המדריך למתחיל למציאת דברים בקובץ ELF

אם נתונה לנו שאלה כגון: "מה נמצא מיד בתחילת .rodata?"

1. מוצאים את ה OFFSET של ה SECTIONS.
2. מוצאים גודל של כל אחד מה SECTIONS. לא לשכוח שזה ב HEXA!
   - שני אלה קלים כי זה אפשר למצוא ישירות מהמבנה של Header Table
3. מסמנים את כל ה SECTIONS, מהתחלה ועד הסוף
4. מוצאים את ה SECTION שהוא RODATA. כלומר: type = 1 & flags = 2
5. מוצאים את ה offset שממנו הוא מתחיל. (offset 10H)
6. הולכים למקום הזה בקובץ ובודקים: אם יש שם טקסט, אז ב RODATA מוגדר הטקסט הזה וסיימנו. אם יש שם משהו אחר (כגון כתובת או משהו אחר) אז זה מסתבך :D
7. אם מצאנו כתובת, זה אומר שה SYMBOL שאנחנו מחפשים, מוגדר הערך שלו שם. אז אנחנו צריכים למצוא את טבלת הסימבולים. לרוב הם נותנים לנו אותה, אבל אם אין אז אנחנו צריכים למצוא SECTION שה type שלו הוא 2.
8. מוצאים את ה OFFSET שלו והולכים לשם.
9. כל 4 רביעיות הם SYMBOL אחד. ממליץ לסמן אותם..
10. עוברים אחד אחד עד שמוצאים אחד שהשם שלו (הרביעייה הראשונה) שונה מ 0.
11. בודקים את ה address שלו, זה הרבייעיה השניה שלו, אם אני רואים שהוא מתחיל באותה כתובת כמו שמצאנו בסעיף 5, מצאנו את שלנו! (אם לא, ממשיכים לחפש)
12. מוצאים איפה מתחיל ה strtab (לרוב נתון, אם לא אז ניתן למצוא אותו כמו שמצאנו את ה symtab אבל עם type = 3, שימו לב שיש כמה..)
13. הולכים לשם וסופרים את המספר שמצאנו בשלב 10-11. (השם, לא הכתובת)
14. וזהו, מצאנו בטקסט את השם של הקבוע שאת הערך שלו מוגדר ב rodata)

למצוא ערך של משתנה:

1. חוזרים על התהליך שעשינו קודם ומוצאים בסעיף 6 מספר כלשהו בעל 4 בייטים. זה הערך (לא לשכוח שזה ב little endian!)

למצוא באיזה SECTION מופיעה מחרוזת כלשהי

1. עוברים על ה SECTIONS (כן, כולם) ובודקים באיזה OFFSET הם מתחילים ומה הגודל שלהם. (OFFSET of the OFFSET: 10H, OFFSET of the SIZE: 14H) ובודקים באיזה SECTION הסימבול שאנו מחפשים מוכל.

Section name	Type	Flags
.bss	8	3H
.comment	1	0H
.data	1	3H
.debug	1	0H
.dynamic	6	2H + processor specific
.dynstr	3	2H
.dynsym	11	2H
.rodata	1	2H
.shstrtab	3	0H
.strtab	3	2H / 0 (symbol string table/NO)
.symtab	2	2H / 0 (symbol string table/NO)
.text	1	6H