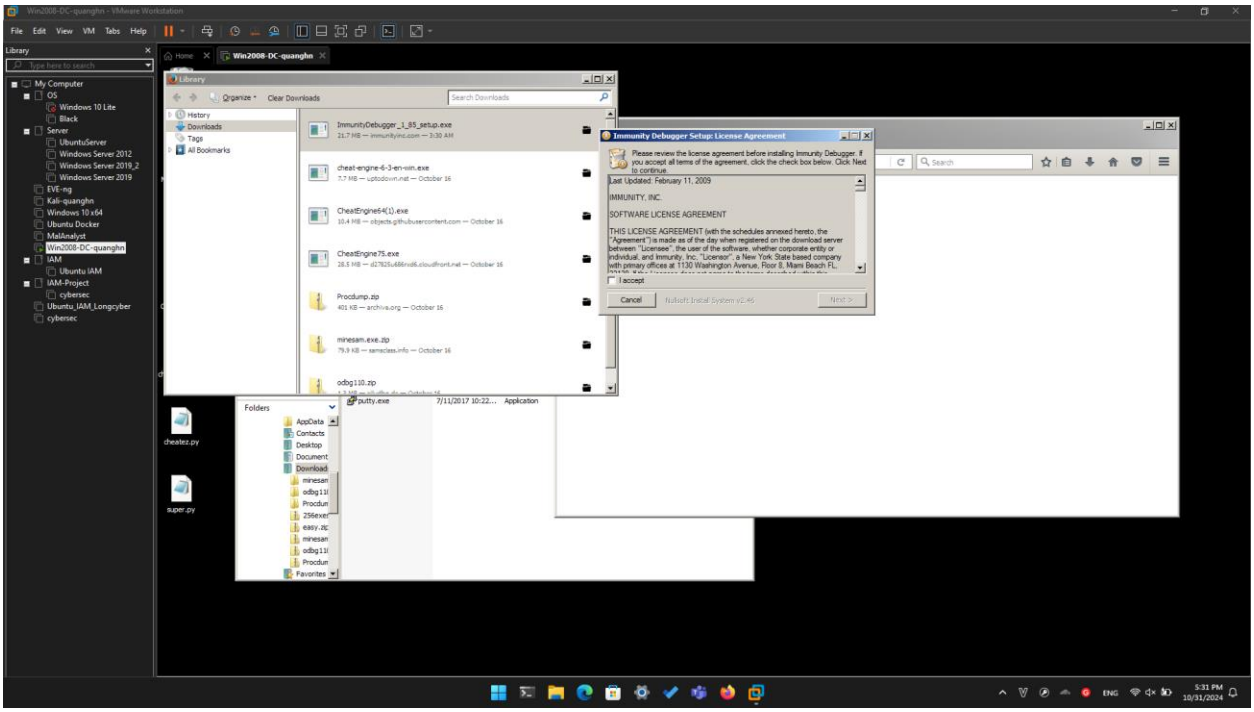
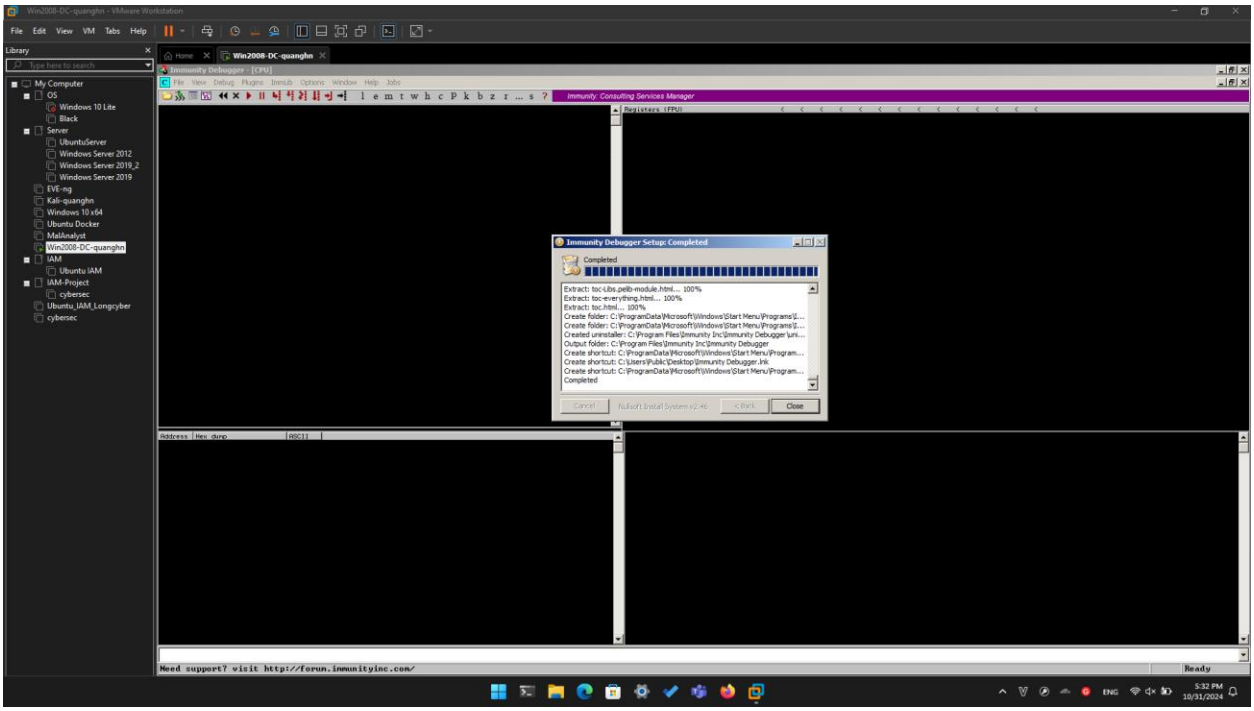
Lab 9: Simple EXE Hacking with Immunity

