**הנדסה לאחור 236496 – תרגיל בית 4**

מגישים:  
אלון פליסקוב 315468116  
שליו ריסין 211578794

חלק יבש

שאלה 1

מדובר ברצף הפקודות:  
  
או, מדובר ברצף הבתים 60 c3.  
את רצף הבתים הזה ניתן למצוא ב-DLL לגיטימי. למשל, עבור הפקודה הבאה:

add BYTE PTR [eax-0x3d], ah

הקידוד שלה הוא רצף הבתים:

00 60 c3

ניתן לראות כי חלק מהקידוד של הפקודה הוא רצף הבתים 60 c3. לכן, ניתן למצוא את הגאדג'ט הנ"ל ב-DLL שבו מופיעה הפקודה שציינו.

שאלה 2

שאלה 3

שרשרת ה-ROP לא עובדת במקרה ספציפי זה, כי strcpy בגרסתה של UNICODE, מפסיקה לקרוא מ-buffer כאשר היא נתקלת ברצף של שני בתים 0x0000. זאת מכיוון שב-UNICODE, הרצף 0x0000 הוא ה-null terminator שמסמן סיום של מחרוזת (bad byte).  
אנחנו חייבים שב-buffer יופיע, למשל, רצף הבתים 0x00000040 צריך להופיע כי הוא מהווה את הארגומנט של ההרשאות החדשות לדף ב-VirtualProtect.

שאלה 4

כעת מסופק לנו ה-gadget שנותן לנו לבצע negation על רצף של ארבעה בתים בזכרון.  
כשנרצה לשים ב-buffer רצף של 4 בתים שבהם יש 2 בתים שהם 0x0000, אז במקום זה נשים את אותם הבתים negated מלכתחילה. כשנצטרך אותם, נוכל לקרוא אותם מהמחסנית באמצעות הגאדג'ט החדש, ואם נצטרך אותם על המחסנית אז נוכל לקרוא אותם באמצעות הגאדג'ט החדש ואז לדחוף מחדש, באמצעות הגאד'גט השמיני (pushad).

שלב שני – התחברות מוצלחת

ניסינו להתחבר לכל 4 המשתמשים.  
A screenshot of a computer error

Description automatically generated with medium confidence  
A screenshot of a computer

Description automatically generated with medium confidence  
A screenshot of a computer screen

Description automatically generated with low confidence  
A screenshot of a computer screen

Description automatically generated with low confidence  
גילינו כי ל-archer יש הרשאות של admin, ולאחרים אין.  
לכן, ל-archer יש את ההרשאות הגבוהות ביותר. האינדיקציה לכך היא הודעת ה-  
“Welcome archer (Admin)” ש-archer מקבל בכניסתו למערכת. בנוסף, ל-archer יש גישה לשתי פקודות נוספות, שלאחרים אין: PEEK, LOAD.  
כתבנו קובץ **users.py** כמו שהתבקשנו.