Proj 8a: Simple EXE Hacking with Immunity (15 pts.)

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.

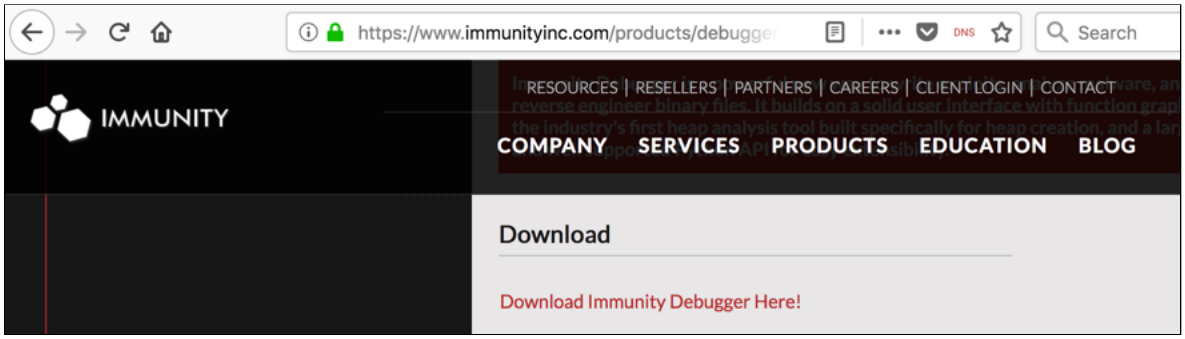
Task 1: Target EXE Recon

Get Immunity

On your Windows machine, in a browser, go to

https://www.immunityinc.com/products/debugger/

Click the "**Download Immunity Debugger Here**" link, as shown below.



If that link is not working, use this alternate download link: **ImmunityDebugger_1_85_setup.exe**

Install it with the default options.

Get putty.exe

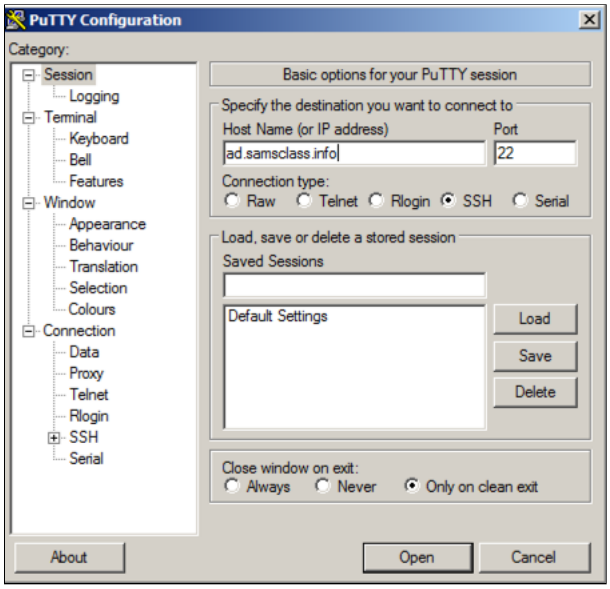
Putty is a common SSH client for Windows. It's harmless, but we will modify it to add Trojan code.

In a Web browser, right-click this link and save the putty.exe file:

https://samsclass.info/127/proj/putty.exe

Running Putty

Double-click **putty.exe**. PuTTY opens, as shown below.

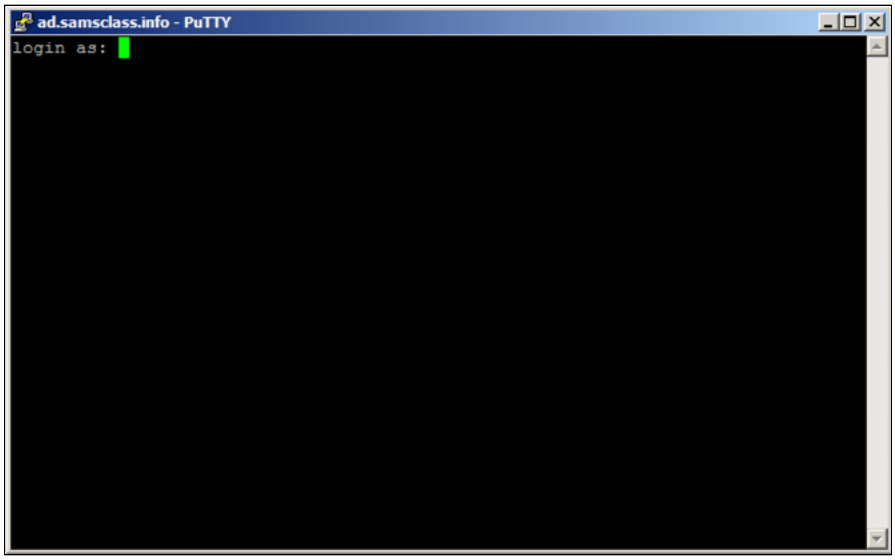


In the "Host Name (or IP address)" box, type

```
ad.samsclass.info
```

At the bottom, click the **Open** button.

A black box opens, and shows a "**login as:**" prompt, as shown below.



You could connect to a server at this point, but that's not the point of this project. We will alter this program to do other things instead of printing "login as".

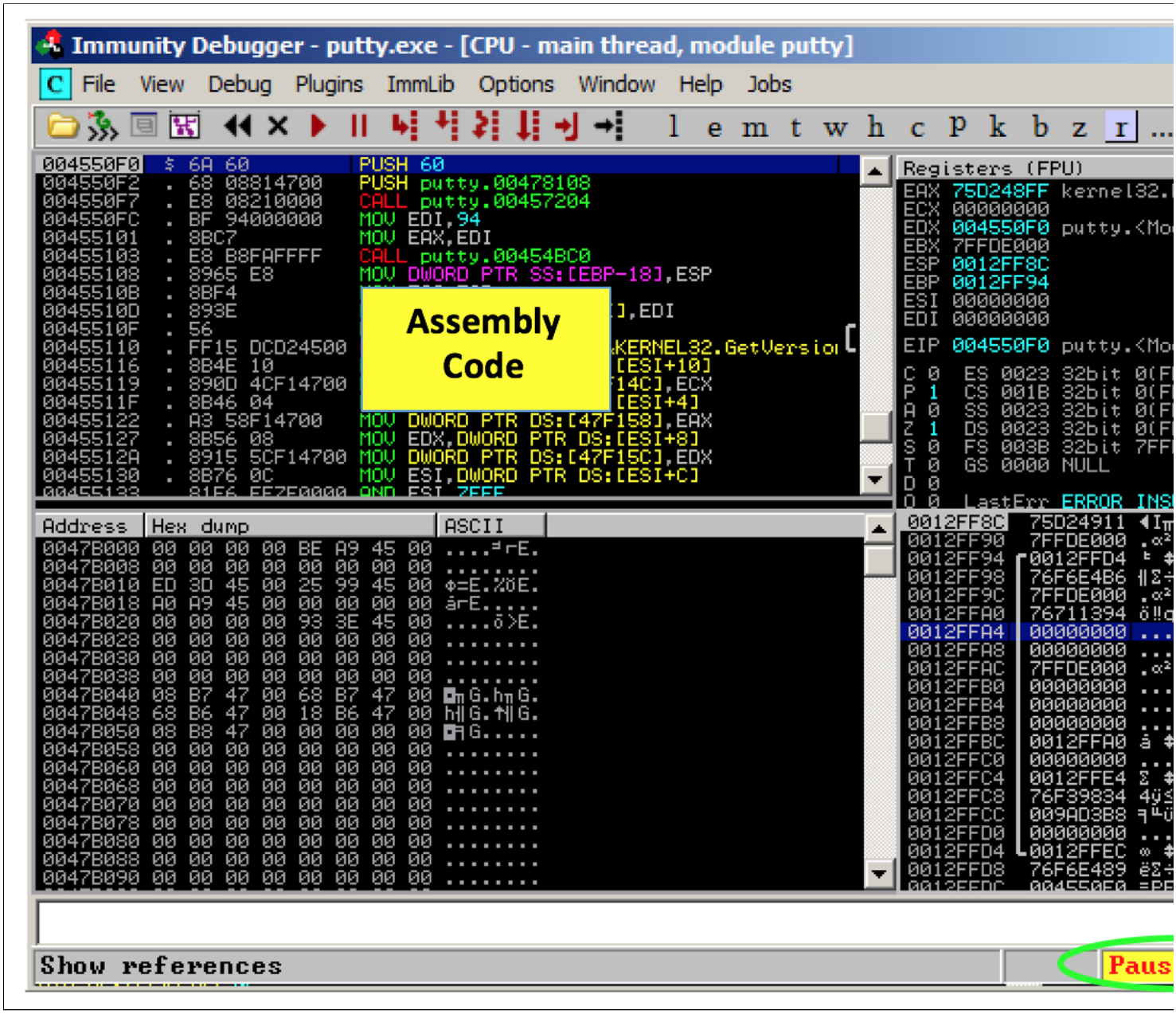
Close the Putty window.

Starting the Immunity Debugger

Click **Start**. Search for **Immunity Debugger** and start it.

In Immunity, from the menu bar, click **File**, **Open**. Navigate to **putty.exe** and open it.

Immunity opens, as shown below. If your screen doesn't look like this, click **View**, **CPU** and maximize the CPU window.



