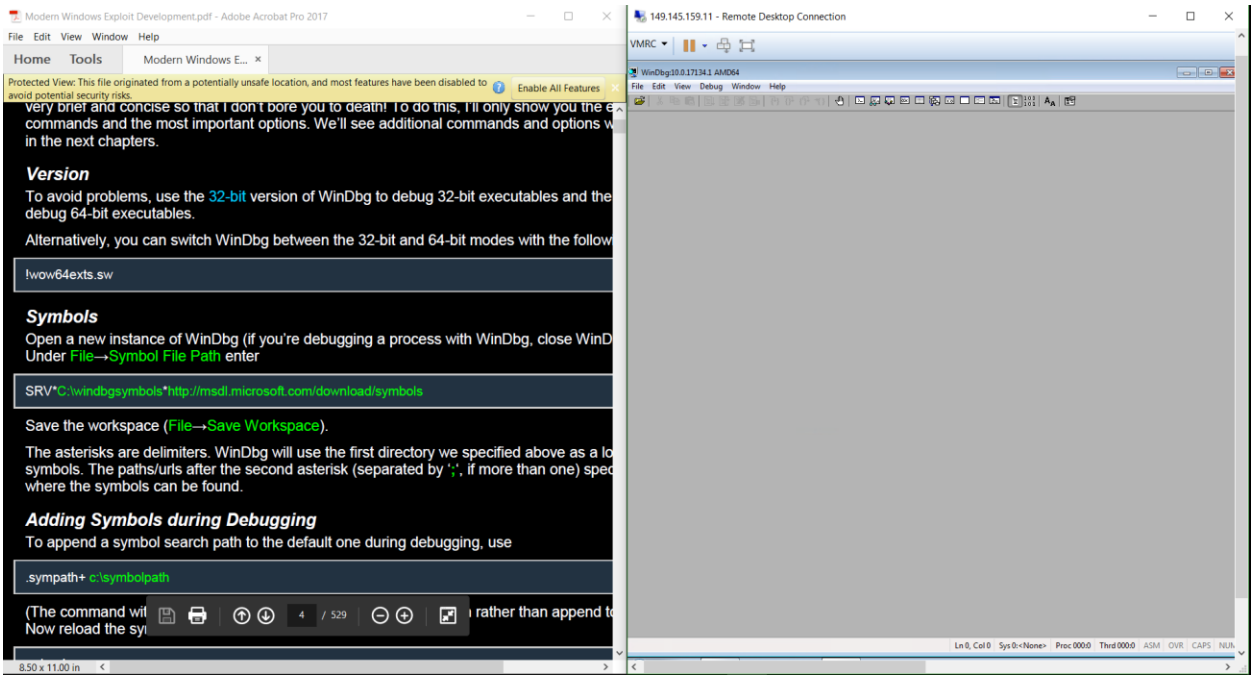
I spent 1-2 hours every day learning how to do these things and still didn't get as far as I would have liked. If you don't want to put in the time or mess around in assembly I'd drop the class now.

While students are getting their environment up and running for a week they should know what exploits are and how people find them. There is also lots of different types of exploit development but in this class we will just be covering c/c++ on Windows. Dealing with web applications is a whole different beast. They need to understand that exploits are found by analyzing source code or reverse engineering the executable. An attacker extract valuable clear text information out of binaries, change an executable, overflow integers, parse strings incorrectly, and most famously redirect the flow of the program's execution. It is still important to conduct your own exploit development against products you field in today's era. Developers should be trained on how to code securely, write tests, and use static analyzers to catch bugs, but there should still be exploit development done to validate the application is safe. Security is getting a TON better with operating systems and developer tools so that's why we are doing this course in windows 7 while using up to date tools. By the end of this course you should understand how to develop more securely, how to decompile someone else's code, how to exploit some basic vulnerabilities, and apply how attackers today could use these same methods.

Hopefully by this point your target machine is in a healthy state. If not look at the installation text file in this directory. You should be able to launch windbg64 and nicely view that and the book at the same time.

Make the directory "C:\windbsymbols" and another "C:\projects" for them to put their vulnerable code in. This windbsymbols directory will save all of your symbol syntax in the coming exercises.



A good intro on what this course is about is 64bit reverse engineering. Know how assembly works.

- https://www.youtube.com/watch?v=75gBFiFtAb8
- https://www.youtube.com/watch?v=rxsBghsrvpI