Lab 19: EXE With Trojan Code in a New Section

Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 18/3/2023

What You Need

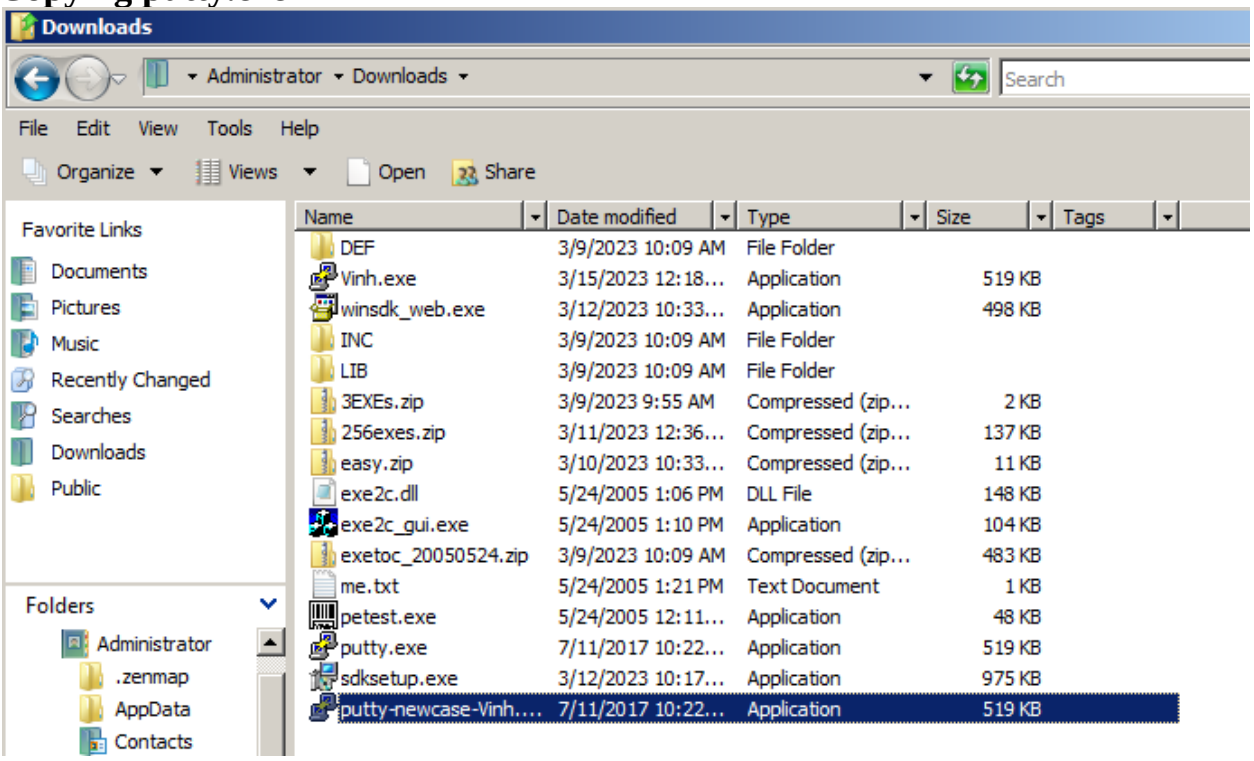
A Windows machine, real or virtual. I used a Windows Server 2008 virtual machine.

Purpose

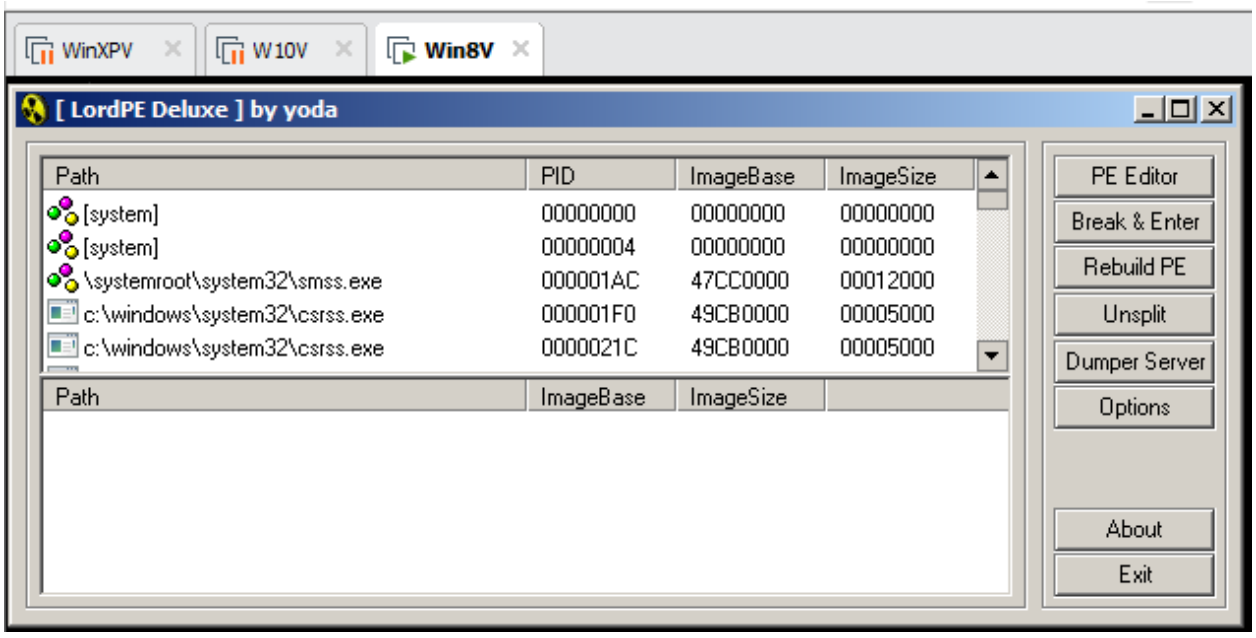
To modify a Windows EXE file and save an altered version containing Trojan code in a new PE section. This gives you practice with very simple features of the Immunity debugger and LordPE

