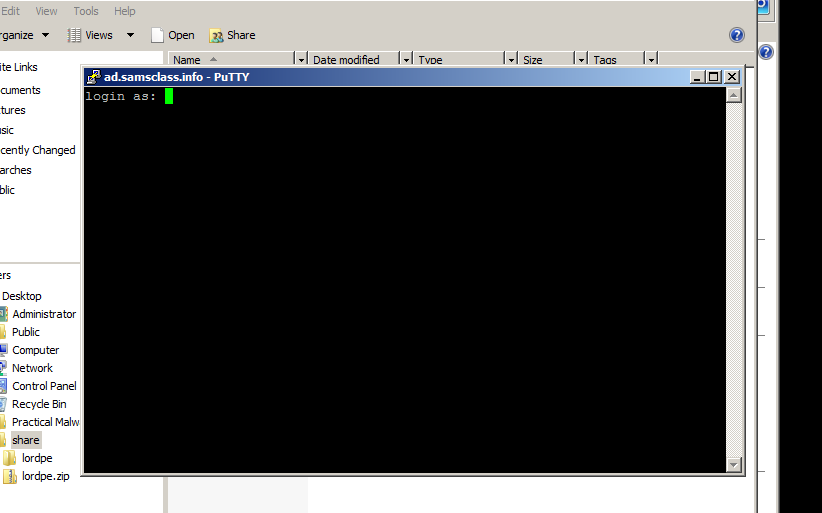
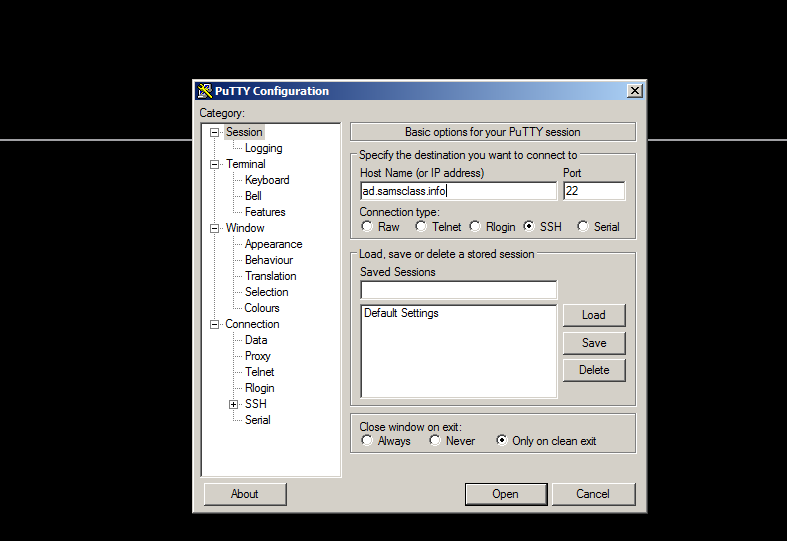
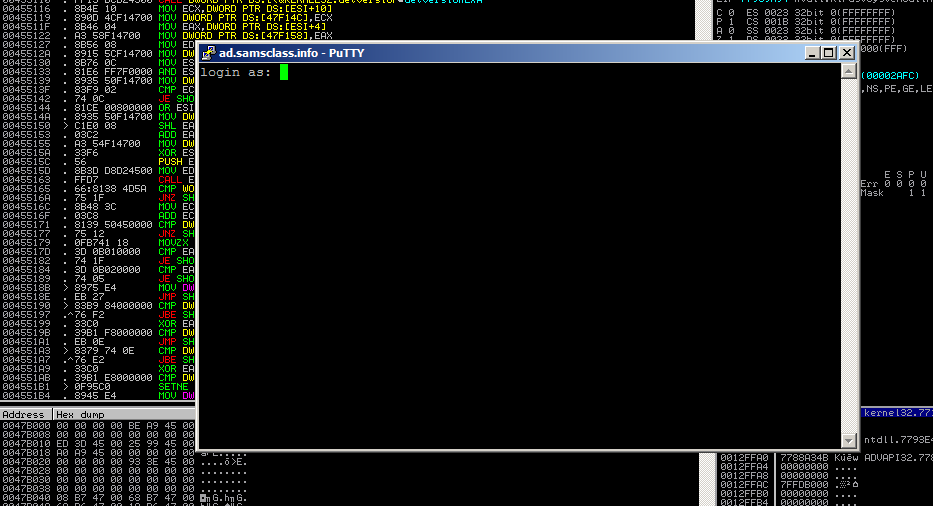
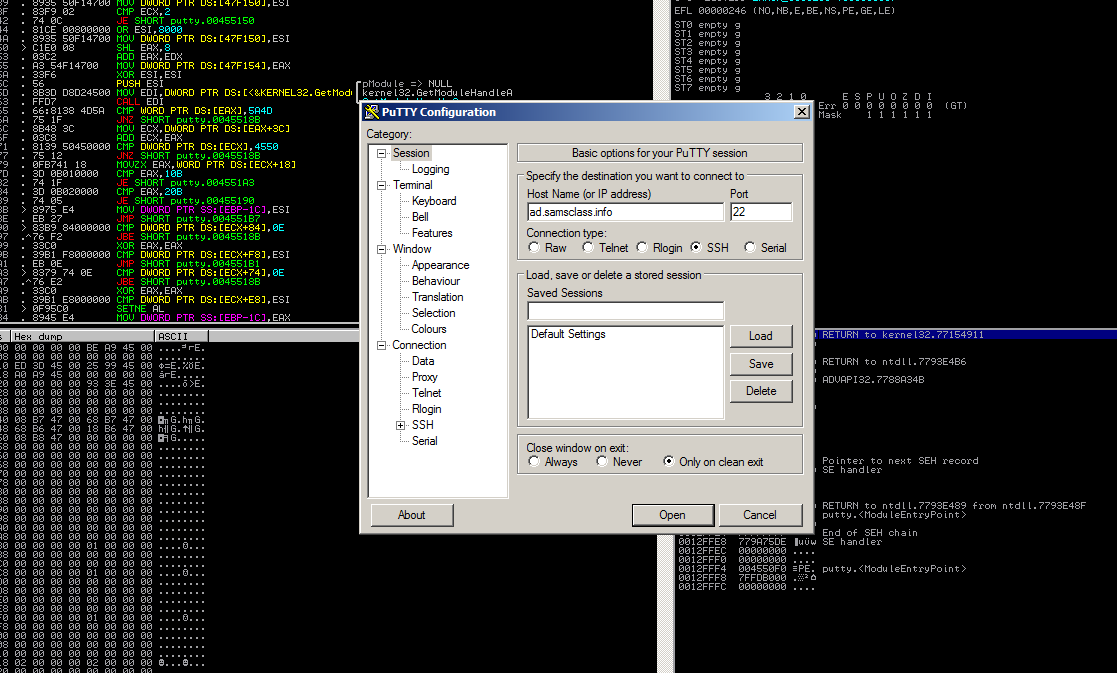
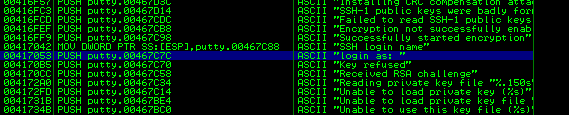
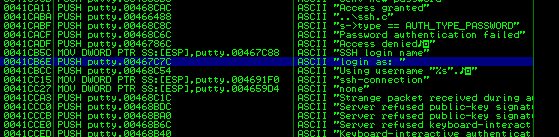
**LAB 19.1: Simple EXE Hacking with Immunity**

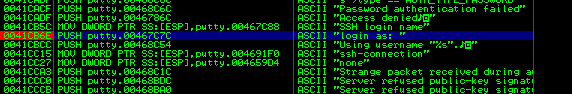
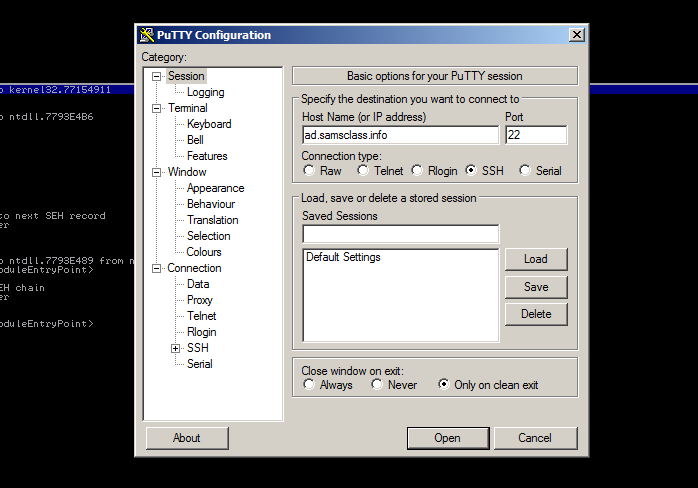
**Task 1: Target EXE Recon**

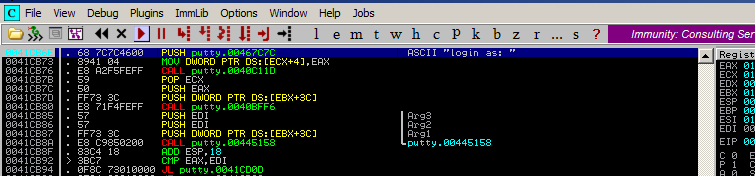
Running PuttyRunning Putty in Immunity

Finding the "login as" Code

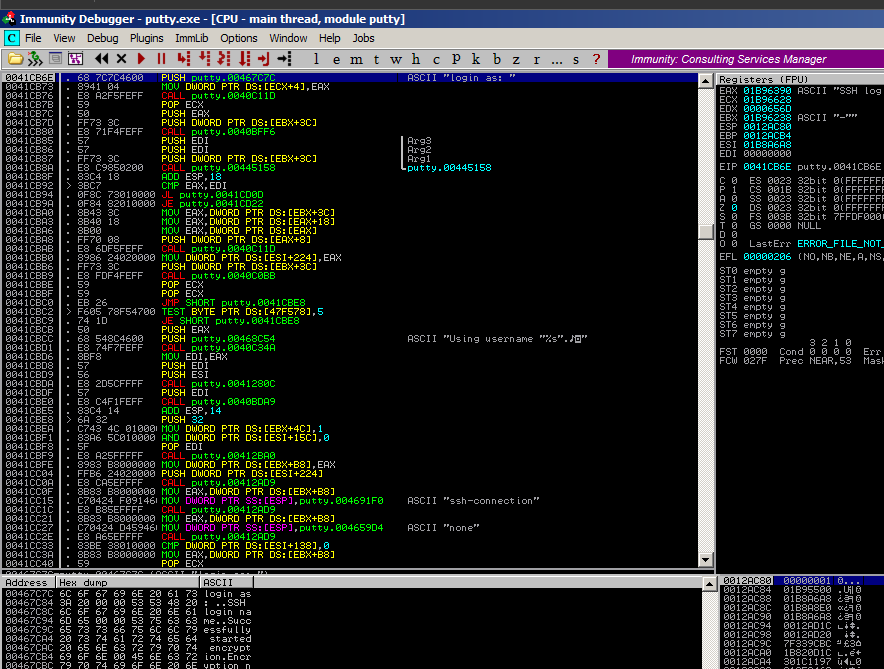
This instruction is at address 00417053.

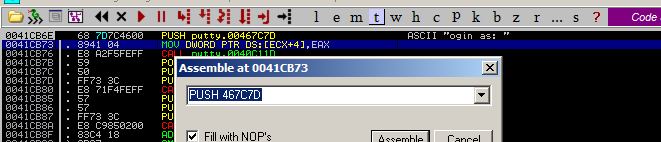
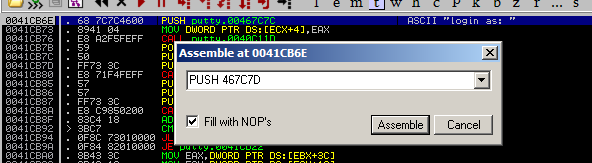
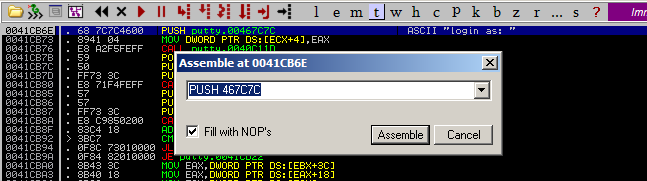
Right-click again, and click "Search next". Immunity finds another line of code that uses this string, as shown below. This instruction is at address 0041CB6E. 

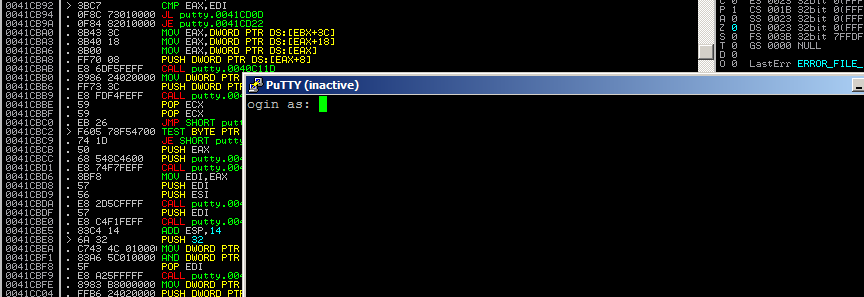
Using BreakpointsIn Immunity, from the menu bar, click Debug, Restart. A box pops up warning you that "Process 'putty' is active". Click Yes. In Immunity, from the menu bar, click Debug, Run. A Putty window opens, as shown below. 

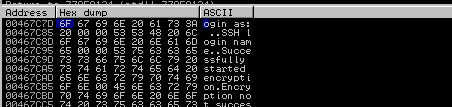
Click in the Putty window. In the "Host Name (or IP address)" box, type ad.samsclass.info At the bottom, click the Open button. A black window opens, but before the "login as" message appears, the program stops, as shown below. 

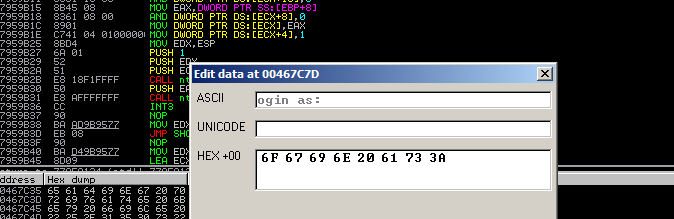
**Task 2: Alter the Login Message**

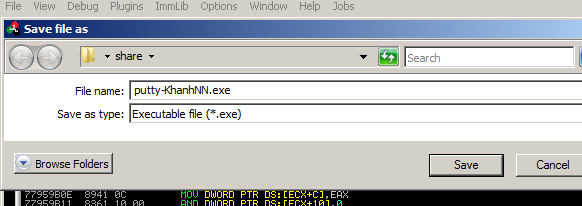
Viewing the Stored Message

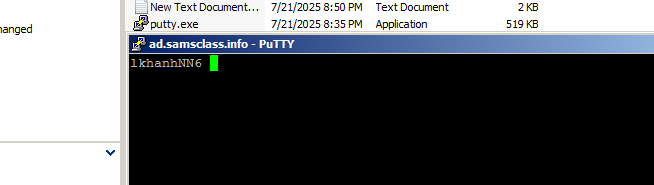
Skipping the First Letter In the Message

Running the Modified Program

Inserting Your Name

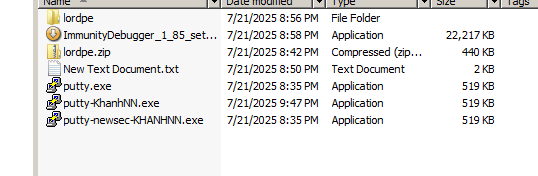
An "Edit data at 00467C7D" box opens, as shown below.

Saving the Modified EXE

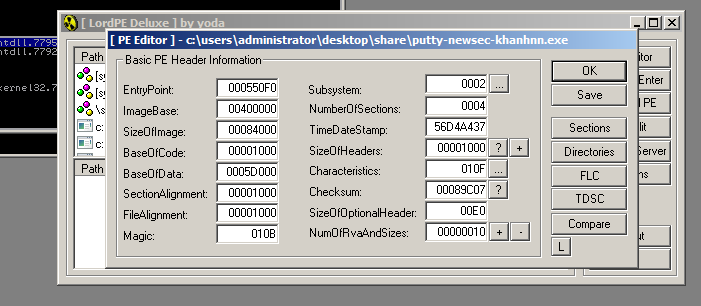
Running the Modified EXE

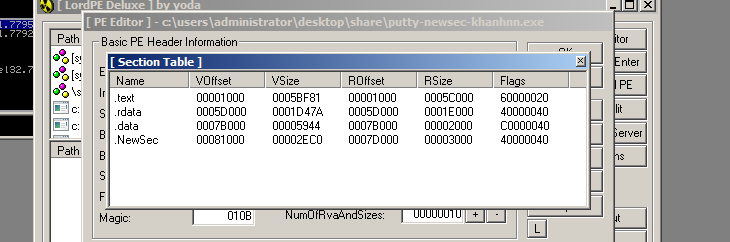
**LAB 19.2: EXE With Trojan Code in a New Section**

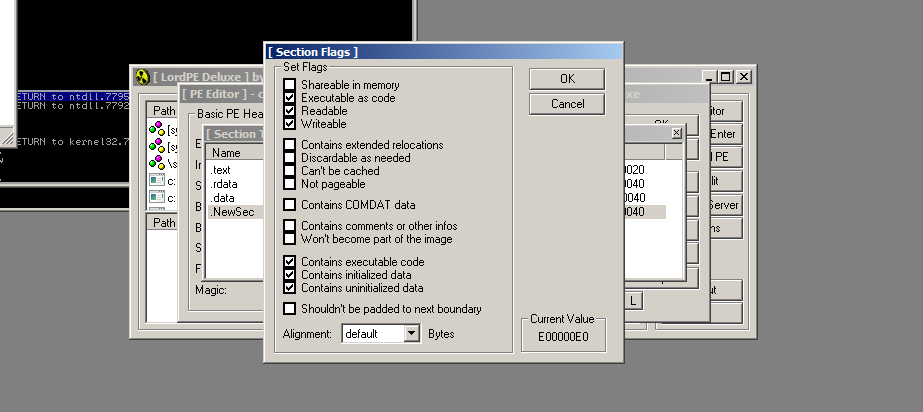
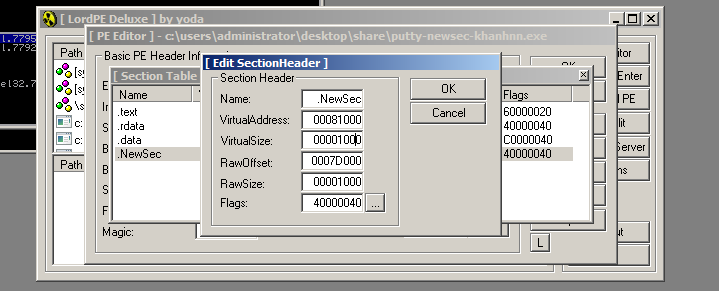
**Task 1: Add a Section with LordPE**



Adding a New Section to the PE Header

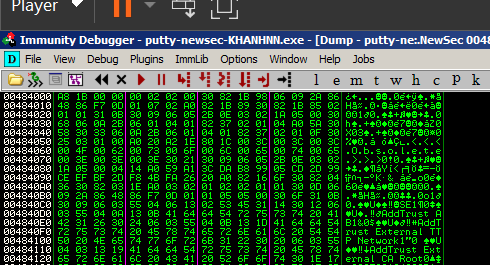
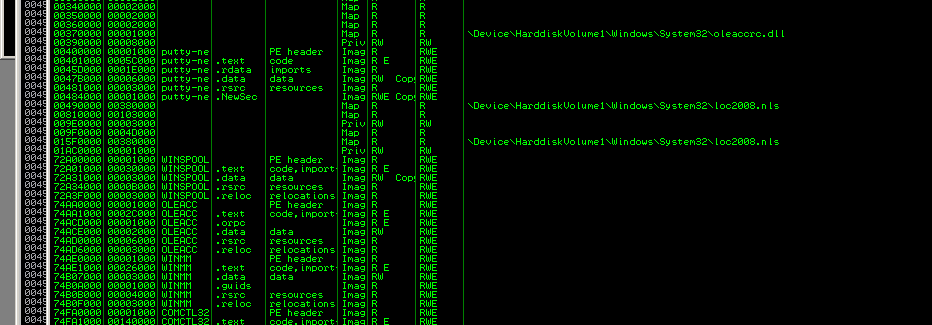
In the LordPE window, on the right side, click the "PE Editor" button. In the Open box, navigate to putty-newsec-YOURNAME.exe and double-click it. A "PE Editor" box opens, showing general information about putty, as shown below.

In the "PE Editor" box, on the right, click the Sections button. A "Section Table" box opens, showing the four sections in the putty executable. Right-click one of the sections and click "add section header", as shown below. In the "Section Table" box, right-click NewSec and click "edit section header".

In the "[Edit SectionHeader]" window, change the VirtualSize and RawSize to 00001000 as shown below. 

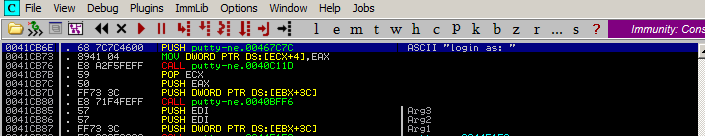
**Task 2: Redirecting Code Execution with Immunity**

Using Immunity to Examine the NewSec Section

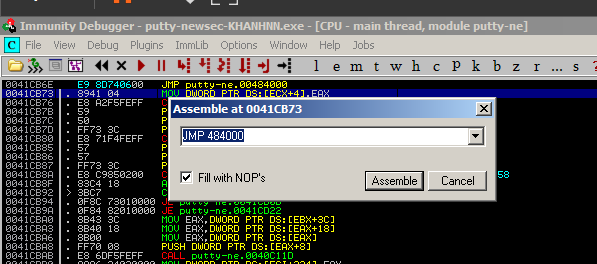
Immunity shows the memory layout of putty. As outlined in blue in the image below, the "NewSec" section begins at address 484000. 

