מבחן בהנדסה לאחור - 236496

סמסטר אביב תשפ"א

מועד א׳, 22.07.2021

מרצה: עומר קדמיאל

מתרגל: עידן רז

חלק ראשון

משך חלק זה של הבחינה: 3 שעות.

בחלק זה של הבחינה ישנן 2 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 12:00. יש להגיש קובץ ZIP (ואך ורק ZIP) ובו כל קבצי ההגשה. ההגשה כוללת בדיוק את הקבצים הבאים:

1. קובץ בשם ID_part1.pdf (כאשר ID זאת תעודת הזהות שלכם) עם התשובות בכתב <u>לכל</u> השאלות.
2. קובץ בשם crackme.txt אותו 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 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:

בתכנית כלשהי קיים buffer overflow, ואנחנו רוצים להשתמש בו על מנת להריץ shellcode הנמצא בבאפר.

במערכת מופעל DEP, כך שקפיצה באופן ישיר לקוד תייצר חריגה. בנוסף, יש שימוש בקנריות ולכן התקפות מסוג ROP לא יעבדו במקרה זה.

מאידך, אנחנו יודעים שלפני שנקראה הפונקציה הנוכחית, הוגדרו שני exception handler-ים באמצעות SEH.

א. הסבירו מהו מנגנון הDEP וכיצד ניתן להתגבר עליו באמצעות פונקציות מ winApi.

ב. הסבירו אודות מנגנון SEH, וכיצד הוא מיושם.

ג. בהנתן שהתוקף רואה את המחסנית לפני השימוש ב-BOF (לדוגמה באמצעות חולשת קריאה), מה הוא יכול ללמוד (מעבר לערך הקנרית)?

ד. באמצעות התשובות לסעיפים הקודמים פרטו כיצד למלא את הבאפר על מנת שירוץ קוד מראש הבאפר. הערות: ניתן להניח כי ידועות הכתובות של פונקציות מkernel32 אך לא ניתן להשתמש בgadgets. בנוסף, ניתן להניח כי אין תווים אסורים בoverflow.

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.**

פתרון סופי בלי הסבר לא יתקבל.

א. תרגמו את הפונקציה **sub_401460** 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.