CrackMe 6

Tìm đến thông báo đầu tiên để tìm cách loại bỏ nó

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Có 1 lệnh jump nhảy đến do chưa registered và hiện các thông báo register như trên. Do đó ta fill with nop từ dòng 004010A7 đến 004010BA (để không hiển thị dialog nữa):

A screenshot of a computer

Description automatically generated

Để thay đổi trạng thái khi ấn re-check, ta cần tìm đoạn not registered và breakpoint nó lại.

A screenshot of a computer

Description automatically generated

Khi chạy đến breakpoint 1, ấn re-check sẽ nhảy sang breakpoint 2:

A screenshot of a computer

Description automatically generated

Ta đặt breakpoint ở lệnh je. Nhận thấy là nó sẽ nhảy vào thông báo Nag not removed, và ZF cần được đổi sang 0:

A screenshot of a computer

Description automatically generated

Nhưng đến đây nó lại đi vào 1 lệnh jump khác, và “jump is not taken” cho thấy nó sẽ không nhảy đến đó, vì thế cần phải cho phép jumpo bằng cách đổi ZF thành 1

A screenshot of a computer

Description automatically generated

Patchfile và chạy lại thì khi đó đã thay đổi được thông báo

A screenshot of a computer

Description automatically generated