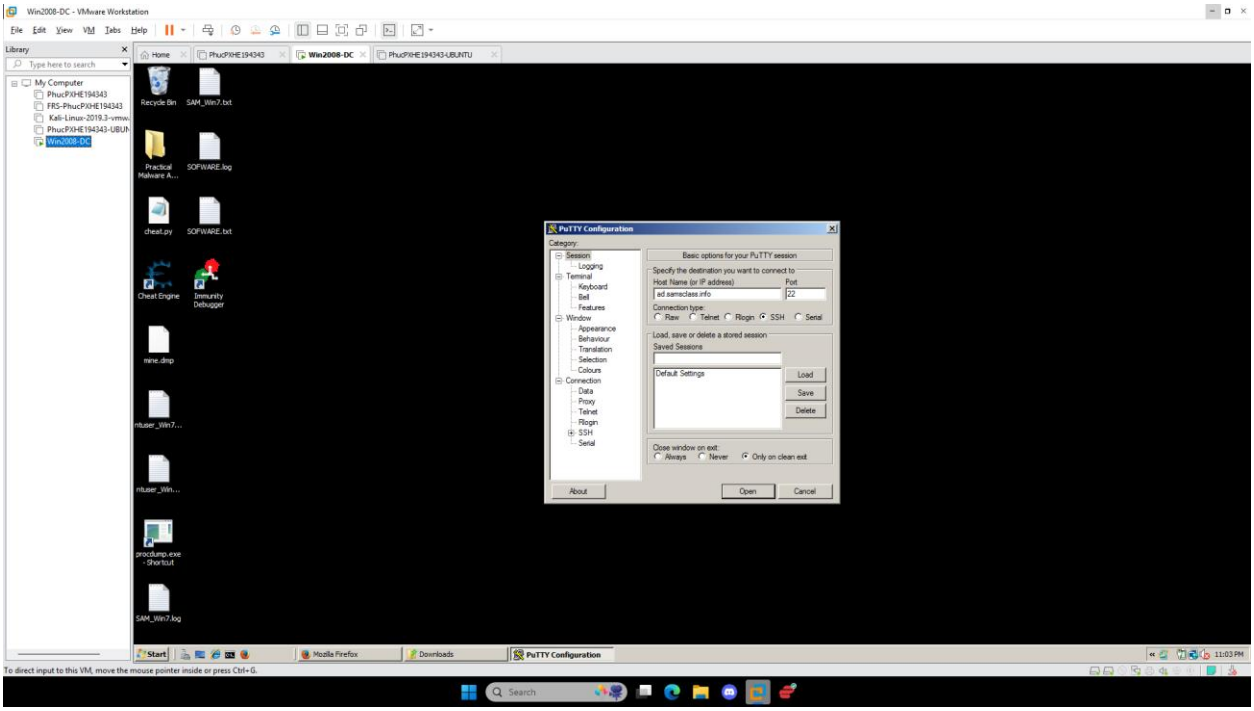
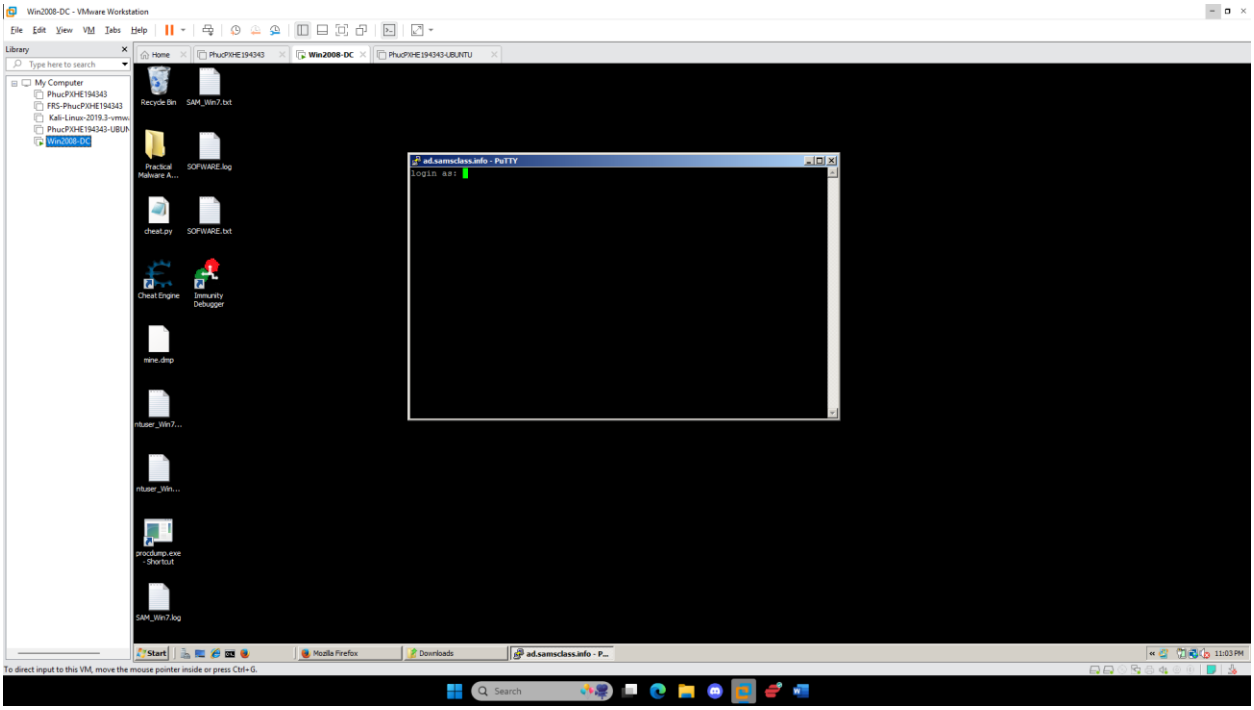
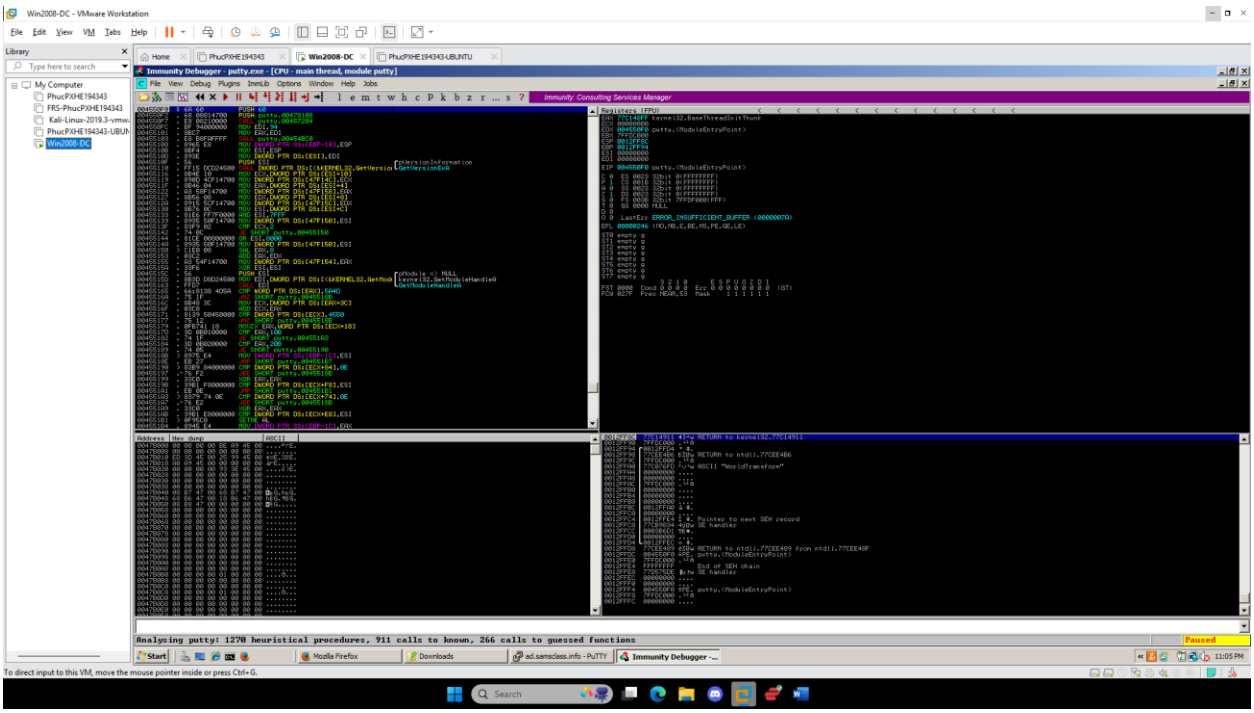
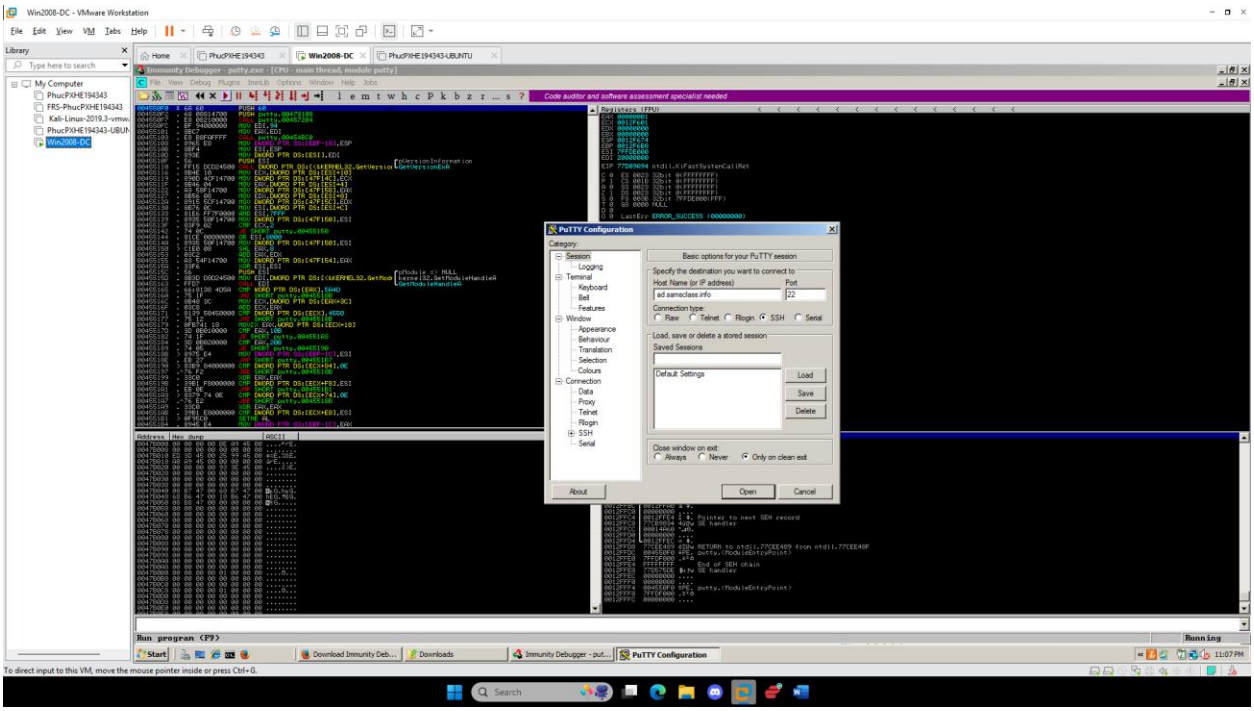
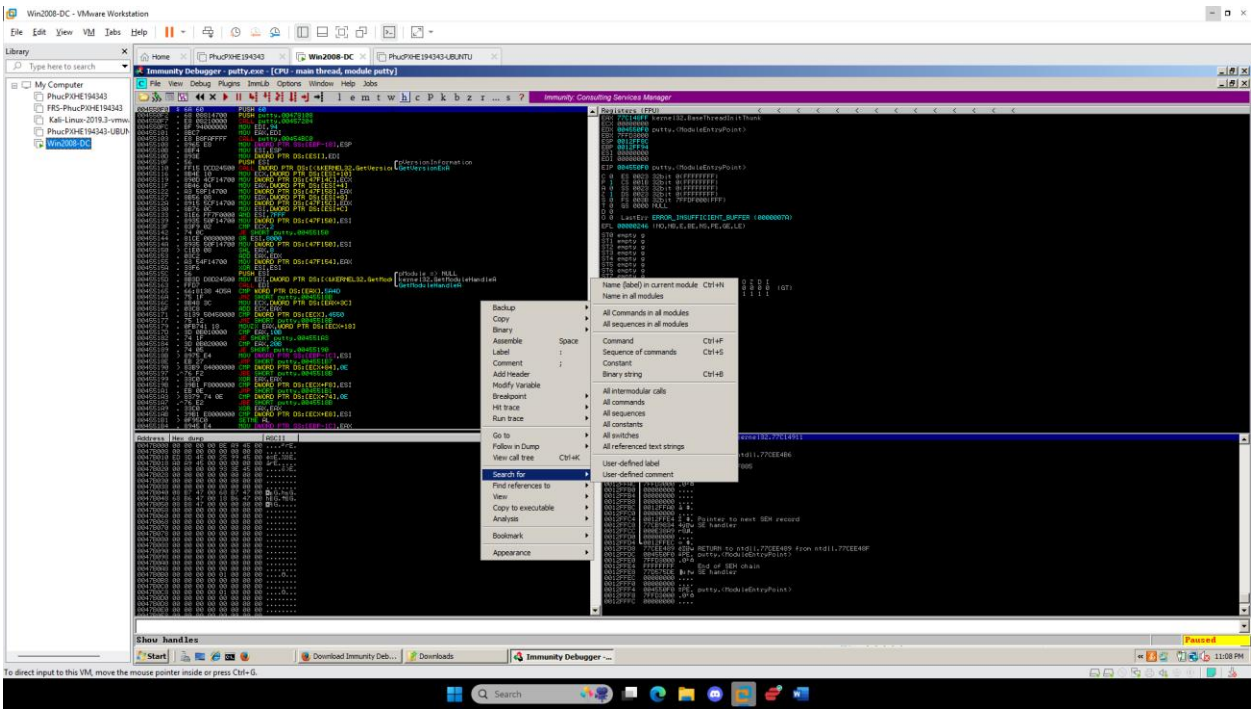
LAB 19

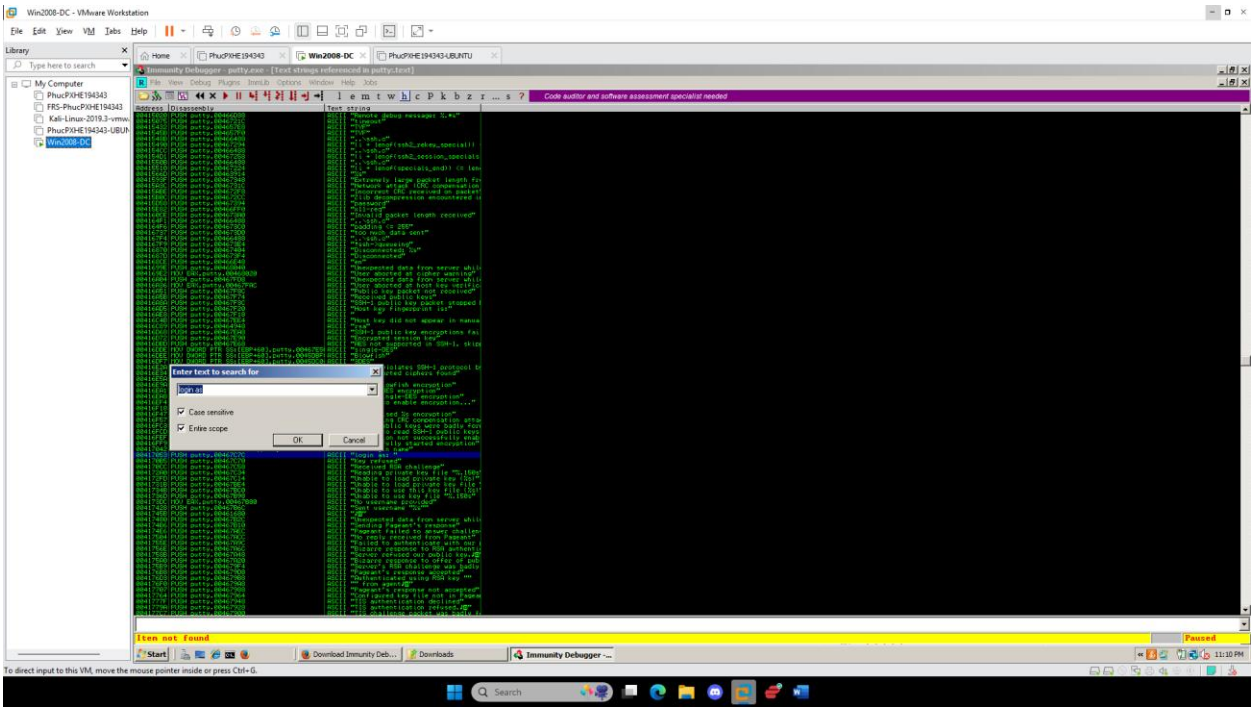

Win2008-DC - VMware Workstation
PuTTY Configuration
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
ad.samsclass.info
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

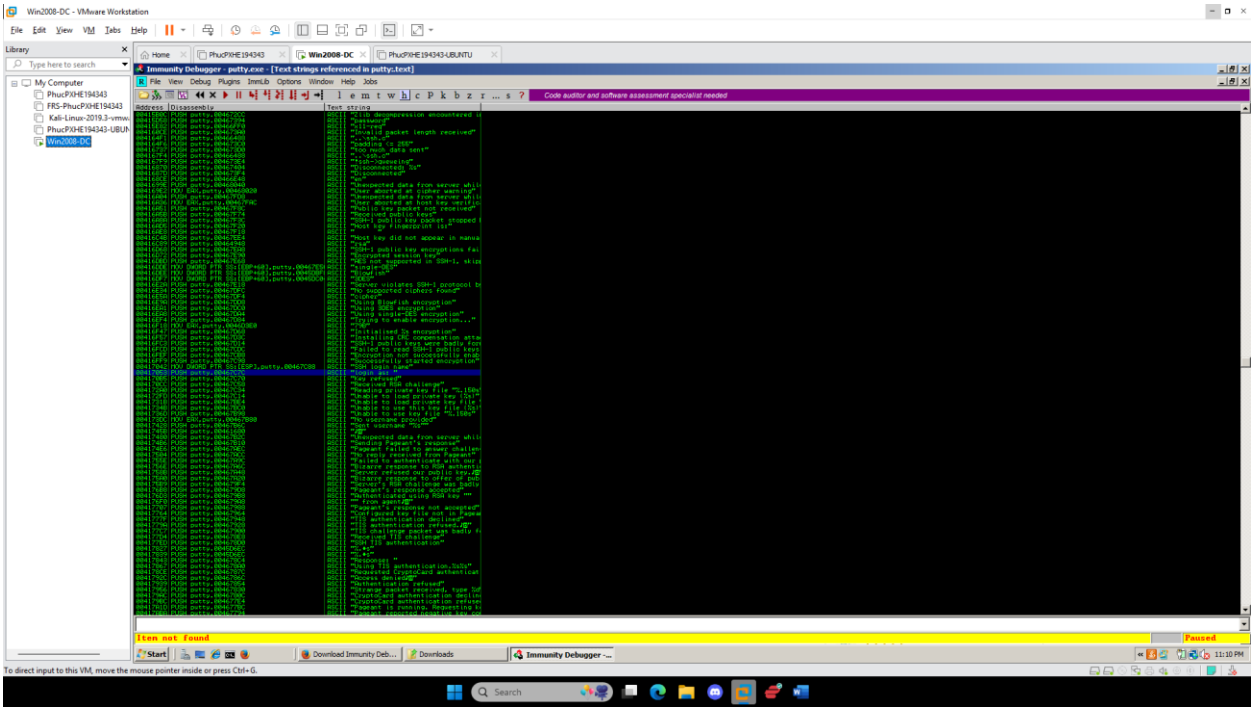

Win2008-DC - VMware Workstation
ad.samsclass.info - PuTTY
login as:

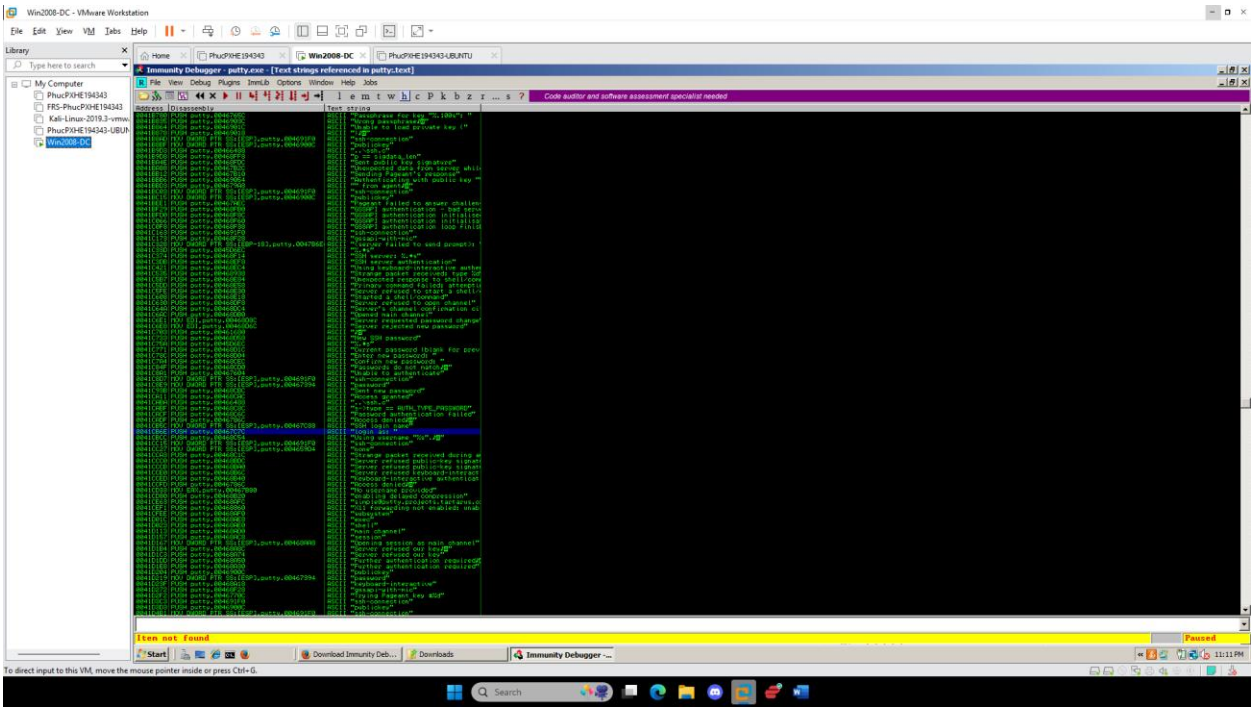

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
Analysing putty: 1270 heuristical procedures, 911 calls to known, 266 calls to guessed functions
Paused

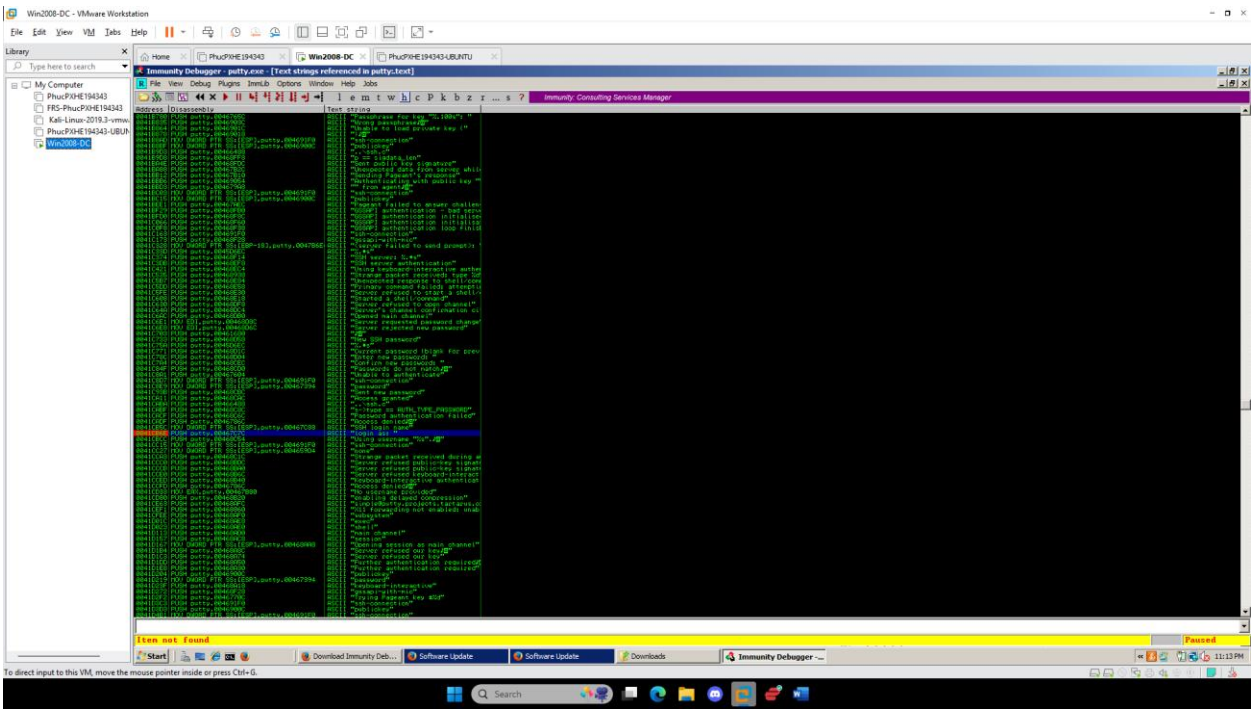

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
PuTTY Configuration
Run program (F9)
Running

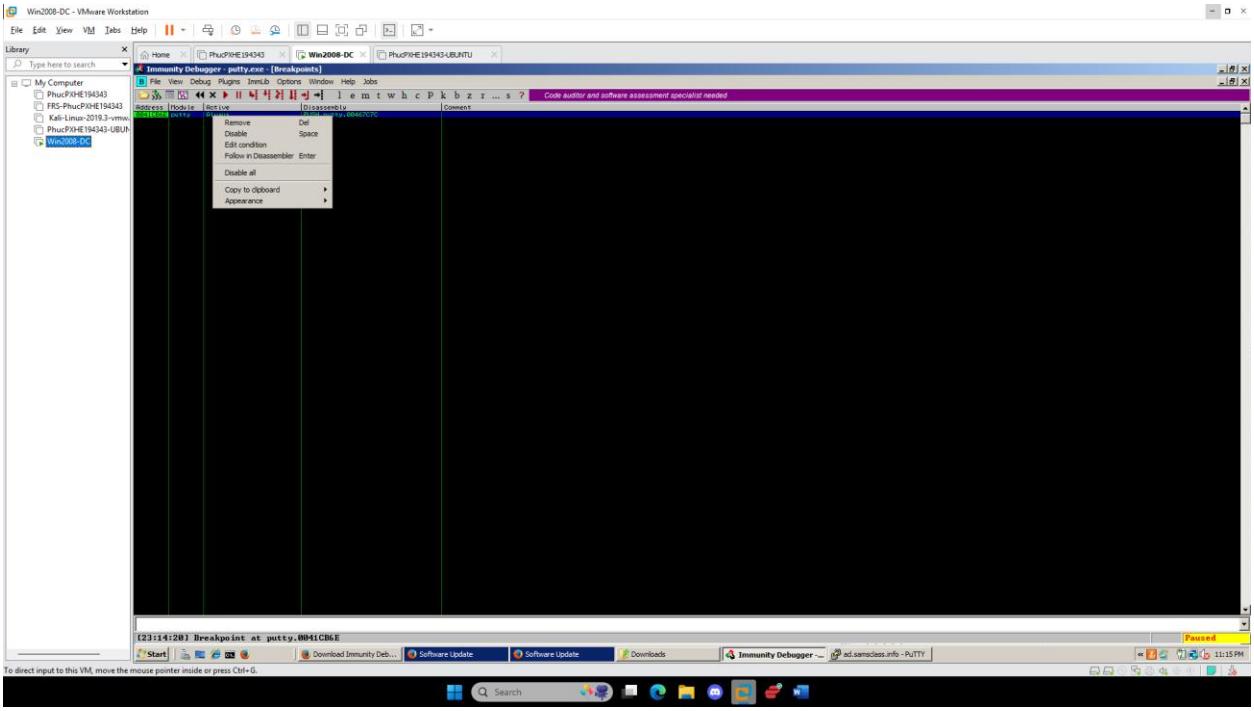

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
Search for
Find references to
Enter text to search for
Case sensitive
Entire scope
OK
Cancel
Show handles
Paused

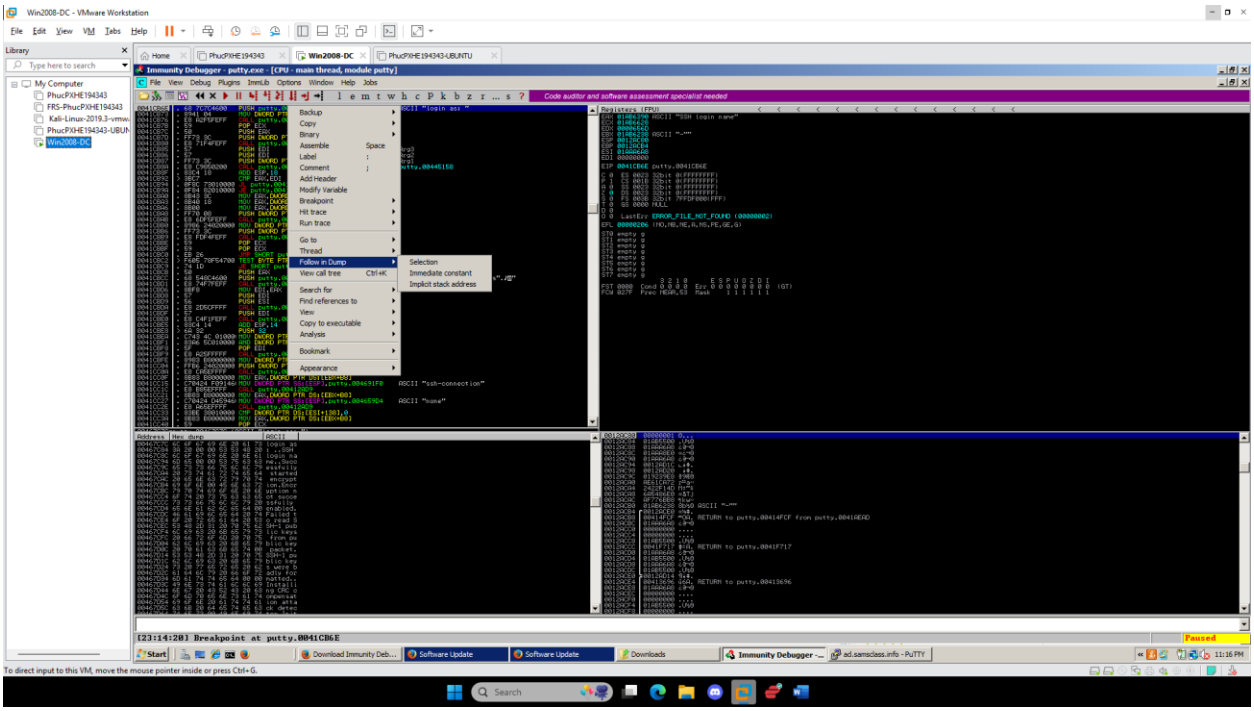

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [Text strings referenced in putty.text]
Enter text to search for
Case sensitive
Entire scope
OK
Cancel
Item not found
Paused

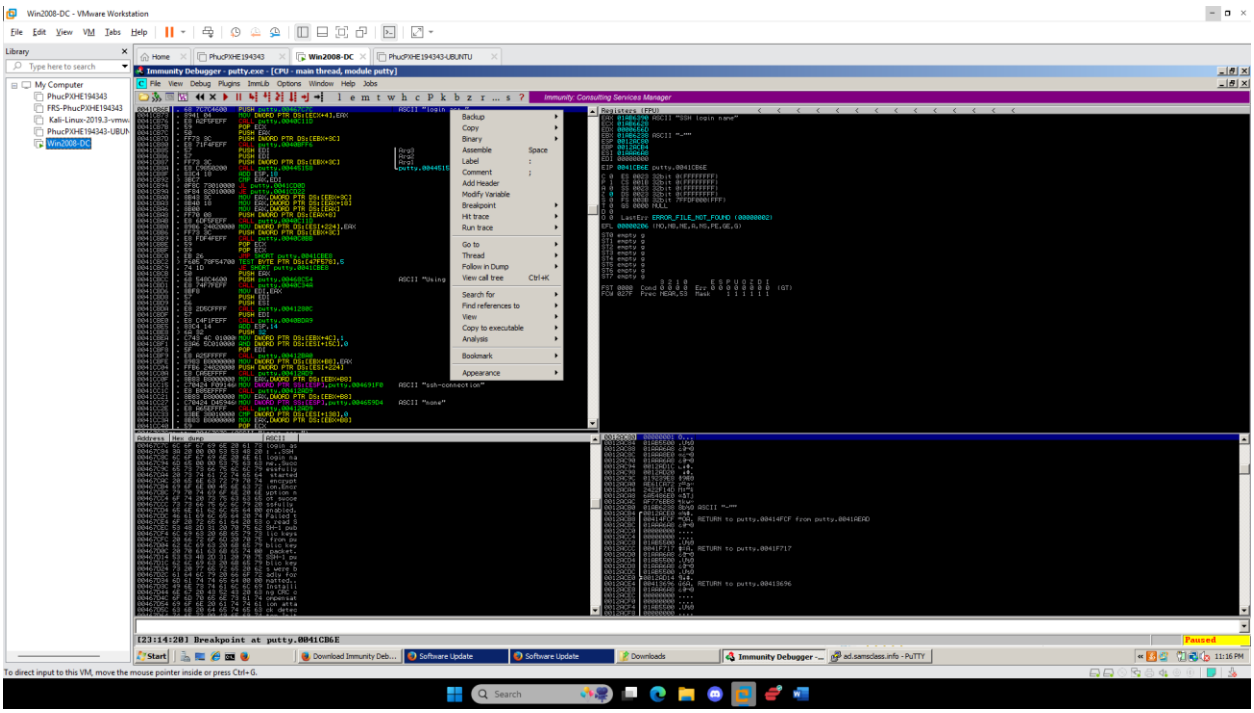

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [Text strings referenced in putty.text]
Item not found
Paused

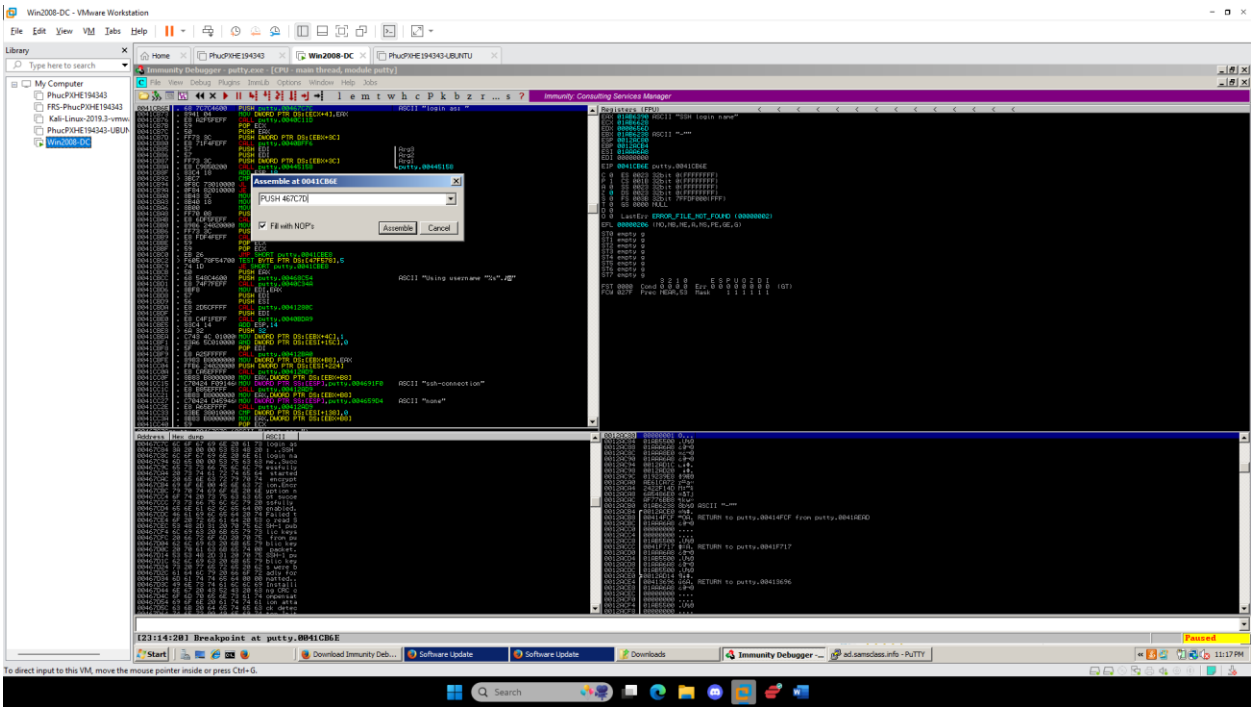

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [Text strings referenced in putty.text]
Item not found
Paused

