Write Up Elad Fisher

המטרה בתרגיל זה היא להכניס קוד שמקפיץ תיבת טקסט עם השם שלי.

כדי לעשות את זה אני אסתכל בקובץ עם התוכנה ואני רואה שבאזור שמריץ את התיבה המקורית אפשר להכניס קוד משלי, בשביל זה אני אכניס במקום הקריאה לפונקציה הראשונה קפיצה לקוד שלי, ואחרי הקוד שלי אני אחזור עם קפיצה לאיפה שהקוד היה. כדי לפצפץ' אני אזריק את הקוד שלי בחלק שמלא בפקודות nop שבצורה מאוד נוחה מישהו סידר לי שאני אוכל לסדר דברים, דבר ראשון אני אעתיק את השורת קוד שנמצאת אחרי הכל שהיא קפיצה ללפני:

```
004010A4   5E                 pop esi                                esi:EntryPoint
004010A5   FF35 0C634000      push dword ptr ds:[40630C]
004010AB   E8 69050000        call injectme.401619
004010B0   E8 1E040000        call injectme.4014D3
004010B5   E9 16040000        jmp <injectme.codeContinue>
004010BA   90                 nop
```

ככה עכשיו יש לי מלק פקודות NOPשלא עושות כלום ולא ירוצו.

לכן אני אכניס את הפקודה שהייתה וחזרה לקוד המקורי לפני שאני משנה עוד דברים:

```
0040114C   90                 nop
0040114D   90                 nop
0040114E   90                 nop
0040114F   90                 nop
00401150   90                 nop
00401151   90                 nop
00401152   E8 7F040000        call <JMP.&InitCommonControls>
00401157   E9 A9FEFFFF        jmp <injectme.ogCode>
0040115C   90                 nop
0040115D   90                 nop
0040115E   90                 nop
0040115F   90                 nop
00401160   90                 nop
00401161   90                 nop
```

אפשר לראות לפי הכתובות שעשיתי את זה ממש למטה כי אני לא יודע בדיוק כמה שורות קוד אני אצטרך לעשות עוד.

כרגע לפני הכל אני מסתכל באתר של מייקרוסופט כדי לראות איך מעלים חלון ואני לפני הכל יודע שאני צריך מחרוזת אחת לפחות של טקסט להעלות אז אני משתמש בזיכרון שאחרי החזרה לקוד המקורי:

```
00401164   90                 nop
00401165   90                 nop
00401166   90                 nop
00401167   49                 dec ecx                                message
00401168   6E                 outsb
00401169   6A 65              push 65
0040116B   637465 64          arpl word ptr ss:[ebp+64],si
0040116F   2062 79            and byte ptr ds:[edx+79],ah            edx+79:&L"systeminputhost-l1-2-0"
00401172   2045 6C            and byte ptr ss:[ebp+6C],al
00401175   61                 popad
00401176   64:2046 69         and byte ptr fs:[esi+69],al
0040117A   73 68              jae injectme.4011E4
0040117C   65:72 10           jb injectme.40118F
0040117F   0090 90909090      add byte ptr ds:[eax-6F6F6F70],dl
00401185   90                 nop
00401186   90                 nop
00401187   90                 nop
00401188   90                 nop
00401189   90                 nop
0040118A   90                 nop
0040118B   90                 nop
0040118C   90                 nop
0040118D   90                 nop
0040118E   90                 nop
0040118F   90                 nop
00401190   90                 nop
00401191   90                 nop

esi=<injectme.EntryPoint>

.text:004010A4 injectme.exe:$10A4 #4A4

Dump 1   Dump 2   Dump 3   Dump 4   Dump 5   צפה1   מקומיים   Struct

כתובת     Hex                                              ASCII
00401167  49 6E 6A 65 63 74 65 64 20 62 79 20 45 6C 61 64  Injected by Elad
00401177  20 46 69 73 68 65 72 10 00 90 90 90 90 90 90 90   Fisher.........
00401187  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00401197  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
004011A7  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
004011B7  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
004011C7  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
004011D7  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
004011E7  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
004011F7  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00401207  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00401217  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00401227  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00401237  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00401247  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00401257  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00401267  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90

פקודה:
```

ניתן לראות את המחרוזת שבחרתי להכניס למטה בעמוד. (injected by Elad Fisher) אבל אני מכניס את זה באזור של הקוד במקום ה NOP's שאני לא צריך. את העריכה עושים תו תו ולכן נחמד שיש לנו את הדבר הנפלא שנקרא טבלת אסקיי.

