

Forum:[Hack Forums](#)

Thread: [Privilege Escalation on Havoc](#)

AnonUserBB - January 20, 2025, 11:34 pm

Hello to all!

Im trying to know how to make privilege Escalation on Havoc Framework C2, and watching tutorials is going a little bit shitty since all the people uses the same script that no longer works on windows machines, so im trying to know if there is some good tools for this or maybe I just need to programming my self this tools (im so fucking bad on programming)

Do you know some tools that are going to make this Privilege Escalation?

Thanks for reading!

AnonUserBB - January 21, 2025, 4:05 am

Havoc doesn't have a incorporated privilege escalation, when you run a code for escalation do you have more available options but it doesn't have any native tool for escalation.

I see tutorials using the same script and doesn't work on the latest windows 10 or 11 machines so its kinda "ridiculous" to teach people script tools that no longer work.

I need sometype of script that works for this or sometype of information to try bulding it myself (its going to be complicated to built it myself since I very bad at programming) but I give it a chance to learn and try it to built it my self if I don't have other options.

DramaKing - January 21, 2025, 11:33 am

Fodhelper works. SilentCleanup bypasses UAC if the user is an administrator. BeRoot, Seatbelt, winPEAS can find security misconfigurations, DLL hijacking vulnerabilities, etc. You do, of course, need to disable antivirus.

AnonUserBB - January 21, 2025, 10:17 pm

Thanks for give me the tools but I have a problem, how do I deactivate Windows Defender from powershell to escalate privileges?

I don't see useful information for that or even if its posible, maybe I see thing for Windows 7 but no for new windows versions

Sorry for the last comment I didn't know that Fodhelper was a windows defender Bypass.

Whatever fodhelper is not working and BeRoot is not working too

1-BeRoot on the victim machine needs python to be installed well (very low percentage of people are going to have python installed)

2-When im running BeRoot on havoc from powershell the windows defender detects the malware and shut down the listener from the windows machine

DramaKing - January 22, 2025, 6:00 am

(Jan 21, 2025 11:17 PM)AnonUserBB Wrote: [\[CITE\]](#) Thanks for give me the tools but I have a

problem, how do I deactivate Windows Defender from powershell to escalate privileges?

Code Start-Process powershell.exe -Verb runAs

Set-MpPreference -DisableRealtimeMonitoring \$true -DisableBehaviorMonitoring \$true

-DisableScriptScanning \$true (Jan 21, 2025 11:17 PM)AnonUserBB Wrote: [\[CITE\]](#) 1-BeRoot on the victim machine needs python to be installed well (very low percentage of people are going to have python installed)

2-When im running BeRoot on havoc from powershell the windows defender detects the malware and shut down the listener from the windows machine

This is not true. And I guess you've learned something about antivirus.

AnonUserBB - January 22, 2025, 6:58 am

When I try to execute BeRoot tells me that some programs are failed to be installed and they are all python programs, when I installed python on the victim machine it gives me the second error (it detects the C2 framework and delete it)

I try later the powershell commands and I tell you if they work, thanks

Script for disable Windows defender works but I need admin permissions to make work the command so its kinda contradictory

If i want to elevate privileges I need to disable Windows Defender to make work the command, and If I want to disable Windows Defender I need to be admin. Looks imposible to do.

You can tell me in what im incorrect? I do not understand how to do this right

benio2 - January 22, 2025, 3:13 pm

(Jan 21, 2025 12:33 PM)DramaKing Wrote: [\[CITE\]](#) Fodhelper works. SilentCleanup bypasses UAC if the user is an administrator. BeRoot, Seatbelt, winPEAS can find security misconfigurations, DLL hijacking vulnerabilities, etc. You do, of course, need to disable antivirus.

Fodhelper does not work and most other similar methods like silentcleanup do not work either. Lets assume this is a pc running basic security and any registry tampering will trigger a detection.

You can do cmstplua right here:

<https://github.com/anand101285/UACBypass-CMSTPLUA>

So basically turn your program into a shellcode file, then use havoc c2 to run the shellcode, then when its run from memory, your shit will run the cmstplua script, direct it to the exe you're trying to execute as admin, bam and there you have it.

Much better if you do some dll hijacking though, you can create an exploit for one of these dlls here: <https://hijacklibs.net/>

Essentially you will have to do some coding to make it work properly. That is without a doubt.

DramaKing - January 23, 2025, 4:32 am

What I don't get is that getting Havoc to run with WD enabled seems to be no problem, but the previously mentioned executables are.

AnonUserBB - January 23, 2025, 8:40 am

I don't understand it neither, maybe a problem of ofuscation of the exec that windows defender detects a malicious behavior but im not sure...

If you don't know when you are for sure more educated than me in this topic im not going to

undestend neither...

DramaKing - January 23, 2025, 12:04 pm

(Jan 23, 2025 09:40 AM)AnonUserBB Wrote: [\[CITE\]](#) I don't undestend it neither, maybe a problem of ofuscation of the exec that windows defender detects a malicious behavior but im not sure...

If you don't know when you are for sure more educated than me in this topic im not going to undestend neither...

My research indicated that Havoc iwas no longer FUD, so I assumed that you were crypting the initial payload but not the later stages. ?

AnonUserBB - January 23, 2025, 11:25 pm

Yeah, first it will be ofuscated on versions like windows 7,10 or even some non-updated versions of Windows 11 but when it comes to put some other scripts to elevate privileges or establish persistence the software is detected and eliminated with Windows Defender.