folder. It may not be updated with Microsoft's latest encryption, so in that case you can try to find Python installed on the system or download a portable version of Python 3, as well as impacket and run 'python3 secretsdump.py -system SYSTEM -sam SAM LOCAL'.

Or you can use the Sticky Keys method to get a SYSTEM-level Command Prompt as previously mentioned as long as your dad never hits the Shift key five times in succession.

Centsicles - August 3, 2024, 6:15 am

(Aug 3, 2024 05:53 AM)DramaKing Wrote: [\[CITE\]](#) Best way to do this is to ask him if he can make you an administrator so that you won't get in trouble. But it sounds like you want to know what his password is so that there are no user changes. So what you can do is boot into the Advanced Startup Options / Advanced System Recovery as mentioned after making sure that BitLocker is not enabled. Then open a Command Prompt and enter the following commands.

Code C:

```
cd C:\Windows\System32\config  
copy SAM C:\Users\<username>\  
copy SYSTEM C:\Users\<username>\  
shutdown /r /t 0
```

Then you can download [samdump2](#) and feed it the registry hives in your home folder. It may not be updated with Microsoft's latest encryption, so in that case you can try to find Python installed on the system or download a portable version of Python 3, as well as impacket and run 'python3 secretsdump.py -system SYSTEM -sam SAM LOCAL'.

Or you can use the Sticky Keys method to get a SYSTEM-level Command Prompt as previously mentioned as long as your dad never hits the Shift key five times in succession.

ok ok,i think im starting to get this, alright,so to make sure..,to go into advanced startup options i have to press shift + restart,then i can go to cmd prompt,i went there once before,what do you mean by registry hives? Im guessing its something to do with registry editor? If thats the case,i cant change any values on there.

DramaKing - August 3, 2024, 6:20 am

You need admin privs for registry editor. The Command Prompt in WinRE is a back way in. You need the SAM file or 'hive' at C:\Windows\System32\config\SAM for the System Accounts Manager and the SYSTEM hive for the encryption key.

Centsicles - August 3, 2024, 12:06 pm

(Aug 3, 2024 06:20 AM)DramaKing Wrote: [\[CITE\]](#) You need admin privs for registry editor. The Command Prompt in WinRE is a back way in. You need the SAM file or 'hive' at C:\Windows\System32\config\SAM for the System Accounts Manager and the SYSTEM hive for the encryption key.

I'm (painfully obviously) not smarter then you....and i cant understand any of this,sorry if this sounds like im whining,but really i dont understand what this is,so i DO need the registry editor with admin privileges?

DramaKing - August 3, 2024, 12:38 pm

(Aug 3, 2024 12:06 PM)Centsicles Wrote: [\[CITE\]](#) I'm (painfully obviously) not smarter then you....and i cant understand any of this,sorry if this sounds like im whining,but really i dont understand what this is,so i DO need the registry editor with admin privileges?

Sorry if I'm not being clear. I should create a full tutorial on this, well, maybe I can make a video or find one.

Centsicles - August 4, 2024, 1:41 am

(Aug 3, 2024 12:06 PM)Centsicles Wrote: [\[CITE\]](#) I'm (painfully obviously) not smarter then you....and i cant understand any of this,sorry if this sounds like im whining,but really i dont understand what this is,so i DO need the registry editor with admin privileges?

please do.And also if it helps when my dad is putting in his password there are two options,he could put in his account password or he could put in his hotmail password.He forgot the account password so he uses his hotmail one.

DramaKing - August 4, 2024, 4:43 am

(Aug 4, 2024 01:41 AM)Centsicles Wrote: [\[CITE\]](#) please do.And also if it helps when my dad is putting in his password there are two options,he could put in his account password or he could put in his hotmail password.He forgot the account password so he uses his hotmail one.

Uh, Windows accounts should be either Microsoft or local, not both. If he used a PIN, I theoretically would be able to retrieve that.

