

Forum:[Hack Forums](#)

Thread: [Networking skills in Malware Analysis](#)

fin3x - November 10, 2017, 12:50 am

Hello everyone

I was wondering how much networking skill is enough?

Right now I'm about to start learning some basic about wireshark and read the Practical packet analysis and then read Computer Networks A Systems Approach book.

keep in mind that I want to learn Malware Analysis. Should I learn how to code C/C++ or Python (*) from the network side of each language? (Does it help me to learn how a malware spread through a network and how I can stop it?)

(*) book references to learn the network programming:
{

Foundation of Python Network Programming 3rd.Edition

C++ Network Programming Mastering Complexity With ACE And Patterns Volume 1 and 2

UNIX Network Programming Networking APIs Sockets And XTI Volume 1 and 2

}

Also do you think I need to reconsider the books that I need to learn the fundamentals of network programming?

Thank you in advance

CyberStrike - November 10, 2017, 1:05 am

Learn C and some assembly as well, and make sure to understand the Windows API. Malware comes in many different flavors like VB .NET. Also get familiar with IDA there is a free IDA 5.0 you can grab also

[https://beginners\[.\]re/](https://beginners[.]re/)

That is a free reverse engineering book, check out Radare2 also You will need a Windows VM on github there is a powershell script to check a windows machine in to a decent shape for RE work it's called FLARE-VM. It just installed things you need. Umm Let's see Remnux that is a linux distro that you can use also for reversing work. Github has some great resources.

[https://github\[.\]com/wtsxDev/reverse-engineering](https://github[.]com/wtsxDev/reverse-engineering)

Remember that if you cannot reverse the malware you will be looking at functions in assembly and from there you write the code yourself, although something like IDA or Hopper can help. Well I hope this helps, and in the Advanced hacking section there is a sub forum for RE.

fin3x - November 10, 2017, 5:26 am

(Nov 10, 2017 02:05 AM)sirru5h Wrote: [\[CITE\]](#) Learn C and some assembly as well, and make sure to understand the Windows API. Malware comes in many different flavors like VB .NET. Also get familiar with IDA there is a free IDA 5.0 you can grab also

beginners[.]re/

That is a free reverse engineering book, check out Radare2 also You will need a Windows VM on github there is a powershell script to check a windows machine in to a decent shape for RE work it's called FLARE-VM. It just installed things you need. Umm Let's see Remnux that is a linux distro that you can use also for reversing work. Github has some great resources.

github[.]com/wtsxDev/reverse-engineering

Remember that if you cannot reverse the malware you will be looking at functions in assembly and from there you write the code yourself, although something like IDA or Hopper can help. Well I hope this helps, and in the Advanced hacking section there is a sub forum for RE.

thank you so much for the great resources ?

right now I'm learning C and Assembly and for the network part and the algorithm of how the malwares are spreading I'm in the right track then?

SIM-3615281 - November 10, 2017, 11:59 am

(Nov 10, 2017 06:26 AM)fin3x Wrote: [\[CITE\]](#) thank you so much for the great resources ?

right now I'm learning C and Assembly and for the network part and the algorithm of how the malwares are spreading I'm in the right track then?

Trie to get as much information as you can. Keep yourself up to date and trie to understand how new malware works if possible it isn't that simple but if you put some effort in you will improve. Programming languages are important too.