Huynh Ngoc Quang – SE181838

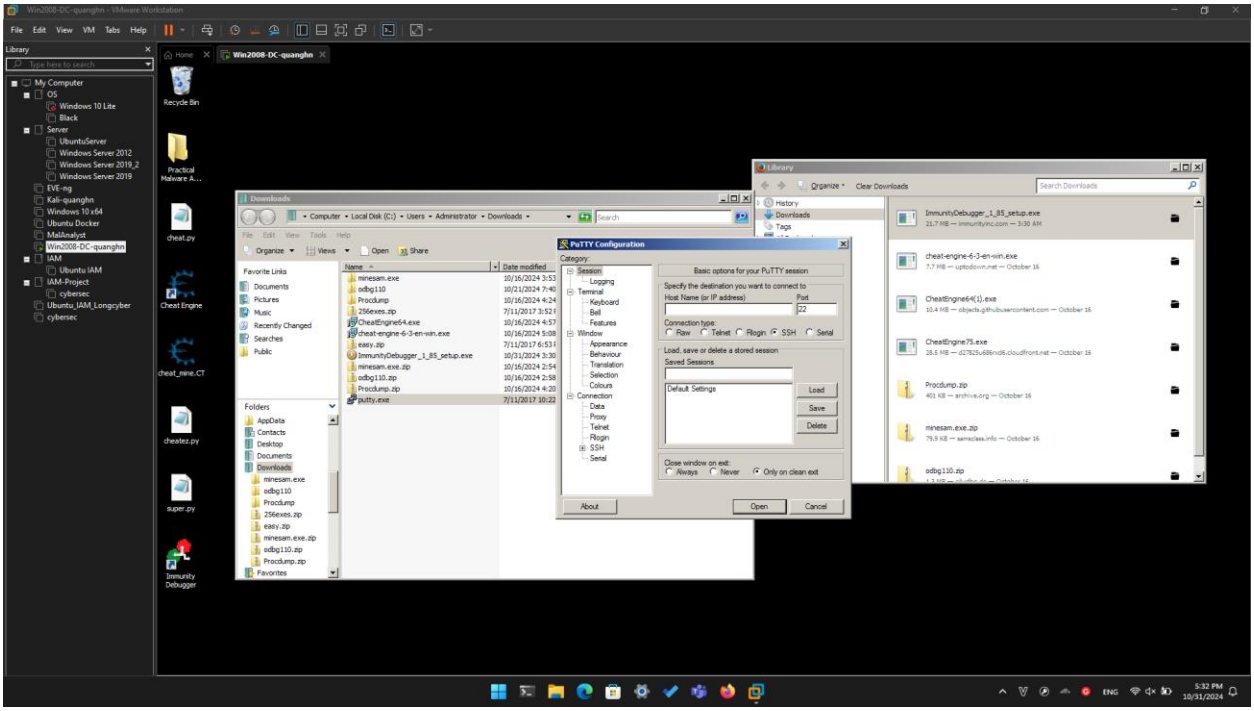
Task 1: Target EXE Recon

Get Immunity

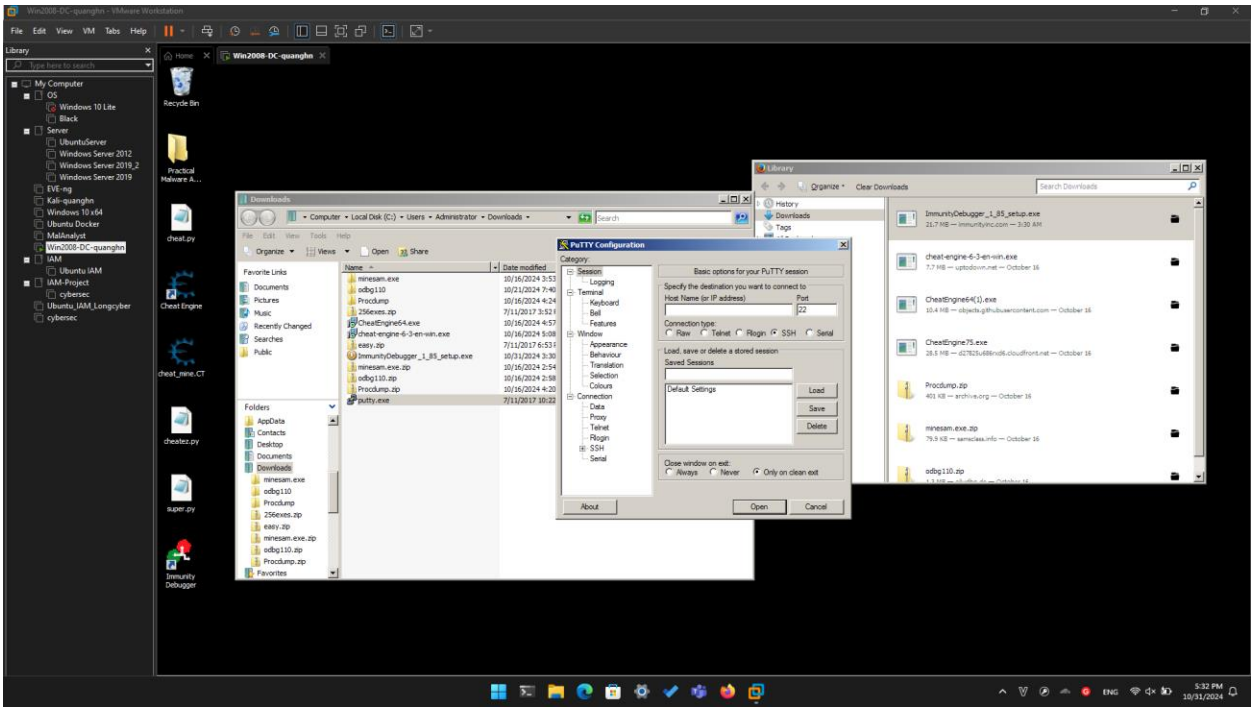


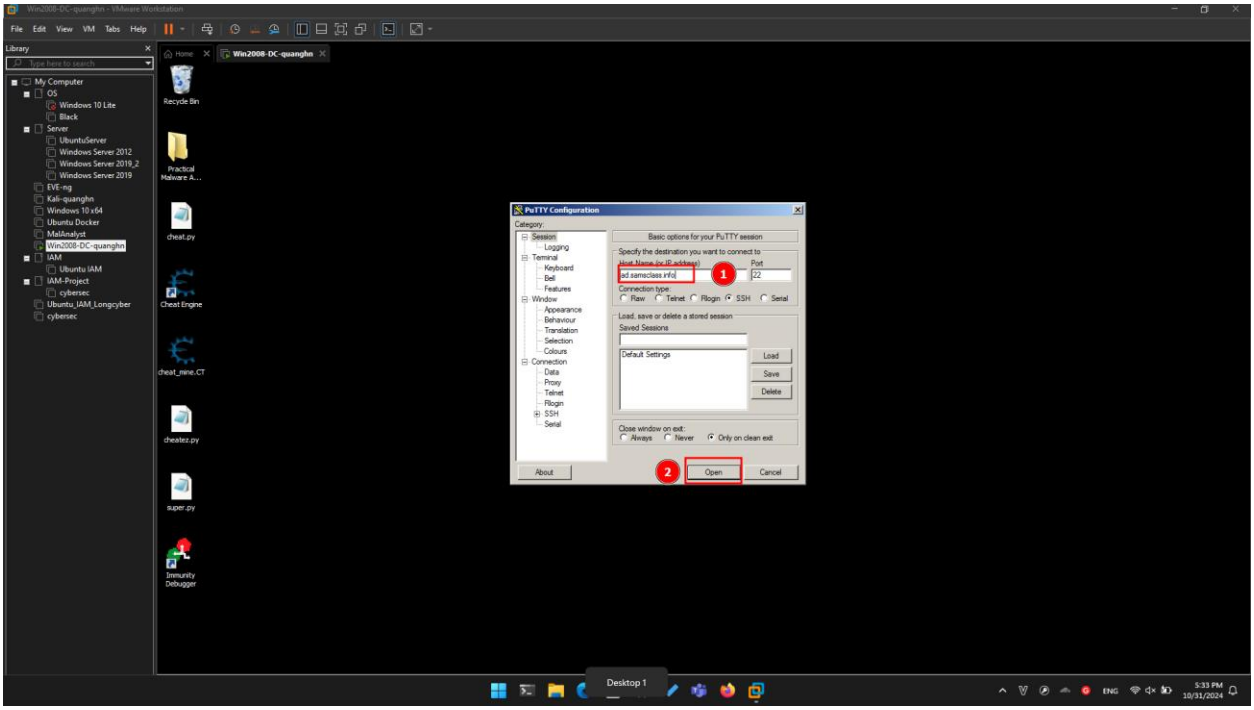


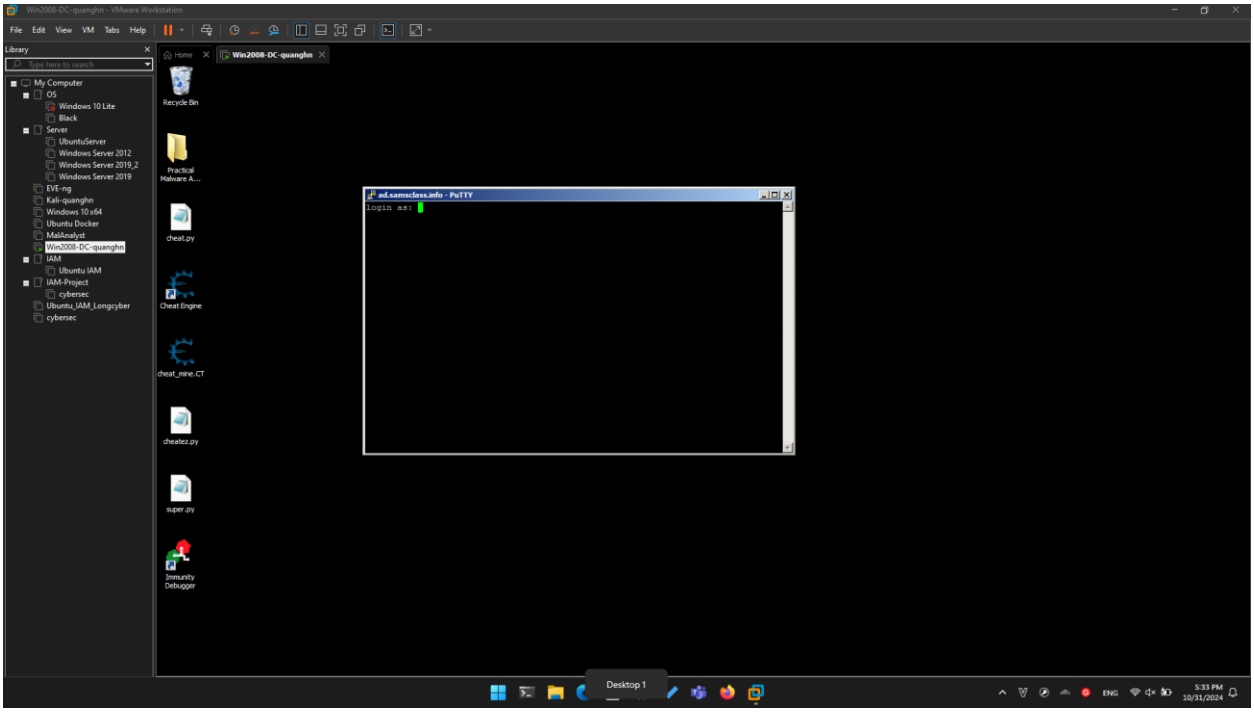
Get putty.exe



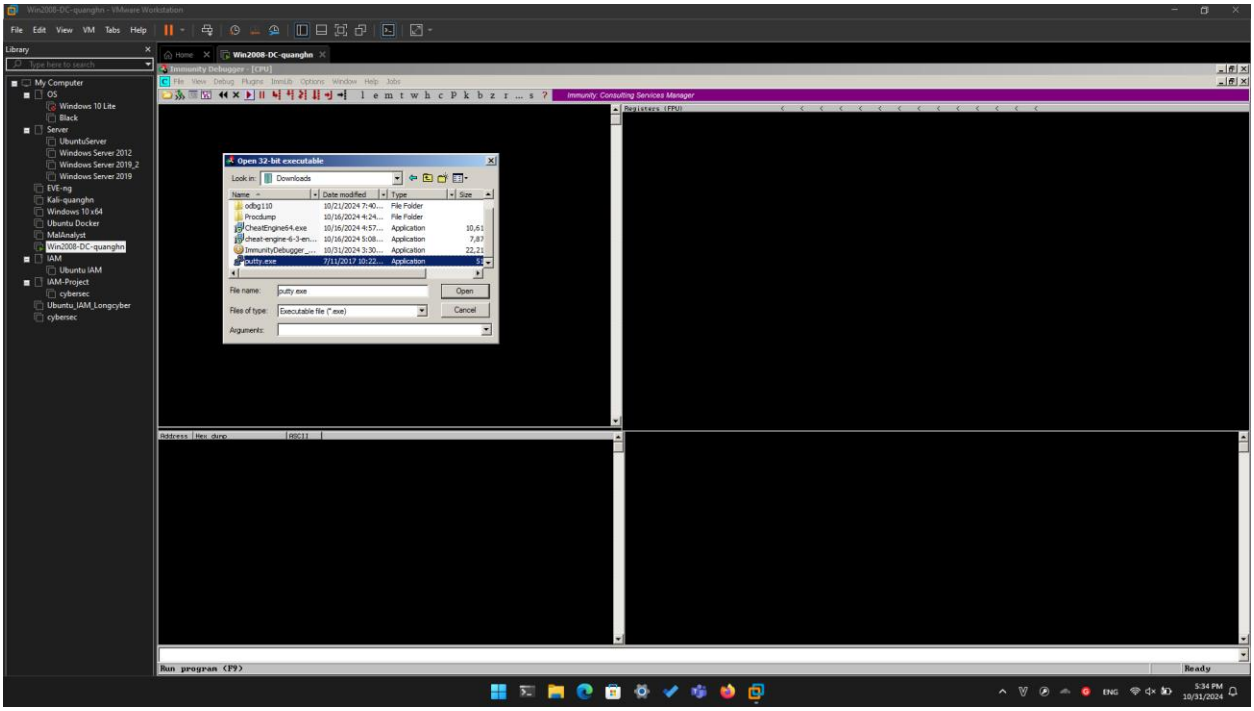
Running Putty

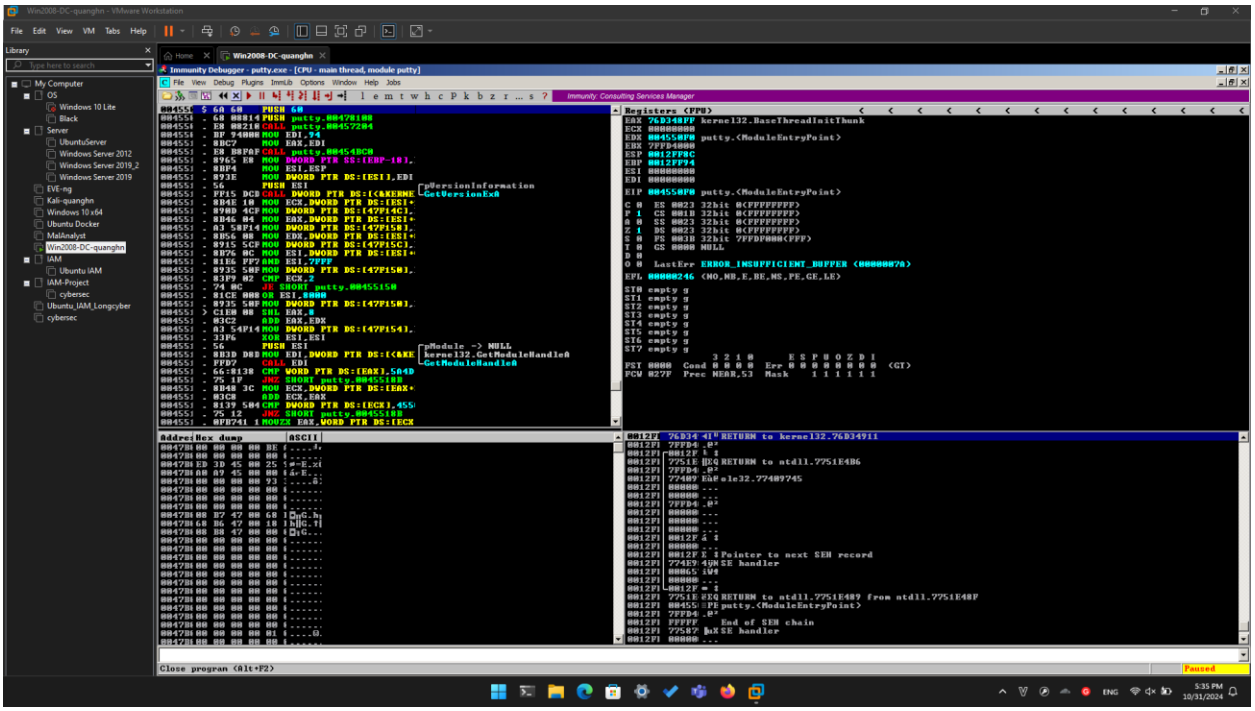

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

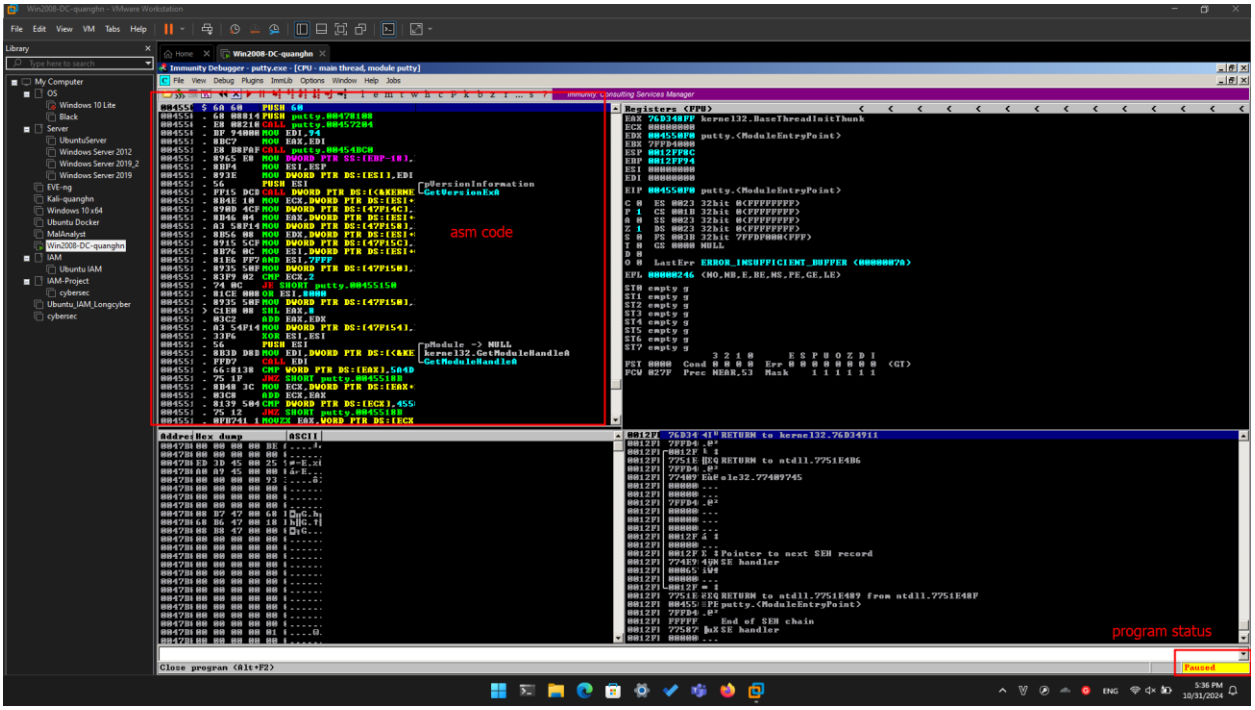

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
ad.samsclass.info
1
Port
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
2
Open
Cancel