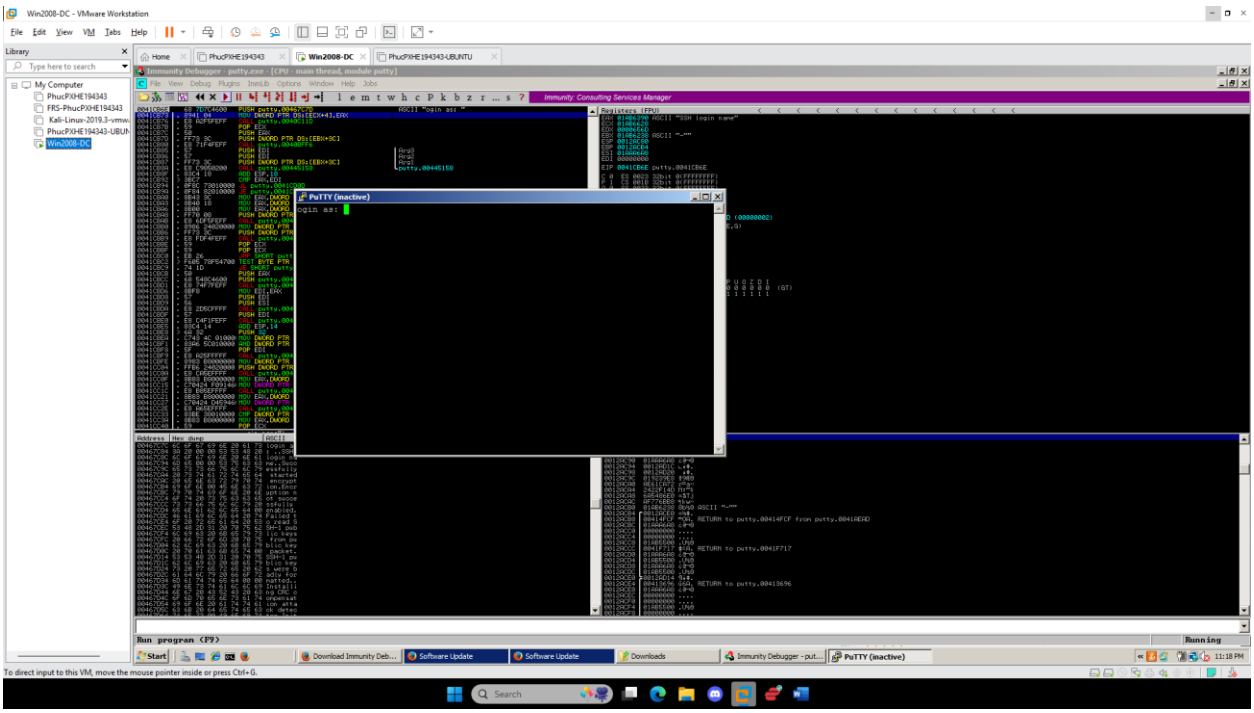

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [Text strings referenced in putty.text]
Item not found
Paused
Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
[23:14:20] Breakpoint at putty.0041CB6E
Paused

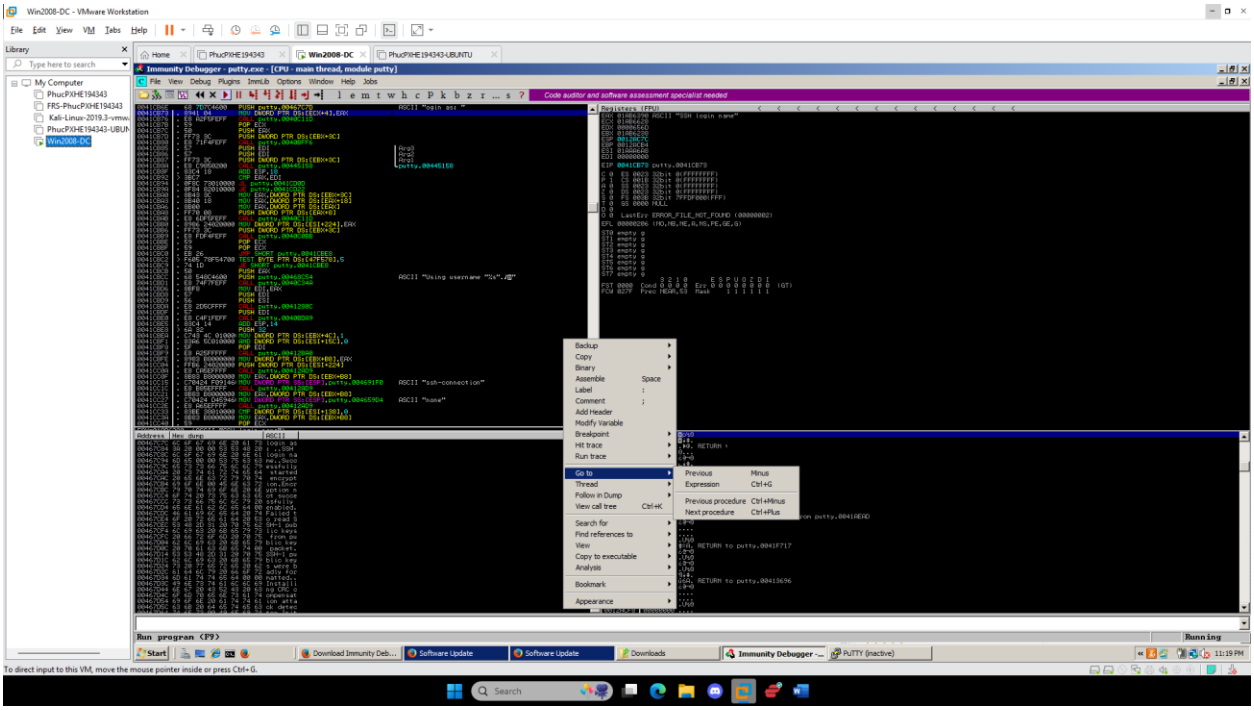

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [Breakpoints]
[23:14:20] Breakpoint at putty.0041CB6E
Paused

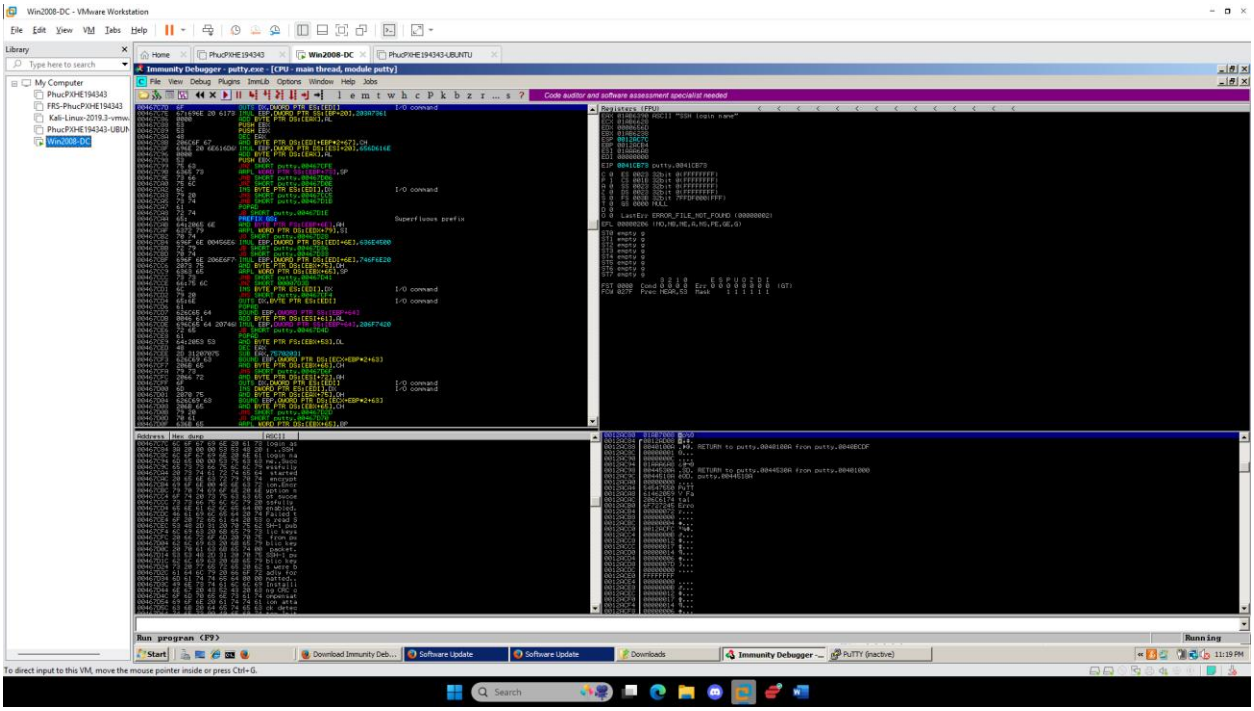

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
[23:14:20] Breakpoint at putty.0041CB6E
Paused

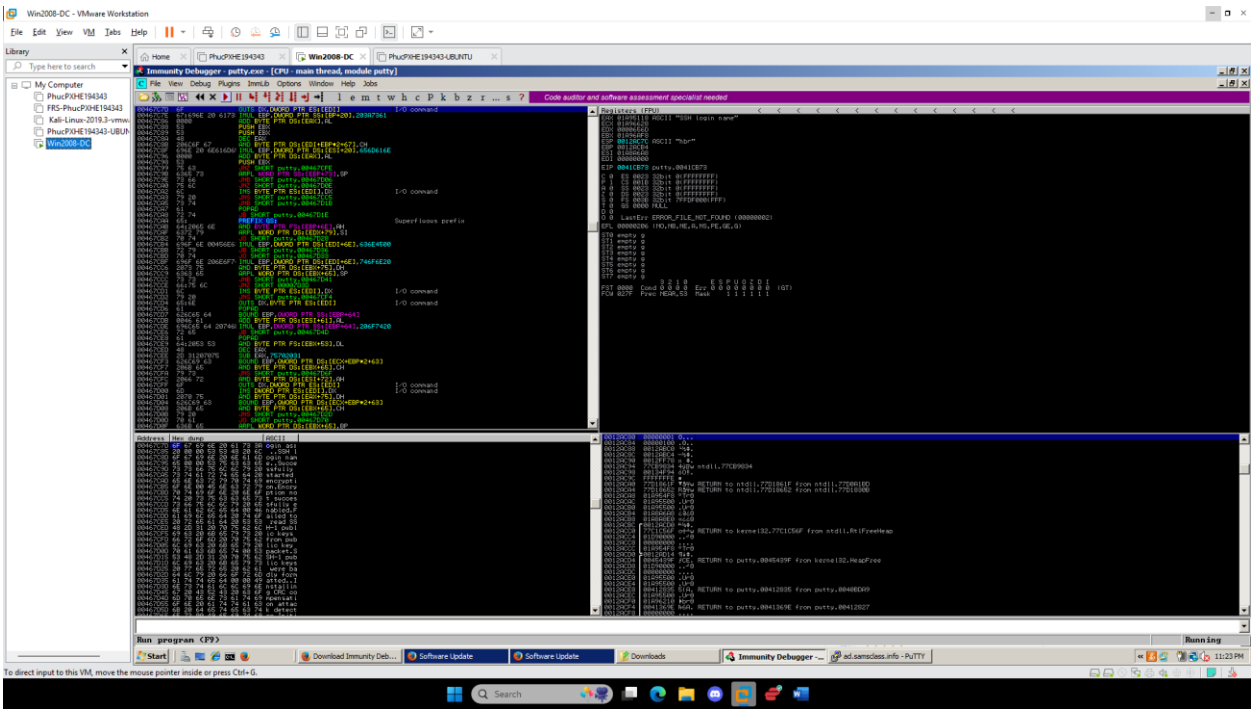

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
Backup
Copy
Binary
Assemble Space
Label :
Comment ;
Add Header
Modify Variable
Breakpoint
Hit trace
Run trace
Go to
Thread
Follow in Dump
View call tree Ctrl+K
Search for
Find references to
View
Copy to executable
Analysis
Bookmark
Appearance
[23:14:20] Breakpoint at putty.0041CB6E
Paused

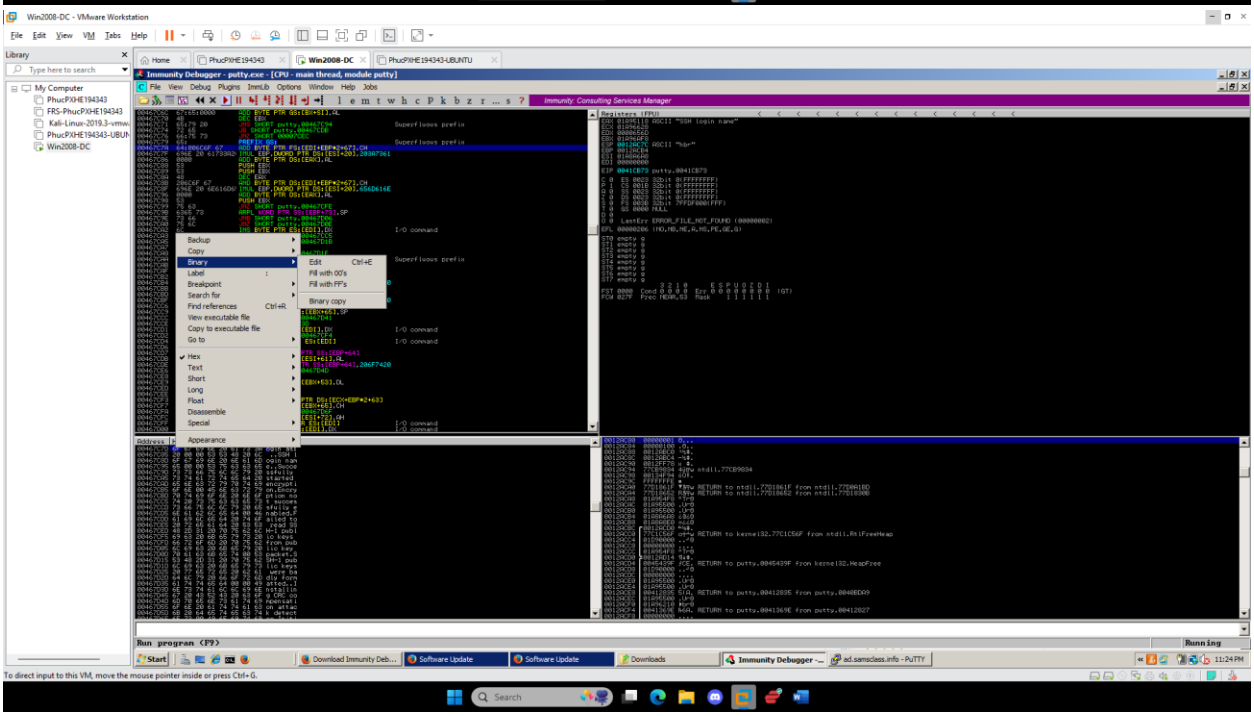

Win2008-DC - VMware Workstation
Assemble at 0041CB6E
PUSH 467C7D
Fill with NOP's
Assemble
Cancel
[23:14:20] Breakpoint at putty.0041CB6E
Paused

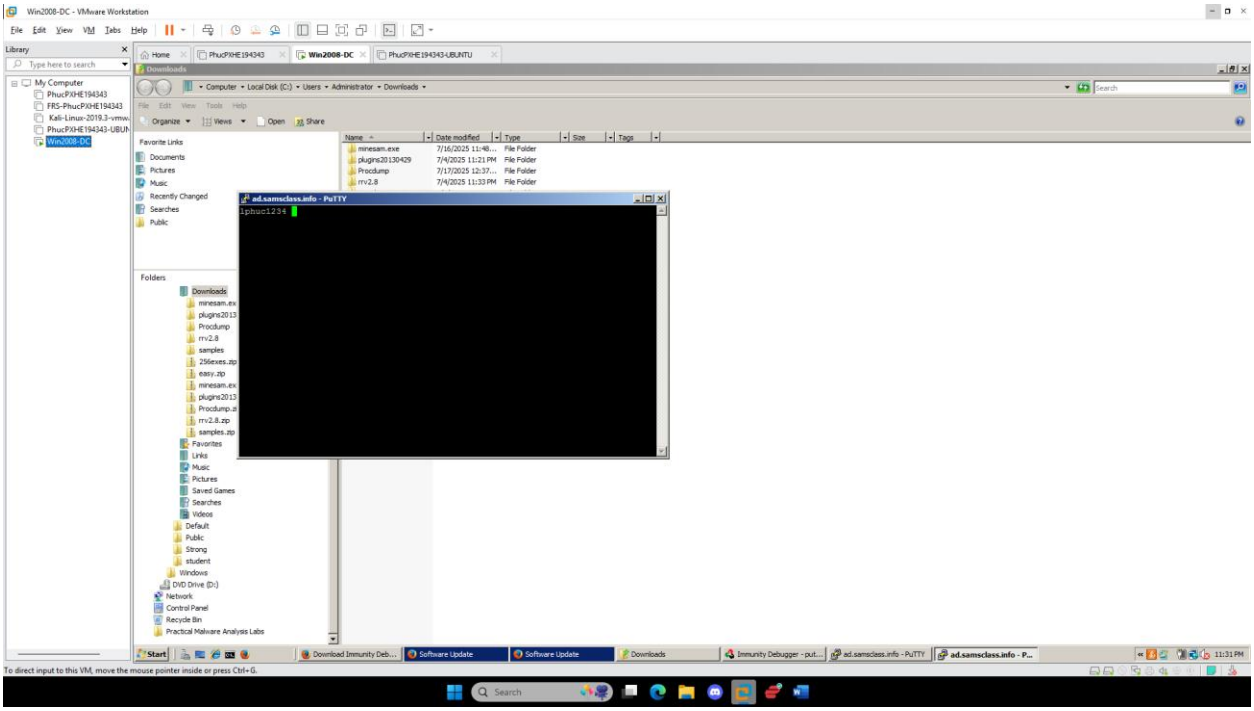

Win2008-DC - VMware Workstation
PuTTY (inactive)
login as:
Run program (F9)

