

Forum:[Hack Forums](#)

Thread: [Can a service process open a handle to a system process?](#)

eskimo1 - October 29, 2016, 3:16 pm

Say you got a service process running your code.

Now, given that youre running at NT AUTHORITY\SYSTEM would you be able to open a process handle to a system process say lsass.exe?

If yes, can you tell me where it states so? (I was unable to google my way to this info)

My system is Windows 7 x64.

Regards

Asdethprime - October 29, 2016, 6:27 pm

Hi eskimo1 ,

Yes it is very possible to do so provided the user you have compromised as the authority to do it.

As per where it says so; Metasploit has a feature whose job is pretty much just that... directly accessing a system API on Windows operating system called Railgun.

<https://github.com/rapid7/metasploit-framework/wiki/How-to-use-Railgun-for-Windows-post-exploitation>

eskimo1 - October 29, 2016, 6:59 pm

(Oct 29, 2016 06:27 PM)Asdethprime Wrote: [CITE](#) Hi eskimo1 ,

Yes it is very possible to do so provided the user you have compromised as the authority to do it.

As per where it says so; Metasploit has a feature whose job is pretty much just that... directly accessing a system API on Windows operating system called Railgun.

~~

Thats the conclusion I've come to aswell - if you're running as NT Authority there shouldn't be anything stopping you from accessing csrss.exe lsass.exe and other protected processes. (Not taking into consideration kernelmode mechanisms).

Gonna try it out, thanks

Regards

Alright, I've tried it out now, and I've come to this conclusion:

Any process can access any process running in usermode - however system / 'Protected Processes' will only allow certain permissions, those being:

PROCESS/THREAD_QUERY_LIMITED_INFORMATION
PROCESS_TERMINATE

PROCESS/THREAD_SUSPEND_RESUME
SYNCHRONIZE

However another process running protected mode aswell will have the benefit of being able to bypass these checks and use ACLs instead.

Regards