Centsicles - August 4, 2024, 5:48 am

(Aug 4, 2024 04:43 AM)DramaKing Wrote: [\[CITE\]](#) Uh, Windows accounts should be either Microsoft or local, not both. If he used a PIN, I theoretically would be able to retrieve that.

when it shows up with the uac prompt,it automatically comes up with local,but if i click more choices,it comes up with pin and underneath it is my dads hotmail

DramaKing - August 4, 2024, 6:27 am

(Aug 4, 2024 05:48 AM)Centsicles Wrote: [\[CITE\]](#) when it shows up with the uac prompt,it automatically comes up with local,but if i click more choices,it comes up with pin and underneath it is my dads hotmail

Okay, it's a Microsoft account, at least currently. Let's start over and go step-by-step.

Never mind. At some point, Microsoft changed WinRE / Advanced Startup Options so that the Command Prompt requires an administrator password. We can consider this patched. If you really want this and just can't get a flash drive, you're going to need to do this the hard way. That means BeRoot, Seatbelt, PowerSploit's Privesc and Power-Up, winPEAS, and other tools that will set AV alarm bells ringing. I'll post the related video for you again, the one that goes in-depth. Then there's UAC bypasses. I'll give you one and leave you to find others. Again, MS will have patched some of them, and many others will have AV signatures created for them.

<https://youtu.be/C9GfMfFjhYI?si=-ZTvTb9zReKjQSHz>

[Video: <https://youtu.be/uTcrbNBcoxQ?si=gxm2oPXI1JyFBnGT>]

P.S. Let me also put this Windows Hello PIN-cracking tool here.

<https://github.com/Banaanhangwagen/WINHELLO2hashcat>

Centsicles - August 4, 2024, 8:20 am

(Aug 4, 2024 06:27 AM)DramaKing Wrote: [\[CITE\]](#) Okay, it's a Microsoft account, at least currently. Let's start over and go step-by-step.

Never mind. At some point, Microsoft changed WinRE / Advanced Startup Options so that the Command Prompt requires an administrator password. We can consider this patched. If you really want this and just can't get a flash drive, you're going to need to do this the hard way. That means BeRoot, Seatbelt, PowerSploit's Privesc and Power-Up, winPEAS, and other tools that will set AV alarm bells ringing. I'll post the related video for you again, the one that goes in-depth. Then there's UAC bypasses. I'll give you one and leave you to find others. Again, MS will have patched some of them, and many others will have AV signatures created for them.

<https://youtu.be/C9GfMfFjhYI?si=-ZTvTb9zReKjQSHz>

[Video: <https://youtu.be/uTcrbNBcoxQ?si=gxm2oPXI1JyFBnGT>]

P.S. Let me also put this Windows Hello PIN-cracking tool here.

<https://github.com/Banaanhangwagen/WINHELLO2hashcat>

So i guess i have to watch the video and what does the pin cracker from github do?

DramaKing - August 4, 2024, 9:20 am

(Aug 4, 2024 08:20 AM)Centsicles Wrote: [\[CITE\]](#) So i guess i have to watch the video and what does the pin cracker from github do?

If you have access to the system directories, you can use it to get the PINs for users.

Centsicles - August 4, 2024, 11:02 am

(Aug 4, 2024 09:20 AM)DramaKing Wrote: [\[CITE\]](#) If you have access to the system directories, you can use it to get the PINs for users.

how do i check for if i have access to the system directories

DramaKing - August 4, 2024, 1:52 pm

(Aug 4, 2024 11:02 AM)Centsicles Wrote: [\[CITE\]](#) how do i check for if i have access to the system directories

Run 'whoami' in the Command Prompt. If it prints anything but 'NT Authority\SYSTEM,' you don't. C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Ngc is locked while the system is running and requires the highest privileges. Even Invoke-NinjaCopy and vssadmin require admin privileges. Expect that you will need a series of techniques.

Byte Wizard - August 4, 2024, 4:17 pm

(Aug 4, 2024 01:52 PM)DramaKing Wrote: [\[CITE\]](#) Run 'whoami' in the Command Prompt. If it prints anything but 'NT Authority\SYSTEM,' you don't.

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Ngc is locked while the system is running and requires the highest privileges. Even Invoke-NinjaCopy and vssadmin require admin privileges. Expect that you will need a series of techniques.

No you can just download RunAsSystem or elevate a cmd shell yourself and then you get access to it

As to the contents being locked I got no idea

DramaKing - August 4, 2024, 4:22 pm

(Aug 4, 2024 04:17 PM)Byte Wizard Wrote: [\[CITE\]](#) No you can just download RunAsSystem or elevate a cmd shell yourself and then you get access to it

As to the contents being locked I got no idea

No, he can't elevate. It's a long thread but at least read the original post. The SAM hive is locked by LSASS. I presume that NGC is the same.

Byte Wizard - August 4, 2024, 4:24 pm

(Aug 4, 2024 04:22 PM)DramaKing Wrote: [\[CITE\]](#) No, he can't elevate. It's a long thread but at least read the original post. The SAM hive is locked by LSASS. I presume that NGC is the same.

Ah my mistake

If theres this much restriction on the PC he should really just go talk to his dad about it if he can

Centsicles - August 5, 2024, 2:18 am

(Aug 4, 2024 01:52 PM)DramaKing Wrote: [\[CITE\]](#) Run 'whoami' in the Command Prompt. If it prints anything but 'NT Authority\SYSTEM,' you don't.

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Ngc is locked while the system is running and requires the highest privileges. Even Invoke-NinjaCopy and vssadmin require admin privileges. Expect that you will need a series of techniques.

it just says johnscomputer\john (and yes my name is john) so im guessing i dont have it.

(Aug 4, 2024 04:17 PM)Byte Wizard Wrote: [\[CITE\]](#) No you can just download RunAsSystem or elevate a cmd shell yourself and then you get access to it

As to the contents being locked I got no idea

i really dont know what to do here.

Centsicles - August 6, 2024, 2:38 am

(Aug 4, 2024 09:20 AM)DramaKing Wrote: [\[CITE\]](#) If you have access to the system directories, you can use it to get the PINs for users.

helloooo?

DramaKing - August 6, 2024, 4:14 am

(Aug 6, 2024 02:38 AM)Centsicles Wrote: [\[CITE\]](#) helloooo?

Don't get pushy. It's going to be up to someone else to weigh in. Any other help that I could give would be doing it myself, and I don't think you want that. I've already done a lot for you.

Centsicles - August 6, 2024, 8:30 am

(Aug 6, 2024 04:14 AM)DramaKing Wrote: [\[CITE\]](#) Don't get pushy. It's going to be up to someone else to weigh in. Any other help that I could give would be doing it myself, and I don't think you want that. I've already done a lot for you.

your right i guess.Seemed a bit odd you take a few more hours then you usually do,but thinking back on it maybe you were busy.

Centsicles - August 13, 2024, 12:31 pm

(Aug 6, 2024 04:14 AM)DramaKing Wrote: [\[CITE\]](#) Don't get pushy. It's going to be up to someone else to weigh in. Any other help that I could give would be doing it myself, and I don't think you want that. I've already done a lot for you.

Its been a week without any response,im sorry if i was being a bit pushy,can you please continue helping me?

DramaKing - August 13, 2024, 12:46 pm

(Aug 13, 2024 12:31 PM)Centsicles Wrote: [\[CITE\]](#) Its been a week without any response,im sorry if i was being a bit pushy,can you please continue helping me?

I've given you what I got. From here it will be running scripts, checking for privesc vulnerabilities, trying exploits, injecting code, etc. These are things that you could learn from the materials I provided. I might be able to do it if I had the computer in front of me, but I've done the best that I can through this forum. Maybe someone else has something more, but everyone else seems to have given up also.