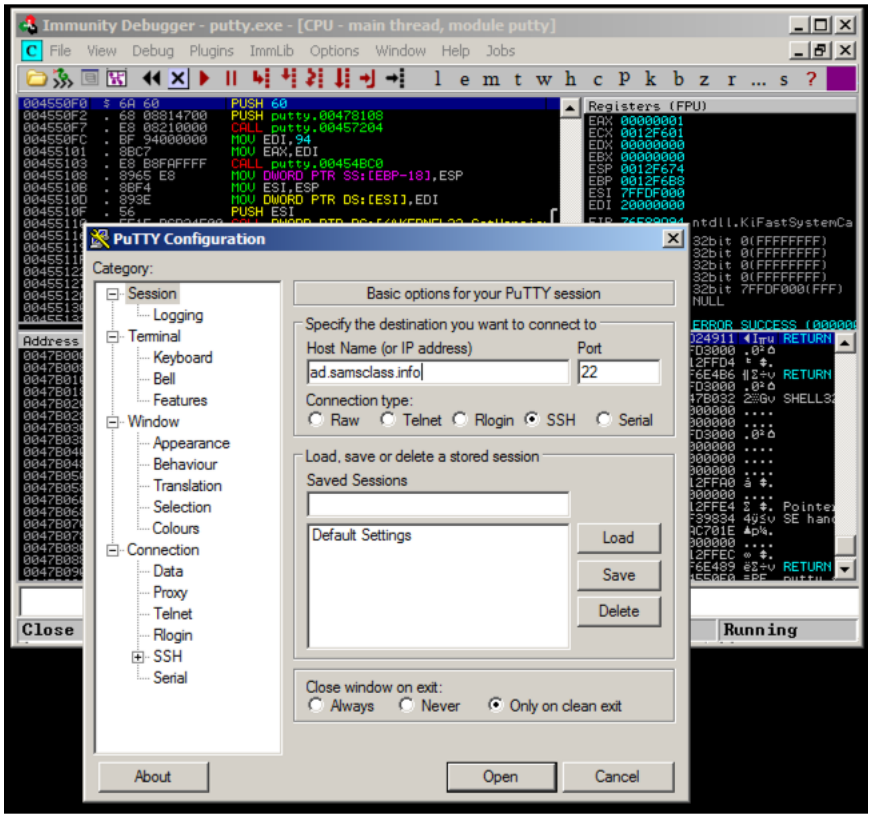
Immunity shows you a lot of data, but for now just notice the **Assembly Code** in the top left pane, and the **Paused** message in the lower right, as indicated in the figure above.

When you load a program into Immunity, it starts in a "Paused" state, with the Assembly Code window showing the first instruction.

Running Putty in Immunity

In Immunity, from the menu bar, click **Debug**, **Run**.

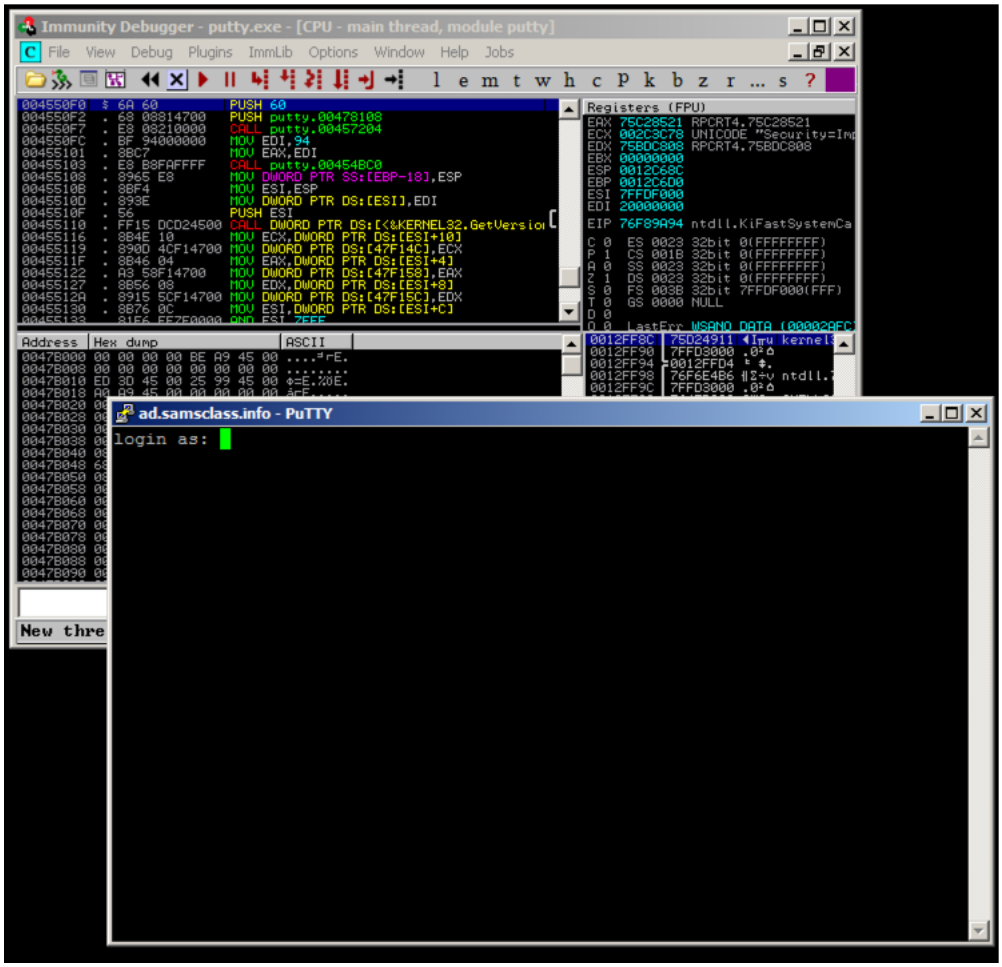
A Putty window opens, as shown below.



Click in the Putty window. In the "Host Name (or IP address)" box, type

`ad.samsclass.info`

At the bottom, click the **Open** button. The "login as" message appears, as shown below.



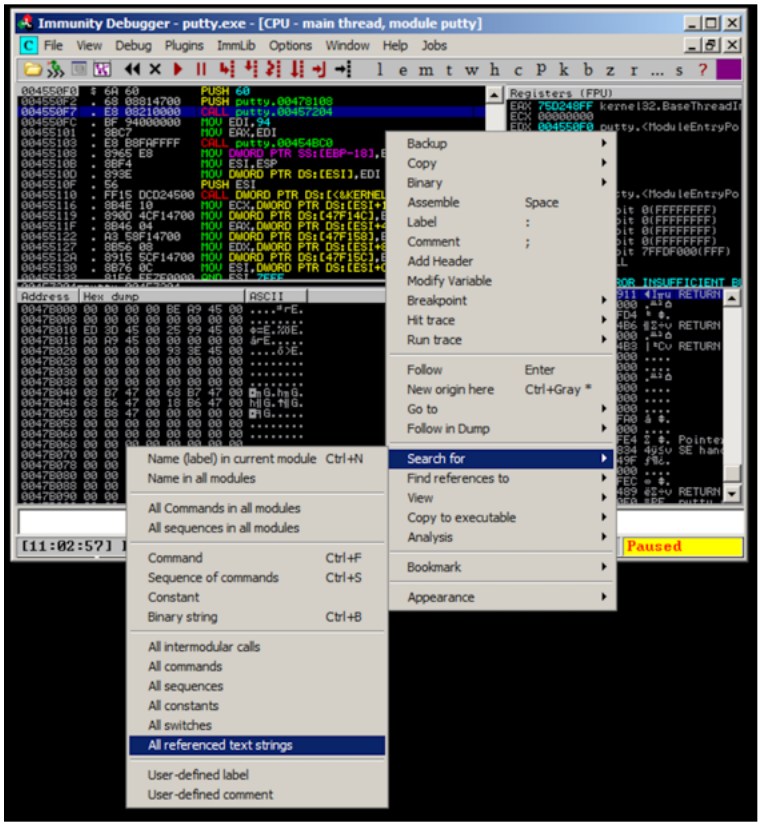
Putty is running, but it's under the control of Immunity, so we can modify its execution.

Finding the "login as" Code

Close the Putty window.

In Immunity, from the menu bar, click **Debug**, **Restart**.

In Immunity, in the "Assembly Code" pane, right-click. Point to "**Search for**". Click "**All referenced text strings**", as shown below.

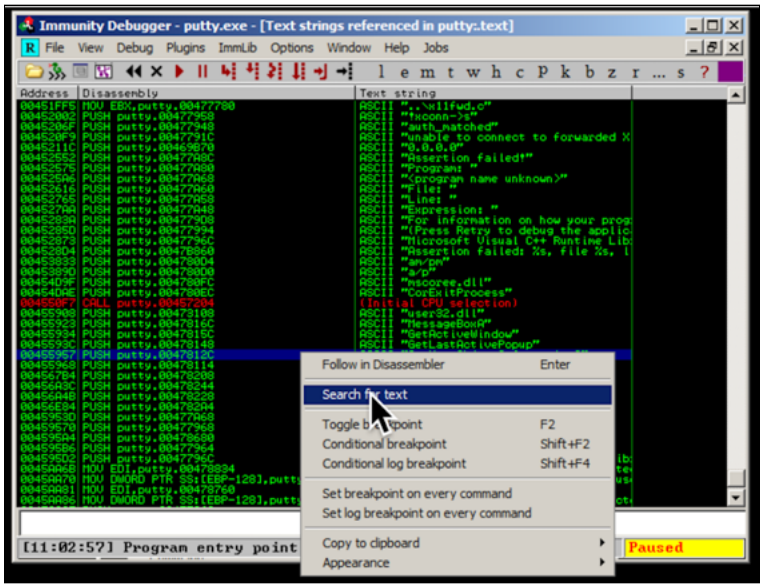


A "Text strings referenced in putty:.text" window opens, showing all the strings in the program.