Task 1: Add a Section with LordPE

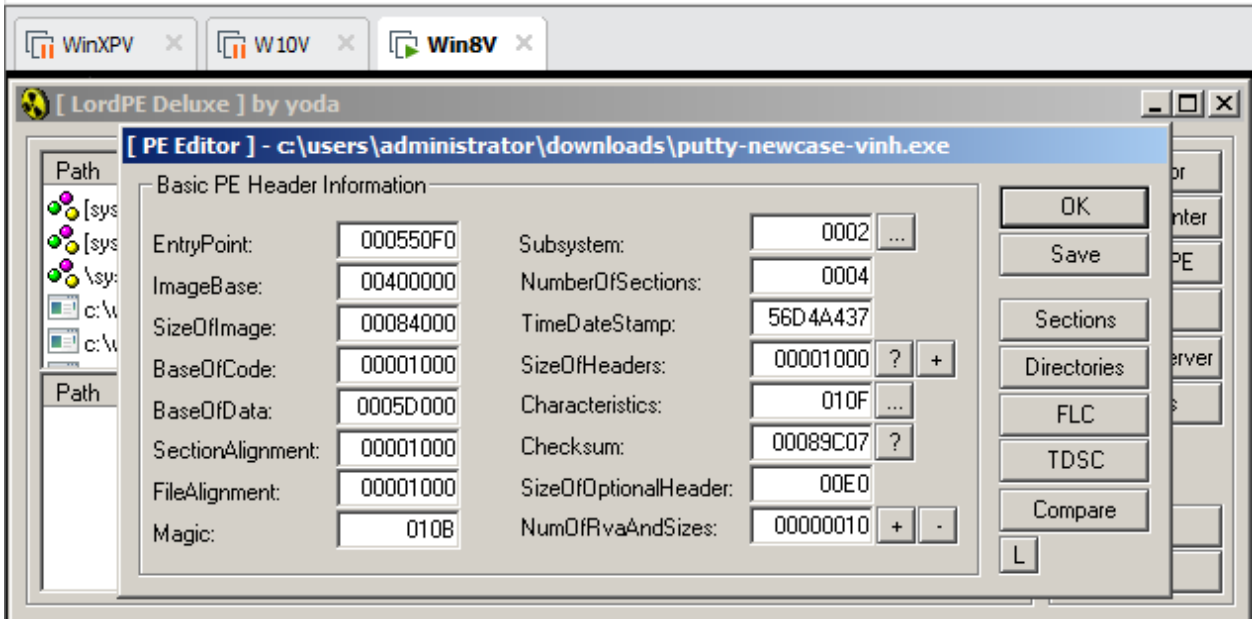
Copying putty.exe

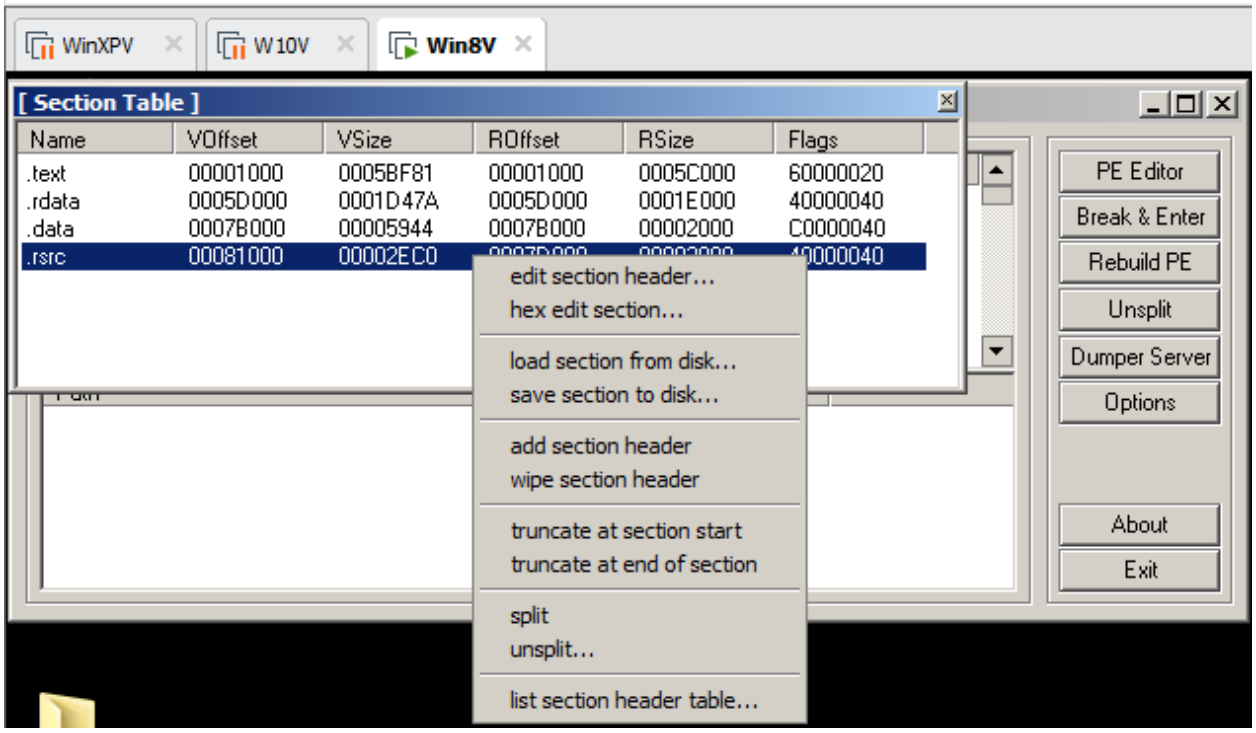


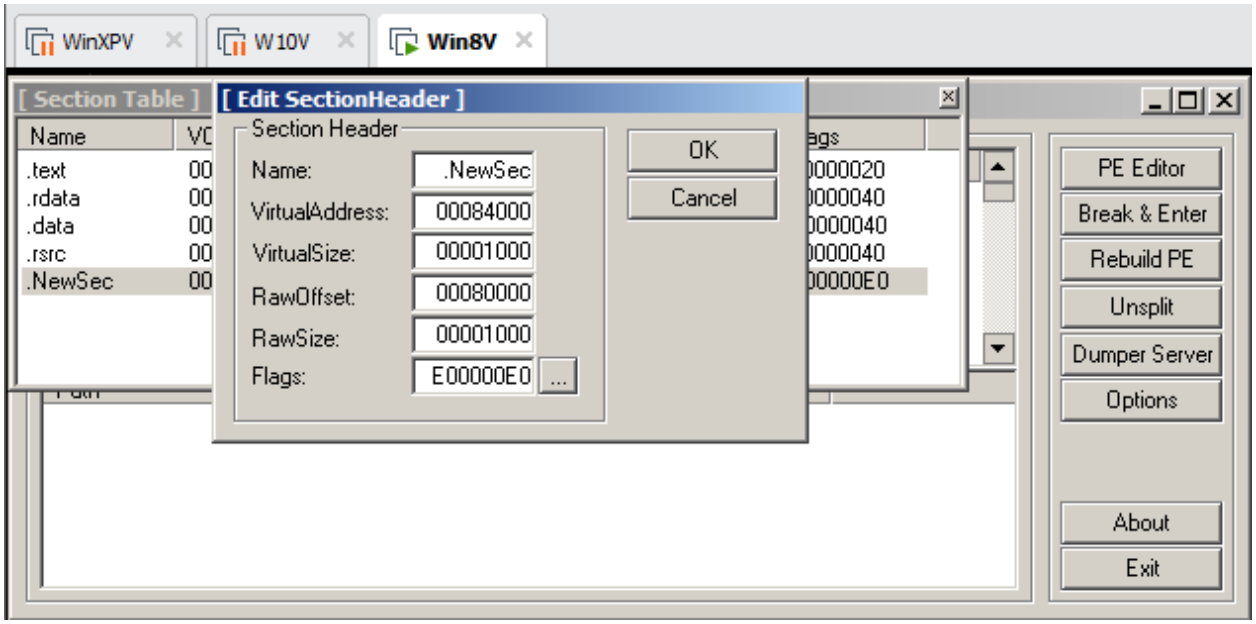
Getting LordPE

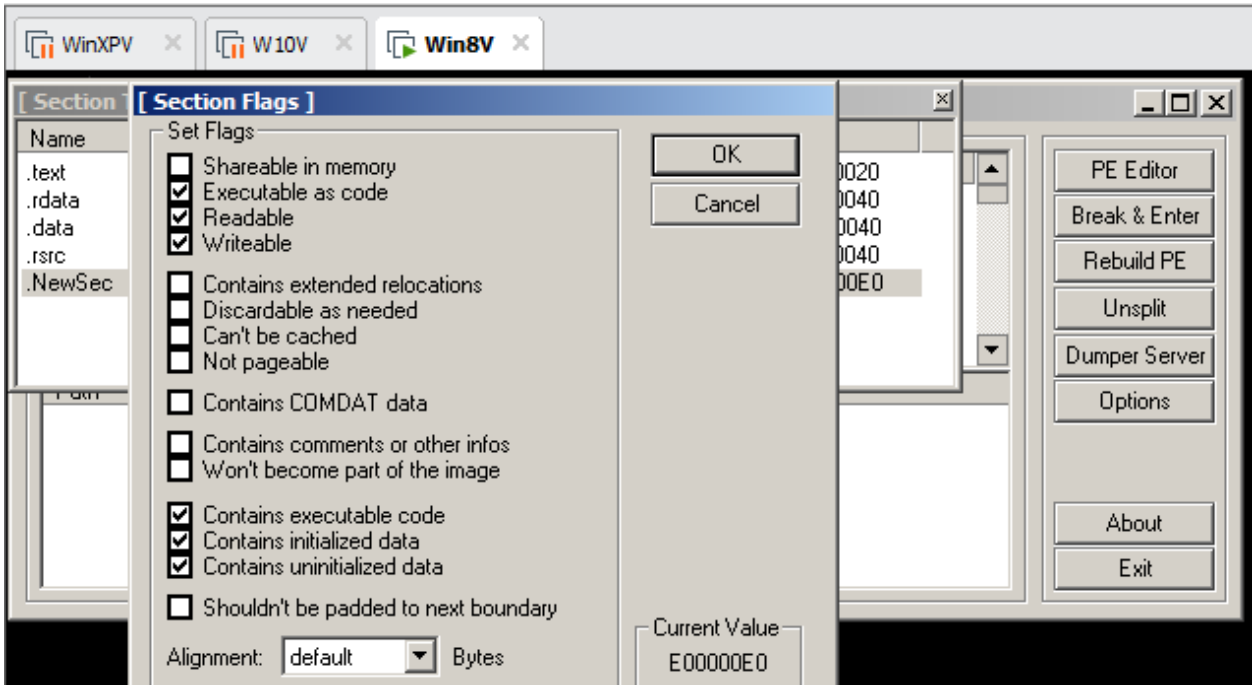


Adding a New Section to the PE Header



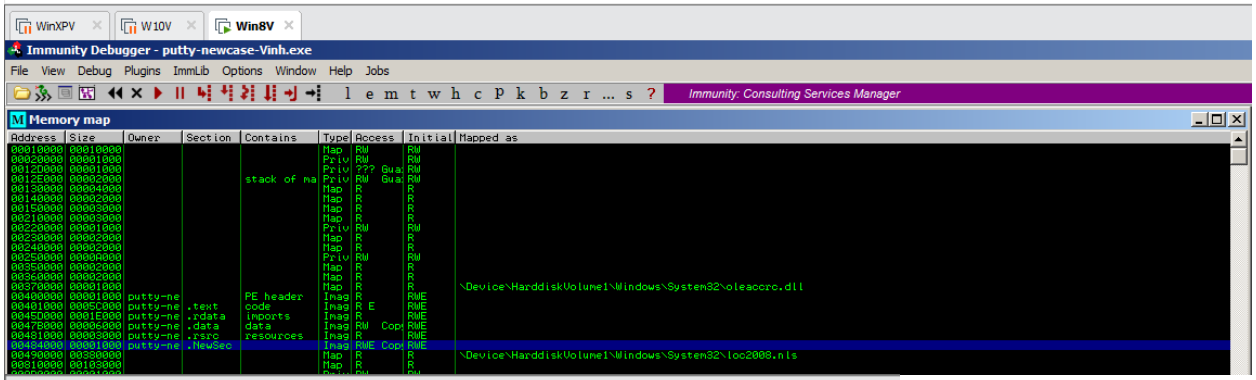

WinXPV
W10V
Win8V
[Section Table]
Name VOffset VSize ROffset RSize Flags
.text 00001000 0005BF81 00001000 0005C000 60000020
.rdata 0005D000 0001D47A 0005D000 0001E000 40000040
.data 0007B000 00005944 0007B000 00002000 C0000040
.rsrc 00081000 00002EC0 40000040
edit section header...
hex edit section...
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...
PE Editor
Break & Enter
Rebuild PE
Unsplit
Dumper Server
Options
About
Exit

