**Lab 18: Simple EXE Hacking with Immunity**

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

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

**Instructor Name**: Mai Hoàng Đỉnh

**Lab Due Date**: 22/3/2023

**What You Need**

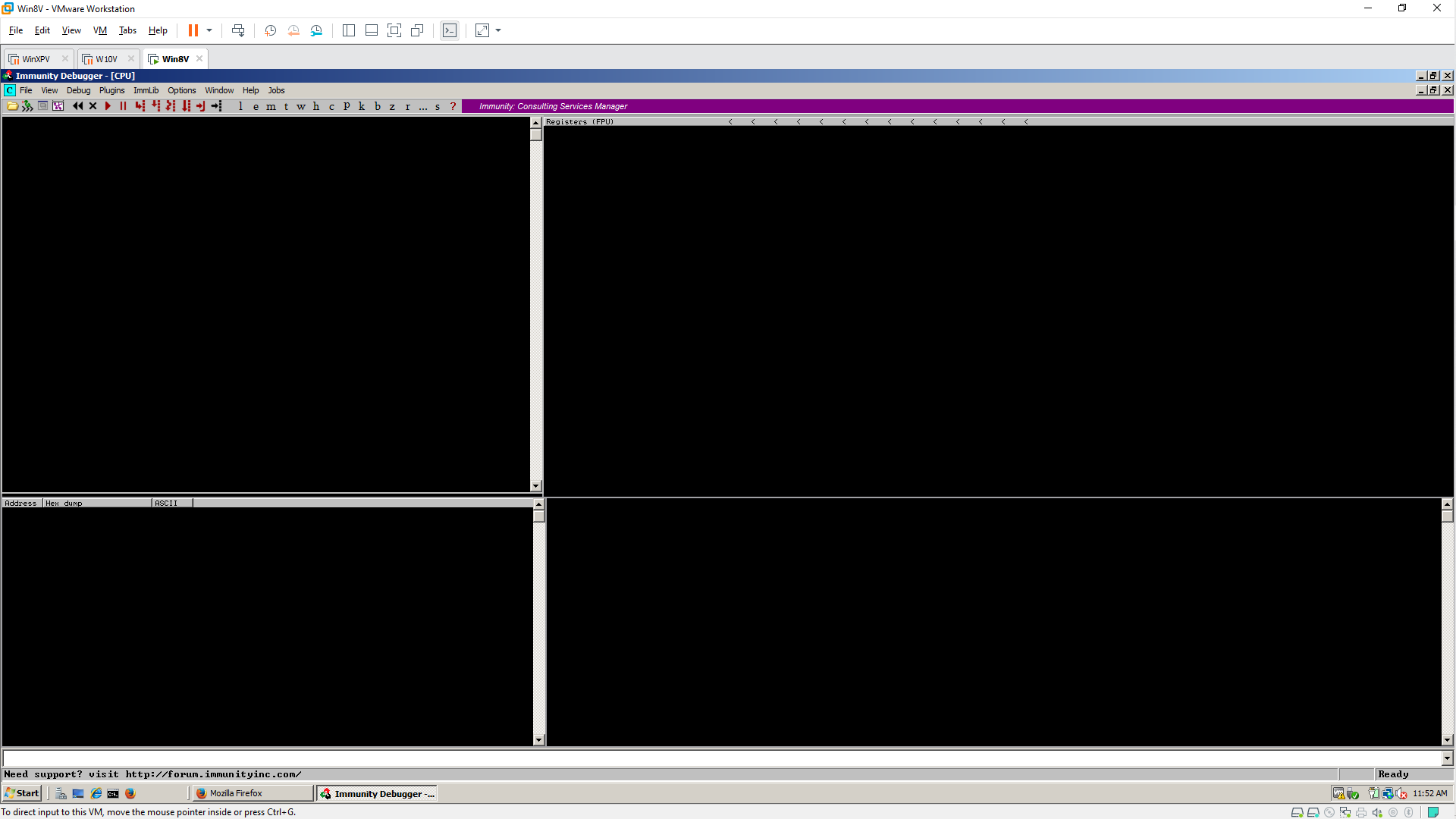
A Windows machine, real or virtual. I used a Windows Server 2008 virtual machine.

**Purpose**

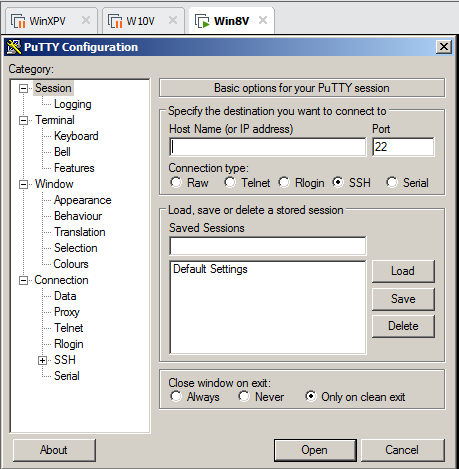
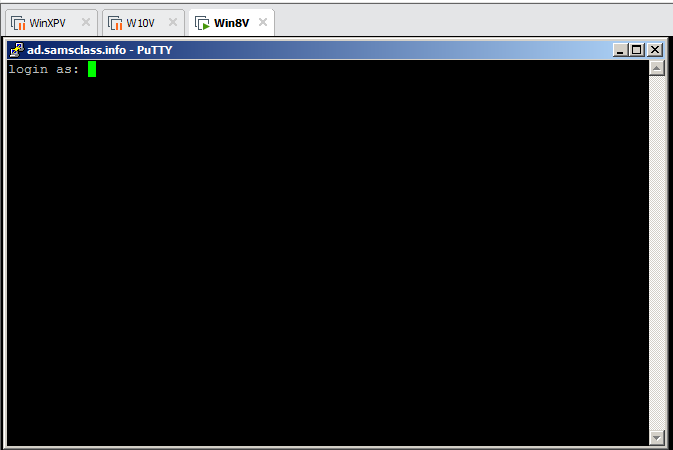
To modify a Windows EXE file and save an altered version. This gives you practice with very simple features of the Immunity debugger.

**Task 1: Target EXE Recon**

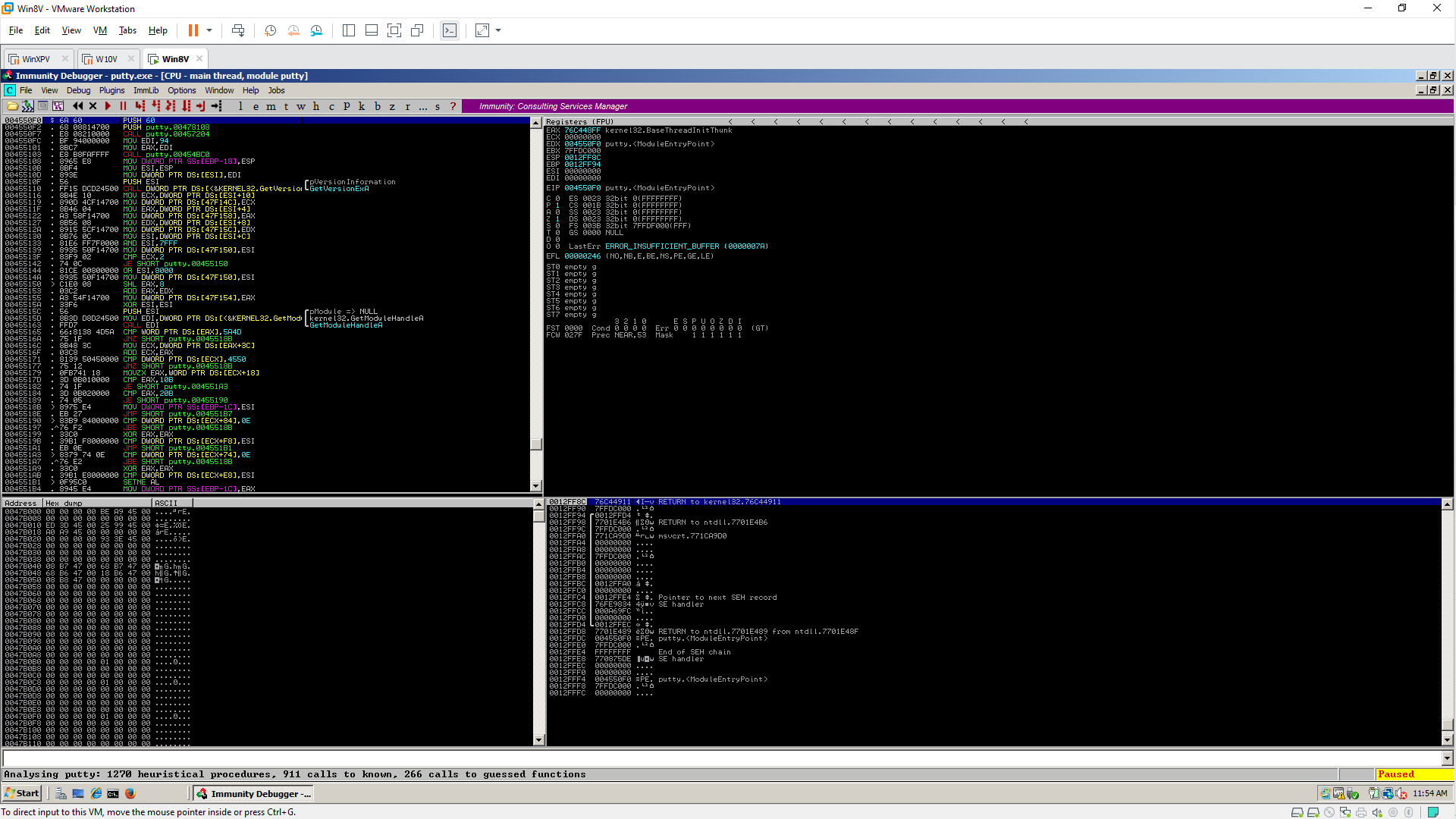
**Get Immunity**

****