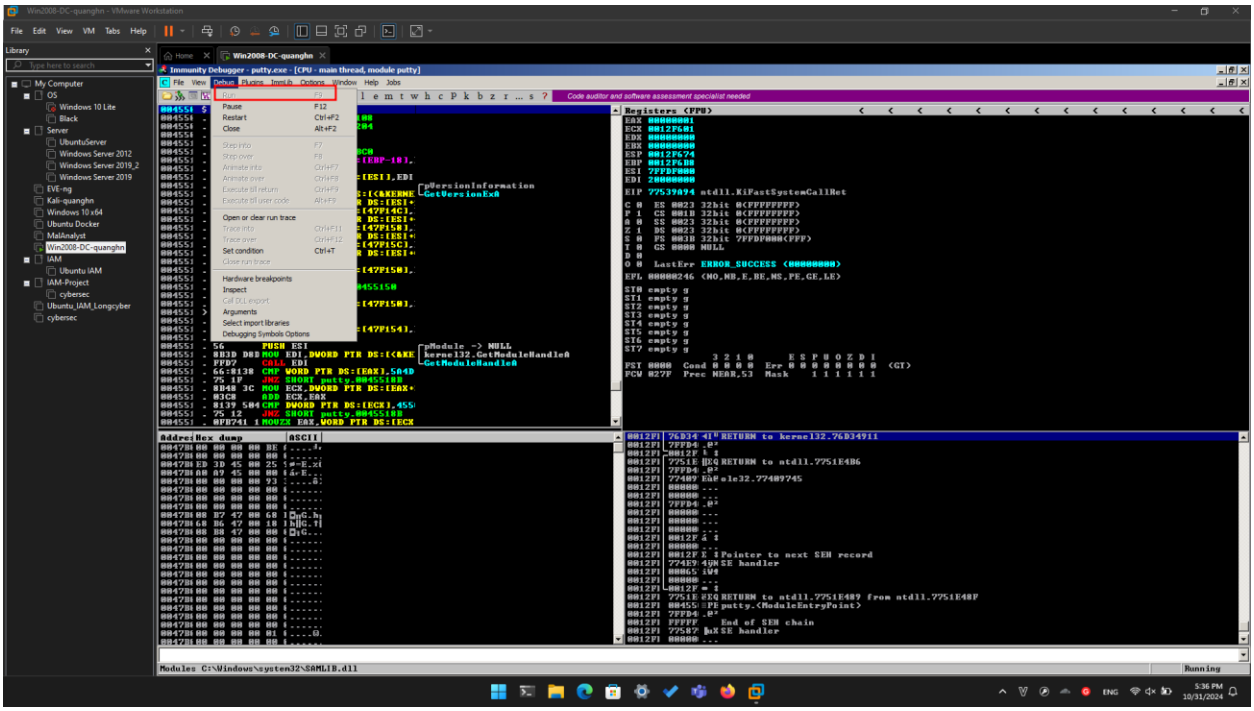
Starting the Immunity Debugger

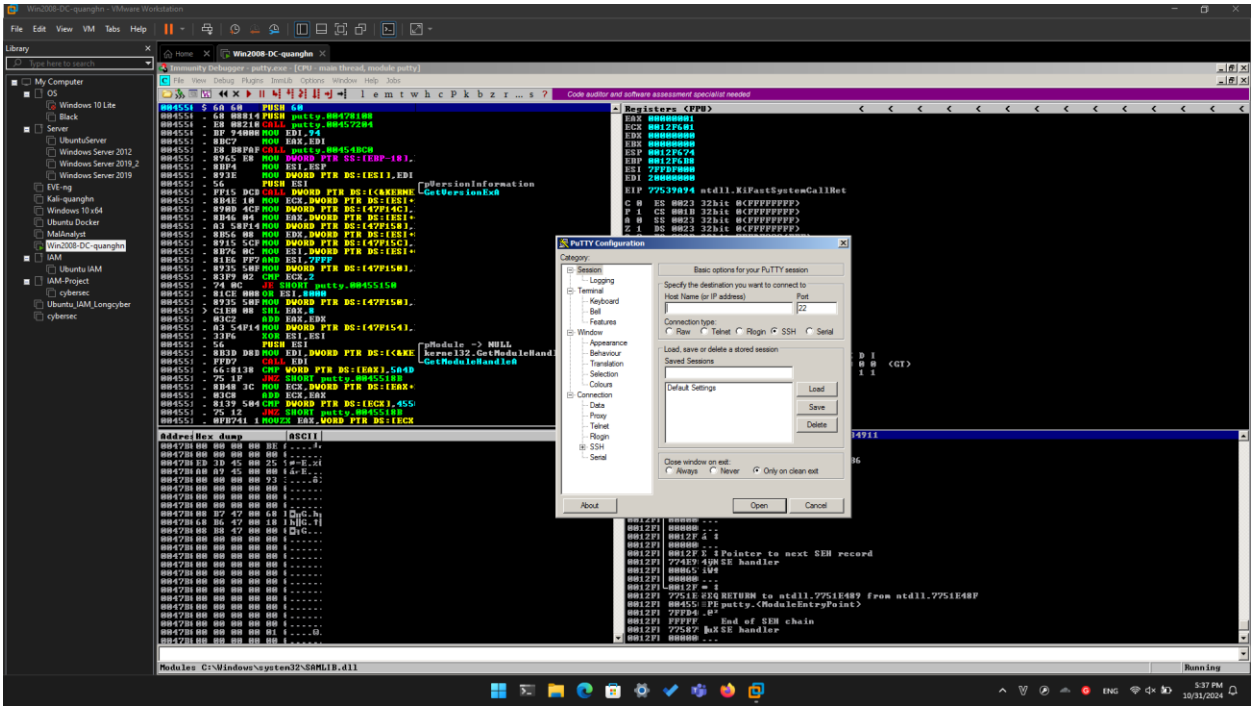


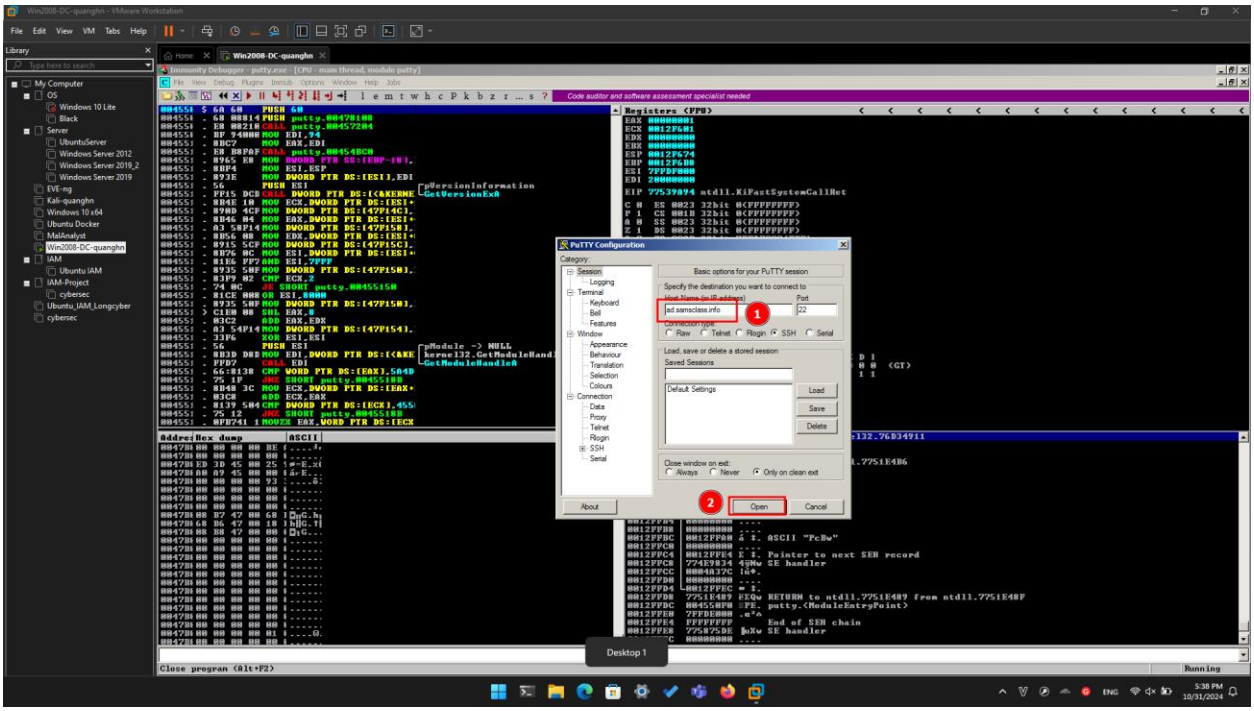


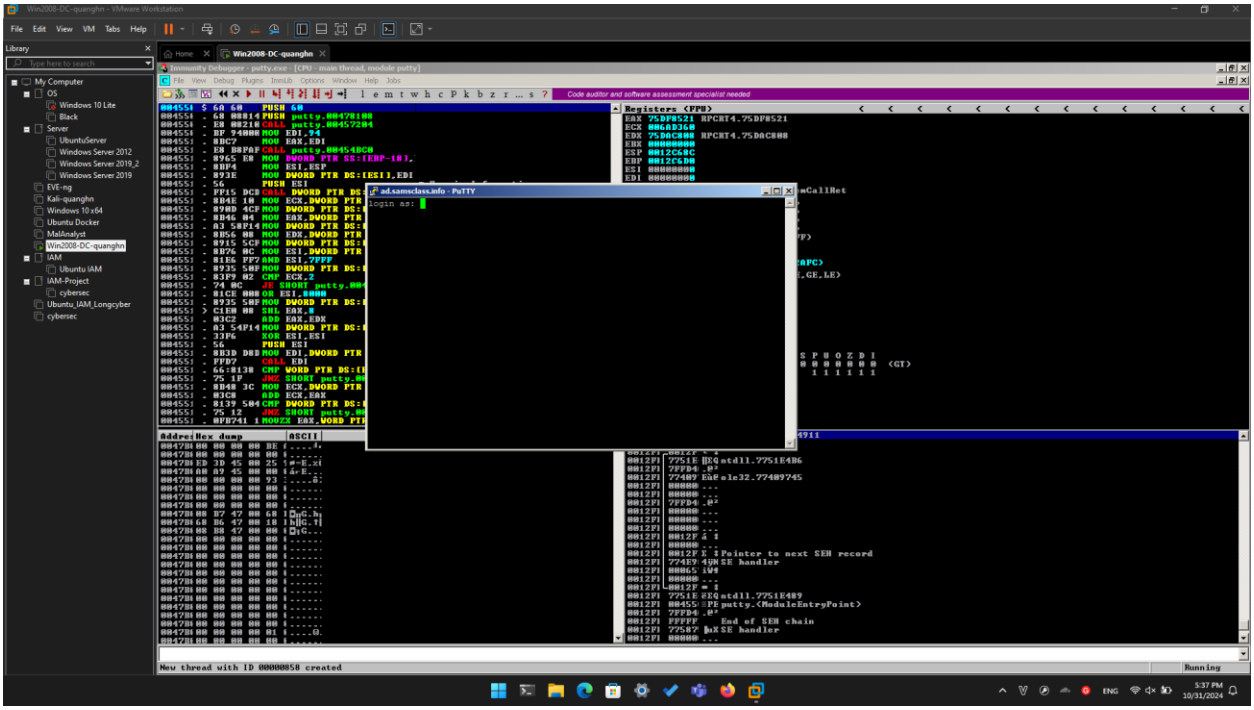


Running Putty in Immunity

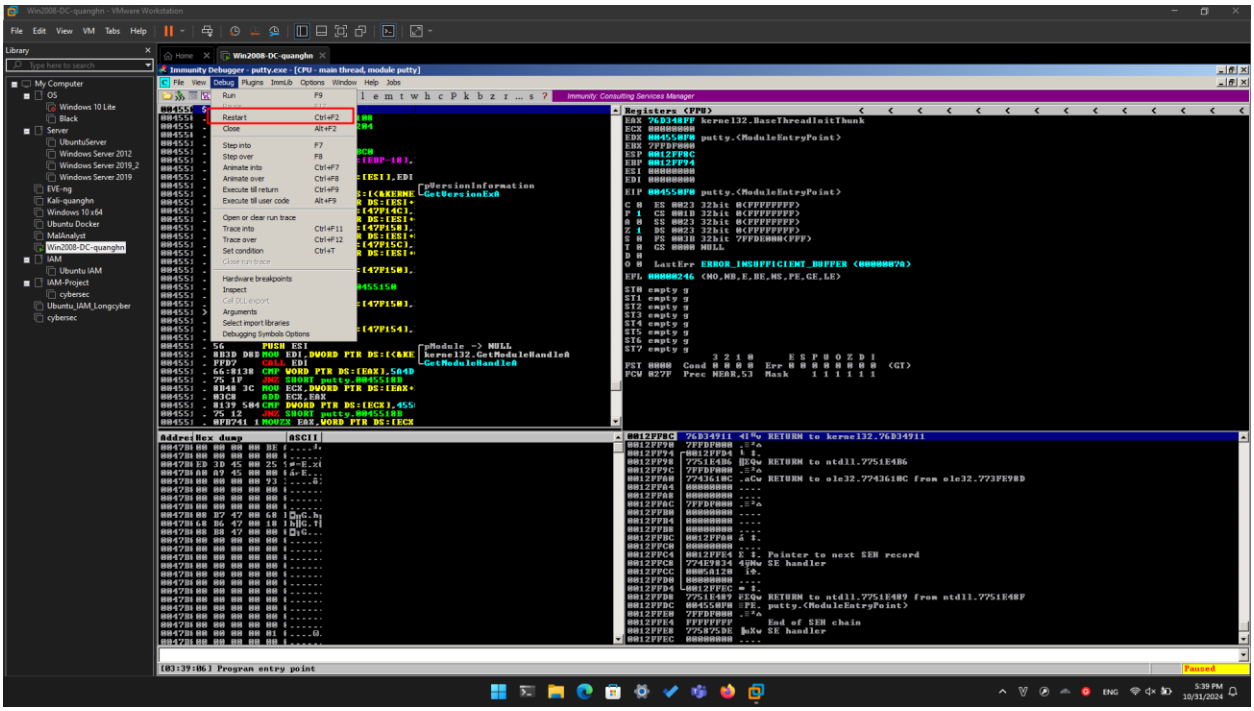


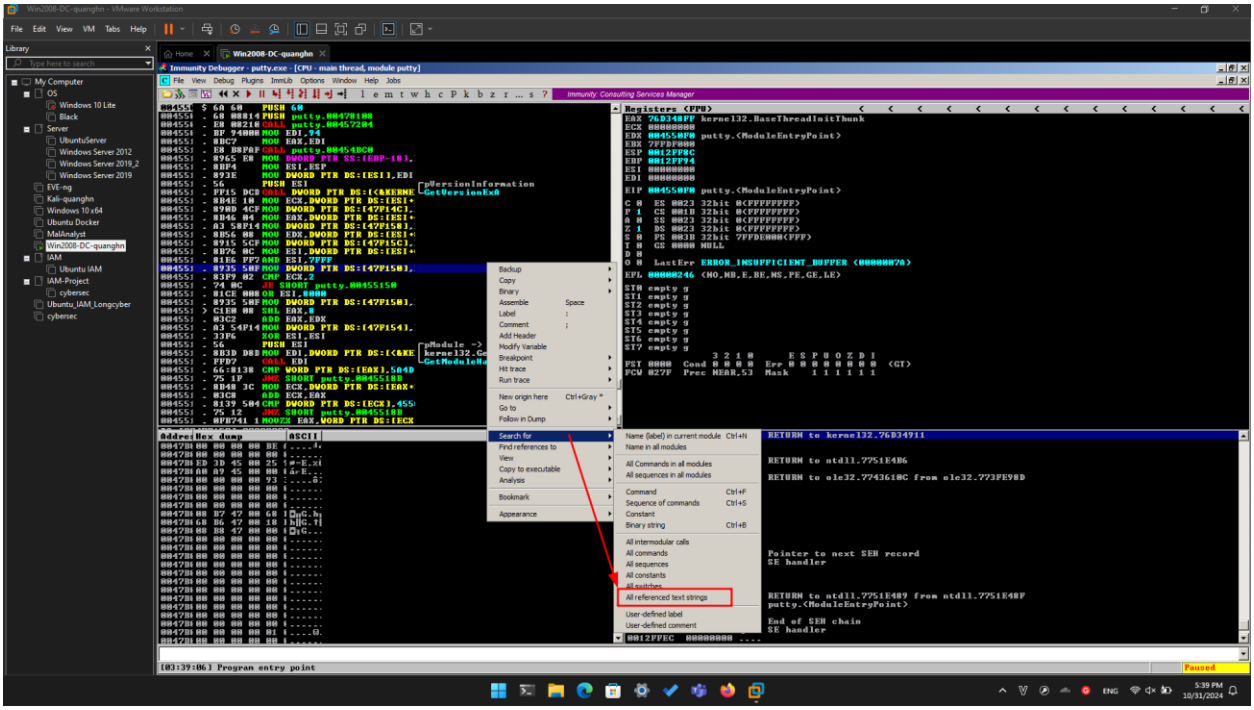


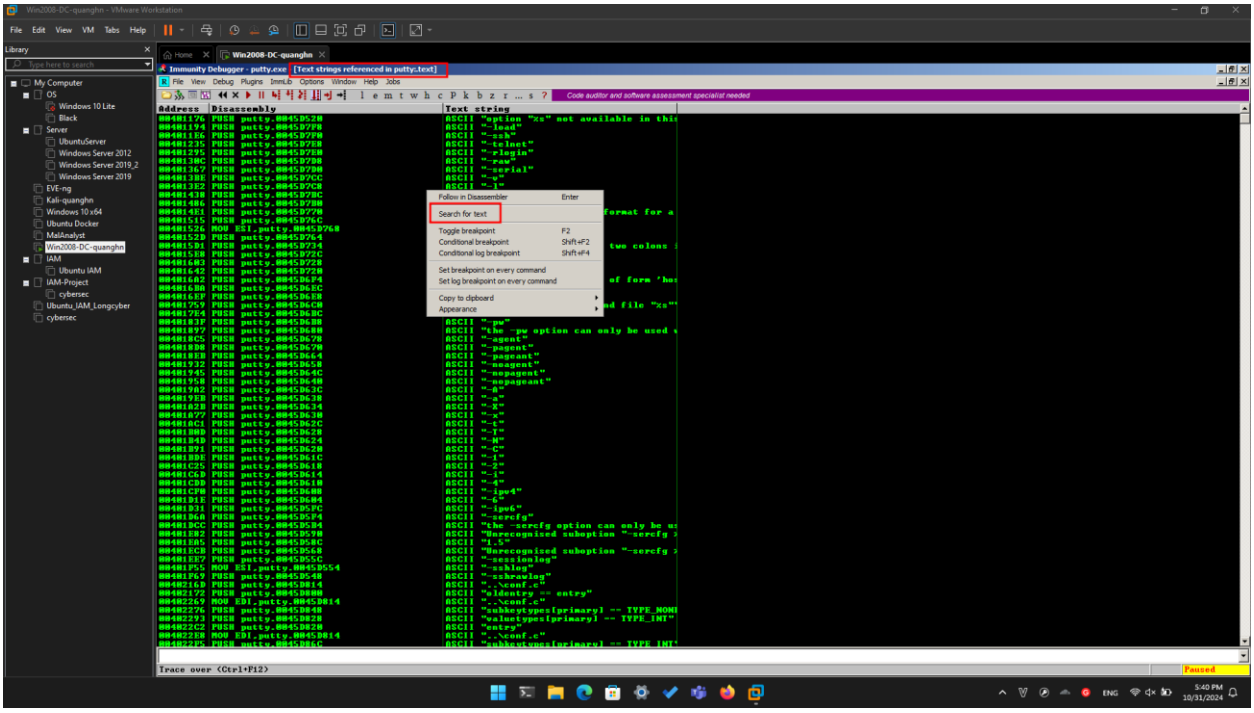


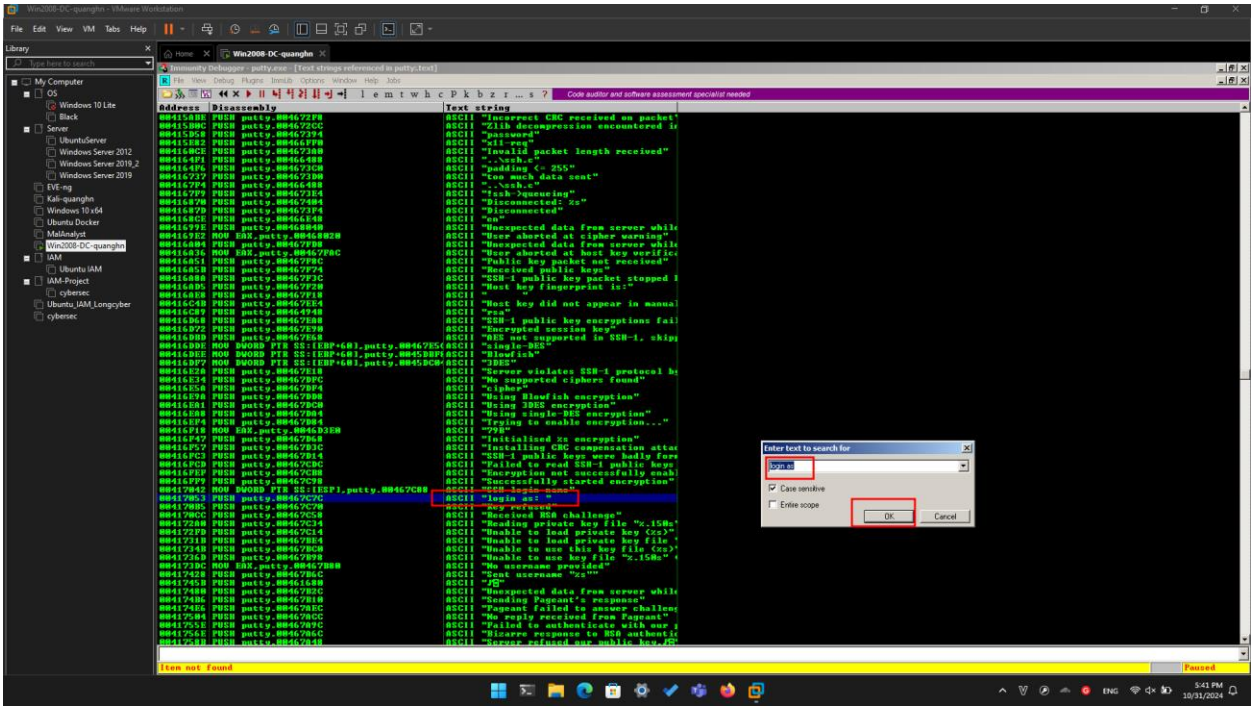


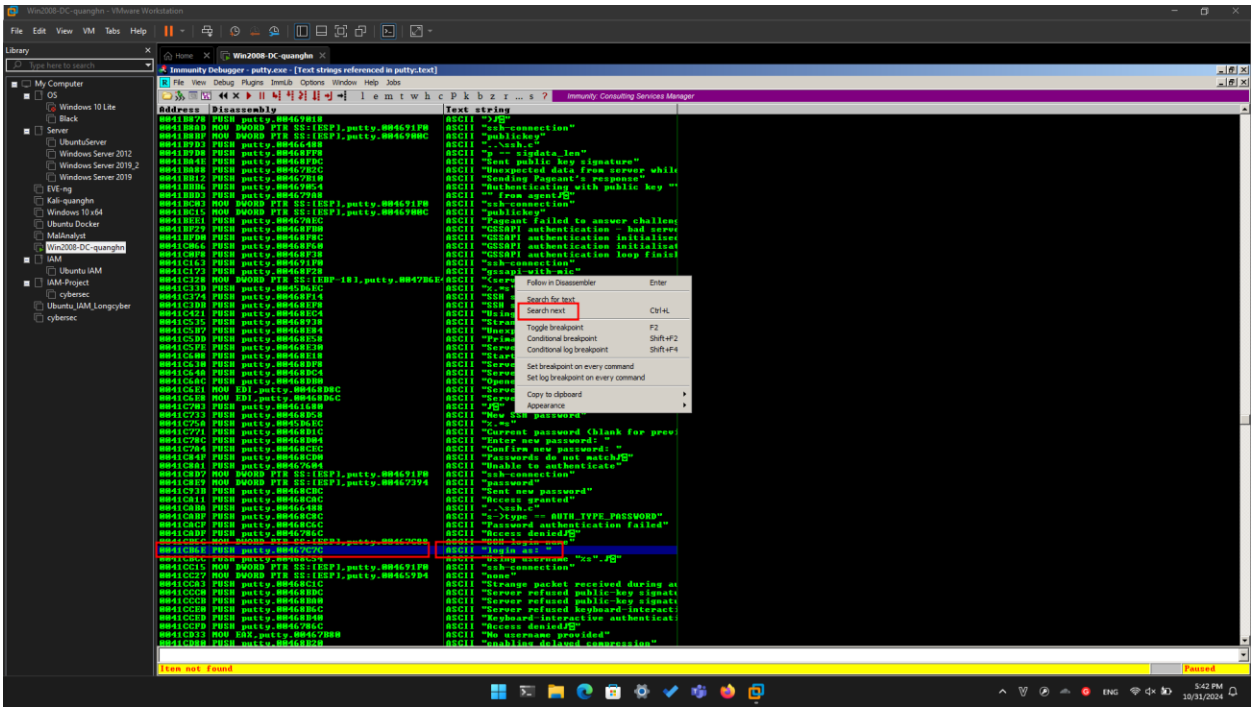
