DLL Injection and OllyDBG

CSC 471 - 02

Tyler Prehl

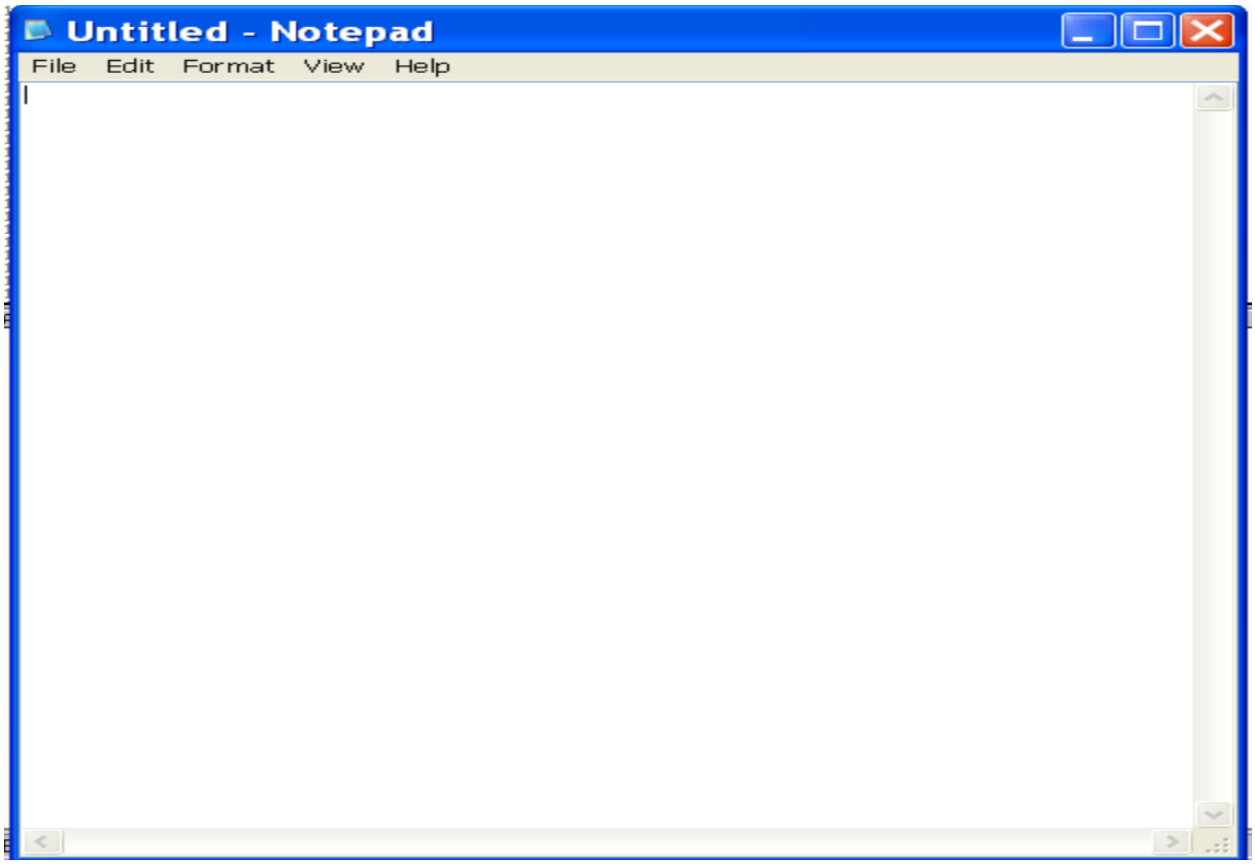
2/12/2022

Introduction

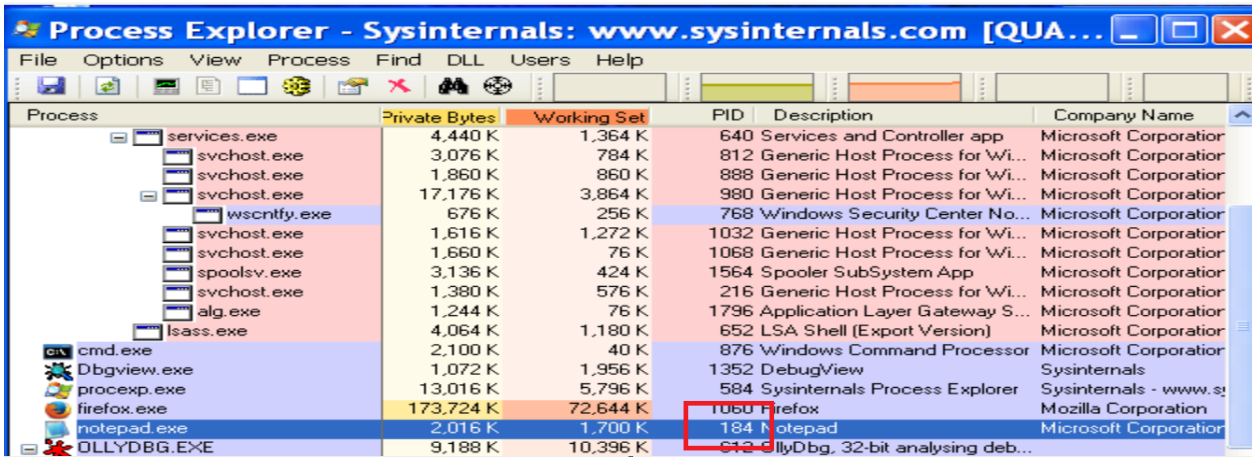
The purpose of this lab is to provide a better understanding of a couple things. First and foremost, it will provide insight into how to execute a dll file injection attack. Secondly, it provides background knowledge on how to navigate various applications, such as VirtualBox, Process Explorer, and OllyDbg. Most importantly, it provides exposure to reading and editing the hex values in memory to recreate files the way we want them from executable files.

Analysis and Results

To start the dll file injection attack, we need a process to attack, so I opened Notepad.

