

Forum:[Hack Forums](#)

Thread: [Escalate the process to SYSTEM level](#)

R4NS0M - December 5, 2018, 6:46 am

I'm willing to make a file that cannot be killed by Task Manager, CMD etc. So my idea was to make a process to System level, when the user wants to kill it it prompts Access Denied. I'm gratefully thankful for every help.

Voqet - December 6, 2018, 4:24 am

A simple google search, 'how to elevate user access using python' provided me with results; albeit I'm not sure if it is what you're after as the question you provided is too vague.

Try this: <https://gist.github.com/GaryLee/d1cf2089c3a515691919>

R4NS0M - December 6, 2018, 8:42 am

(Dec 6, 2018 05:24 AM)Voqet Wrote: [\[CITE\]](#) A simple google search, 'how to elevate user access using python' provided me with results; albeit I'm not sure if it is what you're after as the question you provided is too vague.

Try this: <https://gist.github.com/GaryLee/d1cf2089c3a515691919> Thanks dude but is there any way to make the Privileges higher to SYSTEM, so the user can't terminate it that It will say Access Denied?

jammy47 - December 6, 2018, 10:32 am

(Dec 5, 2018 07:46 AM)Vakaris Wrote: [\[CITE\]](#) I'm willing to make a file that cannot be killed by Task Manager, CMD etc. So my idea was to make a process to System level, when the user wants to kill it it prompts Access Denied. I'm gratefully thankful for every help.

dll injection or dll hijacking should help. unquoted service paths in registry etc. Social engineering can also help.

R4NS0M - December 6, 2018, 11:09 am

(Dec 6, 2018 11:32 AM)jammy47 Wrote: [\[CITE\]](#) dll injection or dll hijacking should help. unquoted service paths in registry etc. Social engineering can also help. Thanks for such great Ideas, will this work with a .exe File ? Because I'm using Pyinstaller.

jammy47 - December 6, 2018, 11:12 am

You can make such things in python and also hook api using python in theory.

<http://www.cnblogs.com/LittleHann/p/6133733.html>

then use those .py scripts to make .exe . So yup it can be done.

quite frankly, you can get such things done better with c++, x86 and winapi/windows internals knowledge. Its not very hard and will give you an edge in the long run.

Saitama - December 8, 2018, 8:05 am

(Dec 6, 2018 11:32 AM)jammy47 Wrote: [\[CITE\]](#) dll injection or dll hijacking should help. unquoted service paths in registry etc. Social engineering can also help.

Social Engineering needed to make a persistent process???? What are you talking about OMG

LOOL ? ?

(Dec 6, 2018 12:12 PM)jammy47 Wrote: [\[CITE\]](#) You can make such things in python and also hook api using python in theory.

<http://www.cnblogs.com/LittleHann/p/6133733.html>

then use those .py scripts to make .exe . So yup it can be done.

quite frankly, you can get such things done better with c++, x86 and winapi/windows internals knowledge. Its not very hard and will give you an edge in the long run.

nibba do you know what the op is asking

Infamia - December 10, 2018, 12:55 am

(Dec 8, 2018 09:05 AM)Saitama Wrote: [\[CITE\]](#) Social Engineering needed to make a persistent process???? What are you talking about OMG LOOL ? ?

nibba do you know what the op is asking

answer the question if you're going to insult everyone else's responses, brainlet

pro tip: the OP is asking how to run his application under SYSTEM, not to have it remain persistent

py_god - December 11, 2018, 4:38 am

Realistically if there is a process running you'll be able to end it one way or another, unless your victim tries twice and gives up and moves on advanced disinfection will work to remove what ever you managed to drop on the system.

A better method would be to migrate processes asap.

If you're using metasploit you can use the get system command which as you might guess... gets system, granted you need admin on the box.

Once you have it MIGRATE PROCESSES don't start new ones, logs are generated for new processes ;)

Saitama - March 6, 2019, 10:43 am

(Dec 10, 2018 01:55 AM)Infamia Wrote: [\[CITE\]](#) answer the question if you're going to insult everyone else's responses, brainlet

pro tip: the OP is asking how to run his application under SYSTEM, not to have it remain persistent late reply but yeah, lmao retard others were spewing bullshit with their answer.