Finding the "login as" Code



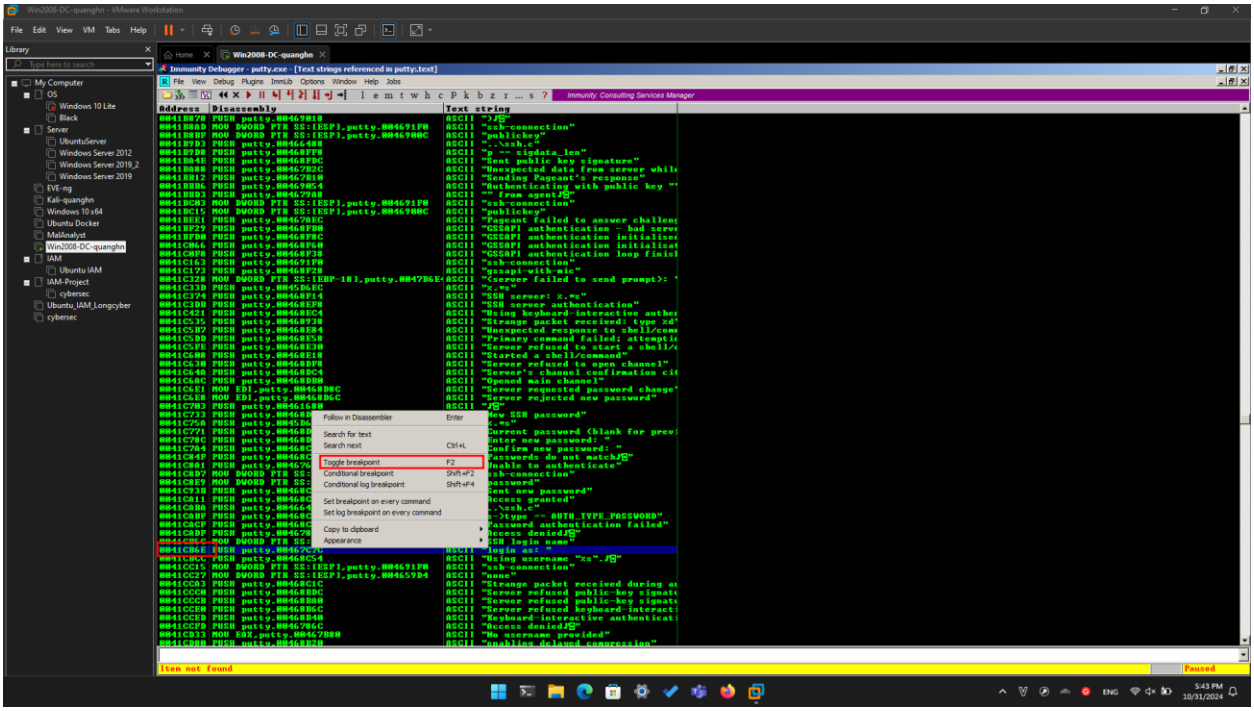


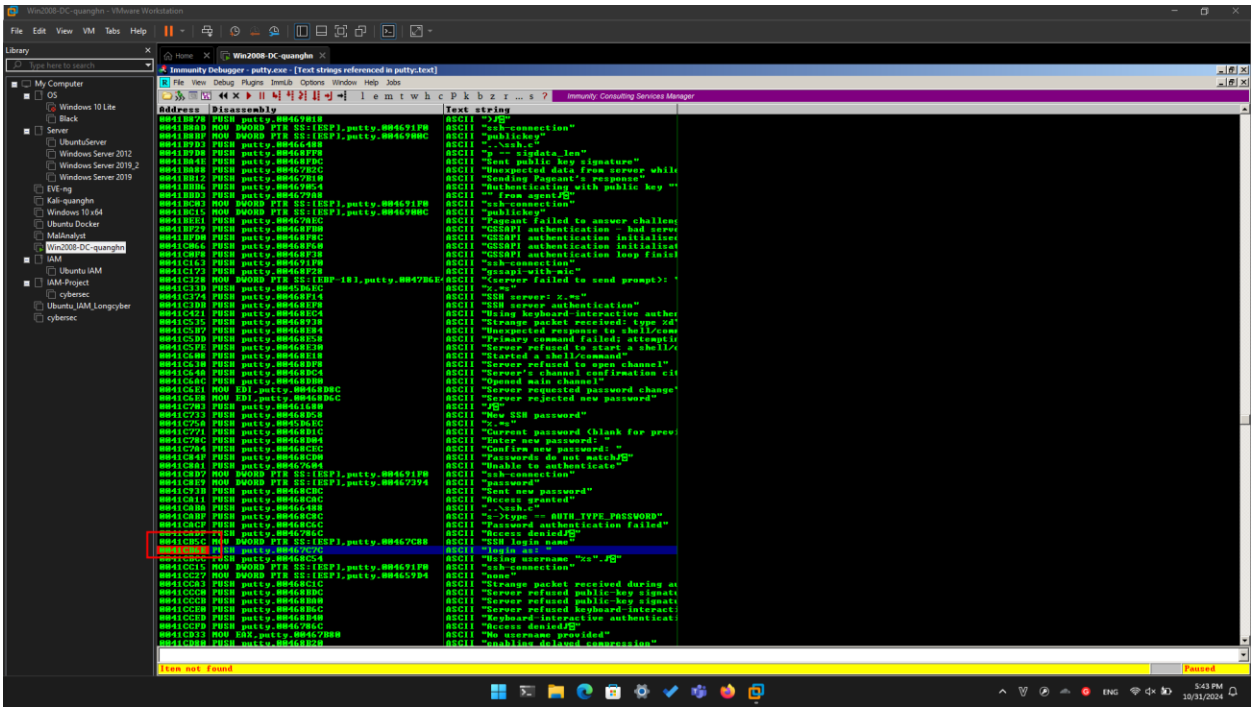

Win2008-DC-quanghn - VMware Workstation
Immunity Debugger - putty.exe [Text strings referenced in putty.text]
Search for text
Trace over (Ctrl+F12)
Paused


Win2008-DC-quanghn - VMware Workstation
Enter text to search for
login as:
Case sensitive
Entire scope
OK
Cancel
Item not found
Paused



Using Breakpoints



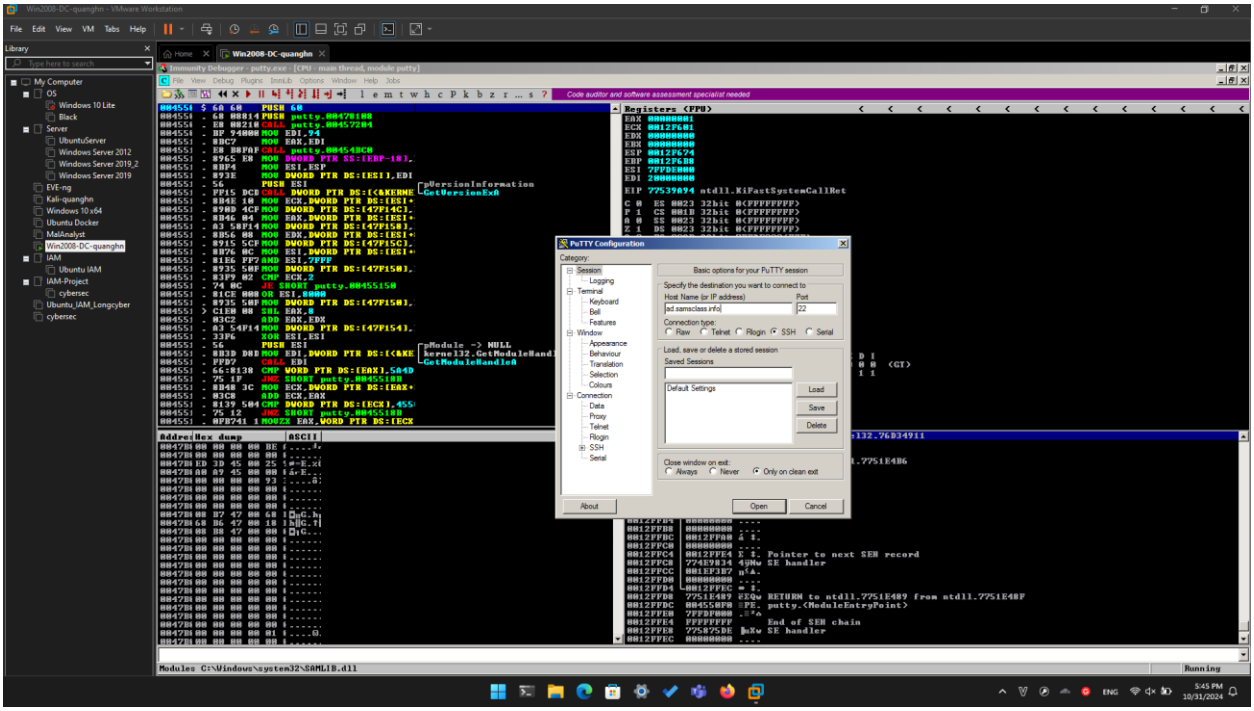


In Immunity, from the menu bar, click **Debug**, **Restart**.

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.

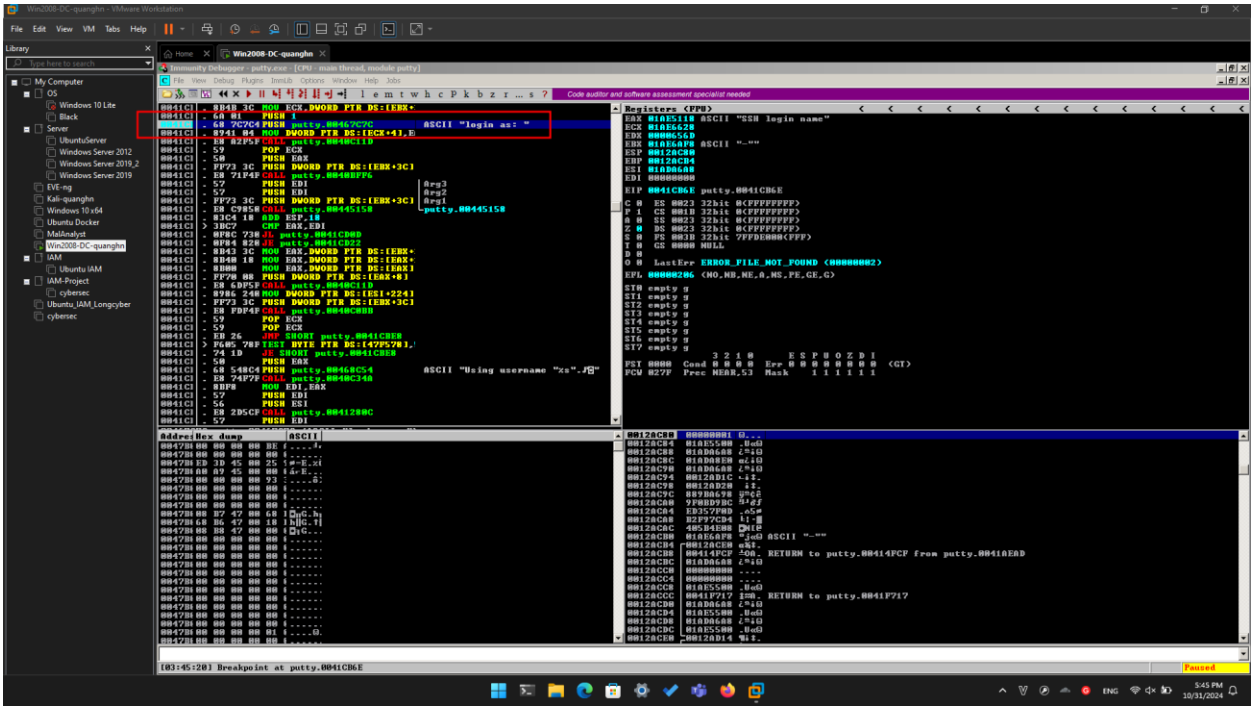


Click in the Putty window. In the "Host Name (or IP address)" box, type

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.

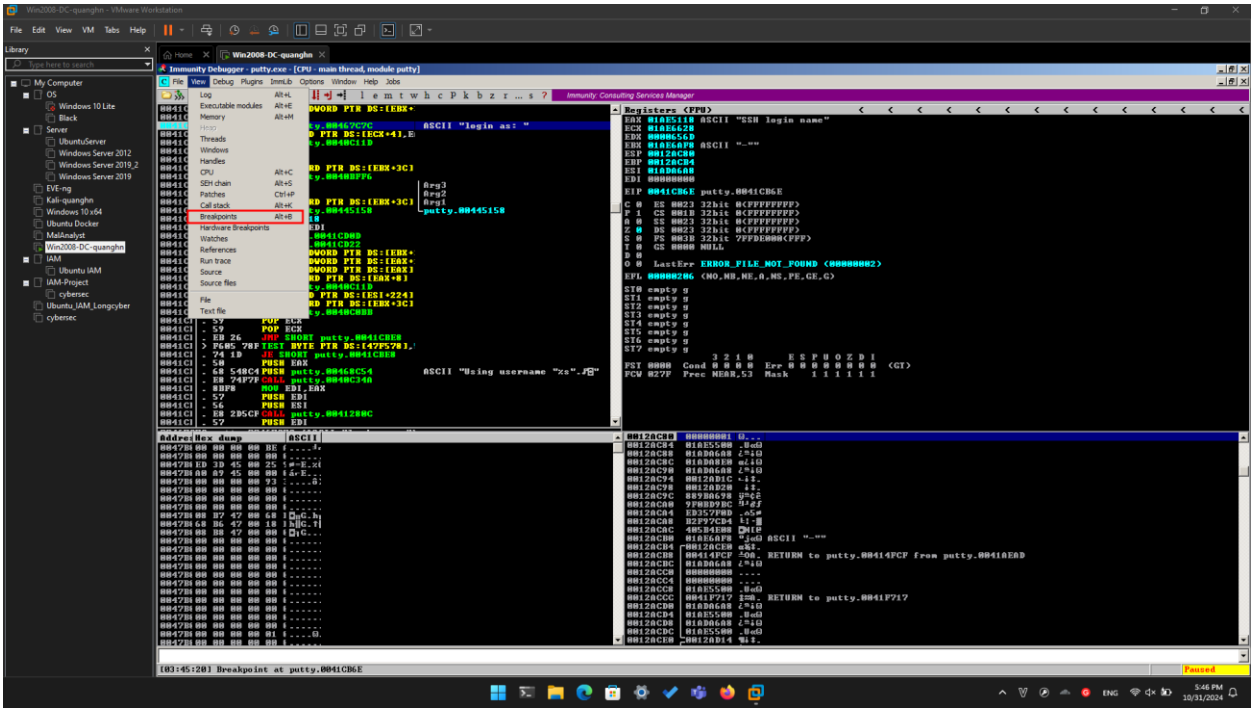


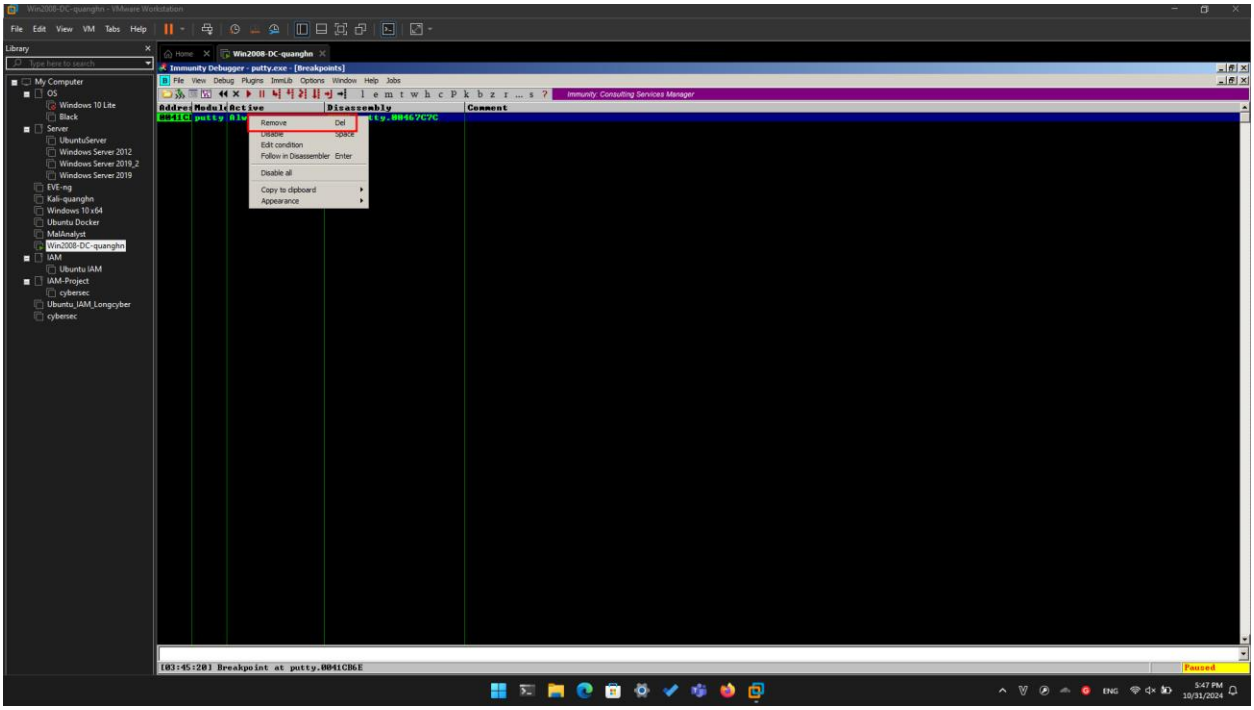
The program stopped at instruction 0041CB6E, as shown in the image above.

