סדנת מבוא ל REVERSING

©אלי ביהם, אביעד כרמל, נערך ע"י טל שנקר

היכרות ראשונית

- הורידו מאתר הקורס את הקובץ sampleNI.exe.
  - Crackme פשוט שמדפיס OK עבור סיסמה נכונה או Wrong אחרת.
  - מצאו את הסיסמה הנכונה.

- שנו את הקוד כך שידפיס OK עבור כל קלט.
  - בהתחלה יש לשנות את הקוד כפי שהוסבר בכיתה.
  - לאחר מכן חפשו מקום נוסף שניתן לשנות על מנת להשיג תוצאה דומה.

מציאת קטע קוד רלוונטי

- נתון הקוד (הפשוט הבא) :

```
int main() {
        printf("Hello World\n");
}
```

- מצאו לפחות 3 דרכים שונות למצוא את קטע הקוד ב-EXE.
  - חשבו אם הדרכים שלכם היו עובדות גם עבור תוכניות גדולות עם הרבה קוד.
- הורידו מאתר הקורס את הקובץ printf.exe.

מציאת קטע קוד רלוונטי
חלק 2

- נתונה תוכנית שמדפיסה את הפלט הבא:

```
Hello World
```

- המתכנת מצא דרך להדפיס מבלי להשתמש ב-printf.
  - ידוע שהוא השתמש בפונקציה שתומכת ב-format string כמו printf.
- כיצד ניתן למצוא את קטע הקוד הרלוונטי?
  - לבדוק את ה-import table על מנת לגלות דרך איזו פונקציה הדפיס.
  - מצאו דרך נוספת - יישמו את הפתרון שלכם על הקובץ printf.exe.

- רמז: איפה printf ממומש? מצאו מכנה משותף לסוג הפונקציות האלו.

תרגיל

- נתון קובץ struct.exe.
  - הבינו את האסמבלי והוסיפו הערות מתאימות עם IDA.

- סוגי הערות:
  - Insert - הערה מעל השורה.
  - Shift + Insert – הערה מתחת לשורה.
  - ; הערה בצד.

מחרוזות

SCAS
SCAS compares EAX with doubleword at [edi], and increments EDI;
scas DWORD PTR [edi]; // or just scas

STOS
STOS (store to string) moves a dword from eax to [edi], and increments EDI.
stos DWORD PTR ES:[edi]

CMPS
compares dword at address [esi] with dword at address [edi];
IF the direction flag is 0 - increments EDI and ESI.
If the direction flag is 1 (STD was executed), the registers decrement.
cmps DWORD PTR DS:[esi], DWORD PTR ES:[edi]

⋮

מחרוזות

REP/REPE/REPNE

The string instructions may be prefixed by REP/REPE/REPNE which will repeat the instructions according to the following conditions:

rep	decrement ecx ; repeat if ecx ≠ 0
repe	decrement ecx ; repeat if ecx ≠ 0 AND zf = 1
repz	decrement ecx ; repeat if ecx ≠ 0 AND zf = 1
repne	decrement ecx ; repeat if ecx ≠ 0 AND zf = 0
repnz	decrement ecx ; repeat if ecx ≠ 0 AND zf = 0

מחרוזות

- מה המטרה של הקוד?

```
; EDI point to "hello world"
xor ecx,ecx
xor eax,eax
not ecx
repne scasb
not ecx
dec ecx

ECX = ?
```

```
ECX = strlen(EDI);
```

סיכום

- ראינו היום
  - כיצד להשתמש ב IDA.
  - כיצד מבנים מסוימים נראים באסמבלי (ולהפך).
  - פקודות נוספות.
  - סביר להניח שיש שוני בין הקומפיילרים השונים אך העקרונות זהים.

- יש עוד המון מה ללמוד מהבחינה הזאת, קוד שהקומפיילר יוצר לא תמיד פשוט להבנה.

CRACKMES

- תוכנית קטנה שנועדה לבחון יכולות הנדסה לאחור.
- בדרך כלל נבנית ע"י חוקרים אחרים - לכן חוקי לחקור אותה.
- מכילים מנגנונים זהים למנגנונים שקיימים בתוכנות מסחריות.

- דוגמא לאתרים:
  - Crackmes.de – מכיל מאגר שלם של תוכניות.
  - Tdhack.com – כנ"ל.
  - וכמובן http://webcourse.cs.technion.ac.il/236653/
    - תחת Assigment 2

- נפתור עכשיו crackme פשוט בתור חימום...