

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 Lab05-01 | 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

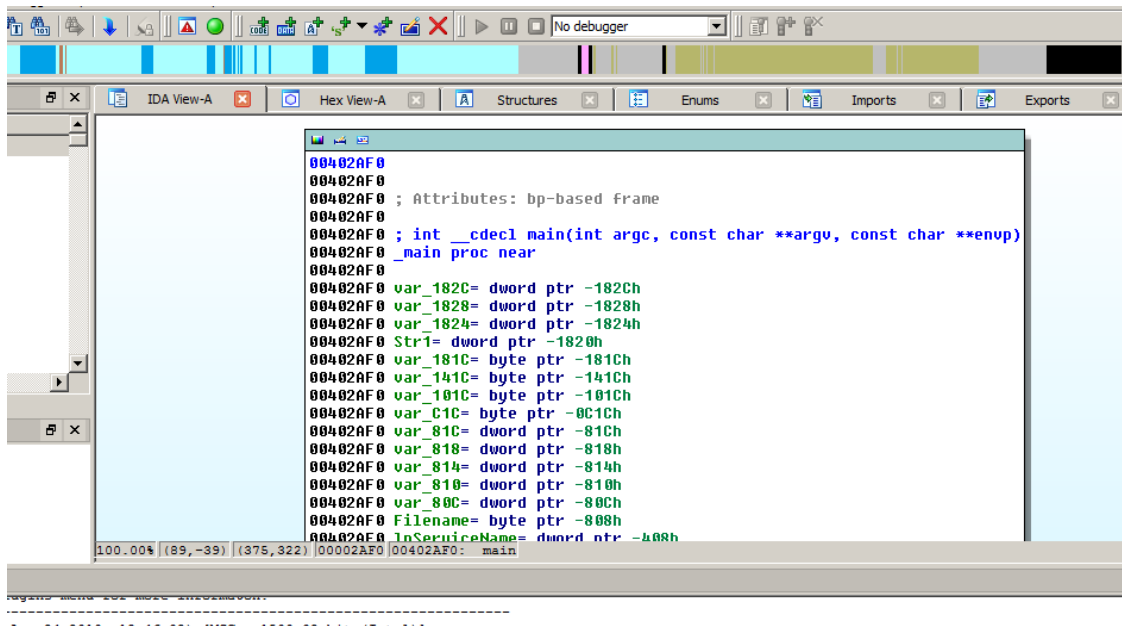
- Môi trường phân tích mã độc đã xây dựng trong Lab 1.

1.3. Phân tích Lab09-01

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

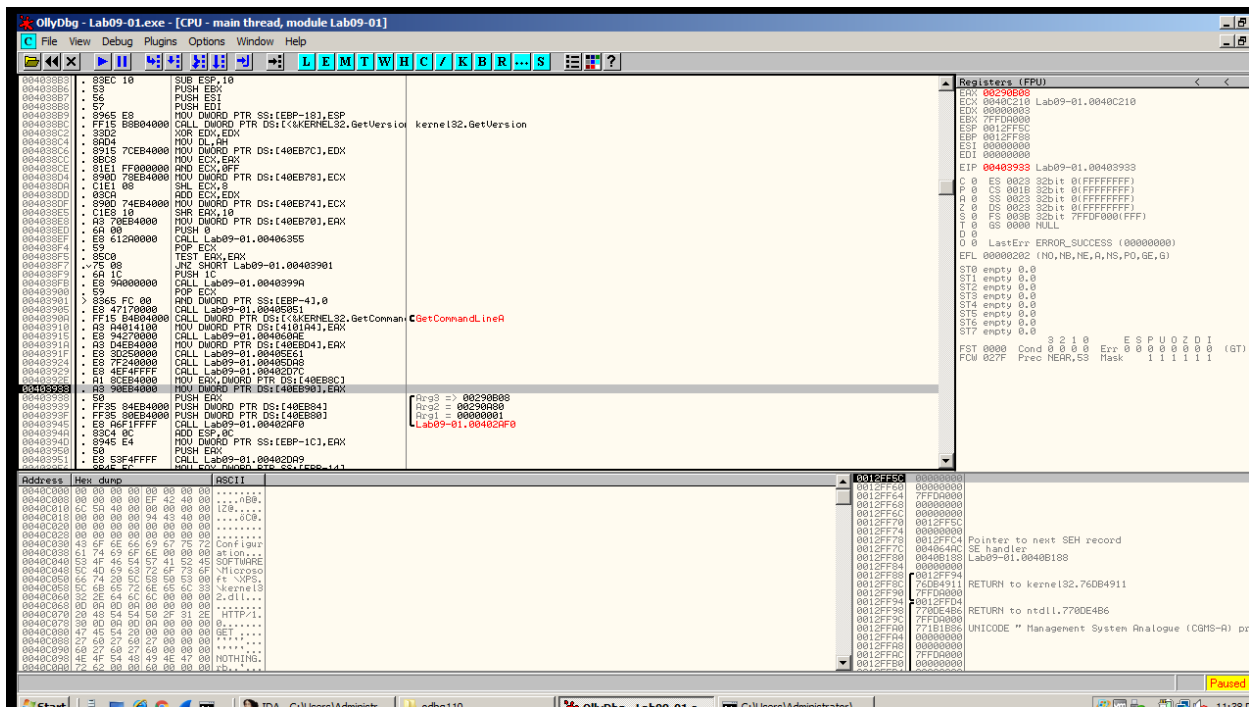
Tìm điểm bắt đầu của hàm main

- 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

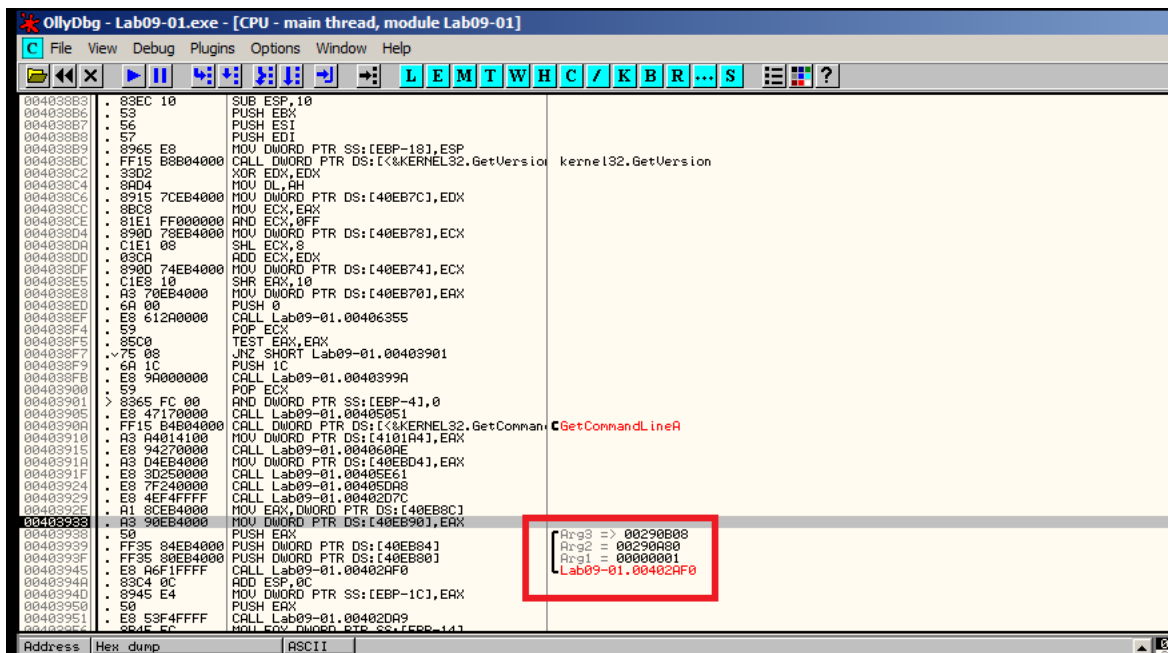


The screenshot shows the IDA Pro interface with the main function at address 00402AF0. The function signature is `int __cdecl main(int argc, const char **argv, const char **envp)`. The function body includes several variable declarations and assignments, such as `var_182C= dword ptr -182Ch`, `var_1828= dword ptr -1828h`, `var_1824= dword ptr -1824h`, `Str1= dword ptr -1820h`, `var_181C= byte ptr -181Ch`, `var_141C= byte ptr -141Ch`, `var_101C= byte ptr -101Ch`, `var_C1C= byte ptr -0C1Ch`, `var_81C= dword ptr -81Ch`, `var_818= dword ptr -818h`, `var_814= dword ptr -814h`, `var_810= dword ptr -810h`, `var_80C= dword ptr -80Ch`, `Filename= byte ptr -808h`, and `InServiceName= dword ptr -408h`. The status bar at the bottom indicates the current address is 00402AF0 and the function is named 'main'.

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]

| Address | Hex | dump | ASCII |
|----------|---------------|---------------------------------|-------|
| 00402BFB | 8BEC | MOV EBP, ESP | |
| 00402BFC | B8 2C100000 | MOV EAX, 152C | |
| 00402BFD | E8 B3030000 | CALL Lab09-01.00402EB0 | |
| 00402BFE | 837D 08 01 | CMF DWORD PTR SS:[EBP+8], 1 | |
| 00402BF0 | 75 10 | JNZ SHORT Lab09-01.00402B1D | |
| 00402BF1 | E8 F8E4FFFF | CALL Lab09-01.00401800 | |
| 00402BF2 | 85C0 | TEST EAX, EAX | |
| 00402BF3 | 74 07 | JE SHORT Lab09-01.00402B13 | |
| 00402BF4 | E8 4FF8FFFF | CALL Lab09-01.00402360 | |
| 00402BF5 | EB 05 | JMP SHORT Lab09-01.00402B18 | |
| 00402BF6 | E8 F8F8FFFF | CALL Lab09-01.00402410 | |
| 00402BF7 | E9 59020000 | JMP Lab09-01.00402076 | |
| 00402BF8 | 8B45 08 | MOV EAX, DWORD PTR SS:[EBP+8] | |
| 00402BF9 | 8B40 0C | MOV ECX, DWORD PTR SS:[EBP+C] | |
| 00402BFA | 8B51 04 | MOV EDX, DWORD PTR DS:[ECX+4] | |
| 00402BFB | 8B55 FC | MOV DWORD PTR SS:[EBP-4], EDX | |
| 00402BFC | 8B45 FC | MOV EAX, DWORD PTR SS:[EBP-4] | |
| 00402BFD | 50 | PUSH EAX | |
| 00402BFE | E8 DD99FFFF | CALL Lab09-01.00402510 | |
| 00402BF0 | 83C4 04 | ADD ESP, 4 | |
| 00402BF1 | 85C0 | TEST EAX, EAX | |
| 00402BF2 | 75 05 | JNZ SHORT Lab09-01.00402B3F | |
| 00402BF3 | E8 D1F8FFFF | CALL Lab09-01.00402410 | |
| 00402BF4 | 8B40 0C | MOV ECX, DWORD PTR SS:[EBP+C] | |
| 00402BF5 | 8B51 04 | MOV EDX, DWORD PTR DS:[ECX+4] | |
| 00402BF6 | 8B55 FC | MOV DWORD PTR SS:[EBP-4], EDX | |
| 00402BF7 | 68 70C14000 | PUSH Lab09-01.0040C170 | |
| 00402BF8 | 8B55 FC | MOV EAX, DWORD PTR SS:[EBP-4] | |
| 00402BF9 | 50 | PUSH EAX | |
| 00402BFA | E8 B30C0000 | CALL Lab09-01.0040380F | |
| 00402BFB | 83C4 08 | ADD ESP, 8 | |
| 00402BFC | 85C0 | TEST EAX, EAX | |
| 00402BFD | 75 64 | JNZ SHORT Lab09-01.00402BC7 | |
| 00402BFE | 837D 08 03 | CMF DWORD PTR SS:[EBP+8], 3 | |
| 00402BF0 | 75 31 | JNZ SHORT Lab09-01.00402B9A | |
| 00402BF1 | 68 00040000 | PUSH 400 | |
| 00402BF2 | 808D FCBFFFFF | LEA ECX, DWORD PTR SS:[EBP-404] | |
| 00402BF3 | 51 | PUSH ECX | |
| 00402BF4 | E8 36FAFFFF | CALL Lab09-01.004025B0 | |
| 00402BF5 | 83C4 08 | ADD ESP, 8 | |
| 00402BF6 | 85C0 | TEST EAX, EAX | |
| 00402BF7 | 74 08 | JE SHORT Lab09-01.00402B89 | |
| 00402BF8 | 83C8 FF | OR EAX, FFFFFFFF | |
| 00402BF9 | E9 FF010000 | JMP Lab09-01.00402078 | |

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

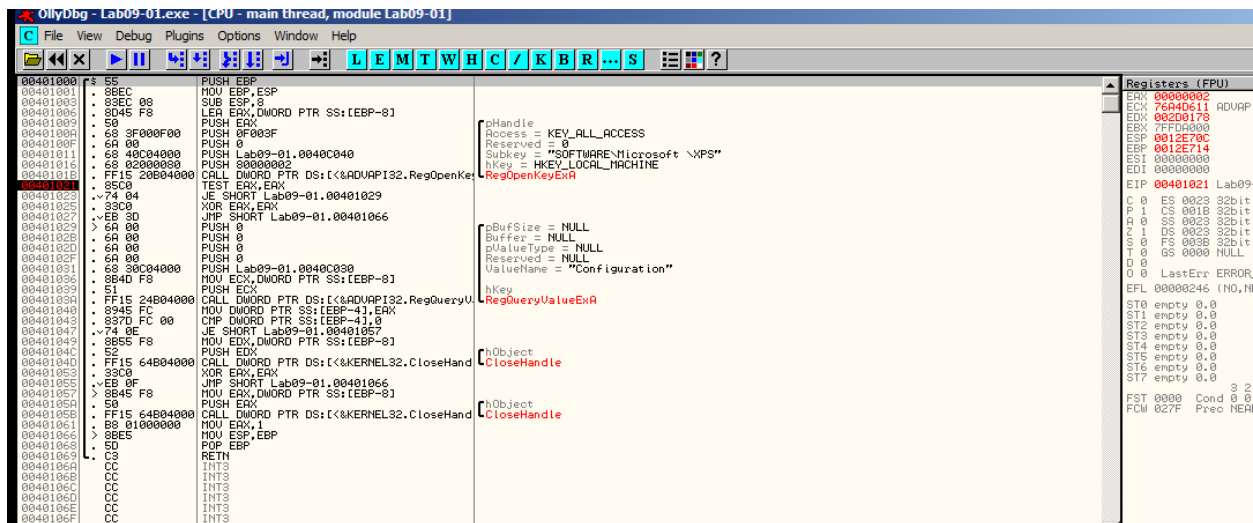
OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]

| Address | Hex | dump | ASCII |
|----------|---------------|---------------------------------|-------|
| 00402BFB | 8BEC | MOV EBP, ESP | |
| 00402BFC | B8 2C100000 | MOV EAX, 152C | |
| 00402BFD | E8 B3030000 | CALL Lab09-01.00402EB0 | |
| 00402BFE | 837D 08 01 | CMF DWORD PTR SS:[EBP+8], 1 | |
| 00402BF0 | 75 10 | JNZ SHORT Lab09-01.00402B1D | |
| 00402BF1 | E8 F8E4FFFF | CALL Lab09-01.00401800 | |
| 00402BF2 | 85C0 | TEST EAX, EAX | |
| 00402BF3 | 74 07 | JE SHORT Lab09-01.00402B13 | |
| 00402BF4 | E8 4FF8FFFF | CALL Lab09-01.00402360 | |
| 00402BF5 | EB 05 | JMP SHORT Lab09-01.00402B18 | |
| 00402BF6 | E8 F8F8FFFF | CALL Lab09-01.00402410 | |
| 00402BF7 | E9 59020000 | JMP Lab09-01.00402076 | |
| 00402BF8 | 8B45 08 | MOV EAX, DWORD PTR SS:[EBP+8] | |
| 00402BF9 | 8B40 0C | MOV ECX, DWORD PTR SS:[EBP+C] | |
| 00402BFA | 8B51 04 | MOV EDX, DWORD PTR DS:[ECX+4] | |
| 00402BFB | 8B55 FC | MOV DWORD PTR SS:[EBP-4], EDX | |
| 00402BFC | 8B45 FC | MOV EAX, DWORD PTR SS:[EBP-4] | |
| 00402BFD | 50 | PUSH EAX | |
| 00402BFE | E8 DD99FFFF | CALL Lab09-01.00402510 | |
| 00402BF0 | 83C4 04 | ADD ESP, 4 | |
| 00402BF1 | 85C0 | TEST EAX, EAX | |
| 00402BF2 | 75 05 | JNZ SHORT Lab09-01.00402B3F | |
| 00402BF3 | E8 D1F8FFFF | CALL Lab09-01.00402410 | |
| 00402BF4 | 8B40 0C | MOV ECX, DWORD PTR SS:[EBP+C] | |
| 00402BF5 | 8B51 04 | MOV EDX, DWORD PTR DS:[ECX+4] | |
| 00402BF6 | 8B55 FC | MOV DWORD PTR SS:[EBP-4], EDX | |
| 00402BF7 | 68 70C14000 | PUSH Lab09-01.0040C170 | |
| 00402BF8 | 8B55 FC | MOV EAX, DWORD PTR SS:[EBP-4] | |
| 00402BF9 | 50 | PUSH EAX | |
| 00402BFA | E8 B30C0000 | CALL Lab09-01.0040380F | |
| 00402BFB | 83C4 08 | ADD ESP, 8 | |
| 00402BFC | 85C0 | TEST EAX, EAX | |
| 00402BFD | 75 64 | JNZ SHORT Lab09-01.00402BC7 | |
| 00402BFE | 837D 08 03 | CMF DWORD PTR SS:[EBP+8], 3 | |
| 00402BF0 | 75 31 | JNZ SHORT Lab09-01.00402B9A | |
| 00402BF1 | 68 00040000 | PUSH 400 | |
| 00402BF2 | 808D FCBFFFFF | LEA ECX, DWORD PTR SS:[EBP-404] | |
| 00402BF3 | 51 | PUSH ECX | |
| 00402BF4 | E8 36FAFFFF | CALL Lab09-01.004025B0 | |
| 00402BF5 | 83C4 08 | ADD ESP, 8 | |
| 00402BF6 | 85C0 | TEST EAX, EAX | |
| 00402BF7 | 74 08 | JE SHORT Lab09-01.00402B89 | |
| 00402BF8 | 83C8 FF | OR EAX, FFFFFFFF | |
| 00402BF9 | E9 FF010000 | JMP Lab09-01.00402078 | |
| 00402BFA | 8085 FCBFFFFF | LEA EDI, DWORD PTR SS:[EBP-404] | |
| 00402BFB | 52 | PUSH EDI | |
| 00402BFC | E8 6BFAFFFF | CALL Lab09-01.00402600 | |
| 00402BFD | 83C4 04 | ADD ESP, 4 | |

- 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.

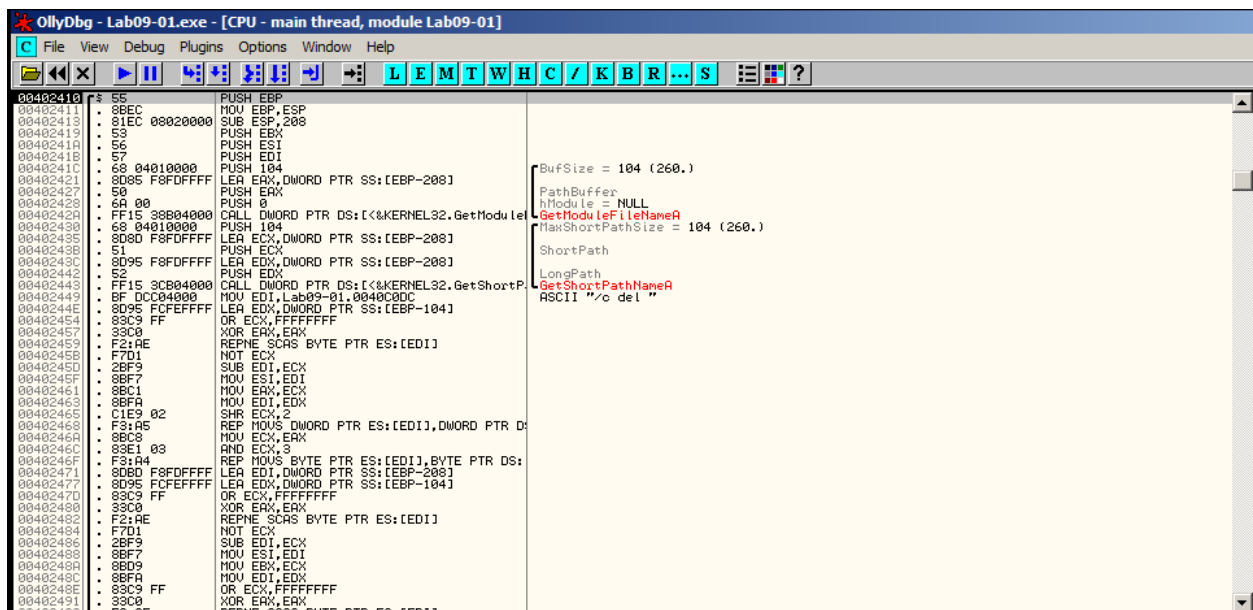
The screenshot shows the OllyDbg interface with the assembly window displaying code from 00401000 to 00401070. The instruction at 00401021 is highlighted in red, indicating a breakpoint. The instruction is `CALL DWORD PTR DS:[<&ADUAPI32.RegOpenKeyExA]`. The right pane shows the function signature for `RegOpenKeyExA` with parameters: `hHandle`, `Access = KEY_ALL_ACCESS`, `Reserved = 0`, `Subkey = "SOFTWARE\Microsoft\XPS"`, and `hKey = HKEY_LOCAL_MACHINE`. The bottom status bar shows the current address as 0012E718 and the CPU registers as 00402B08 and 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-200]
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-200]
0040243B 51 PUSH ECX
0040243C 8D95 F8DFFFFF LEA EDX,DWORD PTR SS:[EBP-200]
00402442 52 PUSH EDX
00402443 FF15 3C040000 CALL DWORD PTR DS:[<&KERNEL32.GetShortP
00402444 BF DCC04000 MOV EDI,Lab09-01.0040C00C
00402445 8D95 FCFFFFFF LEA EDI,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 8BF9 MOV ESI,EDI
0040244C 8BF7 MOV EAX,ECX
0040244D 8BC1 MOV EAX,ECX
0040244E 8BFA MOV EDI,EDX
0040244F C1E9 02 SHR ECX,2
00402450 REP MOVSD DWORD PTR ES:[EDI],DWORD PTR D
00402451 MOV ECX,EAX
00402452 AND ECX,3
00402453 REP MOVSB BYTE PTR ES:[EDI],BYTE PTR DS:
00402454 LEA EDI,DWORD PTR SS:[EBP-200]
00402455 8D95 FCFFFFFF LEA EDX,DWORD PTR SS:[EBP-104]
00402456 83C9 FF OR ECX,FFFFFFFF
00402457 33C0 XOR EAX,EAX
00402458 F2:AE REPNE SCAS BYTE PTR ES:[EDI]

```

The registers window on the right shows the following values:

| Register | Value |
|----------|--------------------------------|
| EAX | 00000000 |
| ECX | 760E16D9 kernel32.760E16D9 |
| EDX | 00000002 |
| EBX | 7FFD4000 |
| ESP | 0012E718 |
| EBP | 0012FF48 |
| ESI | 00000000 |
| EDI | 00000000 |
| EIP | 00402410 Lab09-01.00402410 |
| 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 0 0 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:

```

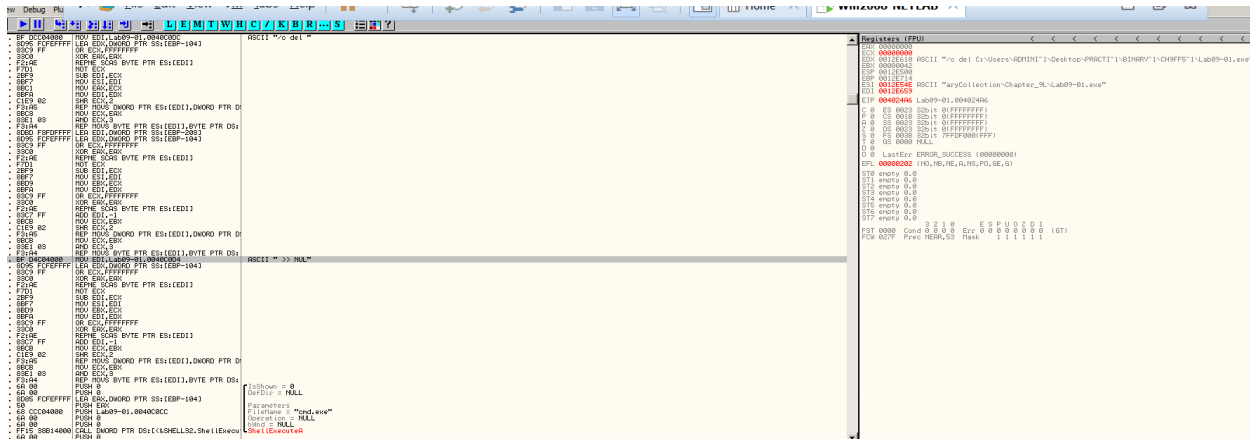
00402410 55 PUSH EBP
00402411 8BEC MOV EBP,ESP
00402413 81EC 00020000 SUB ESP,200
00402419 53 PUSH EBX
0040241A 56 PUSH ESI
0040241B 57 PUSH EDI
0040241C 68 04010000 PUSH 104
00402421 8D85 F8DFFFFF LEA EAX,DWORD PTR SS:[EBP-200]
00402427 50 PUSH EAX
00402428 6A 00 PUSH 0
0040242A FF15 3B040000 CALL DWORD PTR DS:[<&KERNEL32.GetModule
00402430 68 04010000 PUSH 104
00402435 8D8D F8DFFFFF LEA ECX,DWORD PTR SS:[EBP-200]
0040243B 51 PUSH ECX
0040243C 8D95 F8DFFFFF LEA EDX,DWORD PTR SS:[EBP-200]
00402442 52 PUSH EDX
00402443 FF15 3C040000 CALL DWORD PTR DS:[<&KERNEL32.GetShortP
00402444 BF DCC04000 MOV EDI,Lab09-01.0040C00C
00402445 8D95 FCFFFFFF LEA EDI,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 8BF9 MOV ESI,EDI
0040244C 8BF7 MOV EAX,ECX
0040244D 8BC1 MOV EAX,ECX
0040244E 8BFA MOV EDI,EDX
0040244F C1E9 02 SHR ECX,2
00402450 REP MOVSD DWORD PTR ES:[EDI],DWORD PTR D
00402451 MOV ECX,EAX
00402452 AND ECX,3
00402453 REP MOVSB BYTE PTR ES:[EDI],BYTE PTR DS:
00402454 LEA EDI,DWORD PTR SS:[EBP-200]
00402455 8D95 FCFFFFFF LEA EDX,DWORD PTR SS:[EBP-104]
00402456 83C9 FF OR ECX,FFFFFFFF
00402457 33C0 XOR EAX,EAX
00402458 F2:AE REPNE SCAS BYTE PTR ES:[EDI]

```

The registers window on the right shows the following values:

| Register | Value |
|----------|--------------------------------|
| EAX | 00000000 |
| ECX | 760E16D9 kernel32.760E16D9 |
| EDX | 00000002 |
| EBX | 7FFD4000 |
| ESP | 0012E718 |
| EBP | 0012FF48 |
| ESI | 00000000 |
| EDI | 00000000 |
| EIP | 00402410 Lab09-01.00402410 |
| 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 0 0 0 Err 0 0 0 |
| FCW | 027F Prec NEAR,S3 Mask 1 |

- Bằng cách giữ F7 hoặc nhấn vào nó nhiều lần.
- Xem mã từ từ đi qua như một đường dẫn dài trong EDI. Sau đó tên đường dẫn lật nhanh qua một số thanh ghi, kết thúc bằng EDX.
- Dừng lại khi bạn nhìn thấy một chuỗi tron EDX, bắt đầu với ASCII “/c del C:\
C:\”



Chú yí:

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.