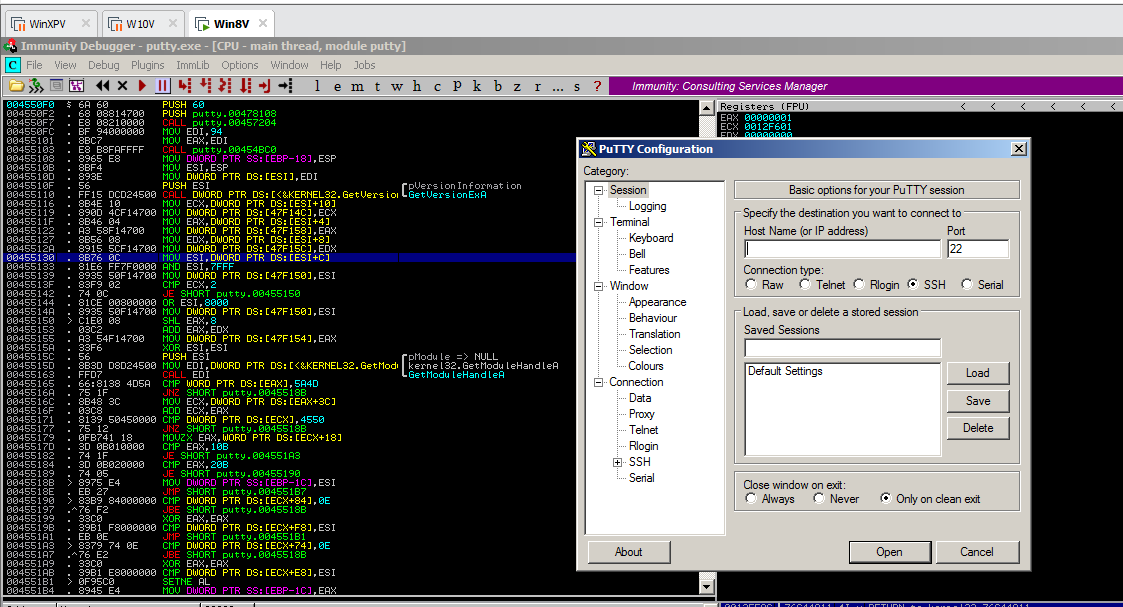
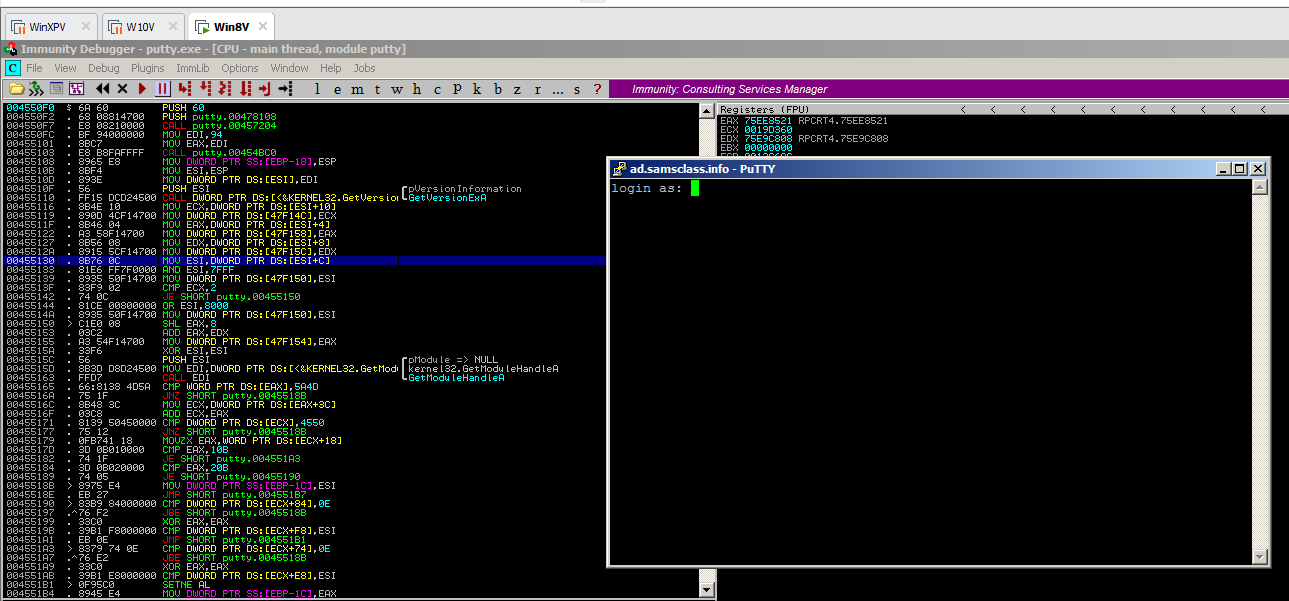
**Get putty.exe**

