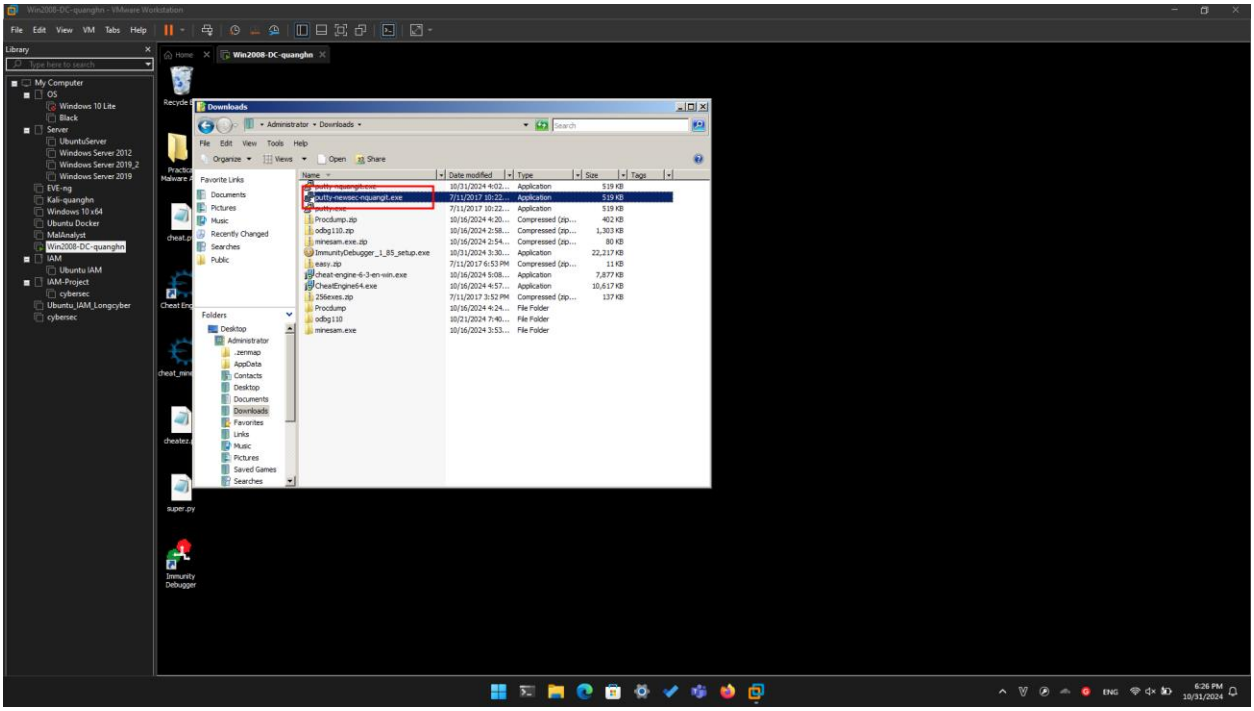
Lab 10: EXE With Trojan Code in a New Section

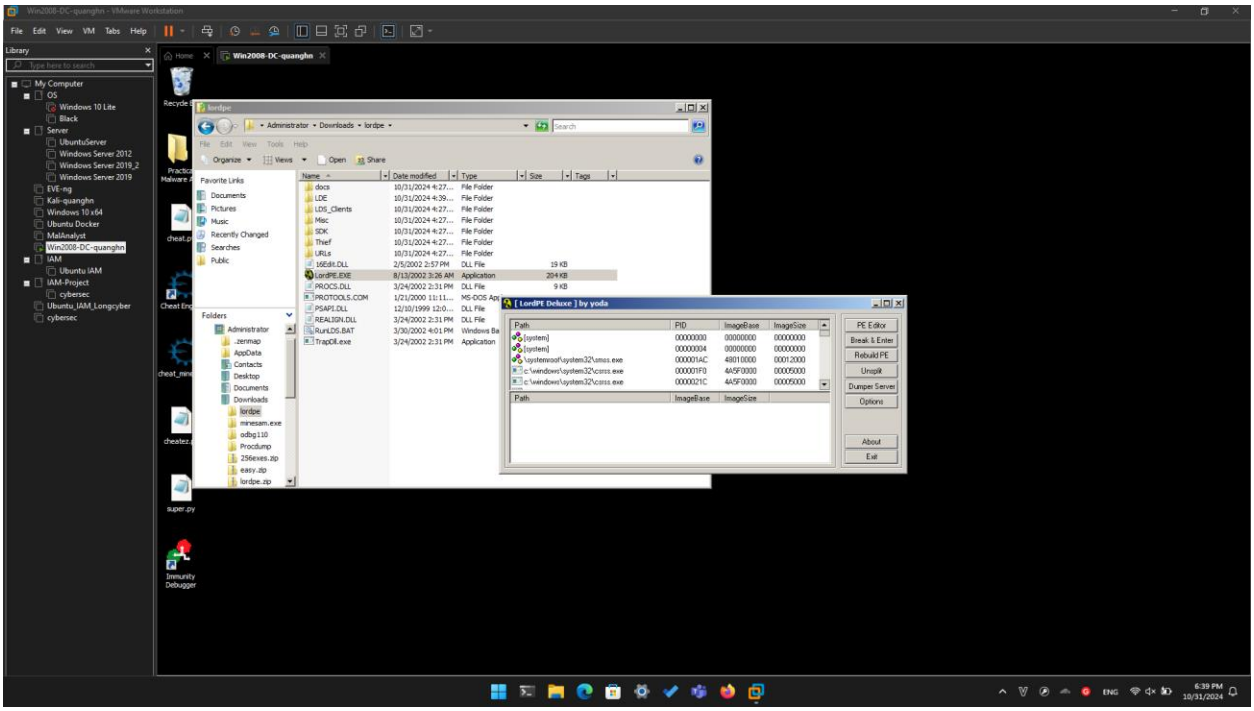
Huynh Ngoc Quang – SE181838

Task 1: Add a Section with LordPE

Copying putty.exe



Getting LordPE

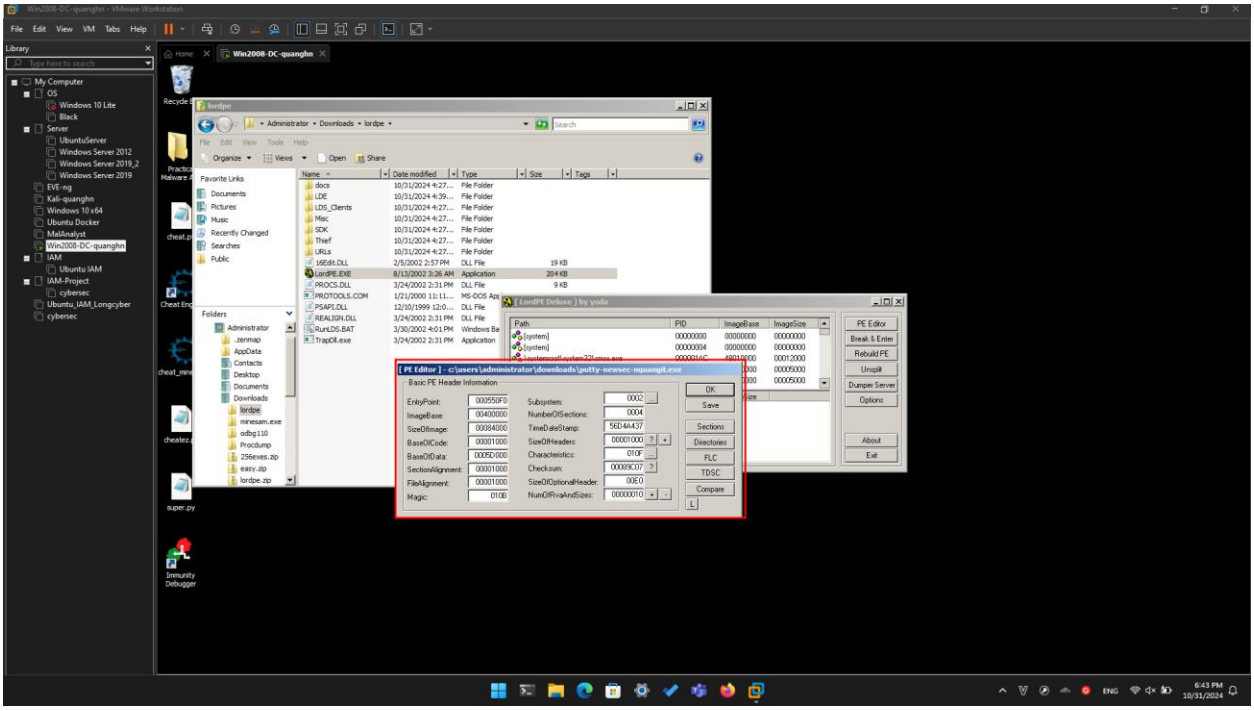


Adding a New Section to the PE Header

In the LordPE window, on the right side, click the "**PE Editor**" button.

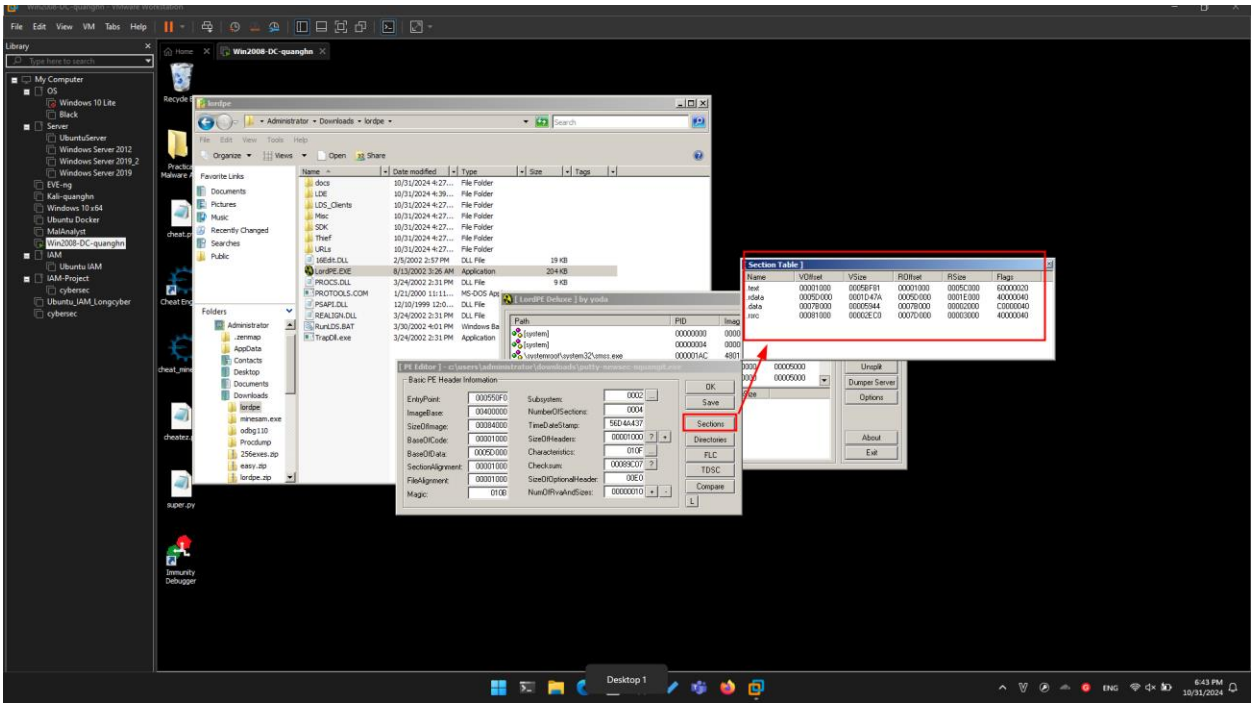
In the Open box, navigate to **putty-newsec-YOURNAME.exe** and double-click it.

A "PE Editor" box opens, showing general information about putty, as shown below.

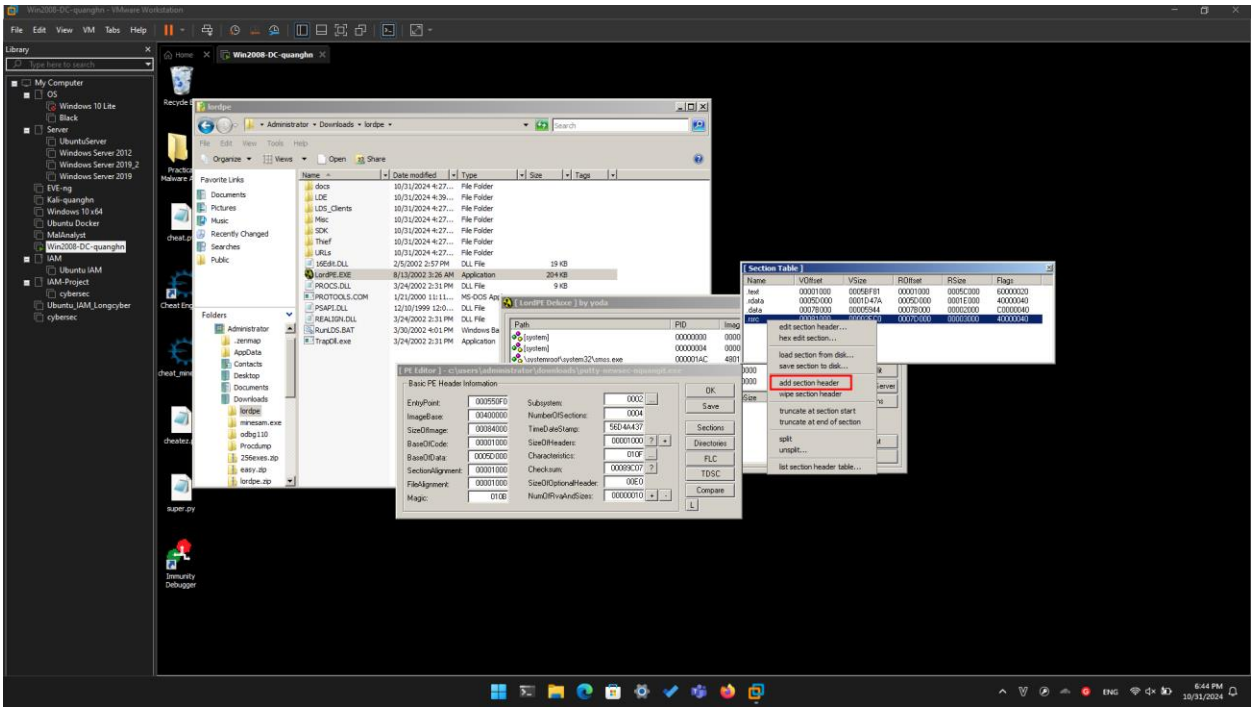


In the "PE Editor" box, on the right, click the **Sections** button.

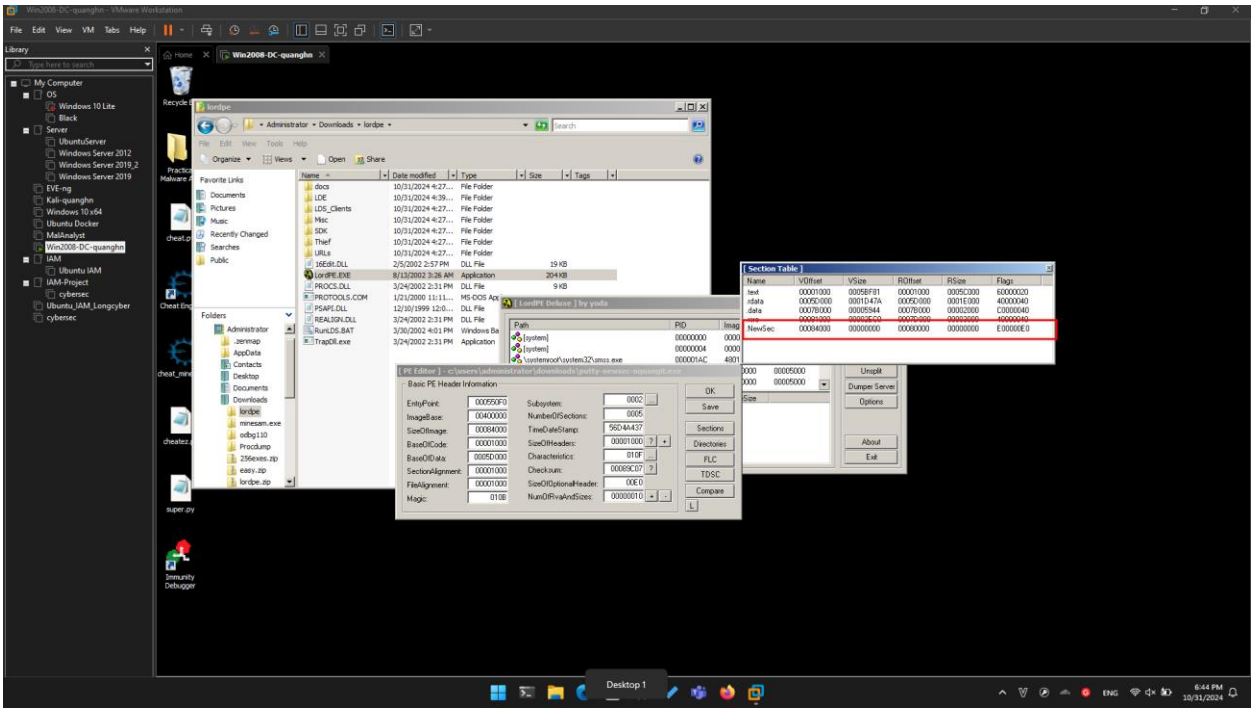
A "Section Table" box opens, showing the four sections in the putty executable.



Right-click one of the sections and click "**add section header**", as shown below.

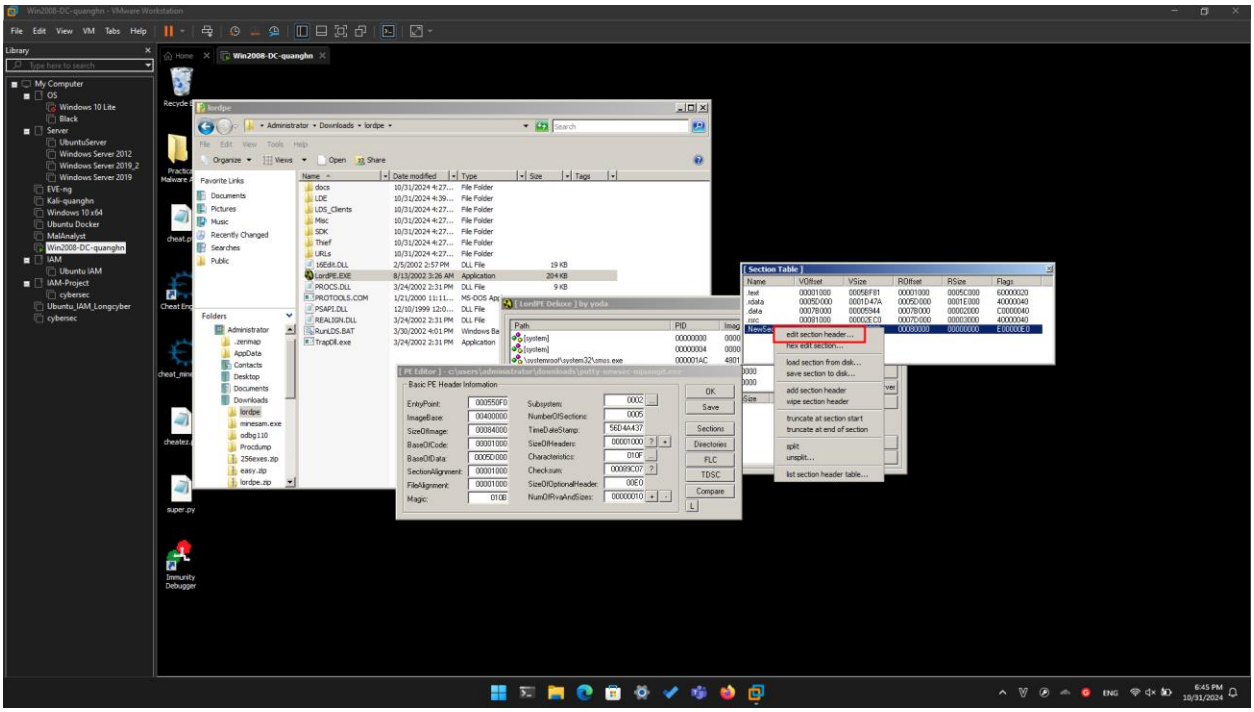


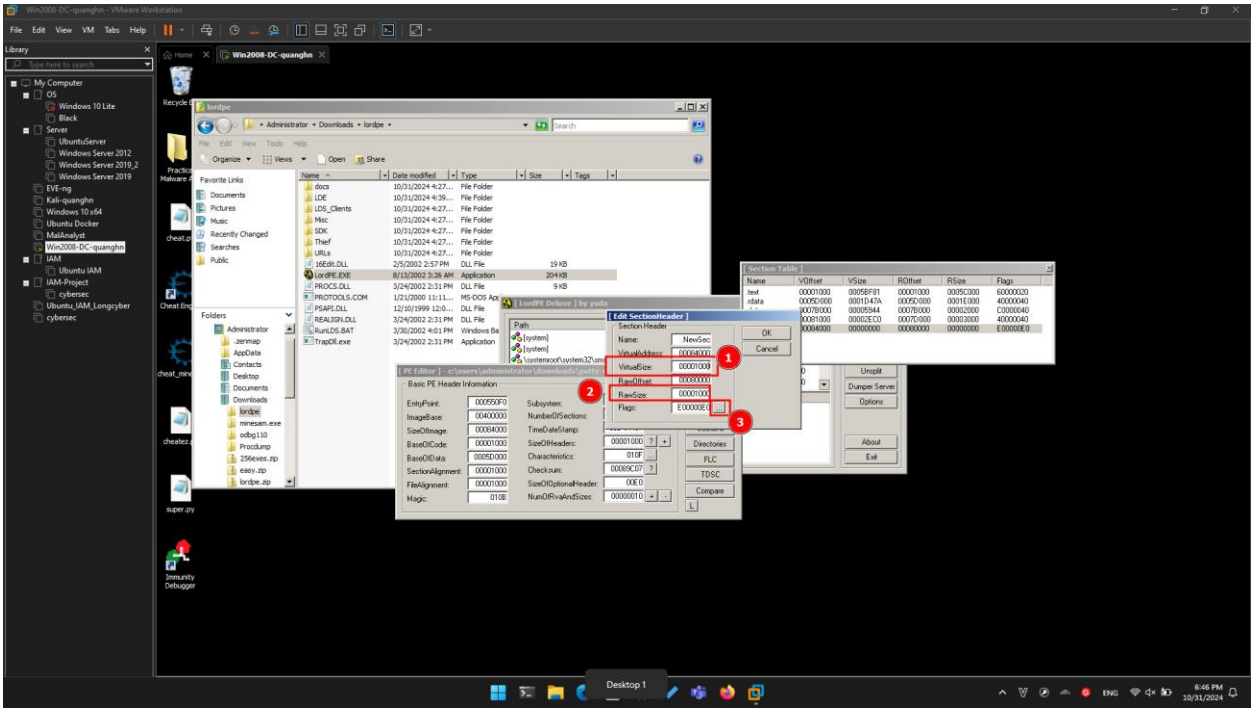
A new section named "NewSec" appears. Currently, this section has "VSize" and "RSize" values of 0, as shown below.



In the "Section Table" box, right-click **NewSec** and click "**edit section header**".

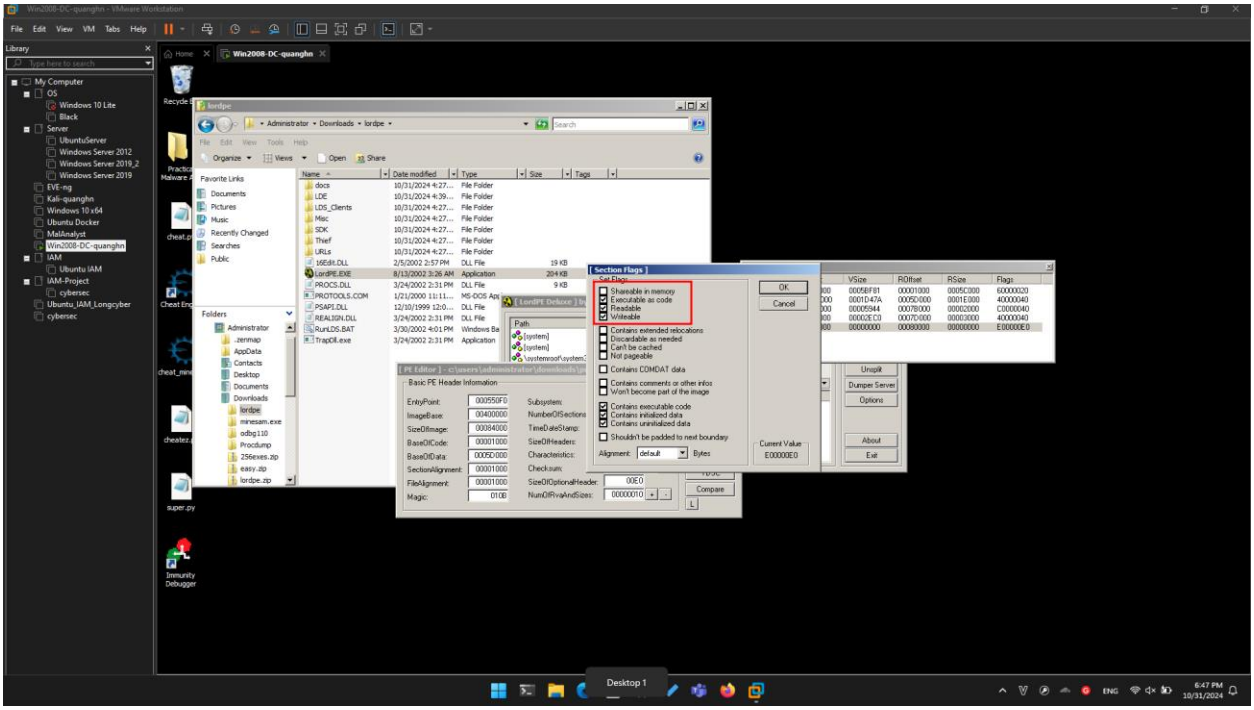
In the "[Edit SectionHeader]" window, change the **VirtualSize** and **RawSize** to **00001000** as shown below.





In the "[Edit SectionHeader]" window, at the bottom, in the "Flags" row, click the square button labelled **...**.

Note the top three check boxes here: this segment is Executable, Readable, and Writeable. That's good; we can place any type of code we want to here, even self-modifying code.



Click **OK**.

Click **OK**.

Close the "Section Table" box.

In the "PE Editor" box, click the **Save** button.

In the "PE Editor" box, click the **OK** button.

Close the LordPE window.

Task 2: Redirecting Code Execution with Immunity

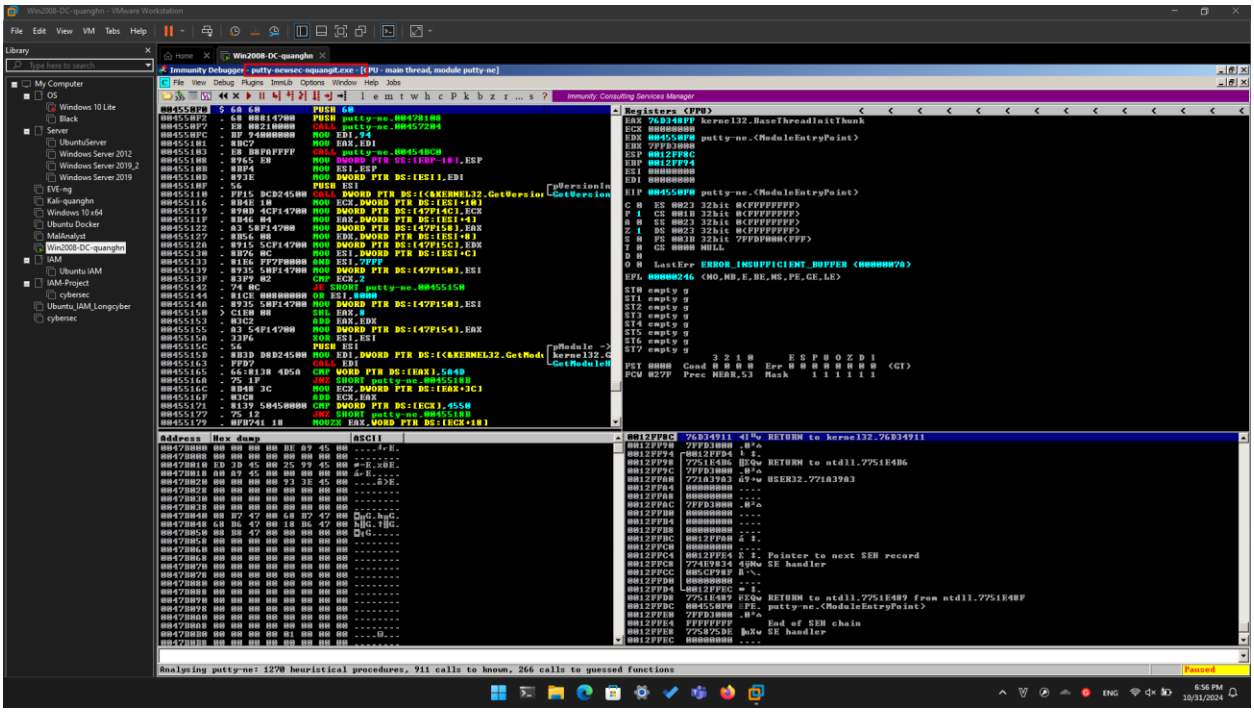
Using Immunity to Examine the NewSec Section

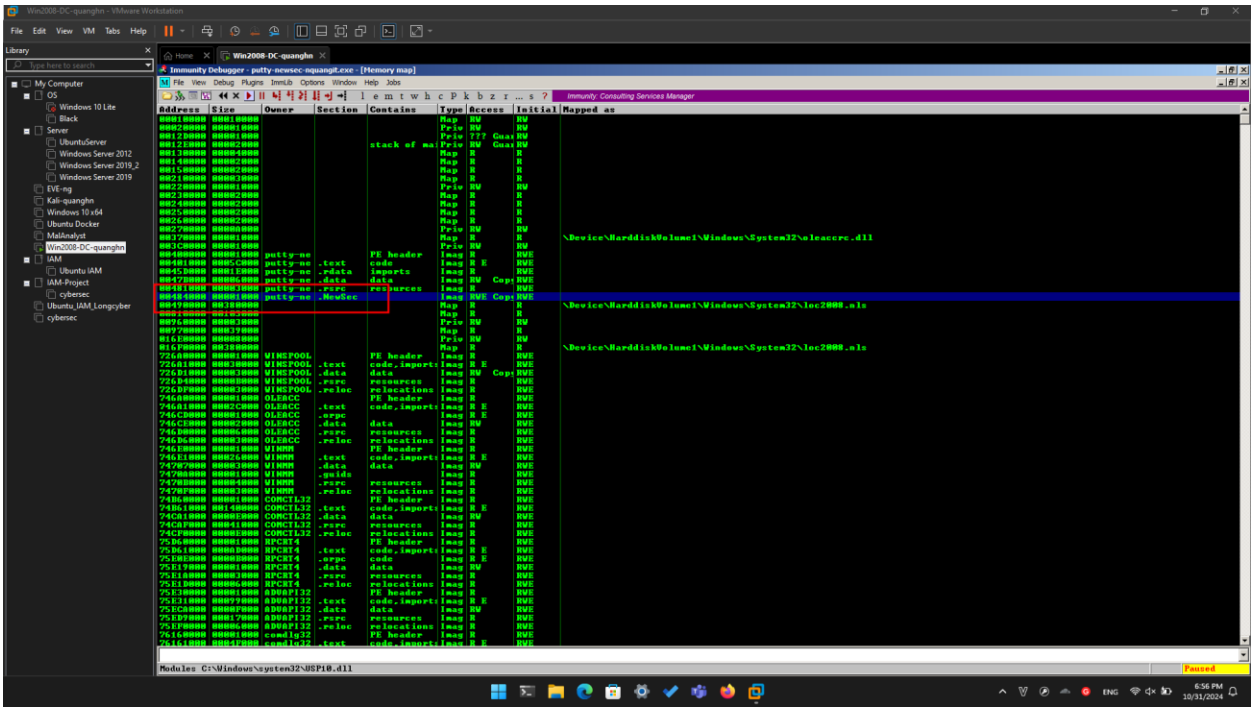
Click **Start**. Search for **Immunity Debugger** and start it.

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

From the Immunity menu bar, click **View**, **Memory**. as shown below.

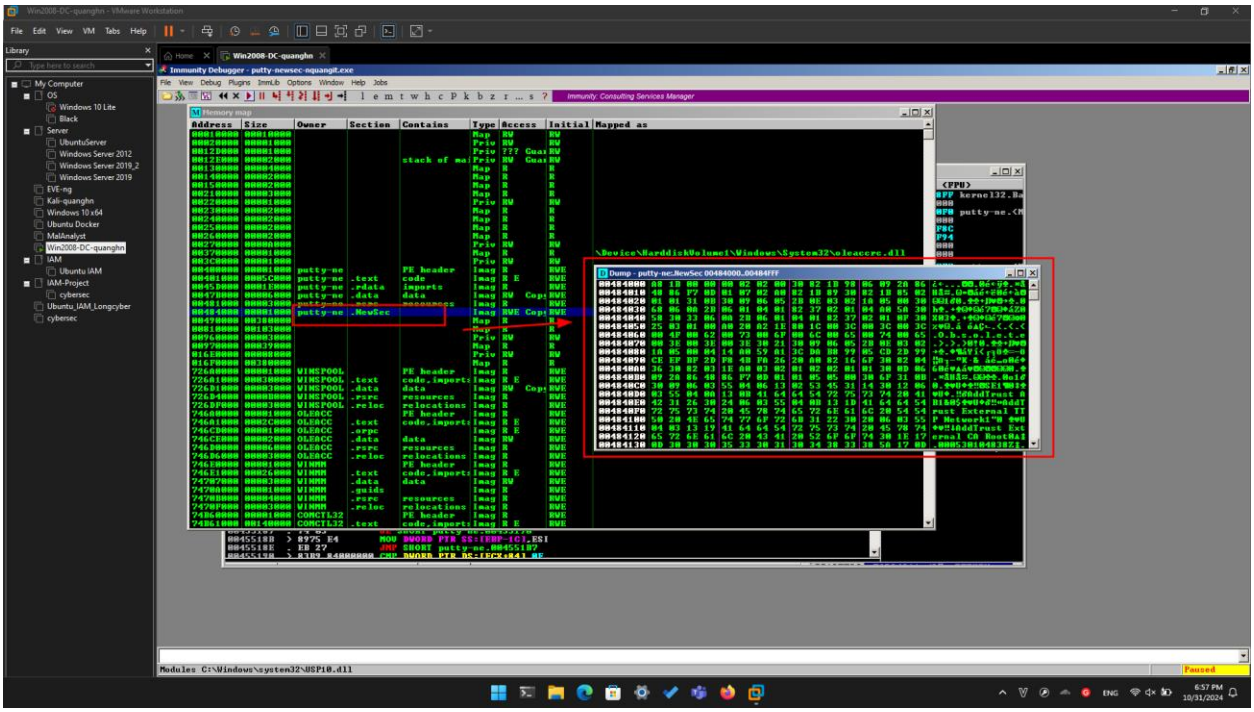
Immunity shows the memory layout of putty. As outlined in blue in the image below, the "NewSec" section begins at address **484000**.





In the "Memory ma[" window, double-click **NewSec**.

A "Dump" window opens, showing the data stored in NewSec, as shown below.



This is a digital signature, added to recent downloads of Putty. Notice the readable text in the lower portion of this window, on the right side, saying "AddTrust External CA Root".

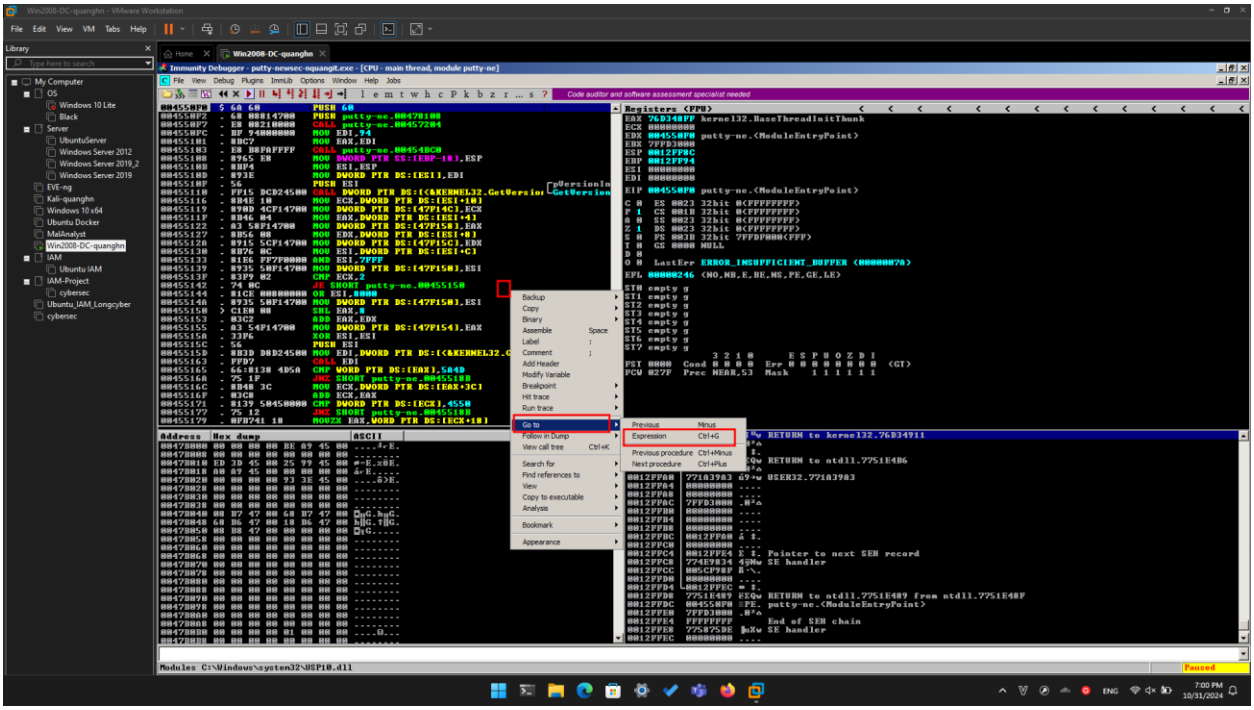
The digital signature is a good way to verify file integrity, but it's not essential for file execution, so we can overwrite it.

Close the Dump window. Close the "Memory map" window.

Using Immunity to Redirect Code Execution

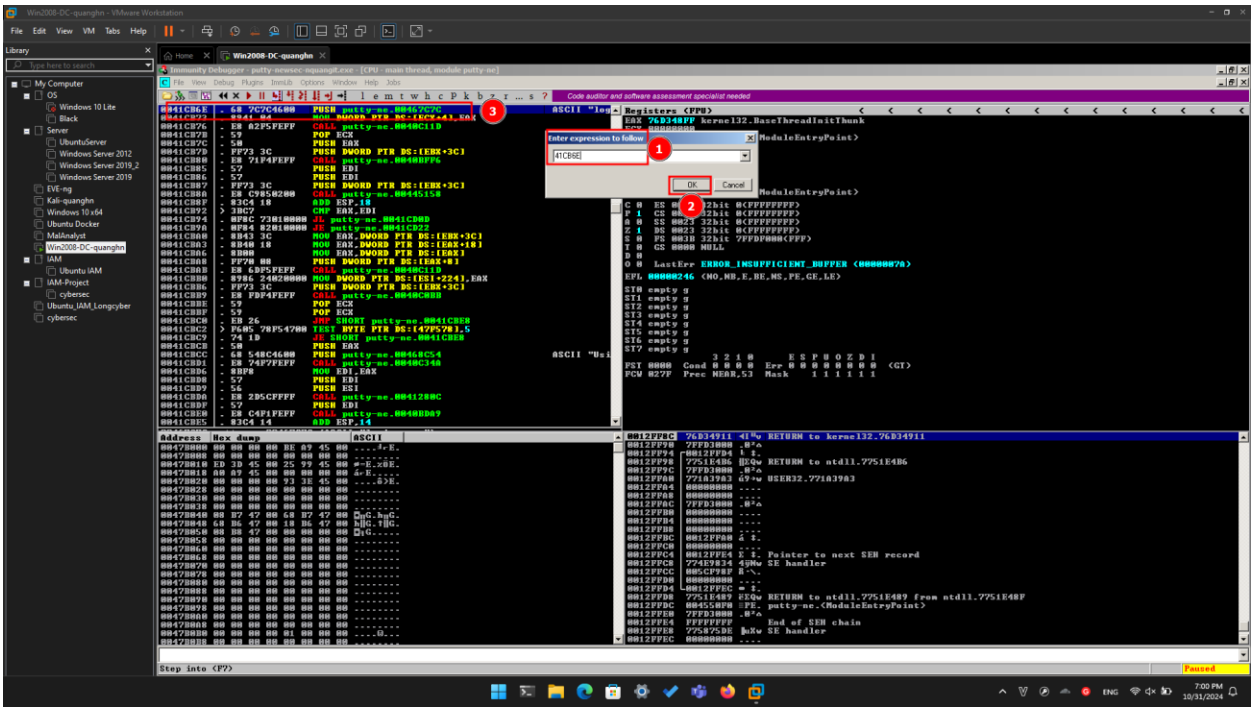
In Immunity, maximize the CPU window.

In the top left pane of the CPU window, right-click, and click "**Go to**", **Expression**, as shown below.



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

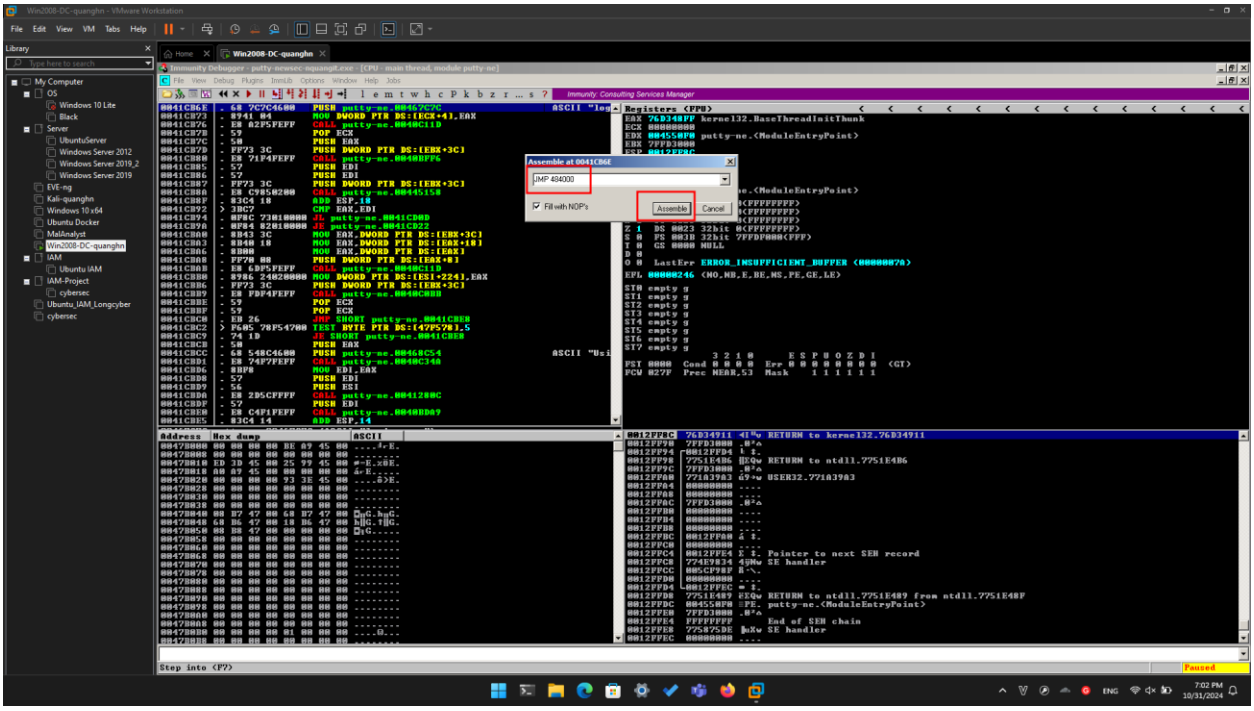
Immunity moves to show the PUSH instruction that loads the "login as: " string, as shown below.



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

In the "Assemble" box, enter this command:

JMP 484000

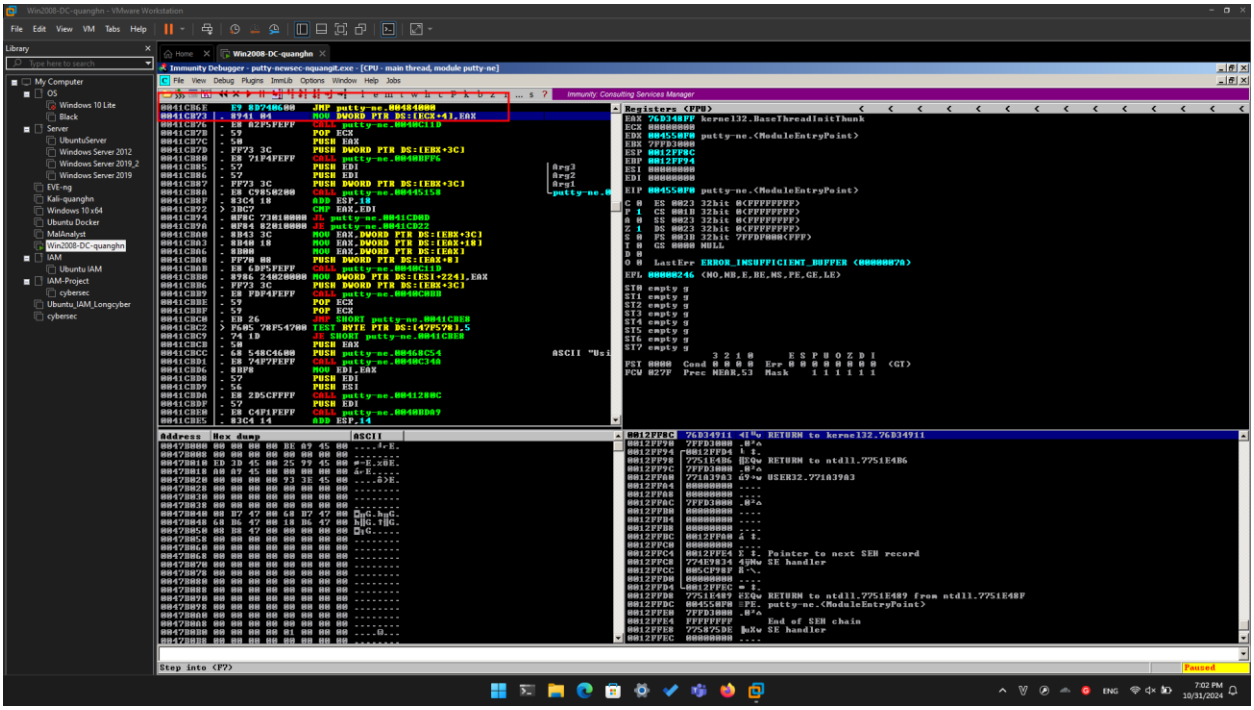


Click the **Assemble** button.

Click the **Cancel** button.

The MOV instruction has been replaced by this instruction, as shown below:

JMP putty-ne.00484000



Adding Trojan Code

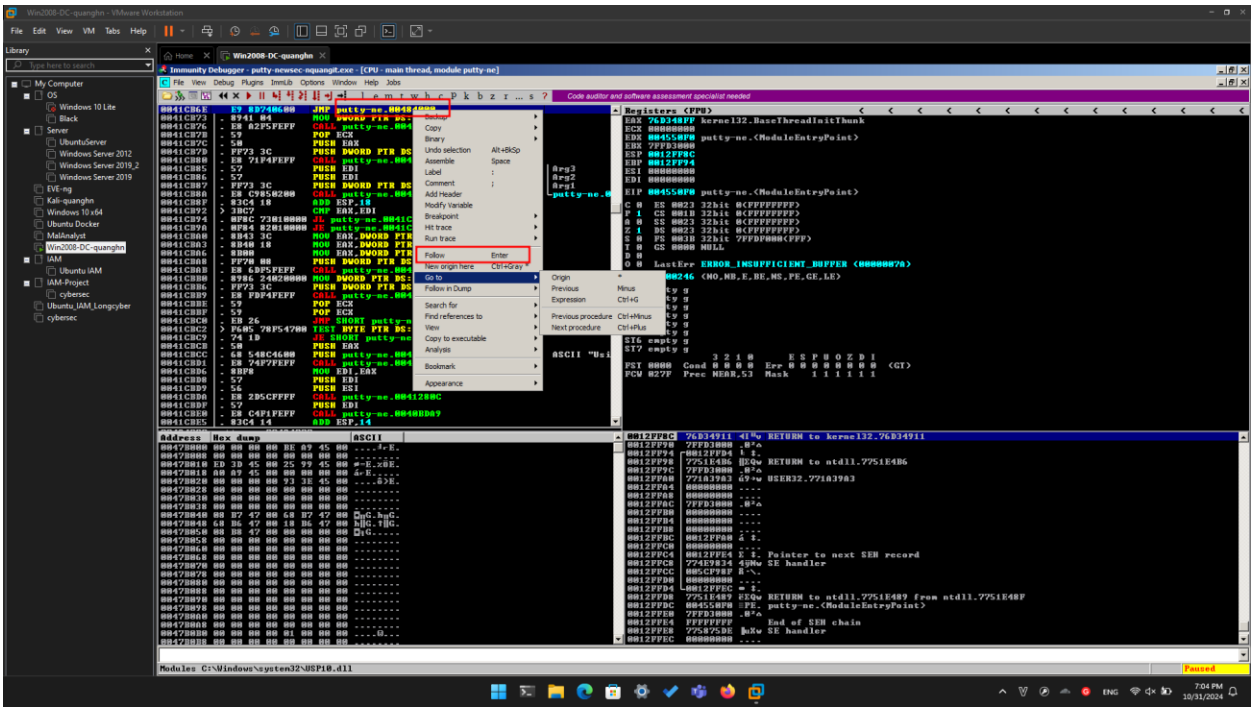
Now we can add extra commands to Putty in ".NewSec". First we'll just put an INT3 there, so we can verify that the redirection works. When the processor executes the INT3 command, the program will stop and show a message in Immunity.

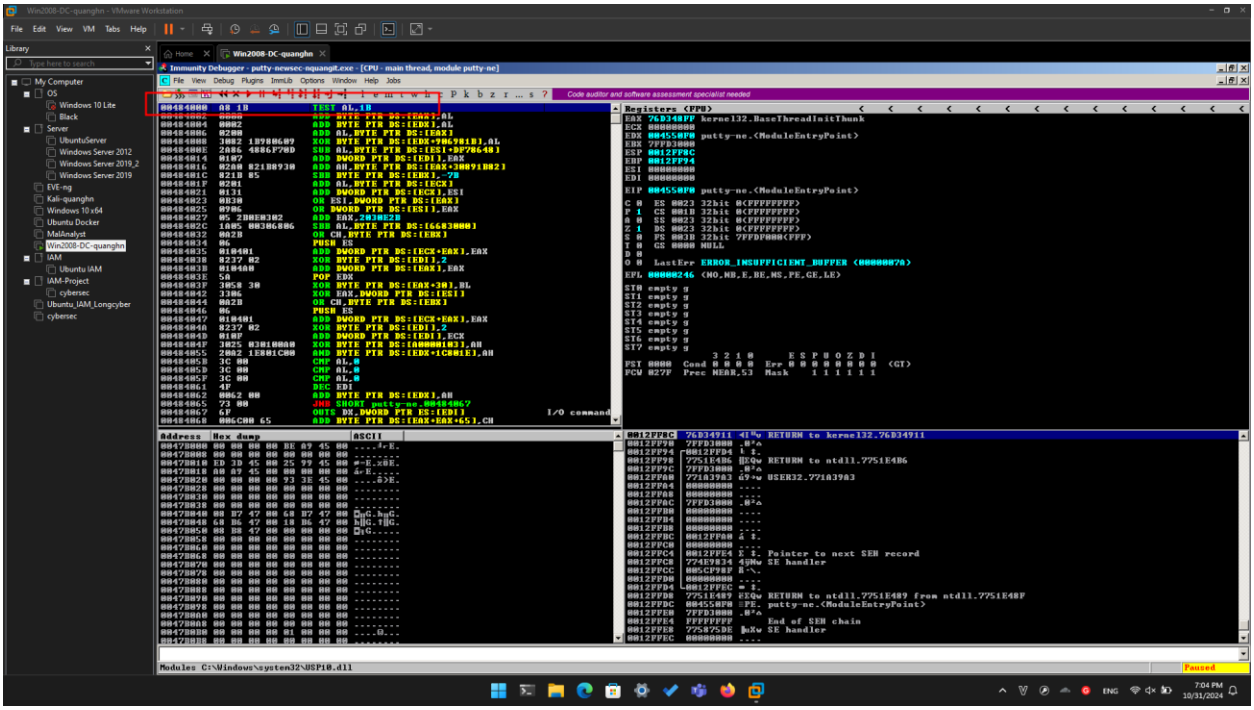
In the JMP insruction, right-click **00484000**. and click **Follow**.

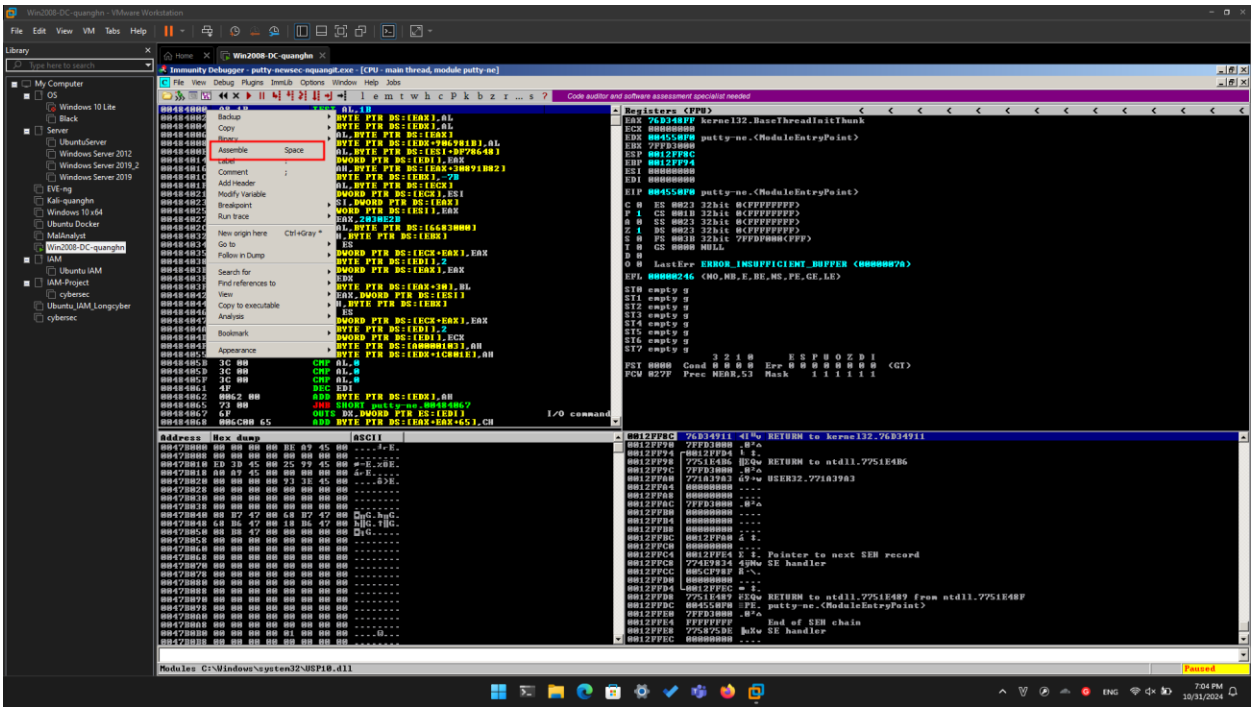
Immunity moves to address 00484000.

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

INT3

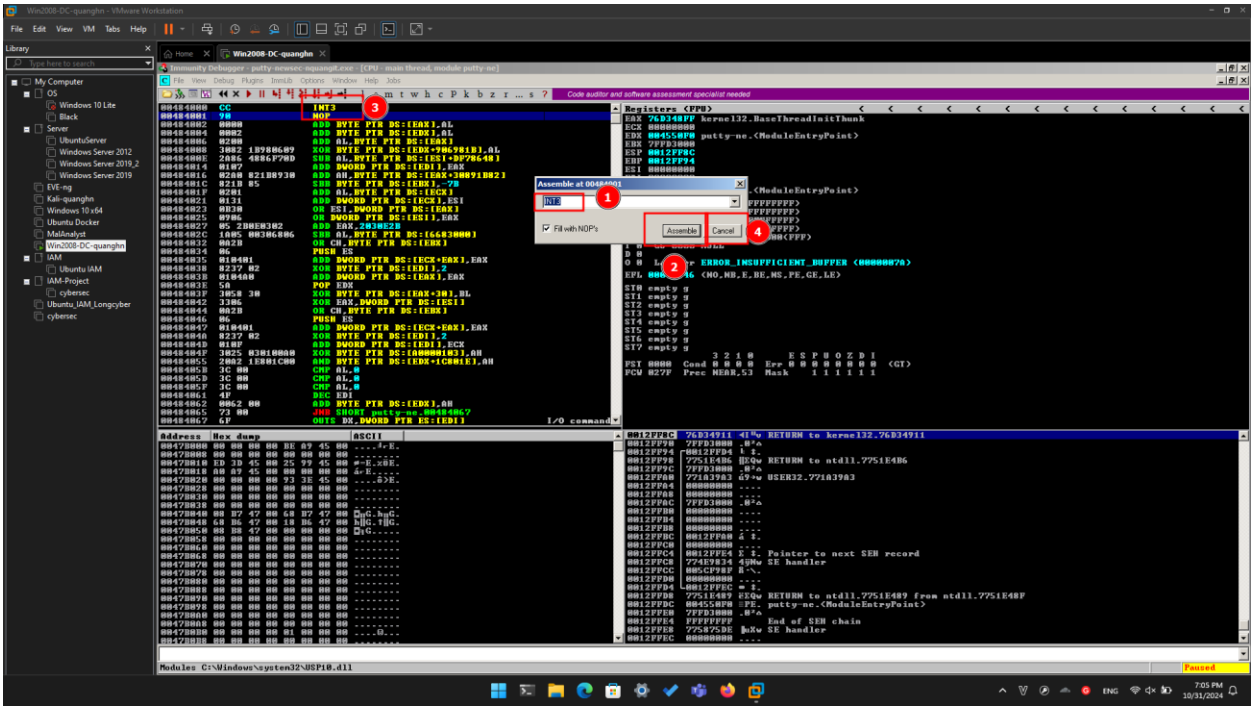






Click **Assemble**. Click **Cancel**.

Address 484000 now contains an INT3 instruction, which is CC in hexadecimal, As shown below.



Running the Modified App in Immunity

In Immunity, click **Debug**, **Run**.

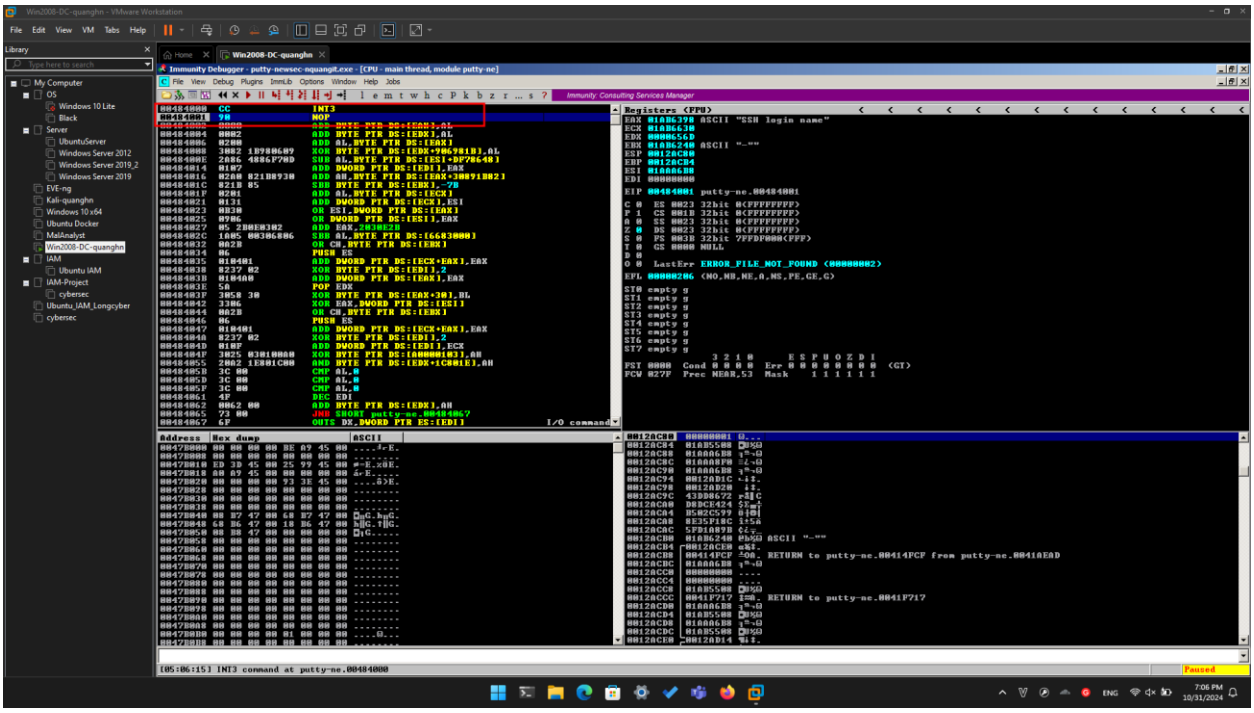
Putty opens. In the "Host Name (or IP address)" box, type

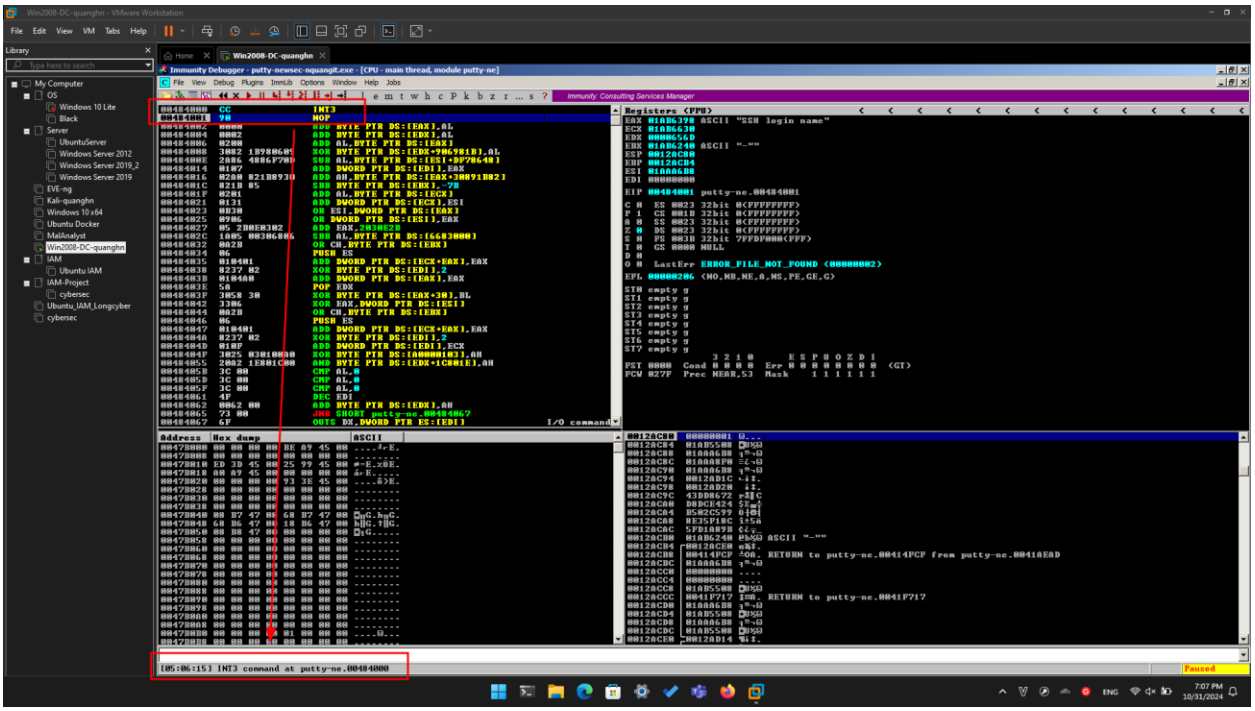
ad.samsclass.info

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!



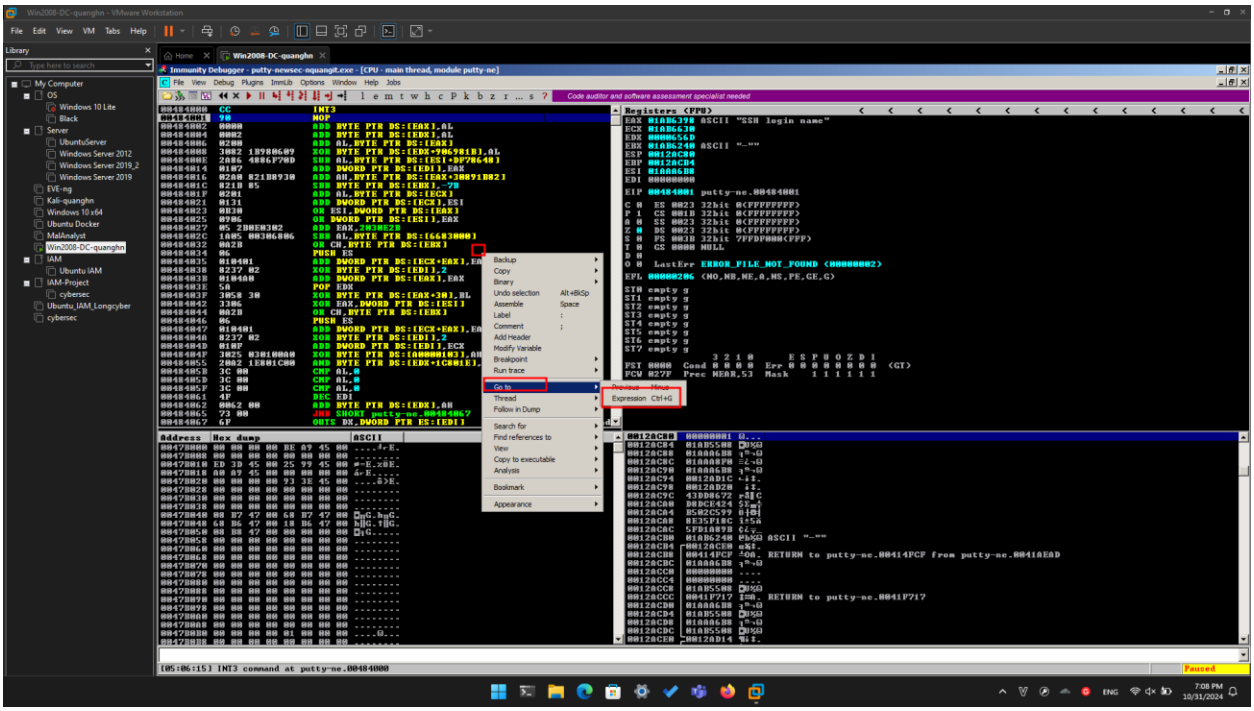


Task 3: Inserting Real Shellcode

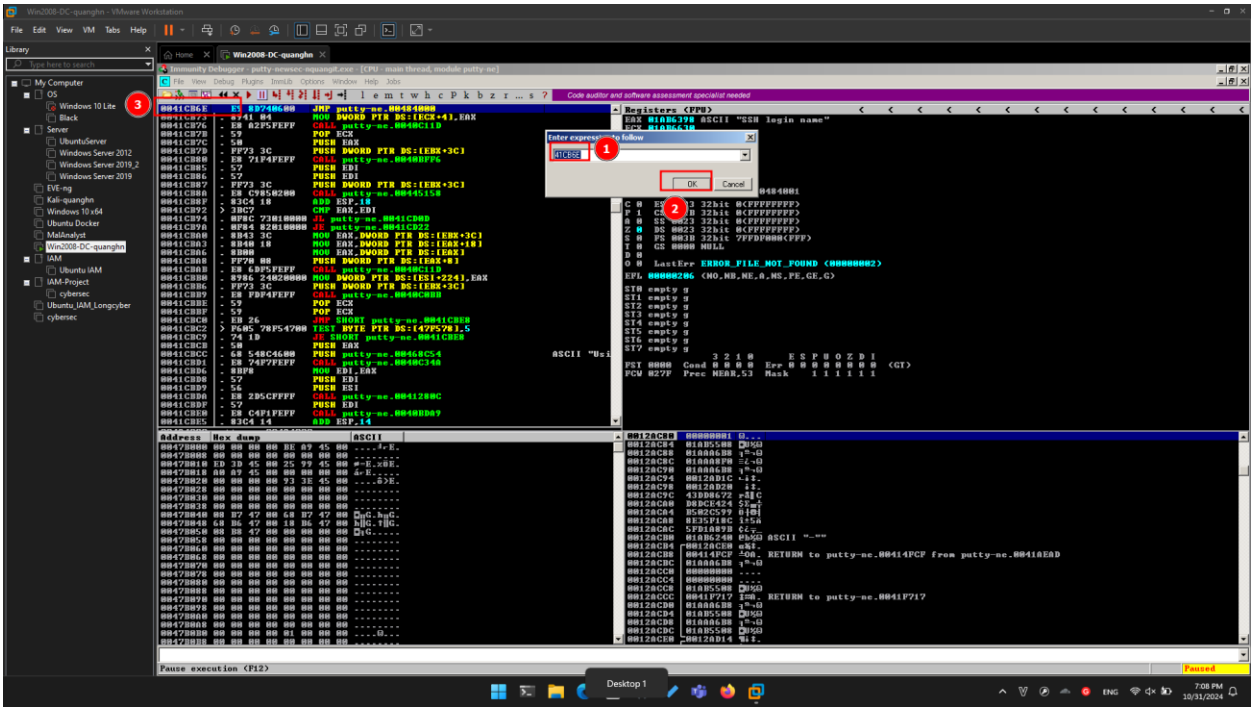
Saving the Modified EXE

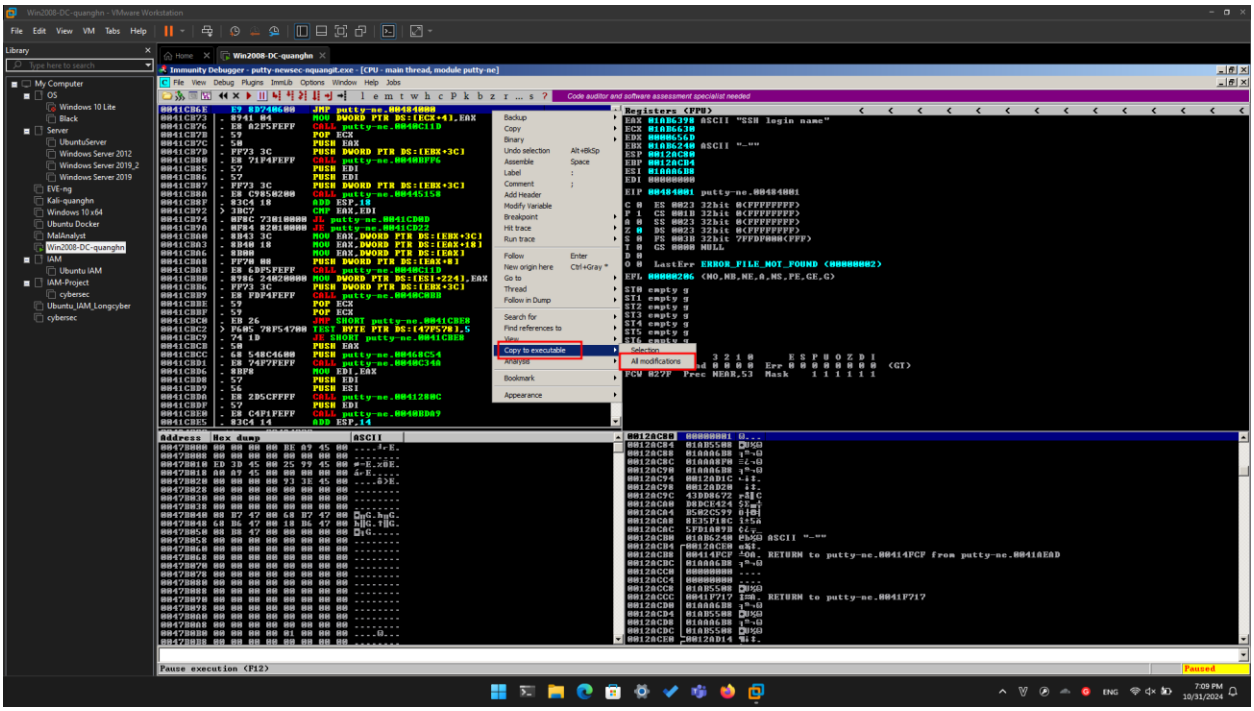
In Immunity, maximize the CPU window.

In the top left pane of the CPU window, right-click, and click "**Go to**", **Expression**, as shown below.

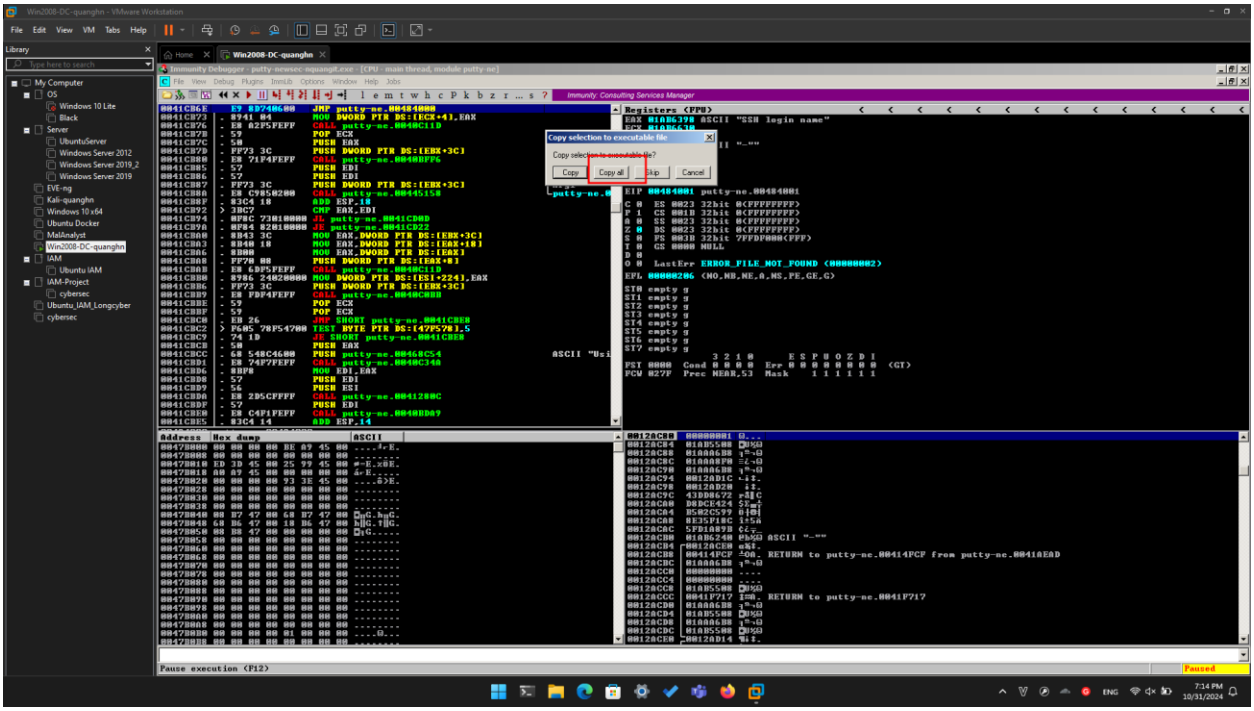


In the "Enter expression to follow" box, enter **41CB6E** as shown below. Click **OK**.