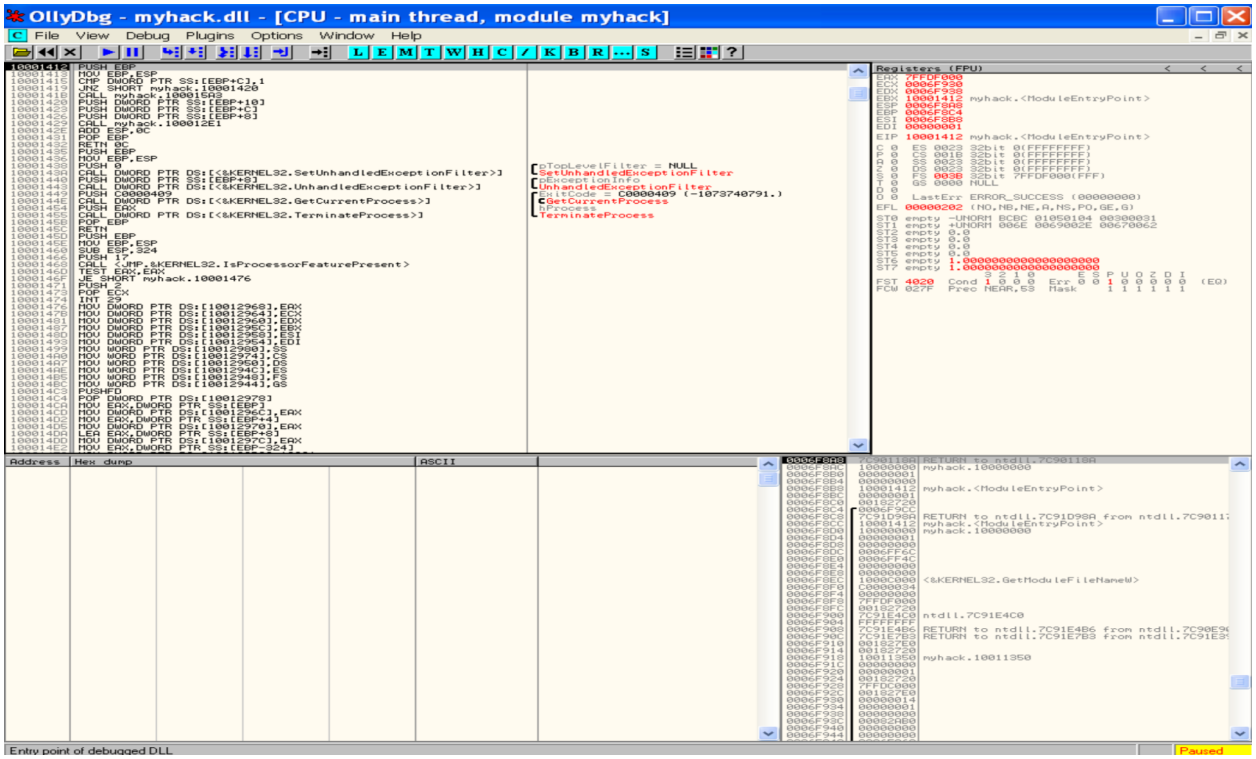


Next, I needed to know what the process ID of the Notepad application was so that the InjectDll.exe file could have a target application to inject with a new dll file.

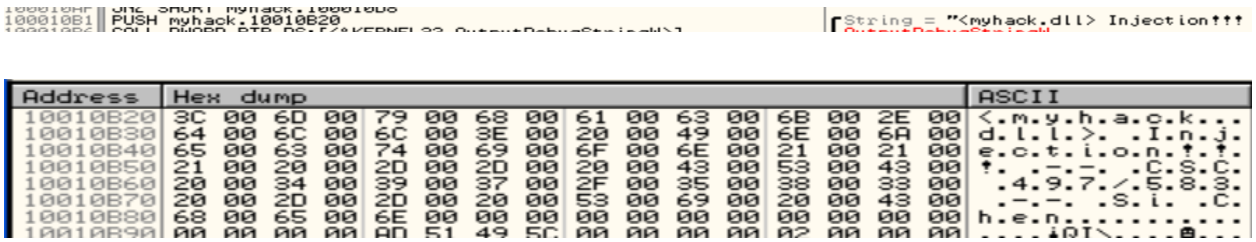


As a test, I attacked the Notepad instance using Dr. Si Chen's myhack.dll file with success.

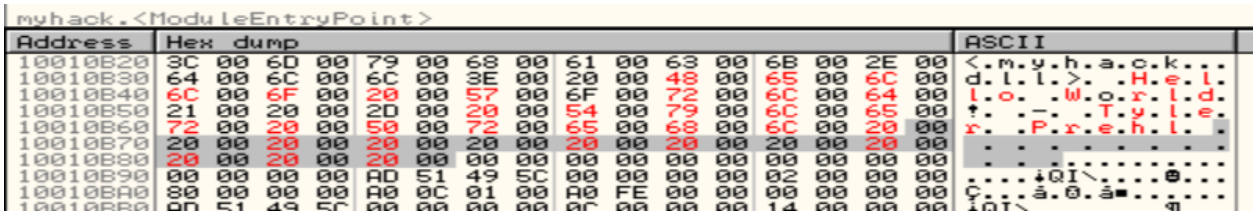
To change myhack.dll to edit the printed line in DebugView, I needed to use OllyDbg, so I opened myhack.dll in OllyDbg.



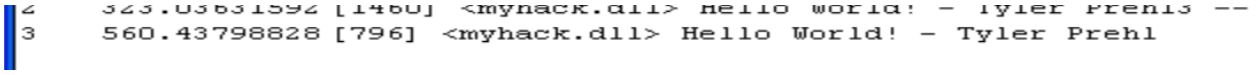
I then navigated to 10010B20 in memory, because it was the actual address in memory where the string that gets printed to DebugView is stored.



With direct access to the location in memory, I edited the binary to include “Hello World! - Tyler Prehl” and copied it to an executable file to be saved as a new dll - myhack_Prehl.dll.



After some failed attempts in trying to edit the binary, I finally was able to properly save and run myhack_Prehl.dll:



Discussion and Conclusion

With a successful dll injection, this lab was a success. I achieved all of my goals, including learning how to properly use VirtualBox and OllyDbg, as well as learning a bit about how to navigate through memory and edit certain pieces to change the outcome of an executable file. This will be useful going forward as our class dives into attacks that require a strong understanding of how to use OllyDbg, and also for any future dll-related attacks we may attempt.