**Lab 19: EXE With Trojan Code in a New Section**

**Course Name**: Malware Analysis and Reverse Engineering (IAM302)

**Student Name**: Nguyễn Trần Vinh – SE160258

**Instructor Name**: Mai Hoàng Đỉnh

**Lab Due Date**: 18/3/2023

**What You Need**

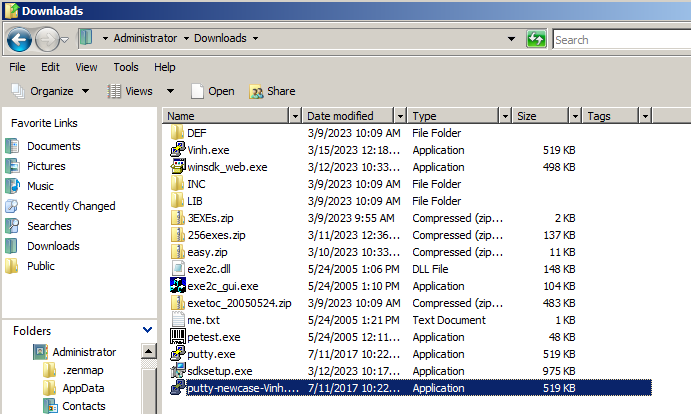
A Windows machine, real or virtual. I used a Windows Server 2008 virtual machine.

**Purpose**

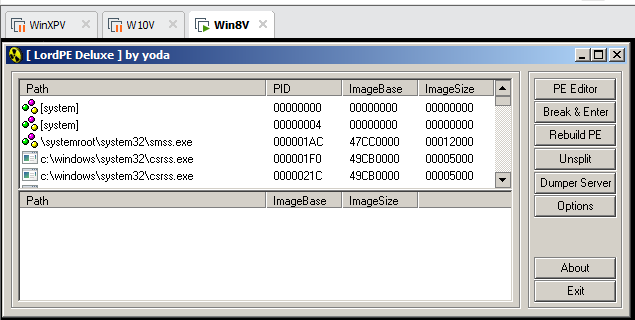
To modify a Windows EXE file and save an altered version containing Trojan code in a new PE section. This gives you practice with very simple features of the Immunity debugger and LordPE

**Task 1: Add a Section with LordPE**

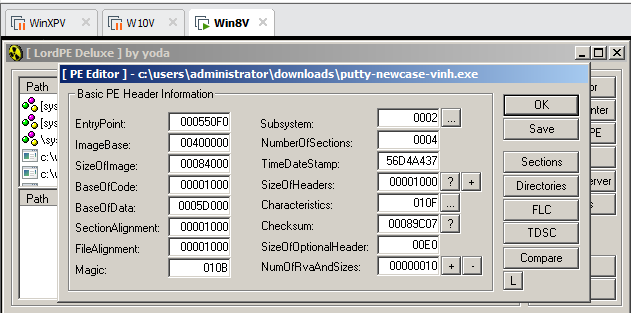
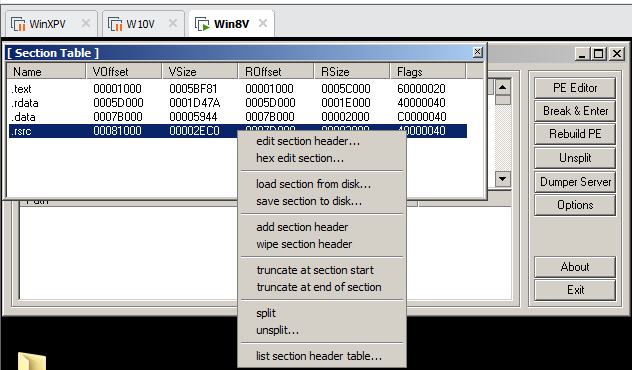
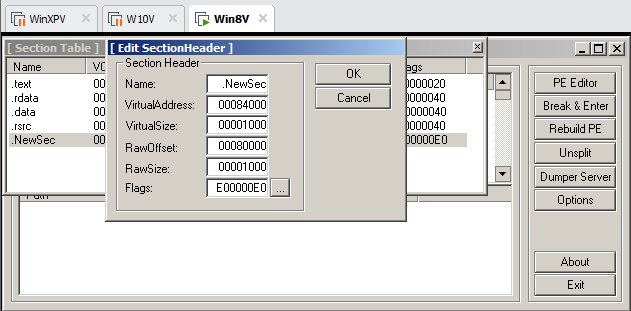
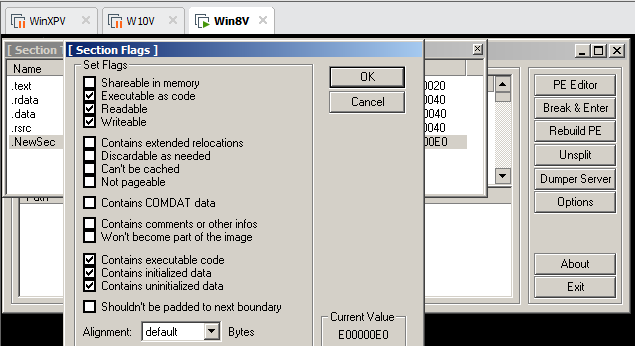
**Copying putty.exe**

****

**Getting LordPE**

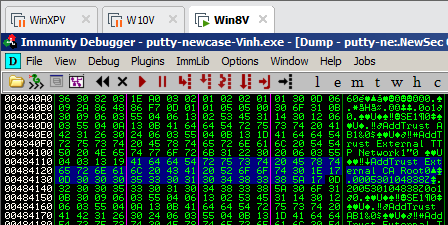
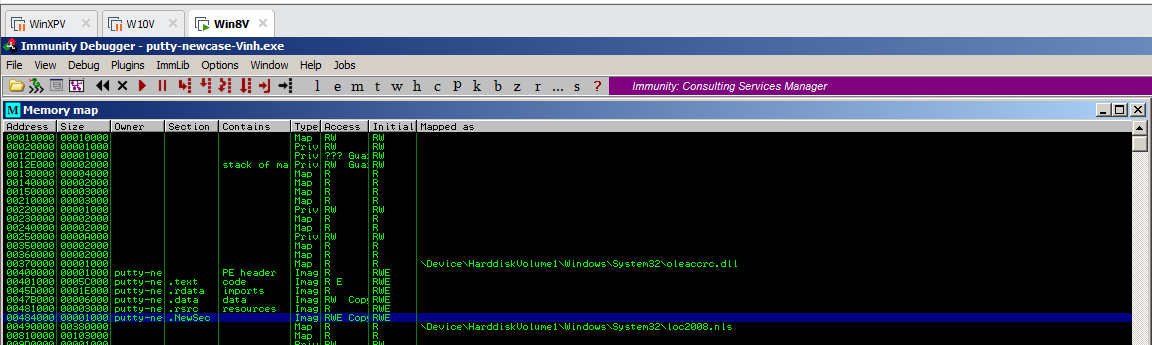
****

**Adding a New Section to the PE Header**

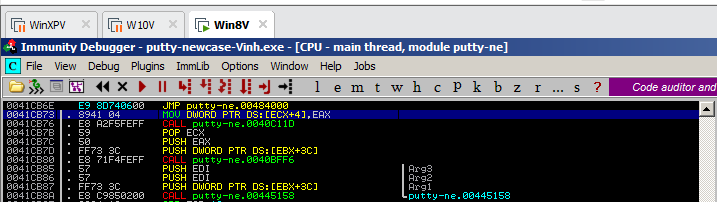
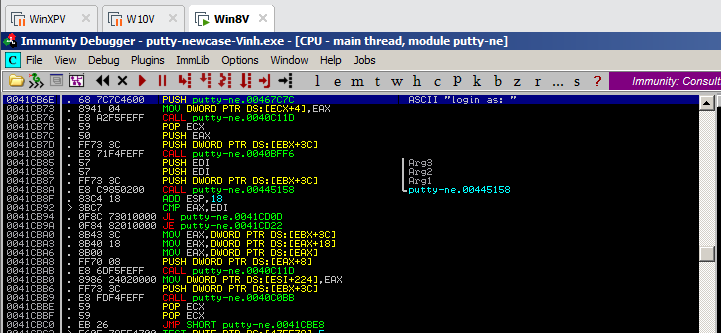
**   **

