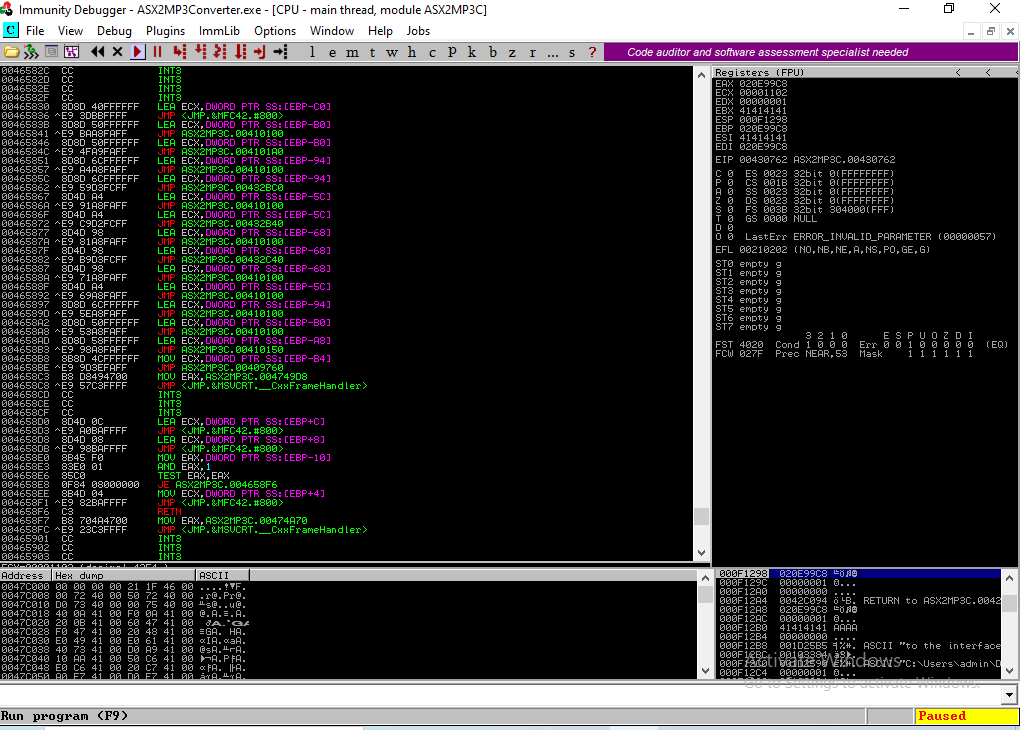
Exploit Test:

First, I spent some time learning the basics of writing Windows Exploits, specifically Buffer Overflow exploits.

