Flag: “vcstraining{Running_in_VM_is_ridiculous}”

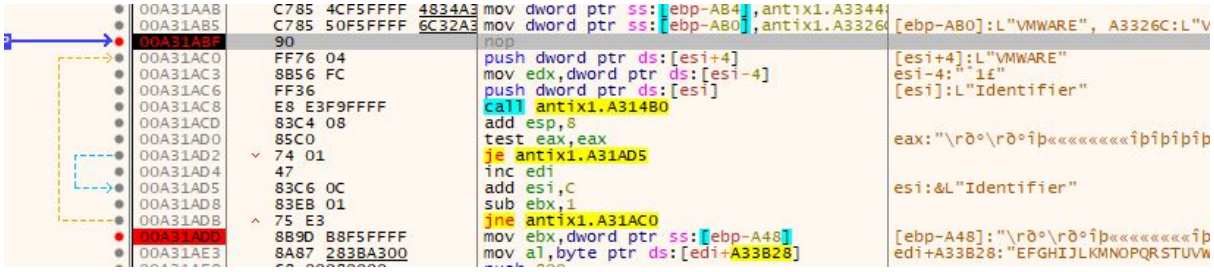
Mô tả:

- Input được truyền khi gọi chương trình
- Với mỗi chuỗi đầu vào, xâu đầu ra khác nhau
- Khi chạy tại máy thật, ta nhận được gợi ý: “Congratulation! Use this password to unlock the flag: BROKENVM (Pass it as argument)” (str0)
- Khi chạy tại máy ảo, chương trình kiểm tra và làm đầu vào mặc định để tạo ra chuỗi đầu ra thay đổi, không nhận được str0

=> Vô hiệu hóa / làm chương trình không kiểm tra được việc chương trình đang chạy trên máy ảo

Debug - Danh sách lỗi và sửa lỗi

1. Compare “VMWARE”

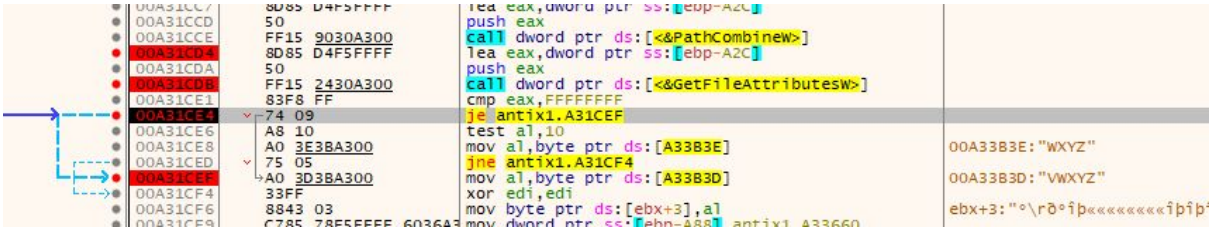


=> bỏ qua đoạn check, jmp từ 0xA31ABF đến 0xA31ADD

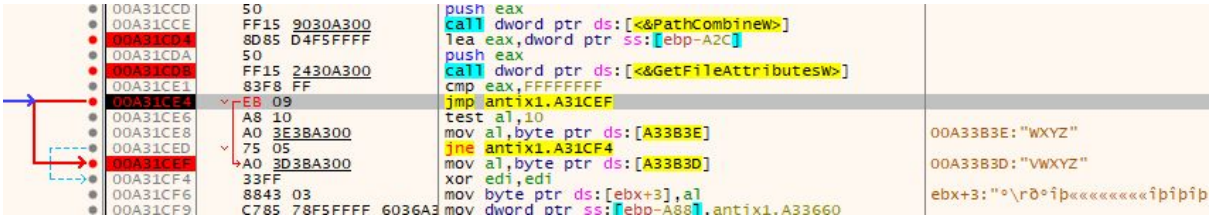
2. GetFileAttribytesW

Hàm trả về thuộc tính của 1 file hay 1 đường dẫn file
=> return thuộc tính nếu thành công
=> return FFFFFFFF nếu thất bại

[ebp-A2C] : C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.V. M.W.a.r.e.\
=> đây là đường dẫn đến file sẽ đọc

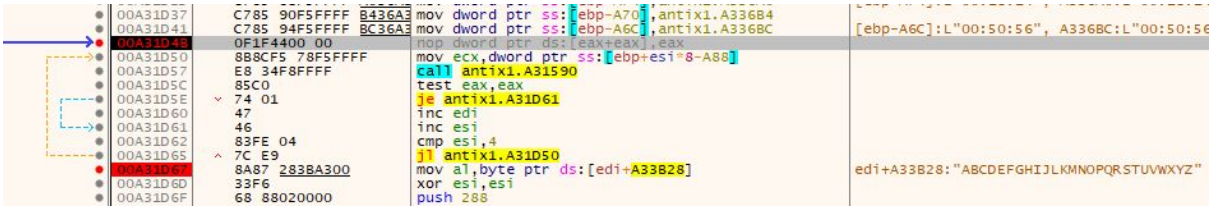


Chạy trong máy ảo => hàm trả về thành công (khác FFFFFFFF)
=> Mặc định jmp (je => jmp) từ 0xA31CE4 đến 0xA31CEF

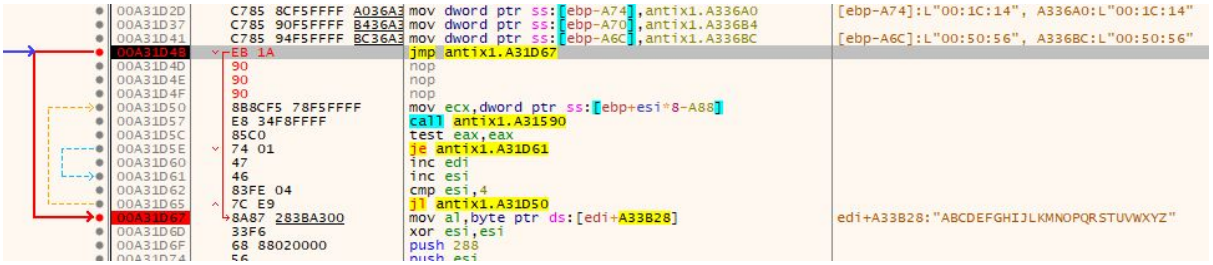


3. Compare “VMWARE”

Tương tự 1

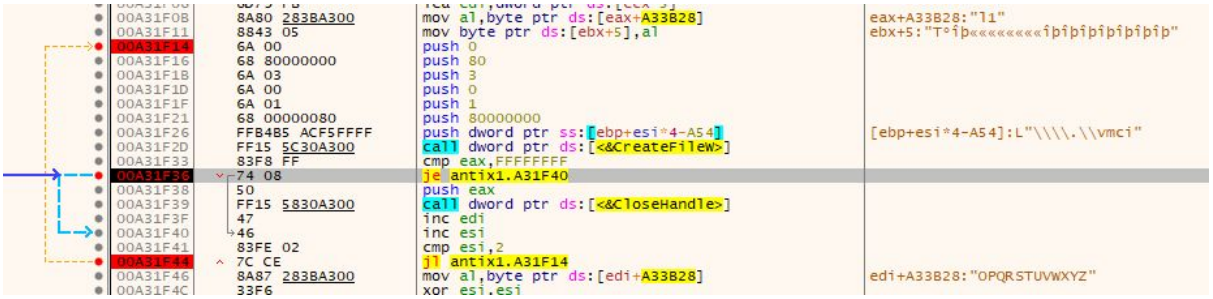


=> Bỏ qua loop (phần check)
=> jmp qua từ 0xA3D48 đến 0xA3D67



4. CreateFileW - vmci

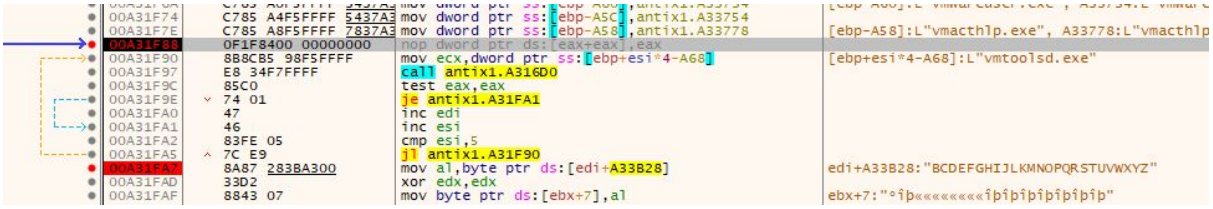
Tạo hoặc mở 1 file hoặc thiết bị I/O
=> return handle nếu thành công
=> return FFFFFFFF nếu thất bại



vmci là virtual device
=> Khi chạy trong VM, có virtual device
=> CreateFileW thành công (khác FFFFFFFF)
=> Mặc định jmp (je => jmp)

5. Compare “vmtoolsd.exe”

Tương tự 1, 3



=> bỏ qua check
=> jmp từ 0xA31F88 đến 0xA31FA7