**Task 2: Redirecting Code Execution with Immunity**

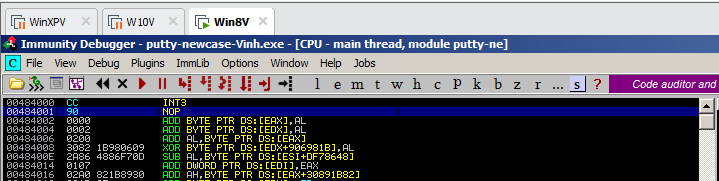
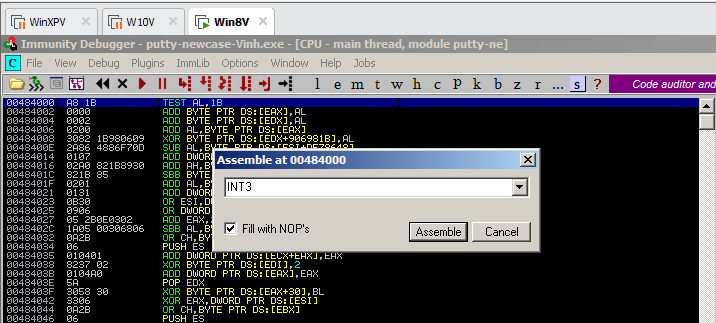
**Using Immunity to Examine the NewSec Section**

****

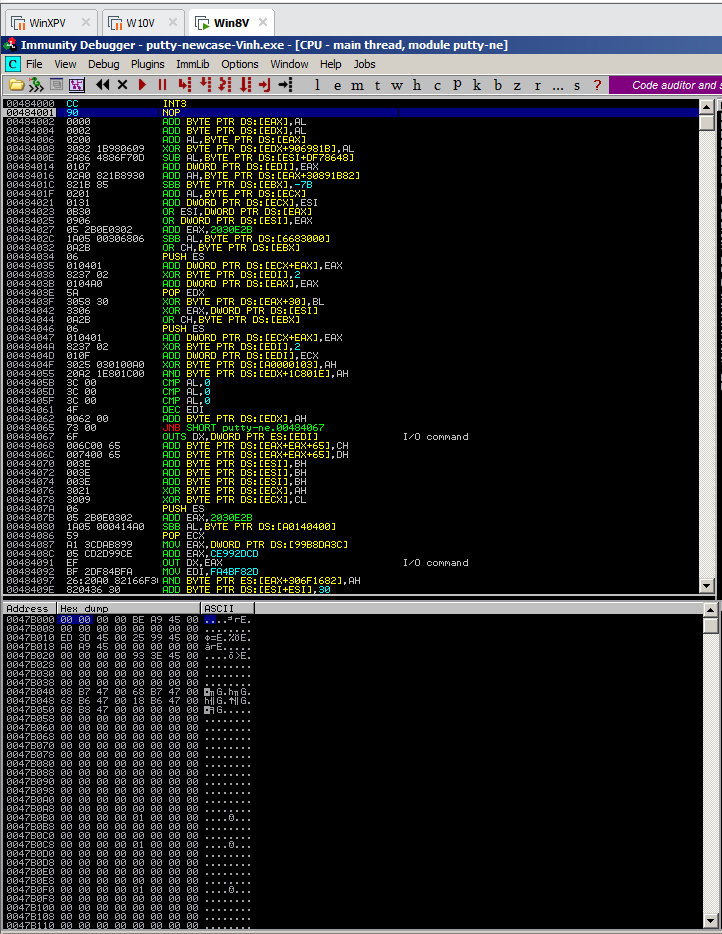
**Using Immunity to Redirect Code Execution**

****

**Adding Trojan Code**

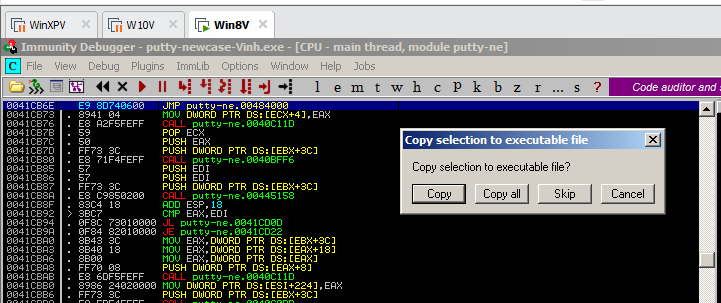
****

**Running the Modified App in Immunity**

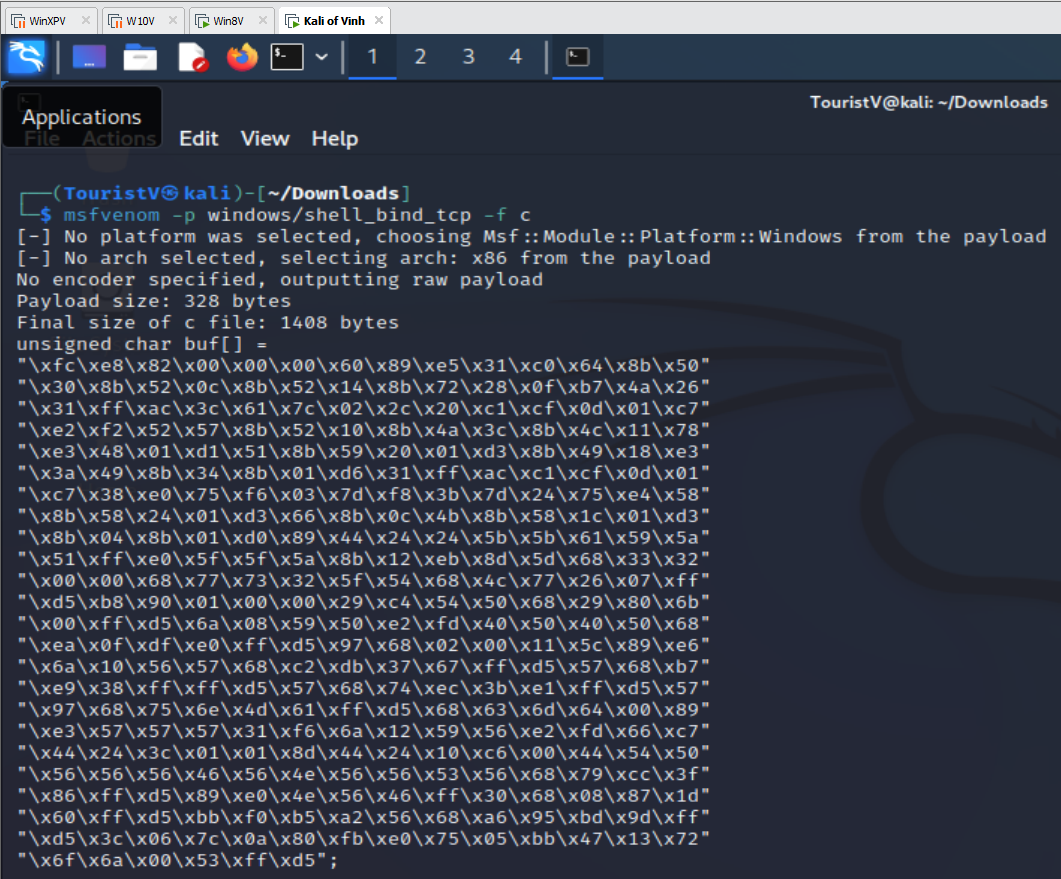
