**תרגיל בית 2 בהנדסה לאחור**

בעזרת רשימת המשתמשים והסיסמאות נכנסנו לאתר, אצל כל אחד מהמשתמשים יש 3 כספות:

* משותפת – מוצפנת ע"י סיסמה
* ציבורית – המכילה:
  + תרשים המתאר כיצד ניתן לפתוח את הכספת המשותפת
  + analyzer.exe המתואר בתרגיל.
* פרטית – מכילה קבצים שונים אצל כל משתמש.

**חלק א'**

לפי התרשים שמצאנו התחלנו לפצח את קבצי הsafe.exe של המשתמשים השתמשנו בניתוח סטטי בעזרת Ida.

 **Giant**

איתרנו את פונק' ה- main של הקובץ safe.exe ע"פ כלל האצבע שהיא הקריאה האחרונה לפני הקריאות ל- cexit ול- ExitProcess. פונקציית main מבצעת קריאות ל4 פונק' אחת אחרי השניה – נסמן אותן f1,f2,f3,f4. לאחר מכאן חיפשנו איפה התוכנית מקבלת קלטים בעזרת הלשונית Imports.

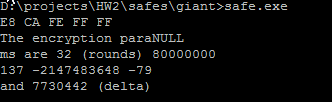
ראינו שיש 4 קריאות לscanf:

1. בפונק' sub\_401683:
   1. הקלט המבוקש הוא מהצורה "%02X %02X %02X %02X %02X", כלומר 5 מספרים בגדול byte בייצוג הקסה.
   2. לאחר קבלת הקלט, יש קריאה לפונק' אשר הערך המוחזר שלה הוא ebp+4, כלומר כתובת החזרה של הפונק'. לכתובת זו מוסיפים 98h מה שמביא אותנו לכתובת 4017B4h שהיא שורה בקוד של הפונק' sub\_401683. הקוד החל משורה זו מכיל 6 פקודות nop.
   3. בעזרת קריאה VirtualProtect משנים את הרשאות של הכתובת שחישבנו בסעיף קודם ל- PAGE\_EXECUTE\_READWRITE ולאחר מכן בעזרת memcpy מעתיקים את 5 הבתים מהקלט אל הכתובת.
   4. הבנו הקלט שאנחנו מחפשים הוא פקודה בינארית שאמורה להחליף את פקודות הnops. המשכנו לחקור את הפונק' וראינו שיש שקריאה רקורסיבית (החלק המתואר בסעיפים 1.2-1.3 מוגן בעזרת דגל גלובאלי כך שיתבצע רק פעם אחת). לאחר הקריאה הרקורסיבית נראה שמכינים שוב פרמטרים לקריאה רקורסיבית אבל במקום הקריאה יש nops, הבאנו שהקלט צריך להכיל את הפקודה call עם הoffset הנכון כך שתתבצע קריאה רקורסיבית.
   5. חישבנו את ה-offset: 401683h – 4017B4h = -131h = FFFFFECF, בעזרת האתר defuse.ca תרגמנו את הפקודה call 0xFFFFFECF 🡨 **E8 CA FE FF FF**
2. בפונק' f3
   1. בתחילת הפונק' יש קריאה ל- SetUnhandledExceptionFilter לפי התיעוד בMSDN היא משמשת לאיתחול פונק לטיפול בחריגות. הפונק מקבלת כפרמטר כתובת של פונק' לטיפול בחריגות. הפונק' לטיפול בחריגות (ExceptionHandler) מקבלת כארגומנט מצביע ל- struct \_EXCEPTION\_POINTERS המכיל מידע על ה- exception. היא מבצעת את הפעולות הבאות:
      1. ניגשים לשדה המתאים ובודקים עם החריגה היא מסוג EXCEPTION\_ACCESS\_VIOLATION, אם לא מחזירים 0 ויוצאים.
      2. ניגשים לשדה המתאים וקוראים אם הכתובת אליה ניסו לגשת היא כתובת 0 , אם לא מחזירים 0 ויוצאים.
      3. מבצעים השמה למשתנה גלובאלי (נקראה לו – isExceptionOccurred) ושמים בו את הערך 1.
      4. ניגשים לשדה המתאים וקוראים את הכתובת של הפקודה שבה התבצעה הגישה הלא חוקית לזיכרון – dest
      5. בעזרת קריאה ל-VirtualProtect משנים את ההרשאות של destו-24h הכתובות העוקבות ל- PAGE\_EXECUTE\_READWRITE.
      6. בעזרת קריאה ל-memset מציבים ב- destו-24h הכתובות העוקבות את הערך 90h (פקודת nop)
      7. בעזרת VirtualProtect משנים שוב את ההרשאות של destו-24h הכתובות העוקבות ל- PAGE\_EXECUTE\_READ.
      8. מחזירים את הערך EXCEPTION\_CONTINUE\_EXECUTION שמסמן שהטיפול בחריגה בוצע ורוצים להמשיך מהמקום בו היא התבצעה.
   2. לאחר מכן בעזרת scanf קולטים 4 תווים (כל אחד בגודל בית) c1,c2,c3,c4 ומציבים את הערך המספרי שלהם לתוך אוגר eax בסדר הבא : c1c3c2c4 לאחר מכן מחסרים מהמספר שיצא את המספר 4E4C554Ch, נשים לב שערכי ה-ascii של רצף הבתים יוצר את המחרוזת "NLUL".
   3. ניגשים לכתובת שמתקבלת מתוצאת החיסור ומנסים לקרוא משם ערך. העובדה שמחסרים את המחרוזת "NLUL" ושמצפים לטפל בחריגה בגישה לכתובת 0, הבנו שהקלט הנדרש הוא **"NULL"**
3. שתי קריאות ב-f4
   1. קריאה ראשונה מבקשת קלט בפורמט "%x" כלומר מספר בייצוג הקסהדצימלי (input)  
      אם הקלט שלילי מבצעים לו היפוך סימן.
   2. קריאה שניה מבקשת קלט בפורמט "%d %d %d" כלומר 3 מספרים (x1,x2,x3)
   3. לאחר מכן יש מספר הסתעפויות בקוד ע"פ ערכי הקלטים. כדי "לעבור בהצלחה" את כל ההסתעפויות ולהגיע לחלק של הפונ' שמבצע משהו הקלטים צרכים לעמוד בתנאים הבאים:

x1 >= 0  
x1 % 256 == 137 🡪 **x1 == 137**  
y = -9164\*x3 -58\*x3^2 – 361977 = 1 🡪 **x3 == -79**  
x2 < 0  
x2 - y > 0 🡪 x2 = -2147483648 (0x80000000)  
Input < 0 🡪 input = 0x80000000

הסבר לשני האחרונים : 0x80000000 הוא המספר המסומן הקטן ביותר שניתן לייצג בעזרת 4 בתים לכן אם מחסירים ממנו את y ששווה 1 אז בגלל overflow הוא הופך ל- 0x7FFFFFFF שהוא המספר החיובי הגדול ביותר בייצוג זה. כנ"ל אם מבצעים עליו neg שהופך את כל הסיביות ומוסיף 1 ולכן הוא נשאר 0x80000000 כלומר נשאר שלילי.

הרצנו את safe.exe:  
קלט ראשון : E8 CA FE FF FF.  
קלט שני: NULL  
קלט שלישי: 80000000   
קלט רביעי: 137 -2147483648 -79  
פלט למסך: The encryption params are 32 (rounds) and 7730442 (delta)



 **wizard**

איתרנו את פונק' ה- main של הקובץ safe.exe ע"פ כלל האצבע שהיא הקריאה האחרונה לפני הקריאות ל- cexit ול- ExitProcess. פונקציית main מבצעת קריאות ל3 פונק' אחת אחרי השניה – נסמן אותן f1,f2,f3. לאחר מכאן חיפשנו איפה התוכנית מקבלת קלטים בעזרת הלשונית Imports.

ראינו שיש 2 קריאות לscanf:

1. בפונק' f2:  
   בתחילת הפונק' בודקים את ערכו של משתנה גלובאלי (נקרא לו f2\_call\_clounter). ערכו של המשתנה גדל באחד כל פעם לפני יציאה תקינה מהפונק' (שחזור מחסנית וקריאה לret).
   1. בפעם הראשונה שמגיעים לפונק' f2, נכנסים לסנף שמצבע את הפעולות הבאות:
      1. שומרים למשתנים גלובאלים את ערכי: כתובת החזרה מהפונק (ebp+4), ערך ebp הקודם, ebp, esp. **זה מרמז לנו שכנראה ערכים אלו ידרסו וצריך לשמור אותם כדי לאפשר המשך ריצה תקינה של הקוד**.
      2. קריאה לקלט מהמשתמש בפורמט מחרוזת.
      3. 28 התווים הראשונים של מחרוזת מתורגמים לערך מספרי ע"י החסרה של התו 'A', כלומר כל תו מקבל את ערכו הלקסיקוגרפי בABC. **זה מרמז שהקלט כנראה צריך להכיל רק אותיות ABC גדולות**.
      4. 28 הערכים הראשוני של הקלט (לאחר ההמרה מסעיף קודם) מעודכנים להיות תוצאת הxor של כל ערך עם הערך הבא אחריו. האחרון הוא תוצאת xor בינו לבין הראשון.
      5. 28 הערכים מומרים שוב להיות תווי asci ע"י הוספת הערך של התו 'A'
      6. 28 הערכים מושווים בעזרת strcnmp למחרוזת "CIONAPGNOGKGEGPFJHEDKNIGNIBK".  
         כדי לשחזר את הקלט הנדרש כתבנו תוכנית אשר מבצעת את הפעולה ההפוכה על מחרוזת הקלט ומחפשת קלט אפשרי תקין.

#define SIZE 28

#define F 15

void findKey()

{

const char\* ref = "CIONAPGNOGKGEGPFJHEDKNIGNIBK";

int ref\_num[SIZE];

int key[SIZE];

for (int i = 0; i < SIZE; i++)

{

ref\_num[i] = ref[i] - 'A';

}

for (int k = 0; k <= F; k++)

{

key[1] = k;

key[0] = key[1] ^ ref\_num[0];

for (int i = 2; i < SIZE; i++)

{

key[i] = key[i - 1] ^ ref\_num[i - 1];

}

if ((key[SIZE - 1] ^ ref\_num[0]) == ref\_num[SIZE - 1])

{

//found input key !!

break;

}

}

//print result

for (int i = 0; i < SIZE; i++)

{

printf("%c", key[i] + 'A');

}

printf("\n");

}

בעזרת הפונק' מצאנו את הקלט הנדרש "NPHJEELNAOICEAGJMFCGFPCKMBJI"

* + 1. לאחר הכנסת הקלט התקין מגיעים לחלק בקוד שמעתיק (בעזרת sprintf) את ערכי הקלט (ללא הגבלת גודל) ולאחריו את כתובת הפונק' f2 לכתובת שנמצאת על המחסנית. לאחר מכן מבצעים בדיקה אם כתובת החזרה (ebp+4) זהה לכתובת הפונק' עצמה (f2). כדי שמצב זה יקרה אנחנו צריך לבצע דריסה של כתובת החזרה ע"י כך שניתן קלט באורך מתאים ואז sprintf תדרוס את כתובת החזרה בכתובת של f2. חישבנו שכדי שזה יקרה צריך להוסיף לקלט 16 בתים כלשהם ולכן הכנסו את הקלט: "**NPHJEELNAOICEAGJMFCGFPCKMBJI1234123412341234**".
    2. לאחר מכן מגיעים לחלק שבמצע עדכון של f2\_call\_clounter, ניקוי מחסנית וחזרה, מכיוון שדרסנו את כתובת החזרה מגיעים שוב לתחילת הפונק' f2.
  1. בפעם השניה שמגיעים לf2 הפונק' מבצעת הדפסה למסך של הפלט :

**"The hashed password is: a60b"**

לאחר מכן מתבצע שחזור של ערכי המחסנית שנדרסו בשלבים הקודמים וחזרה לmain.

1. הפונק' f3 מגדירה שני מערכים הראשון מאותחל בערכים כך:

int arr[12] = { 6,10,1,2,8,5,12,7,4,11,3,9 };

* 1. המערך השני (int input[12]) מאותחל ע"י קלט מהמשתמש באופן הבא:

for (int i = 0; i < 12; i++)

{

int x;

scanf("%d", &x);

input[i] = arr[x];

}

לאחר מכן נבדקים התנאים הבאים:

1. no duplicate value in input.
2. input [1]+ input [2]+ input [3]+ input [4] == 16
3. input [7]+ input [8]+ input [9]+ input [10] == 16
4. input [0]+ input [2]+ input [5]+ input [7]) == 16
5. input [0]+ input [3]+ input [6]+ input [10]) == 16
6. input [1]+ input [5]+ input [8]+ input [11]) == 16
7. input [4]+ input [6]+ input [9]+ input [11]) == 16
8. input [0]+ input [1]+ input [4]+ input [7]+ input [10]+ input [11]) == 16

השתמשנו בקוד הבא ע"מ למצוא את הקלט הנדרש:

void solverf3()

{

std::vector<int> ind = { 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 };

std::vector<int> arr = { 6, 10, 1, 2, 8, 5, 12, 7, 4 ,11, 3, 9 };

const int target = 26;

do {

int& x0 = arr[ind[0]];

int& x1 = arr[ind[1]];

int& x2 = arr[ind[2]];

int& x3 = arr[ind[3]];

int& x4 = arr[ind[4]];

int& x5 = arr[ind[5]];

int& x6 = arr[ind[6]];

int& x7 = arr[ind[7]];

int& x8 = arr[ind[8]];

int& x9 = arr[ind[9]];

int& x10 = arr[ind[10]];

int& x11 = arr[ind[11]];

bool B1 = (x1 + x2 + x3 + x4 == target);

bool B2 = (x7 + x8 + x9 + x10 == target);

bool B3 = (x0 + x2 + x5 + x7 == target);

bool B4 = (x0 + x3 + x6 + x10 == target);

bool B5 = (x1 + x5 + x8 + x11 == target);

bool B6 = (x4 + x6 + x9 + x11 == target);

bool B7 = (x0 + x1 + x4 + x7 + x10 + x11 == target);

if (B1 && B2 && B3 && B4 && B5 && B6 && B7)

{

for (auto i : ind) { std::cout << i << " "; }

std::cout << std::endl;

return;

}

} while (std::next\_permutation(ind.begin(), ind.end()));

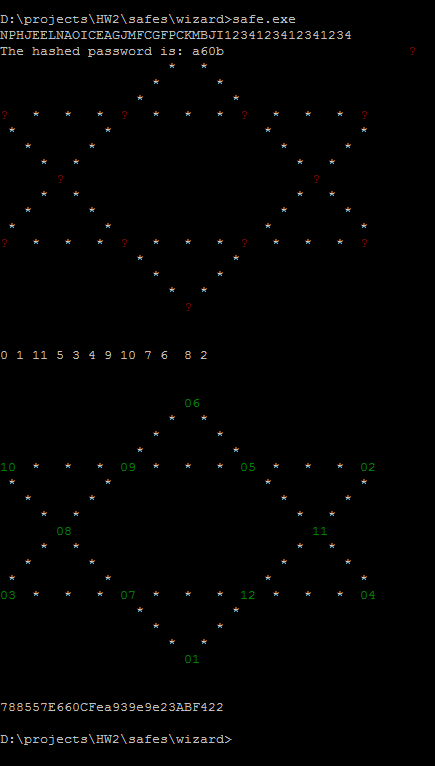
}

בעזרת הפונק' מצאנו את הקלט הנדרש "**0 1 11 5 3 4 9 10 7 6 8 2**"

לאחר הכנסת הקלט קיבלנו את המשך הפלט:

**The hashed password is: a60b788557E660CFea939e9e23ABF422**

**וציור של מגן דוד המכיל מספרים בקודקודיו:**



 **goblin**

איתרנו את פונק' ה- main של הקובץ safe.exe ע"פ כלל האצבע שהיא הקריאה האחרונה לפני הקריאות ל- cexit ול- ExitProcess. בפונקציית main יש קריאה לפונק אתחול ואחר מכן לולאה מרכזית עם 8 איטרציות.  
בפונק' האתחול, מאתחלים 3 משתנים a=0, b=7, c='L' ובנוסף מערך בגדול 64 בתים (arr64) בהמשך נראה שפונים למערך בצורה הבאה arr64[a\*8+b] לכן זהו מערך דו-מימדי.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | . | . | 7 | F | . | 4 | . | . |
| 1 | X | X | X | X | X | X | X | X |
| 2 | . | . | . | . | . | . | . | . |
| 3 | X | X | X | X | X | X | X | X |
| 4 | F | . | . | . | . | . | . | . |
| 5 | 2 | . | . | . | . | . | . | . |
| 6 | X | X | X | X | X | X | X | X |
| 7 | . | 3 | . | . | . | . | . | . |

לאחר מכאן חיפשנו איפה התוכנית מקבלת קלטים בעזרת הלשונית Imports וראינו שיש 2 קריאות לscanf בתוך אותה הפונק' סימנו אותה func\_with\_scanf. היא מקבלת מstdin קלט הראשון בפורמט "%c". הקלט חייב להיות אחד מהתוים: C,D,U אחרת התוכנית מסתיימת. אם הקלט הראשון היה C אז ממשיכים לשני גם בפורמט "%c", הקלט השני חייב להיות תו המייצג ספרה 0-9 אחרת התוכנית מסתיימת. את התו השני ממירים לערך שהוא מייצג (ספרה integer). שני הקלטים מוחזרים בעזרת שני ארגומנטים שהפונ' קיבלה (מצביעים כפולים).

חזרנו לנתח את main, בכל אחת מהאיטרציות של main מתבצעים השלבים הבאים:

1. קריאה לפונק' func\_with\_scanf . ובדיקת הקלט הראשון: 🡪 🡨 ← ⬆ ↓⇓
   1. אם הקלט הראשון היה 'C' מבצעים סריקה של המערך arr64[a\*8+b] לפי החוקיות הבאה:

start

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | ⇓ | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 |
| 1 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | ⇓ |
| 2 | ⇓ | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 |
| 3 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | ⇓ |
| 4 | ⇓ | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 |
| 5 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | ⇓ |
| 6 | ⇓ | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 | 🡨 |
| 7 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | 🡪 | ⇓ |

* + 1. מספר הצעדים בסריקה הוא לפי הקלט השני.
    2. אם מגיעים לאחד הקצוות של השורה, יורדים שורה וכיוון הסריקה מתהפך.
    3. אם נוחתים על X התוכנית מסתיימת
    4. סופרים את מספר הפעמים שעברנו דרך F
  1. אם הקלט הראשון הוא U קופצים מספר שורות למעלה לפי הערך הנוכחי של arr64[a\*8+b].
  2. אם הקלט הראשון הוא D קופצים מספר שורות למטה לפי הערך הנוכחי של arr64[a\*8+b].

1. אם a==7 ו- b==7 כלומר הגענו לפינה ימנית תחתונה ואם עברנו פעמיים דרך F אז הלולאה מסתיימת ומודפס הפלט עם התשובה למסך.
2. אם לא סיימנו את הסעיף הקודם תוך 8 איטרציות, התוכנית מסתיימת.

הרצנו את safe.exe ועם הקלט הבא:

C 5

U

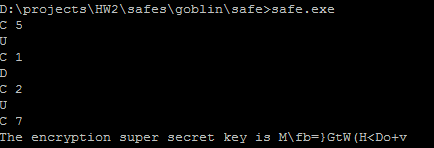
C 1

D

C 2

U

C 7



**חלק ב' - decrypt.exe**

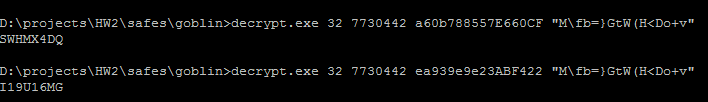
לאחר שיש בידינו את הקלטים הנדרשים ל decrypt:

* The encryption params are 32 (rounds) and 7730442 (delta)
* The hashed password is: a60b788557E660CFea939e9e23ABF422
* The encryption super secret key is M\fb=}GtW(H<Do+v

ביצענו ניתוח סטטי של decrypt.exe כדי להבין איך להשתמש בקלטים.

1. בפונק' main בודקים את מספר הארגומנטים שהתוכנית מקבלת וצריך שיהיו בדיוק 4 ארגומנטים.
2. ארגומנט 4 – צריך להיות בגודל 16 בתים אחרת מודפסת ההודעה: "Error: Key must be 128 bits in length." לכן הבנו שהוא ה – key.
3. ארגומנטים 1,2 מומרים למספרים לכן הם הפרמטרים.
4. ארגומנט 3 (הסיסמה) צריכה להיות באורך זוגי, ומתייחסים רק לחצי הראשון של הססמה.

הרצנו את ה decrypt.exeפעמיים ובכל פעם הצגנו לה חצי מהסיסמה.



איחדנו בחזרה את הסיסמה שקיבלנו : **SWHMX4DQI19U16MG** ופתחנו בעזרתה את הכספת ה משותפת. בתוך הכספת מצאנו שני קבצים:

* codes.pdf – מסביר איך אפשר להפוך אריח.
* sheep.jpg – קובץ תמונה, בדקנו אותה בעזרת analyzer.exe והתקבל הקובץ sheep.out.

פתחנו את sheep.out לעריכה בעזרת notpad וראינו שהוא מתחיל ב-"MZ" מה משעיד שהוא מכיל תוכנית מקומפלת. שינינו את השם שלו ל- sheep.exe ופתחנו אותו לניתוח בעזרת ida .