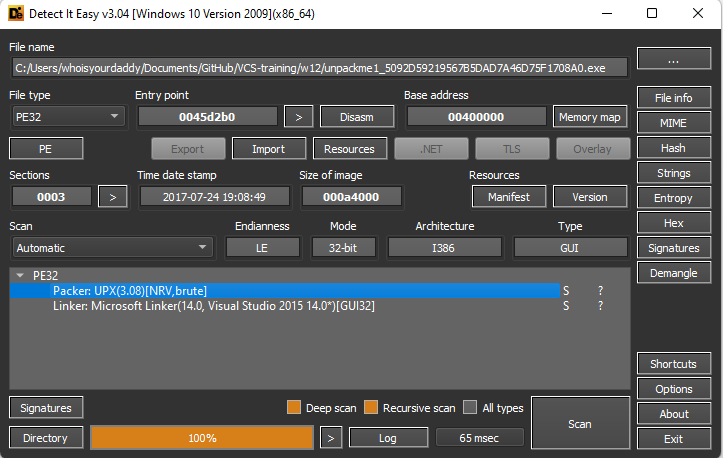
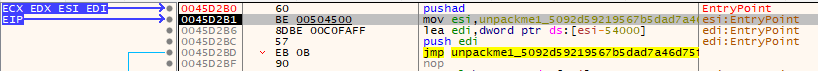
Bài 1 sử dụng packer UPX



Tắt ASLR bằng CFF explorer

Load vào x64dbg. F9 1 lần để nhảy tới entry point. Nhìn thấy lệnh đầu tiên là pushad.



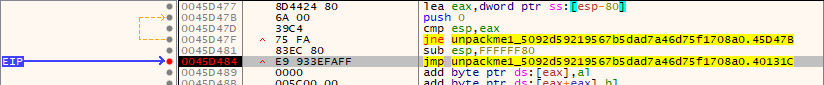
Step into 1 instruction, check ESP, sau đó follow in dump và đặt breakpoint tại đó. Bản chất của việc breakpoint là đợi cho packer dump hết code, trả lại các giá trị của các thanh ghi (popad) thì ta breakpoint.

F9 tiếp thì, breakpoint hit:

Text

Description automatically generated with medium confidence

F8 tiếp tới lệnh jump



F7 step into lệnh này.



Vậy OEP là 0x40131C.

Scylla để dump, tìm IAT, sau đó dump ra và fix dump là xong

Graphical user interface, application

Description automatically generated

Xóa entry không hợp lệ đi.

A screenshot of a computer

Description automatically generated with medium confidence

File dump chạy thành công

Graphical user interface, text, application

Description automatically generated