****

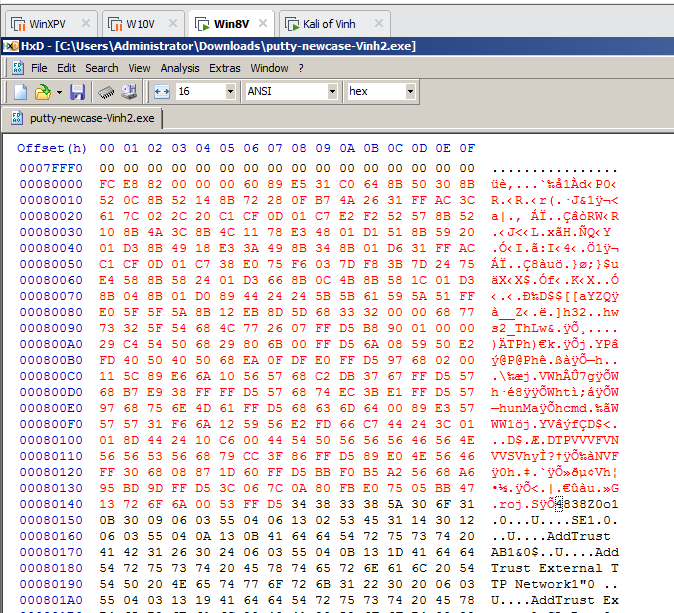
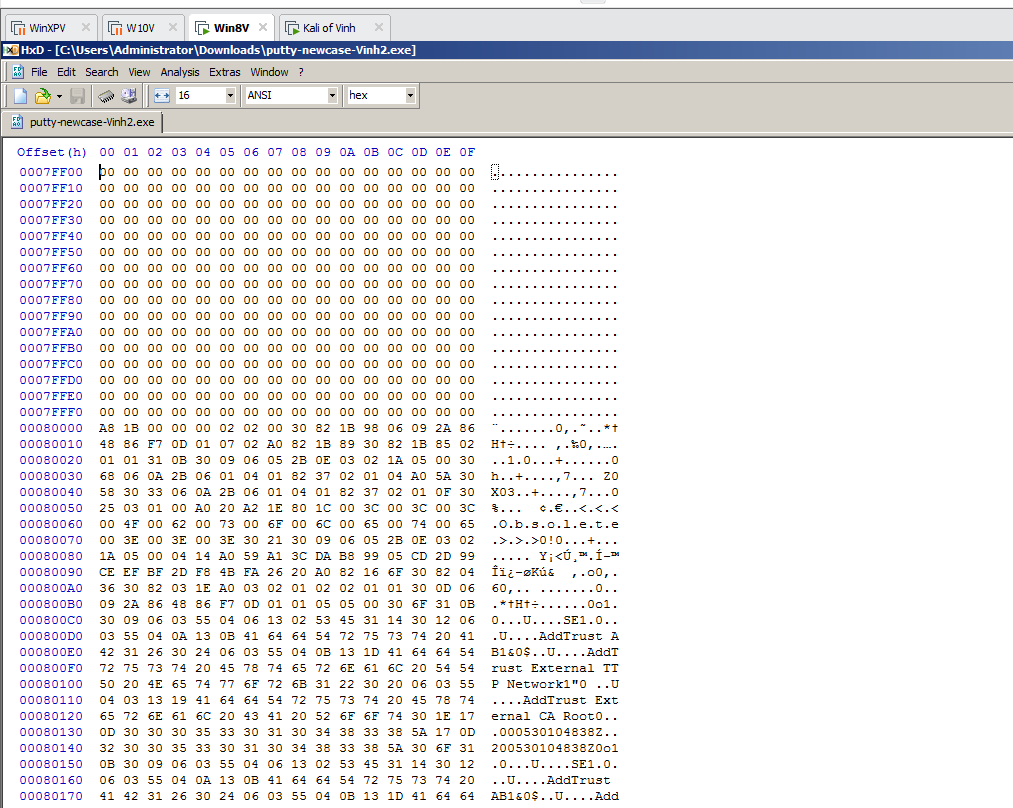
**Task 3: Inserting Real Shellcode**