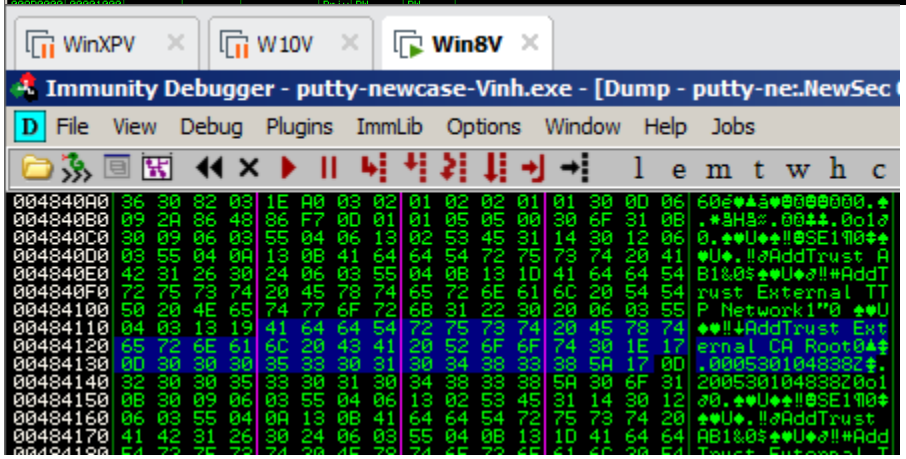

WinXPV
W10V
Win8V
[Section Table]
[Edit SectionHeader]
Section Header
Name: .NewSec
VirtualAddress: 00084000
VirtualSize: 00001000
RawOffset: 00080000
RawSize: 00001000
Flags: E00000E0
OK
Cancel
.text
.rdata
.data
.rsrc
.NewSec
PE Editor
Break & Enter
Rebuild PE
Unsplit
Dumper Server
Options
About
Exit



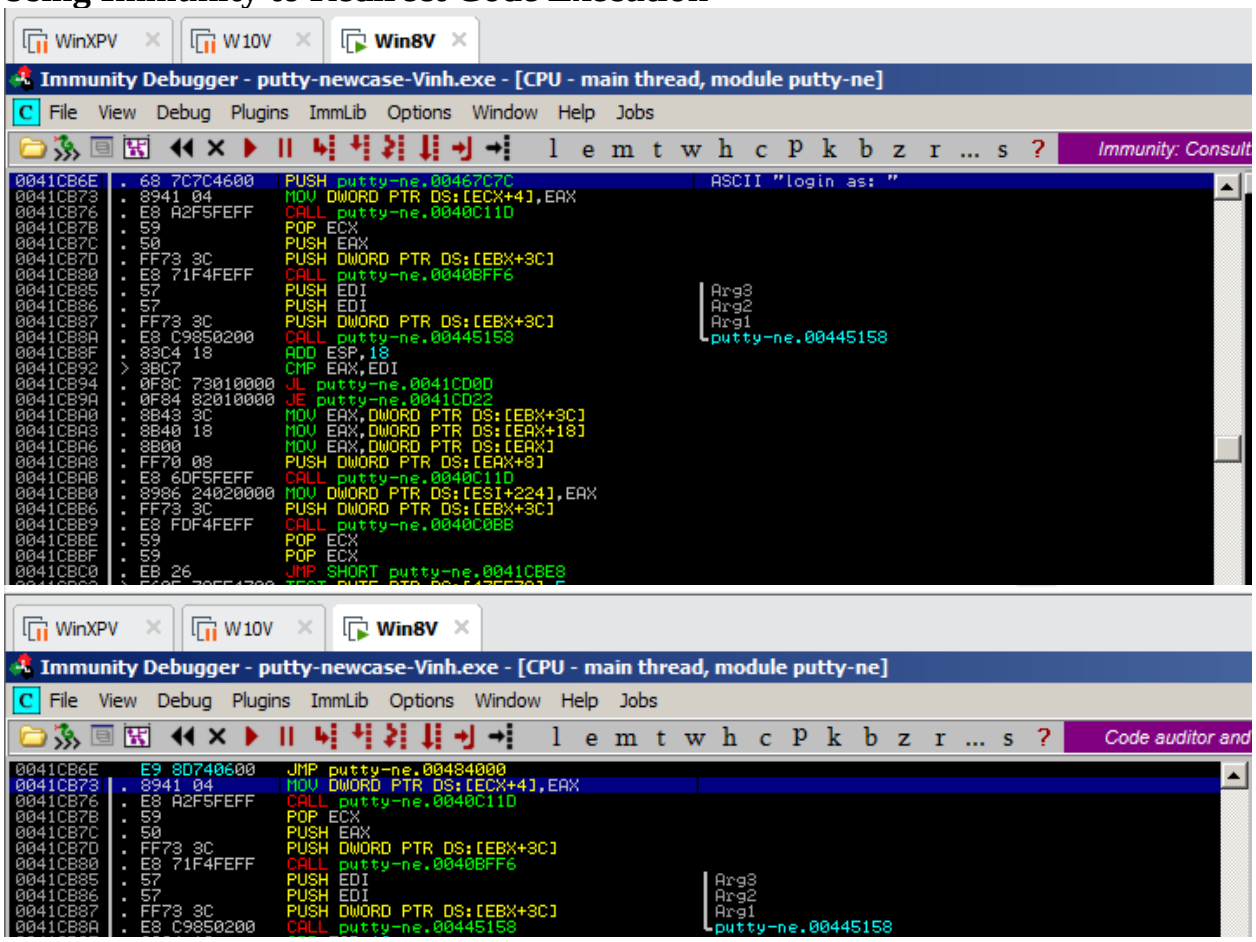
Task 2: Redirecting Code Execution with Immunity