Centsicles - August 14, 2024, 8:03 am

(Aug 13, 2024 12:46 PM)DramaKing Wrote: [\[CITE\]](#) I've given you what I got. From here it will be running scripts, checking for privesc vulnerabilities, trying exploits, injecting code, etc. These are things that you could learn from the materials I provided. I might be able to do it if I had the computer in front of me, but I've done the best that I can through this forum. Maybe someone else has something more, but everyone else seems to have given up also.

i mean is there a way to theoretically get my dad's hotmail password,since that is the one he uses for administrator.

DramaKing - August 14, 2024, 8:10 am

(Aug 14, 2024 08:03 AM)Centsicles Wrote: [\[CITE\]](#) i mean is there a way to theoretically get my dad's hotmail password,since that is the one he uses for administrator.

Without admin?

At your age, don't try this: <https://github.com/EricksonAtHome/blackeye>. Didn't even work for another new member who tried it on Windows. A keylogger would do it, but the antivirus would surely quarantine and log it.

ttbr0 - August 14, 2024, 8:18 am

what is your windows version and os build? you should be able to see it in your settings under about

Centsicles - August 15, 2024, 12:42 pm

(Aug 14, 2024 08:10 AM)DramaKing Wrote: [\[CITE\]](#) Without admin?

At your age, don't try this: <https://github.com/EricksonAtHome/blackeye>. Didn't even work for another new member who tried it on Windows. A keylogger would do it, but the antivirus would surely quarantine and log it.

luckily enough,somebody made a keylogger in python,but the keylogger doesnt work when uac is active.Anyway so lets say THEORETICALLY i just use that github tool and maybe somebody on here read my post,is it possible i could get in trouble,and no,it didnt get flagged by my antivirus,just for educational purposes can you tell me the steps on how to download it?

(Aug 14, 2024 08:18 AM)ttbr0 Wrote: [\[CITE\]](#) what is your windows version and os build? you should be able to see it in your settings under about

on windows 11, my os build is os build 22631.3958

DramaKing - August 15, 2024, 12:56 pm

(Aug 15, 2024 12:42 PM)Centsicles Wrote: [\[CITE\]](#) luckily enough,somebody made a keylogger in python,but the keylogger doesnt work when uac is active.Anyway so lets say THEORETICALLY i just use that github tool and maybe somebody on here read my post,is it possible i could get in trouble,and no,it didnt get flagged by my antivirus,just for educational purposes can you tell me the steps on how to download it?

You can either clone the repository with git or click on 'Code' and then 'Download ZIP.' Since it's a shell script, it won't run in Windows without some kind of virtualization or emulation. It would run in Termux for Android. And if your dad realizes that the Microsoft login page is actually a phishing page, you could be in some trouble. I am not recommending this.

(Aug 15, 2024 12:42 PM)Centsicles Wrote: [\[CITE\]](#) on windows 11, my os build is os build 22631.3958

Welp, at least we've ruled out known vulnerabilities.

Centsicles - August 16, 2024, 1:42 am

(Aug 15, 2024 12:56 PM)DramaKing Wrote: [\[CITE\]](#) You can either clone the repository with git or click on 'Code' and then 'Download ZIP.' Since it's a shell script, it won't run in Windows without some kind of virtualization or emulation. It would run in Termux for Android. And if your dad realizes that the Microsoft login page is actually a phishing page, you could be in some trouble. I am not recommending this.

Welp, at least we've ruled out known vulnerabilities.

So my dad would have to put in his credentials for this?

DramaKing - August 16, 2024, 4:20 am

(Aug 16, 2024 01:42 AM)Centsicles Wrote: [\[CITE\]](#) So my dad would have to put in his credentials for this?

He would have to login to the blackeye page like it was the real Microsoft login, yes.

Centsicles - August 16, 2024, 11:02 am

(Aug 16, 2024 04:20 AM)DramaKing Wrote: [\[CITE\]](#) He would have to login to the blackeye page like it was the real Microsoft login, yes.

yeah...maybe we shouldn't do that,my dad is 200% percent not doing that lol,i mean is there any way to create a fake uac,he'll believe a uac for sure,but he would definitely be super suspicious about logging into his hotmail using mine,any other ideas?

DramaKing - August 16, 2024, 2:04 pm

(Aug 16, 2024 11:02 AM)Centsicles Wrote: [\[CITE\]](#) yeah...maybe we shouldn't do that,my dad is 200% percent not doing that lol,i mean is there any way to create a fake uac,he'll believe a uac for sure,but he would definitely be super suspicious about logging into his hotmail using mine,any other ideas?

Never heard of UAC phishing. He'd be really suspicious if a UAC prompt asked him for his password on his administrator account.

Centsicles - August 17, 2024, 1:41 am

(Aug 16, 2024 02:04 PM)DramaKing Wrote: [\[CITE\]](#) Never heard of UAC phishing. He'd be really suspicious if a UAC prompt asked him for his password on his administrator account.

i mean im thinking the only viable way is to find my dads hotmail password

DramaKing - August 17, 2024, 4:21 am

(Aug 17, 2024 01:41 AM)Centsicles Wrote: [\[CITE\]](#) i mean im thinking the only viable way is to find my dads hotmail password

No, it isn't. I'm sorry to say so, but you seem to want everything handed to you. I've given you videos, tools, and lengthy other resources, some of which should work. And you have enough info to do your own research and find fodhelper and other exploits. Don't know if I shared this before, but you'll find plenty of privesc methods by clicking [here](#).

super_sayan - August 17, 2024, 6:13 am

then do it my friend, what's stopping you?

DramaKing - August 17, 2024, 7:05 am

(Aug 17, 2024 06:13 AM)super_sayan Wrote: [\[CITE\]](#) then do it my friend, what's stopping you? UAC is stopping him. Duh. Or you could say lack of knowledge.

super_sayan - August 17, 2024, 7:10 am

(Aug 17, 2024 07:05 AM)DramaKing Wrote: [\[CITE\]](#) UAC is stopping him. Duh. Or you could say lack of knowledge.

lack of motivation as well maybe

Centsicles - August 17, 2024, 12:01 pm

(Aug 17, 2024 04:21 AM)DramaKing Wrote: [\[CITE\]](#) No, it isn't. I'm sorry to say so, but you seem to want everything handed to you. I've given you videos, tools, and lengthy other resources, some of which should work. And you have enough info to do your own research and find fodhelper and other

exploits. Don't know if I shared this before, but you'll find plenty of privesc methods by clicking [here](#).

I mean do you know how to bypass admin? If you do,dont worry,i guess its up to me now lol,but i am curious,and 1-10 how hard would you say bypassing uac is? (in my scenario)

DramaKing - August 17, 2024, 12:06 pm

(Aug 17, 2024 12:01 PM)Centsicles Wrote: [\[CITE\]](#) I mean do you know how to bypass admin? If you do,dont worry,i guess its up to me now lol,but i am curious,and 1-10 how hard would you say bypassing uac is? (in my scenario)

Answer: It depends. Different vulnerabilities will be present on different setups, and antiviruses will have more or less of a problem with specific scripts used to check for vulnerabilities and binaries used to exploit those vulnerabilities.

Centsicles - August 18, 2024, 5:40 am

(Aug 17, 2024 12:06 PM)DramaKing Wrote: [\[CITE\]](#) Answer: It depends. Different vulnerabilities will be present on different setups, and antiviruses will have more or less of a problem with specific scripts used to check for vulnerabilities and binaries used to exploit those vulnerabilities. well do you have any scripts to check for them?

