שנה"ל **תשפ"א**__, סמסטר _**ב**_, מועד א___
שאלון בחינה בקורס : מבוא לרברסינג
מספר קורס: 157130.3.5781

- שם המרצה: ברק גונן
- תאריך הבחינה: 10.6.2022
- משך הבחינה (בדקות): 180
- חומר עזר מותר לשימוש: הכל
- מחשבון: כן
- המבחן כולל סה"כ 1 שאלות, יש לענות על 1 שאלות.

תלמיד.ה יקר.ה,

1. **נוהל הבחינות של המרכז האקדמי לב מחייב אותך**, באחריותך לקוראו ולהכירו - בחינה עלולה להיפסל על כל חריגה מהנוהל.
2. אם אינך מבין את כוונת המרצה בשאלה כלשהי, עליך לכתוב בראש התשובה כיצד הינך מבין את השאלה ולפתור בהתאם. המרצה ישקול האם יש מקום להבנה זו ואז ינקד בהתאם.
3. לידיעתך, תורדנה נקודות לא רק על שגיאות, אלא גם על תוספות לא רלוונטיות, העדר נימוק הולם לתשובה, חוסר סדר ותשובה דו-משמעית, כאשר נדרשת תשובה חד משמעית.

בהצלחה רבה !

שנה״ל **תשפ״א**__, סמסטר _**ב**_, מועד א___
שאלון בחינה בקורס: מבוא לרברסינג
מספר קורס: 157130.3.5781

<u>שאלה 1</u>

כיתבו דו״ח מחקר (קובץ word) ובצעו תיעוד של העבודה שלכם תוך כדי מענה על השאלות הבאות. מומלץ לצרף צילומי מסך של דברים שיסייעו להבנת דרך הפתרון שלכם. עליכם להגיש:

א. דוח המחקר. היקף מומלץ לדו״ח המחקר הוא כ-4 עד 5 עמודים, כולל צילומי מסך.
ב. קובץ ה-exe לאחר ההטלאה (patching)
ג. קוד בשפה עילית

השאלות הבאות מתייחסות לקובץ MoedA2022.exe.

סעיף 1- זיהוי והסרת האנטידיבאג (30 נקודות)

א. כיתבו ב-Write Up כיצד והיכן מבוצע אנטידיבאג. הוסיפו צילומי מסך של קטעי הקוד הרלבנטיים – 15 נקודות
ב. בצעו patching שיעקוף את מנגנון האנטידיבאג, מבלי לשנות את אופן פעולת התוכנית. צרפו צילום מסך של הקוד המפוצ׳פץ׳ – 15 נקודות

סעיף 2 – הגעה למסר ההצלחה (50 נקודות)

א. מיצאו את main ב-IDA. תנו שמות משמעותיים לכל המשתנים הלוקליים (כל המשתנים ש-IDA מפרשת בתור var_xx, לדוגמה var_24). שמות משמעותיים יהיו שמות שסביר שמתכנת ייתן למשתנים בקוד. צרפו צילומי מסך מתוך IDA בהם ניתן לראות את כל main יחד עם השמות שנתתם – 25 נקודות
ב. הסבירו מהן כל הפעולות שהמשתמש צריך לעשות על מנת להגיע למסר ההצלחה, מבלי לעקוף חלקים מהתוכנית באמצעות פצ׳פוץ׳ (כלומר הניחו שהמשתמש אינו יודע לפצ׳פץ׳ וצריך לקיים את דרישות התוכנית כדי להגיע למסר ההצלחה). ה-Write Up צריך לכלול הסבר כיצד הגעתם למסקנות הללו. טיפ: מסר ההצלחה מורכב מתווים דפיסים ובעלי משמעות. לדוגמה hello world יכול להיות מסר הצלחה, אך dasd4bsQs אינו מסר הצלחה – 25 נקודות.

סעיף 3 – ביצוע רברסינג (20 נקודות)

א. כיתבו את הקוד של main בשפת פייתון או CPP. **אין צורך לכתוב קוד שאינו בתוך main או קוד של פונקציות ש- main קורא להן**.
   a. הקוד שמטפל בבדיקה האם הסיסמה היא נכונה – 10 נקודות
   b. הקוד שמפענח את מסר ההצלחה– 10 נקודות

בהצלחה!

ברק