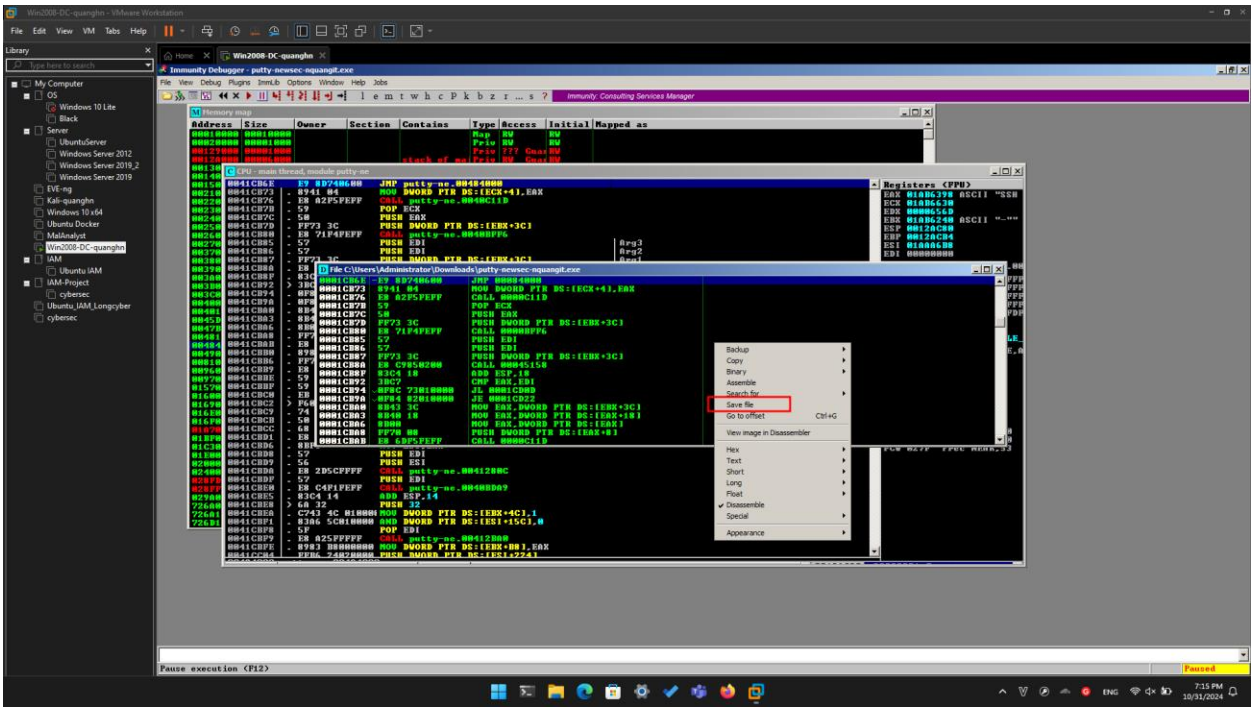


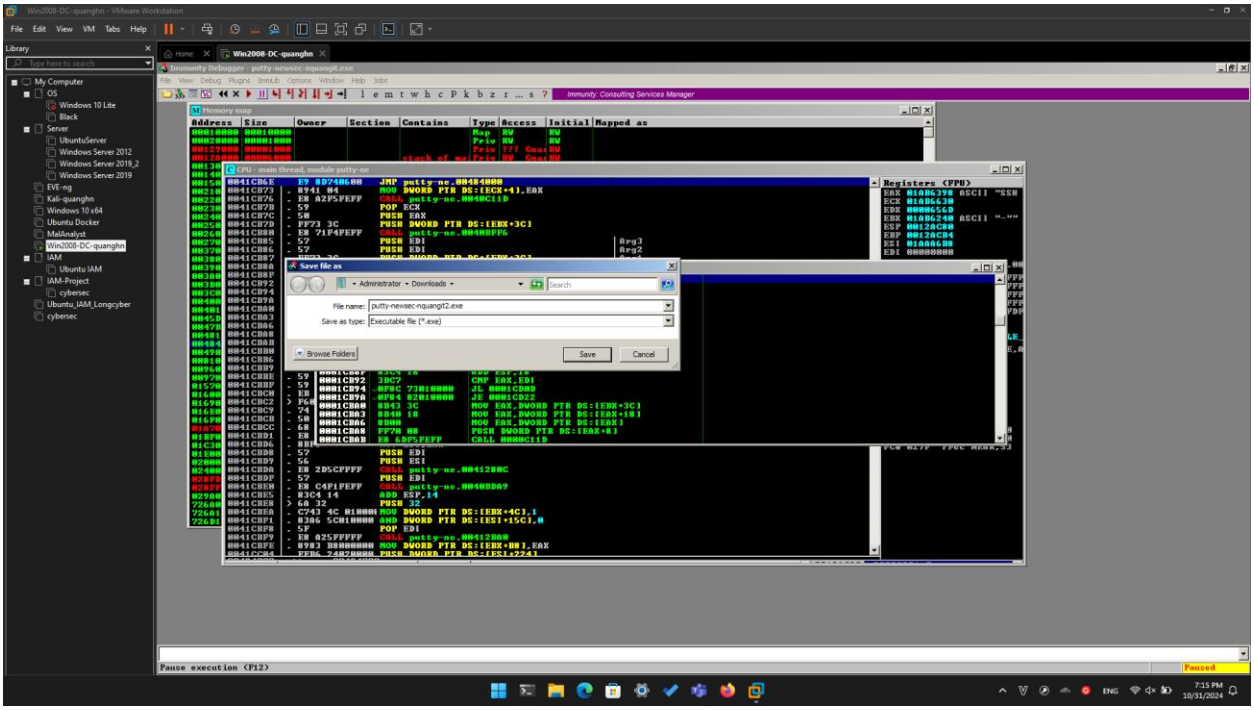
A "Copy selection to executable file" box pops up. Click the "**Copy all**" button.



A new window pops up, with a title ending in "putty.exe", as shown below.

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





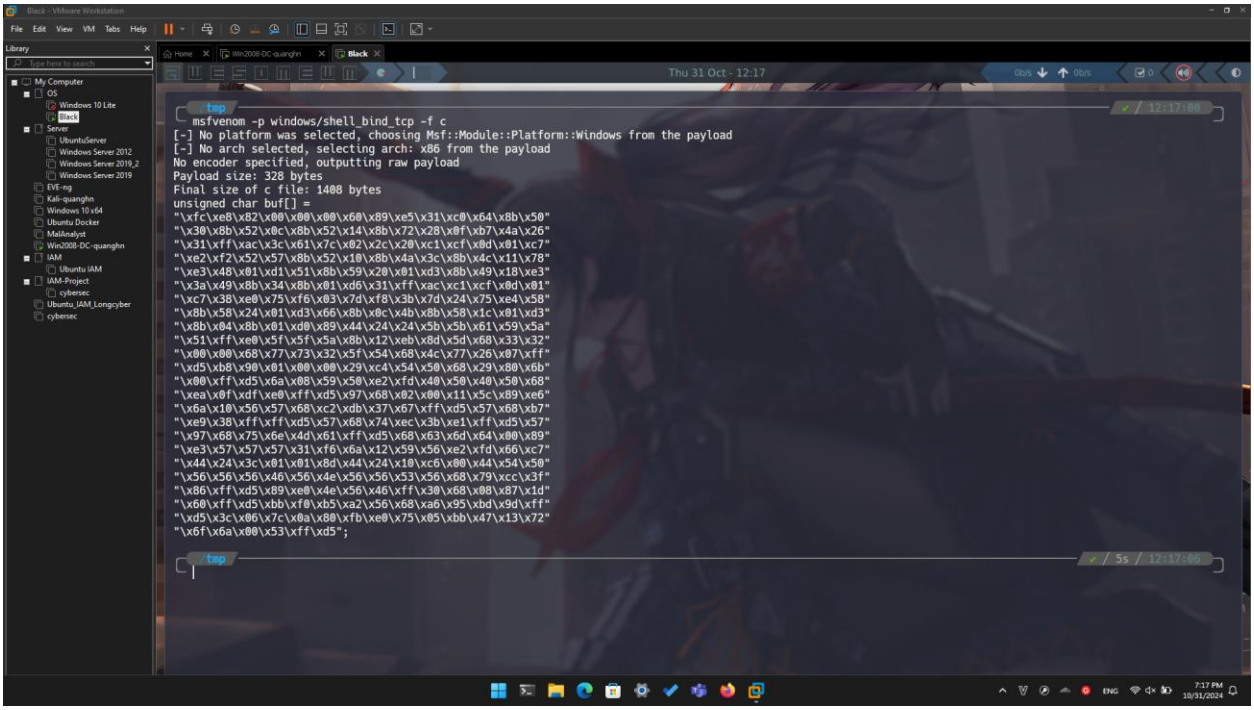
Getting Simple Shellcode

Usually it's best to generate custom shellcode for each attack, and use a reverse shell that calls your Command-and-Control server. But for this project, we'll use a simpler attack, that merely opens a listening port on port 4444. This is a weak attack that can be stopped by any firewall, but it's good enough to practice the exploitation

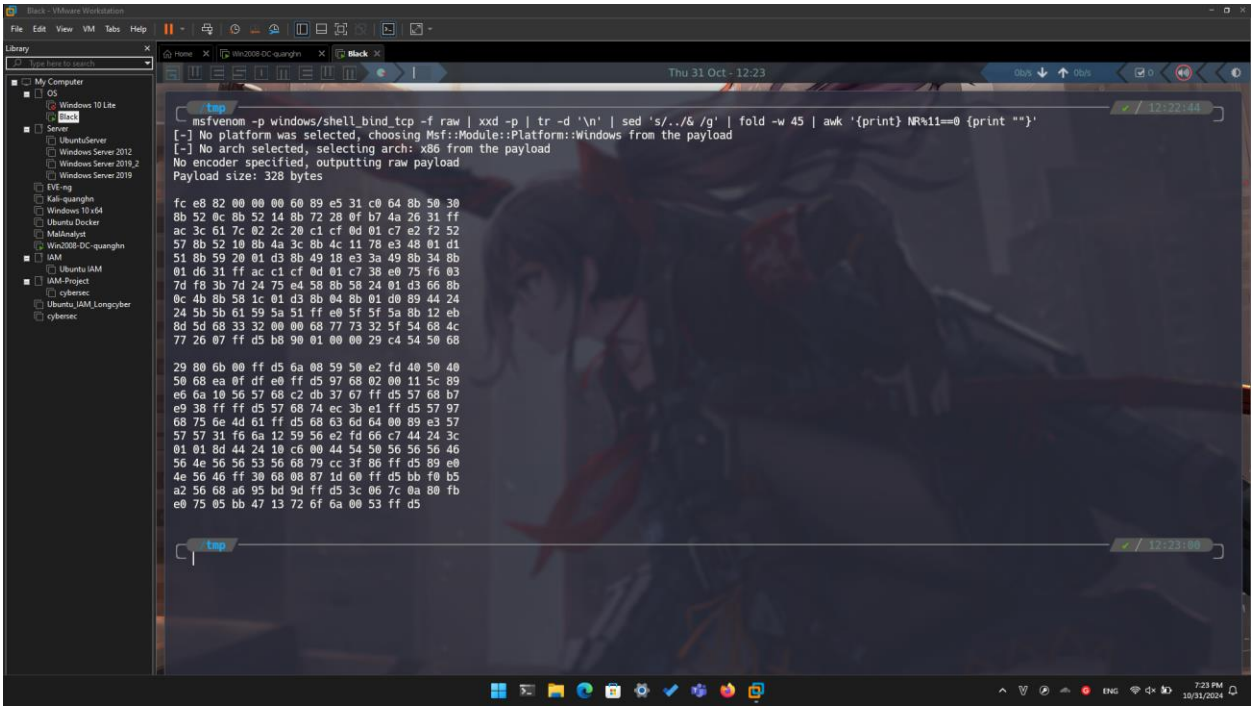
techniques,

You can generate shellcode with msfvenom, on Kali. Here's what I got when I did it:

root@kali:~/Cminer# msfvenom -p windows/shell_bind_tcp -f c



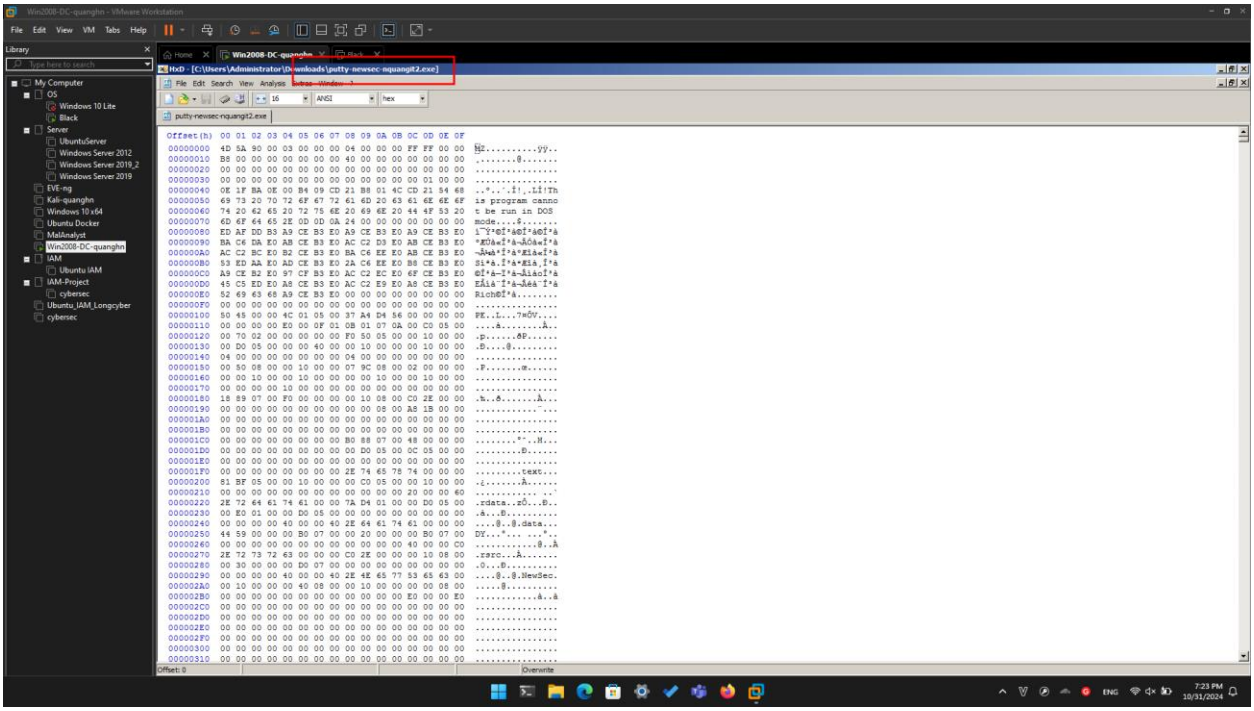
Here's the shellcode, reformatted and broken into two sections.

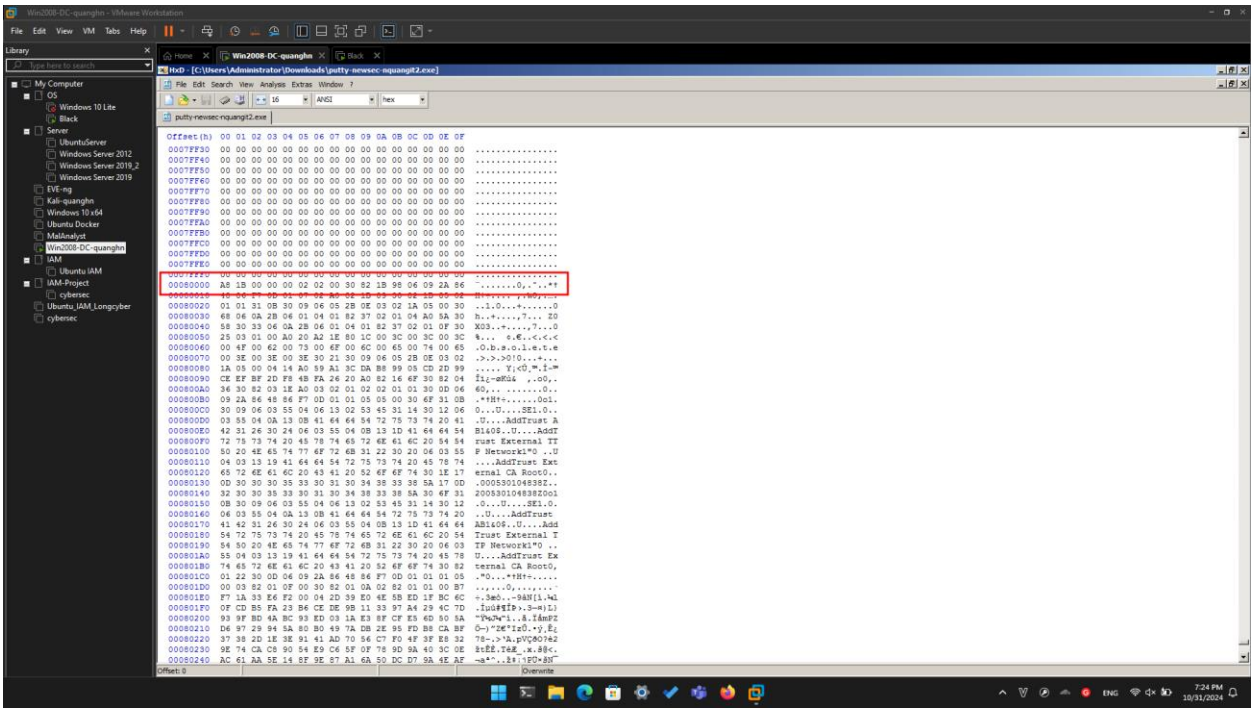


Inserting Shellcode with HxD

Open HxD. Click **File**, **Open**. Open **putty-newsec-YOURNAME2.exe**.