DramaKing - August 18, 2024, 6:14 am

(Aug 18, 2024 05:40 AM)Centsicles Wrote: [\[CITE\]](#) well do you have any scripts to check for them?
(Aug 4, 2024 06:27 AM)DramaKing Wrote: [\[CITE\]](#) Okay, it's a Microsoft account, at least currently. Let's start over and go step-by-step.

Never mind. At some point, Microsoft changed WinRE / Advanced Startup Options so that the Command Prompt requires an administrator password. We can consider this patched. If you really want this and just can't get a flash drive, you're going to need to do this the hard way. That means BeRoot, Seatbelt, PowerSploit's Privesc and Power-Up, winPEAS, and other tools that will set AV alarm bells ringing. I'll post the related video for you again, the one that goes in-depth. Then there's UAC bypasses. I'll give you one and leave you to find others. Again, MS will have patched some of them, and many others will have AV signatures created for them.

<https://youtu.be/C9GfMfFjhYI?si=-ZTvTb9zReKjQSHz>

[Video: <https://youtu.be/uTcrbNBcoxQ?si=gxm2oPXI1JyFBnGT>]

P.S. Let me also put this Windows Hello PIN-cracking tool here.

<https://github.com/Banaanhangwagen/WINHELLO2hashcat>

Do you need me to put links? The hacktricks.xyz page is a master list for privesc itself.

<https://github.com/peass-ng/PEASS-ng>

<https://github.com/GhostPack/Seatbelt>

<https://github.com/AlessandroZ/BeRoot>

<https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc>

<https://hackforums.net/search.php?action=results&sid=3dde8c5135ca4510e93329f763c7c5d5&sortby=&order=desc>

<https://github.com/redteamsocietegenerale/DLLirant>

<https://github.com/gentilkiwi/mimikatz> (Windows password extractor)

If you have specific questions about the output of a tool or how to exploit a vulnerability, it would be

time to move to a new thread or convo.

Centsicles - August 18, 2024, 12:04 pm

(Aug 18, 2024 06:14 AM)DramaKing Wrote: [\[CITE\]](#) Do you need me to put links? The hacktricks.xyz page is a master list for privesc itself.

<https://github.com/peass-ng/PEASS-ng>
<https://github.com/GhostPack/Seatbelt>
<https://github.com/AlessandroZ/BeRoot>
<https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc>

<https://hackforums.net/search.php?action=results&sid=3dde8c5135ca4510e93329f763c7c5d5&sortby=&order=desc>
<https://github.com/redteamsocietegenerale/DLLirant>
<https://github.com/gentilkiwi/mimikatz> (Windows password extractor)

If you have specific questions about the output of a tool or how to exploit a vulnerability, it would be time to move to a new thread or convo.

alright dude thanks ??,you play any steam games? Let me gift you some games dude,i dont know if you heard about valve's new game called deadlock but i got early acces,i can invite you :)

Centsicles - August 21, 2024, 4:27 am

(Aug 18, 2024 06:14 AM)DramaKing Wrote: [\[CITE\]](#) Do you need me to put links? The hacktricks.xyz page is a master list for privesc itself.

<https://github.com/peass-ng/PEASS-ng>
<https://github.com/GhostPack/Seatbelt>
<https://github.com/AlessandroZ/BeRoot>
<https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc>

<https://hackforums.net/search.php?action=results&sid=3dde8c5135ca4510e93329f763c7c5d5&sortby=&order=desc>
<https://github.com/redteamsocietegenerale/DLLirant>
<https://github.com/gentilkiwi/mimikatz> (Windows password extractor)

If you have specific questions about the output of a tool or how to exploit a vulnerability, it would be time to move to a new thread or convo.

