

Forum:[Hack Forums](#)

Thread: [Intermediate programmer need some advice.](#)

Adam2017 - December 1, 2018, 5:04 pm

Hello guys,

I have been programming in C++ on and off for about 3 years now and I am at the point where I feel comfortable with the language, I have used libraries such as SDL and have made a few games but to be honest game dev isn't really my thing, obviously I'm here so I'm more interested in how machines work and how they can be exploited (not for malicious purposes ofc),

I have also a good idea how a computer works, I know about logic gates (encoders, decoders, flip flops, binary counters etc), boolean algebra to simplify logic gates, not a great understanding of Operating systems but that is a work in progress, and I have a grasp on the basics of how memory, processors, opcode work.

so yeah my question is what libraries or API's should I learn to start to understand how to exploit systems or even how to write my own exploits?

if someone could point be in the right direction and give me a run down on what I should know and how/where to learn it, would be great

thanks

Europa - December 2, 2018, 6:48 am

If you want to learn how to write your own exploits and understand how OS security works on Windows for example you would be interested into advancing research into OS internals which will increase your knowledge in understanding how the OS works. Look up windows internals, windows system programming books for understanding win exploitation and purchase a copy of them. Some of the win api's documented inside them include PSAPI and some functions that involve direct communication with ntoskrnl.exe for e.g NtQuerySystemInformation (to grab all running PIDs), EnumDeviceDrivers (retrieve load addresses from each specific installed driver on the system), ReadProcessMemory etc which are just some. Learn how the hypervisor kernel works, loader, boot driver, I/O manager etc. There's lots you'll need to learn but if you put the time and dedication you'll get through it.

Adam2017 - December 3, 2018, 2:06 pm

Thanks Europa, great insight :) I will look into it!