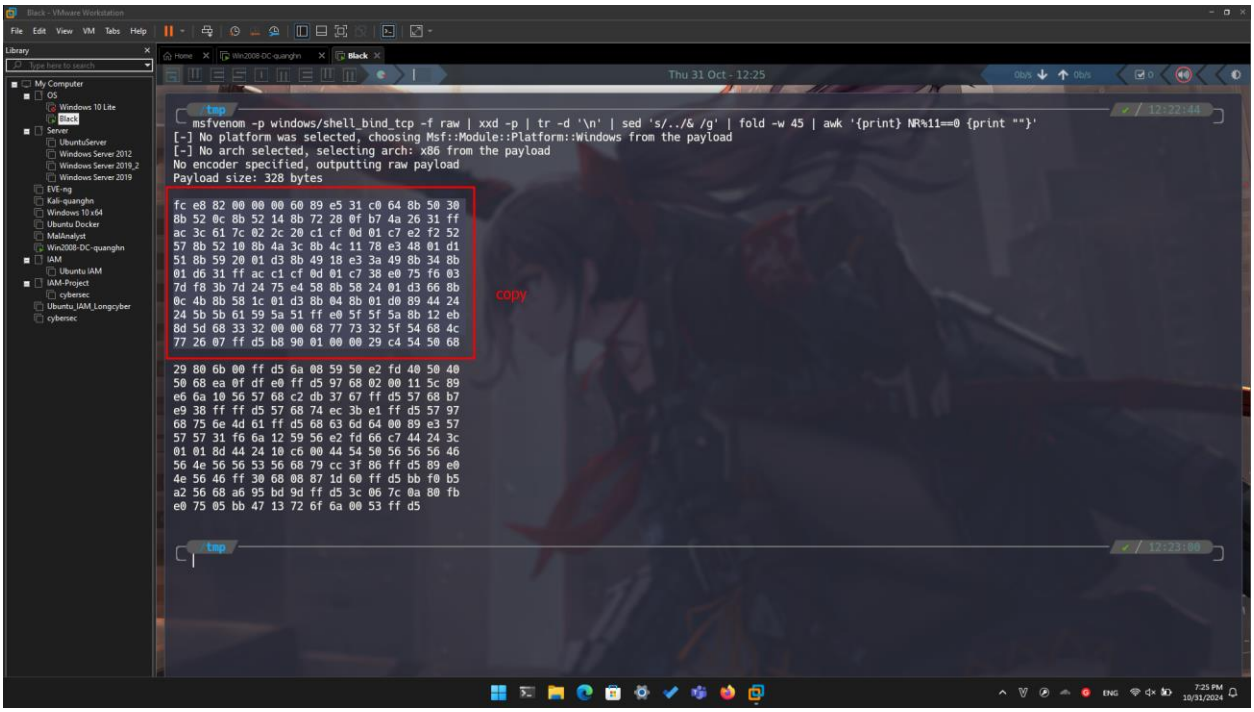
Scroll to address 00080000. After a region filled with zeroes, it starts with these bytes: "A8 1B 00", as shown below.



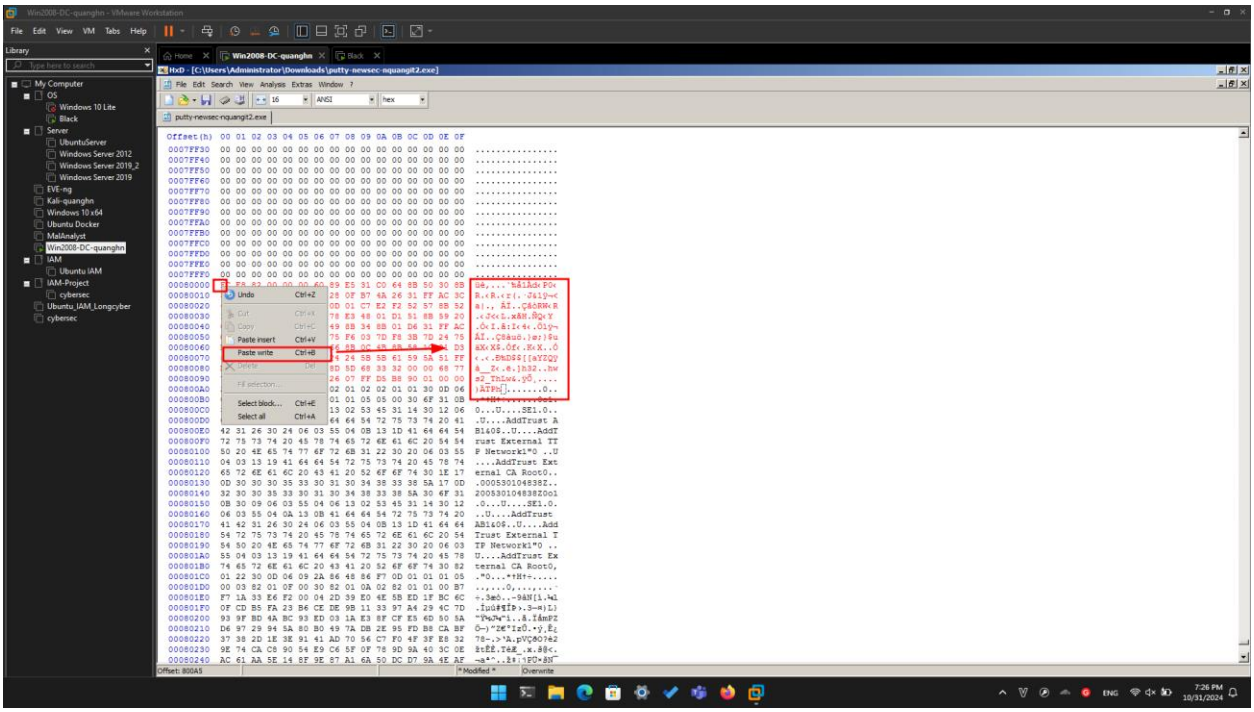


Above, on this Web page, highlight and copy the first set of shellcode bytes, from "fc" through "68".

In HxD, right-click the byte at address 00080000 and click "**Paste write**", as shown below.

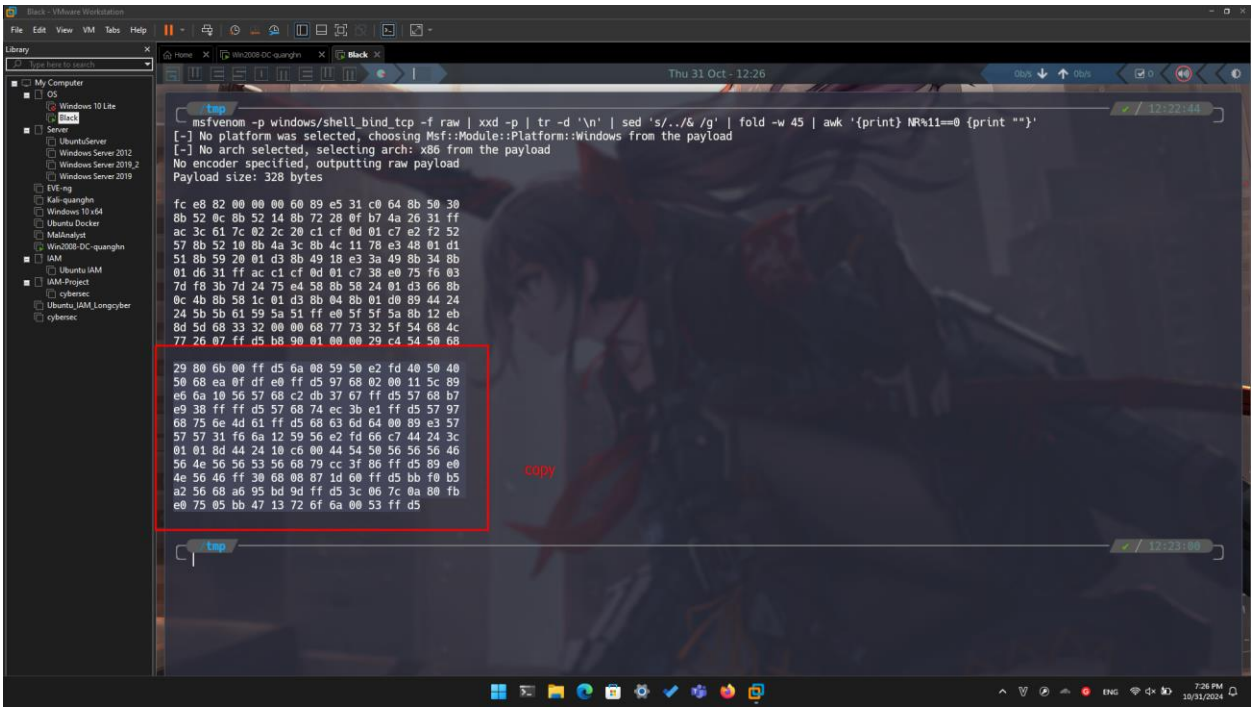


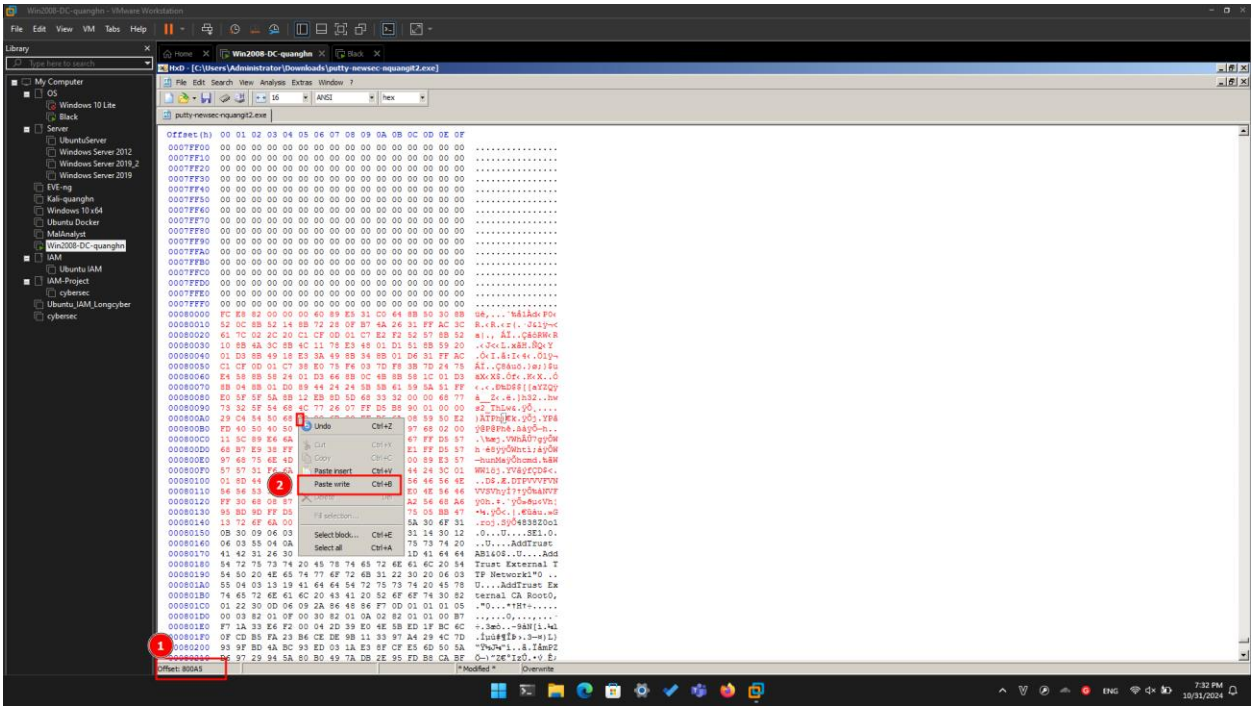
The first portion of the shellcode appears in red text, as shown below.

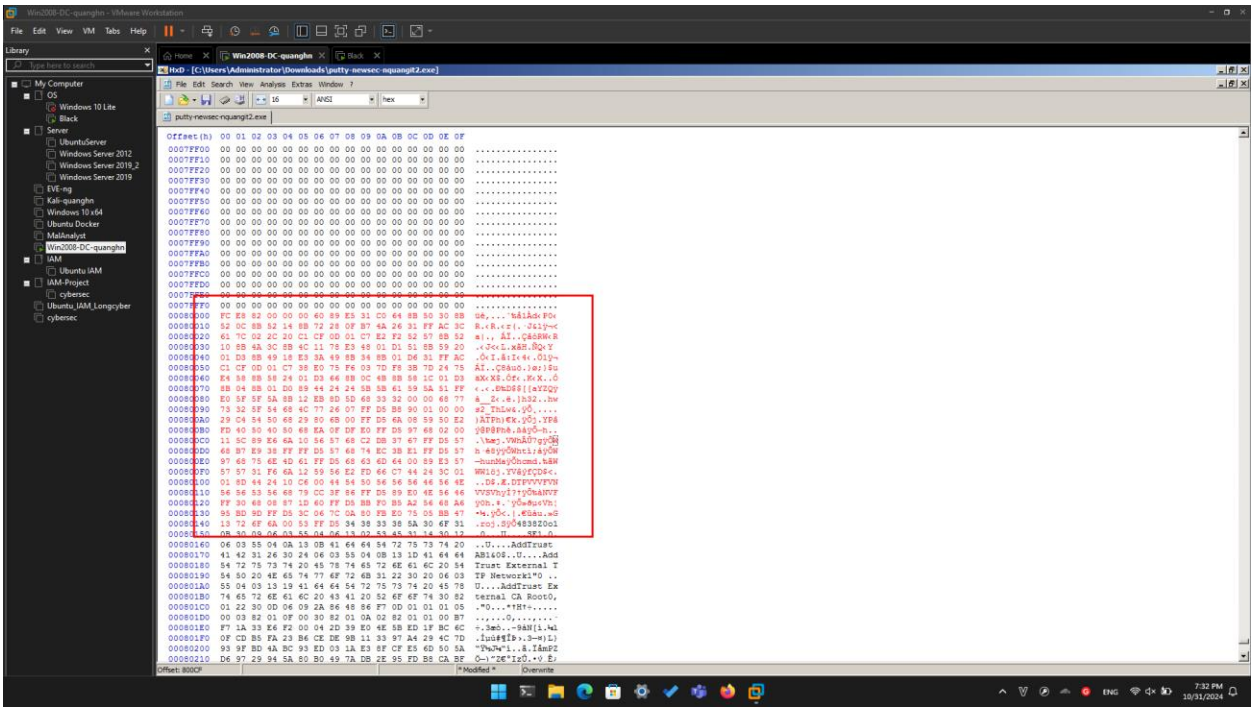


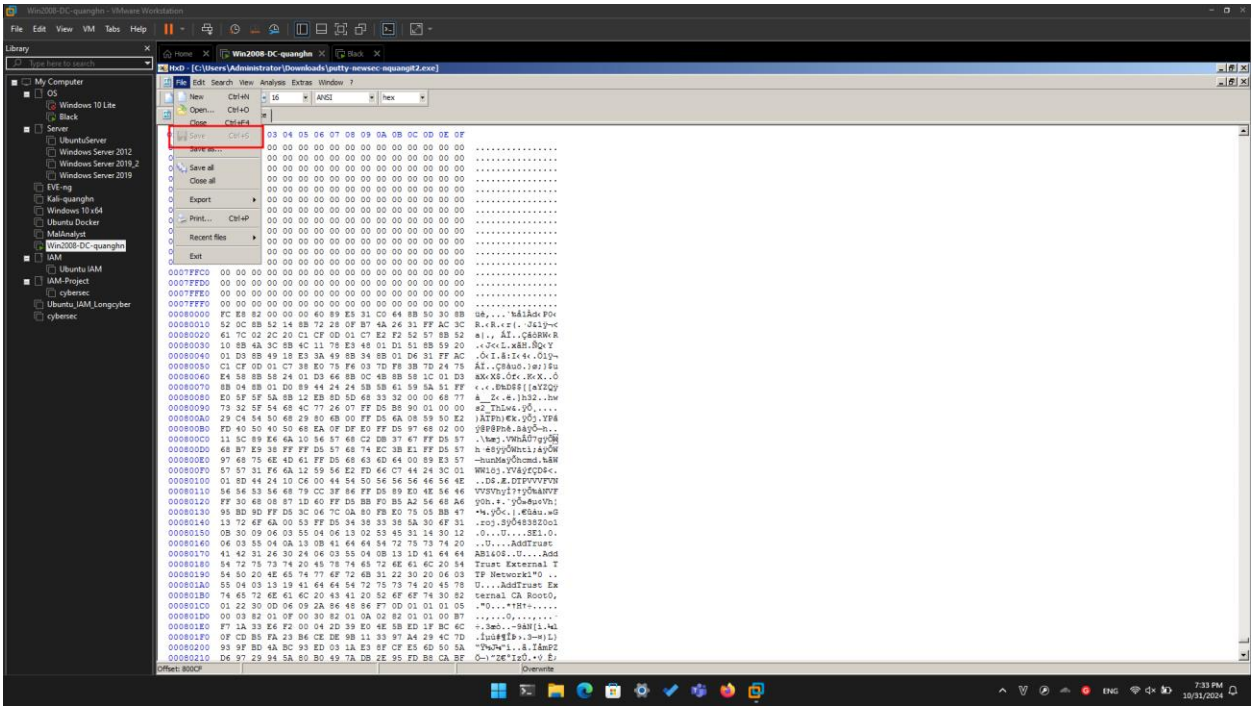
Above, on this Web page, highlight and copy the first set of shellcode bytes, from "29" through "d5".

