

Forum:[Hack Forums](#)

Thread: [\[POC\] From Administrator to Nt Authority\System](#)

Paskowsky - November 18, 2019, 10:46 am

From Administrator To Nt Authority\System

If you want check out my blog where I explain how it works!

<https://blog.dreamsoftwares.cc/2019/11/18/from-standard-user-to-nt-authoritysystem/>

Code :

Hope you enjoy and if you have any question or suggestion please comment down here!

gigajew - November 18, 2019, 5:06 pm

Cool post, but it's no exploit just basic token cloning to gain other privileges?

Paskowsky - November 19, 2019, 1:44 am

(Nov 18, 2019 06:06 PM)gigajew Wrote: [\[CITE\]](#) Cool post, but it's no exploit just basic token cloning to gain other privileges?

Yes, I've never mentioned exploiting ?

Have a good day ?

Accord - November 21, 2019, 7:12 pm

Your blog is a good read for a begginer like me. I followed everything and what is being happened.

Kallu609 - November 21, 2019, 8:05 pm

This is great repo too: [GitHub - rootm0s/WinPwnage: UAC bypass, Elevate, Persistence and Execution methods](#)

There's 7 different elevation techniques there.

Dat Phan - November 21, 2019, 11:24 pm

please can you give me pass

Kallu609 - November 22, 2019, 2:44 am

(Nov 22, 2019 12:24 AM)Dat Phan Wrote: [\[CITE\]](#) please can you give me pass

What pass? Password? Where? Are u ok? ?

Fr3eD0M - November 22, 2019, 7:10 am

I have read your blog.Very nice tutorial.

Thanks for share

0x414243ffffff - November 28, 2019, 1:41 pm

ermm you can do the same in metasploit i guess for token stealing

BadByte - November 30, 2019, 7:12 pm

Nice and Thanks, i'll try this!

tux1 - December 1, 2019, 7:15 am

Very interesting, thanks for sharing!

Hannah - December 12, 2019, 4:05 pm

Nice, thanks for sharing. Will use this soon

BadByte - January 9, 2020, 10:07 am

escalation doesn't work for me!

I integrated it into my client, it all seems to be performing as it should be but nothing is happening on the side escalation!.

Tested on Win7(32) for moment and nothing and without AV.

Always working? It's me (my code..)?

Just to known or to understand where is my error, just to advance..

Ty.

Cap1

Spoiler [\(Click to View\)](#)

Cap2

Spoiler [\(Click to View\)](#)

Cap3

Spoiler [\(Click to View\)](#)

Cap4

Spoiler [\(Click to View\)](#)

I just modified in the Class the PathFileName, isn't "winlogon", the name of target_process is send by the server (see capture) but i think all is OK, my code seem just, then i don't know...

Paskowsky - January 9, 2020, 10:23 am

You have to be atleast in the administrator group to escalate to ntauthority.

This is not an exploit!

Regards,
Paskowsky

BadByte - January 9, 2020, 10:46 am

(Jan 9, 2020 11:23 AM)Paskowsky Wrote: [\[CITE\]](#) You have to be atleast in the administrator group to escalate to ntauthority.

This is not an exploit!

Regards,
Paskowsky

Ok, but my user is the admin, i haven't verified but i think this account is in admin group!
I'll apply the modifications and i'll add an function to be sure the user is in good group..

Thx for reply, i'll try so later, i'm in pause ^^ :p

Re.
I'm already in admin groupe :(

I spent the night on it, it's not that the class is complex, it's just that it works with a client suddenly every time I have to recompile, test and it's boring serious: p
I checked the membership of the user in the admin group admin it is, ok, I get all the SIDs of the user, I checked if it is a SID / adm_grp and if not then I add it to the group and if yes then: escalation (filepath), but none of this allows you to see this Class escalate cmd.exe ..

In any case it gave me ideas, I will work on SIDs (cloning, copying, new ..)

Celiform - January 10, 2020, 9:15 pm

(Jan 9, 2020 11:07 AM)BadByte Wrote: [\[CITE\]](#) escalation doesn't work for me!

I integrated it into my client, it all seems to be performing as it should be but nothing is happening on the side escalation!.
Tested on Win7(32) for moment and nothing and without AV.

Always working? It's me (my code..)?
Just to known or to understand where is my `_error_`, just to advance..

Ty.

Cap1
Spoiler [\(Click to View\)](#)
Cap2
Spoiler [\(Click to View\)](#)
Cap3
Spoiler [\(Click to View\)](#)
Cap4
Spoiler [\(Click to View\)](#)

I just modified in the Class the PathFileName, isn't "winlogon", the name of target_process is send by the server (see capture) but i think all is OK, my code seem just, then i don't know...
no offence brother but tat ui is trash

BadByte - January 11, 2020, 3:13 am

whaoouu, What a constructive comment !! Nice!

the main thing is that the major part of the functionalities work correctly then the theme 'is
secondary for the moment, you offer what to your users, the colors or tools, I prefer the bro tools, I
will end up adjusting the theme

your UI is trash: lol! y u r welcome, i'll modify this, ty for help
(lol)

your popularity is trash too: Popularity:
-6

@Paskowsky: working now!

Ty bro :) Good job
Next function.. and UI for Mr.... :p

New UI