

Forum:[Hack Forums](#)

Thread: [Windows Reverse Shell Source Code](#)

ApexLead - August 1, 2018, 3:29 am

Hey guys,

I'm trying to implement the simplest and shortest CPP Reverse Shell Code (no evasion methods or anything) withing a code of mine for educational purposes about AVs.

I'm new to CPP and trying to learn it the hard way, but couldn't find anything that can help me.

Can someone help me with it? Or direct me to a source code that can be found somewhere?

Thanks upfront :)

HFDone - August 1, 2018, 4:04 am

<http://sh3llc0d3r.com/windows-reverse-shell-shellcode-i>

ApexLead - August 1, 2018, 6:03 am

(Aug 1, 2018 04:04 AM)HFDone Wrote: [\[CITE\]](#)

<http://sh3llc0d3r.com/windows-reverse-shell-shellcode-i>

Thanks mate, Ive seen it already but he said it only works on Windows 7, I'm looking for something that's version independent :/

HFDone - August 1, 2018, 6:08 am

you said you want cpp code

asm (not hardcoded addresses)

<http://ly0n.me/2015/08/29/windows-reverse-shell-universal-shellcode>

ApexLead - August 1, 2018, 6:21 am

(Aug 1, 2018 06:08 AM)HFDone Wrote: [\[CITE\]](#) you said you want cpp code

asm (not hardcoded addresses)

<http://ly0n.me/2015/08/29/windows-reverse-shell-universal-shellcode>

Hmm apparently I don't understand what it means then, can you explain what hardcoded addresses mean? Isn't there a CPP code that works on all Windows versions?

HFDone - August 1, 2018, 7:19 am

as you can see in the first link theres c code and assembly code at the bottom

to use the c code you compile it to exe and run it on the victim any win os then you can connect to its ip and send commands

shellcode means asm bytes code you code the reverse shell in asm so you can convert it to shellcode

the problem with shellcode is the api calls which their address is different for each win os this is the different between the asm code in the first link and the second

ApexLead - August 1, 2018, 9:07 am

(Aug 1, 2018 07:19 AM)HFDone Wrote: [\[CITE\]](#) as you can see in the first link theres c code and assembly code at the bottom

to use the c code you compile it to exe and run it on the victim any win os then you can connect to its ip and send commands

shellcode means asm bytes code you code the reverse shell in asm so you can convert it to

shellcode

the problem with shellcode is the api calls which their address is different for each win os

this is the different between the asm code in the first link and the second

Thanks for the explanation but I don't really get what shellcode means.. is it like a programming language?

And is it possible writing a Reverse-Shell with CPP that will run on all Windows versions?

HFDone - *August 1, 2018, 11:12 am*

<https://en.wikipedia.org/wiki/Shellcode>

you can but you will need to convert it to asm and then to shellcode bytes see the first link

the different is that to get it to work on all win os you need to loop through the dlls and the api calls address see the second link