Using Immunity to Examine the NewSec Section

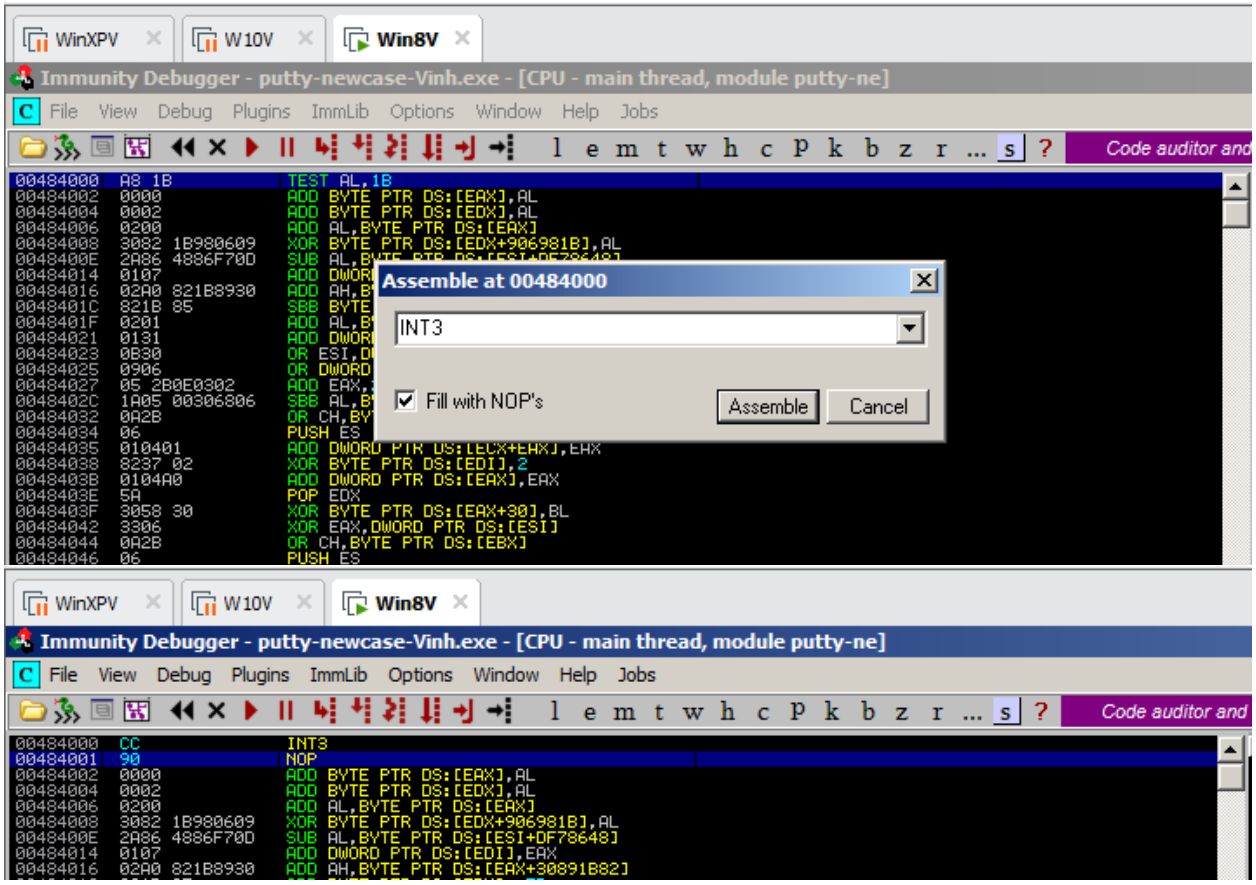




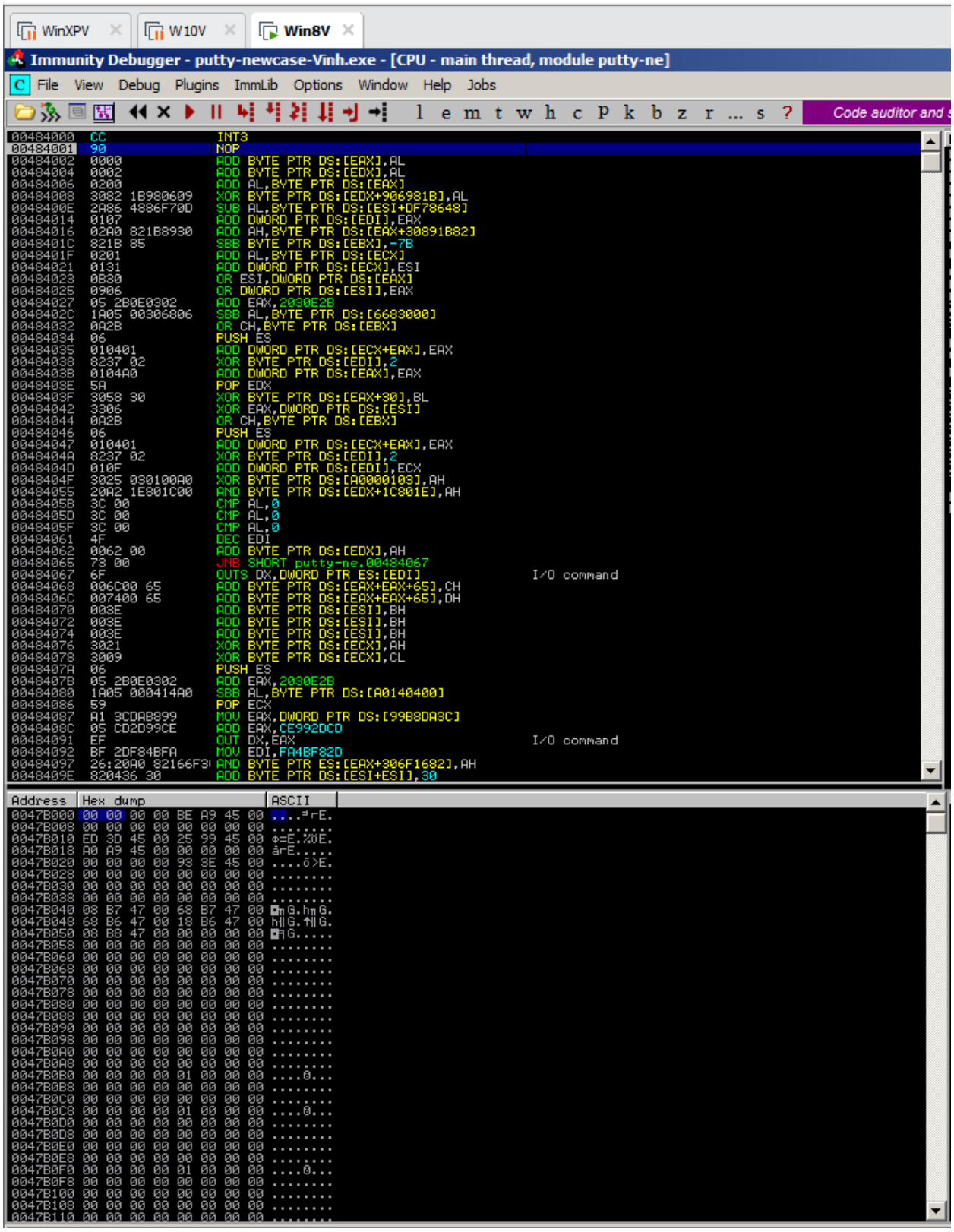
Using Immunity to Redirect Code Execution



Adding Trojan Code

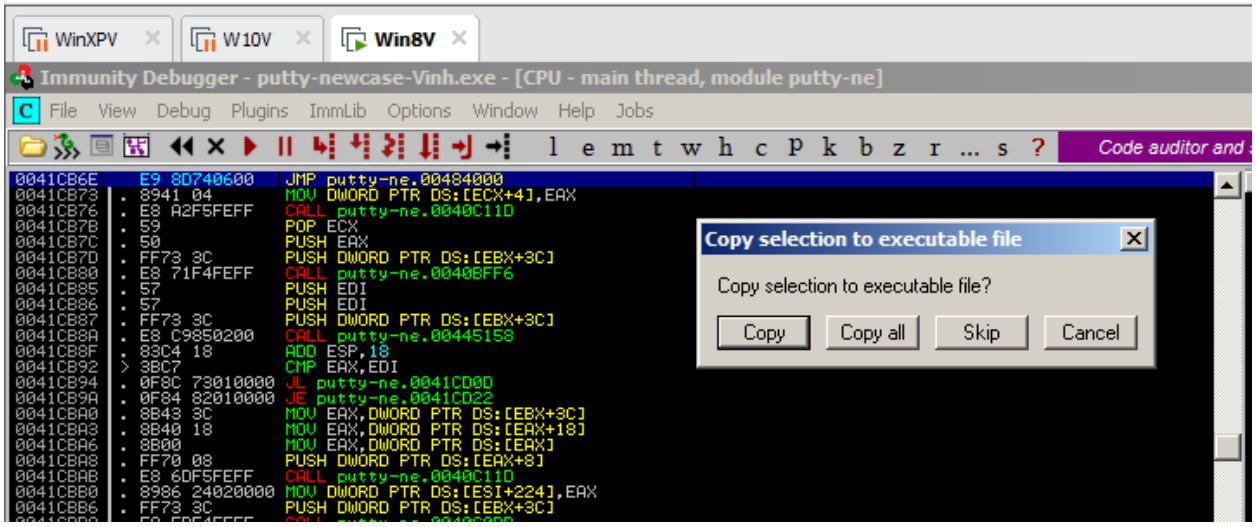


Running the Modified App in Immunity

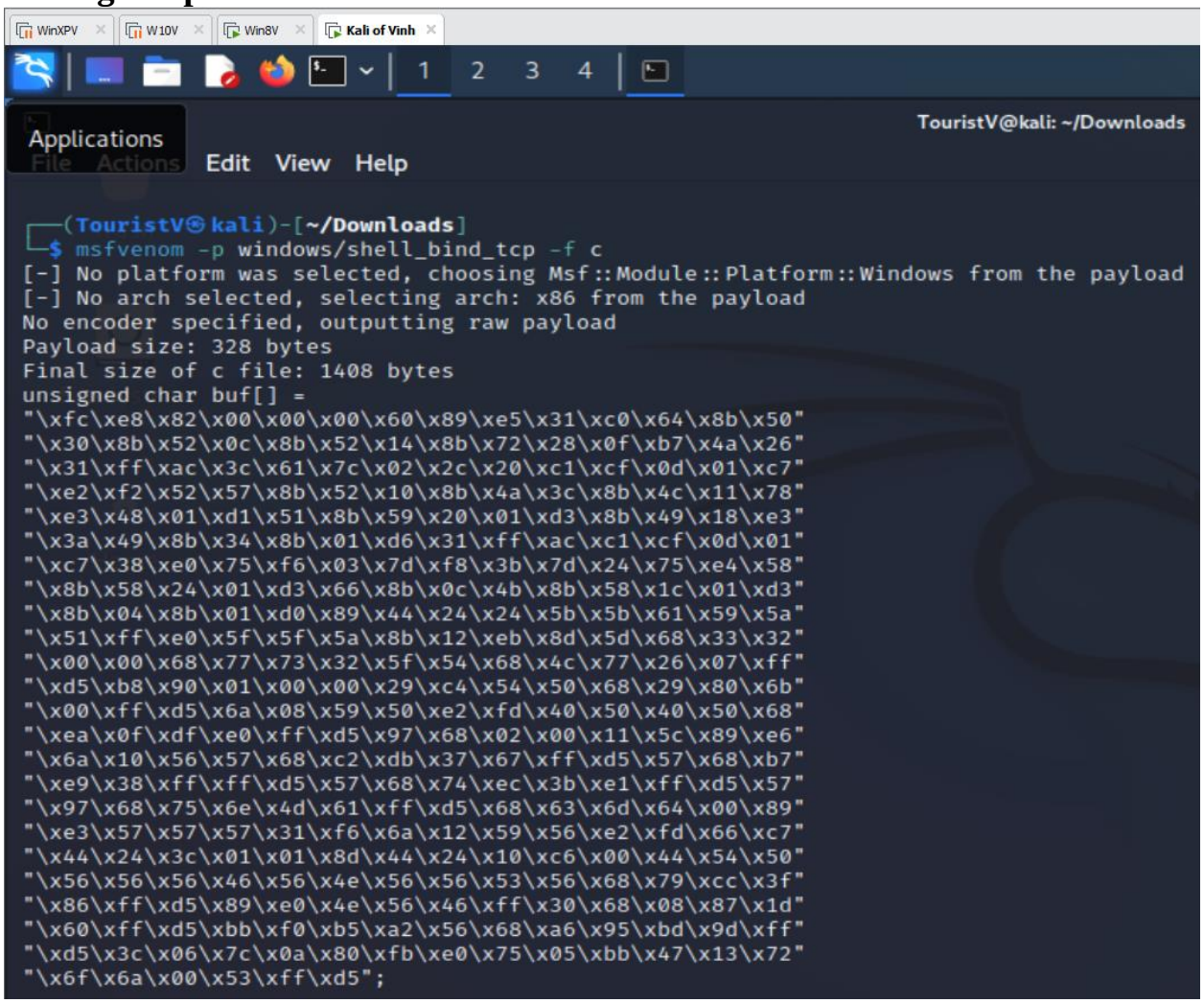


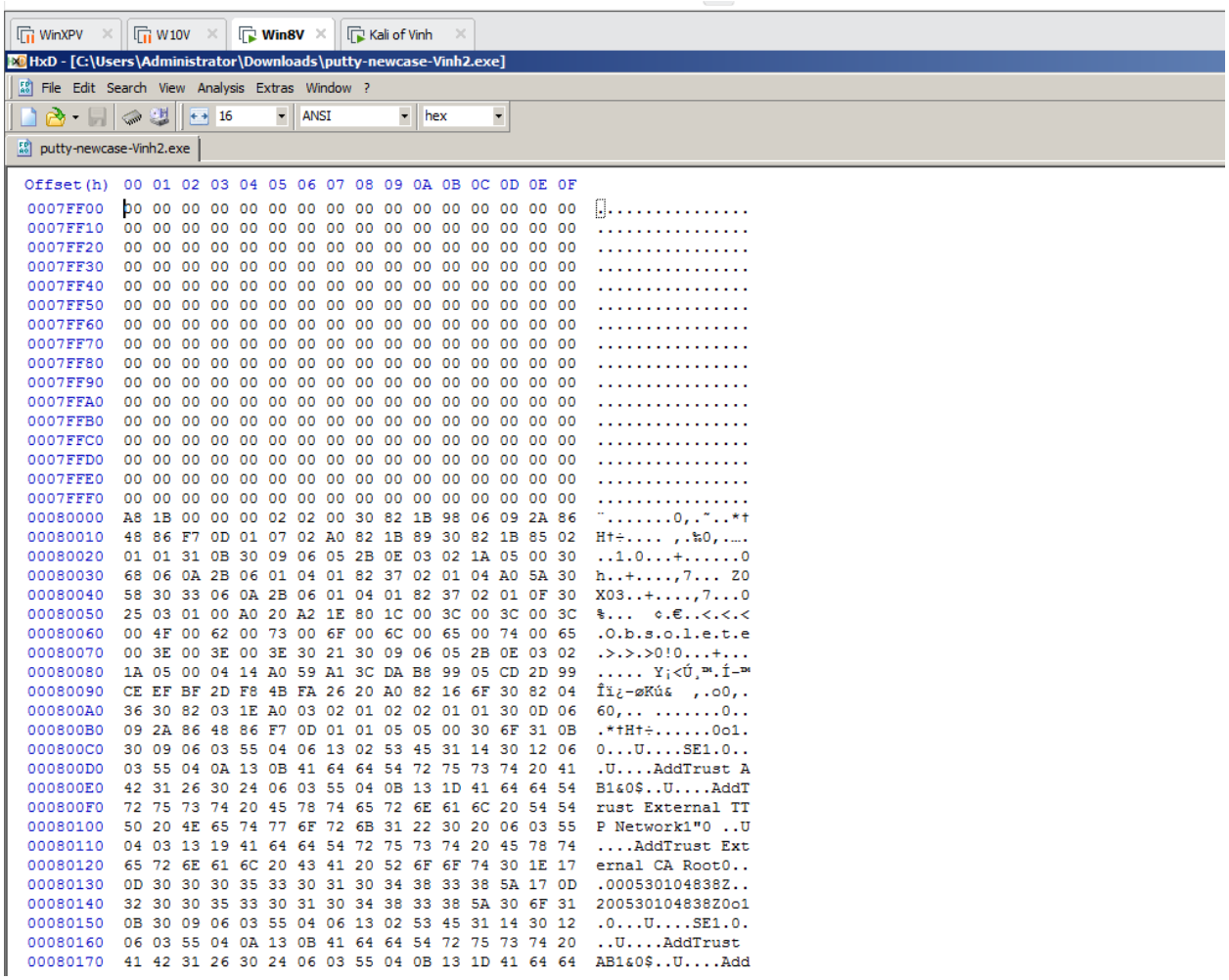
Task 3: Inserting Real Shellcode

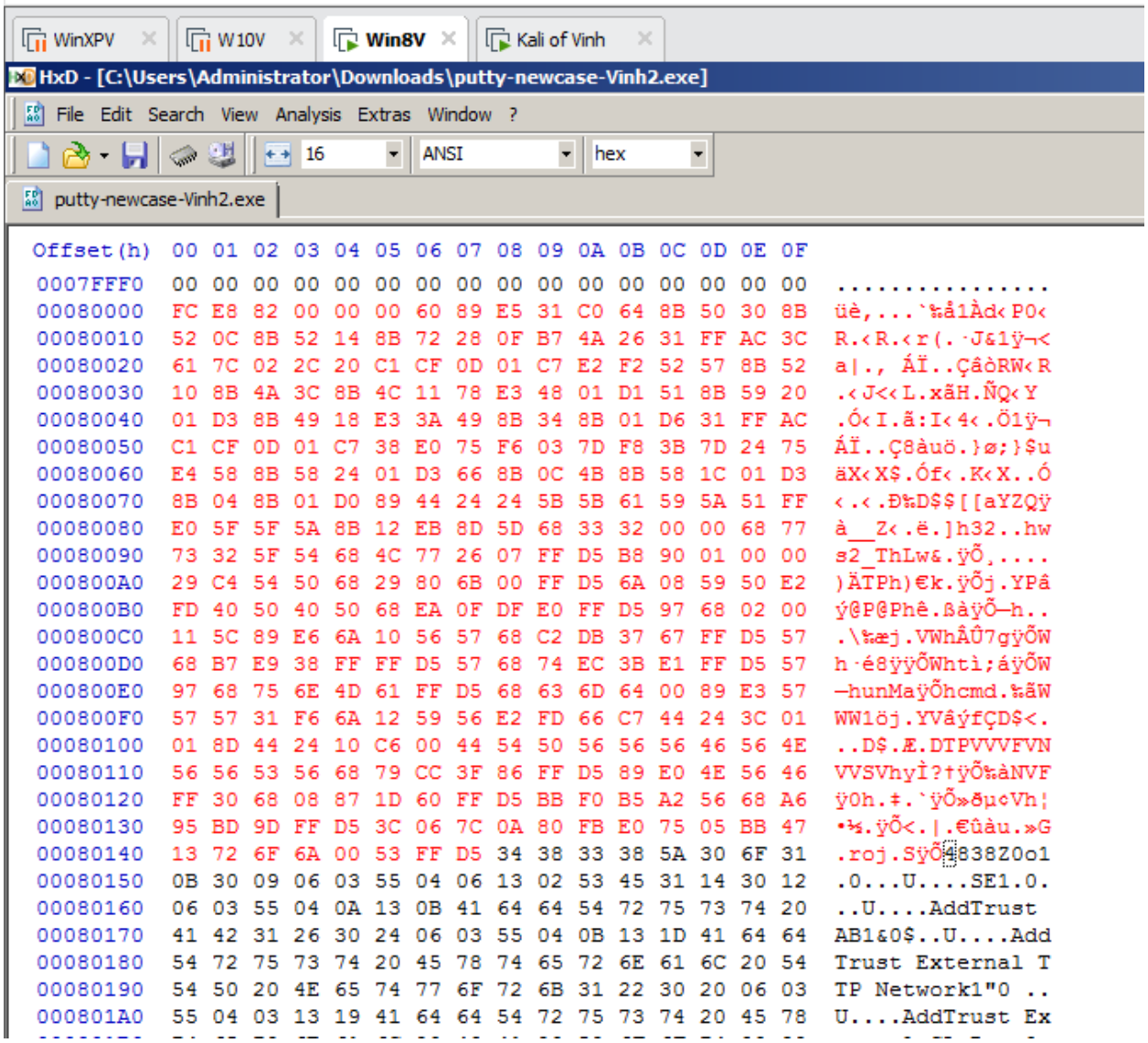
Saving the Modified EXE



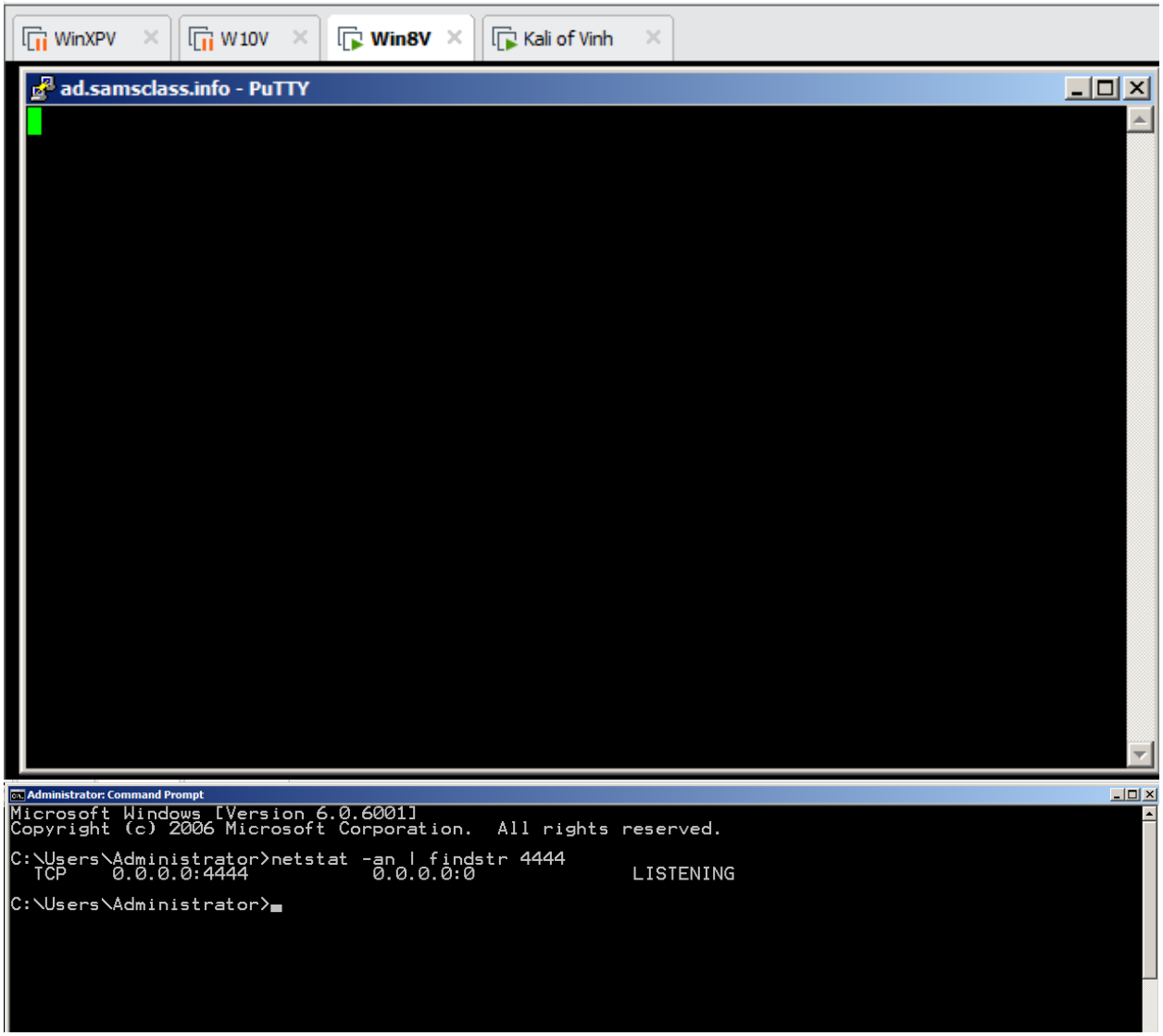
Getting Simple Shellcode




WinXPV
W10V
Win8V
Kali of Vinh
HxD - [C:\Users\Administrator\Downloads\putty-newcase-Vinh2.exe]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
putty-newcase-Vinh2.exe
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0007FF00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FF10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FF20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FF30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FF40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FF50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FF60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FF70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FF80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FF90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FFA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FFB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FFC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FFD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FFE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0007FFF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00080000 A8 1B 00 00 00 02 02 00 30 82 1B 98 06 09 2A 86 ¨.......0,.˜..*†
00080010 48 86 F7 0D 01 07 02 A0 82 1B 89 30 82 1B 85 02 H†÷.... ,.‰0,….
00080020 01 01 31 0B 30 09 06 05 2B 0E 03 02 1A 05 00 30 ..1.0...+......0
00080030 68 06 0A 2B 06 01 04 01 82 37 02 01 04 A0 5A 30 h..+....,7... Z0
00080040 58 30 33 06 0A 2B 06 01 04 01 82 37 02 01 0F 30 X03..+....,7...0
00080050 25 03 01 00 A0 20 A2 1E 80 1C 00 3C 00 3C 00 3C %... ¢.€..<.<.<
00080060 00 4F 00 62 00 73 00 6F 00 6C 00 65 00 74 00 65 .O.b.s.o.l.e.t.e
00080070 00 3E 00 3E 00 3E 30 21 30 09 06 05 2B 0E 03 02 .>.>.>0!0...+...
00080080 1A 05 00 04 14 A0 59 A1 3C DA B8 99 05 CD 2D 99 ..... Y¡<Ú¸™.Í-™
00080090 CE EF BF 2D F8 4B FA 26 20 A0 82 16 6F 30 82 04 Îï¿-øKú& ,.o0,.
000800A0 36 30 82 03 1E A0 03 02 01 02 02 01 01 30 0D 06 60,.. ....0..
000800B0 09 2A 86 48 86 F7 0D 01 01 05 05 00 30 6F 31 0B .*†H†÷......0o1.
000800C0 30 09 06 03 55 04 06 13 02 53 45 31 14 30 12 06 0...U....SE1.0..
000800D0 03 55 04 0A 13 0B 41 64 64 54 72 75 73 74 20 41 .U....AddTrust A
000800E0 42 31 26 30 24 06 03 55 04 0B 13 1D 41 64 64 54 B1&0$..U....AddT
000800F0 72 75 73 74 20 45 78 74 65 72 6E 61 6C 20 54 54 rust External TT
00080100 50 20 4E 65 74 77 6F 72 6B 31 22 30 20 06 03 55 P Network1"0 ..U
00080110 04 03 13 19 41 64 64 54 72 75 73 74 20 45 78 74 ....AddTrust Ext
00080120 65 72 6E 61 6C 20 43 41 20 52 6F 6F 74 30 1E 17 ernal CA Root0..
00080130 0D 30 30 30 35 33 30 31 30 34 38 33 38 5A 17 0D .000530104838Z..
00080140 32 30 30 35 33 30 31 30 34 38 33 38 5A 30 6F 31 200530104838Z0o1
00080150 0B 30 09 06 03 55 04 06 13 02 53 45 31 14 30 12 .0...U....SE1.0.
00080160 06 03 55 04 0A 13 0B 41 64 64 54 72 75 73 74 20 ..U....AddTrust
00080170 41 42 31 26 30 24 06 03 55 04 0B 13 1D 41 64 64 AB1&0$..U....Add



Running the Trojaned Putty



Connecting to the Target