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

Task 2: Alter the Login Message

Removing the Breakpoint

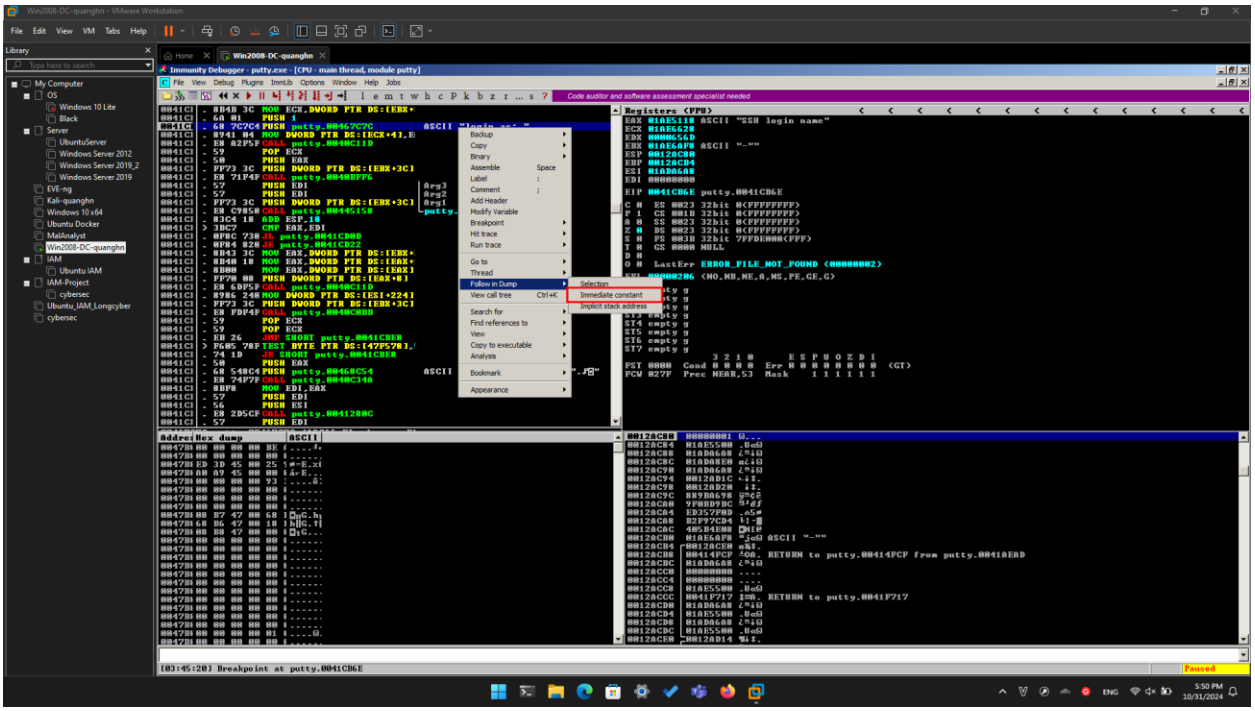


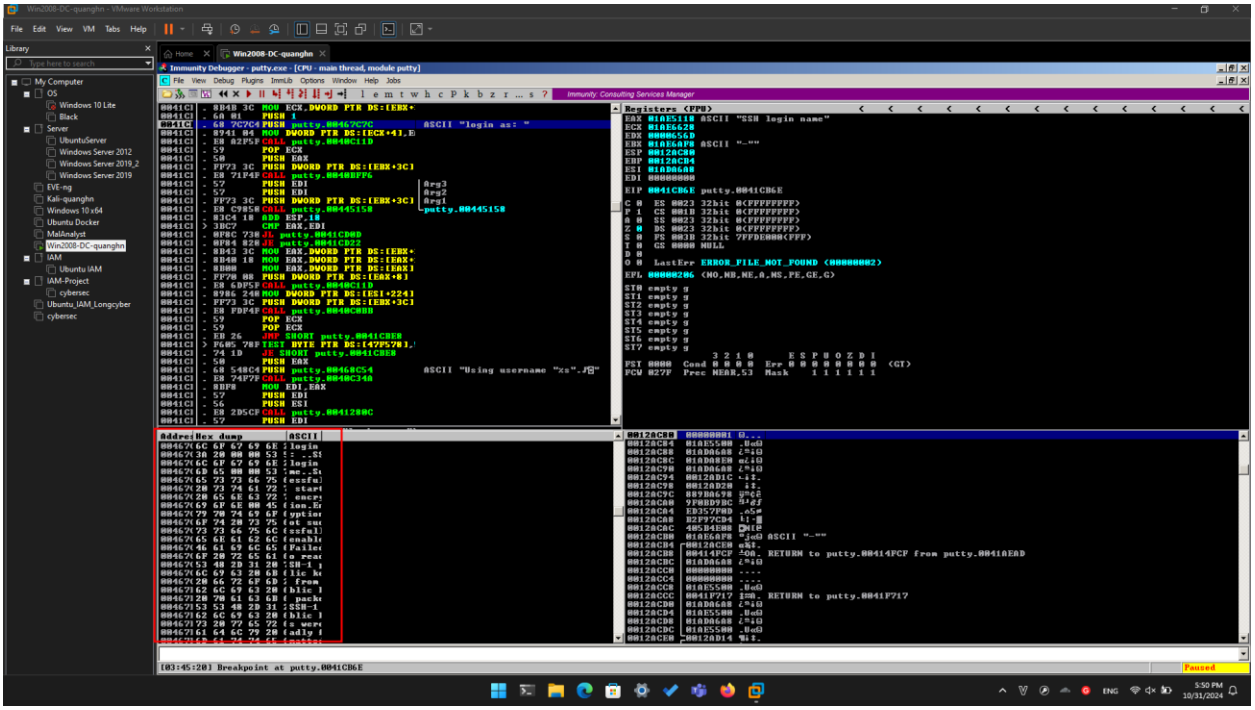


Viewing the Stored Message

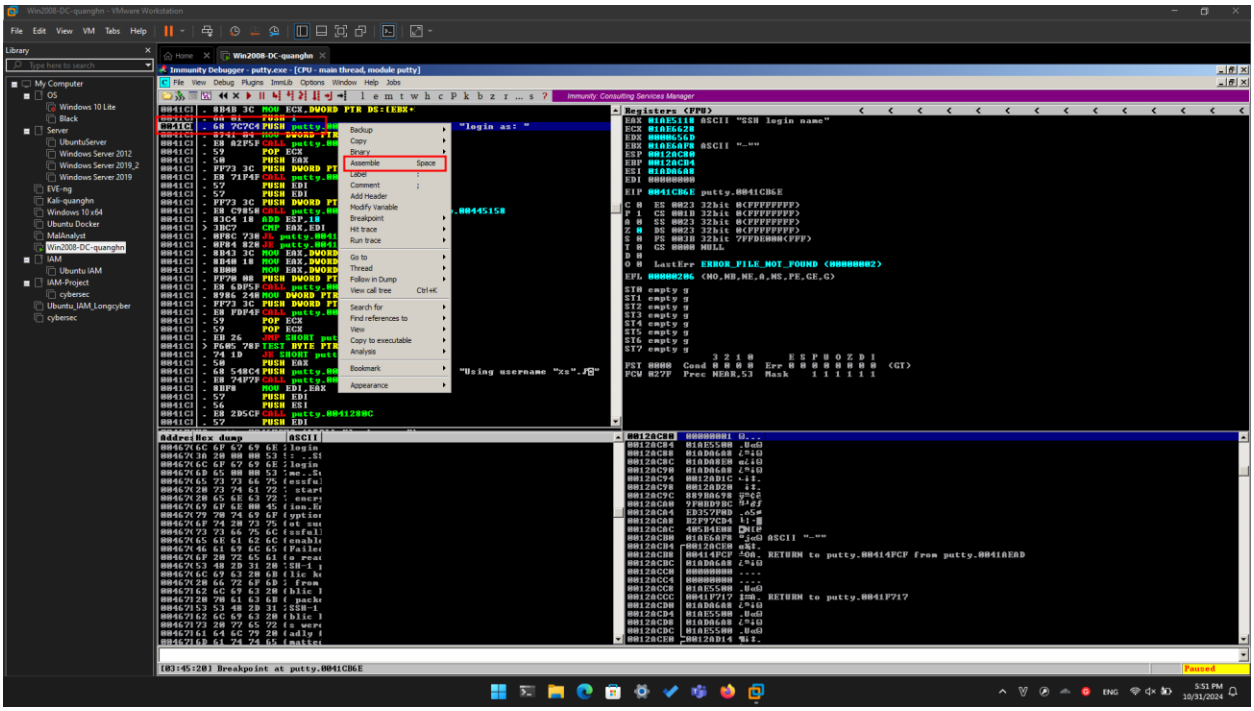
In Immunity, in the CPU window, in the Assembly Code pane, right-click the intruction at address **0041CB6E** and click "**Follow in Dump**", "**Immediate constant**", as shown below.

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



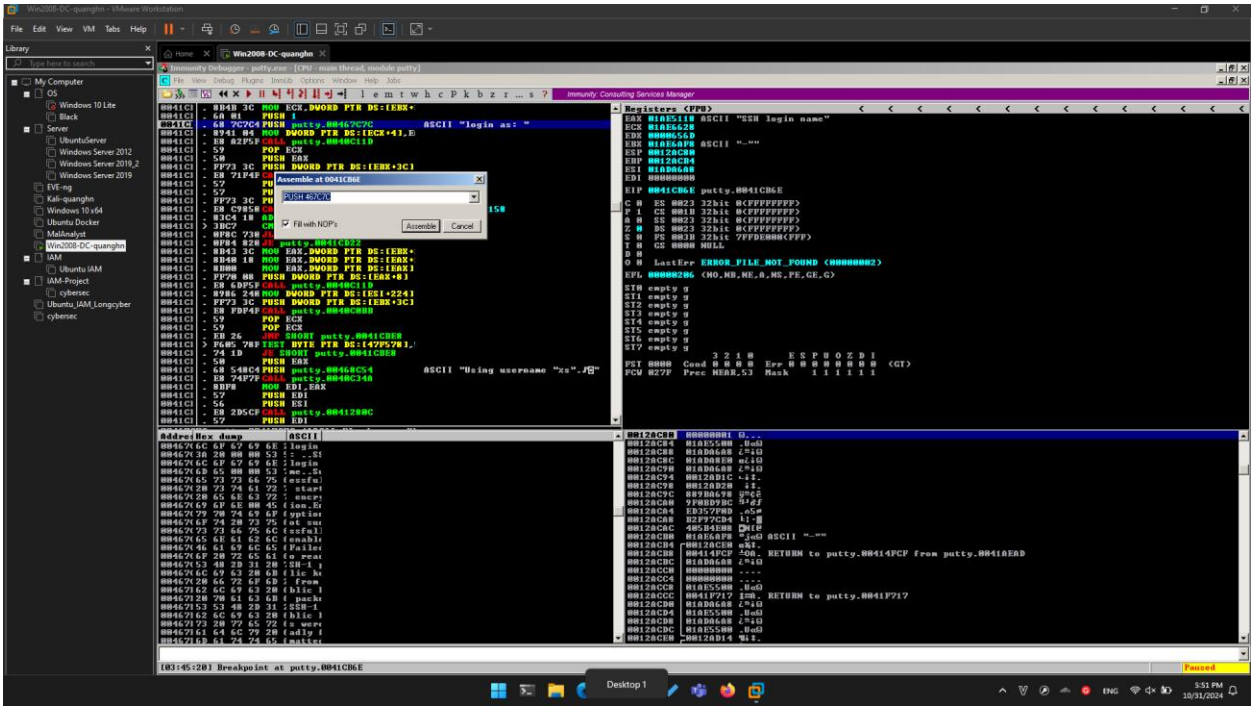


Skipping the First Letter In the Message

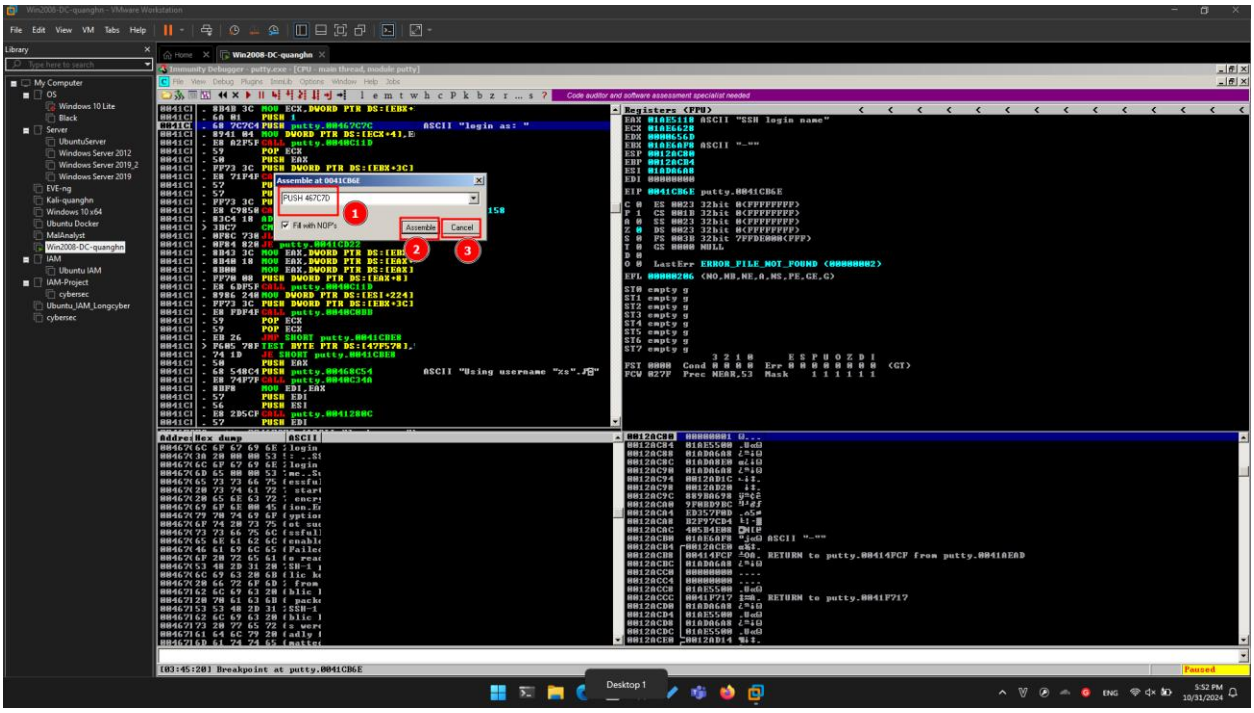


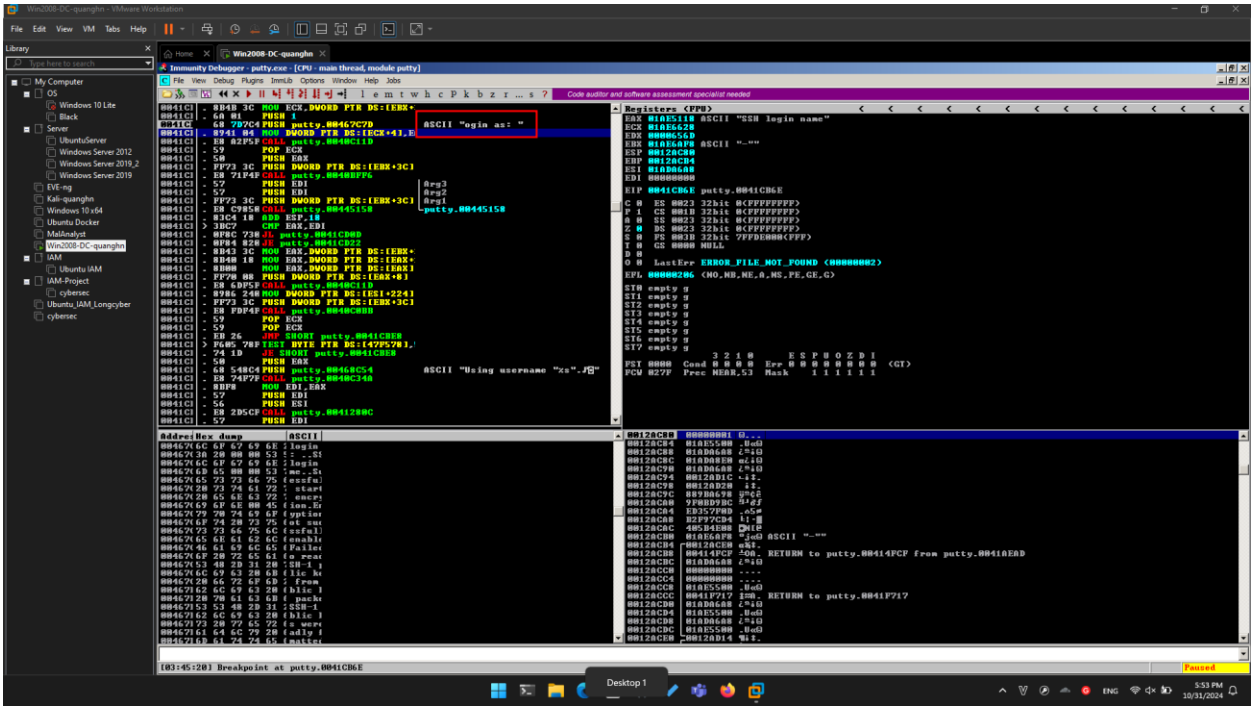
An "Assemble at 0041CB6E" box appears, as shown below.

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.

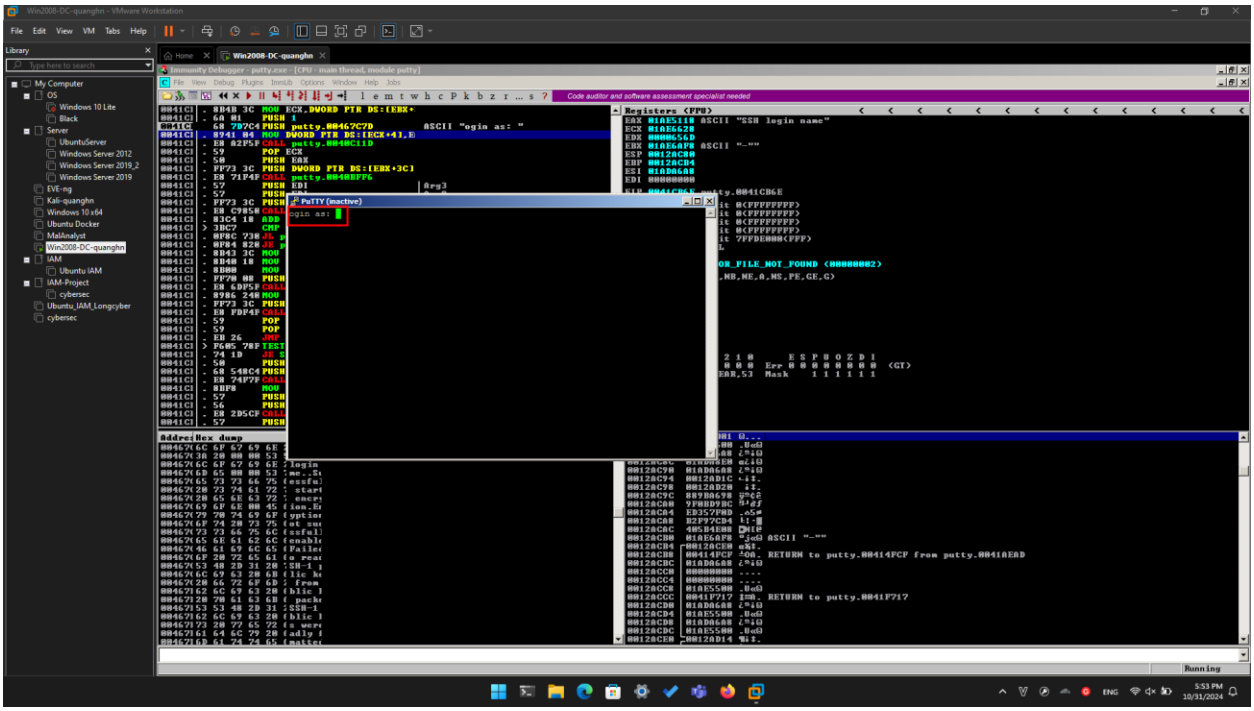


In the "Assemble at 0041CB6E" box, change the last character to **D**, as shown below. This will move the pointer from the "l" to the "o" in the string "login as: ".





Running the Modified Program

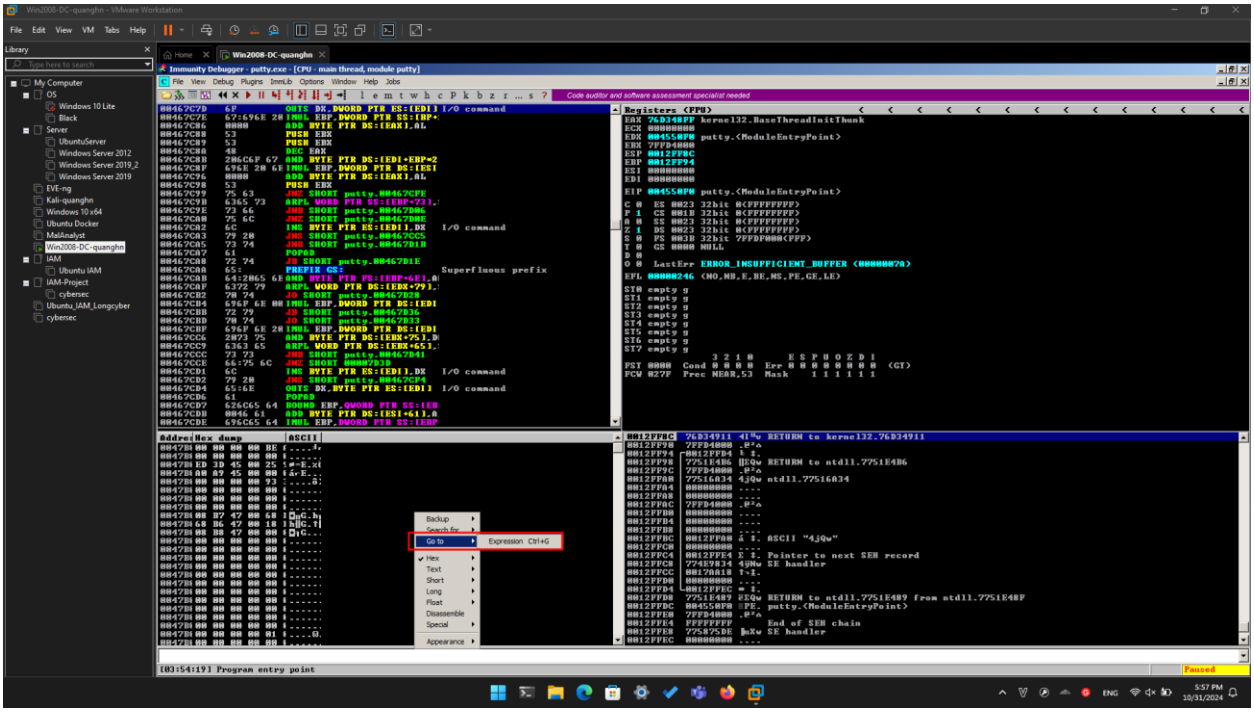


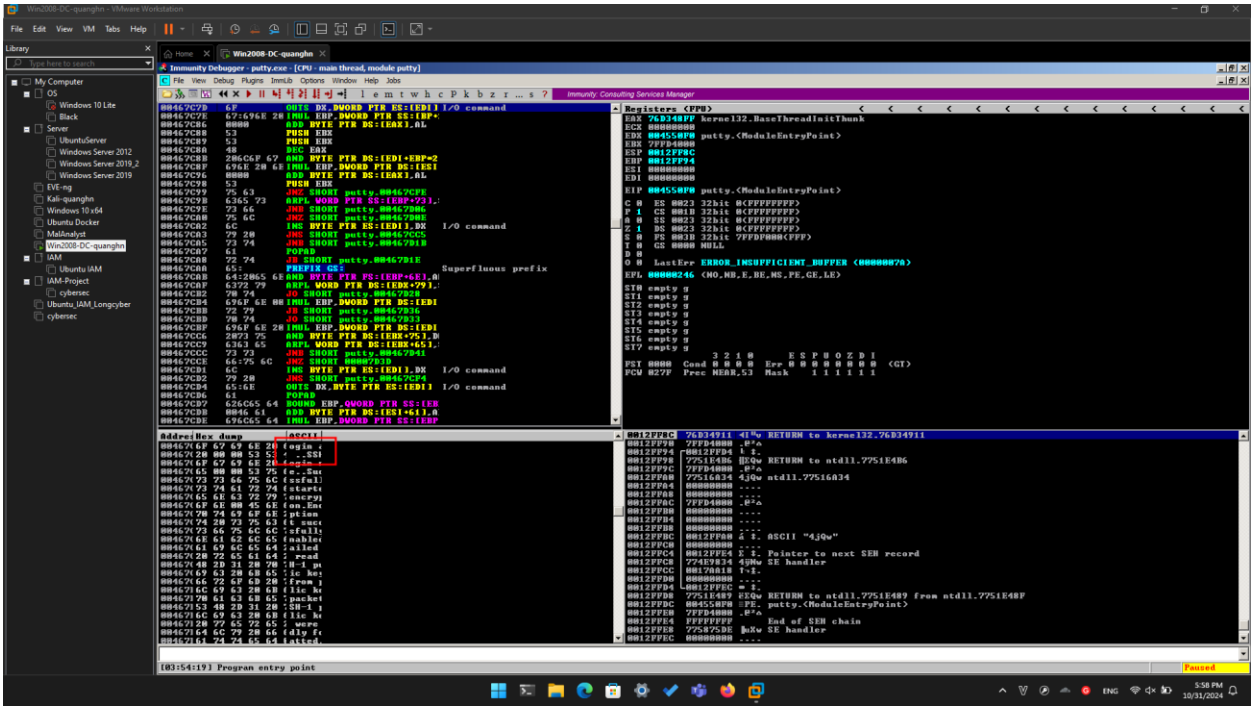
Inserting Your Name

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

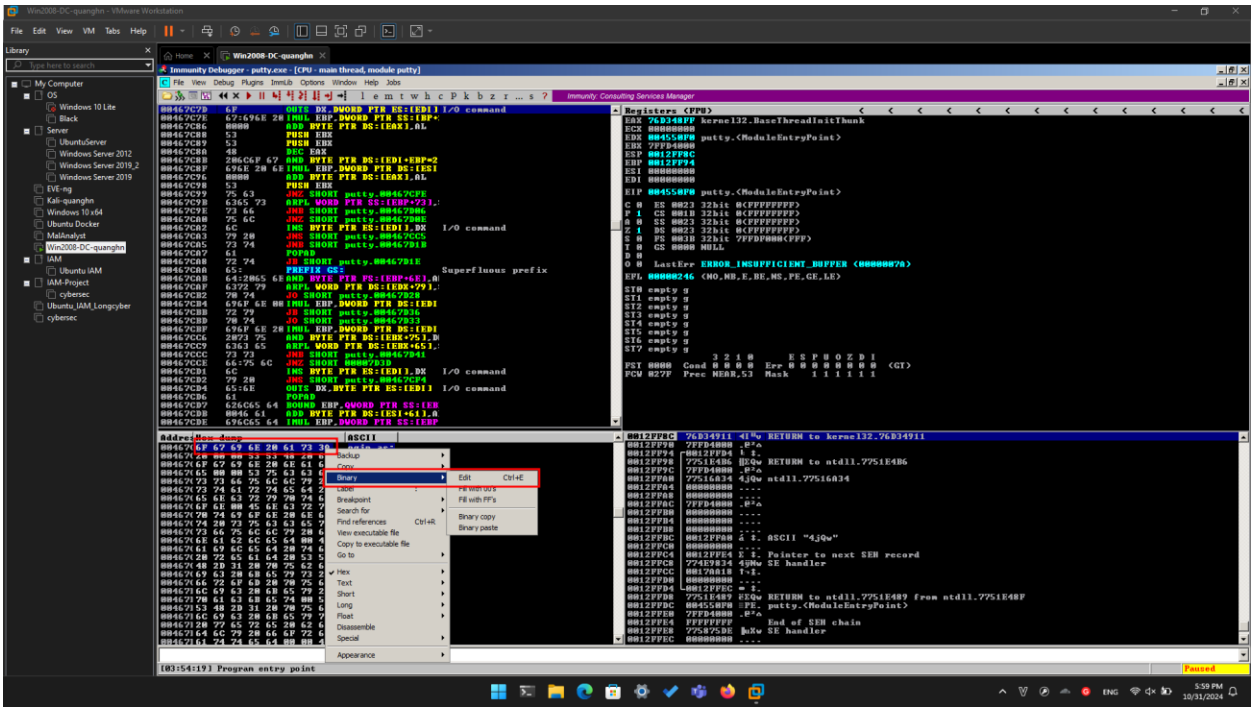
Move your mouse into the lower left pane of the CPU window, which is the "hex dump" pane.

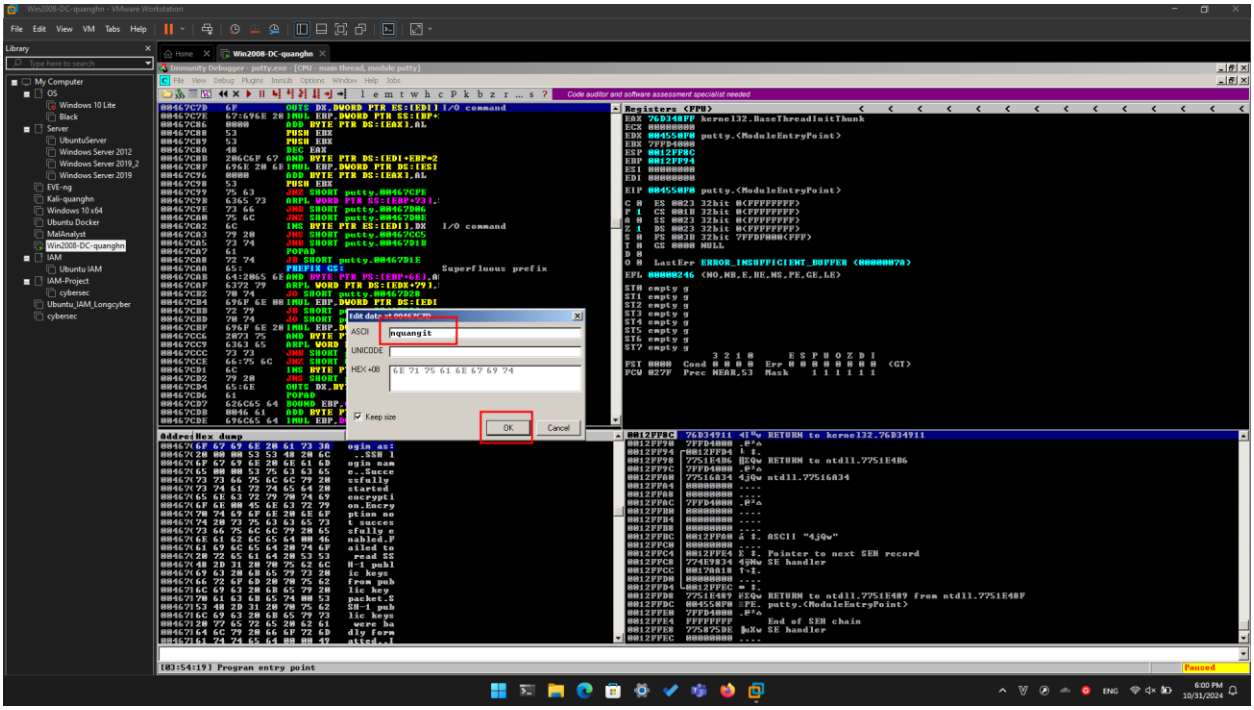
Right click, point to "**Go to**", and click **Expression**, as shown below.