Using Immunity to Redirect Code Execution

In the "Enter expression to follow" box, enter 41CB6E as shown below. Click OK.

Immunity moves to show the PUSH instruction that loads the "login as: " string, as shown below

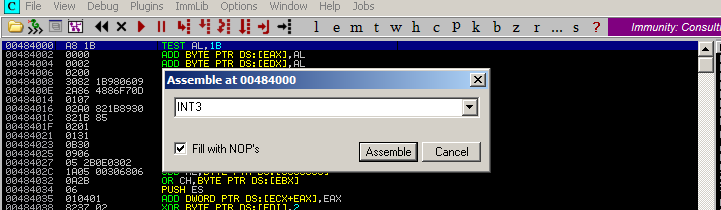
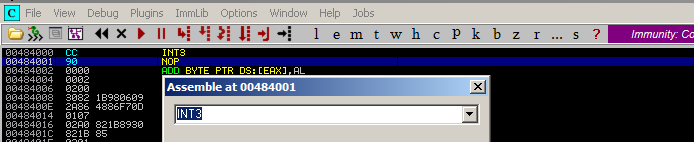
Right-click the PUSH instruction and click Assemble, as shown below.

In the "Assemble" box, enter this command: JMP 484000 

Adding Trojan Code

Now we can add extra commands to Putty in ".NewSec". First we'll just put an INT3 there, so we can verify that the redirection works. When the processor executes the INT3 command, the program will stop and show a message in Immunity.

In the JMP insruction, right-click 00484000. and click Follow. Immunity moves to address 00484000.

Right-click 00484000 and click Assemble. Enter this command, as shown below. **INT3** **** 

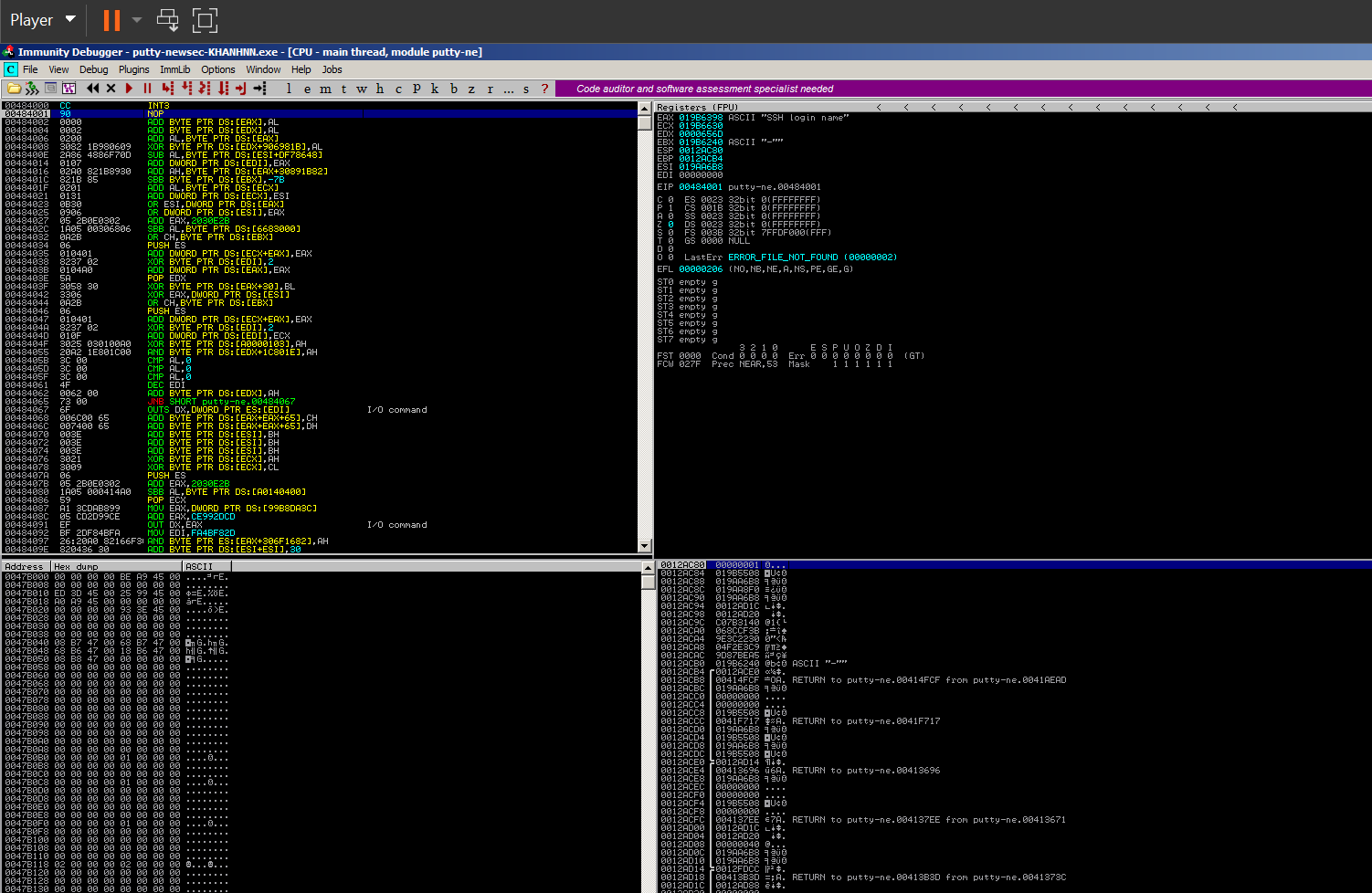
Running the Modified App in Immunity

In Immunity, click Debug, Run.

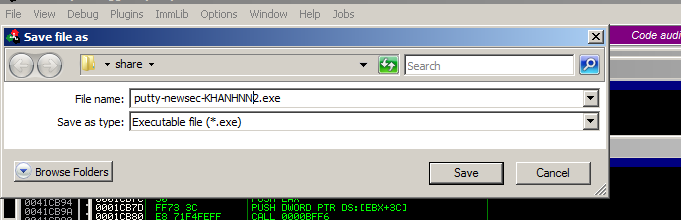
Putty opens. In the "Host Name (or IP address)" box, type **ad.samsclass.info**

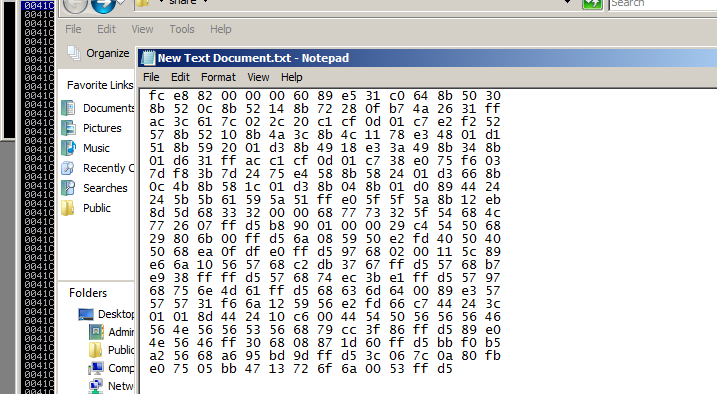
At the bottom, click the Open button.

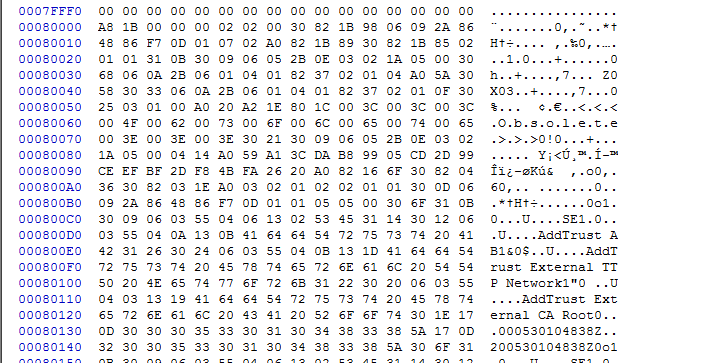
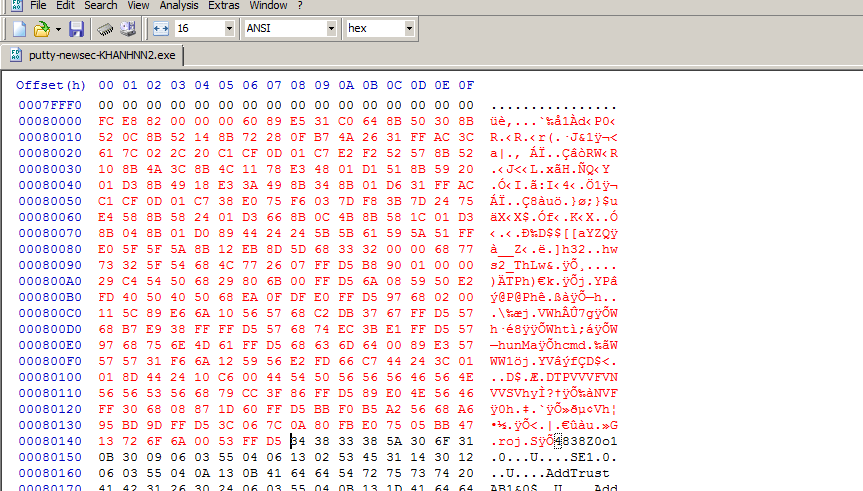
The program stops, and the status bar at the bottom of the Immunity window says "INT3 command ...", as shown below.

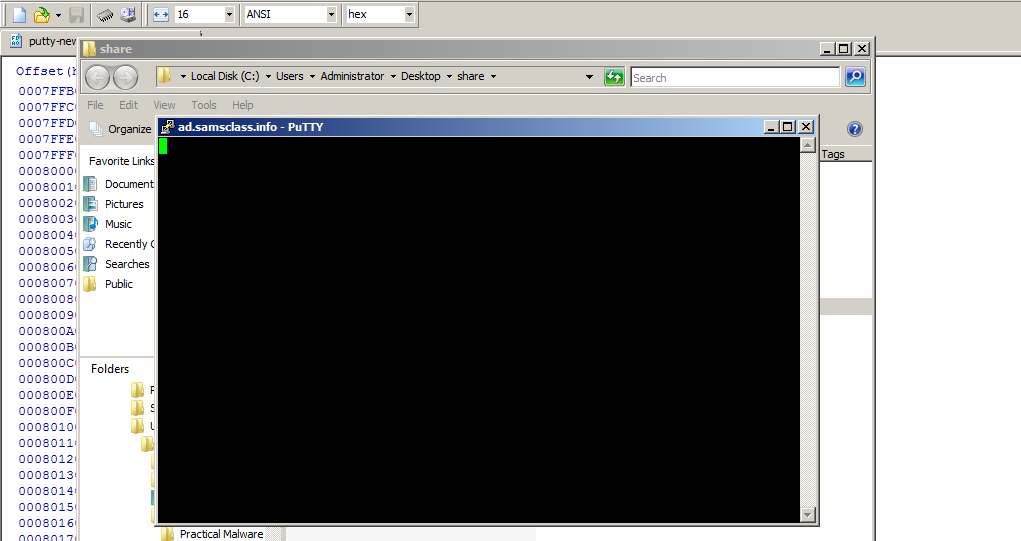
This shows that the code redirection worked, and executed the first instruction in the .NewSec section! 

**Task 3: Inserting Real Shellcode**

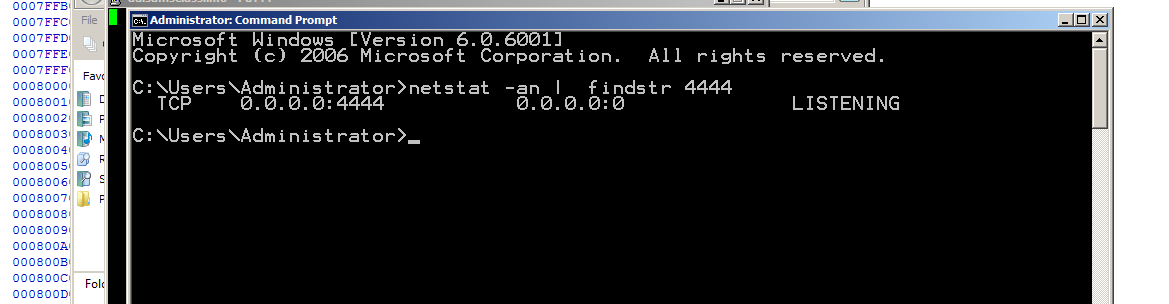
Saving the Modified EXE

Getting Simple Shellcode 

Inserting Shellcode with HxD  

Running the Trojaned Putty 

Open a Command Prompt and execute this command: netstat -an | findstr 4444

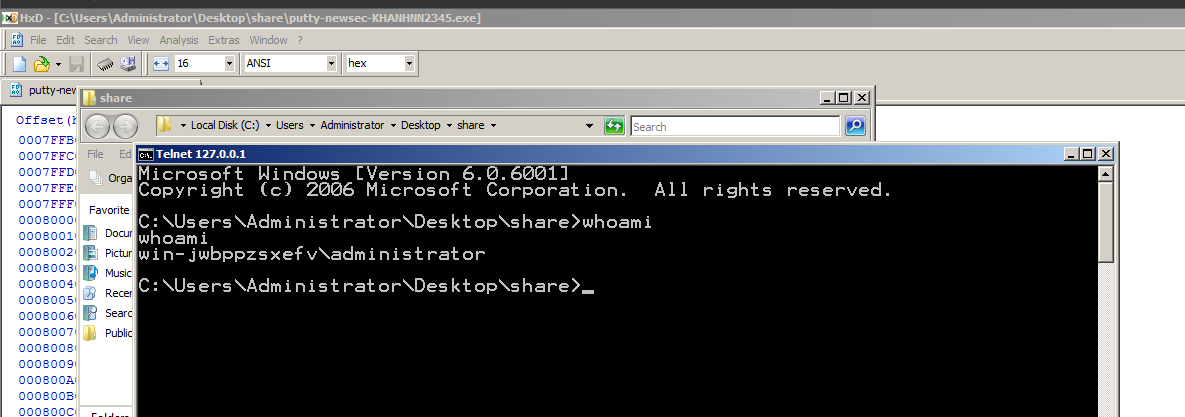
You should see port 4444 LISTENING, as shown below.

Connecting to the Target

Open another Command Prompt window. Execute this command: **telnet 127.0.0.1 4444**

A Command Prompt opens, allowing you to execute commands on the server, as shown below.

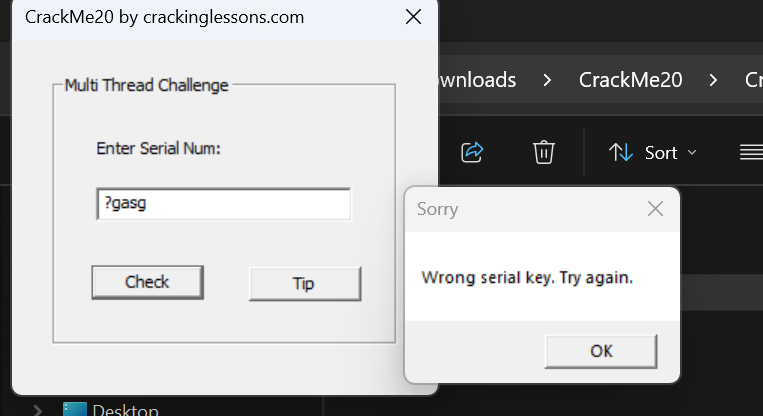
Execute this command: **whoami**

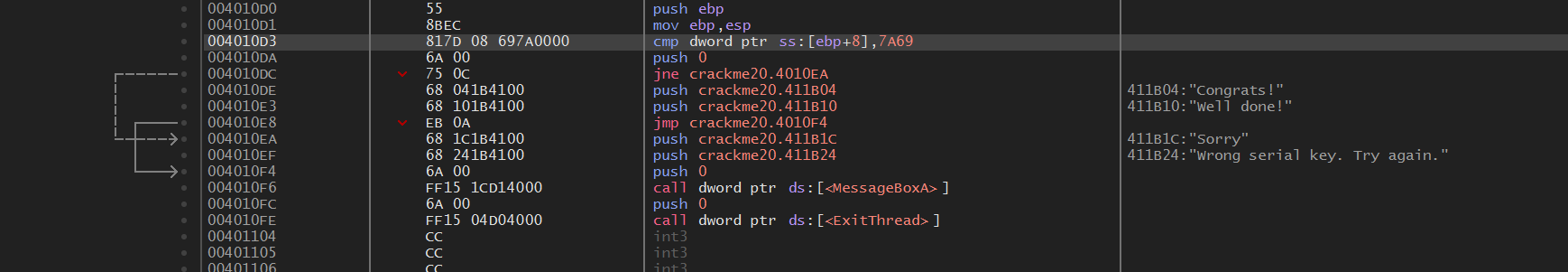
You are the local administrator, as shown below, and so is anyone else who connects to this machine on port 4444.

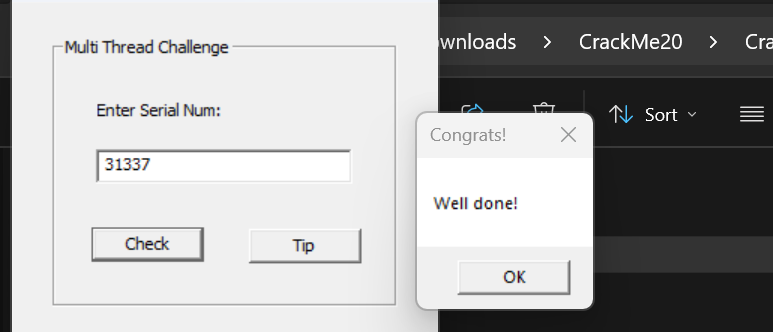
**CRACKME 20**

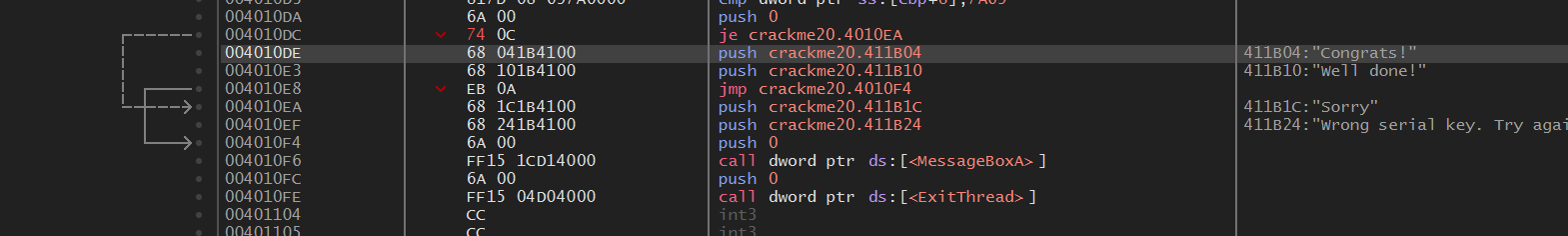
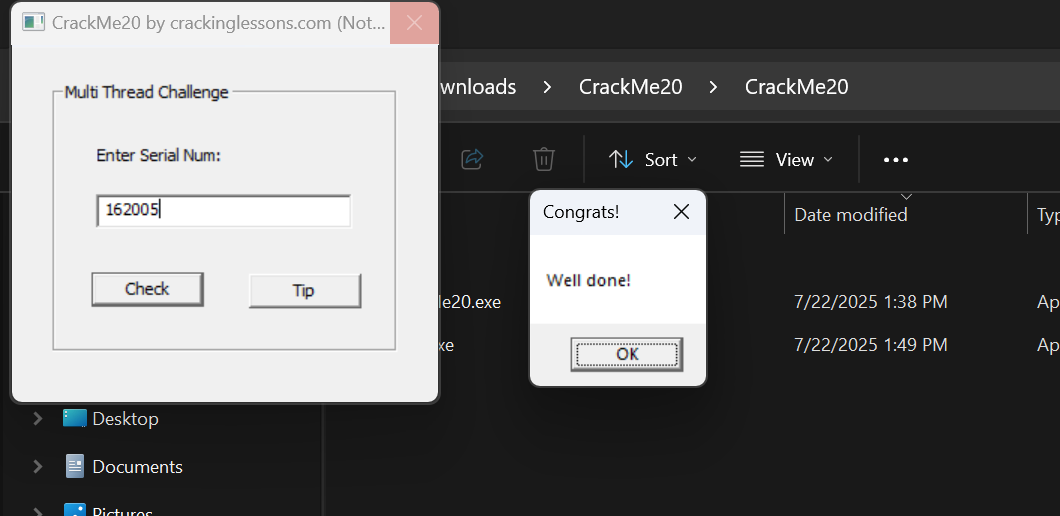
A crackme with multi-threads for you to practice cracking. The objectives are:

1. Patch the thread that checks for the correct serial number
2. Do serial fishing for the serial number



Notice that code first it compares 7A69 in hexa (equals to 31337) with ptr, may be that is the my input serial key. So I check the value 31337 firstly, to try to fishing serial key.

And we finished the challenge fishing, next move to patch thread checking for the correct serial number.

Look at the code above, in the address 004010DC, the JNE will jump to wrong status if the serial key is incorrect, so I change it into JE to display true status ignoring the value of serial key.  

DONE!!!