Ok well the first video does not work,first of all if you scroll down you can see somebody named "jdgregon" who said "This is NOT a privilege escalation vulnerability. The user must already be a member of the Local Administrators group. This only bypasses the UAC prompt." and unfortunately i am not a member of the local administrators group.Atleast the video is ruled out,havent tried your other links,will get back to you :)

EDIT: So underneath the video i found,this guy who has like an updated version or something??,heres the link:<https://www.youtube.com/watch?v=nBNmupIBI54>

Ok so the problem is,im super confused with all of this stuff,would you mind helping out? I've been stuck on what to do for like 15 minutes

Centsicles - August 22, 2024, 5:50 am

(Aug 18, 2024 06:14 AM)DramaKing Wrote: [\[CITE\]](#) Do you need me to put links? The hacktricks.xyz page is a master list for privesc itself.

<https://github.com/peass-ng/PEASS-ng>
<https://github.com/GhostPack/Seatbelt>
<https://github.com/AlessandroZ/BeRoot>
<https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc>

<https://hackforums.net/search.php?action=results&sid=3dde8c5135ca4510e93329f763c7c5d5&sortby=&order=desc>

<https://github.com/redteamsocietegenerale/DLLirant>
<https://github.com/gentilkiwi/mimikatz> (Windows password extractor)

If you have specific questions about the output of a tool or how to exploit a vulnerability, it would be time to move to a new thread or convo.

yeah,i've tried most of this stuff, a few of them got blocked my antivirus (which i cant disable) and some of them i dont even know how to run,i always had trouble with getting stuff to run on github after downloading the zip

DramaKing - August 22, 2024, 6:30 am

(Aug 21, 2024 04:27 AM)Centsicles Wrote: [\[CITE\]](#) Ok well the first video does not work,first of all if you scroll down you can see somebody named "jdgregson" who said "This is NOT a privilege escalation vulnerability. The user must already be a member of the Local Administrators group. This only bypasses the UAC prompt." and unfortunately i am not a member of the local administrators group.Atleast the video is ruled out,havent tried your other links,will get back to you :)

EDIT: So underneath the video i found,this guy who has like an updated version or something??,heres the link:<https://www.youtube.com/watch?v=nBNmuplBI54>

Ok so the problem is,im super confused with all of this stuff,would you mind helping out? I've been stuck on what to do for like 15 minutes

IAmJakoby is a well-known whitehat. I've used some of his code before. Now this does get detected by antivirus.

I did just have a thought about whether your antivirus and/or AMSI gets loaded in Safe Mode.

Centsicles - August 22, 2024, 12:02 pm

(Aug 22, 2024 06:30 AM)DramaKing Wrote: [\[CITE\]](#) IAmJakoby is a well-known whitehat. I've used some of his code before. Now this does get detected by antivirus.

I did just have a thought about whether your antivirus and/or AMSI gets loaded in Safe Mode. what should i do now? I just need help with some of the code

DramaKing - August 22, 2024, 7:36 pm

I did try running in Safe Mode, and the UAC bypass script completed successfully. Windows Defender flagged nothing.

Centsicles - August 23, 2024, 12:54 pm

(Aug 22, 2024 10:23 PM)blyat1337 Wrote: [\[CITE\]](#) So much yapping.. There are methods that completely fly under defender and from win7 till win11. could you help me?

(Aug 22, 2024 07:36 PM)DramaKing Wrote: [\[CITE\]](#) I did try running in Safe Mode, and the UAC bypass script completed successfully. Windows Defender flagged nothing.

do you mean the jakoby script? And if so can you help me im so confuseddd

Tyr - August 23, 2024, 1:44 pm

(Jul 29, 2024 11:38 AM)Centsicles Wrote: [\[CITE\]](#) How do i bypass uac,its been going on for a decade,its super annoying had this for my whole life.I dont have access to bios aswell,please help (also i dont have a usb stick and i can access cmd but it needs admin for certain command's,e.g changing admin password)

This guys gonna brick his PC

Centsicles - August 25, 2024, 7:24 am

(Aug 23, 2024 01:44 PM)Osiris? Wrote: [\[CITE\]](#) This guys gonna brick his PC
uh,sorry brother i only play csgo and half life