

Forum:[Hack Forums](#)

Thread: [Memory dump on a windows pc with UAC enabled?](#)

chaose_marine - September 3, 2016, 2:25 pm

I was thinking through some ideas so i could write some exploit scripts ? with the help of volatility and I've ran in to a problem, how would i go about getting a memory dump of a windows (7) PC that has UAC enabled.

I've seen plenty of tools which get memory dumps, but have yet to find a way to get a memory dump with UAC.

Are there any tools out there that any one knows of that can do this?

Or

Is there a way to get a memory dump with Python?

craig131 - September 3, 2016, 9:18 pm

Yeah, UAC does not take kindly to that kind of thing. The Invoke-BypassUAC.ps1 script on Powershell Empire (it's also a metasploit module 'bypassuac') can be used to get around it.

chaose_marine - September 5, 2016, 12:29 pm

(Sep 3, 2016 09:18 PM)craig131 Wrote: [\[CITE\]](#) Yeah, UAC does not take kindly to that kind of thing. The Invoke-BypassUAC.ps1 script on Powershell Empire (it's also a metasploit module 'bypassuac') can be used to get around it.

Thanks for the reply man. Personally I've tried to avoid metasploit as much as i can so i could learn the ins and outs first hand so i'm lacking in that department, could you maybe go into a little more detail on how i could do this?

Also would i be able to call this said script from in python?

Thank you

phugqr - September 5, 2016, 4:20 pm

As mentioned before its a powershell script which can be run in powershell empire.

Do some searching on powershell empire.

chaose_marine - September 7, 2016, 8:34 am

(Sep 5, 2016 04:20 PM)phugqr Wrote: [\[CITE\]](#) As mentioned before its a powershell script which can be run in powershell empire.

Do some searching on powershell empire.

Cool, Thanks for the help