Scroll to the top of the window and click on the first line, so it is highlighted.

Right-click in the window, and click "**Search for text**", as shown below.

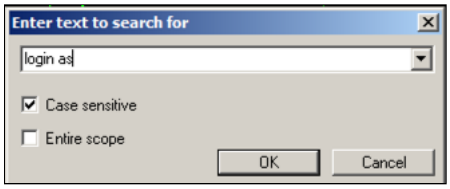
Note: the search only goes down, and does not wrap, so if you begin a search near the bottom of the window it won't find "login as".



In the "Enter text to search for" box, type

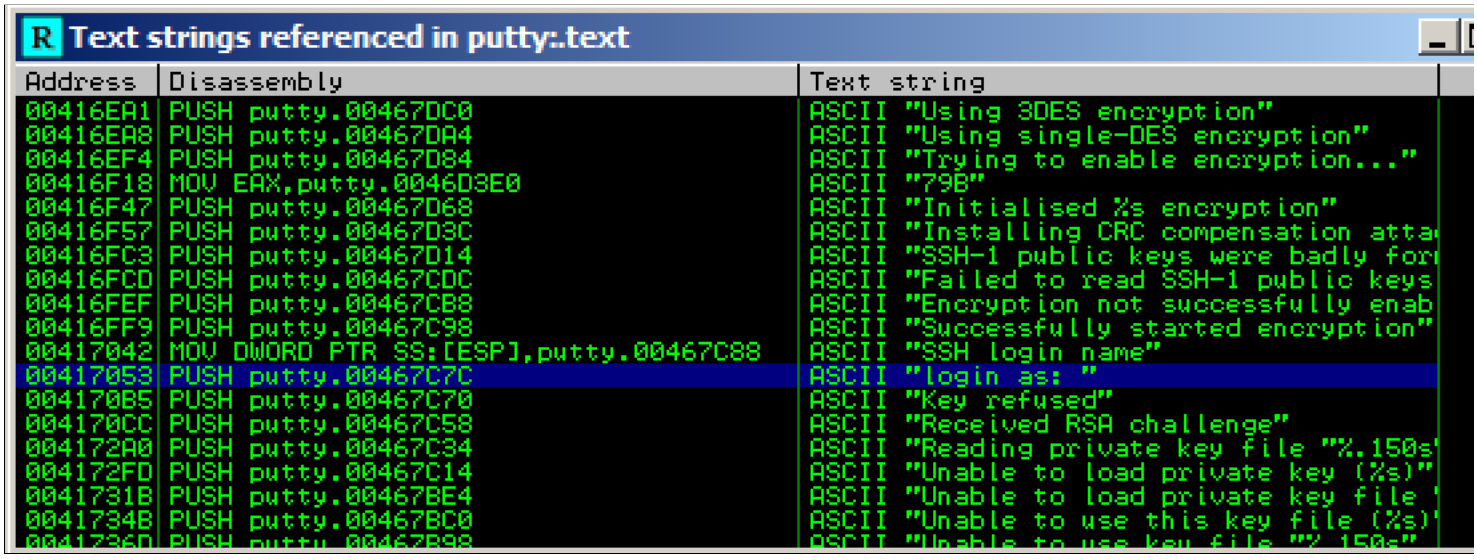
```
login as
```

as shown below.



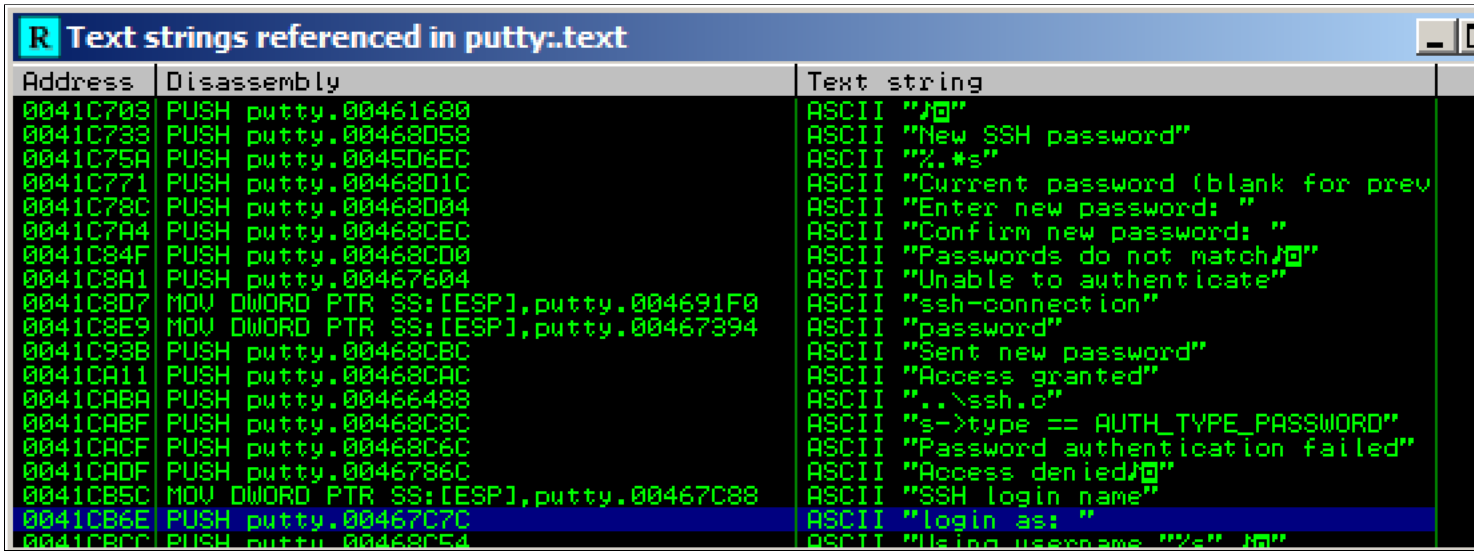
Click **OK**.

Immunity finds the ASCII string "login as", and the instruction that uses it, as shown below. This instruction is at address 00417053.



Right-click again, and click "**Search next**".

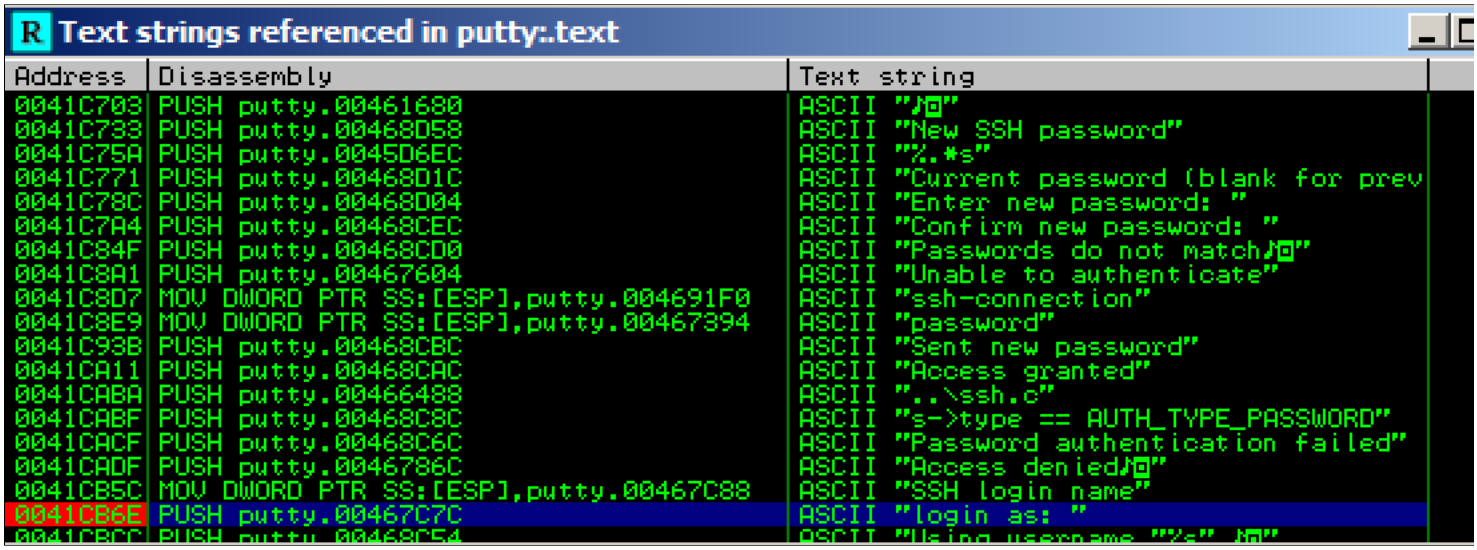
Immunity finds another line of code that uses this string, as shown below. This instruction is at address 0041CB6E.



Using Breakpoints

We'll set a breakpoint at this instruction, at address 0041CB6E.

