**הנדסה לאחור 236496 – תרגיל בית 3**

מגישים: אלון פליסקוב 315468116 שליו ריסין 211578794

חלק יבש

1. הפונקציה poll:

ראשית – מקריאת השאלה, הנחנו את הדבר הבא – הפונקציה poll אינה אחראית על בדיקת המספר בזכרון הגלובלי, אלא שכאשר עבר הזמן שכתוב בזכרון הגלובלי, היא נקראת.  
בתחילת הפונקציה נזריק פקודת jmp. יעד ה-jmp הוא קוד שלנו. בקוד שלנו יתבצעו הדברים הבאים:

1. שחזור הקוד המקורי ב-poll (החזרת הפקודות שהיו במקום ה-jmp שהזרקנו).
2. קריאה ל-poll, על מנת שתרוץ כרגיל ותגרום לכל ה-side effects הצפויים, כולל כתיבה לזכרון הגלובאלי.

**לעשות : להבין מה רוצים בסעיף 1**

1. מזריקים לסוף הפונקציה פקודת jmp לקוד שלנו.

בקוד שלנו:

1. נשמור את תוצאת הריצה של mine. נסמנה ב-y.
2. הארגומנט x זמין על המחסנית ולא השתנה לפי ההנחה בשאלה שהפונקציה mine משפיעה רק על משתנים לוקליים ורגיסטרים. לכן, ניקח את x ונריץ את mine מהקוד שלנו (לאחר שהסרנו את ה-hook בסוף הפונקציה), כל פעם מנקודת כניסה אחרת.
3. אם אחת הריצות של mine הניבה תוצאה ששווה ל-y, אז נקרא ל-mine מנקודת הכניסה המתאימה לריצה זו, עם הארגומנט .
4. נבצע ret כשה-return value מהפונקציה הוא התוצאה מ- ג'.
5. ש'םקכחש'
6. פש'קכ
7. ש'קחםכ'
8. ש'קןכמ'ןקכי