מבחן בהנדסה לאחור - 236496

סמסטר חורף תש"ף

מועד א׳, 20.02.2020

מרצה: עומר קדמיאל

מתרגל: טל שנקר

חלק ראשון

משך חלק זה של הבחינה: 3 שעות.

בחלק זה של הבחינה ישנן 2 שאלות. ענו על כולן.

בחלק זה 3 עמודים, כולל עמוד זה. וודאו שכל הדפים נמצאים.

מותר להשתמש בכל חומר עזר, אך אין לשוחח, להתייעץ, לקבל רמז, לתת רמז, או להיעזר בשום אדם אחר על המבחן, על תוכנו, והתשובות לשאלות. <u>יש לפתור את השאלות לבד.</u>

נא לכבות מכשירים סלולריים ושעונים חכמים.

בכל מקרה של שימוש בחומר חיצוני יש לתת הפניה אליו.

תוכנות מותרות: התוכנות אשר נלמדו בקורס. בפרט, אין להשתמש בכלי Decompilation!

ענו תשובות ברורות ככל האפשר. **<u>נמקו את כל תשובותיכם</u>**.

במידה שניתן לענות על שאלה במספר דרכים, **<u>ניקוד מלא יינתן לפתרונות קצרים ופשוטים</u>**.

<u>השאלות והקבצים המצורפים דומים אך אינם זהים לכל הסטודנטים</u>.

הגשה אלקטרונית באתר המקצוע עד השעה 12:00. יש להגיש קובץ ZIP (ואך ורק ZIP) ובו כל קבצי ההגשה. ההגשה כוללת בדיוק את הקבצים הבאים:

1. קובץ בשם part1.pdf עם התשובות בכתב <u>לכל</u> השאלות.
2. קבצים בשמות crackme.txt ו crackme.args אותם תצרו בשאלה 2.

<u>הערה לכל המבחן: בתרגילים הרטובים, אם אינכם מצליחים להגיע לפתרון שרץ בפועל, תארו במילים מה ניסיתם לעשות - זה עשוי לזכות אתכם בניקוד חלקי!</u>

בהצלחה!

שאלה 1 (20 נקודות) - יבש:

לפניכם הפונקציות Foo ו Bar. קראו את הקוד וענו על השאלות שאחריו.

```
Foo proc near (int)

push    ebp
mov     ebp, esp
sub     esp, 168
mov     DWORD PTR [ebp-168], 1
mov     DWORD PTR [ebp-164], 1
mov     ecx, 2

L1:
cmp     ecx, DWORD PTR [ebp+8]
jg      L2
push    ecx
lea     eax, [ebp-168]
push    eax
call    Bar
add     esp, 8
inc     ecx
jmp     L1

L2:
mov     eax, DWORD PTR [ebp+8]
lea     eax, [ebp-168+eax*4]
mov     eax, DWORD PTR [eax]
leave
ret
```

```
Bar proc near (int, int)

push    ebp
mov     ebp, esp
push    ebx
mov     eax, DWORD PTR [ebp+12]
add     eax, 1073741823
lea     edx, [0+eax*4]
mov     eax, DWORD PTR [ebp+8]
add     eax, edx
mov     ecx, DWORD PTR [eax]

mov     eax, DWORD PTR [ebp+12]
add     eax, 1073741822
lea     edx, [0+eax*4]
mov     eax, DWORD PTR [ebp+8]
add     eax, edx
mov     edx, DWORD PTR [eax]

mov     eax, DWORD PTR [ebp+12]
lea     ebx, [0+eax*4]
mov     eax, DWORD PTR [ebp+8]
add     eax, ebx
add     edx, ecx
mov     DWORD PTR [eax], edx
mov     eax, DWORD PTR [eax]
pop     ebx
pop     ebp
ret
```

א. מה מבצע קטע הקוד המודגש בפונקציה Bar?

הציעו פקודה פשוטה יותר להבנה, המבצעת בדיוק את אותו החישוב (פקודה אחת בלבד).

ב. איזה חישוב מוכר מבצעת הפונקציה Foo? מה הפונקציה מחזירה? הסבירו.

ג. איזו חולשה קיימת בקוד? מצאו אותה והסבירו כיצד היה ניתן לתקנה.

ד. כיצד ניתן לנצל את החולשה על מנת להריץ קוד הנמצא בכתובת 0x 29CEA5DD.

רמז: מספר פיבואנצ'י ה-44 הוא 701408733.

שאלה 2 (30 נקודות) - CrackMe:

למבחן מצורף הקובץ crackme.exe. חקרו את הקובץ וענו על השאלות שלהלן. את התשובות המילוליות יש לרשום בקובץ part1.pdf ואילו את הקלט המבוקש בסעיף ג', **יש לרשום הן בקובץ part1.pdf והן בקובץ crackme.txt.**

א. תרגמו את הפונקציה **401410** לקוד דמוי C. אין להשתמש בכלי decompilation אלא לתרגם בעצמכם לקוד אשר המתכנת הסביר היה כותב. מה מטרת פונקציה זו בתכנית? מה היא מקבלת כקלט, מחזירה כפלט, וכיצד היא מבצעת את פעולותיה?

ג. התכנית שקיבלתם הינה משחק. תארו את פעולת המשחק על פי הסעיפים הבאים:

1. מהם מבני הנתונים במשחק? כיצד הם מאותחלים?
2. איזה קלט מהמשתמש נחשב חוקי?
3. התכנית מקבלת ארגומנטים בשורת הפקודה. כיצד הם משפיעים על מהלך המחשק?
4. בהינתן קלט חוקי, מהי השפעתו על המשחק? למשל, אם ישנו לוח, כיצד מושפע הלוח? איך משתנים מבני הנתונים כתוצאה מקלט זה?
5. מהם חוקי המשחק? בנוסף, מהם התנאים המובילים לניצחון במשחק?

ד. מצאו ארגומנטים וקלט המובילים לניצחון במשחק. עליכם להגיש קובץ crackme.txt המכיל את הקלט, וקובץ crackme.args המכיל את רשימת הארגומנטים. שימו לב שעל הקלט לעבוד, כלומר, להוציא פלט המעיד על הצלחה, עבור הרצת השורה הבאה ב Windows PowerShell:

```
Get-Content crackme.txt | crackme.exe "$(Get-Content crackme.args)"
```

יש לצטט את הקלט והארגומנטים גם ב part1.pdf.