On your keyboard, press the **F2** key. Mac users, press **fn+F2**. The address turns red, as shown below, to indicate that there's a breakpoint here.

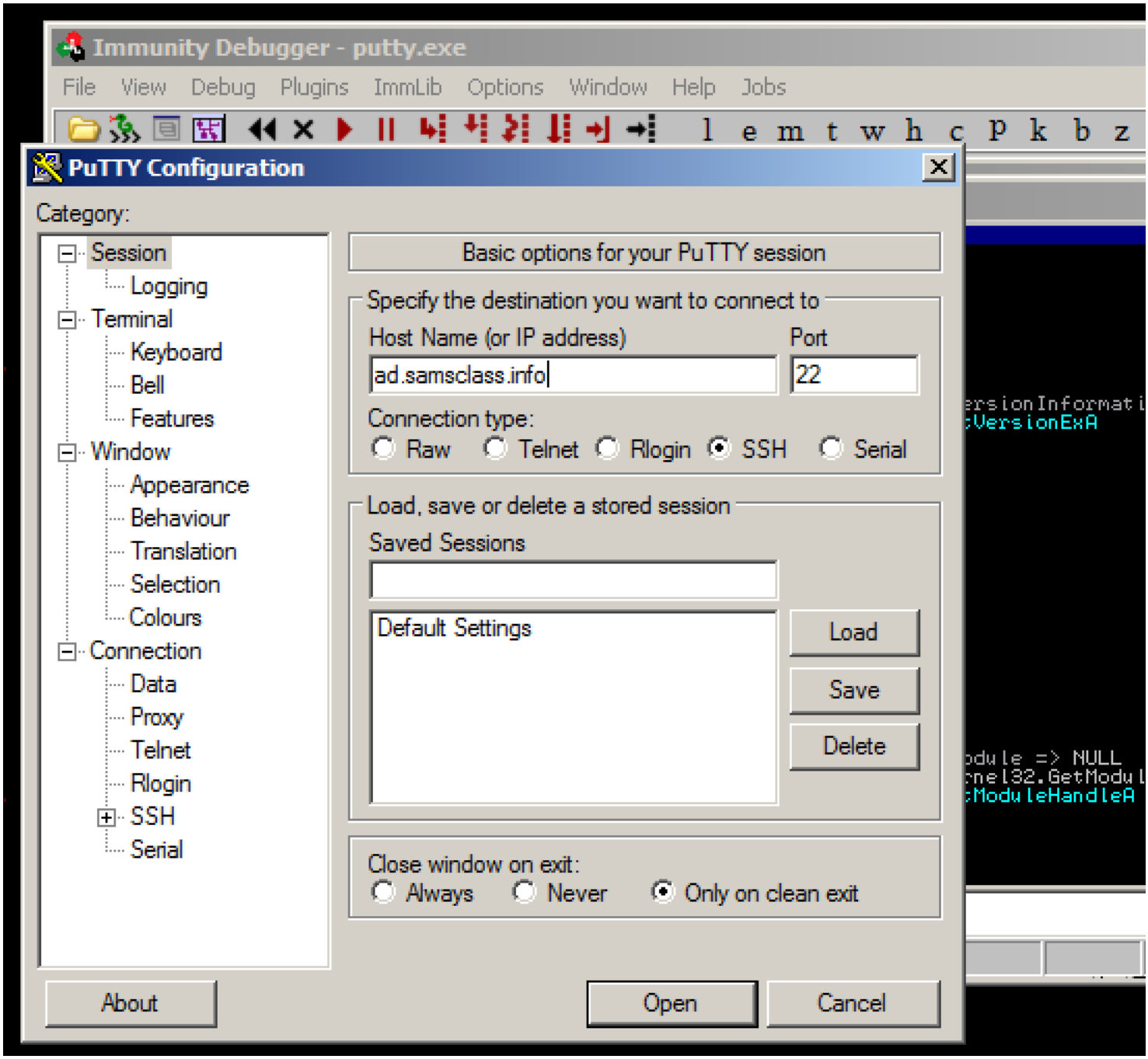


In Immunity, from the menu bar, click **Debug**, **Restart**.

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.

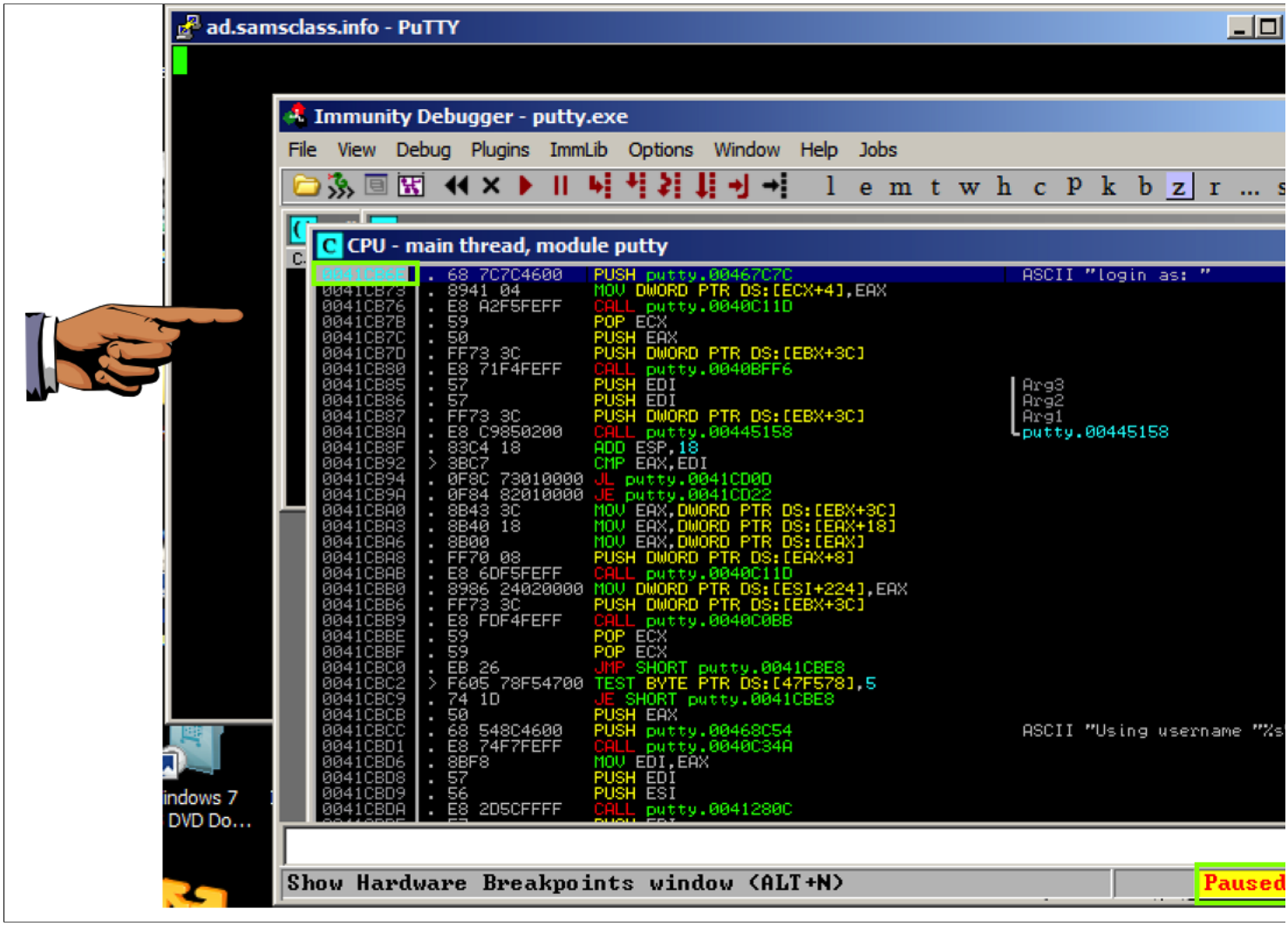


Click in the Putty window. In the "Host Name (or IP address)" box, type

`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.



The program stopped at instruction 0041CB6E, as shown in the image above.

We'll use this instruction to hijack the program's execution.

Saving a Screen Image

Make sure you can see the address **0041CB6E** in the top left of the CPU window, and **Paused** in the lower right, as shown above.

Press the **PrintScrn** key to copy the whole desktop to the clipboard.

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

Paste the image into Paint.

Save the document with the filename "**YOUR NAME Proj 8a1**", replacing "YOUR NAME" with your real name.

Task 2: Alter the Login Message

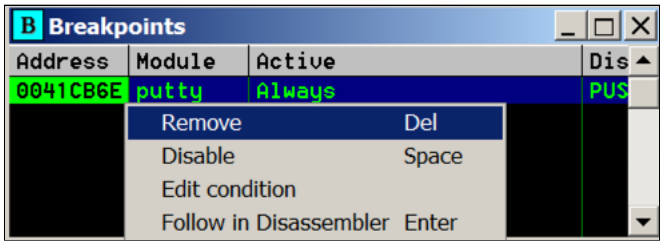
Removing the Breakpoint

We don't need the breakpoint any more, so we'll remove it.

In Immunity, from the menu bar, click **View**, **Breakpoints**.

A "Breakpoints" window opens, showing the breakpoint.

Right-click the breakpoint and click **Remove**, as shown below.

