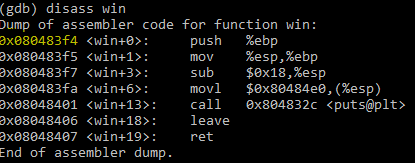
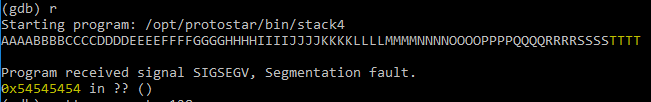
המטרה שלנו: לשנות את הכתובת כתובת החזרה של הפונקציה על מנת שתחזור לwin.  
  
נשים לב שמשתמשים בפונקציה gets, כלומר אין בדיקה על כמה תווים קולטים למשתנה buffer לכן נוכל לכתוב כמה תווים שנרצה ולדרוס משתנים אחרים ואפילו את כתובת החזרה!

נשתמש בgdb:

* נמצא את כתובת החזרה של win:  
  

הinstruction הראשון של הפונקציה הוא גם הכתובת של הפונקציה.

* לאחר מכן נריץ את התוכנית ובקלט נכניס pattern מסוים שאיתו נבין היכן התוכנית מנסה לקפוץ:

  
נשים לב כי התוכנית קרסה כיוון שהיא לא הבינה לאן היא צריכה לקפוץ ולא מכירה בכתובת 0x54545454, 0x54 הוא ערך האסקי של האות T ולכן נצטרך פשוט להחליף אותה בכתובת של הפונקציה שמצאנו קודם.

* נעזר בפייתון.

EXPLOIT:

python -c "print 'a'\*4\*19 + '\xf4\x83\x04\x08'" | ./stack4