**Saving the Modified EXE**

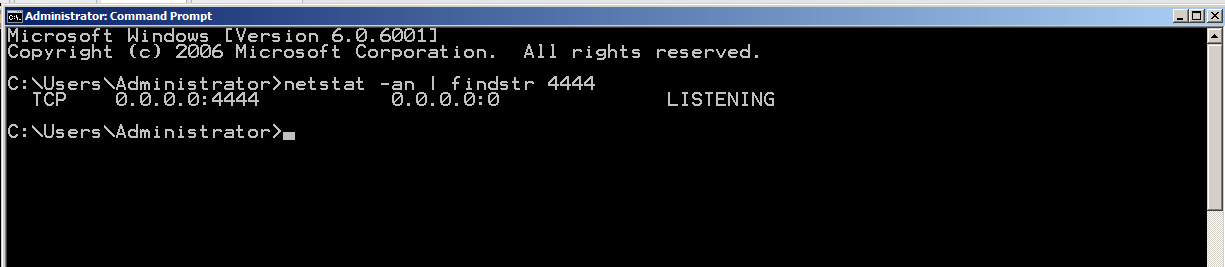
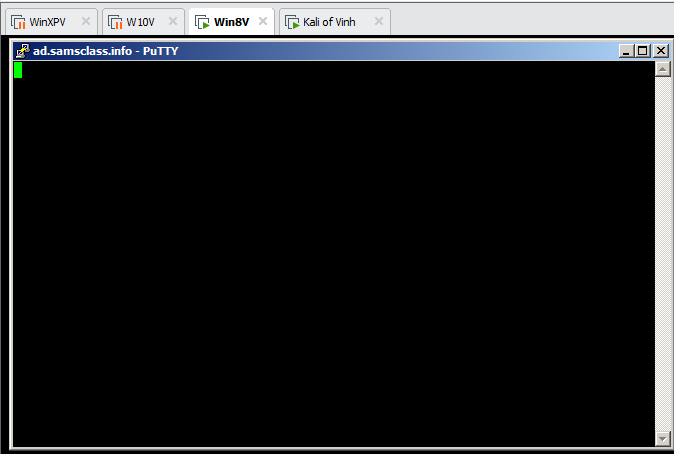
****

**Getting Simple Shellcode**

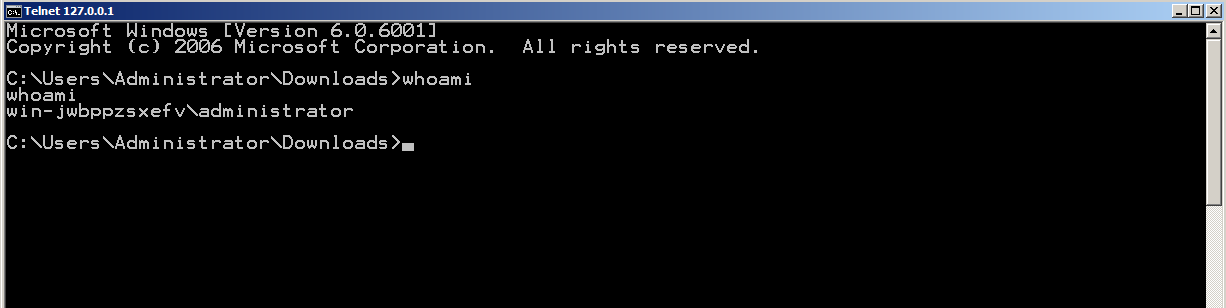
****

****

**Running the Trojaned Putty**

****

**Connecting to the Target**

****