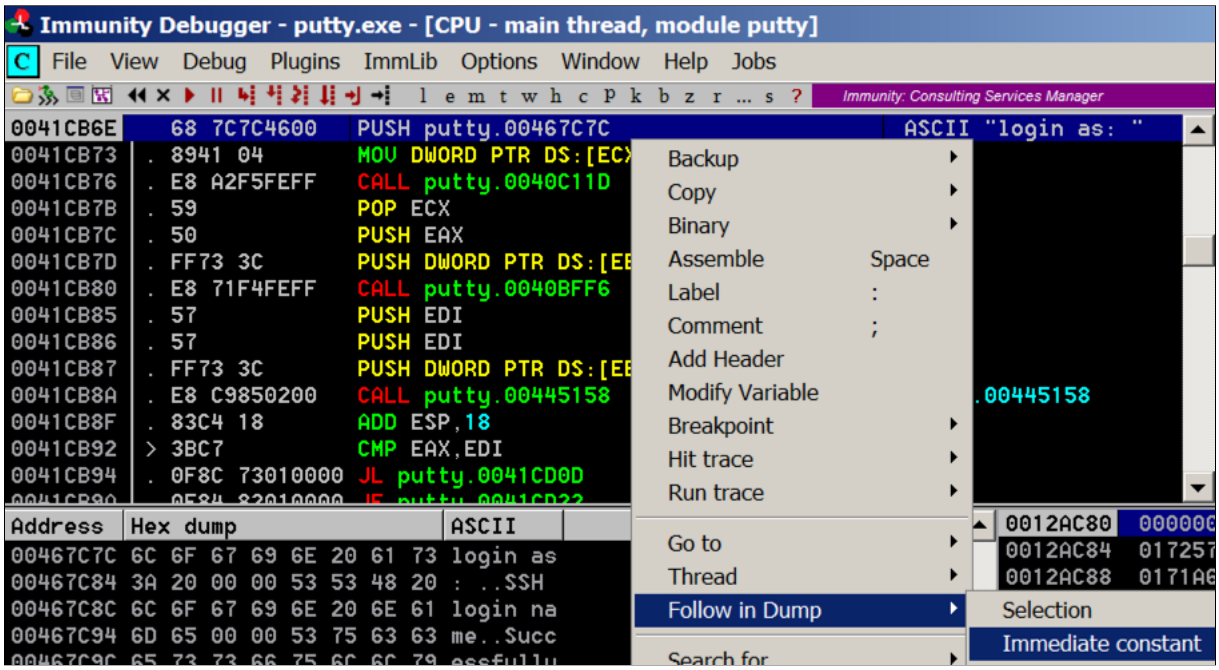


Close the "Breakpoints" window.

Viewing the Stored Message

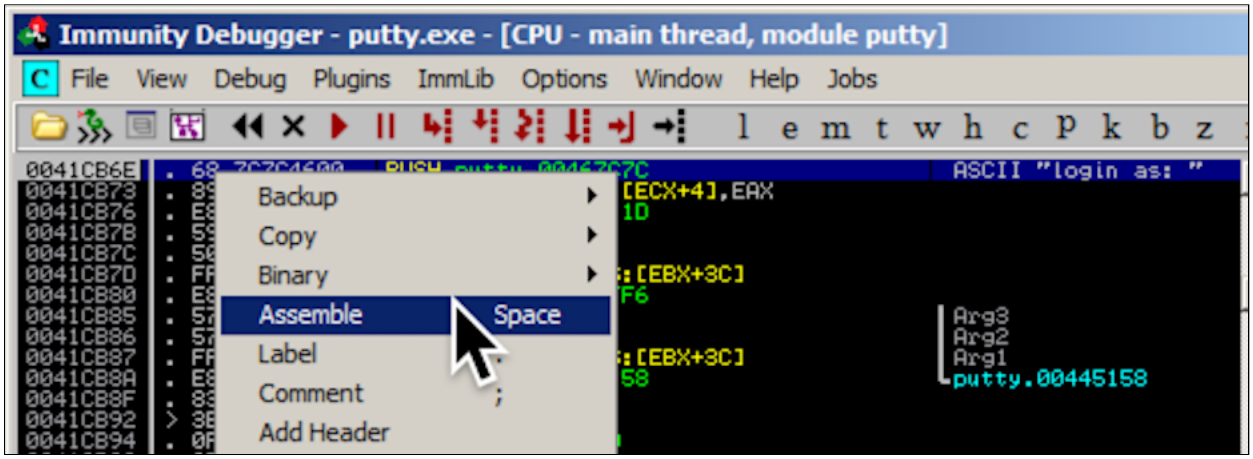
In Immunity, in the CPU window, in the Assembly Code pane, right-click the intruction at address **0041CB6E** and click "**Follow in Dump**", "**Immediate constant**", as shown below.

The lower left pane shows the stored "login as" message, in hexadecimal and ASCII text.



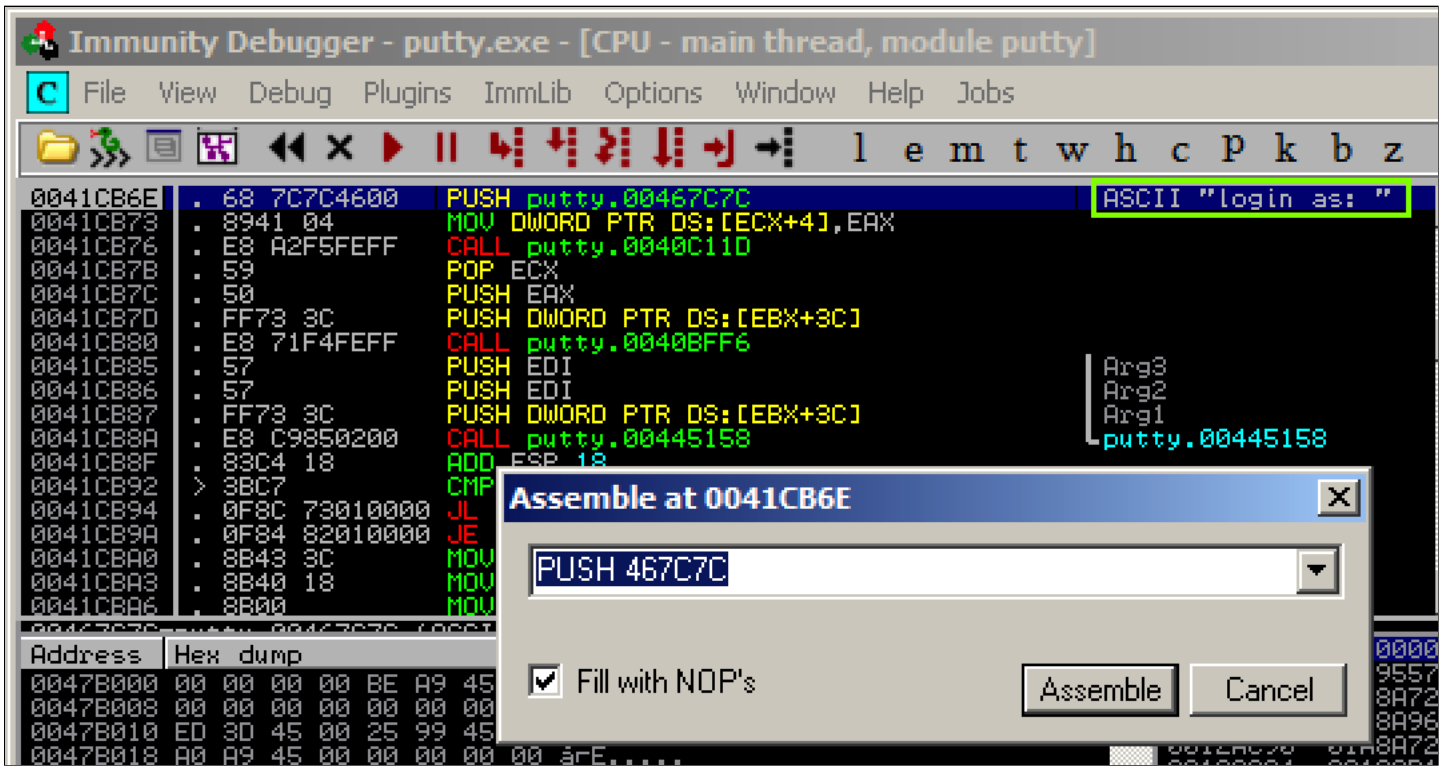
Skipping the First Letter In the Message

In Immunity, in the CPU window, in the Assembly Code pane, right-click the intruction at address **0041CB6E** and click **Assemble**, as shown below.

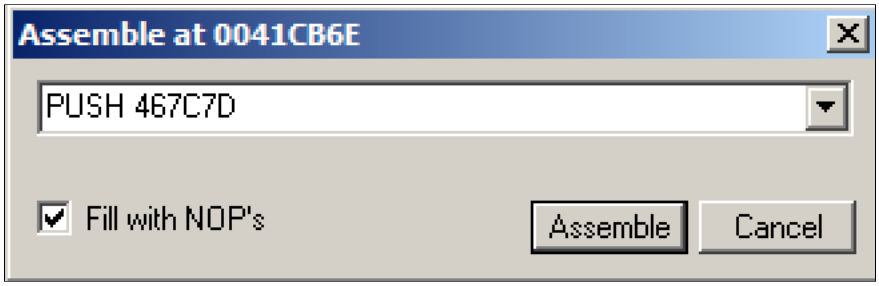


An "Assemble at 0041CB6E" box appears, as shown below.