** **

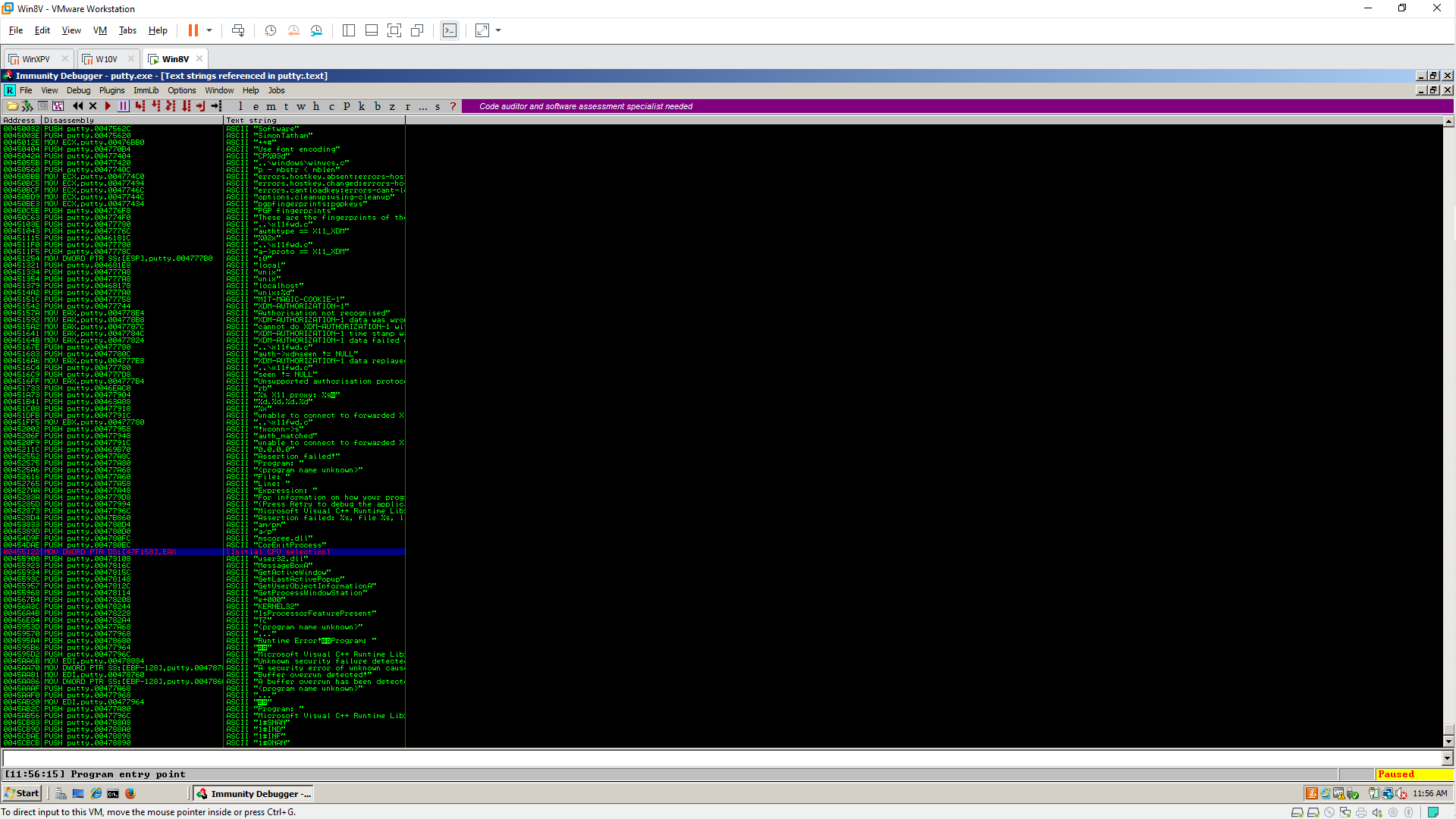
**Starting the Immunity Debugger**

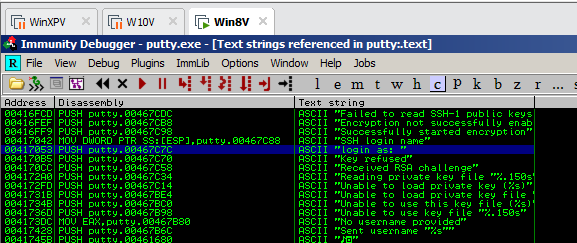
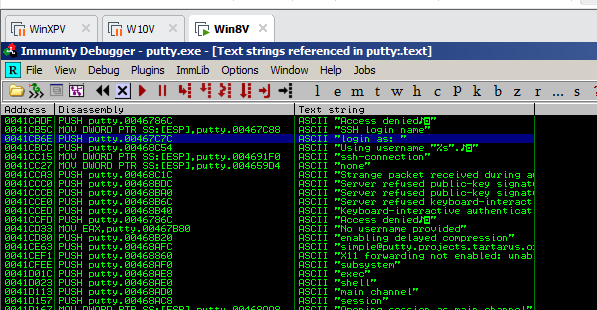
****

**Running Putty in Immunity**

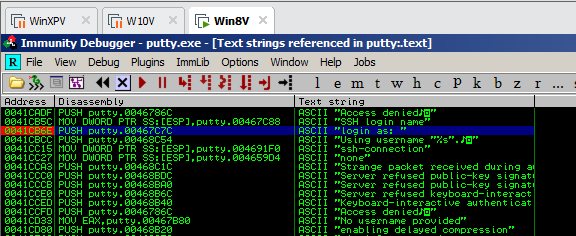
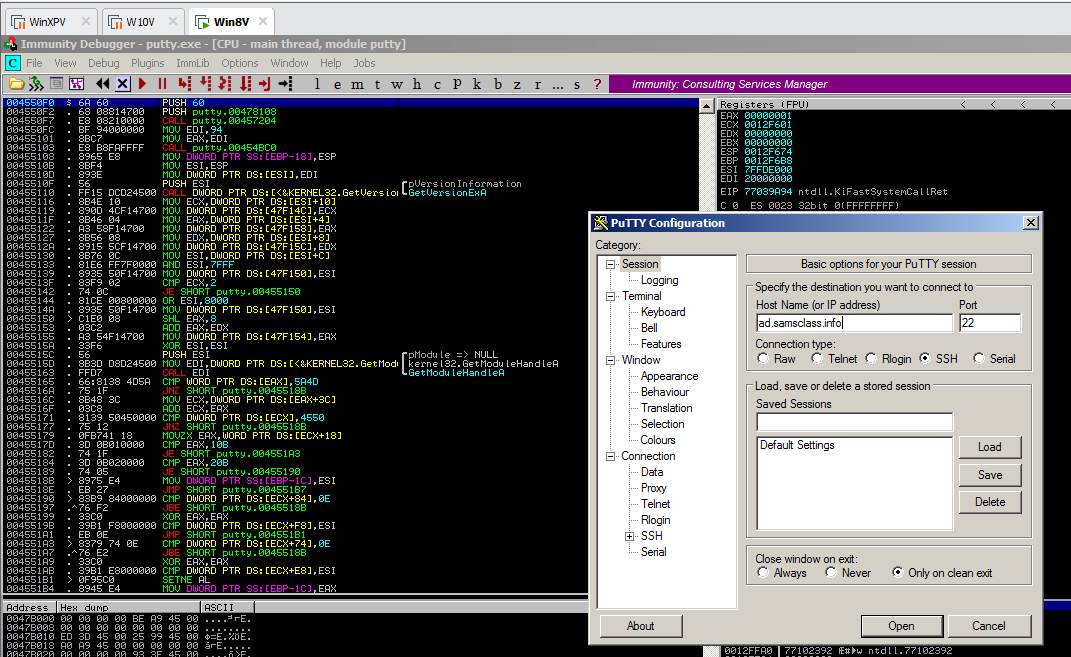
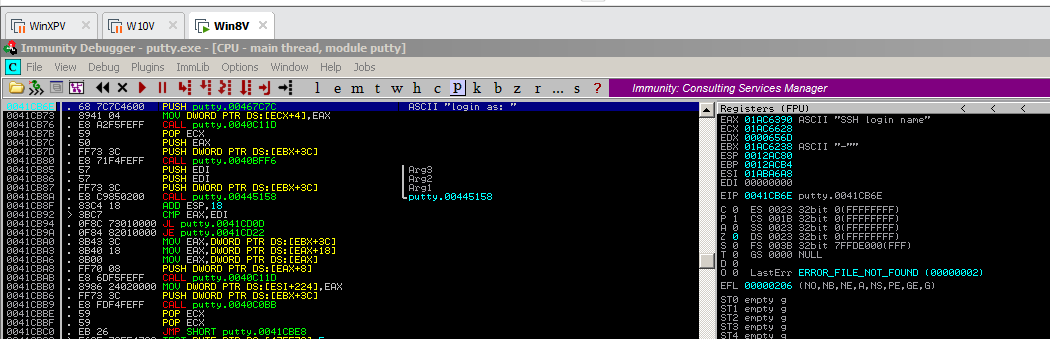
** **

