# Lab 18: Simple EXE Hacking with Immunity

**Course Name**: Malware Analysis and Reverse Engineering (IAM302)
**Student Name**: Nguyễn Trần Vinh – SE160258
**Instructor Name**: Mai Hoàng Đỉnh
**Lab Due Date**: 22/3/2023

## What You Need

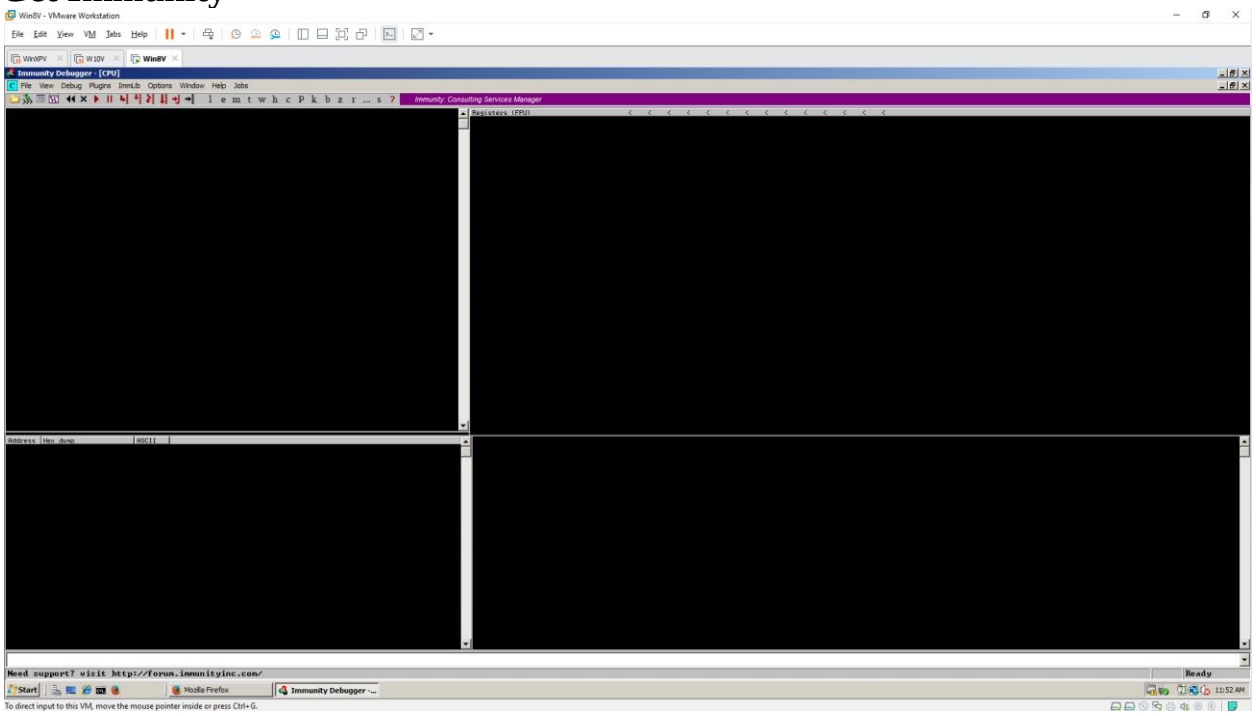
A Windows machine, real or virtual. I used a Windows Server 2008 virtual machine.

## Purpose

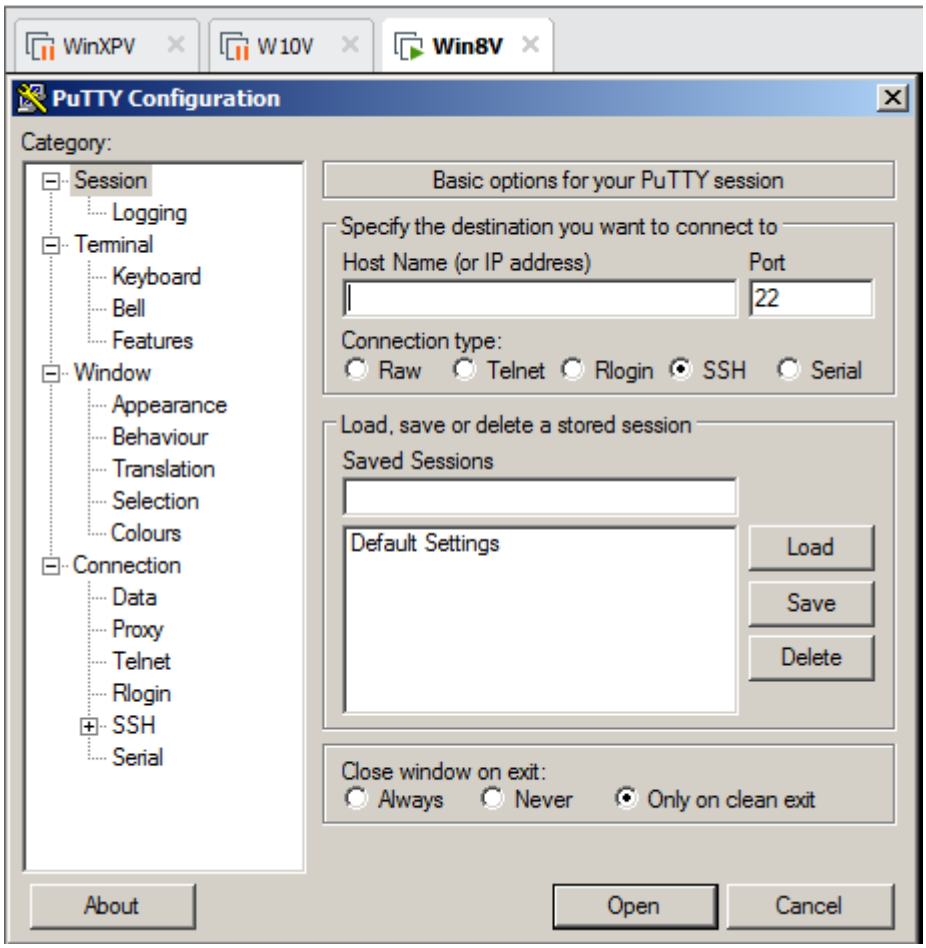
To modify a Windows EXE file and save an altered version. This gives you practice with very simple features of the Immunity debugger.