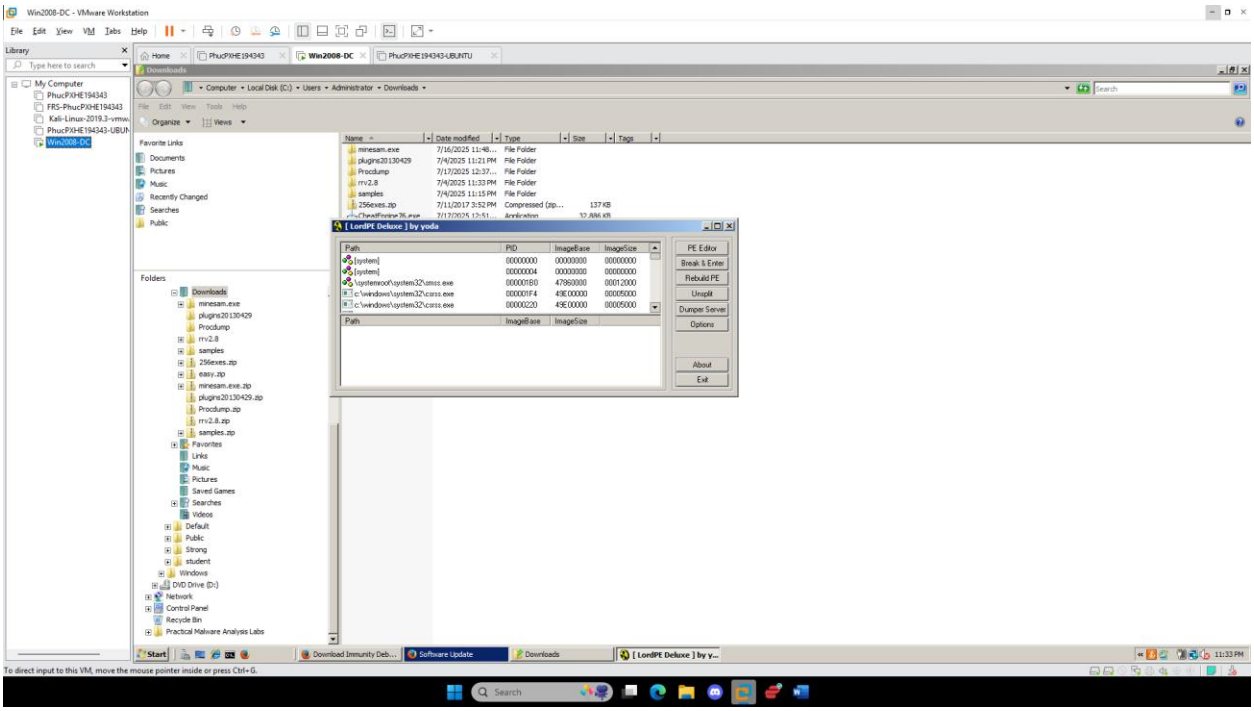

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
Run program (F9)

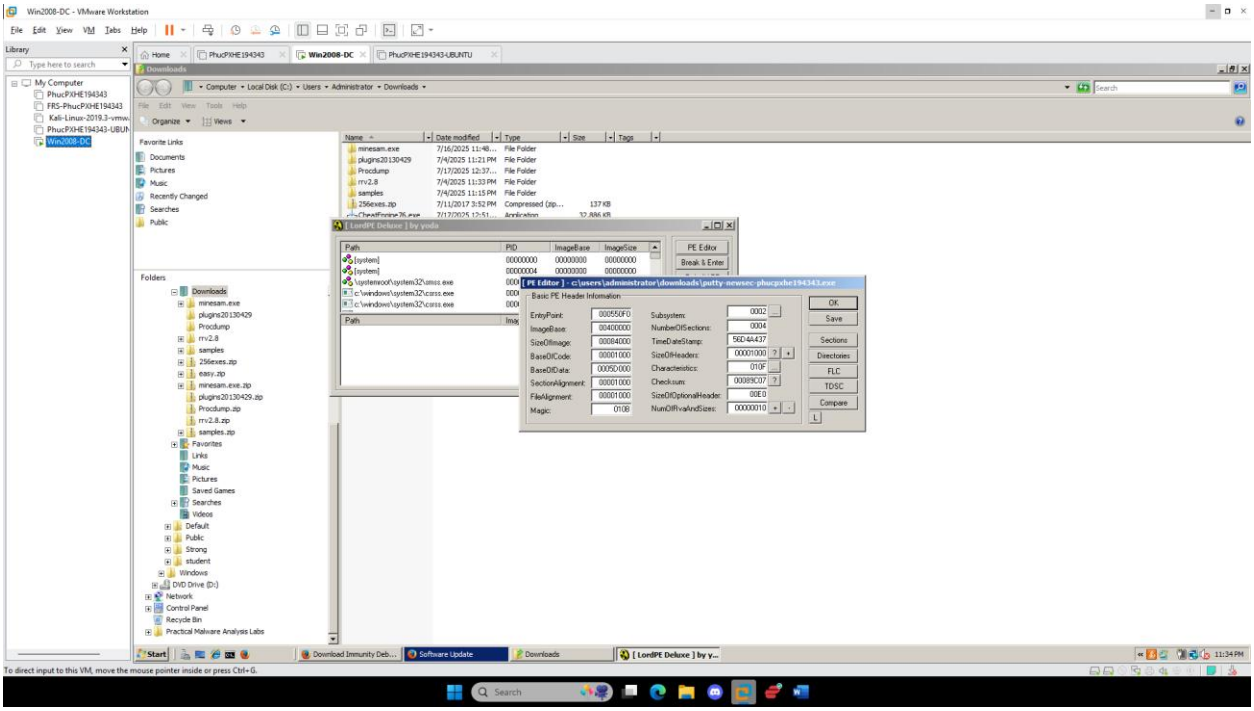

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
Code auditor and software assessment specialist needed
Run program (F9)
Running

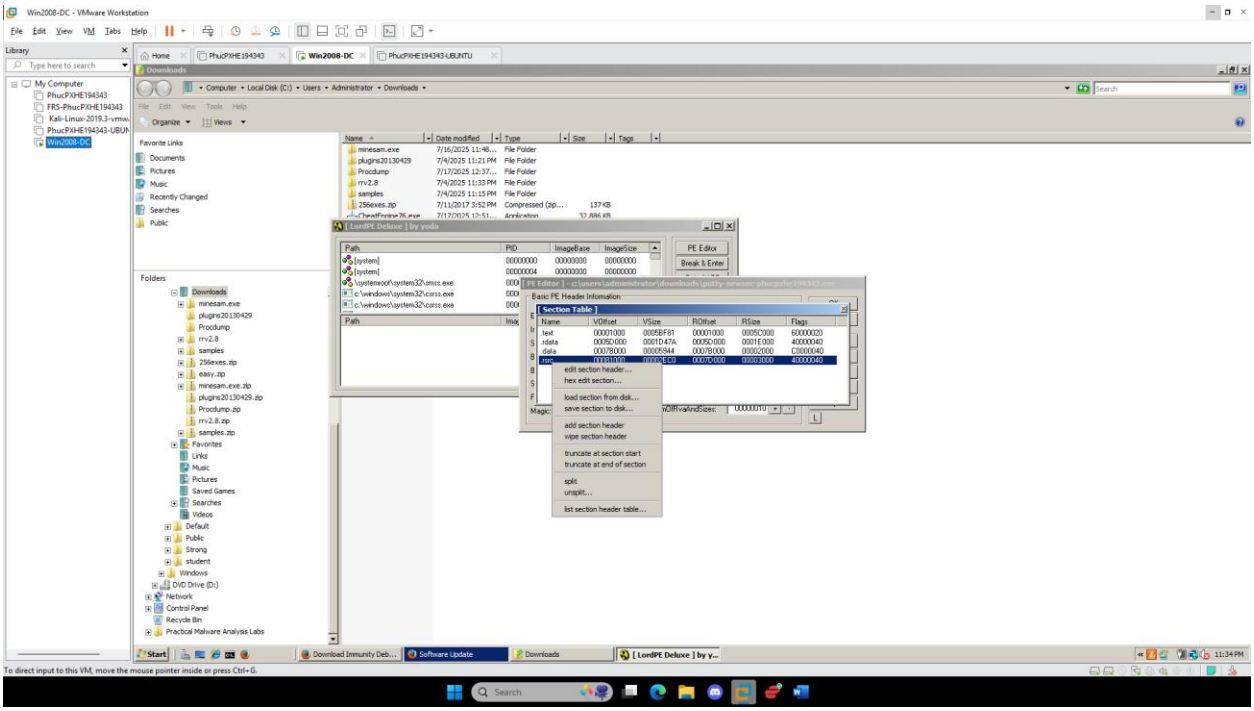

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
Run program (F9)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

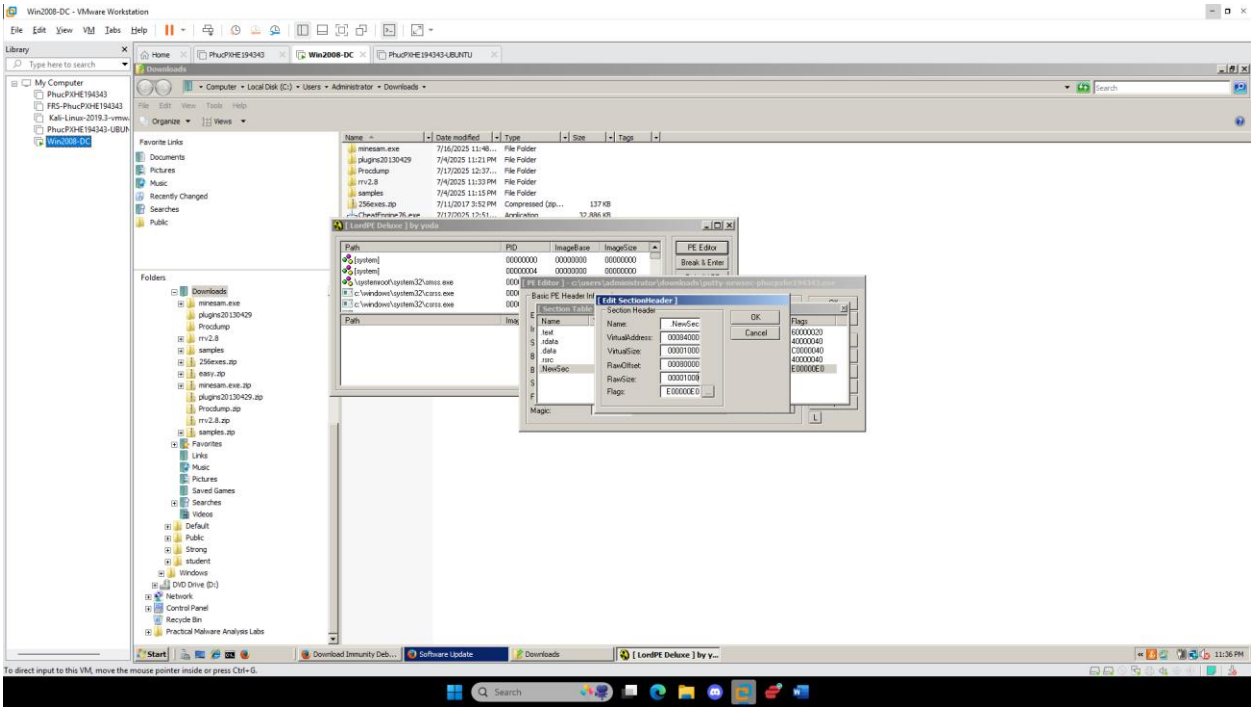

Win2008-DC - VMware Workstation
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
Run program (F9)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

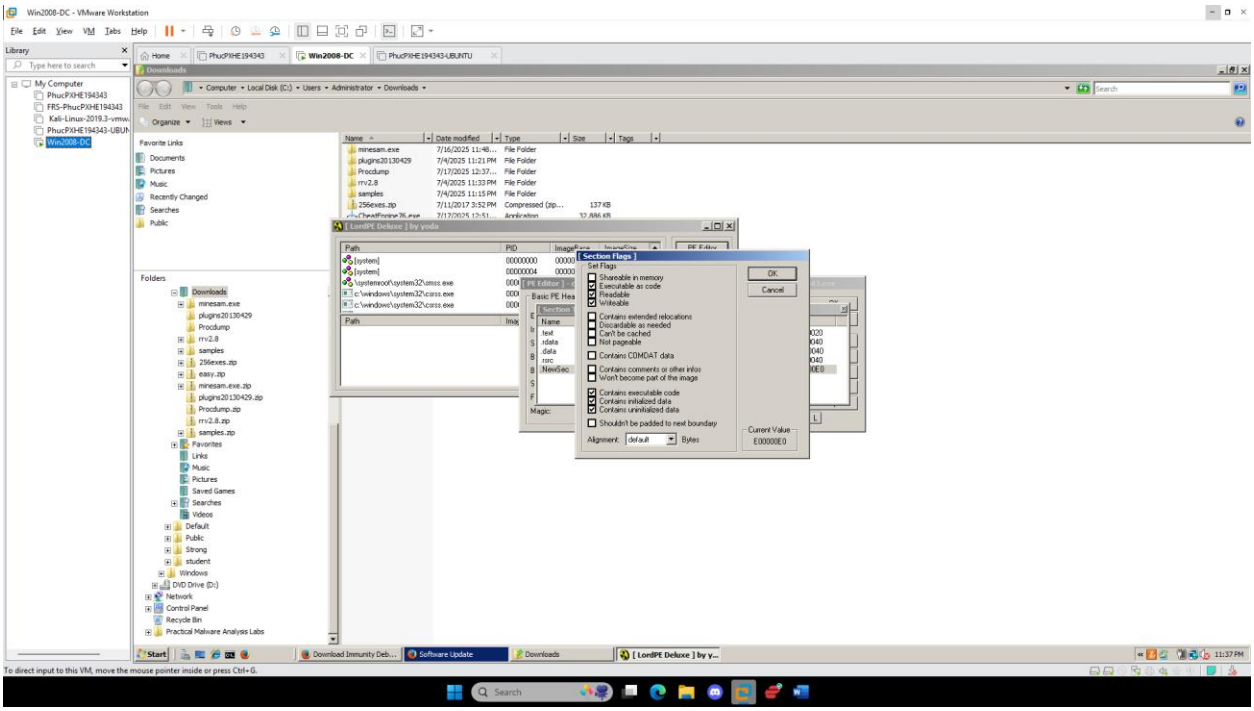

Win2008-DC - VMware Workstation
ad.samsclass.info - PuTTY
lphuc1234
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

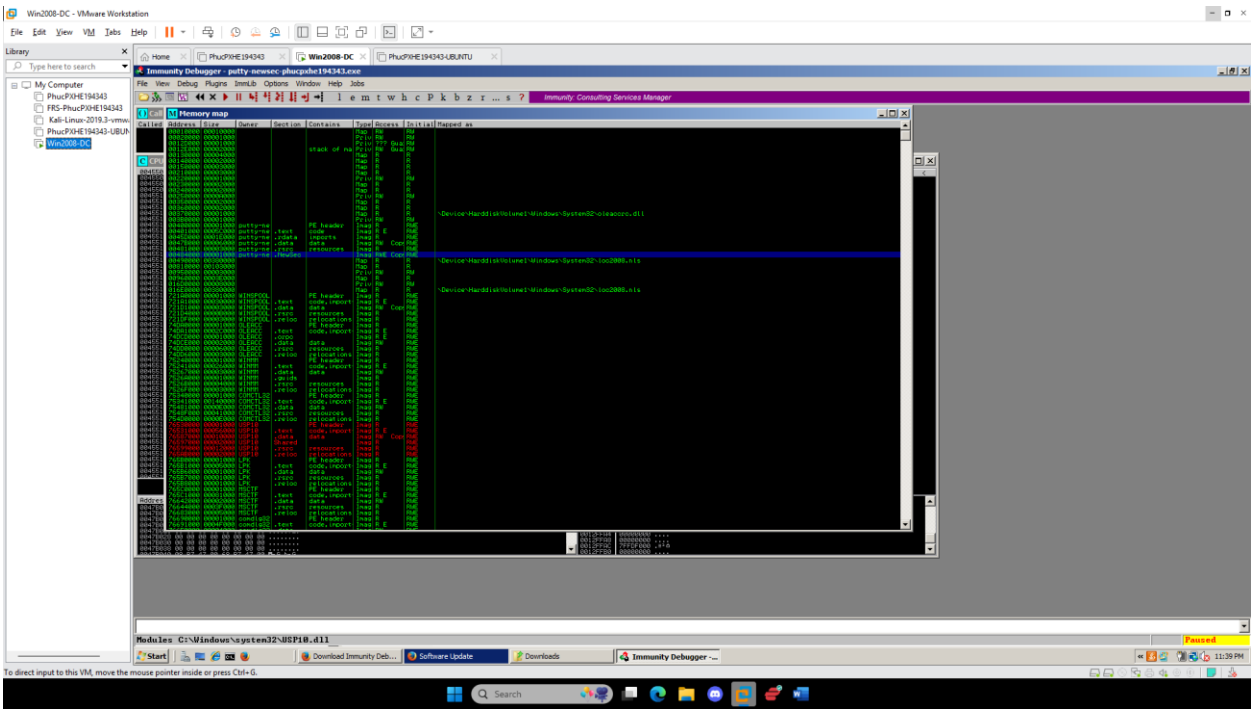

Win2008-DC - VMware Workstation
[LordPE Deluxe] by yoda
PE Editor
Break & Enter
Rebuild PE
Unspli
Dumper Server
Options
About
Exit
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

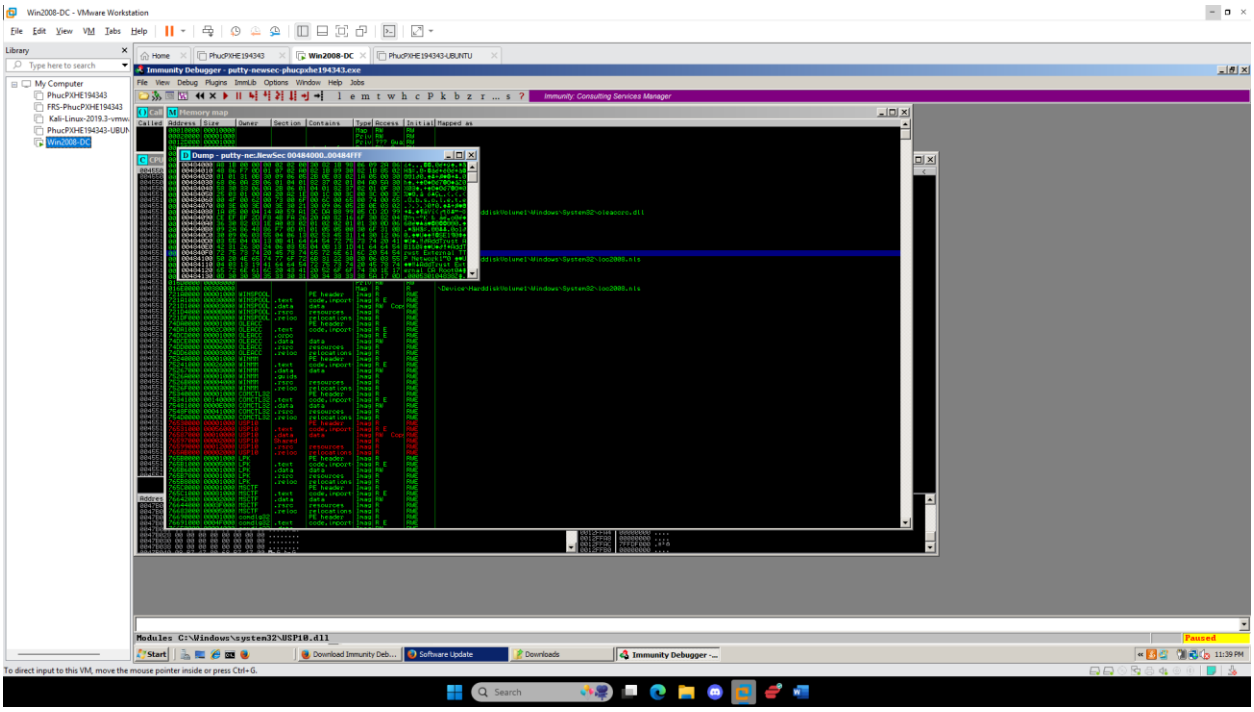

Win2008-DC - VMware Workstation
[LordPE Deluxe] by yoda
PE Editor
Break & Enter
PE Editor] - c:\users\administrator\downloads\putty-newsec-phucpxhe194343.exe
Basic PE Header Information
OK
Save
Sections
Directories
FLC
TDSC
Compare

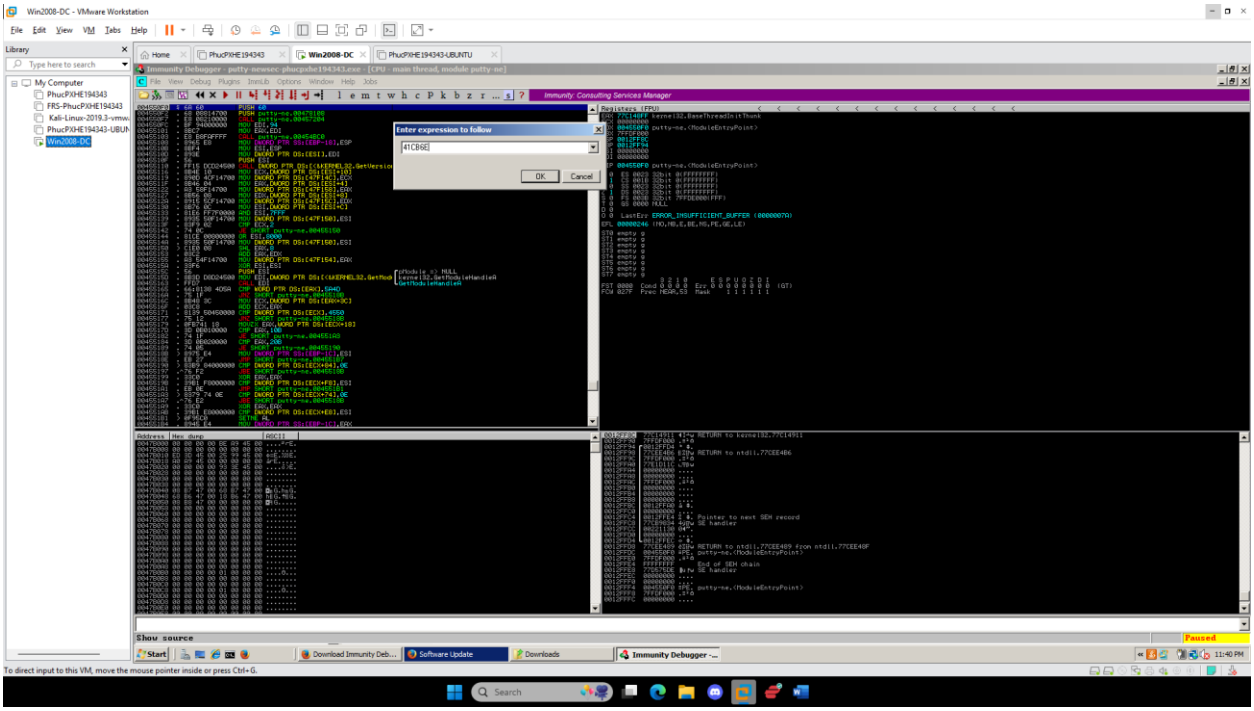

Win2008-DC - VMware Workstation
[LordPE Deluxe] by yoda
PE Editor
Break & Enter
Section Table
edit section header...
hex edit section...
load section from disk...
save section to disk...
add section header
wipe section header
truncate at section start
truncate at end of section
split
unsplit...
list section header table...

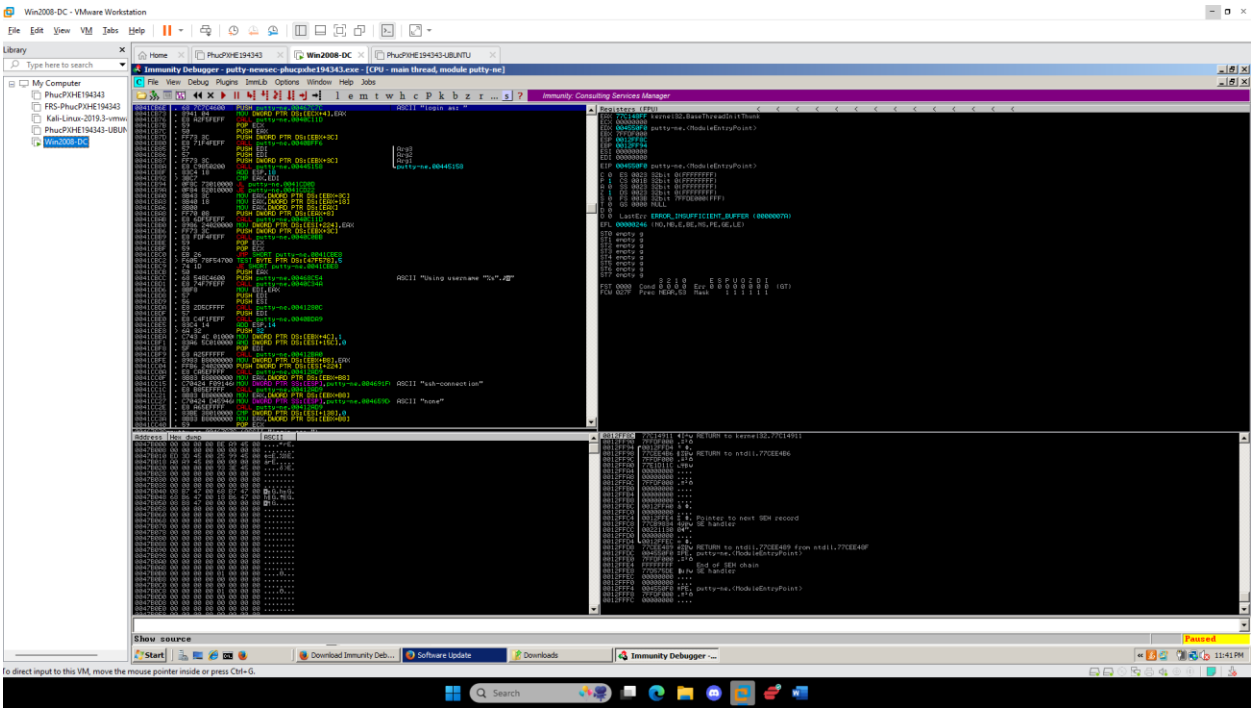

Win2008-DC - VMware Workstation
[LordPE Deluxe] by yoda
Edit SectionHeader
Name: NewSec
VirtualAddress: 00084000
VirtualSize: 00001000
RawOffset: 00080000
RawSize: 00001000
Flags: E00000E0
OK
Cancel

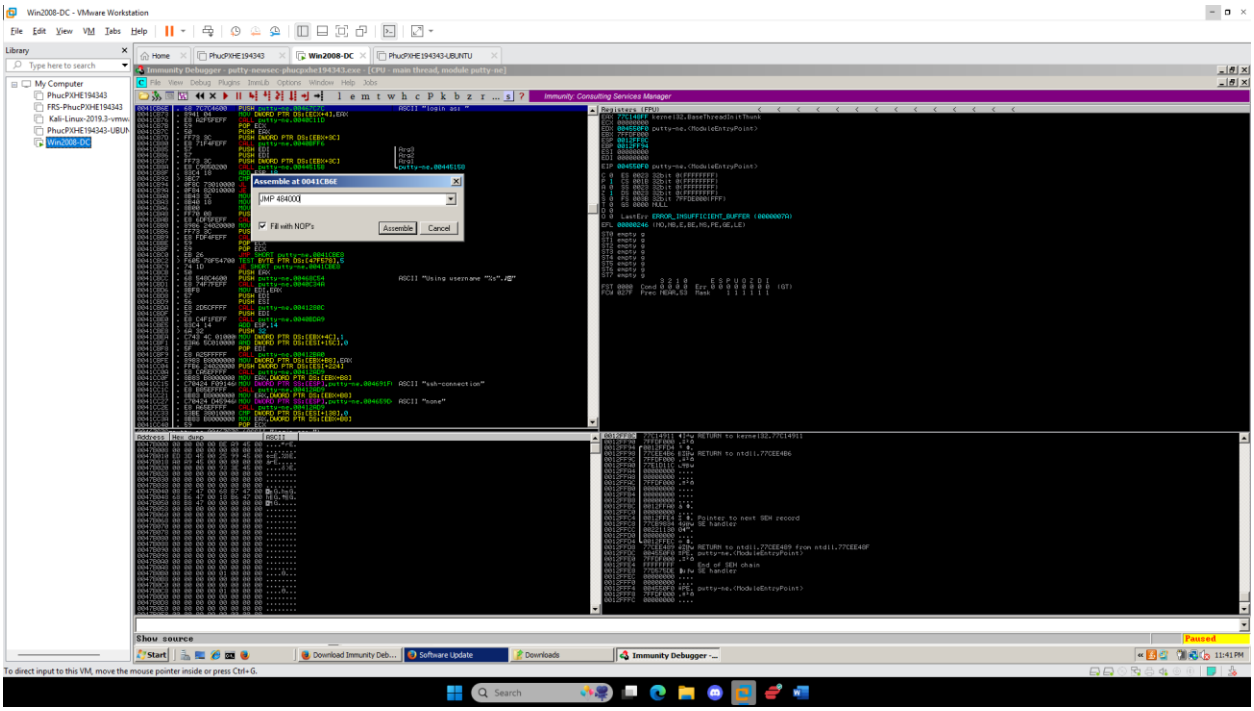

Win2008-DC - VMware Workstation
[LordPE Deluxe] by yoda
Section Flags
Set Flags
Shareable in memory
Executable as code
Readable
Writeable
Contains extended relocations
Discardable as needed
Can't be cached
Not pageable
Contains COMDAT data
Contains comments or other infos
Won't become part of the image
Contains executable code
Contains initialized data
Contains uninitialized data
Shouldn't be padded to next boundary
Alignment: default
Bytes
Current Value
E00000E0
OK
Cancel

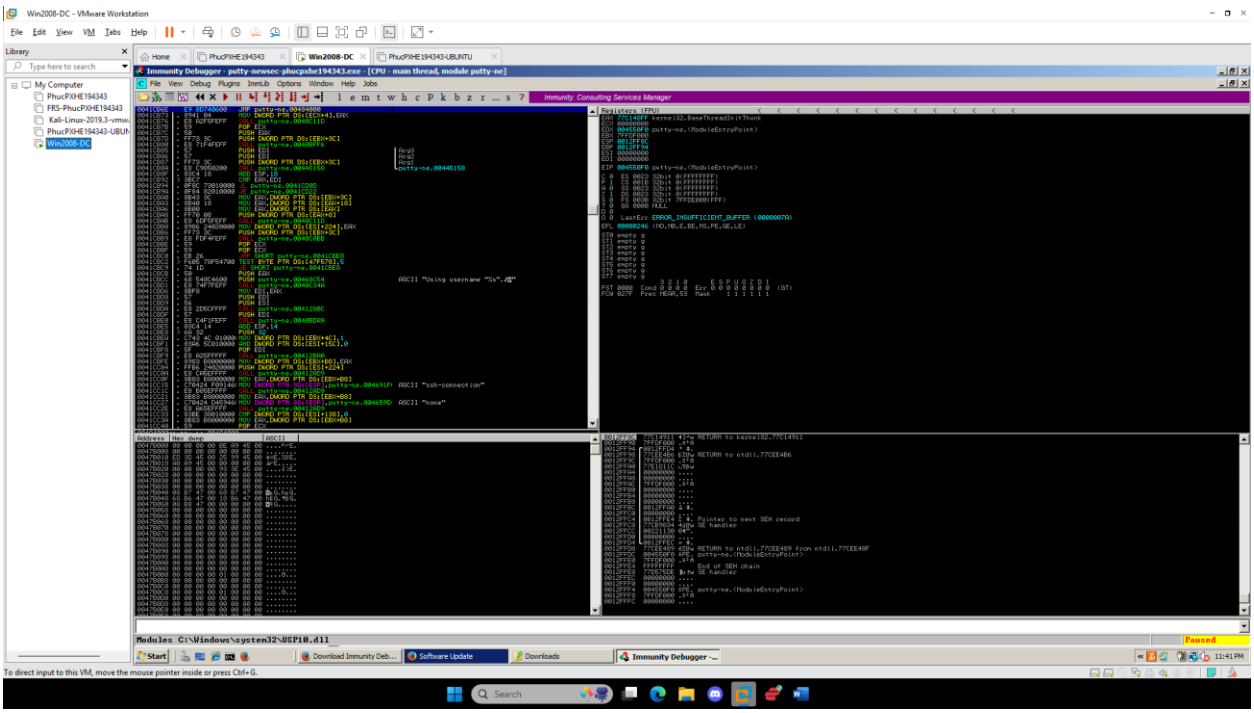

Win2008-DC - VMware Workstation
Immunity Debugger - putty-newsec-phucpxhe194343.exe
Memory map
Modules C:\Windows\system32\USP10.dll
Paused

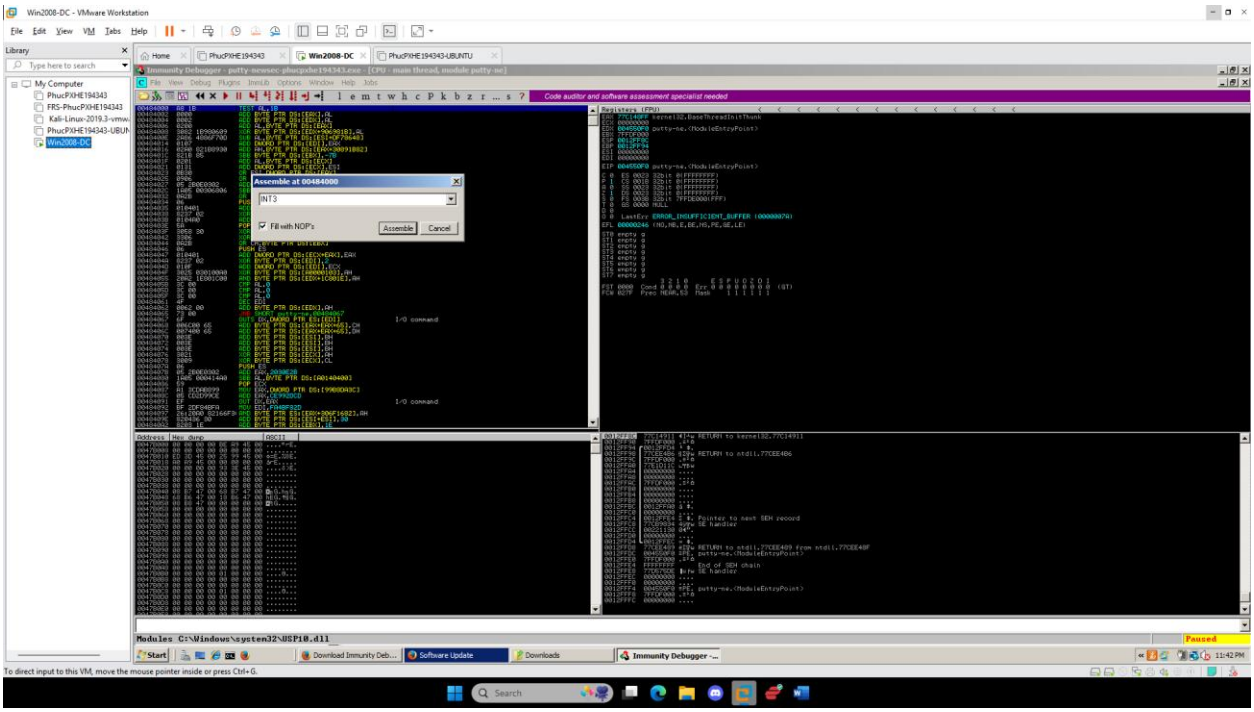

Win2008-DC - VMware Workstation
Immunity Debugger - putty-newsec-phucpxhe194343.exe
Dump - putty-ne:,NewSec 00484000..00484FFF
Memory map
Modules C:\Windows\system32\USP10.dll
Paused

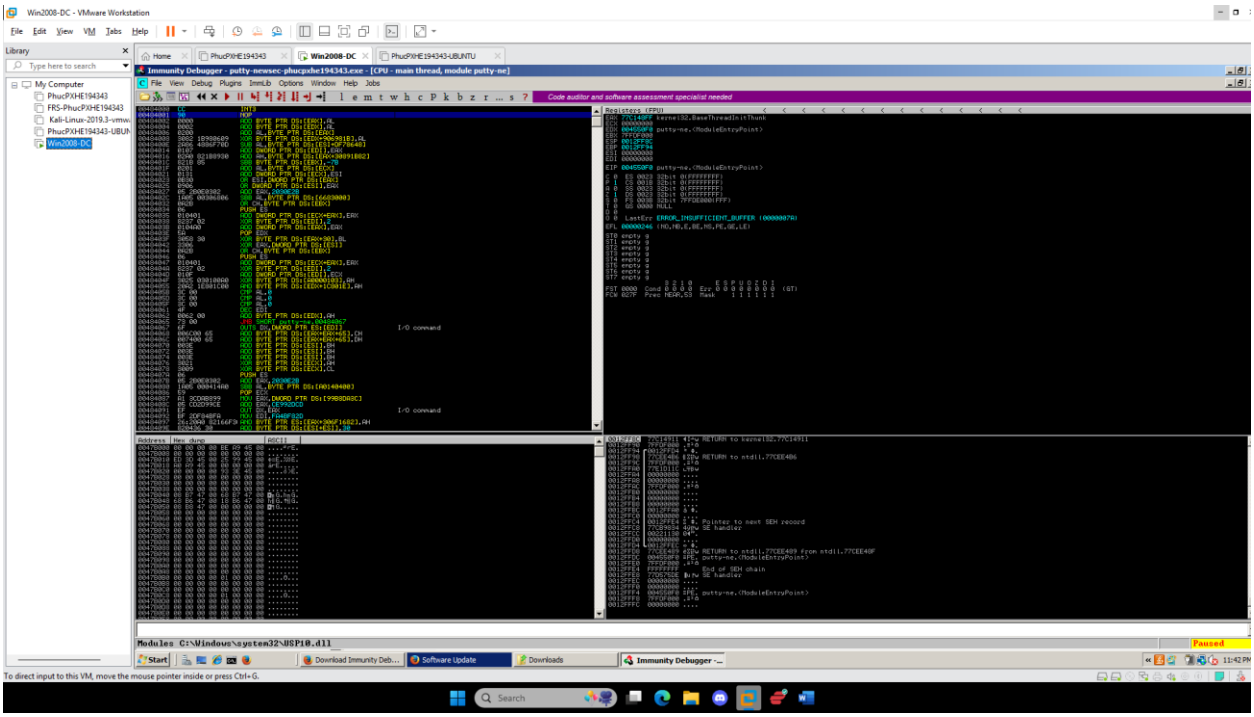

Win2008-DC - VMware Workstation
Enter expression to follow
41CB6E
OK
Cancel
Immunity Debugger - putty-newsec-phucpxhe194343.exe - [CPU - main thread, module putty-ne]
Immunity: Consulting Services Manager
Show source
Paused
Start
Search

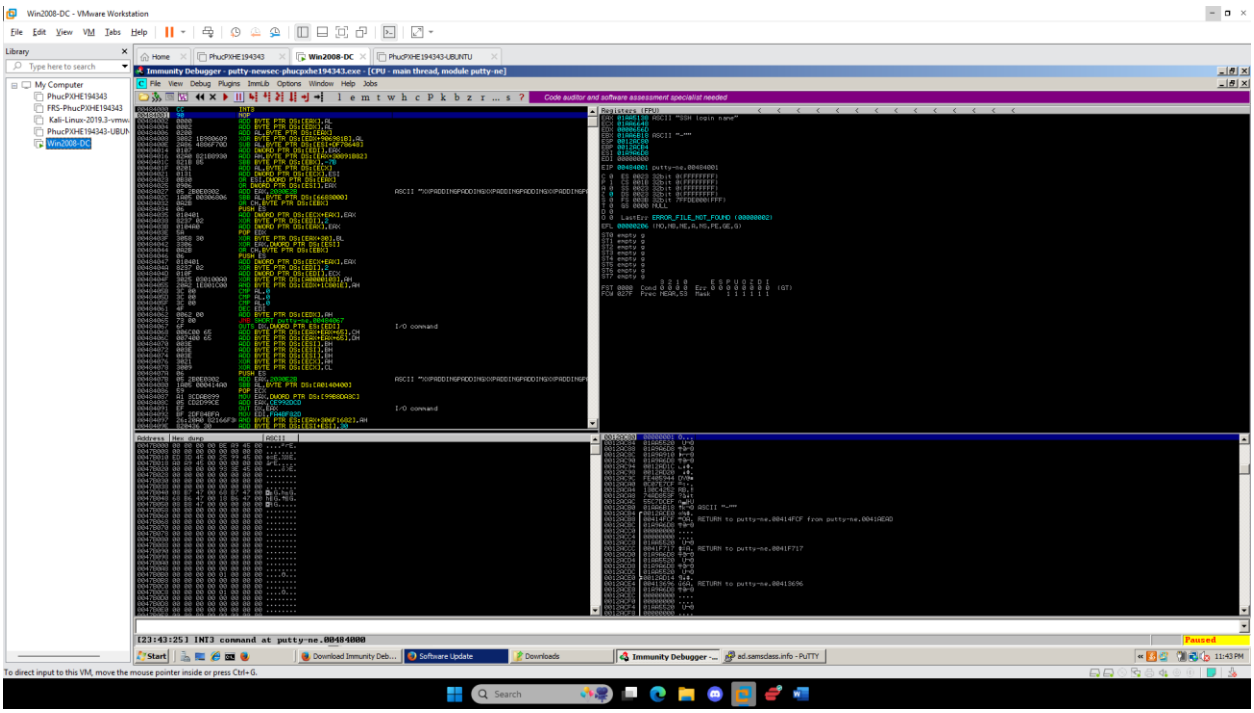

Win2008-DC - VMware Workstation
Immunity Debugger - putty-newsec-phucpxhe194343.exe - [CPU - main thread, module putty-ne]
Immunity: Consulting Services Manager
Show source
Paused
Start
Search

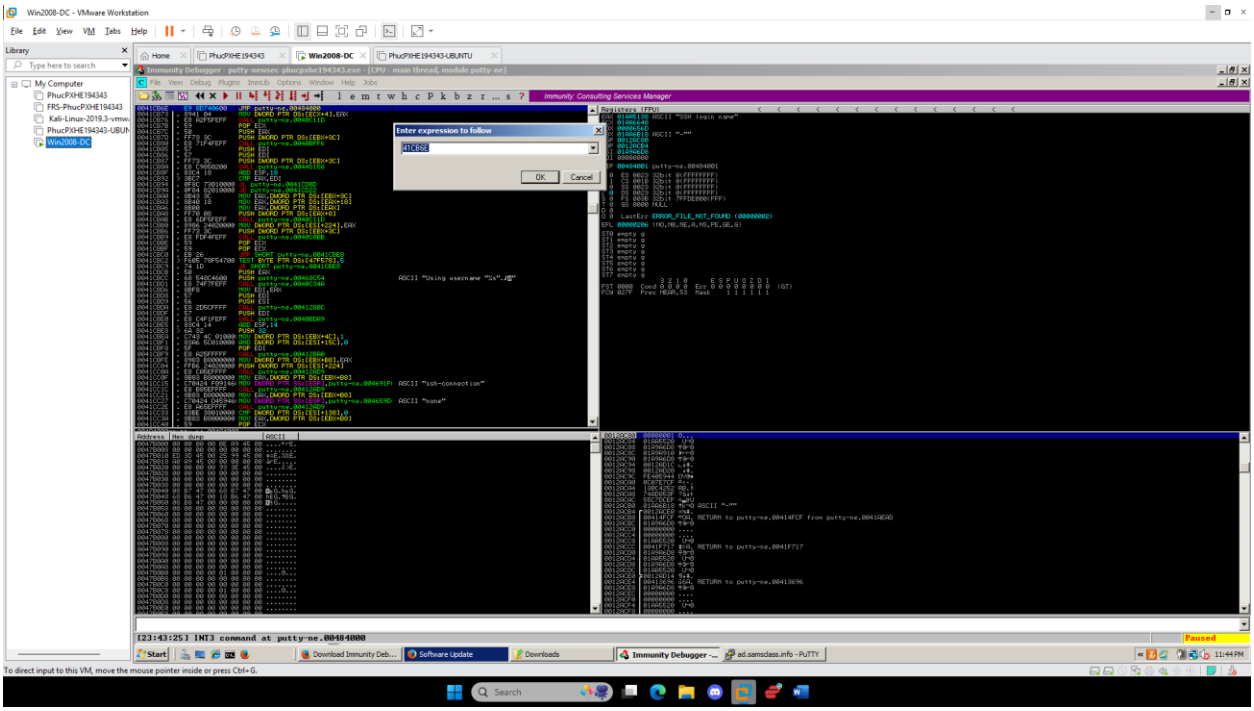

Win2008-DC - VMware Workstation
Assemble at 0041CB6E
JMP 484000
Fill with NOP's
Assemble
Cancel
Show source
Paused
Start
Search

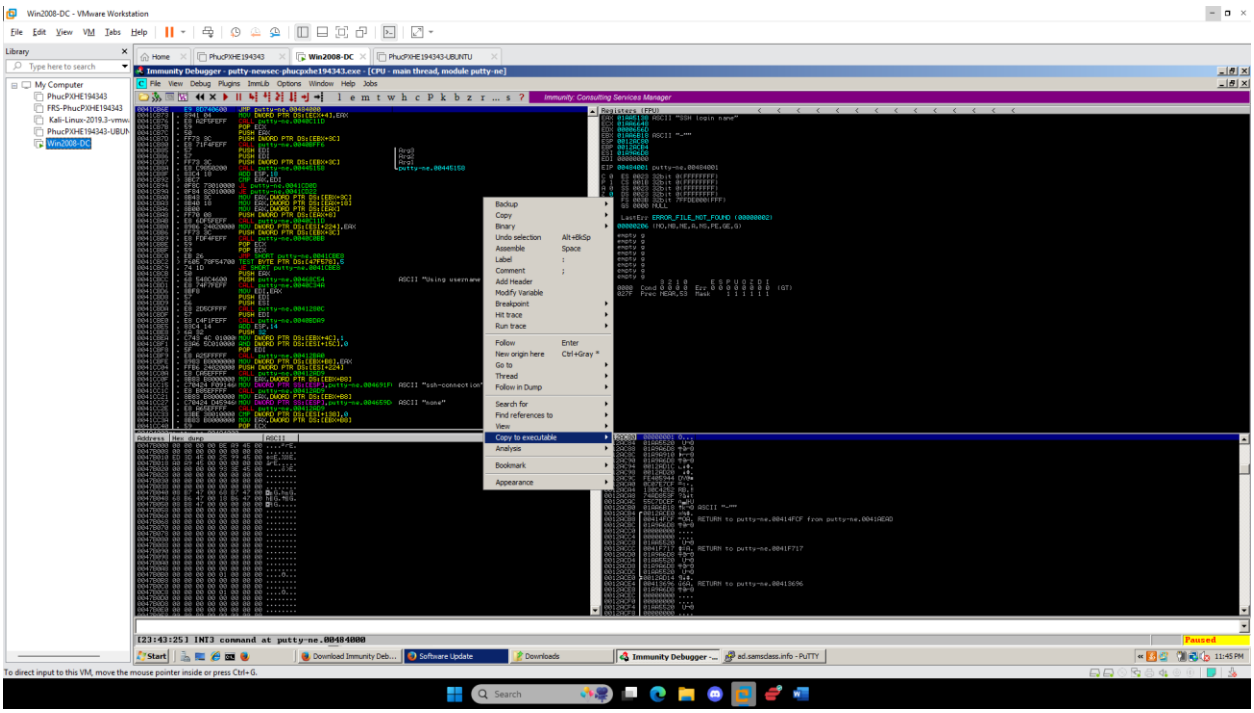

Win2008-DC - VMware Workstation
Modules C:\Windows\system32\DSPI0.dll
Paused
Start
Search

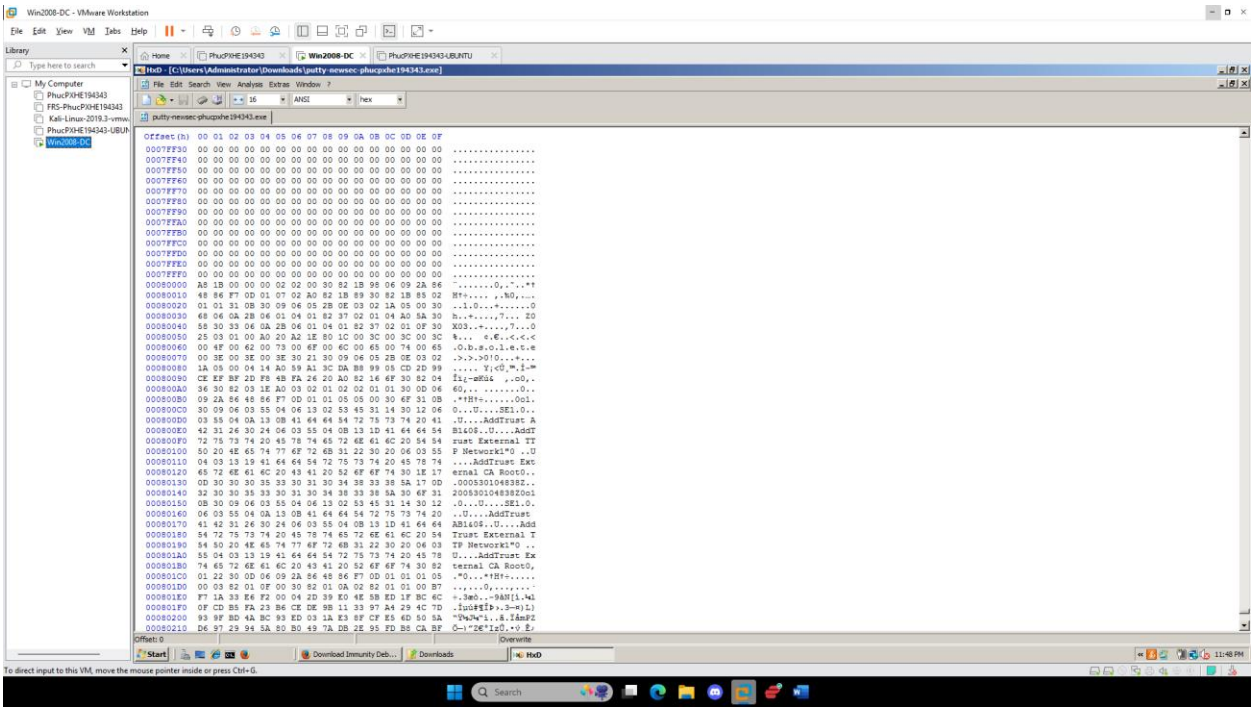

Win2008-DC - VMware Workstation
Immunity Debugger - putty-newsec-phucpxhe194343.exe - [CPU - main thread, module putty-ne]
Assemble at 00484000
INT3
Fill with NOP's
Assemble
Cancel
Modules C:\Windows\system32\USP10.dll
Paused

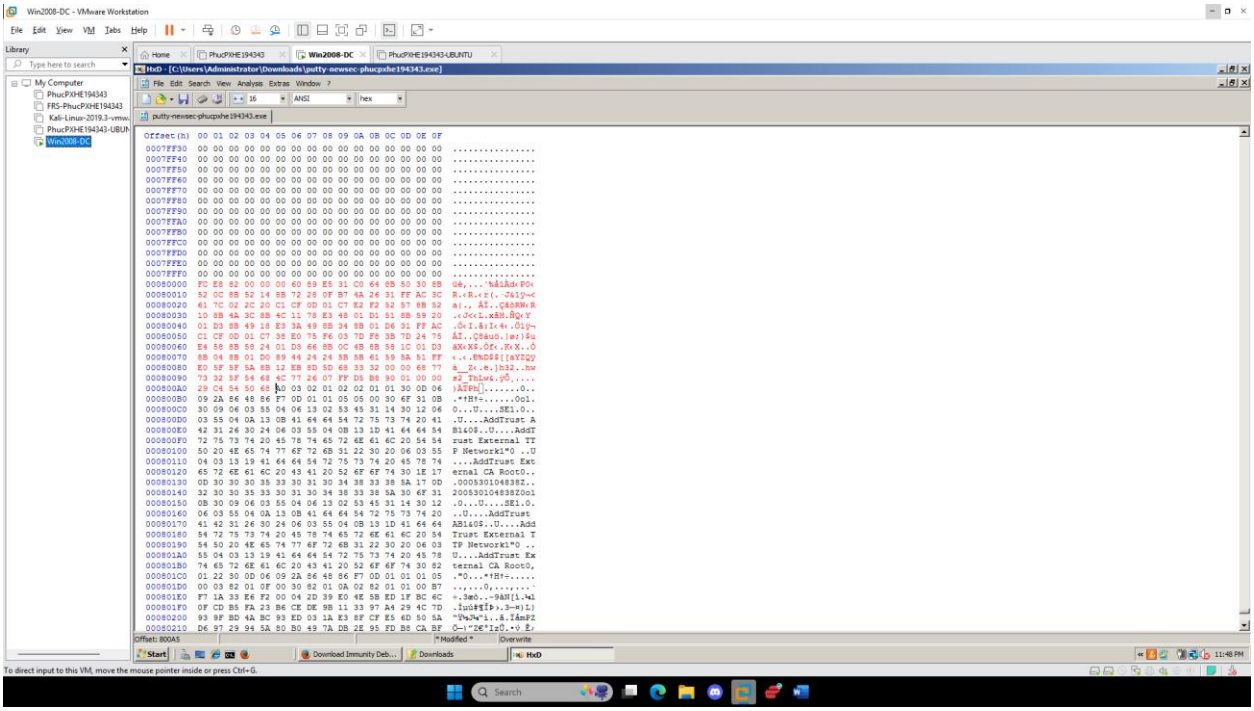

Win2008-DC - VMware Workstation
Immunity Debugger - putty-newsec-phucpxhe194343.exe - [CPU - main thread, module putty-ne]
Modules C:\Windows\system32\USP10.dll
Paused

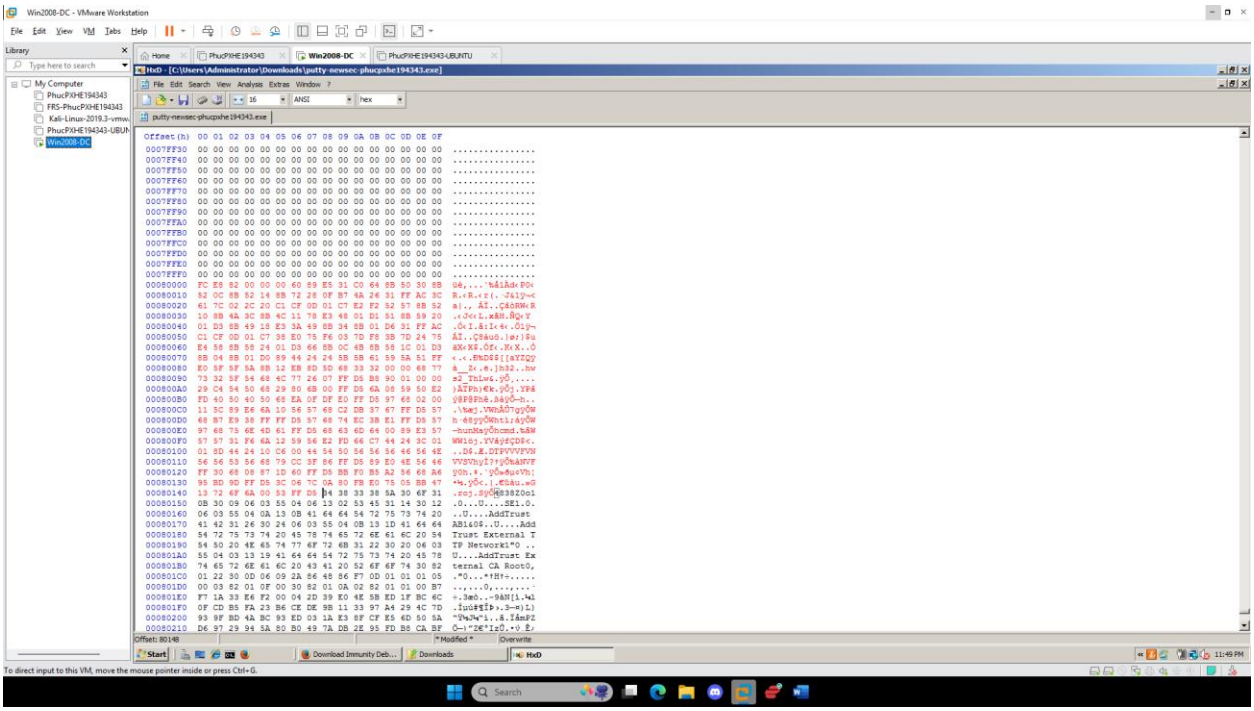

Win2008-DC - VMware Workstation
Immunity Debugger - putty-newsec-phucpxhe194343.exe - [CPU - main thread, module putty-ne]
[23:43:25] INT3 command at putty-ne.00484000
Paused

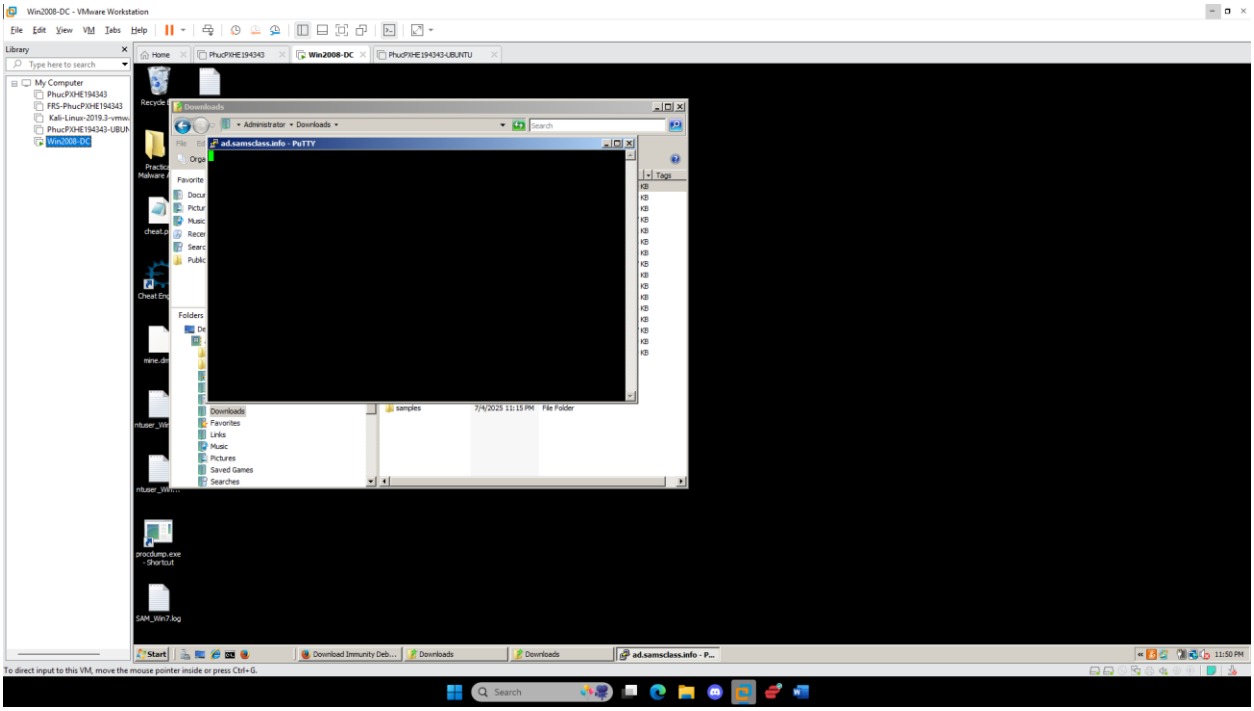

Win2008-DC - VMware Workstation
Immunity Debugger - putty-newsec-phucpxhe194343.exe - [CPU - main thread, module putty-ne]
Enter expression to follow
OK
Cancel
[23:43:25] INT3 command at putty-ne.00484000
Paused

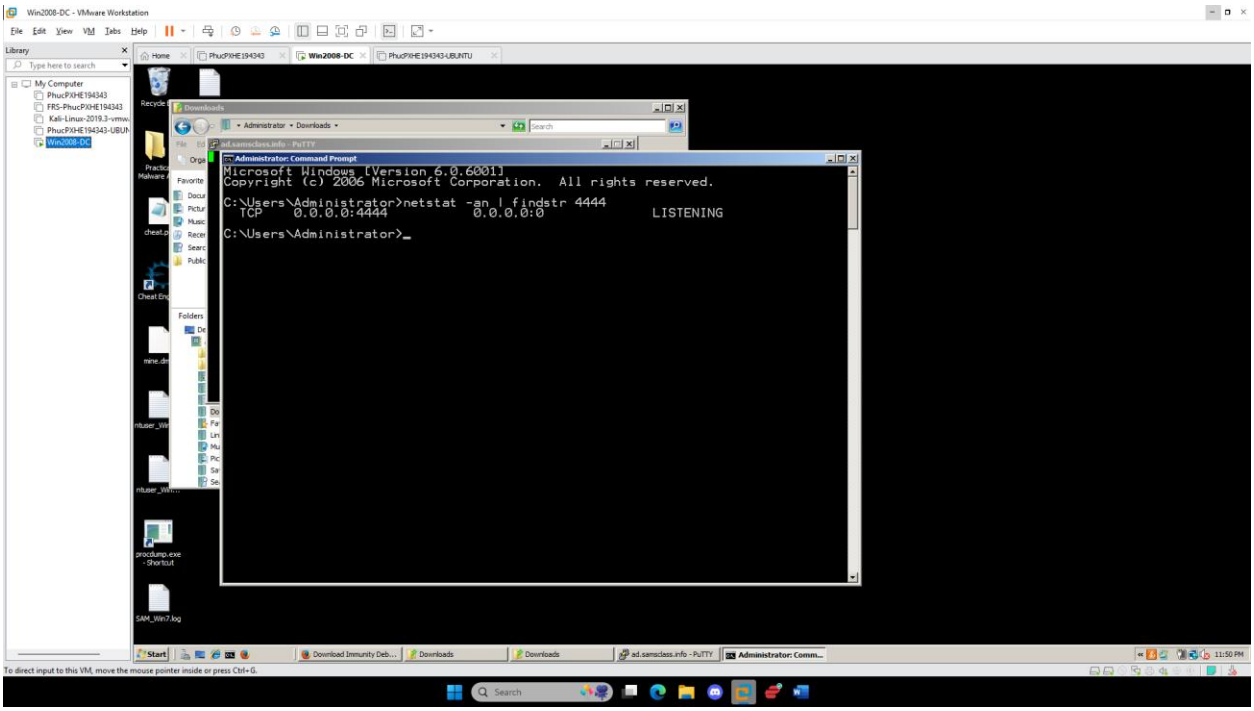

Win2008-DC - VMware Workstation
Immunity Debugger - putty-newsec-phucpxhe194343.exe - [CPU - main thread, module putty-ne]
[23:43:25] INT3 command at putty-ne.00484000
Paused

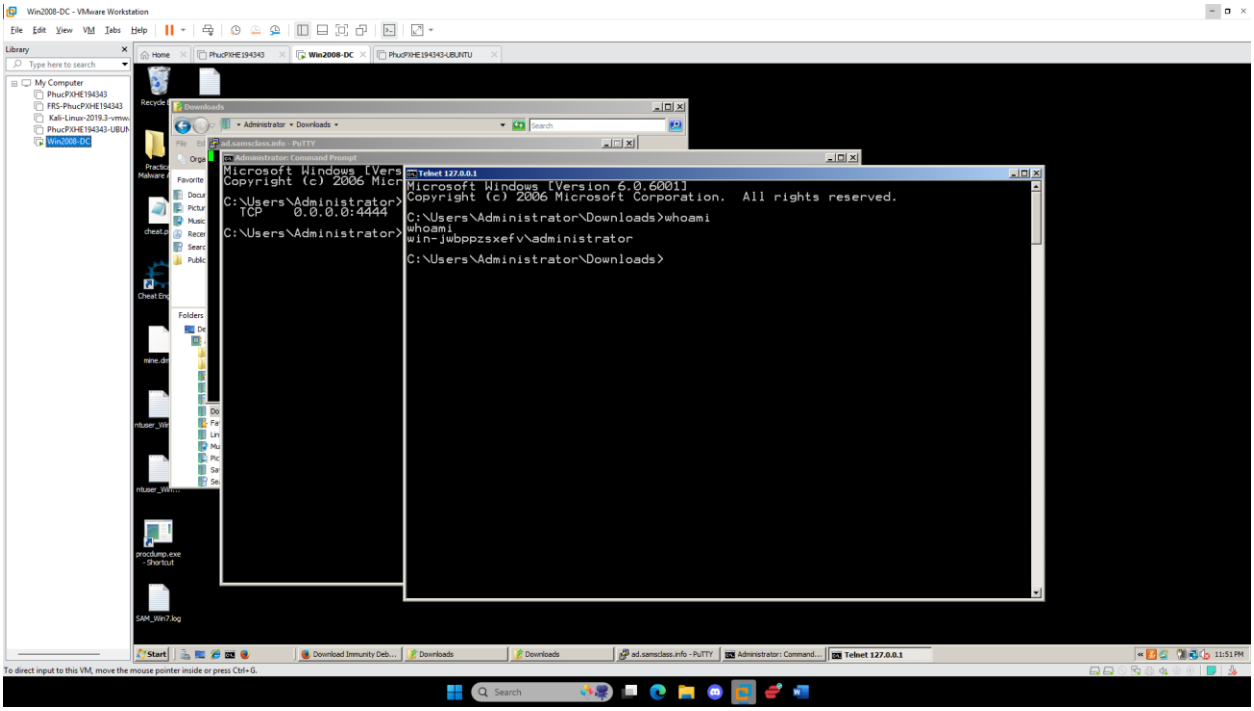

Win2008-DC - VMware Workstation
HxD - [C:\Users\Administrator\Downloads\putty-newsec-phucpxhe194343.exe]


Win2008-DC - VMware Workstation
HxD - [C:\Users\Administrator\Downloads\putty-newsec-phucpxhe194343.exe]
putty-newsec-phucpxhe194343.exe
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
Offset: 800A5
Modified
Overwrite
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Win2008-DC - VMware Workstation
HxD - [C:\Users\Administrator\Downloads\putty-newsec-phucpxhe194343.exe]
putty-newsec-phucpxhe194343.exe
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
Offset: 80148
Modified
Overwrite
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Win2008-DC - VMware Workstation
ad.samsclass.info - PuTTY

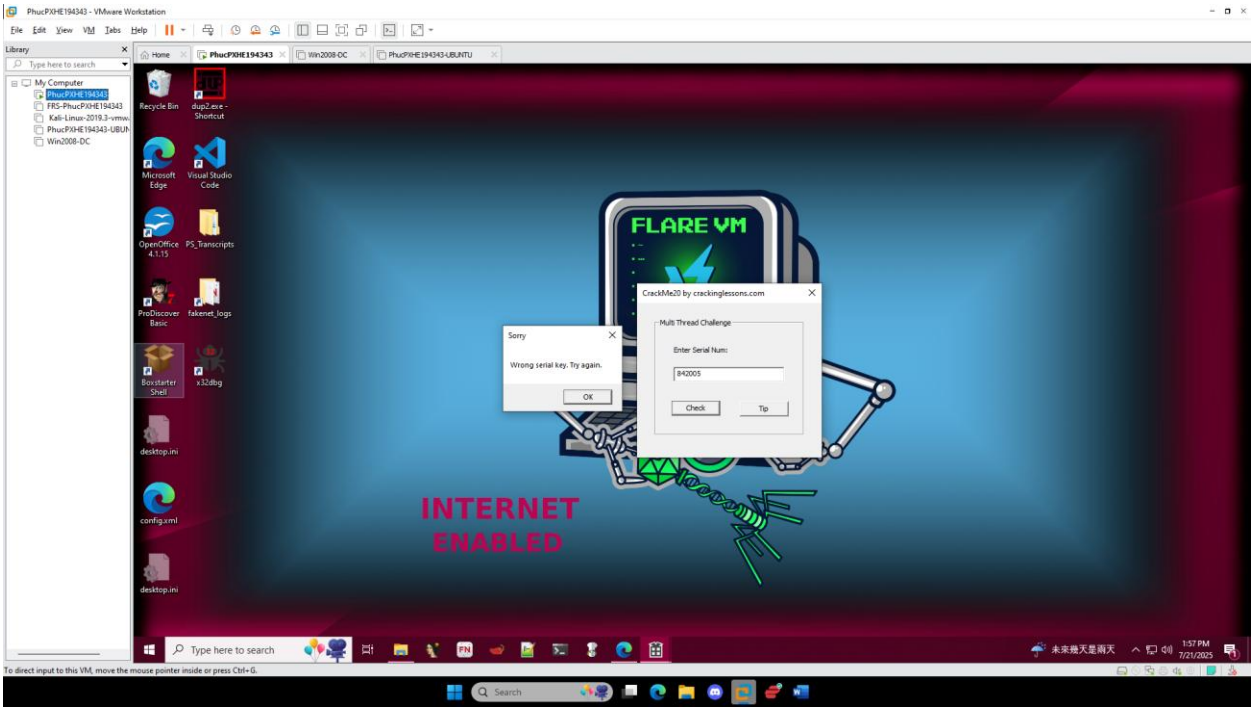

Win2008-DC - VMware Workstation
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>netstat -an | findstr 4444
TCP 0.0.0.0:4444 0.0.0.0:0 LISTENING
C:\Users\Administrator>



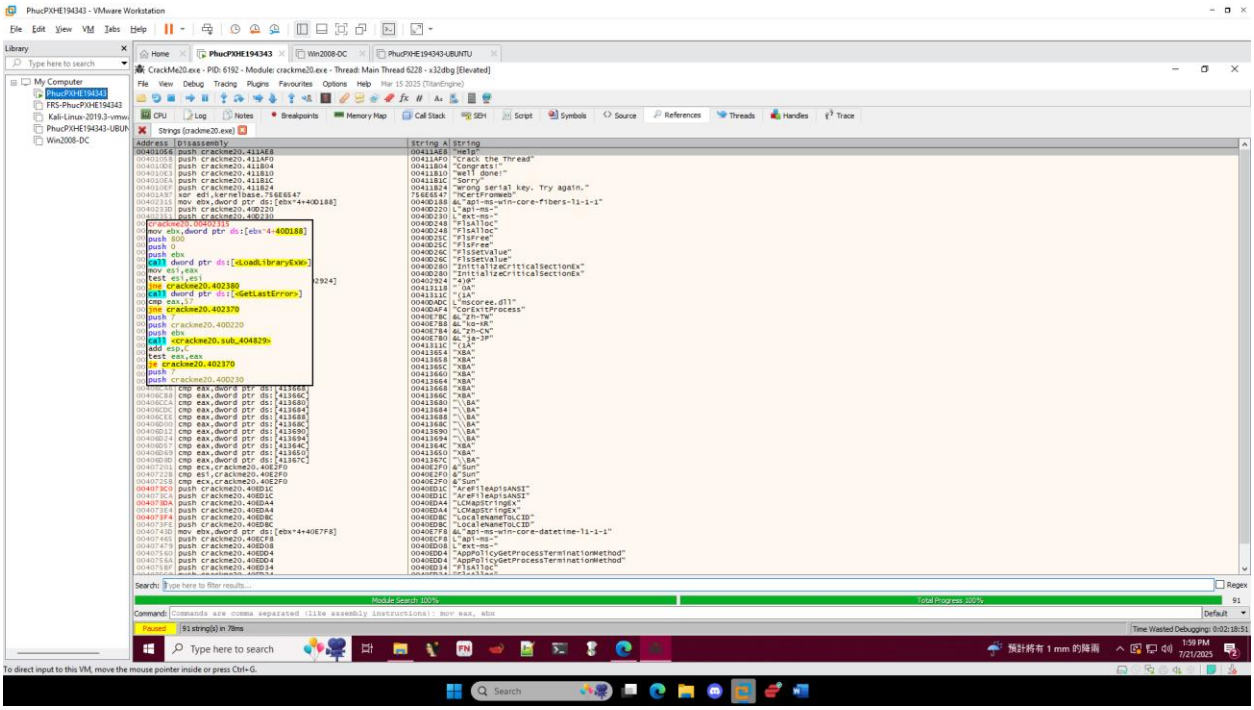
Crack Me 20

Part 1: Patch the thread that checks for the correct serial number

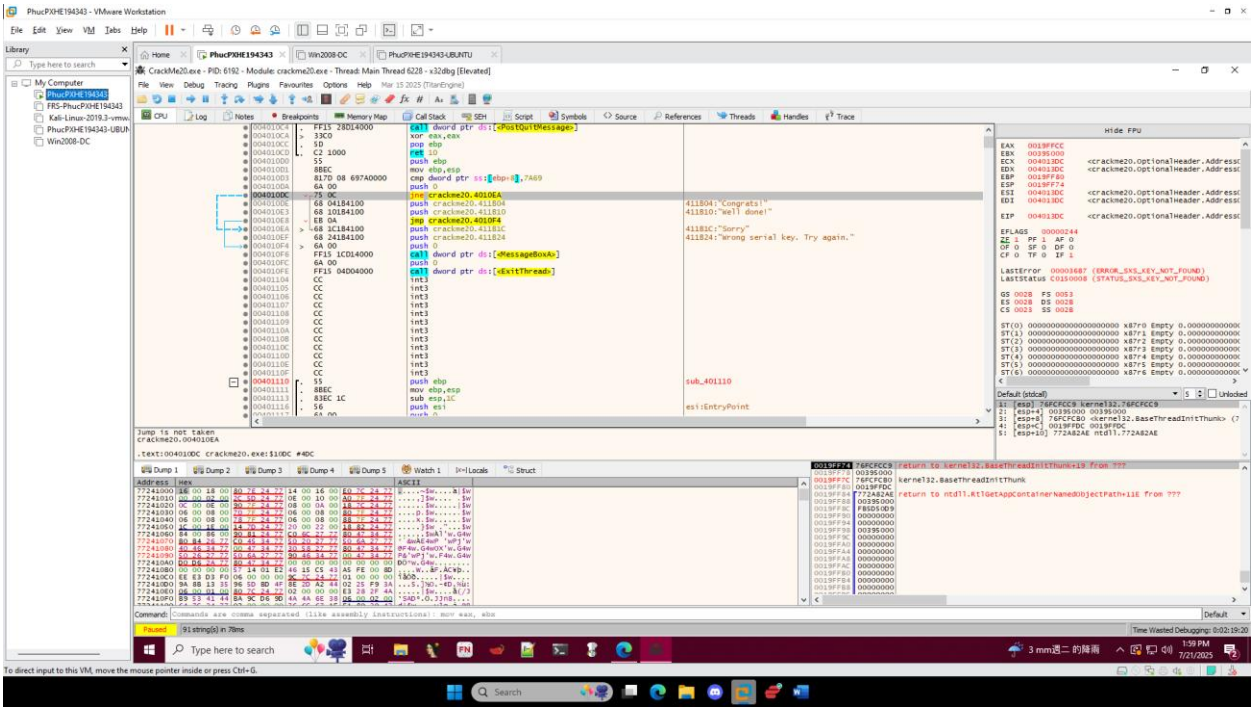
Step 1: Bài này khác những bài trước vì bài này sử dụng đa luồng (multi-thread), chương trình sẽ thực hiện nhiều tác vụ đồng thời thay vì xử lý tuần tự từng việc một.

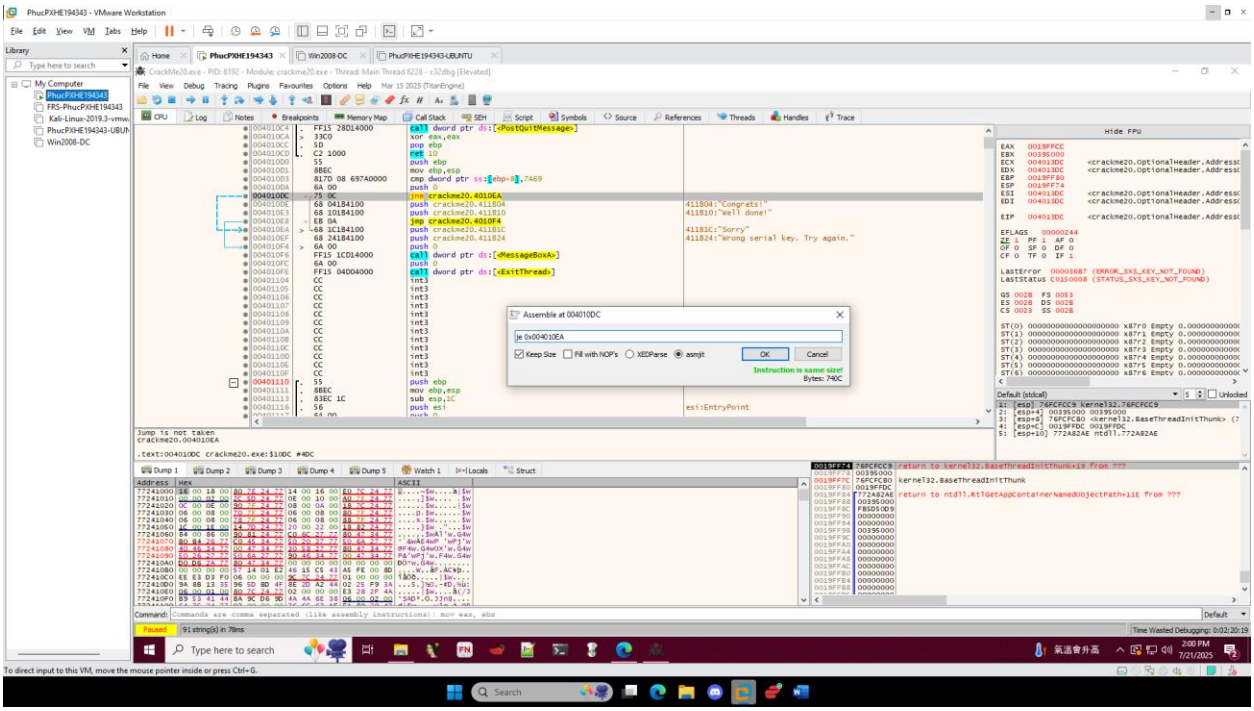


Step 2: Mở String preference

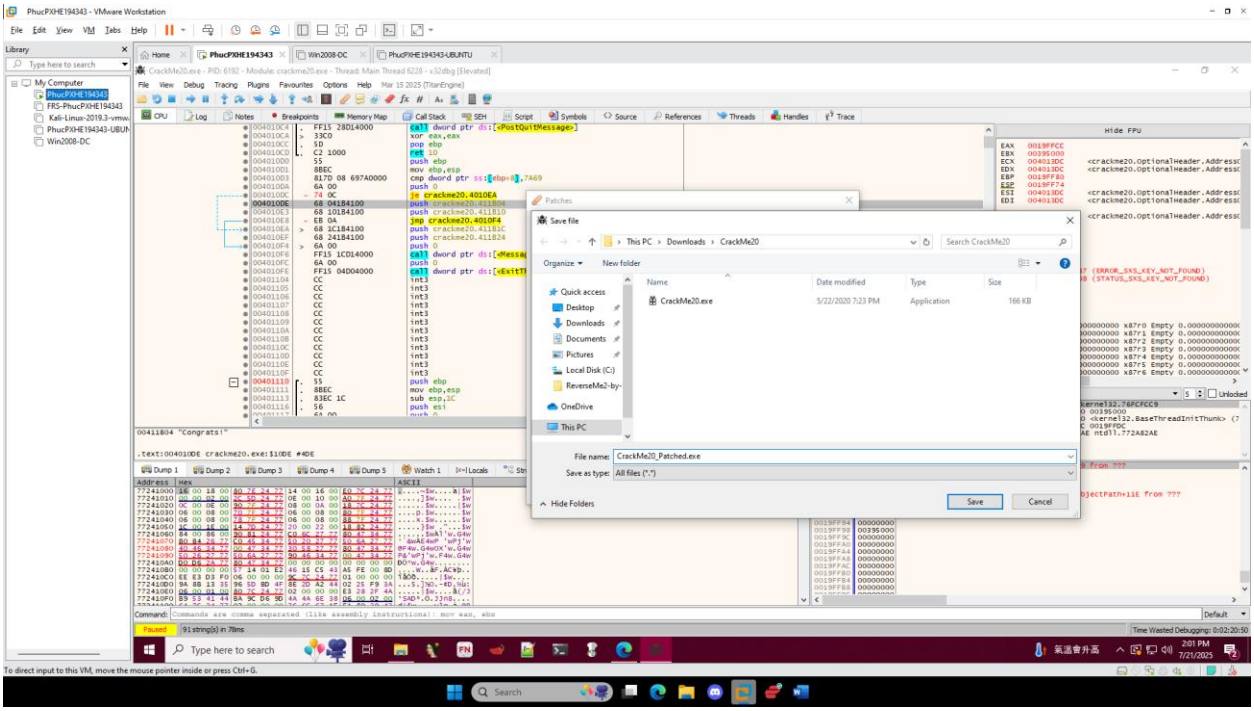


Step 3: Khi quan sát trong x32dbg, em thấy chương trình sử dụng lệnh jne để nhảy qua thông báo "success". Vì vậy, em đã sửa lệnh đó thành je để thay đổi logic: chương trình sẽ chỉ hiển thị thông báo "success" khi người dùng nhập sai, còn nếu nhập đúng thì sẽ không được chấp nhận.

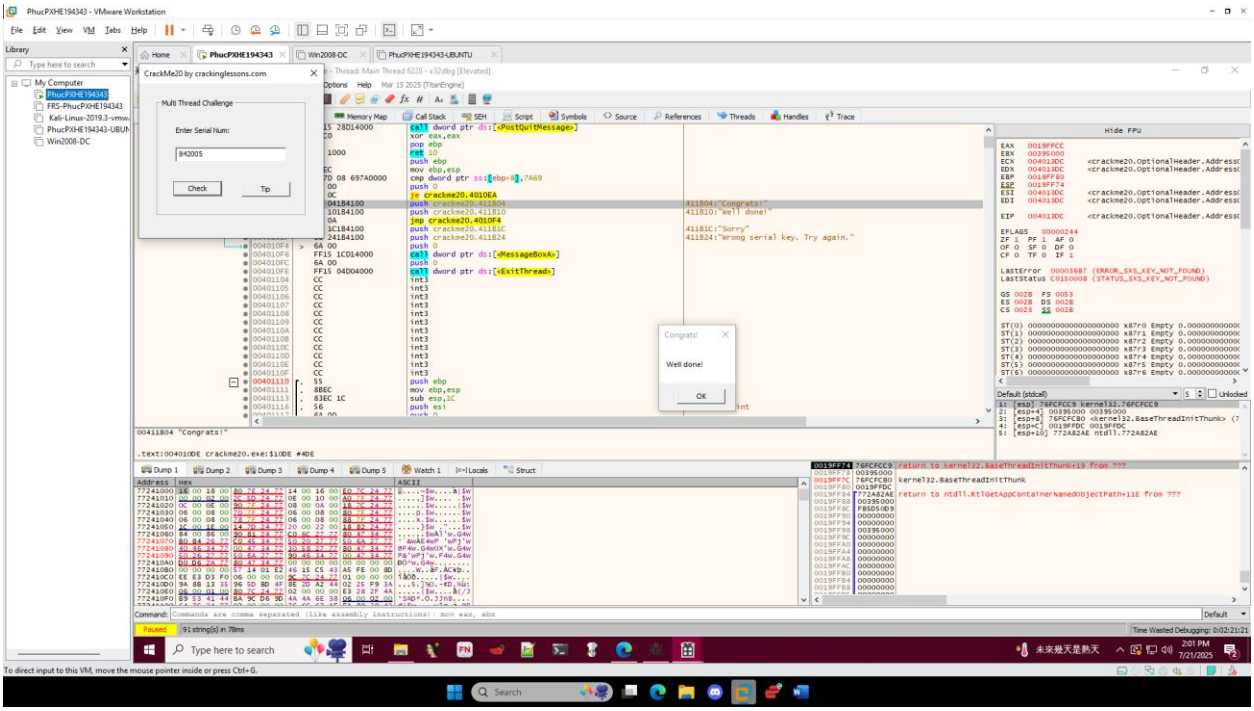




Step 4: Tiến hành patch file

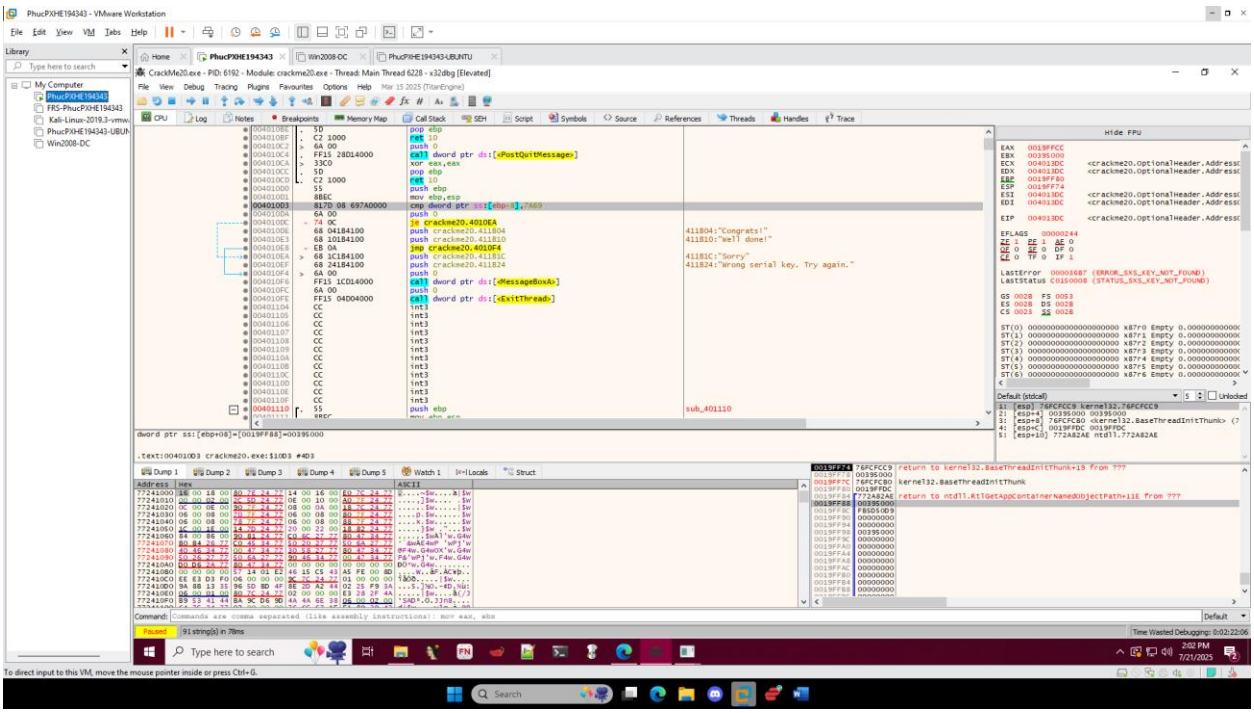


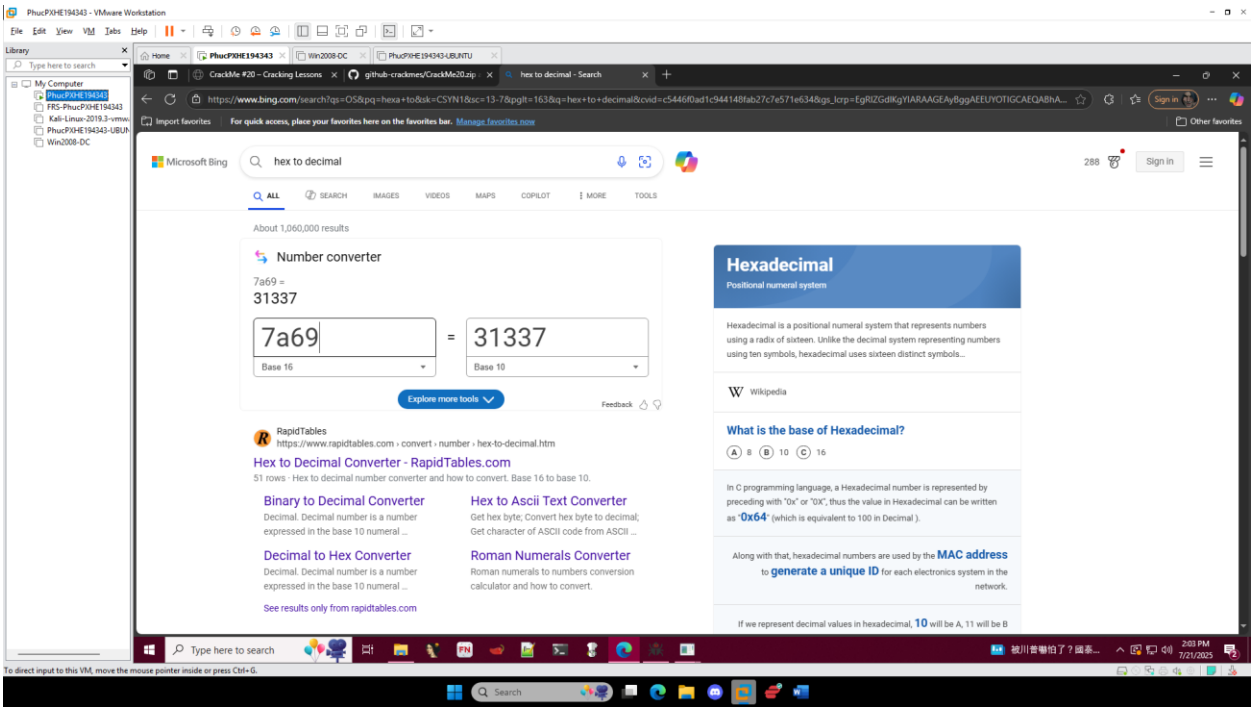
Step 5: Thử file và thành công



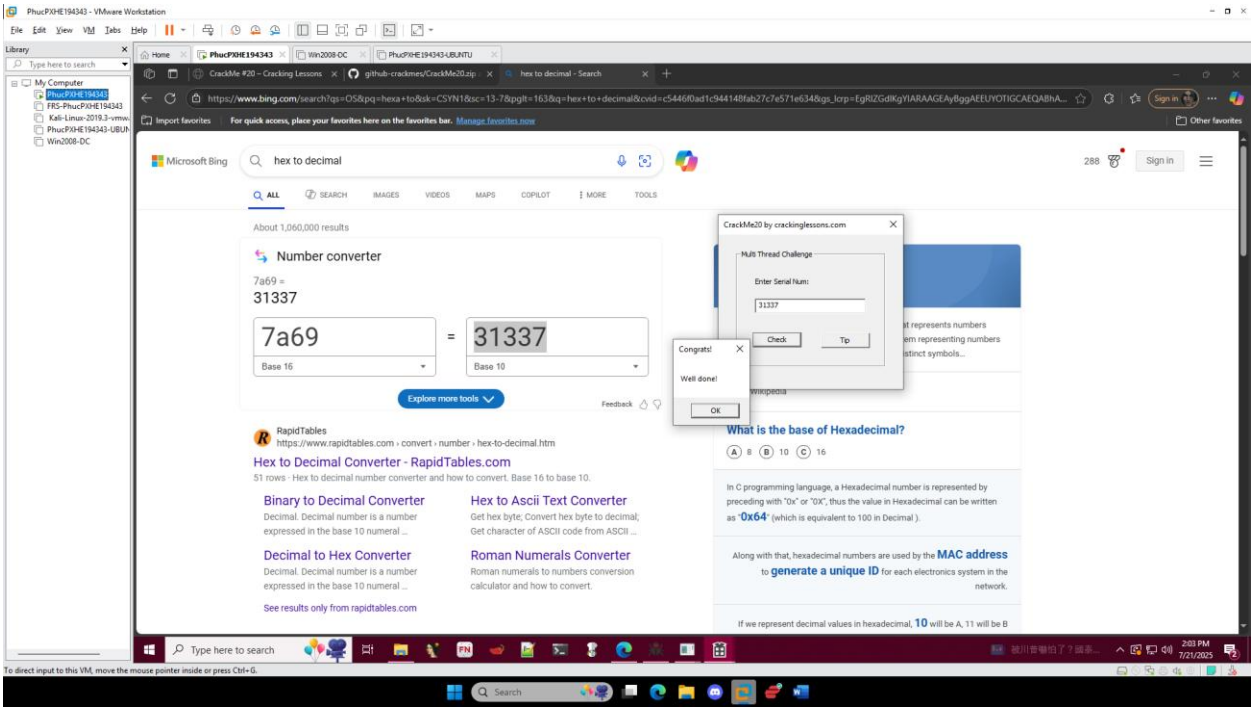
Part 2: Do serial fishing for the serial number

Step 1: Nếu quan sát kỹ hơn ở phía trên, ta có thể thấy chương trình thực hiện so sánh với giá trị 7A69 ở hệ thập lục phân, tương đương với 31337 ở hệ thập phân. Do đó, key hợp lệ chính là 31337.





Step 2: Thử key


PhucPXHE194343 - VMware Workstation
hex to decimal
Number converter
7a69 =
31337
7a69
Base 16
=
31337
Base 10
Explore more tools
RapidTables
https://www.rapidtables.com › convert › number › hex-to-decimal.htm
Hex to Decimal Converter - RapidTables.com
51 rows · Hex to decimal number converter and how to convert. Base 16 to base 10.
Binary to Decimal Converter
Hex to Ascii Text Converter
Decimal to Hex Converter
Roman Numerals Converter
See results only from rapidtables.com
CrackMe20 by crackinglessons.com
Multi Thread Challenge
Enter Serial Num:
31337
Check
Tip
Congrats!
Well done!
OK
What is the base of Hexadecimal?
In C programming language, a Hexadecimal number is represented by preceding with "0x" or "0X", thus the value in Hexadecimal can be written as "0x64" (which is equivalent to 100 in Decimal).
Along with that, hexadecimal numbers are used by the MAC address to generate a unique ID for each electronics system in the network.
Type here to search
Search