**Finding the "login as" Code**

****

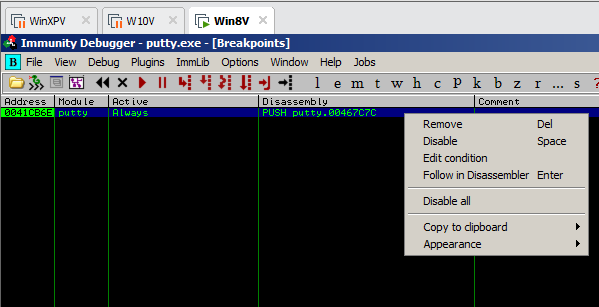
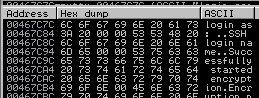
** **

**Using Breakpoints**

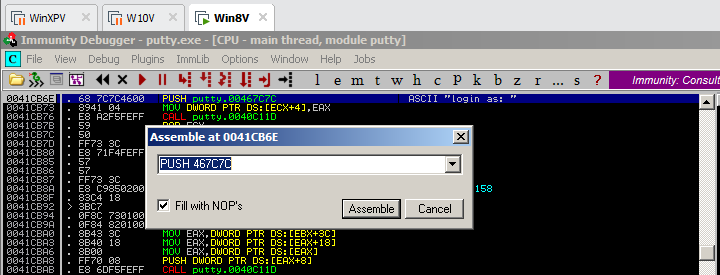
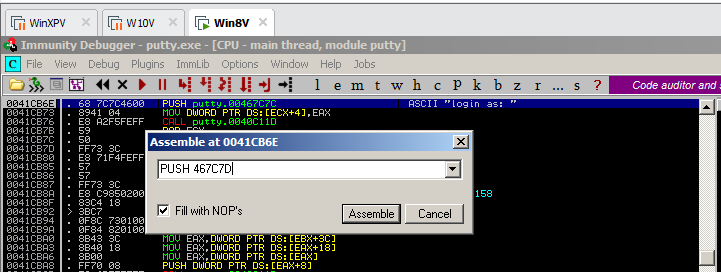
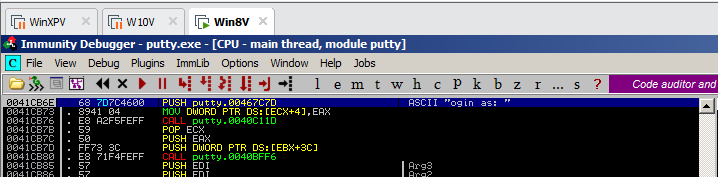
**  **

**Task 2: Alter the Login Message**

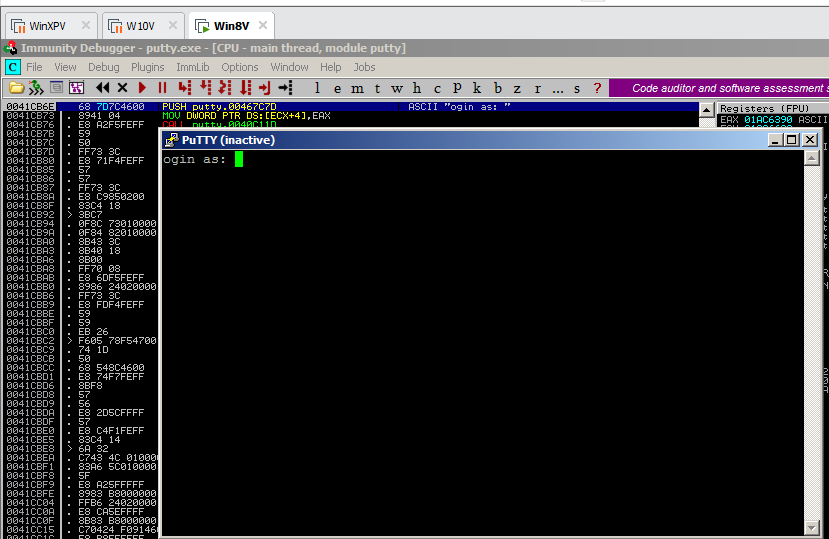
**Removing the Breakpoint**

** **

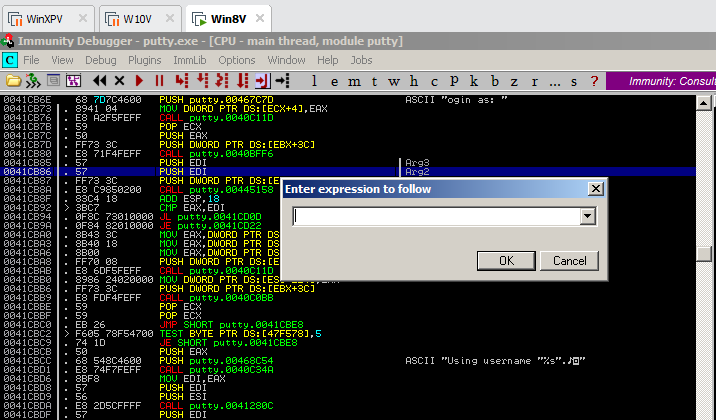
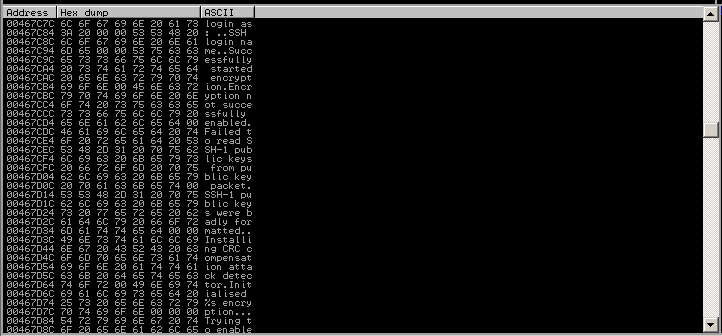
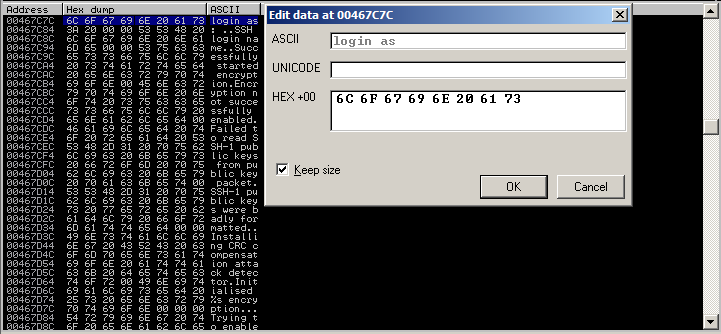
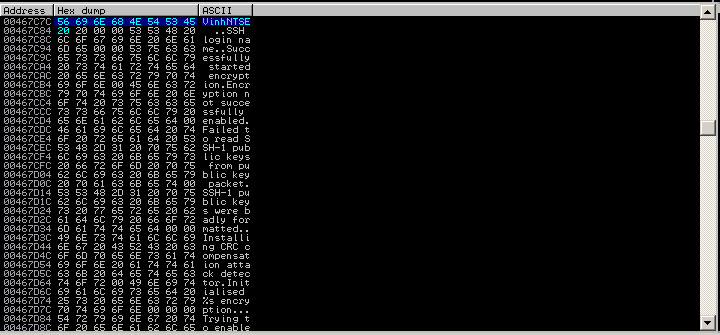
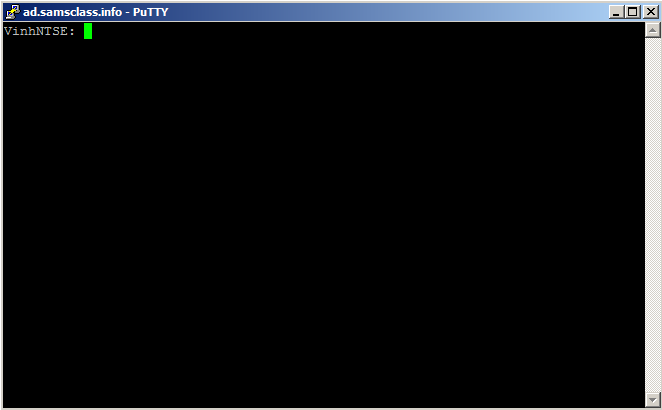
**Skipping the First Letter In the Message**

**  **

**Running the Modified Program**

****

**Inserting Your Name**

**    **