Mark Seliternikov
picoCTF - strings it [100 points]

באתגר זה מקבלים קובץ עם הרבה מידע שנראה רנדומלי.
האתגר מרמז להשתמש בפקודה של strings בלינוקס.
לפני שניסיתי את זה פתחתי את הקובץ ב-Notepad++ וחיפשתי picoCTF.

```
picoCTF{5tRIng5_1T_827aee91}
```

כך פתרתי את האתגר בלי להשתמש בלינוקס.
רציתי לתרגל פתרון גם עם לינוקס כי אני מתכנן להתחיל ללמוד את זה בקרוב.
כמו שציינתי קודם האתגר מרמז להשתמש בפקודה strings. כאשר עושים זאת זה הפלט:

```
s8744
s8374
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.data
.bss
.comment
mark@DESKTOP-19NBBKR:/mnt/c/Users/markm/desktop/projects/strings$
```

מכיוון שכבר פתרתי ב-Notepad++ ידעתי שתהיה רשימה ארוכה של strings כבר מראש.
לא הכרתי בשלב זה דרך לסנן את הפלט לפי דפוס מסוים.
לאחר חיפוש מצאתי את הפקודה grep שאמורה לעזור לי עם ה-CTF.
הכנסתי את הפקודה הבאה:

```
mark@DESKTOP-19NBBKR:/mnt/c/Users/markm/desktop/projects/strings$ strings strings | grep picoCTF
picoCTF{5tRIng5_1T_827aee91}
mark@DESKTOP-19NBBKR:/mnt/c/Users/markm/desktop/projects/strings$
```

ניתן לראות שזה אכן הדגל שמצאתי גם בשיטה הראשונה. לדעתי הפתרון דרך לינוקס הרבה יותר קצרה והרבה יותר יפה.

<u>מה למדתי</u>

למדתי קצת על פקודות לינוקס, אין לי ספק שזה ישרת אותי בהמשך הדרך.