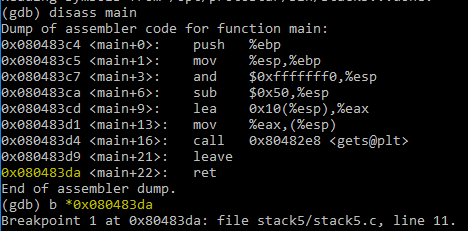
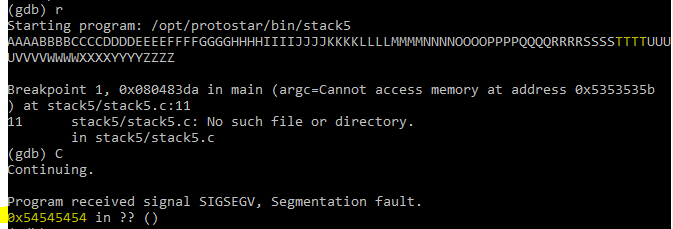
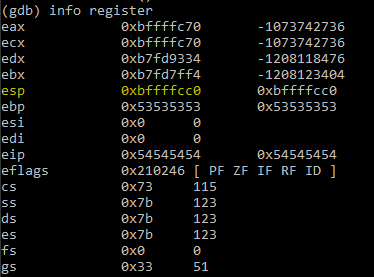
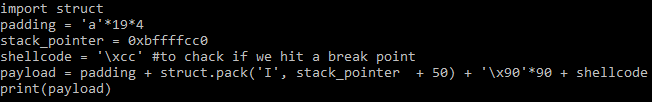
המטרה שלנו: להריץ shellcode.  
  
נשים לב שמשתמשים בפונקציה gets, כלומר אין בדיקה על כמה תווים קולטים למשתנה buffer לכן נוכל לכתוב כמה תווים שנרצה ולכתוב למחסנית את הקוד שלנו ולאחר מכן לדרוס את eip לכתובת של הshellcode שלנו.

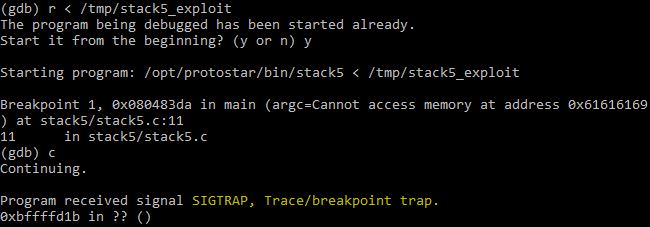
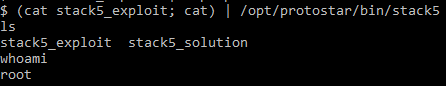
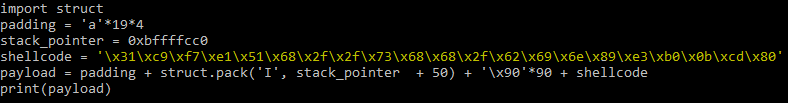
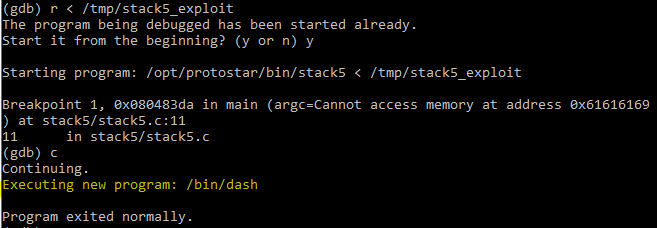
נשתמש בgdb:

* נשים break point בret :  
  
* לאחר מכן נריץ את התוכנית ובקלט נכניס pattern על מנת לראות מתי אנחנו דורסים את ret 

נשים לב כי אנו מנסים לחזור ל0x54545454 (אות T).

* לאחר מכן נחליף את הreturn address לכתובת ששם תמצא הshellcode שלנו. הכתובת של הshellcode שלנו לא חייבת להיות כתובת מדויקת של הבית הראשון שלה כיוון שאנו נשתמש בnop slide.  
  נמלא את המחסנית שלנו בnop כך שכאשר נקפוץ לnop כלשהו התוכנית תמשיך לnop הבא עד שתגיע לinstruction הראשון של הshellcode.  
  נקח את הstack pointer שלנו ונוסיף לה כמה בתים כך שלדעתי נגיע לnop כלשהו.  
  על מנת למצוא את הstack pointer:

נתחיל לכתוב קוד בפייתון:  
  
נכתוב את התוצאה לקובץ **python stack5\_solution > stack5\_exploit**

* נחזור לgdb:  
    
  הגענו ל**\xcc** כלומר לbreak point של הshellcode שלנו! מה שנשאר זה רק להחליף אותו בshellcode שבאמת עובד.
* נשתמש בShellcode הזה - <http://shell-storm.org/shellcode/files/shellcode-517.php>  
  שמטרתו להריץ את /bin/bash .  
  נשנה את הshellcode בקוד שלנו ונכניס מחדש לקובץ  
    
    
    
  הצלחנו! הרצנו את bin/dash.  
    
  נבדוק זאת בלי gdb: