תרגיל בית 3 – חלק ב'

1. הבעיה בקריאה לפונקציה scanf היא שהקלט אותו מכניס המשתמש יכול להיות גדול מגדול ה-buffer ובכך לדרוס ערכים קודמים במחסנית בעת כתיבתו אליה (שכן קריאה מתבצעת לכתובת זיכרון והשימוש הסטנדרטי הוא במחסנית), דבר שעלול להוביל להתנהגות בלתי מוגדרת.
2. הכתובת תהיה ערך ה-ascii של התווים "mMnNoOpP", כלומר, **0x6d4d6e4e6f4f7050 (**או ב-little endian**: 0x50704f6f4e6e4d6d**) וזה מפני שמכיוון שגודל ה-buffer המוקצה על המחסנית יהיה 16 תווים – 16 בייטים, ועוד 8 בייטים שישמרו עבור old\_rbp, ערך ההחזרה של המחסנית ישמר 24 בייטים לפני הכתובת במחסנית עליה יכנס הקלט. לכן 24 הבייטים הראשונים ישמרו על מקומות אלה והשמונה שיבואו אחרים ידרסו את הערך אליו אמורה התוכנית לחזור.

|  |  |  |
| --- | --- | --- |
| **כתובת** | **קידוד** | **פקודות** |
| 0x401d13 | 5f  c3 | pop %rdi  ret |
| 0x400e2c | 58  c3 | Pop %rax  ret |
| 0x40114f | 0f 05 | syscall |
| 0x401d11 | 5e  41 5f  c3 | pop %rsi  pop %r15  ret |
| 0x400624 | 55  bf 20 2e 60 00  48 89 e5  ff d0 | push %rbp  mov $0x602e20, %edi  mov %rsp, %rbp  call \*%rax |
| 0x4008bc | 4c 01 ff  c3 | add %r15, %rdi  ret |

1. הטבלה:
2. הפקודה תהיה: