**תרגיל בית 4 בהנדסה לאחור**

**Vulnerabilities**

**דרור כרמון 036861292**

**עידו מנגר 212324313**

**חלק יבש**

1. יתכן שרצף הפקודות 60 C3 הוא חלק מפקודה ארוכה יותר שתחילתה כתובת נמוכה מ- 0x9ad9e71c אבל כאשר מפרשים אותה מהכתובת הנ"ל היא מתורגמת לפעולות שהתקבלו. למשל הפקודה המלאה בגודל 3 בתים היא 24 60 C3 והיא מתורגמת לפקודות:

0x9ad9e71b:  24 60      and    al,0x60  
0x9ad9e71d:  c3         ret

Part1-

9ad9e700- 3 pops for 3 args

70707070- file handler

00000001- SE\_OBJECT\_TYPE Enum value that means FILE\_OBJECT

11111111- Security information parameter, we want permissions will be set all to 1 including read/write

# SetSecurityInfo -windows function that sets the security info of the file to what we gave it- we now should have all of the permissions

# Part 2-

# 0x7070708b-will jump to the file?

1. כשstrcpy מקבל null char הוא מסיים את הקליטה ומפרש את זה כסוף הקלט, בגלל שאנחנו מכניסים כאלה בחלק הראשון, הקלט יפסק שם ומה שהכנסנו לא יעבוד
2. בשביל לתקן את זה נרצה להשתמש בגאדגטים החדשים כל פעם ששמנו null char ,

הכתובת 9ad9e700 היא הבעייתית, אם נשים 1AD9E6FF נפעיל עליו את הגאדגט השני ואז את הראשון אז נקבל את הכתובת לכן נשים בהתחלה במקום הכתובת את הקטע הבא-

6ad6e720-not

9ad9e711-will call the next line

6ad6e71d-neg

1AD9E6FF-eventually will become the address we want

החלק הבעייתי האחר הוא ה 00000001 של הenum

שבמקרה הוא שווה ערך לnot fffffffd – נרצה להשתמש בגאדג'ט השני שלנו, נשים לב שמקודם הייתה לנו שורה שרק דילגנו עליה, עכשיו נחליף אותה בפעולה ובגלל שהיא מדלגת על שני כתובות היא תפעל על המקום שאנו רוצים

6ad6e720-not

6ad6e720-will call the next line

6ad6e71d-neg

1AD9E6FF-eventually will become the address we want  
fffffffd- will become the enum we want

**חלק רטוב**