מבחן בהנדסה לאחור - 236496

סמסטר חורף תשפ"א

מועד ב׳, 18.03.2021

מרצה: עומר קדמיאל

מתרגל: עידן רז

חלק ראשון

משך חלק זה של הבחינה: 3 וחצי שעות.

בחלק זה של הבחינה ישנן 3 שאלות. ענו על כולן.

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>

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 12:30. 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. קובץ בשם crackme.txt אותו תצרו בשאלה 2.
3. קובץ הi64/idb מIDA המתאים לcrackme.exe.

<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 0:

נא להעתיק את הקטע הבא בתחילת ה-PDF ולמלא את שמכם המלא ותעודת הזהות שלכם כאישור לכך שקראתם אותו.

אני _____, ת.ז. _____, מאשר/ת כי אני מכיר את מדיניות הקורס והפקולטה בנושא יושר אקדמי במהלך הבחינה. בפרט, אני מאשר/ת כי אני מודע/ת לכך שבמהלך הבחינה אסור לי לתקשר עם אחרים בכל אמצעי כל שהוא, למעט עם צוות הקורס.

שאלה 1 (20 נקודות) - יבש:

א. על מנת להתמודד עם הסכנה של buffer overflow, מימשו בקומפיילר את ההצעה הבאה למילוי buffer בגודל 0x100 (כאשר ecx בשליטת המשתמש):

```
        Add esi, ecx
        Add edi, ecx
Start:  Cmp ecx, 100
        Jg END
        Dec esi
        Dec edi
        Dec ecx
        Movsb
        Cmp ecx, 0
        Jnz Start
End:
```

1. הסבירו במילותיכם מה מתבצע בקטע הקוד. למה משמש כל רגיסטר?
2. האם מול מימוש זה ניתן לדרוס את כתובת החזרה אשר נמצאת לאחר ה-buffer?
3. האם בכל זאת קיימת חולשה במימוש זה? פרטו והסבירו. אם קיימת חולשה – מה השינוי המינימלי הנדרש על מנת לתקן אותה?

ב. קיימת במערכת פונקציה בשם myVirtaulAlloc.

1. הסבירו במילותיכם כיצד ניתן לנטר את כלל התוכניות המשתמשות בפונקציה זו מעתה ואילך.
   a. בהינתן שהיא נמצאת ב-dll ידוע.
   b. בהינתן שהיא נמצאת באותו קובץ עם התוכנית, וקובץ זה הוא read only.
2. אנחנו רוצים להריץ את הפונקציה, אבל אנחנו יודעים שתהליך אחר (antivirus) עשה עליה הוקינג סטנדרטי (הפונקציה אינה מוכנה עם hot patching) ומוודא את קיום ההוקינג באופן רציף. כיצד ניתן לחמוק ממנגנון הזיהוי?

ג. הניחו שלאור האיומים של ערוץ הצד התזמוני, נבנתה ארכיטקטורה שבה כל פעולת מעבד לוקחת בדיוק אותו זמן (הניחו שאין pipeline). הסבירו כיצד הדבר משפיע על התקפות ערוצי צד אחרות בדגש על em ו-power.

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 **sub_4015F2** 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?

ב. 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. בהינתן קלט חוקי, מהי השפעתו על המשחק? למשל, אם ישנו לוח, כיצד מושפע הלוח? איך משתנים מבני הנתונים כתוצאה מקלט זה?
4. מהם חוקי המשחק? בנוסף, מהם התנאים המובילים לניצחון במשחק?

ג. מצאו וקלט המוביל לניצחון במשחק. שימו לב שעל הקלט לעבוד, כלומר, להוציא פלט המעיד על הצלחה, עבור הרצת השורה הבאה :

```
crackme.exe < crackme.txt
```

יש לצטט את הקלט גם ב part1.pdf.