This shows the command at this location. It's a PUSH instruction, placing the address 467C7C onto the stack. That address points to the letter "l" in the ASCII string "login as: ", as shown on the right side of the instruction line, outlined in green in the image below.



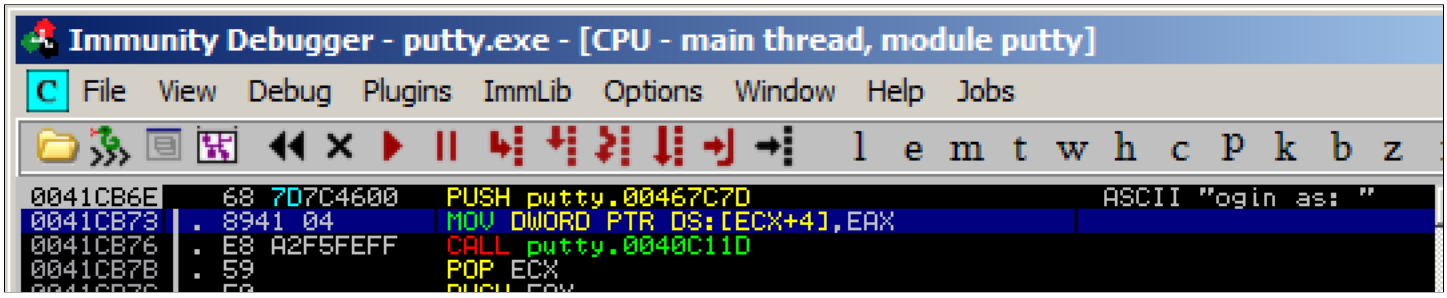
In the "Assemble at 0041CB6E" box, change the last character to **D**, as shown below. This will move the pointer from the "l" to the "o" in the string "login as: ".



Click the **Assemble** button.

Click the **Cancel** button.

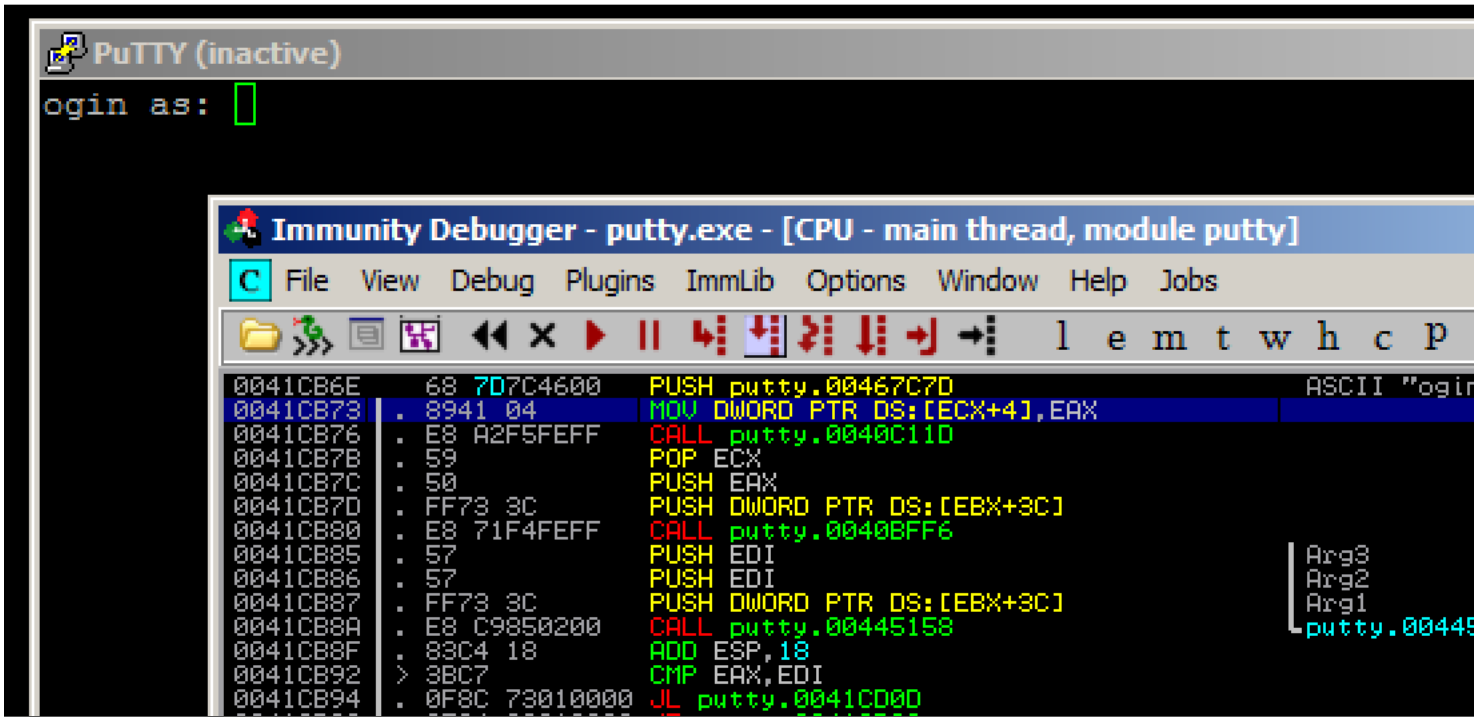
The message on the right now says "ogin as: ", as shown below.



Running the Modified Program

In Immunity, from the menu bar, click **Debug**, **Run**.

The black login window appears, with the message "ogin as: ", as shown below.

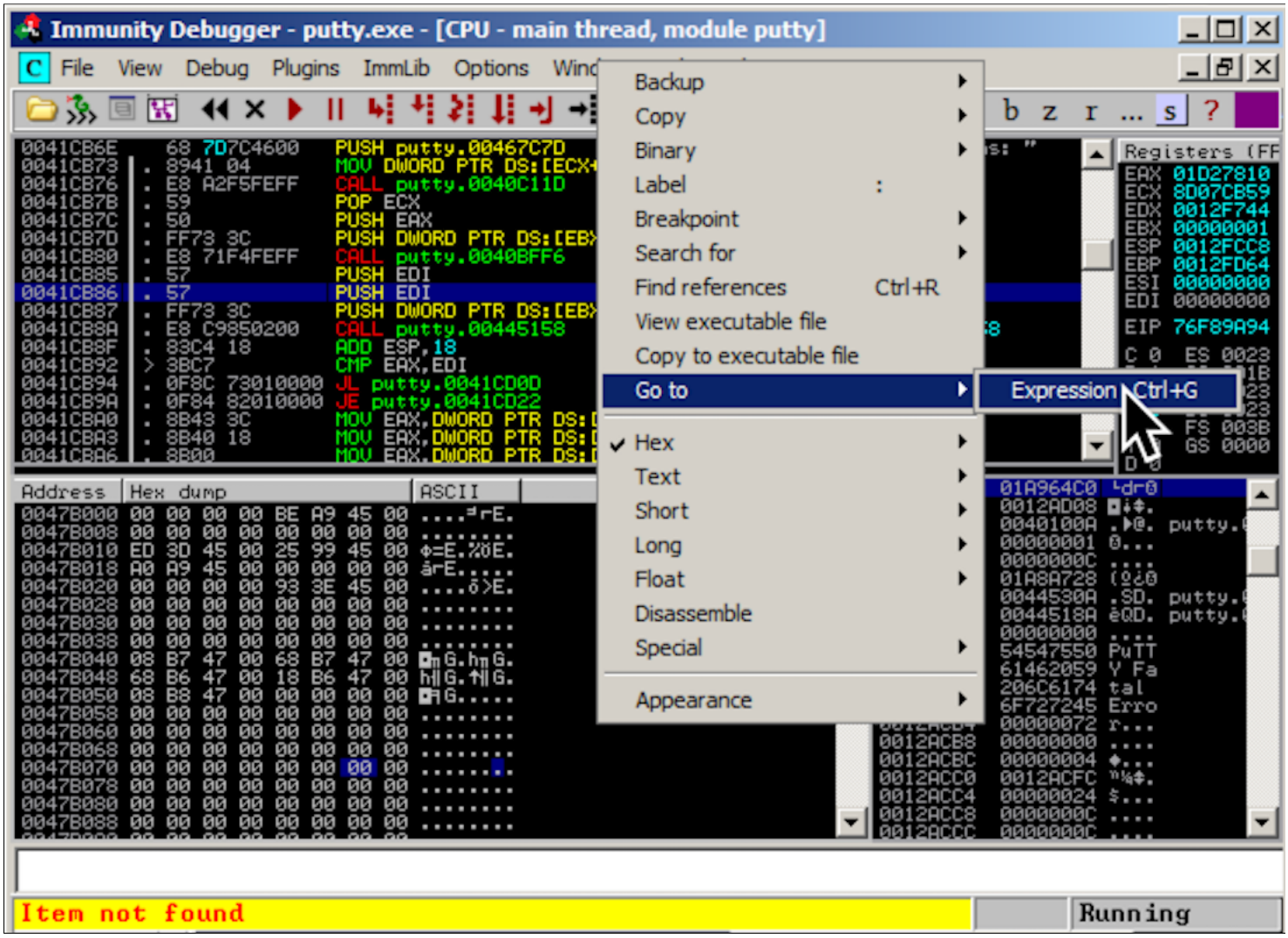


Inserting Your Name

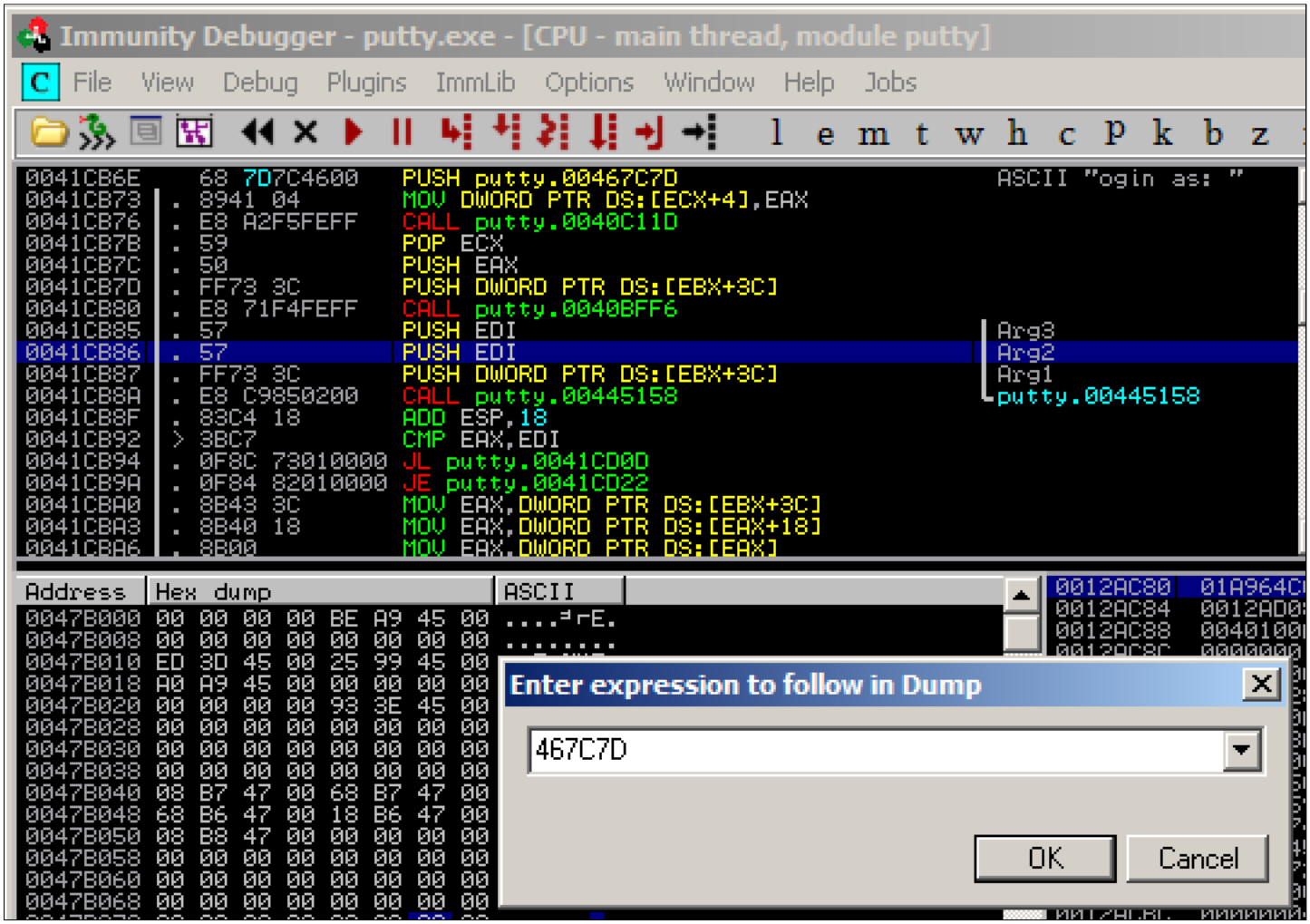
Now we want to change the text from "ogin as: " to your name.

Move your mouse into the lower left pane of the CPU window, which is the "hex dump" pane.

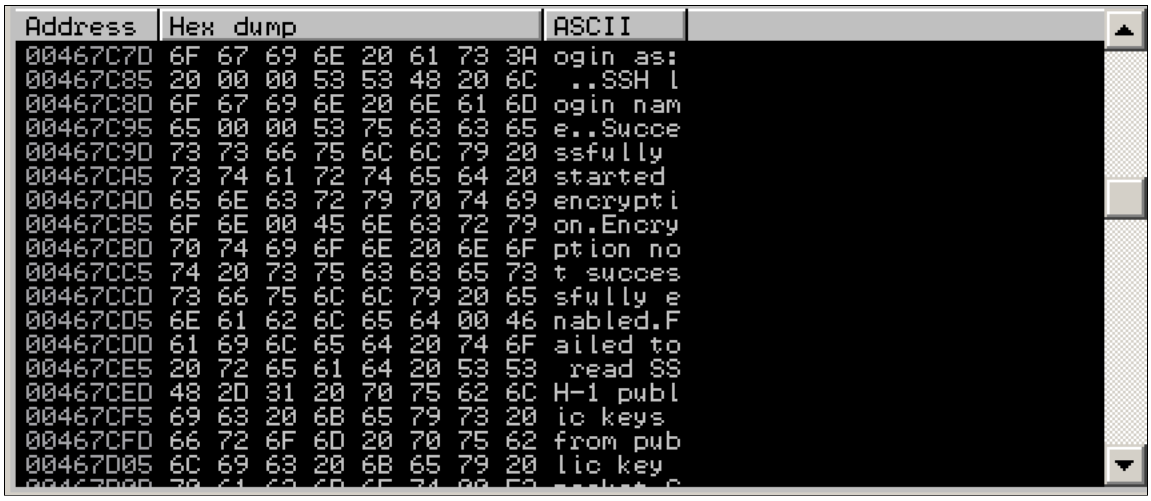
Right click, point to "**Go to**", and click **Expression**, as shown below.



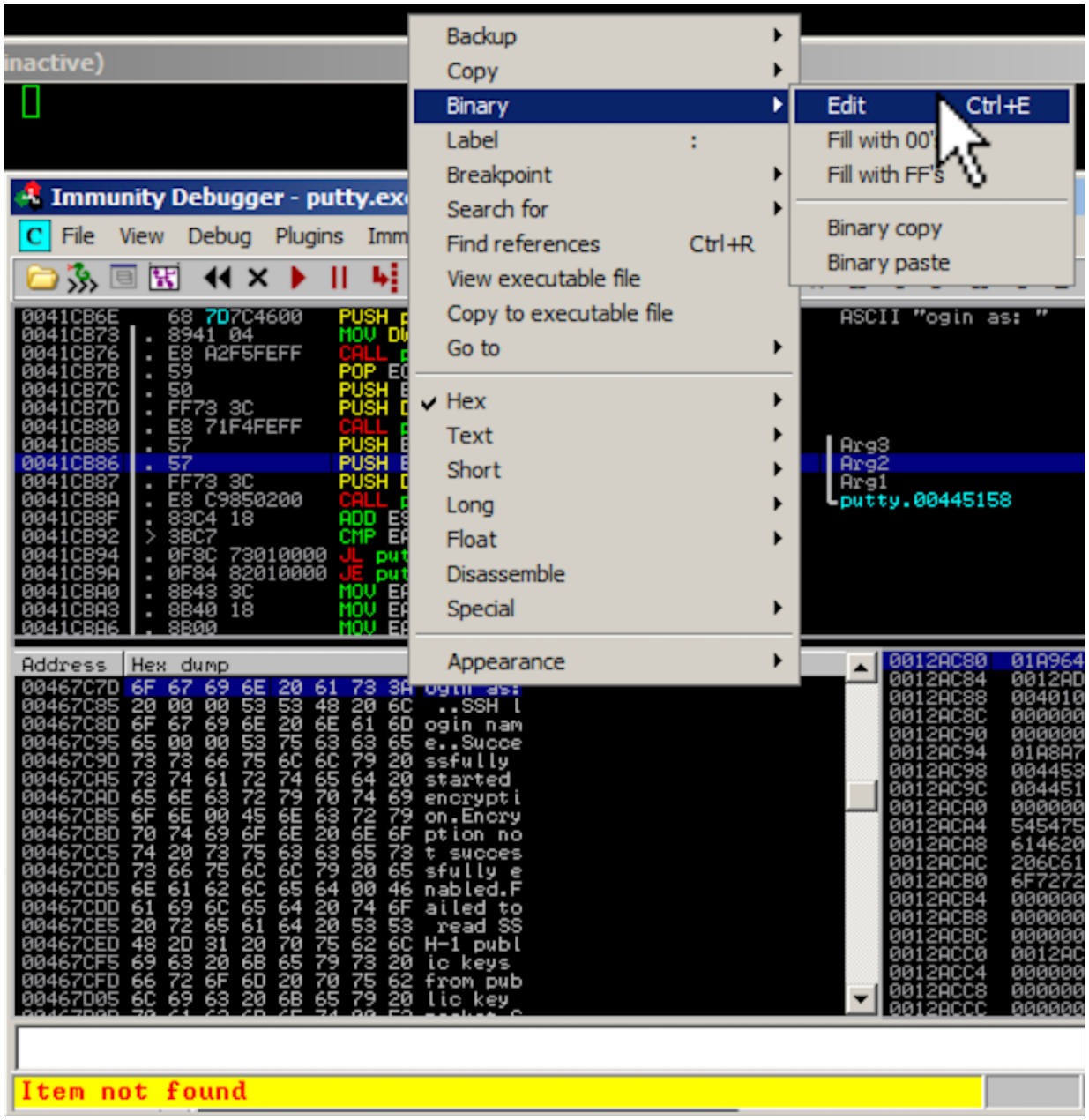
Enter **467C7D** into the box, as shown below. Click **OK**.