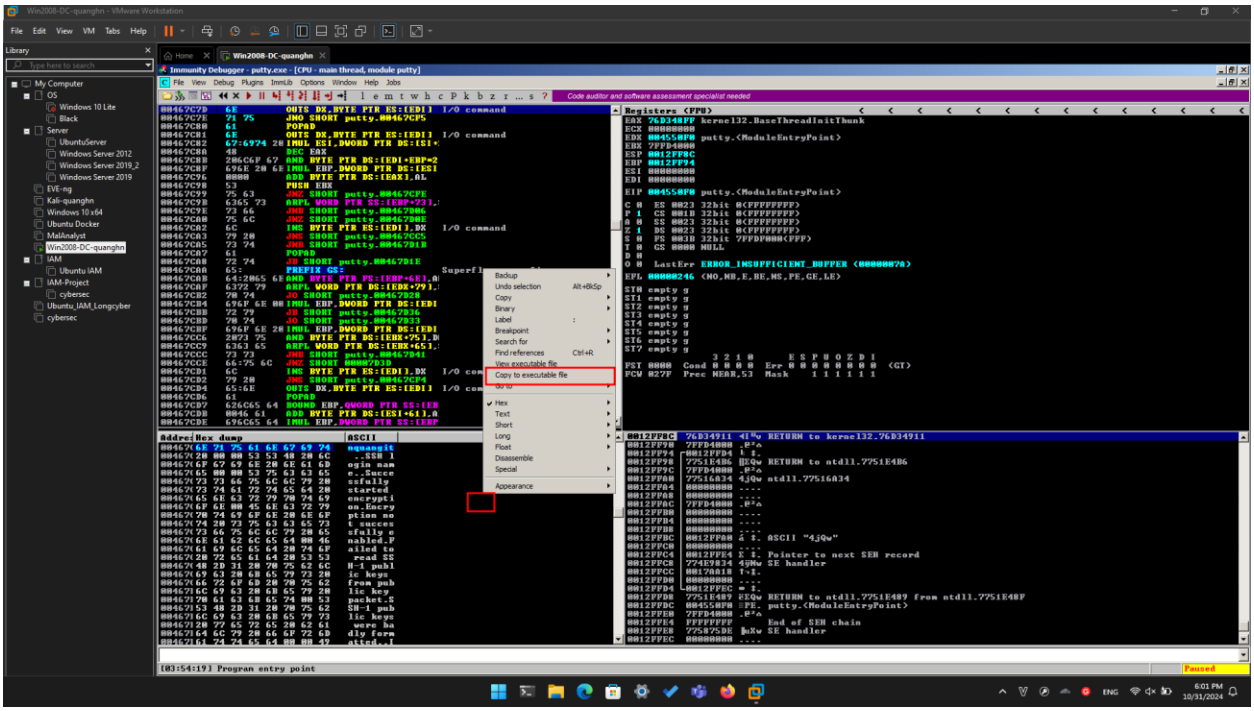


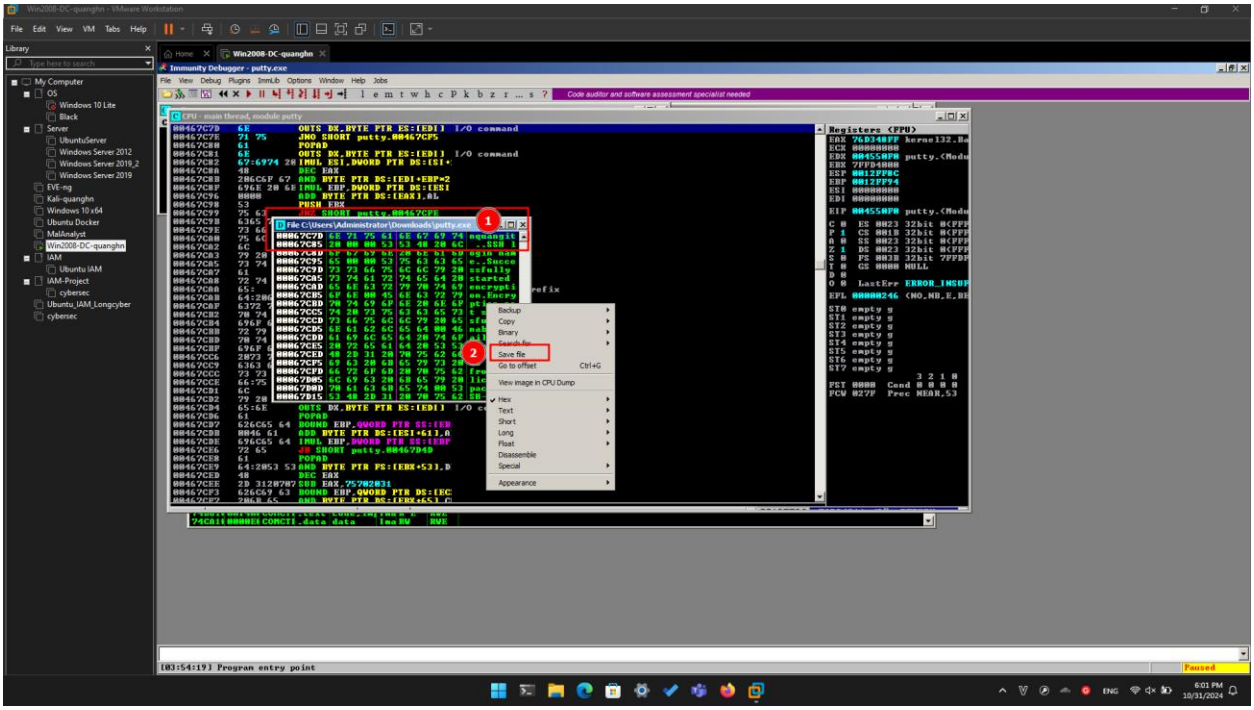
In the top left of the Hex Dump pane, point to **6F**, hold down the left mouse button, and select the entire row of 8 bytes. Then release the left button, point to **Binary**, and click **Edit**, as shown below.

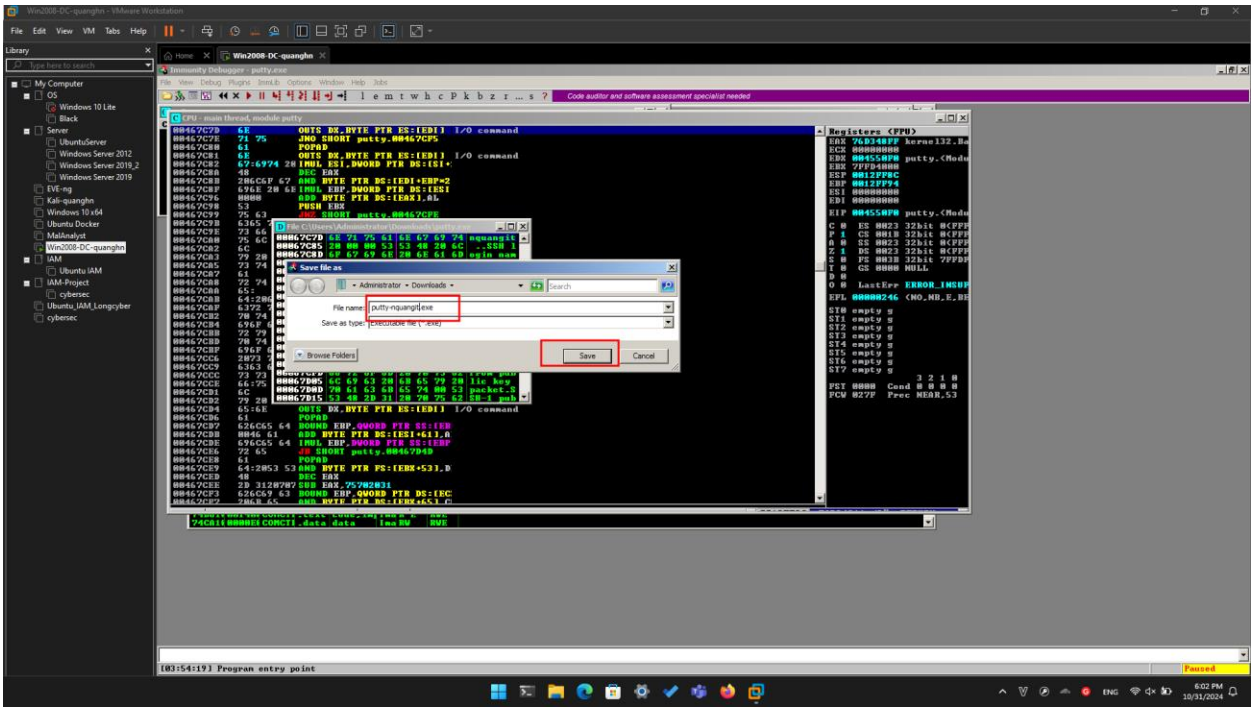




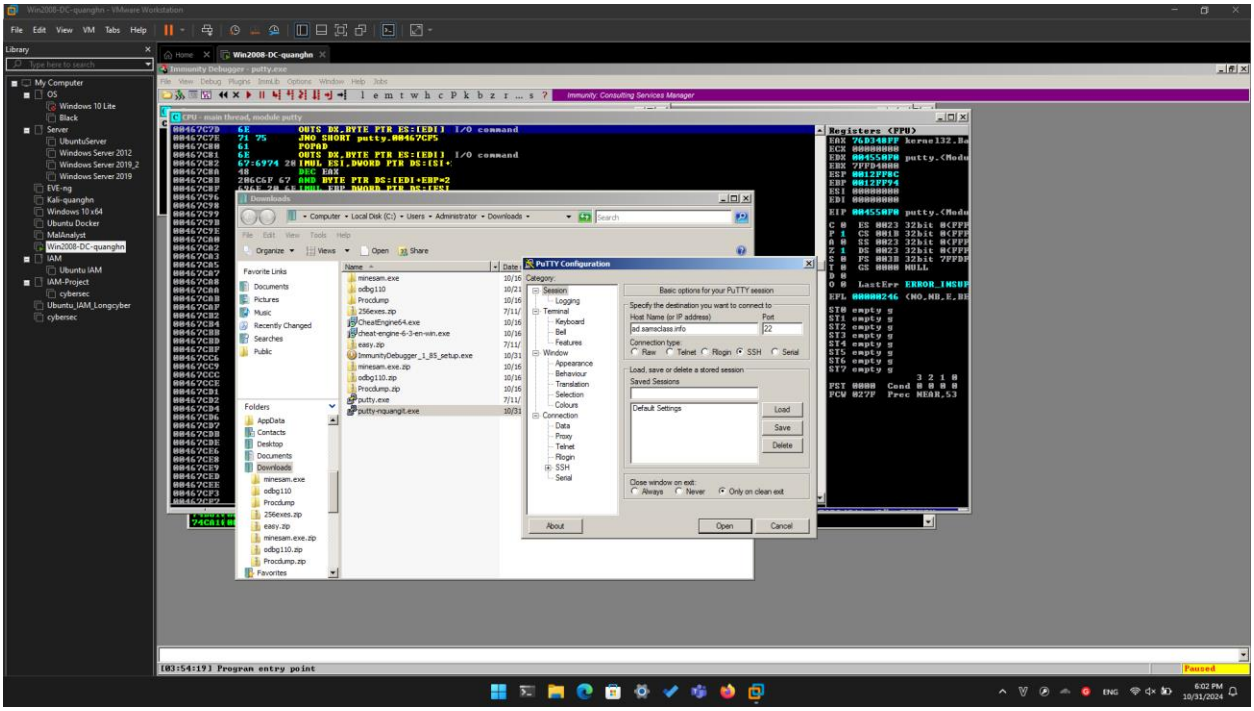
Saving the Modified EXE

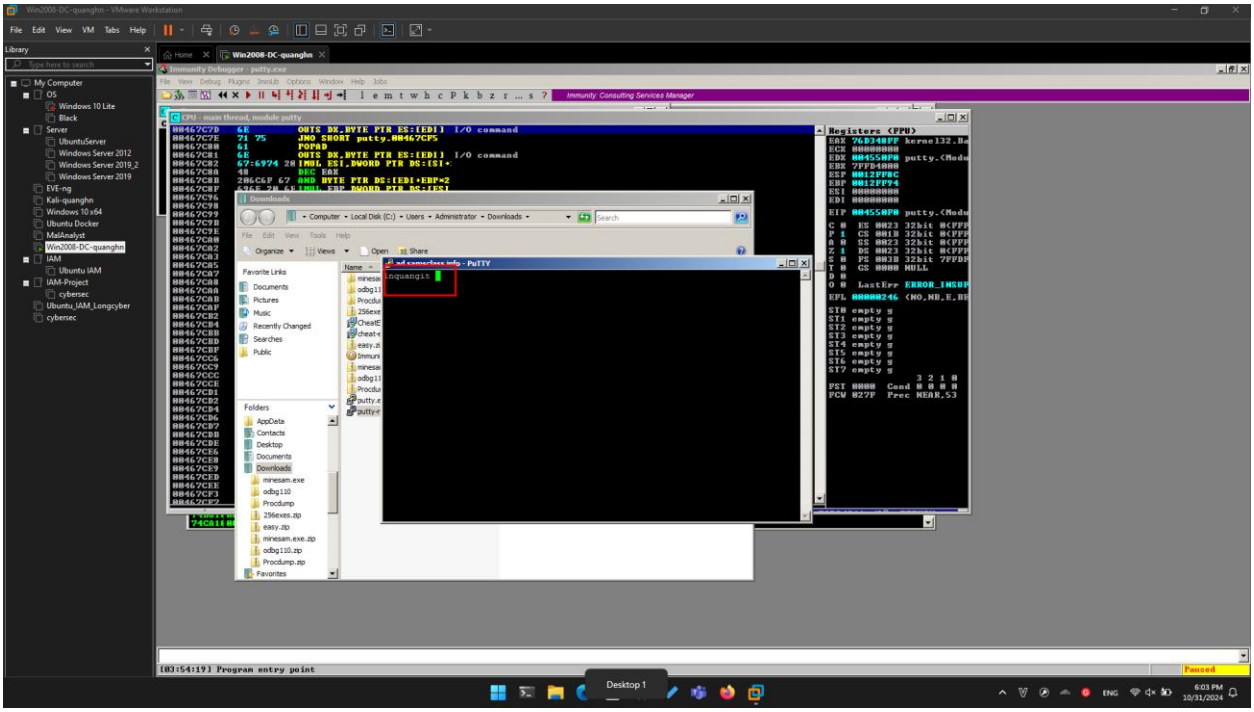






Running the Modified EXE




Win2008-DC-quanghn - VMware Workstation
Immunity Debugger - putty.exe
Immunity: Consulting Services Manager
CPU - main thread, module putty
Registers (FPU)
Downloads
PuTTY
inquangit
[03:54:19] Program entry point
Paused
Desktop 1