אחרי שעשינו את כל ההכנה הזאת כולל הקפיצה והחזרה צריך רק לקרוא לתיבת הטקסט עצמה, על פי הMSDN זה הצורה של קריאה לתיבת טקסט:

Syntax

C++ Copy

```
int MessageBox(
  [in, optional] HWND    hWnd,
  [in, optional] LPCTSTR lpText,
  [in, optional] LPCTSTR lpCaption,
  [in]           UINT    uType
);
```

כמובן שאני קראתי את התיעוד שנוסף שיש ולכן אני יודע שאני אדחוף 2 כתובות של טקסט ואני במקרה אדחוף את אותה מחרוזת שתהיה גם בכותרת וגם בתוכן. את הכפתורים וההנדל אני מתכוון לשים 0 בתור דיפולט אופציונלי....

את המיקום של הפונקציה לקחתי בעזרת הקריאה שיש בקוד המקורי....

```
004010C2   90                 nop
004010C3   90                 nop
004010C4   90                 nop
004010C5   90                 nop
004010C6   90                 nop
004010C7   90                 nop
004010C8   90                 nop
004010C9   90                 nop                                  inject
004010CA   90                 nop
004010CB   90                 nop
004010CC   90                 nop
004010CD   6A 00              push 0
004010CF   68 67114000        push <injectme.message>
004010D4   68 67114000        push <injectme.message>
004010D9   6A 00              push 0
004010DB   90                 nop
004010DC   90                 nop
004010DD   90                 nop
004010DE   90                 nop
004010DF   90                 nop
004010E0   90                 nop
004010E1   90                 nop
004010E2   90                 nop
004010E3   90                 nop
004010E4   E8 AB040000        call <JMP.&MessageBoxA>
004010E9   90                 nop
004010EA   90                 nop
004010EB   90                 nop
004010EC   90                 nop
004010ED   90                 nop
```

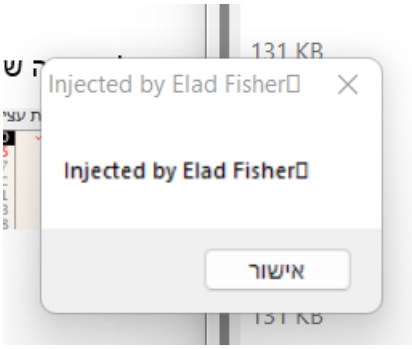
והנה יש את הקריאה לפונקציה שמדפיסה עם הדחיפות של הנתונים (התווית message זה המסר שלי) וככה אני סידרתי את הקובץ

נשאר רק לקפוץ לתווית inject מהתוכנית בעזרת דריסה של השורה ששחזרנו אחרי:

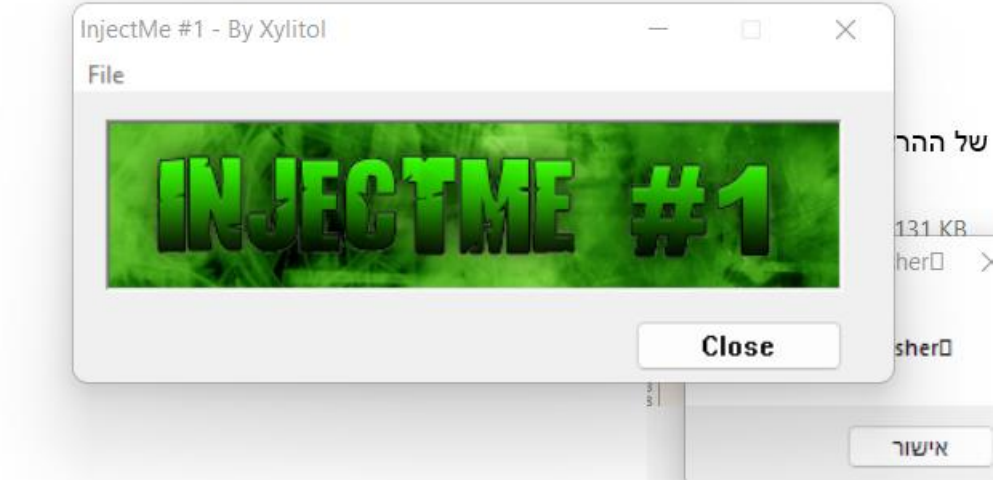
```
CPU   Log   הערות   נקודת עצירה   Memory Map   Call Stack   SEH   סקריפט   סמלים   מקור
EIP ECX EDX ESI EDI
00401000   E9 C4000000   jmp <injectme.inject>                EntryPoint
00401005   6A 00         push 0                               ogCode
00401007   E8 A6050000   call <JMP.&GetModuleHandleA>
0040100C   A3 00614000   mov dword ptr ds:[406100],eax
00401011   6A 00         push 0
00401013   68 30104000   push injectme.401030
00401018   6A 00         push 0
```

וככה הכנסנו קוד משלנו לתוך הקובץ שלהם, יאיי!

דומה של ההרצה והתיבה שתיפתח:



ואז יופיע התיבה המקורית אחרי שנלחץ על אישור.



הסוף!