LEARN EXPLOIT DEVELOPMENT WHILE AVOIDING THE PLAGUE

Author: dropzone

This article is a complement to the following video: https://www.youtube.com/watch?v=Eu9eArjLS_E (42min)

With so many countries recommending self-isolation in the past, little while we thought it might be useful to recommend some excellent learning resources to help enable you make the most of the extra time you might find yourself with.

The *Youtube* video itself contains a discussion about all of the resources, but to save some time, I've listed the bullet points below. Though **I do recommend giving the video a watch or listen**, we discuss all of the resources and what we recommend from them, but we also talk about some related information like whether or not you should reference write-ups when learning *(while talking about Nightmare)* and the benefit of learning out-dated material *(during the Open Security Training discussion)* so there is good content besides just the list.

Open Security Training

- Introduction to Software Exploits: This is my go-to recommendation for anyone getting started with exploit development. Even more so than *Hacking: Art of Exploitation*. Its a reasonably gentle introduction, it does assume you know some C and x86.
- Introductory Intel x86: *Really* dry class, but its good if you can get through it. Covers the fundamentals you need to know, and not a lot of crap to dig through.
- Life of Binaries: Great course, can be a little rough depending on your background but its a good source of just getting some of the found additional knowledge and understanding the whole process.
- Exploits 2: Exploitation in the Windows Environment: Another good course, its pretty dated at this point but we discuss the merits of learning the history before diving into modern exploitation in the video during this section.

Web Security Academy

- From the authors of the *Web Application Hackers Handbook*, rather than updating the book they've produced an online lab environment they can keep up-to-date. Covers several web-related topics and provides labs for you to play around with the issues.
- Solid resource, even if just to play around with an issue or two rather than working through everything.

Nand2tetris

- This is less about the exploit *dev*, and just good for getting that found additional, breadth of knowledge. Work through building a computer from *NAND* gates to building and running a Tetris clone. Its the type of holistic understanding that won't initially seem to matter but will eventually pay off when you need to start digging deep you'll have an understanding of the necessary concepts.

Pwn Adventure 3: Pwnie Island

- If you're into gaming hacking, this is a game that is meant to be hacked that you can run your own server for.

Pwn Adventure: Sorcery

- This one is a CTF you can largely do in your browser and still gets into the binary level exploitation, it just provides the tools you need in the in-browser *NES* style video game. I've not finished it myself but I've enjoyed the time I have put into it.

Microcorruption Embedded Security CTF

- Another in-browser CTF, this one is a bit more educational and structured than *Sorcery*, better for beginners. Less graphical and more focused on teaching.

Nightmare Exploitation / Reverse Engineering Reference

- This, *imo* is probably the main resource for those of you more seasoned, effectively its a bunch of CTF challenges organized into topics with *writeups*. A ton of content, broken up into the various issues being exploited, so if you want to learn about a particular technique, its a good reference to grab a challenge from, work through it and compare with the *writeup*. You have the benefit of knowing the type of issue going into it so you can focus on what matters.

Exploit Excercises (lains.space mirrors)

- There are several servers here you can download and run in a VM locally to attack. Unfortunately the original has gone down but there are a couple mirrors.

- Nebula Server: This is the beginner server, general application level issues, not getting into the binary level exploitation. Gives hints regarding what topic you might want to research and think about how to attack. I like to recommend this server to beginners to give it a try to see if they enjoy the puzzle solving and research aspects. Its a good taste of what vulnerability research is like.

- Protostar covers a lot of the same content that the Intro to Software Exploits from Open Security Training covers, as such I think its a good resource after you've done that course to work through Protostar, and then onto Fusion to learn more.

ROP Emporium

- One of the next steps after Protostar from Exploit Exercises is learning Return-Oriented-Programming, ROP Emporium is an excellent resource for that, pretty gentle introduction and gets you into 64bit exploitation which is a bit different from 32bit.

0X0539 CHALLENGE SITE

- Really any challenge site could probably hold your attention for awhile. This is just a project Specter and I built so we are plugging it here, but you can get a ton more sites from https://www.wechall.net/active_sites.