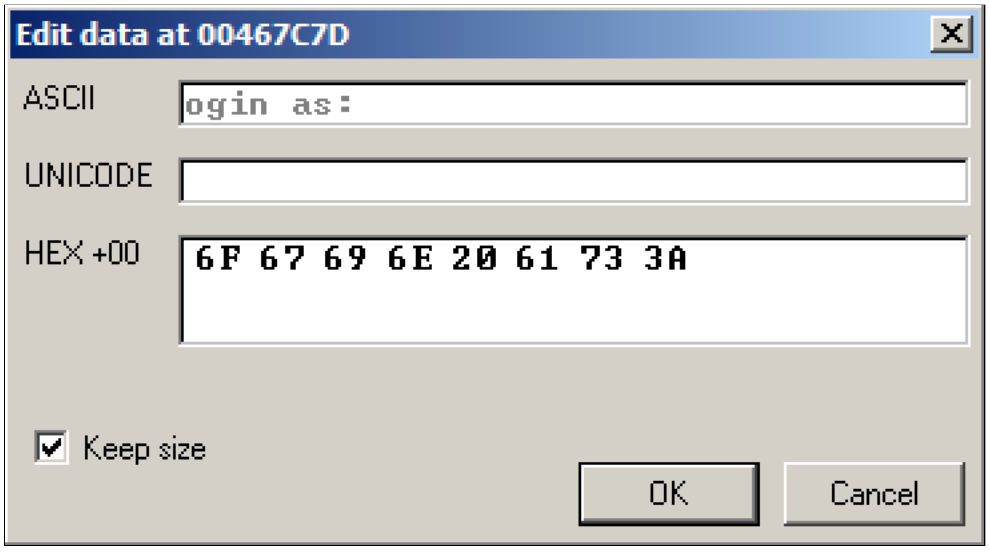
The Hex Dump shows the text "ogin as: ", as shown below.



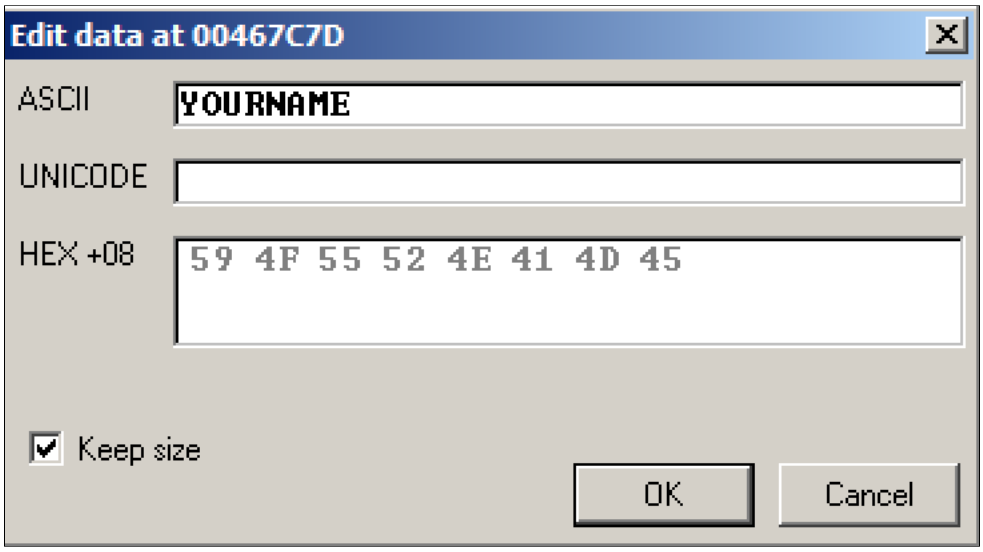
In the top left of the Hex Dump pane, point to **6F**, hold down the left mouse button, and select the entire row of 8 bytes. Then release the left button, point to **Binary**, and click **Edit**, as shown below.



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



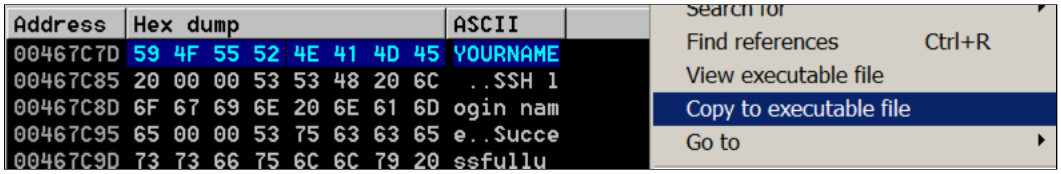
Click in the ASCII box, press Backspace to move back to the start, and overwrite the message with some version of your name. Make sure you insert exactly 8 letters. Don't use the literal text "YOURNAME", replace it with your own name.



Click **OK**.

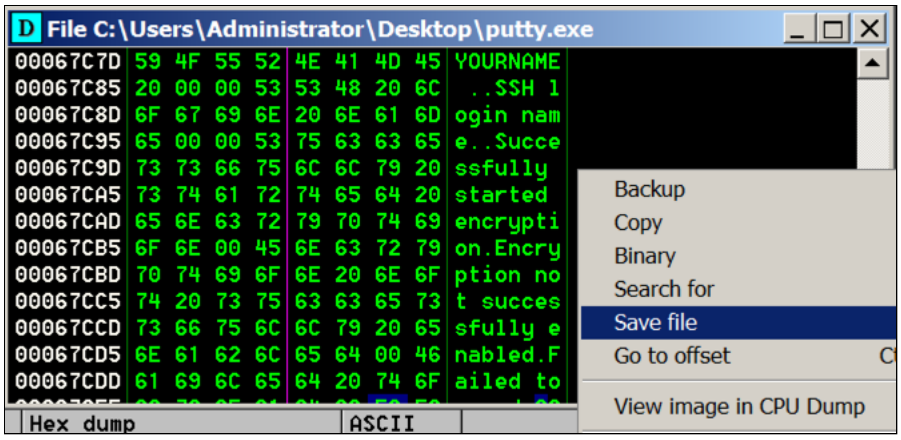
Saving the Modified EXE

In Immunity, in the lower left pane of the CPU window, right-click and click "**Copy to Executable File**", as shown below.



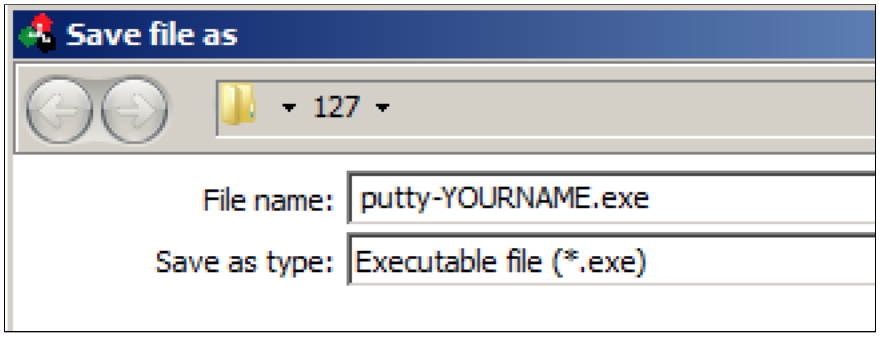
A new window pops up, with a title beginning with "File", as shown below.

Right-click in the new window and click "**Save file**".



Save the file as "putty-YOURNAME.exe", replacing YOURNAME with your own name, as shown below.

Click **Save**.



Running the Modified EXE

Close Immunity.

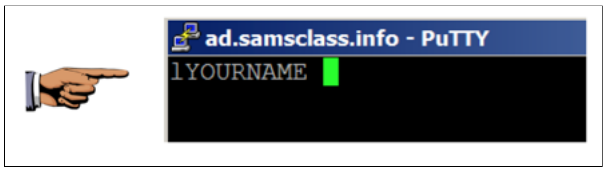
Double-click **putty-YOURNAME.exe**.

In the "Host Name (or IP address)" box, type

```
ad.samsclass.info
```

At the bottom, click the **Open** button.

A black box opens, and shows a prompt containing **YOURNAME**, as shown below.



Saving a Screen Image

Make sure you can see **YOURNAME** in the PuTTY window, as shown above.

Press the **PrintScrn** key to copy the whole desktop to the clipboard.

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

Paste the image into Paint.

Save the document with the filename "**YOUR NAME Proj 8a2**", replacing "YOUR NAME" with your real name.

Turning in your Project

Email the images to **cnit.127sam@gmail.com** with the subject line: **Proj 8a from YOUR NAME**

Sources

Backdooring PE Files - Part 1

Art of Anti Detection 2 â€“ PE Backdoor Manufacturing

https://github.com/EgeBalci/Cminer

https://en.wikipedia.org/wiki/Code_cave

http://stackoverflow.com/questions/787100/what-is-a-code-cave-and-is-there-any-legitimate-use-for-one

The Beginners Guide to Codecaves

Reversing with immunity debugger

Revised 3-3-18
Immunity download link updated 10-6-18