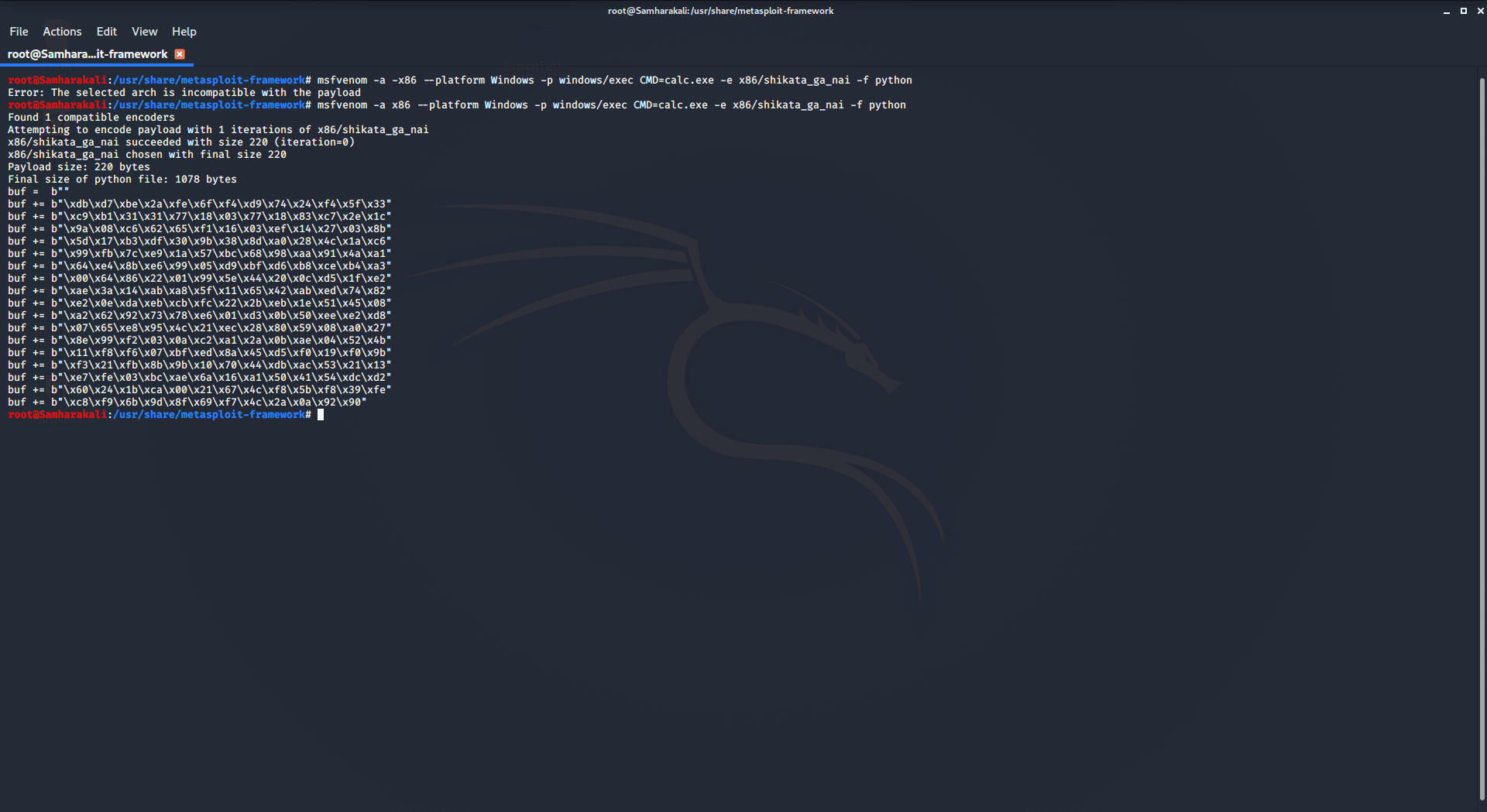
This eventually lead me to the Immunity debugger application to monitor the state of the application in question under various conditions. I had never used a debugger before so I did spend some time learning the application itself and making sense of the information it provided.



I was able to locate an exploit for this specific application (version included) which was invaluable. Replicating his steps gave me considerable insight into the timing necessary for a buffer overflow exploit to work.

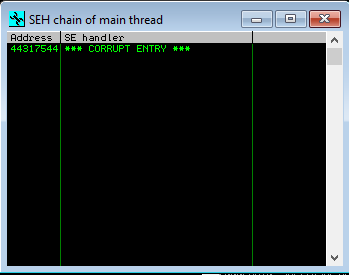
To create a novel exploit, instead of simply using one I had found, I decided to adapt existing methods and apply them to a new file location. I selected the standard downloads folder as my target (the existing exploits I found would only work on C:\).

I created my own payload using Metasploit:



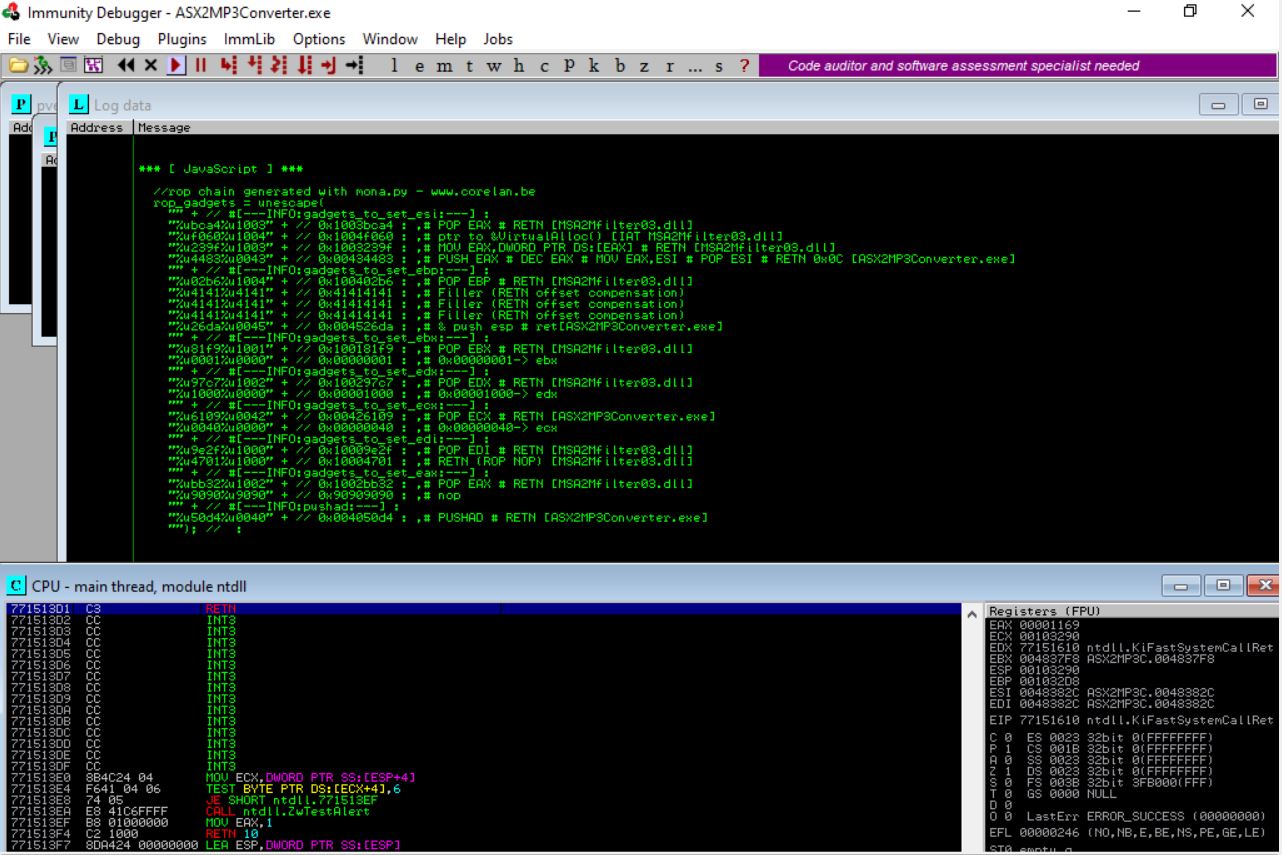
To determine the appropriate place for my shell code, I created a pattern file in Metasploit that allowed me to discover the appropriate characters in EIP. However, here I ran into a bottle neck, my results weren’t working as intended my payload was executing.

After considerable trial and error, I realized I had appended my pattern code to the back of the provided test file. The extra characters in front of the pattern file were having an impact on my pattern so that my offsets weren’t lining up correctly. Once I corrected that problem I was able to create an exploit that executed the necessary code functions.



Note: The exploit only works in the default Downloads folder for NT Username’s 5 characters long (admin for instance)

Research into bypassing DEP restrictions lead me to ROP chains. This brought me back to the Mona plugin for Immunity and with that I was able to investigate potential targets (ASX2MP3.exe and MSA2Mfilter03.dll). Unfortunately, I was not able to successfully create a novel ROP chain exploit in the time allotted, but my attempts are included. I was able to find code someone else had created to do so, but wasn’t able to stitch together a novel ROP chain exploit.



My working notes are included in the repository, and I am including the ROP Chain exploit that I found that does work, in addition to my versions that do not.

Sources:

<https://www.fuzzysecurity.com/tutorials.html>

<https://www.exploit-db.com/papers/13147>

<https://www.exploit-db.com/exploits/47468>

<https://www.fatrodzianko.com/2019/03/13/asx-to-mp3-converter-seh-exploit/>

<https://www.securitysift.com/windows-exploit-development-part-2-intro-stack-overflow/>

<https://www.corelan.be/index.php/2009/07/23/writing-buffer-overflow-exploits-a-quick-and-basic-tutorial-part-2/>

<https://www.corelan.be/index.php/2010/06/16/exploit-writing-tutorial-part-10-chaining-dep-with-rop-the-rubikstm-cube/>

<https://cxsecurity.com/issue/WLB-2019100028>