In HxD, right-click the byte at address 000800A5 and click "**Paste write**". Your screen should look like the image below.









Running the Trojaned Putty

Double-click **putty-newsec-YOURNAME2.exe**.

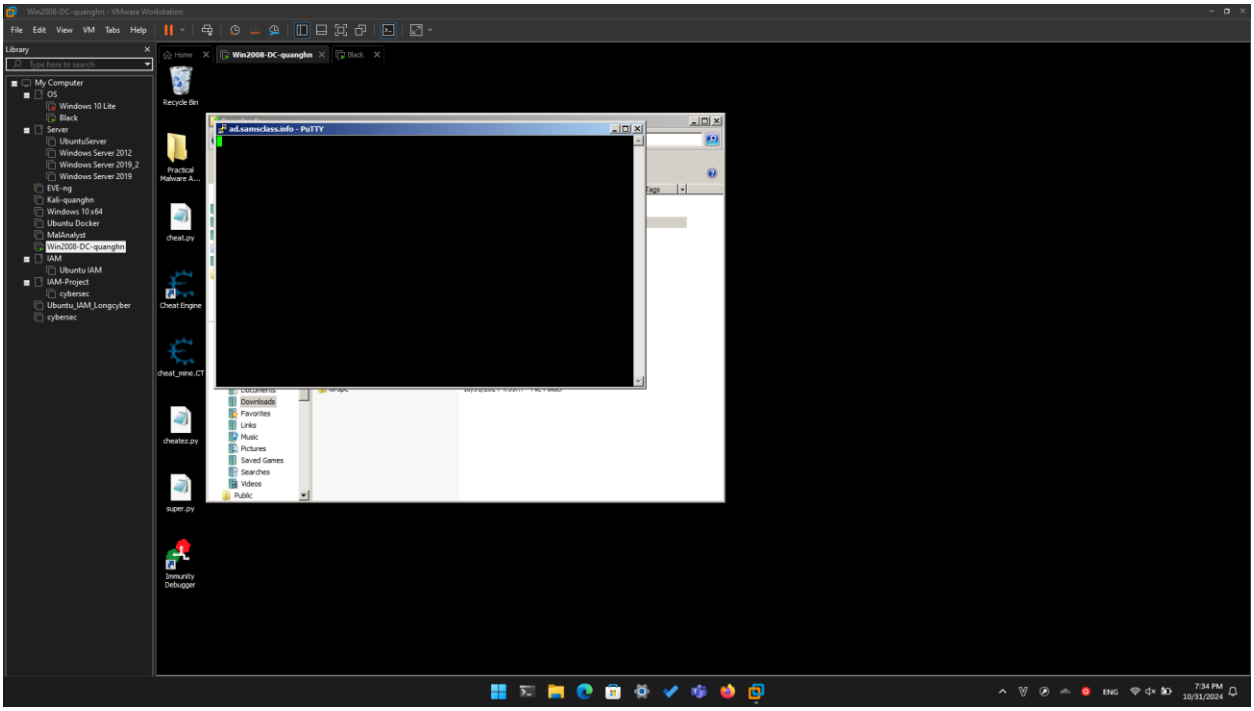
Putty opens. In the "Host Name (or IP address)" box, type

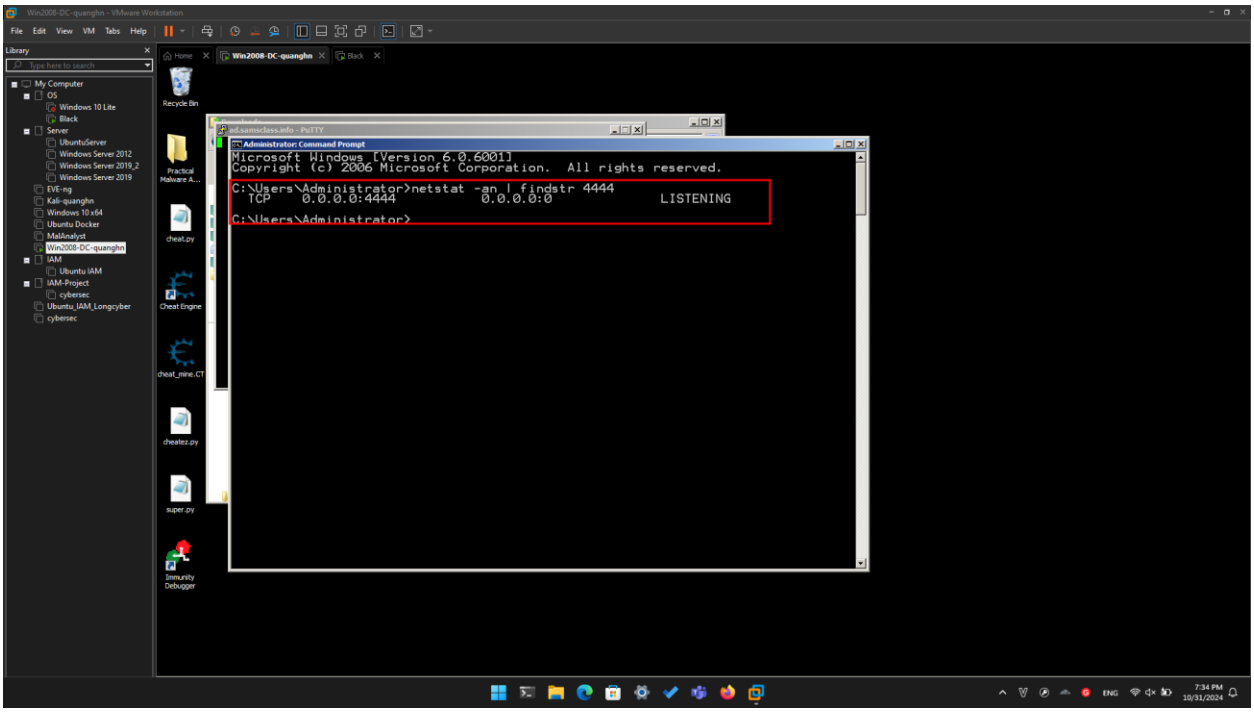
ad.samsclass.info

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

A black Putty window opens, but remains blank, as shown below.

This is because we were sloppy when inserting shellcode, and broke the normal operation of Putty.





Connecting to the Target

Open another Command Prompt window. Execute this command:

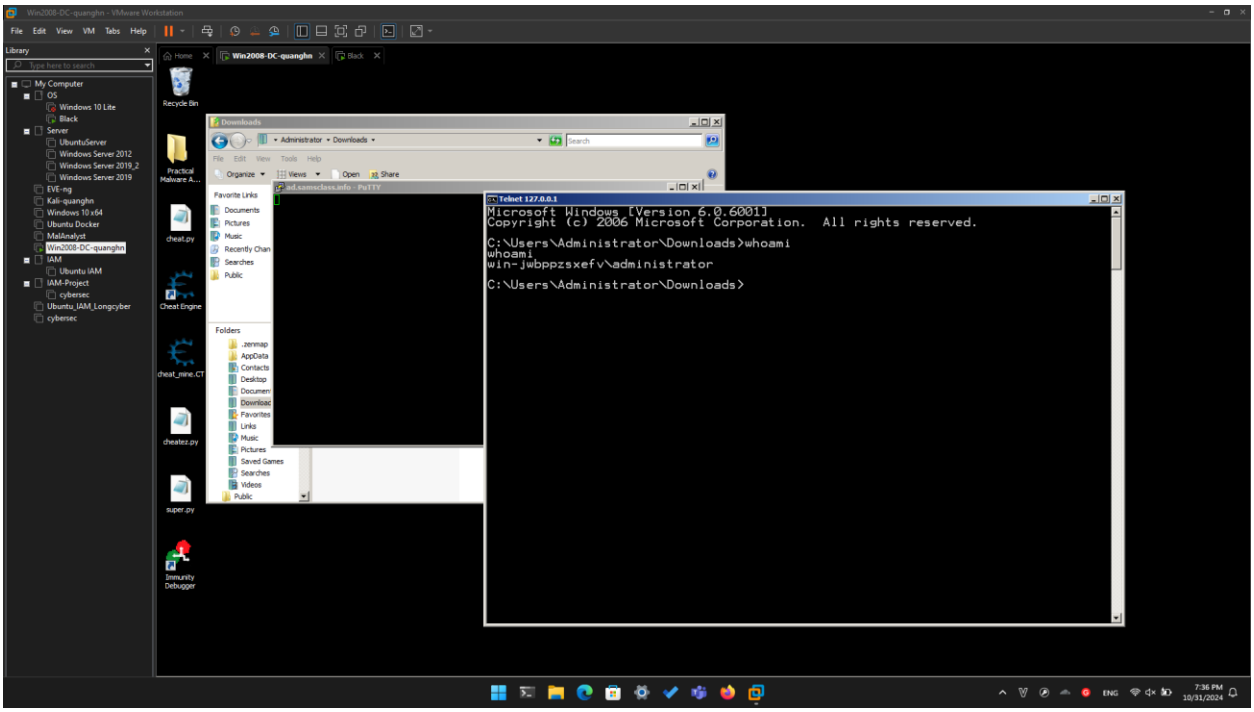
telnet 127.0.0.1 4444

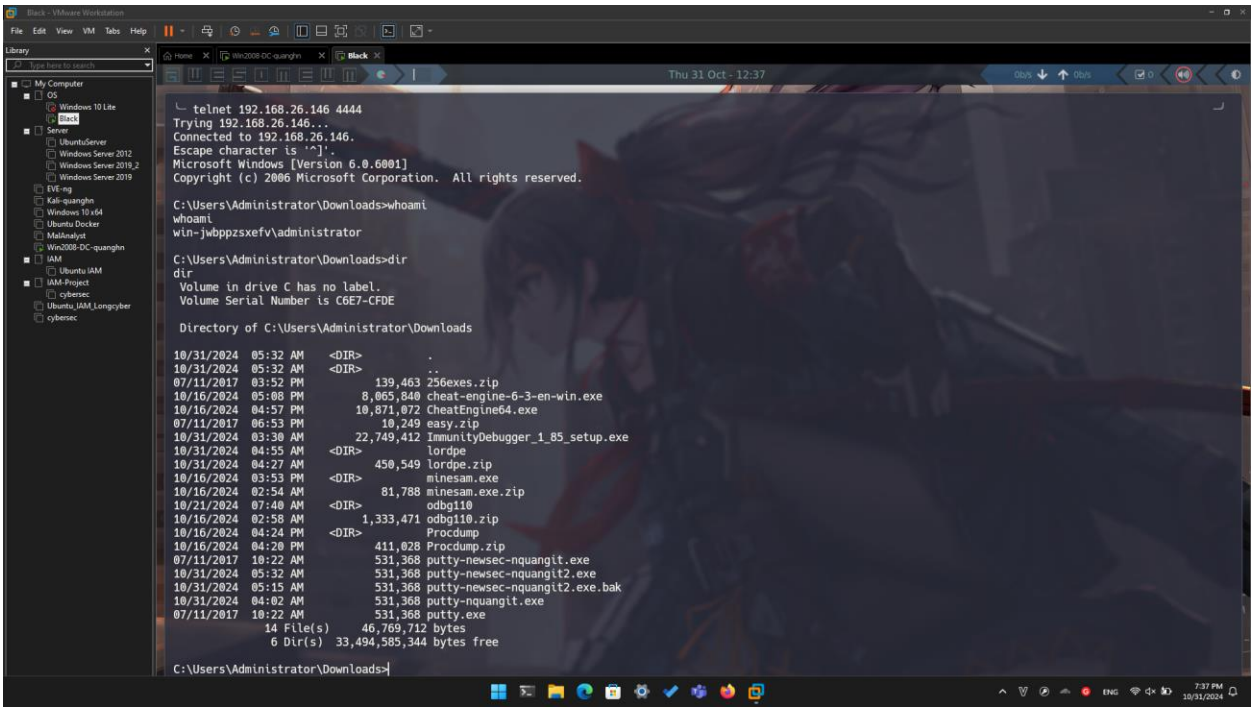
A Command Prompt opens, allowing you to execute commands on the server, as shown below.

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.




Black - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
OS
Windows 10 Lite
Black
Server
UbuntuServer
Windows Server 2012
Windows Server 2019_2
Windows Server 2019
EVE-ng
Kali-quanghn
Windows 10 x64
Ubuntu Docker
MalAnalyst
Win2008-DC-quanghn
IAM
Ubuntu IAM
IAM-Project
cybersec
Ubuntu_IAM_Longcyber
cybersec
Home
Win2008-DC-quanghn
Black
Thu 31 Oct - 12:37
└─ telnet 192.168.26.146 4444
Trying 192.168.26.146...
Connected to 192.168.26.146.
Escape character is '^]'.
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Administrator\Downloads>whoami
whoami
win-jwbppzsxefv\administrator
C:\Users\Administrator\Downloads>dir
dir
Volume in drive C has no label.
Volume Serial Number is C6E7-CFDE
Directory of C:\Users\Administrator\Downloads
10/31/2024 05:32 AM <DIR> .
10/31/2024 05:32 AM <DIR> ..
07/11/2017 03:52 PM 139,463 256exes.zip
10/16/2024 05:08 PM 8,065,840 cheat-engine-6-3-en-win.exe
10/16/2024 04:57 PM 10,871,072 CheatEngine64.exe
07/11/2017 06:53 PM 10,249 easy.zip
10/31/2024 03:30 AM 22,749,412 ImmunityDebugger_1_85_setup.exe
10/31/2024 04:55 AM <DIR> lordpe
10/31/2024 04:27 AM 450,549 lordpe.zip
10/16/2024 03:53 PM <DIR> minesam.exe
10/16/2024 02:54 AM 81,788 minesam.exe.zip
10/21/2024 07:40 AM <DIR> odbg110
10/16/2024 02:58 AM 1,333,471 odbg110.zip
10/16/2024 04:24 PM <DIR> Procdump
10/16/2024 04:20 PM 411,028 Procdump.zip
07/11/2017 10:22 AM 531,368 putty-newsec-nquangit.exe
10/31/2024 05:32 AM 531,368 putty-newsec-nquangit2.exe
10/31/2024 05:15 AM 531,368 putty-newsec-nquangit2.exe.bak
10/31/2024 04:02 AM 531,368 putty-nquangit.exe
07/11/2017 10:22 AM 531,368 putty.exe
14 File(s) 46,769,712 bytes
6 Dir(s) 33,494,585,344 bytes free
C:\Users\Administrator\Downloads>
ENG
7:37 PM
10/31/2024