

West Chester University

CSC 471

Dr. Si Chen

Spring 2024 Lab 1

Submitted by

Sean Berlin

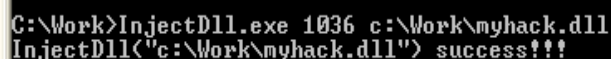
2/20/24

1. Introduction: The purpose of this lab was for students to understand the concepts of DLL Injection and understand how to use OllyDbg to modify binary files. To be specific, the target was to ultimately change the debug information in, DebugView window, from “Injection!!! – CSC 497/583 – Si Chen” to “Hello World! – XXX (Replace “XXX” with your name :)”. Students constructed this experiment through the VirtualBox software along with a custom Windox XP image provided by the instructor. Programs used included DebugView, Notepad, Process Explorer, OLLYDBG, CMD prompt, and the provided “myhack.dll” file.

2. Analysis and Results:

Analysis: The first step once set up in the Windoxs XP inside VirtualBox was to download the “myhack_dll.zip” from the class website. Once unzipped, the contents included the “myhack.dll” and “InjectDll”. The next step was to launch the first attack. This was done by running the Notepad application in order to use its PID. The PID was able to be easily found by using the systems Process Explorer which in essence acts as a task manager. In this case, the PID used was 1036, so that was then inputted into the executable to launch the attack in the command prompt. This is shown in *Figure 1*. The first attack serves as a downloader malware where the initial attack will to download a more powerful malware. However, currently, the attack just simply downloaded a html file to the system. The HTML file content has no significant meaning but serves to act as a placeholder. The next part of the lab was to modify the binary files of the “myhack.dll”. The first step to do this was to use OLLYDBG to open up the specified file and find the location of the output message. This is shown in *Figure 2*. Specifically, the memory address that serves value was “10010B20” as it is the address pushed onto the stack. Then, that address was searched by right-clicking and using the “Go to” and “Expression” function. This is shown in *Figure 3*. The next step was to simply edit the specific binaries of the message to the desired output. Then, the file was saved as a new DLL and needs to be used in another attack. The new DLL file is shown in *Figure 4* with the desired output. The same process as the first attack was replicated and the output is shown using the Debug View application in *Figure 5*.

Screenshot of successful first attack



```
C:\Work>InjectDll.exe 1036 c:\Work\myhack.dll
InjectDll("c:\Work\myhack.dll") success!!!
```

Figure 1

Screenshot of OLLYDBG

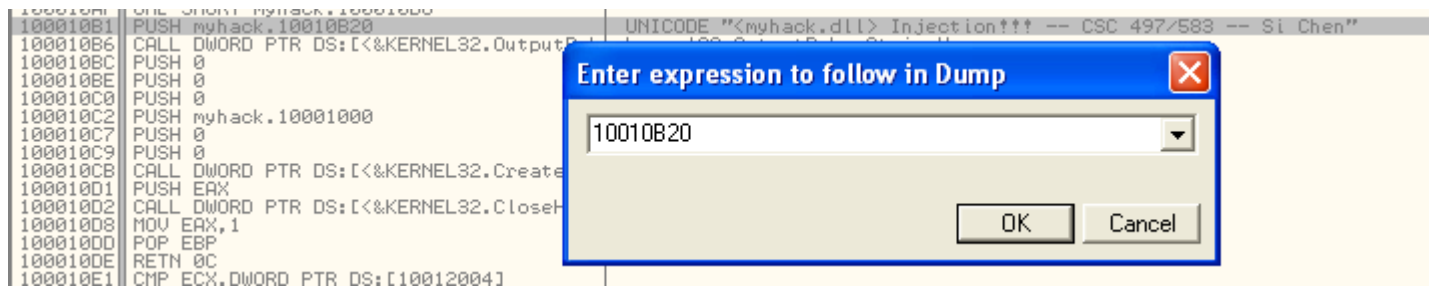
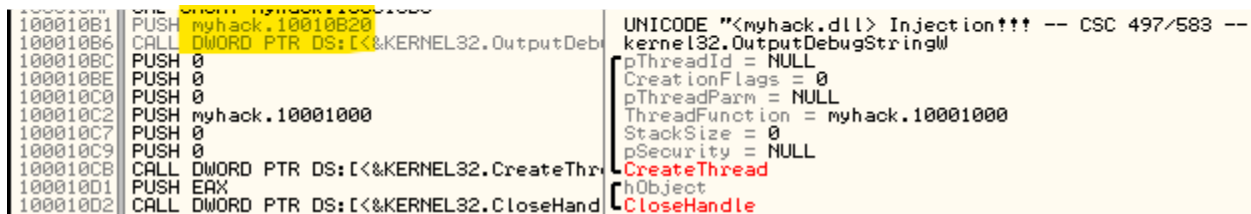
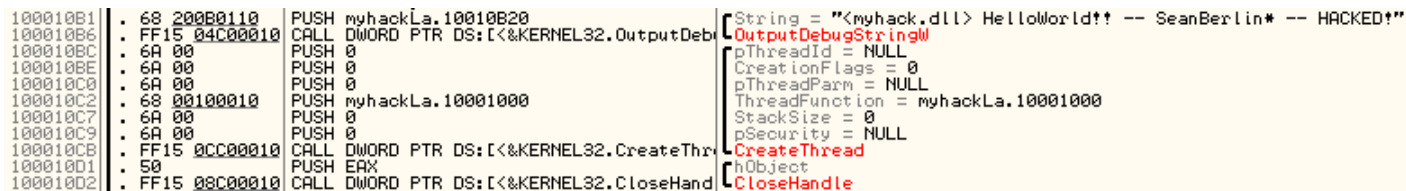


Figure 2



Screenshot of OLLYDBG

Figure 3

Screenshot of Modified Binary

Figure 4

Screenshot of Successful Modified Binary Attack

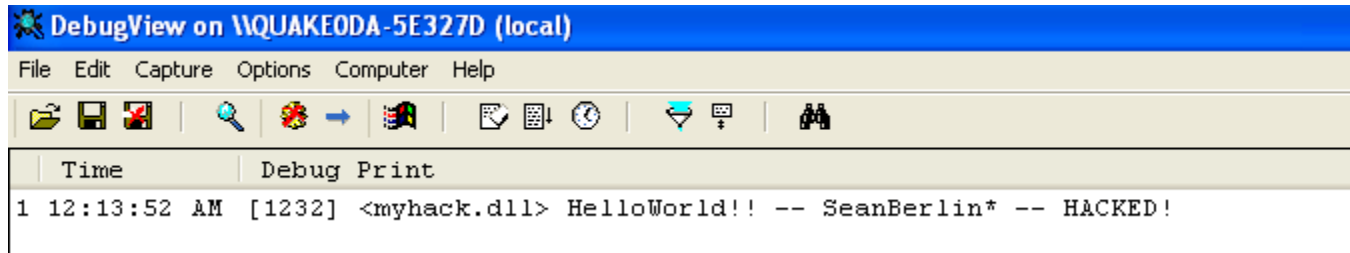


Figure 5

3. Discussion and Conclusion:

Generated by ChatGPT- In this lab, the objective was to gain a practical understanding of DLL Injection and the usage of OllyDbg to modify binary files. The primary goal was to alter the debug information displayed in the DebugView window from "Injection!!! – CSC 497/583 – Si Chen" to "Hello World! – [Your Name]". Through a series of steps outlined in the analysis, including identifying process IDs, modifying binary files using OllyDbg, and executing attacks, we were able to accomplish this objective. The analysis revealed that the first attack, designed as a downloader malware, successfully initiated the download of an HTML file onto the system. Although the content of the HTML file was a placeholder in nature, this initial step demonstrated the functionality of DLL Injection. Subsequently, by employing OllyDbg, we accessed and modified the binary files of the "myhack.dll" to change the output message. This involved locating the memory address containing the desired output and editing the binaries accordingly. The successful modification of the DLL file was evidenced by the altered debug information displayed in the DebugView window during the subsequent attack. Throughout the experiment, we encountered no significant deviations from theoretical expectations or accepted experimental data. The observed outcomes aligned with the principles of DLL Injection and binary file modification as described in the literature and demonstrated in class materials. However, it's crucial to note that while the lab provided valuable hands-on experience, the ethical considerations and potential real-world implications of such techniques must always be acknowledged and respected. In conclusion, this lab effectively facilitated an understanding of DLL Injection and OllyDbg usage, allowing us to manipulate binary files and observe the resulting changes

in system behavior. By successfully modifying the debug information, we attained the desired outcome, thereby fulfilling the lab's purpose and expanding our knowledge in the field of cybersecurity and software exploitation.