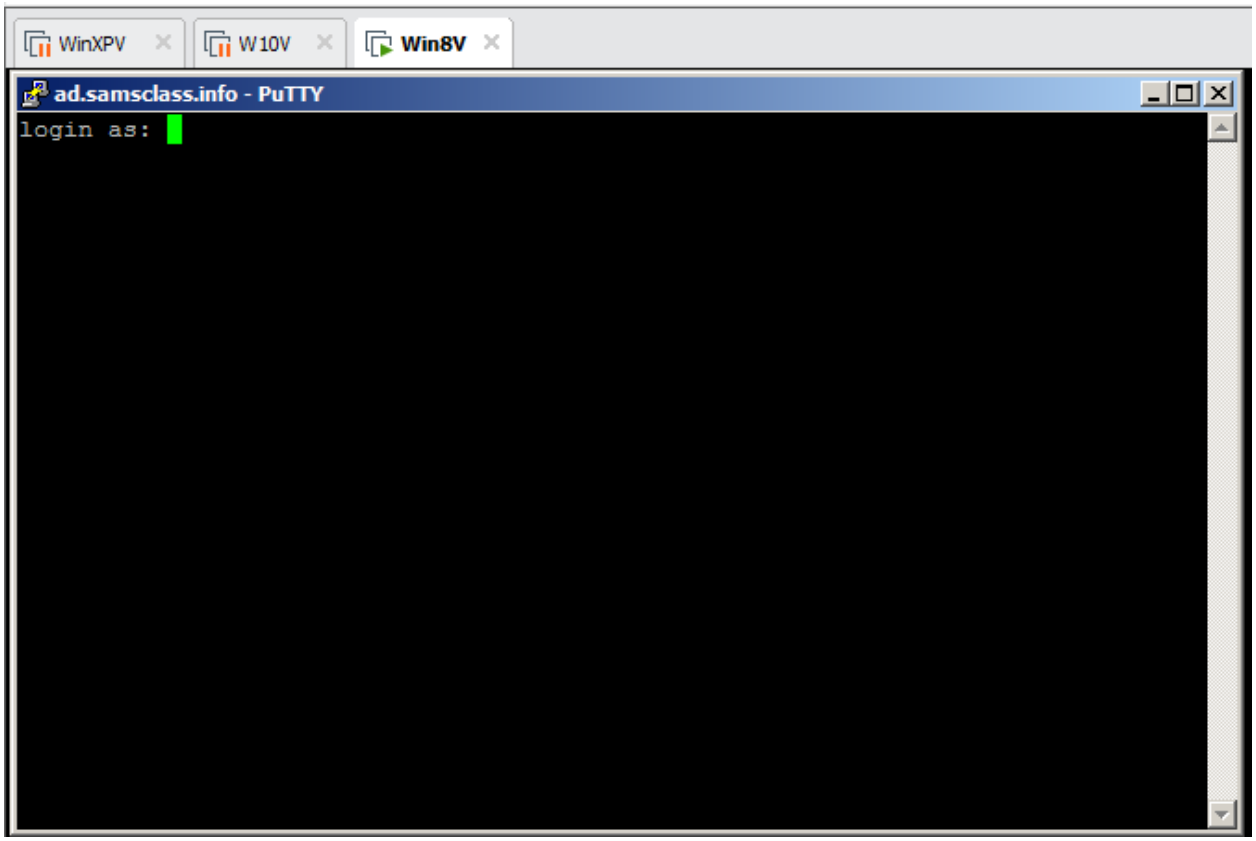
## Task 1: Target EXE Recon

### Get Immunity

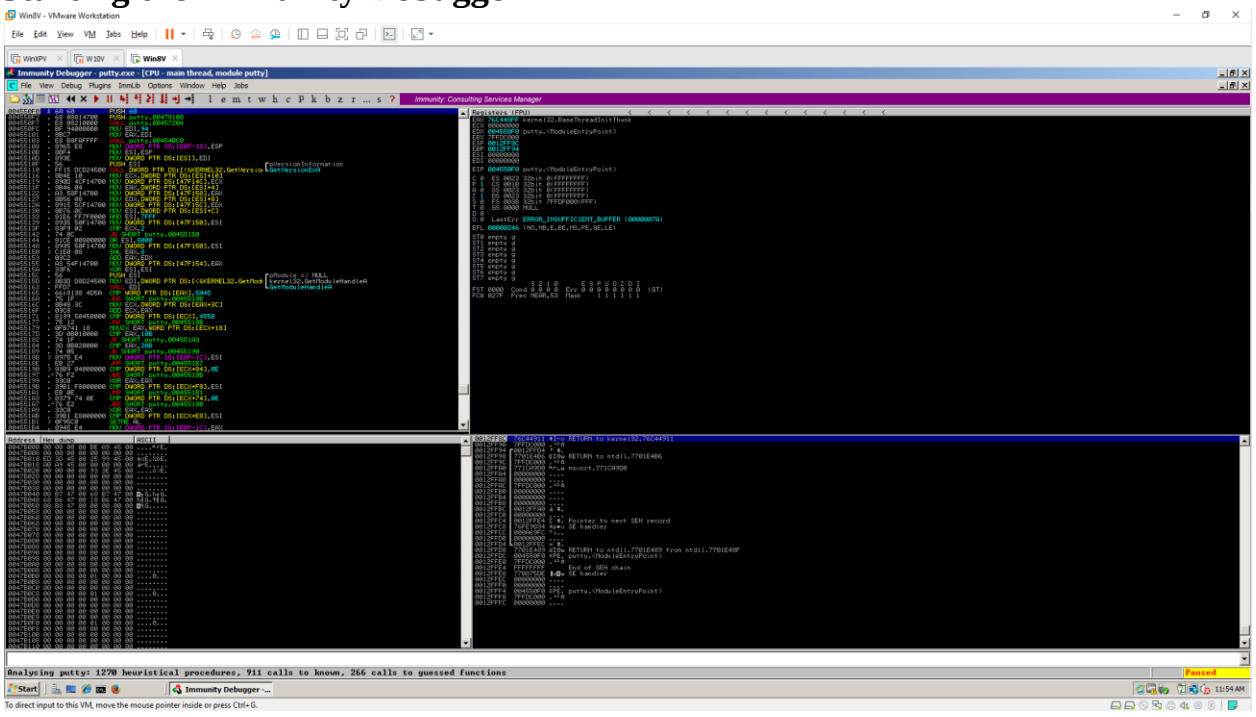



### Get putty.exe

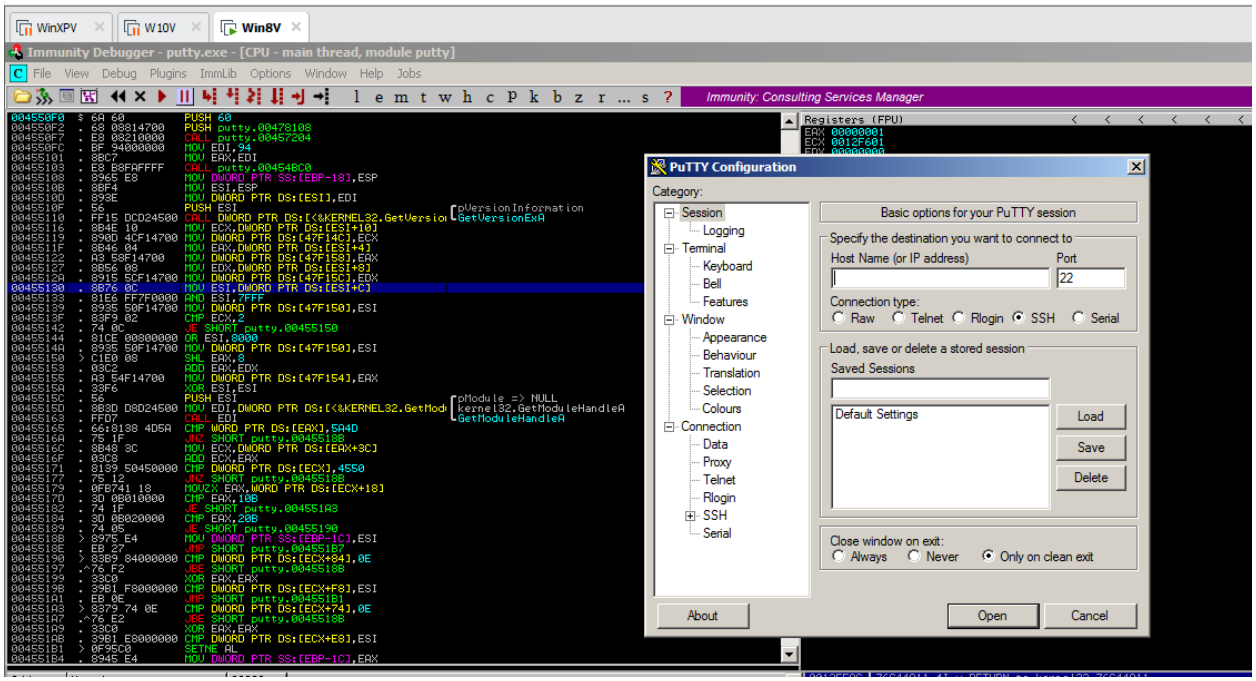

WinXPV
W10V
Win8V
PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP 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

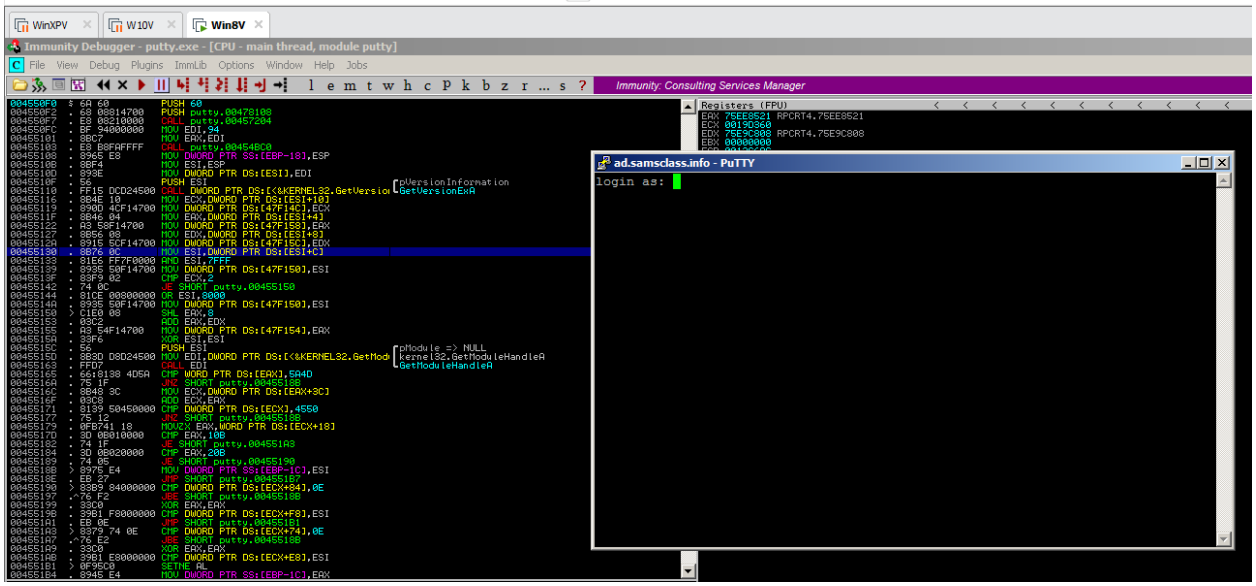



## Starting the Immunity Debugger

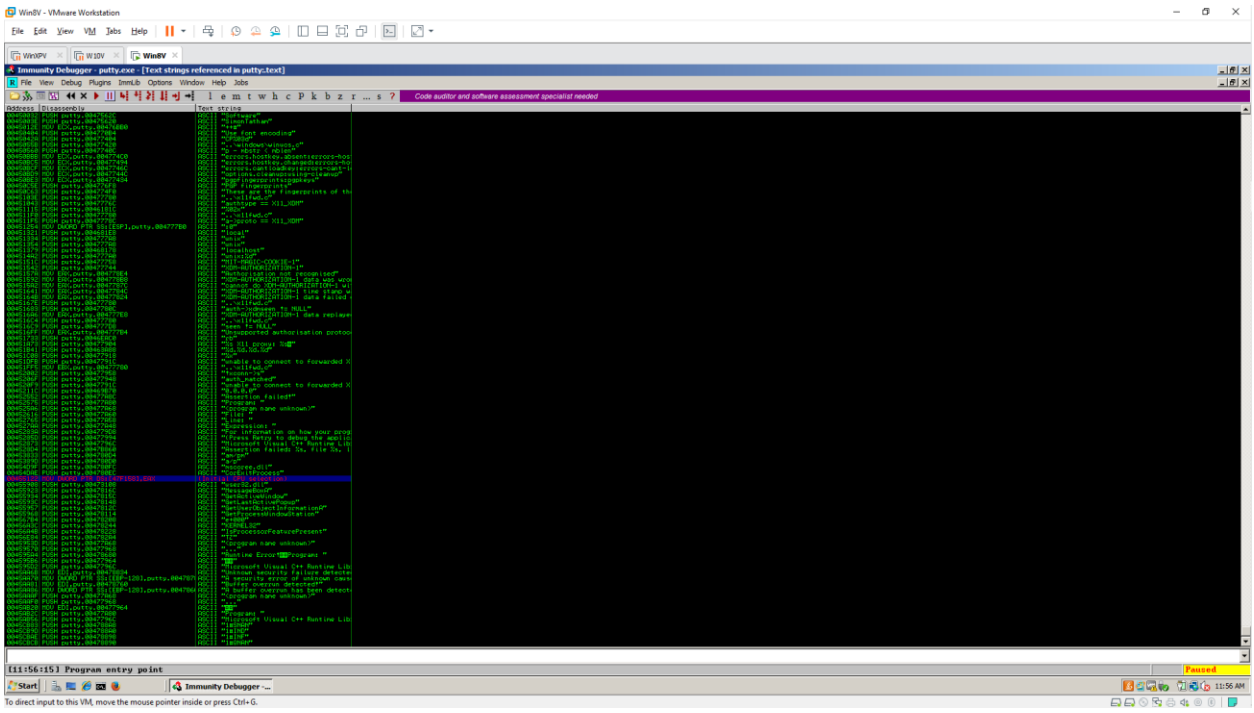


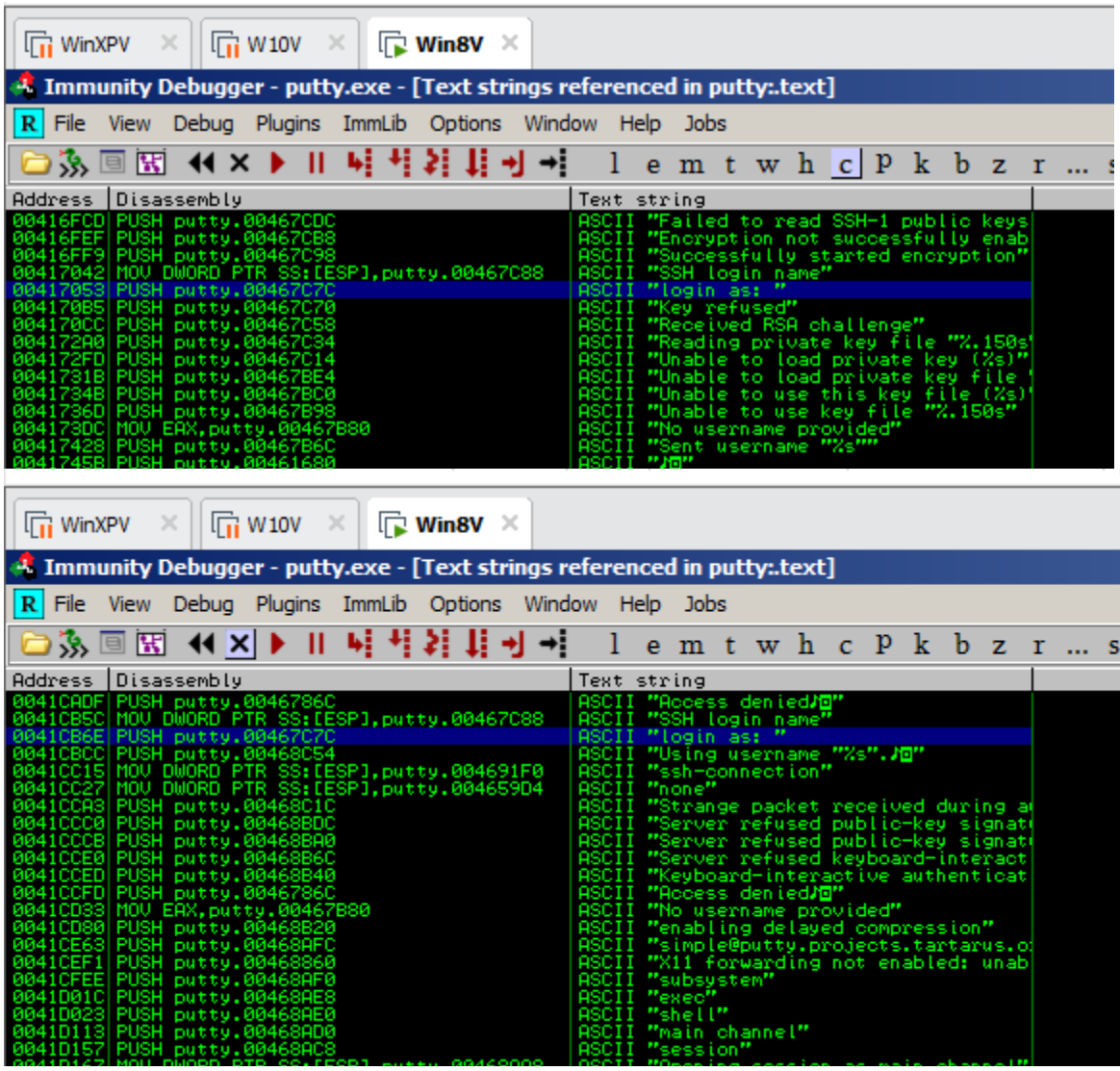

## Running Putty in Immunity




# Finding the "login as" Code

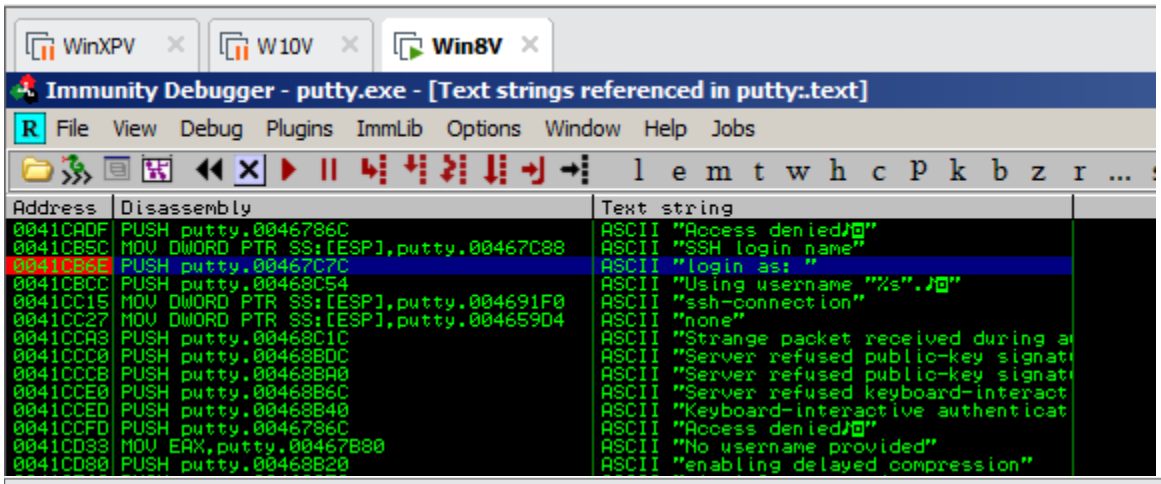

WinBV - VMware Workstation
Immunity Debugger - putty.exe - [Text strings referenced in putty.text]
Code auditor and software assessment specialist needed
[11:56:15] Program entry point
Paused

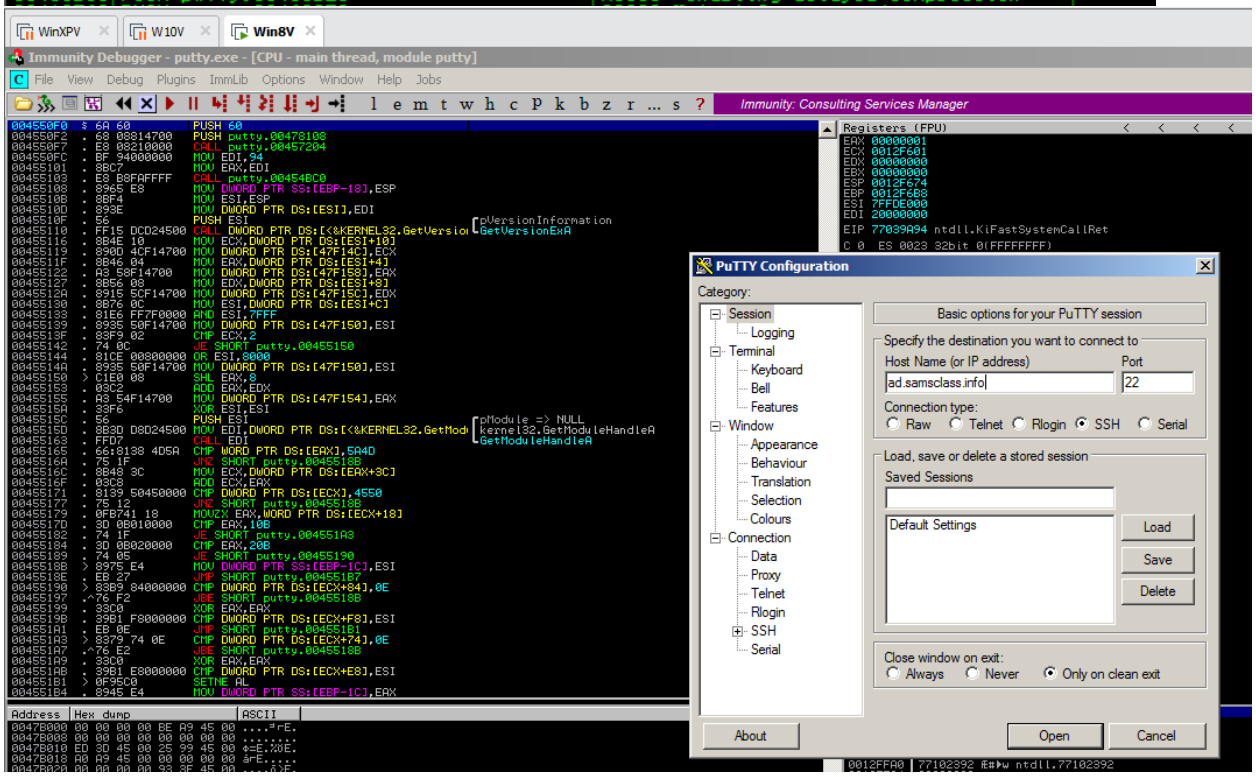


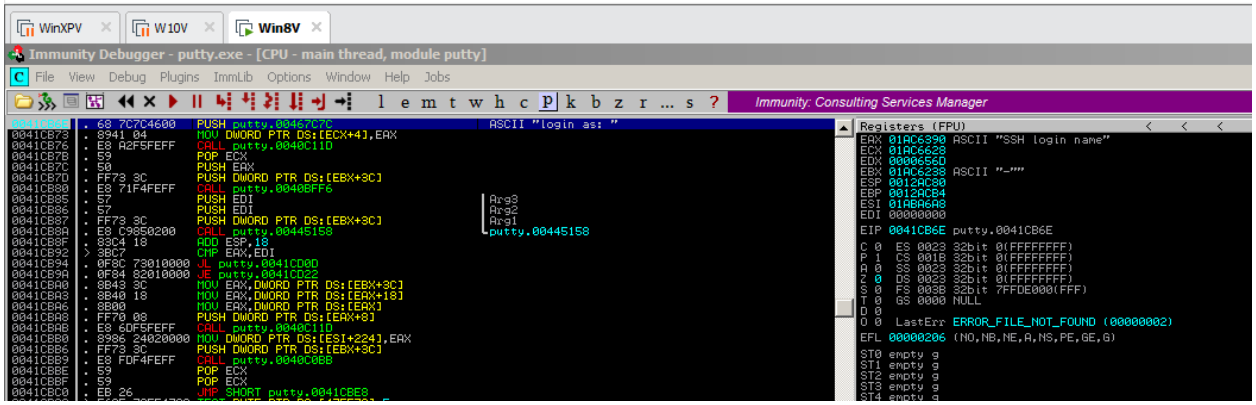




## Using Breakpoints

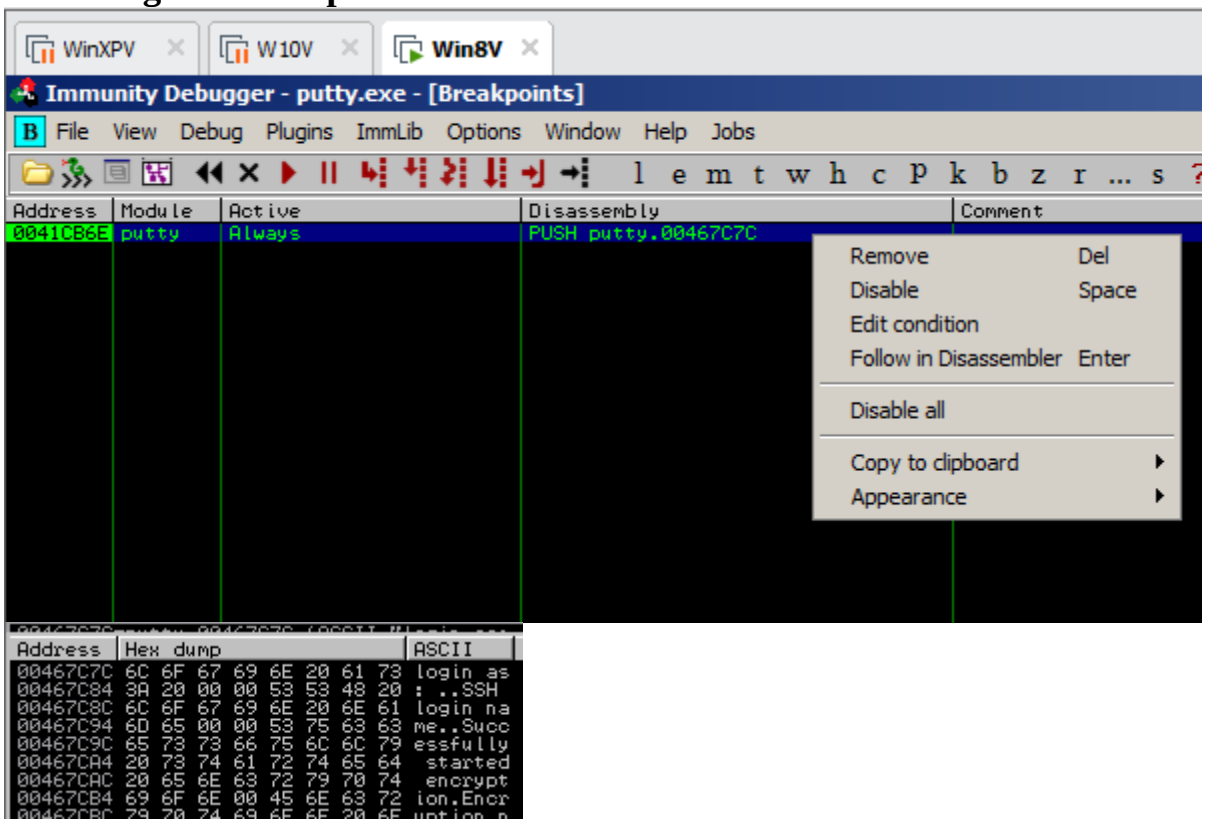

WinXPV
W10V
Win8V
Immunity Debugger - putty.exe - [Text strings referenced in putty:.text]
File View Debug Plugins ImmLib Options Window Help Jobs
Address Disassembly Text string
0041CADF PUSH putty.0046786C ASCII "Access denied♪◘"
0041CB5C MOV DWORD PTR SS:[ESP],putty.00467C88 ASCII "SSH login name"
0041CB6E PUSH putty.00467C7C ASCII "login as: "
0041CBCC PUSH putty.00468C54 ASCII "Using username ""%s".♪◘"
0041CC15 MOV DWORD PTR SS:[ESP],putty.004691F0 ASCII "ssh-connection"
0041CC27 MOV DWORD PTR SS:[ESP],putty.004659D4 ASCII "none"
0041CCA3 PUSH putty.00468C1C ASCII "Strange packet received during a
0041CCC0 PUSH putty.00468BDC ASCII "Server refused public-key signat
0041CCCB PUSH putty.00468BA0 ASCII "Server refused public-key signat
0041CCE0 PUSH putty.00468B6C ASCII "Server refused keyboard-interact
0041CCED PUSH putty.00468B40 ASCII "Keyboard-interactive authenticat
0041CCFD PUSH putty.0046786C ASCII "Access denied♪◘"
0041CD33 MOV EAX,putty.00467B80 ASCII "No username provided"
0041CD80 PUSH putty.00468B20 ASCII "enabling delayed compression"


WinXPV
W10V
Win8V
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
Registers (FPU)
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
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

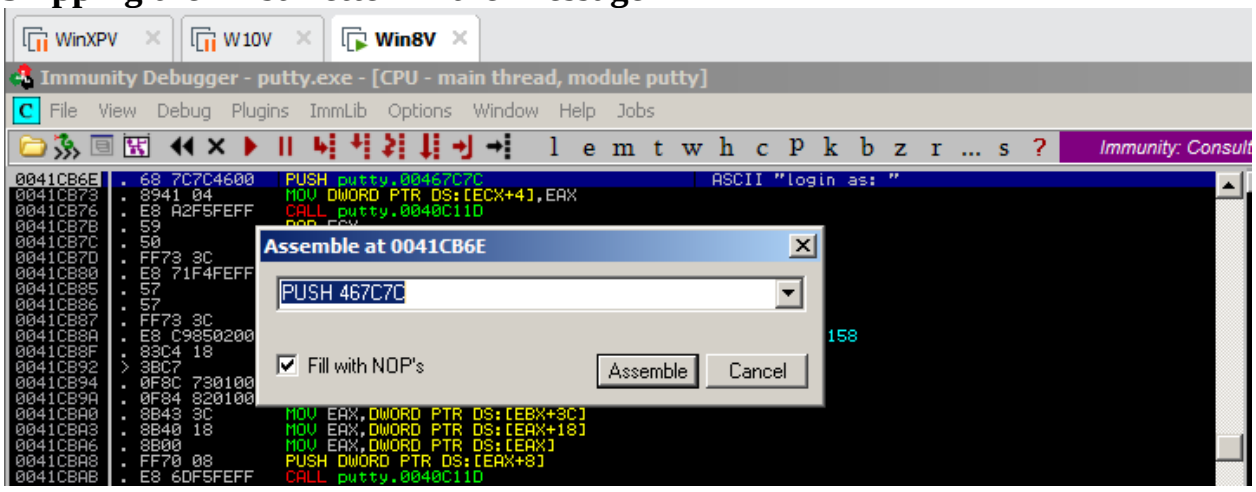

WinXPV
W10V
Win8V
Immunity Debugger - putty.exe - [CPU - main thread, module putty]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
Registers (FPU)

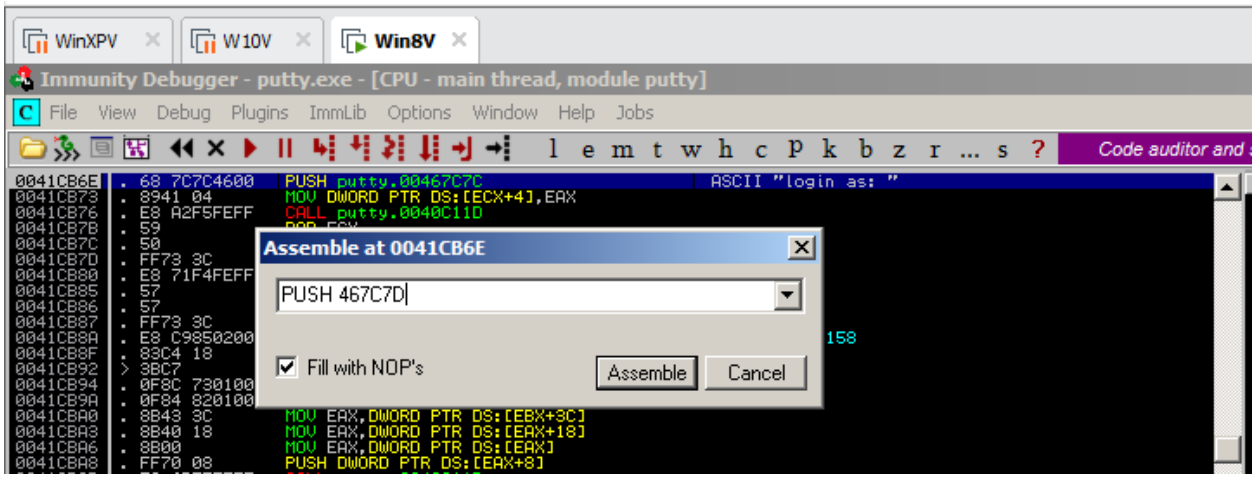
## Task 2: Alter the Login Message

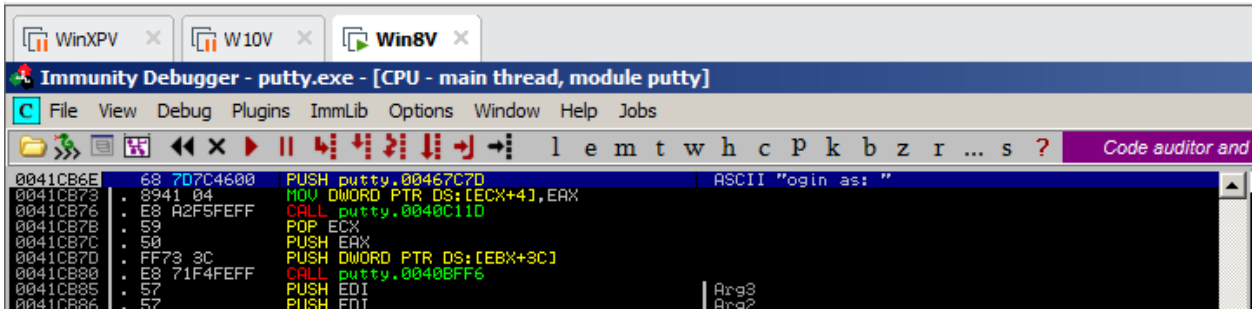
### Removing the Breakpoint



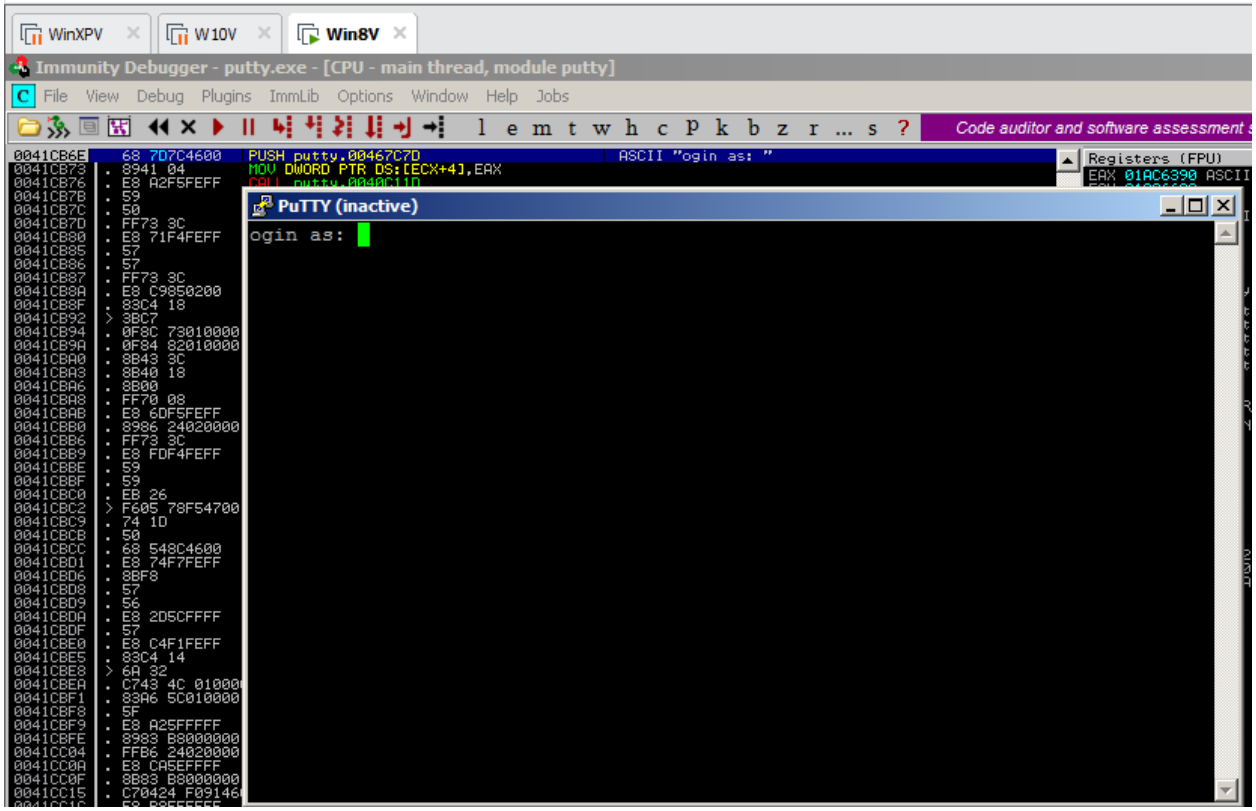

### Skipping the First Letter In the Message



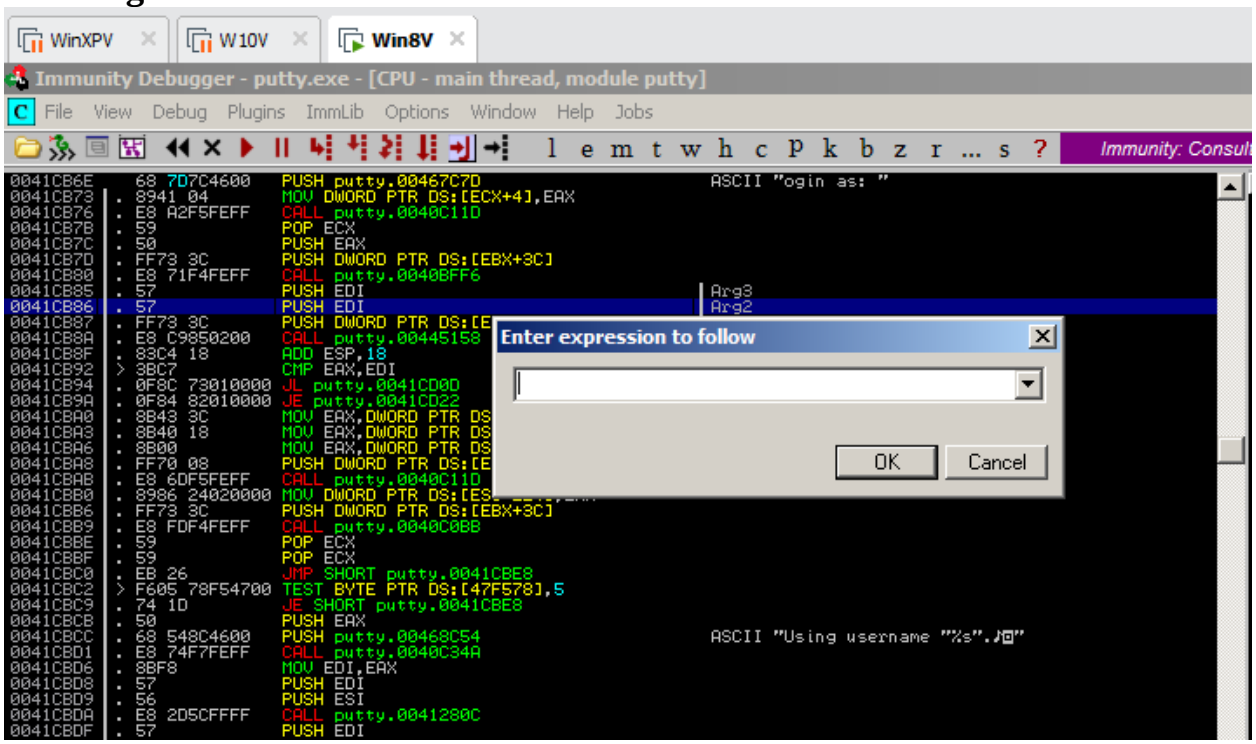


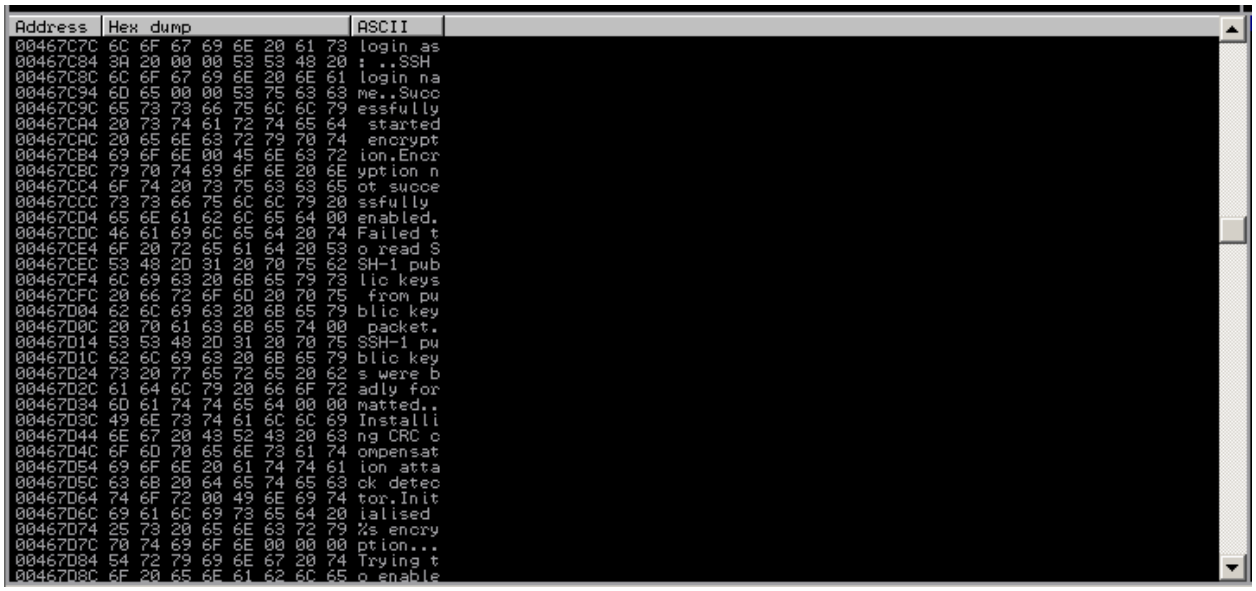



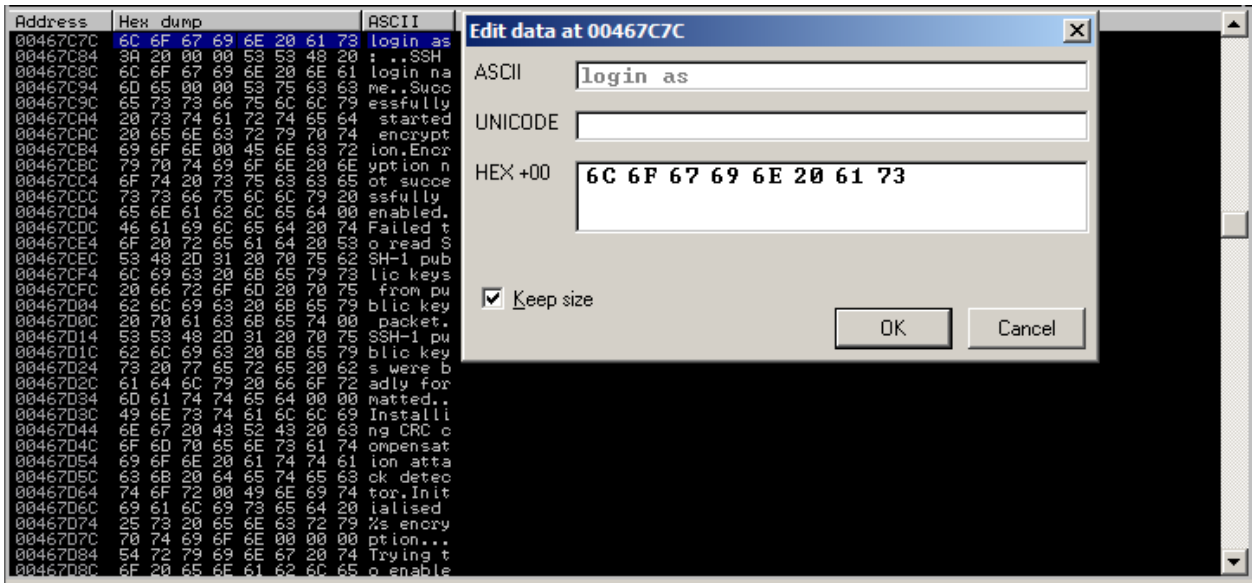

## Running the Modified Program

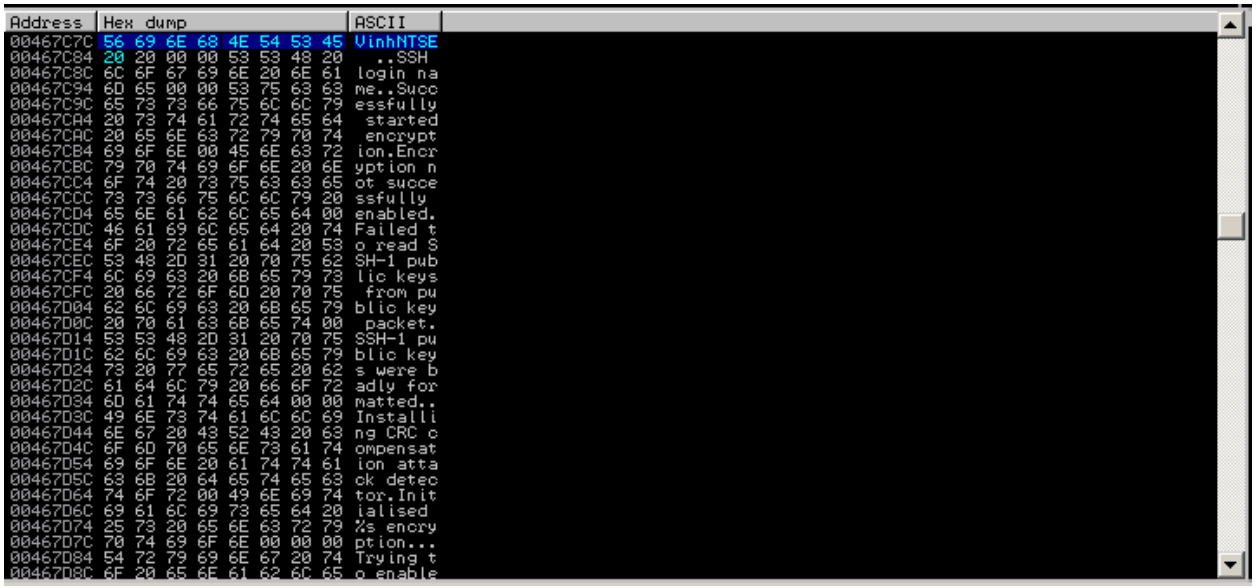


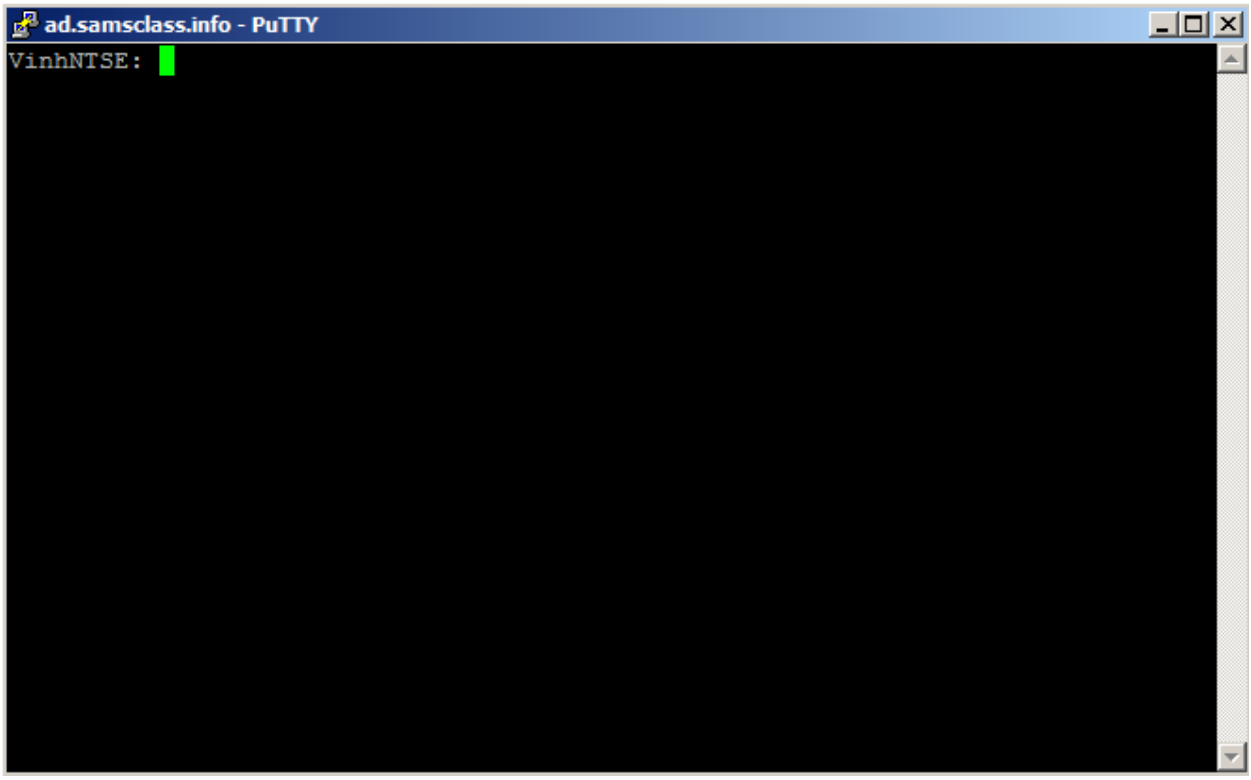
## Inserting Your Name




Address
Hex dump
ASCII
00467C7C 6C 6F 67 69 6E 20 61 73 login as
00467C84 3A 20 00 00 53 53 48 20 : ..SSH
00467C8C 6C 6F 67 69 6E 20 6E 61 login na
00467C94 6D 65 00 00 53 75 63 63 me..Succ
00467C9C 65 73 73 66 75 6C 6C 79 essfully
00467CA4 20 73 74 61 72 74 65 64 started
00467CAC 20 65 6E 63 72 79 70 74 encrypt
00467CB4 69 6F 6E 00 45 6E 63 72 ion.Encr
00467CBC 79 70 74 69 6F 6E 20 6E yption n
00467CC4 6F 74 20 73 75 63 63 65 ot succe
00467CCC 73 73 66 75 6C 6C 79 20 ssfully
00467CD4 65 6E 61 62 6C 65 64 00 enabled.
00467CDC 46 61 69 6C 65 64 20 74 Failed t
00467CE4 6F 20 72 65 61 64 20 53 o read S
00467CEC 53 48 2D 31 20 70 75 62 SH-1 pub
00467CF4 6C 69 63 20 6B 65 79 73 lic keys
00467CFC 20 66 72 6F 6D 20 70 75 from pu
00467D04 62 6C 69 63 20 6B 65 79 blic key
00467D0C 20 70 61 63 6B 65 74 00 packet.
00467D14 53 53 48 2D 31 20 70 75 SSH-1 pu
00467D1C 62 6C 69 63 20 6B 65 79 blic key
00467D24 73 20 77 65 72 65 20 62 s were b
00467D2C 61 64 6C 79 20 66 6F 72 adly for
00467D34 6D 61 74 74 65 64 00 00 matted..
00467D3C 49 6E 73 74 61 6C 6C 69 Installi
00467D44 6E 67 20 43 52 43 20 63 ng CRC c
00467D4C 6F 6D 70 65 6E 73 61 74 ompensat
00467D54 69 6F 6E 20 61 74 74 61 ion atta
00467D5C 63 6B 20 64 65 74 65 63 ck detec
00467D64 74 6F 72 00 49 6E 69 74 tor.Init
00467D6C 69 61 6C 69 73 65 64 20 ialised
00467D74 25 73 20 65 6E 63 72 79 %s encry
00467D7C 70 74 69 6F 6E 00 00 00 ption...
00467D84 54 72 79 69 6E 67 20 74 Trying t
00467D8C 6F 20 65 6E 61 62 6C 65 o enable
Edit data at 00467C7C
ASCII
login as
UNICODE
HEX +00
6C 6F 67 69 6E 20 61 73
Keep size
OK
Cancel


Address
Hex dump
ASCII
00467C7C 56 69 6E 68 4E 54 53 45 VinhNTSE
00467C84 20 20 00 00 53 53 48 20 ..SSH
00467C8C 6C 6F 67 69 6E 20 6E 61 login na
00467C94 6D 65 00 00 53 75 63 63 me..Succ
00467C9C 65 73 73 66 75 6C 6C 79 essfully
00467CA4 20 73 74 61 72 74 65 64 started
00467CAC 20 65 6E 63 72 79 70 74 encrypt
00467CB4 69 6F 6E 00 45 6E 63 72 ion.Encr
00467CBC 79 70 74 69 6F 6E 20 6E yption n
00467CC4 6F 74 20 73 75 63 63 65 ot succe
00467CCC 73 73 66 75 6C 6C 79 20 ssfully
00467CD4 65 6E 61 62 6C 65 64 00 enabled.
00467CDC 46 61 69 6C 65 64 20 74 Failed t
00467CE4 6F 20 72 65 61 64 20 53 o read S
00467CEC 53 48 2D 31 20 70 75 62 SH-1 pub
00467CF4 6C 69 63 20 6B 65 79 73 lic keys
00467CFC 20 66 72 6F 6D 20 70 75 from pu
00467D04 62 6C 69 63 20 6B 65 79 blic key
00467D0C 20 70 61 63 6B 65 74 00 packet.
00467D14 53 53 48 2D 31 20 70 75 SSH-1 pu
00467D1C 62 6C 69 63 20 6B 65 79 blic key
00467D24 73 20 77 65 72 65 20 62 s were b
00467D2C 61 64 6C 79 20 66 6F 72 adly for
00467D34 6D 61 74 74 65 64 00 00 matted..
00467D3C 49 6E 73 74 61 6C 6C 69 Installi
00467D44 6E 67 20 43 52 43 20 63 ng CRC c
00467D4C 6F 6D 70 65 6E 73 61 74 ompensat
00467D54 69 6F 6E 20 61 74 74 61 ion atta
00467D5C 63 6B 20 64 65 74 65 63 ck detec
00467D64 74 6F 72 00 49 6E 69 74 tor.Init
00467D6C 69 61 6C 69 73 65 64 20 ialised
00467D74 25 73 20 65 6E 63 72 79 %s encry
00467D7C 70 74 69 6F 6E 00 00 00 ption...
00467D84 54 72 79 69 6E 67 20 74 Trying t
00467D8C 6F 20 65 6E 61 62 6C 65 o enable


ad.samsclass.info - PuTTY
VinhNTSE: