

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
MÃ ĐỘC

BÀI THỰC HÀNH SỐ 05
Sử dụng ollydbg phân tích mã độc

Người thực hiện bài thực hành:

TS. Đặng Xuân Bảo

Hà Nội, 2020

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH.....	3
CHUẨN BỊ BÀI THỰC HÀNH.....	4
Sử dụng ollydbg phân tích mã độc	5
1.1. Mô tả	5
1.2. Chuẩn bị	5
1.3. Phân tích Lab09-01	5

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Sử dụng ollydbg phân tích mã độc

Học phần: Mã độc

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
 - + Máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 4GB, HDD 500GB
- Yêu cầu phần mềm trên máy:
 - + Hệ điều hành Windows 10
 - + VMware Workstation 15.0
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

Sử dụng ollydbg phân tích mã độc

1.1. Mô tả

Bài thực hành hướng dẫn sinh viên sử dụng một số công cụ trong việc phân tích động một số mẫu mã độc đơn giản..

1.2. Chuẩn bị

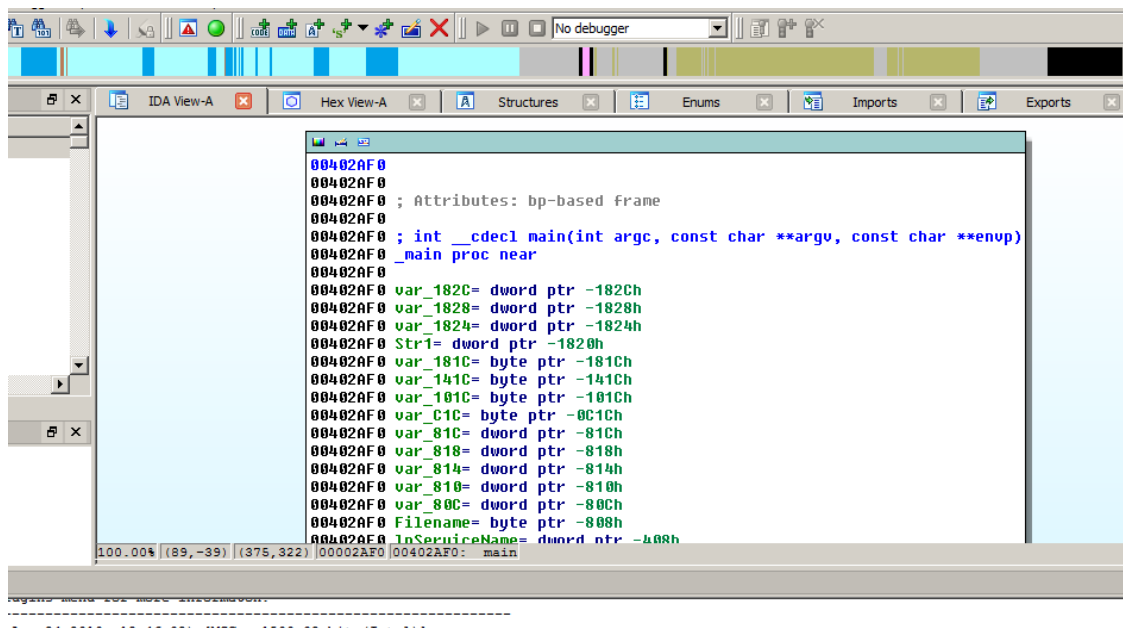
- Môi trường phân tích mã độc đã xây dựng trong Lab 1.

1.3. Phân tích Lab09-01

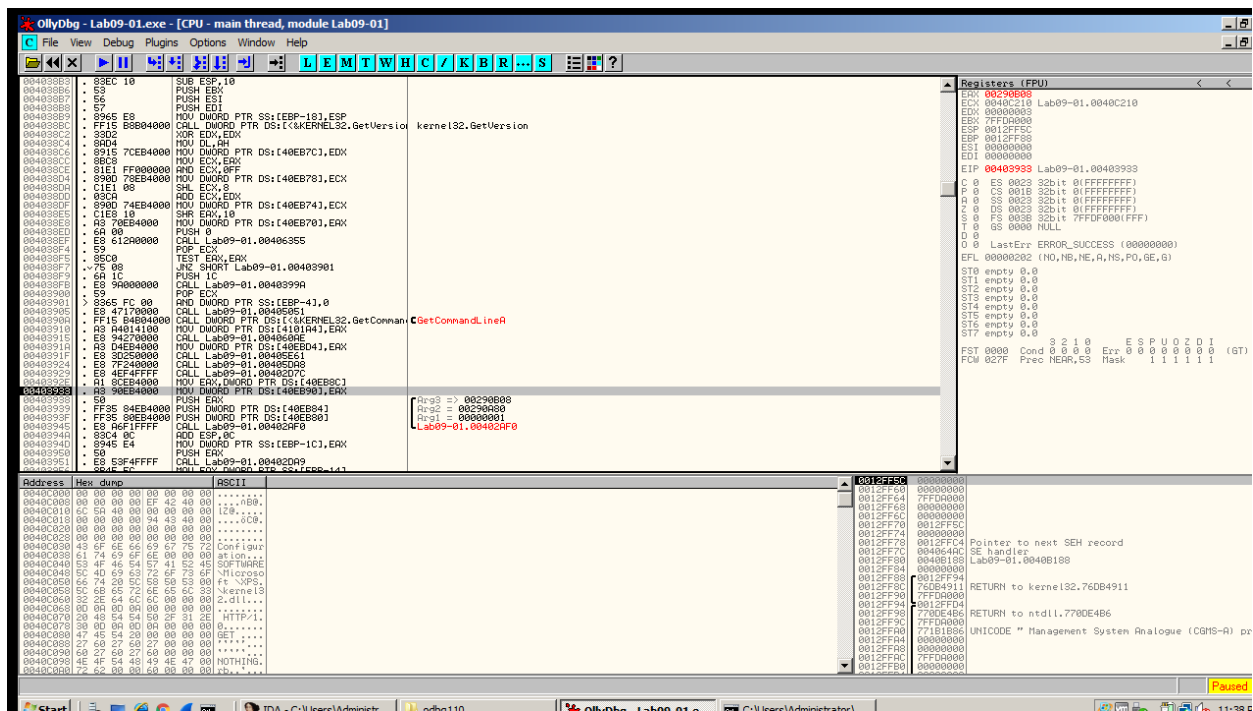
Thực hiện các yêu cầu với Lab09-01.exe có trong tài liệu Practical Malware Analysis.

Tìm điểm bắt đầu của hàm main

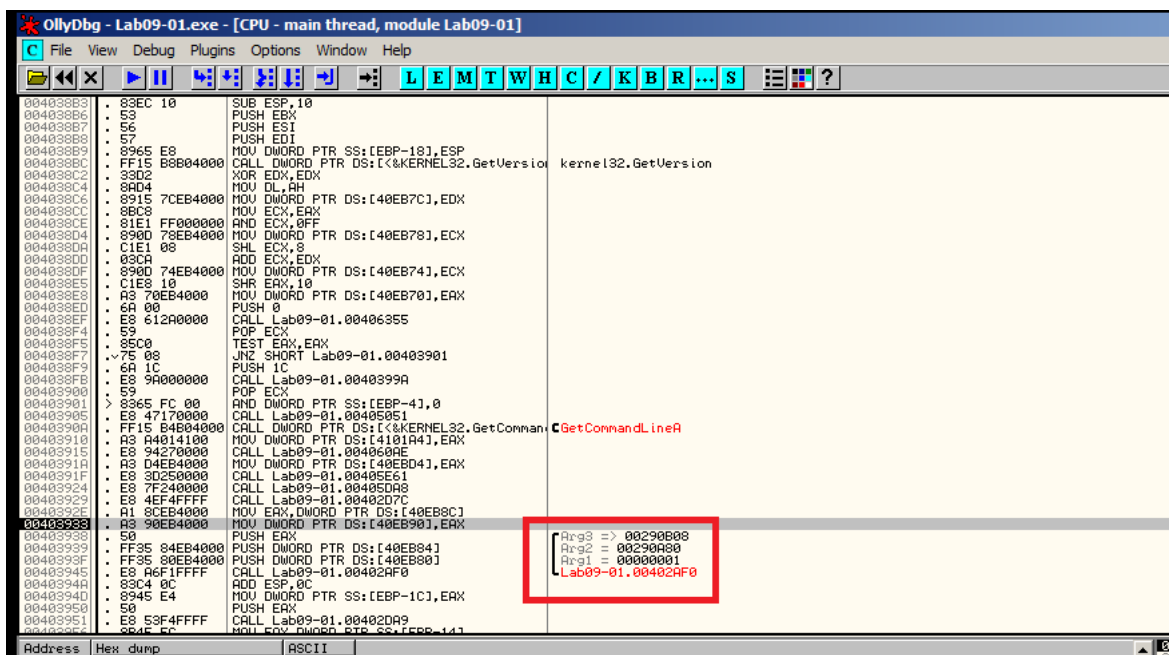
- Sử dụng IDA pro để phân tích Lab09-01.exe.
- Chọn Option → General, đánh dấu Line Prefixes, chọn OK.
- Sau đó chọn Window, “Reset Desktop”
- IDA pro sẽ hiển thị địa chỉ hàm main tại 0x402AF0



Dùng ollydbg đọc Lab09-01.exe



- Nhấn F8 40 lần, để đến được địa chỉ 0x403933, cuộn xuống vài dòng ta sẽ thấy được mã đối số và hàm gọi chính.



- Tiếp tục nhấn F7 5 lần để tải các tham số và gọi hàm main từ địa chỉ 0x403945, phần mã mới hiển thị bắt đầu từ địa chỉ 0x402AF0.

OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]

File View Debug Plugins Options Window Help

File View Debug Plugins Options Window Help

00402B00 8BEC MOV EBP,ESP
 00402B01 8B2C MOV EAX,12C
 00402B02 E8 B3030000 CALL Lab09-01.00402EB0
 00402B03 837D 08 01 CMP DWORD PTR SS:[EBP+8],1
 00402B04 JNZ SHORT Lab09-01.00402B1D
 00402B05 E8 F8E4FFFF CALL Lab09-01.00401800
 00402B06 85C0 TEST EAX,EAX
 00402B07 J74 07 JE SHORT Lab09-01.00402B13
 00402B08 E8 4FF8FFFF CALL Lab09-01.00402360
 00402B09 JEB 05 JMP SHORT Lab09-01.00402B18
 00402B0A E8 F8F8FFFF CALL Lab09-01.00402410
 00402B0B J9 59020000 JMP Lab09-01.00402076
 00402B0C 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
 00402B0D 8B40 0C MOV ECX,DWORD PTR SS:[EBP+C]
 00402B0E 8B54 14 MOV EDX,DWORD PTR DS:[ECX+4]
 00402B0F 8B55 FC MOV DWORD PTR SS:[EBP-4],EDX
 00402B10 8B45 FC MOV EAX,DWORD PTR SS:[EBP-4]
 00402B11 50 PUSH EAX
 00402B12 E8 DD9FFFFF CALL Lab09-01.00402510
 00402B13 83C4 04 ADD ESP,4
 00402B14 85C0 TEST EAX,EAX
 00402B15 J75 05 JNZ SHORT Lab09-01.00402B3F
 00402B16 E8 D1F8FFFF CALL Lab09-01.00402410
 00402B17 8B40 0C MOV ECX,DWORD PTR SS:[EBP+C]
 00402B18 8B51 14 MOV EDX,DWORD PTR DS:[ECX+4]
 00402B19 8B95 E0E7FFFF MOV DWORD PTR SS:[EBP-1820],EDX
 00402B1A 68 70C14000 PUSH Lab09-01.0040C170
 00402B1B 8B95 E0E7FFFF MOV EAX,DWORD PTR SS:[EBP-1820]
 00402B1C 50 PUSH EAX
 00402B1D E8 B30C0000 CALL Lab09-01.0040380F
 00402B1E 83C4 08 ADD ESP,8
 00402B1F 85C0 TEST EAX,EAX
 00402B20 J75 64 JNZ SHORT Lab09-01.00402B27
 00402B21 837D 08 03 CMP DWORD PTR SS:[EBP+8],3
 00402B22 JNZ SHORT Lab09-01.00402B9A
 00402B23 68 00040000 PUSH 400
 00402B24 8B40 0C MOV ECX,DWORD PTR SS:[EBP-404]
 00402B25 51 PUSH ECX
 00402B26 E8 36FAFFFF CALL Lab09-01.004025B0
 00402B27 83C4 08 ADD ESP,8
 00402B28 85C0 TEST EAX,EAX
 00402B29 J74 08 JE SHORT Lab09-01.00402B89
 00402B2A 83C8 FF OR EAX,FFFFFFFF
 00402B2B E8 FF010000 CALL Lab09-01.00402078

Registers: EAX 002, ECX 004, EDI 000, EBP 7FF, ESP 001, ESI 000, EDI 000, EIP 004, C 0 ES, P 0 CS, 0 0 SS, 2 0 DS, 3 0 FS, 7 0 GS, D 0, 0 0 La, EFL 000, ST0 emp, ST1 emp, ST2 emp, ST3 emp, ST4 emp, ST5 emp, ST6 emp, ST7 emp, FST 000, FCW 027

Address Hex dump ASCII

0040C000 00 00 00 00 00 00 00 00
 0040C005 00 00 00 00 EF 42 40 00
 0040C010 6C 5A 40 00 00 00 00 00 IZ0....
 0040C015 00 00 00 94 43 40 006C0

0012FF4E 0040209A RETURN
 0012FF50 00000001
 0012FF54 00290A00
 0012FF58 00290B00
 0012FF5C 00000000

- Tiếp tục nhấn F7 21 lần, để gọi một chương trình con ngắn và đến địa chỉ 0x402AFD.

OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]

File View Debug Plugins Options Window Help

File View Debug Plugins Options Window Help

00402B00 8BEC MOV EBP,ESP
 00402B01 8B2C MOV EAX,12C
 00402B02 E8 B3030000 CALL Lab09-01.00402EB0
 00402B03 837D 08 01 CMP DWORD PTR SS:[EBP+8],1
 00402B04 JNZ SHORT Lab09-01.00402B1D
 00402B05 E8 F8E4FFFF CALL Lab09-01.00401800
 00402B06 85C0 TEST EAX,EAX
 00402B07 J74 07 JE SHORT Lab09-01.00402B13
 00402B08 E8 4FF8FFFF CALL Lab09-01.00402360
 00402B09 JEB 05 JMP SHORT Lab09-01.00402B18
 00402B0A E8 F8F8FFFF CALL Lab09-01.00402410
 00402B0B J9 59020000 JMP Lab09-01.00402076
 00402B0C 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
 00402B0D 8B40 0C MOV ECX,DWORD PTR SS:[EBP+C]
 00402B0E 8B54 14 MOV EDX,DWORD PTR DS:[ECX+4]
 00402B0F 8B55 FC MOV DWORD PTR SS:[EBP-4],EDX
 00402B10 8B45 FC MOV EAX,DWORD PTR SS:[EBP-4]
 00402B11 50 PUSH EAX
 00402B12 E8 DD9FFFFF CALL Lab09-01.00402510
 00402B13 83C4 04 ADD ESP,4
 00402B14 85C0 TEST EAX,EAX
 00402B15 J75 05 JNZ SHORT Lab09-01.00402B3F
 00402B16 E8 D1F8FFFF CALL Lab09-01.00402410
 00402B17 8B40 0C MOV ECX,DWORD PTR SS:[EBP+C]
 00402B18 8B51 14 MOV EDX,DWORD PTR DS:[ECX+4]
 00402B19 8B95 E0E7FFFF MOV DWORD PTR SS:[EBP-1820],EDX
 00402B1A 68 70C14000 PUSH Lab09-01.0040C170
 00402B1B 8B95 E0E7FFFF MOV EAX,DWORD PTR SS:[EBP-1820]
 00402B1C 50 PUSH EAX
 00402B1D E8 B30C0000 CALL Lab09-01.0040380F
 00402B1E 83C4 08 ADD ESP,8
 00402B1F 85C0 TEST EAX,EAX
 00402B20 J75 64 JNZ SHORT Lab09-01.00402B27
 00402B21 837D 08 03 CMP DWORD PTR SS:[EBP+8],3
 00402B22 JNZ SHORT Lab09-01.00402B9A
 00402B23 68 00040000 PUSH 400
 00402B24 8B40 0C MOV ECX,DWORD PTR SS:[EBP-404]
 00402B25 51 PUSH ECX
 00402B26 E8 36FAFFFF CALL Lab09-01.004025B0
 00402B27 83C4 08 ADD ESP,8
 00402B28 85C0 TEST EAX,EAX
 00402B29 J74 08 JE SHORT Lab09-01.00402B89
 00402B2A 83C8 FF OR EAX,FFFFFFFF
 00402B2B E8 FF010000 CALL Lab09-01.00402078
 00402B2C E8 FF010000 CALL Lab09-01.00402078
 00402B2D 8B40 0C MOV ECX,DWORD PTR SS:[EBP-404]
 00402B2E 52 PUSH EDI
 00402B2F E8 6FAFFFFF CALL Lab09-01.00402600
 00402B30 83C4 04 ADD ESP,4

Registers: EAX 002, ECX 004, EDI 000, EBP 7FF, ESP 001, ESI 000, EDI 000, EIP 004, C 0 ES, P 0 CS, 0 0 SS, 2 0 DS, 3 0 FS, 7 0 GS, D 0, 0 0 La, EFL 000, ST0 emp, ST1 emp, ST2 emp, ST3 emp, ST4 emp, ST5 emp, ST6 emp, ST7 emp, FST 000, FCW 027

Address Hex dump ASCII

0040C000 00 00 00 00 00 00 00 00
 0040C005 00 00 00 00 EF 42 40 00
 0040C010 6C 5A 40 00 00 00 00 00 IZ0....
 0040C015 00 00 00 94 43 40 006C0

0012E71C 271B356F
 0012E71D 0012E71D 0012E71D

- Nhấn F7 3 lần để vượt qua bài kiểm tra, và nhảy đến địa chỉ 0x401000.
- Bây giờ chúng ta đang ở địa chỉ 0x401000
- Chương trình gọi RegOpenkeyExA tại địa chỉ 0x40101B
- Nhấp chuột trái vào dòng bắt đầu với địa chỉ 0x401021, và nhấn F2 để đặt điểm dừng tại đó. Địa chỉ đó sẽ chuyển sang màu đỏ.
- Nhấn chuột trái vào dòng bắt đầu tại địa chỉ 0x401000. Nhấn F9 để chạy điểm dừng. Kết quả ở hình bên dưới.

OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]

File View Debug Plugins Options Window Help

Address Hex dump ASCII

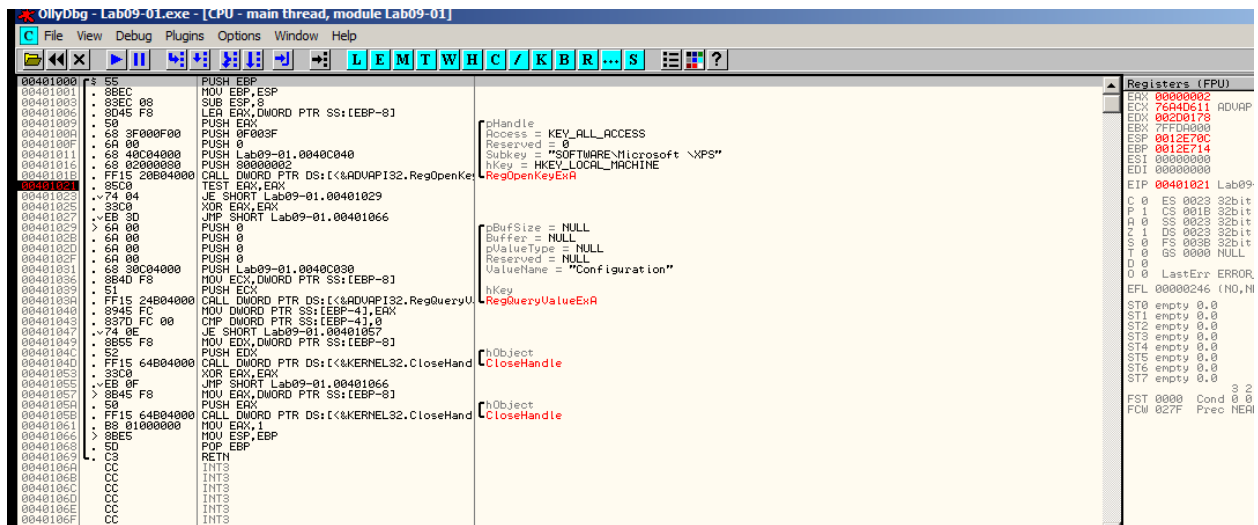
00401000 55 PUSH EBP
 00401001 8BEC MOV EBP,ESP
 00401003 83EC 08 SUB ESP,8
 00401006 8B45 F8 LEA EAX,DWORD PTR SS:[EBP-8]
 00401009 59 PUSH EAX
 0040100A 68 3F00F00 PUSH 0F003F
 0040100F 6A 00 PUSH 0
 00401011 68 40C04000 PUSH Lab09-01.0040C040
 00401016 68 02000000 PUSH 00000002
 0040101B FF15 20B04000 CALL DWORD PTR DS:[<&ADUAPI32.RegOpenKeyExA
 00401021 59 PUSH EAX
 00401022 74 04 JE SHORT Lab09-01.00401029
 00401025 33C0 XOR EAX,EAX
 00401027 EB 30 JMP SHORT Lab09-01.00401066
 00401029 6A 00 PUSH 0
 0040102B 6A 00 PUSH 0
 0040102D 6A 00 PUSH 0
 0040102F 6A 00 PUSH 0
 00401031 68 30C04000 PUSH Lab09-01.0040C030
 00401036 8B4D F8 MOV ECX,DWORD PTR SS:[EBP-8]
 00401039 51 PUSH ECX
 0040103A FF15 24B04000 CALL DWORD PTR DS:[<&ADUAPI32.RegQueryValueExA
 0040103D 9945 FC MOV DWORD PTR SS:[EBP-4],EAX
 00401043 837D FC 00 CMP DWORD PTR SS:[EBP-4],0
 00401047 74 0E JE SHORT Lab09-01.00401057
 00401049 8B55 F8 MOV EDI,DWORD PTR SS:[EBP-8]
 0040104C 52 PUSH EDI
 0040104D FF15 64B04000 CALL DWORD PTR DS:[<&KERNEL32.CloseHandle
 00401053 33C0 XOR EAX,EAX
 00401055 EB 0F JMP SHORT Lab09-01.00401066
 00401057 8B45 F8 MOV EAX,DWORD PTR SS:[EBP-8]
 0040105A 59 PUSH EAX
 0040105B FF15 64B04000 CALL DWORD PTR DS:[<&KERNEL32.CloseHandle
 00401061 8B 01000000 MOV EAX,1
 00401066 8BEC MOV ESP,EBP
 00401068 5D POP EBP
 00401069 C3 RETN
 0040106A CC INT3
 0040106B CC INT3
 0040106C CC INT3
 0040106D CC INT3
 0040106E CC INT3
 0040106F CC INT3
 00401070 55 PUSH EBP
 00401071 8BEC MOV EBP,ESP

hObject
 RegOpenKeyExA
 pBufSize = NULL
 Buffer = NULL
 pValueType = NULL
 Reserved = NULL
 ValueName = "Configuration"

hObject
 CloseHandle
 hObject
 CloseHandle

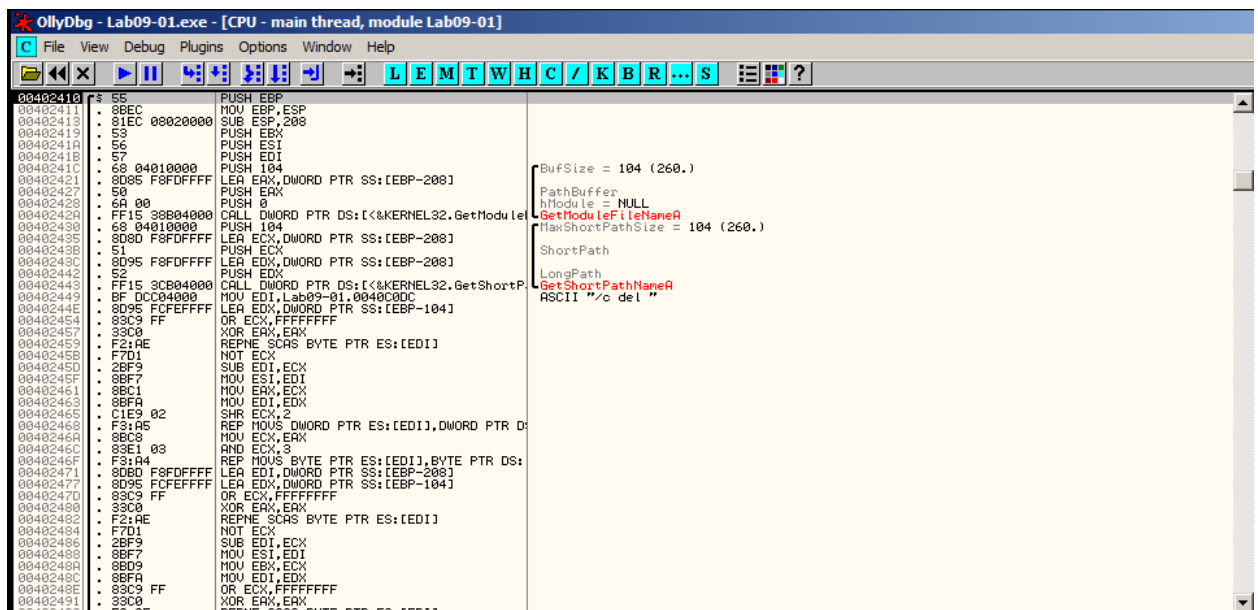
0012E718 00402B08
 0012E71C 771B036A

- Nhìn phía trên bên phải để xem thanh ghi EAX chứa 2.



→ Đây là mã lỗi khác không.

- Điều này có nghĩa là thử nghiệm thất bại, không tìm được khóa đăng ký mà nó đang tìm kiếm.
- Nhấn F7 3 lần để đến địa 0x401027
- Nhấn F7 để thực thi JMP
- Nhấn F7 3 lần để đi qua chương trình con để đến địa chỉ 0x402B08
- Nhấn F7 3 lần để đến địa chỉ 0x402410



- Hàm này sử dụng GetModuleFileName để có được đường dẫn đến tệp thực thi hiện tại và xây dựng chuỗi ASCII
- Để nhìn thấy điều đó, hãy đặt một điểm dừng ngay sau GetShortPathName, để địa chỉ của nó chuyển sang màu đỏ.

The screenshot shows a debugger window with the following assembly code and registers:

```

00402410 55 PUSH EBP
00402411 8BEC MOV EBP,ESP
00402413 81EC 00020000 SUB ESP,200
00402419 53 PUSH EBX
0040241A 56 PUSH ESI
0040241B 57 PUSH EDI
0040241C 68 04010000 PUSH 104
00402421 8D85 F8DFFFFF LEA EAX,DWORD PTR SS:[EBP-208]
00402427 50 PUSH EAX
00402428 6A 00 PUSH 0
0040242A FF15 3B040000 CALL DWORD PTR DS:[<&KERNEL32.GetModule
00402430 68 04010000 PUSH 104
00402435 8D8D F8DFFFFF LEA ECX,DWORD PTR SS:[EBP-208]
0040243B 51 PUSH ECX
0040243C 8D95 F8DFFFFF LEA EDX,DWORD PTR SS:[EBP-208]
00402442 52 PUSH EDX
00402443 FF15 3C040000 CALL DWORD PTR DS:[<&KERNEL32.GetShortP
00402444 BF 0C040000 MOV EDI,Lab09-01.0040C0DC
00402445 8D95 FCFFFFFF LEA EDX,DWORD PTR SS:[EBP-104]
00402446 83C9 FF OR ECX,FFFFFFFF
00402447 33C0 XOR EAX,EAX
00402448 F2:AE REPNE SCAS BYTE PTR ES:[EDI]
00402449 7D01 NOT ECX
0040244A SUB EDI,ECX
0040244B 8BF7 MOV ESI,EDI
0040244C 8BC1 MOV EAX,ECX
0040244D 8BFA MOV EDI,EDX
0040244E C1E9 02 SHR ECX,2
0040244F F3:A5 REP MOVS DWORD PTR ES:[EDI],DWORD PTR D
00402450 8BC8 MOV ECX,EAX
00402451 83E1 03 AND ECX,3
00402452 F3:A4 REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:
00402453 8D8D F8DFFFFF LEA EDI,DWORD PTR SS:[EBP-208]
00402454 8D95 FCFFFFFF LEA EDX,DWORD PTR SS:[EBP-104]
00402455 83C9 FF OR ECX,FFFFFFFF
00402456 33C0 XOR EAX,EAX
00402457 F2:AE REPNE SCAS BYTE PTR ES:[EDI]

```

The registers window on the right shows the following values:

```

Registers (FPU)
EAX 00000000
ECX 760E16D9 kernel32.760E16D9
EDX 00000002
EBX 7FFD4000
ESP 0012E718
EBP 0012FF48
ESI 00000000
EDI 00000000
EIP 00402410 Lab09-01.00402410
C 0 ES 0028 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FST 0000 Cond 0 2 1 0 Err 0 0 0
FCW 027F Prec NEAR,S3 Mask 1

```

- Nhấp vào dòng bắt đầu 0x402410 để tô sáng nó
- Nhấn F9 để chạy điểm dừng.
- Bây giờ bạn sẽ dòng có kết thúc bằng “ASCII “/c del””

The screenshot shows a debugger window with the following assembly code and registers:

```

00402410 55 PUSH EBP
00402411 8BEC MOV EBP,ESP
00402413 81EC 00020000 SUB ESP,200
00402419 53 PUSH EBX
0040241A 56 PUSH ESI
0040241B 57 PUSH EDI
0040241C 68 04010000 PUSH 104
00402421 8D85 F8DFFFFF LEA EAX,DWORD PTR SS:[EBP-208]
00402427 50 PUSH EAX
00402428 6A 00 PUSH 0
0040242A FF15 3B040000 CALL DWORD PTR DS:[<&KERNEL32.GetModule
00402430 68 04010000 PUSH 104
00402435 8D8D F8DFFFFF LEA ECX,DWORD PTR SS:[EBP-208]
0040243B 51 PUSH ECX
0040243C 8D95 F8DFFFFF LEA EDX,DWORD PTR SS:[EBP-208]
00402442 52 PUSH EDX
00402443 FF15 3C040000 CALL DWORD PTR DS:[<&KERNEL32.GetShortP
00402444 BF 0C040000 MOV EDI,Lab09-01.0040C0DC
00402445 8D95 FCFFFFFF LEA EDX,DWORD PTR SS:[EBP-104]
00402446 83C9 FF OR ECX,FFFFFFFF
00402447 33C0 XOR EAX,EAX
00402448 F2:AE REPNE SCAS BYTE PTR ES:[EDI]
00402449 7D01 NOT ECX
0040244A SUB EDI,ECX
0040244B 8BF7 MOV ESI,EDI
0040244C 8BC1 MOV EAX,ECX
0040244D 8BFA MOV EDI,EDX
0040244E C1E9 02 SHR ECX,2
0040244F F3:A5 REP MOVS DWORD PTR ES:[EDI],DWORD PTR D
00402450 8BC8 MOV ECX,EAX
00402451 83E1 03 AND ECX,3
00402452 F3:A4 REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:
00402453 8D8D F8DFFFFF LEA EDI,DWORD PTR SS:[EBP-208]
00402454 8D95 FCFFFFFF LEA EDX,DWORD PTR SS:[EBP-104]
00402455 83C9 FF OR ECX,FFFFFFFF
00402456 33C0 XOR EAX,EAX
00402457 F2:AE REPNE SCAS BYTE PTR ES:[EDI]

```

The registers window on the right shows the following values:

```

Registers (FPU)
EAX 00000000
ECX 760E16D9 kernel32.760E16D9
EDX 00000002
EBX 7FFD4000
ESP 0012E718
EBP 0012FF48
ESI 00000000
EDI 00000000
EIP 00402410 Lab09-01.00402410
C 0 ES 0028 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FST 0000 Cond 0 2 1 0 Err 0 0 0
FCW 027F Prec NEAR,S3 Mask 1

```

- [illegible]

Nếu nhấn F7 quá nhiều lần, thì EDX sẽ trông, để trở về điểm này bạn cần thực hiện các bước sau:

- Trên menu OllyDbg, chọn Debug, Restart
- Chọn Yes
- Nhấn F9 để chạy điểm dừng 0x401021
- Nhấn F9 để chạy điểm dừng 0x402449
- Giữ hoặc nhấn F7 để đến điểm mong muốn.