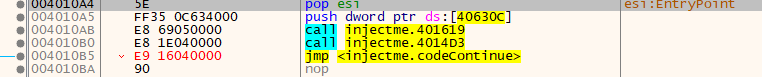
Write Up Elad Fisher

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:



ככה עכשיו יש לי מלק פקודות NOP שלא עושות כלום ולא ירוצו.

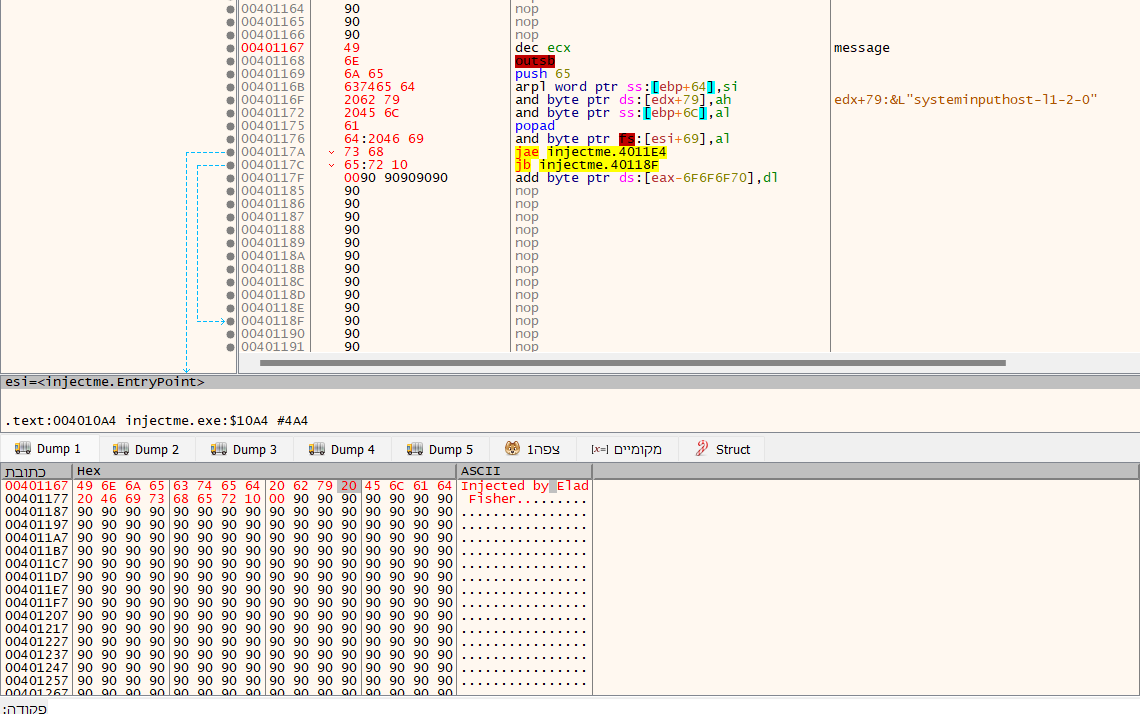
לכן אני אכניס את הפקודה שהייתה וחזרה לקוד המקורי לפני שאני משנה עוד דברים:

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי

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:



ניתן לראות את המחרוזת שבחרתי להכניס למטה בעמוד. (injected by Elad Fisher) אבל אני מכניס את זה באזור של הקוד במקום הNOP'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:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

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....

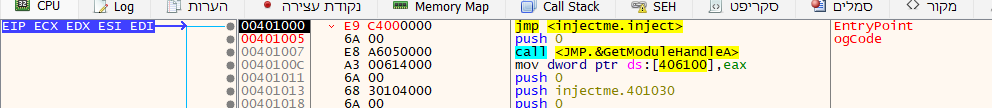
את המיקום של הפונקציה לקחתי בעזרת הקריאה שיש בקוד המקורי....

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

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:



וככה הכנסנו קוד משלנו לתוך הקובץ שלהם, יאיי!

דומה של ההרצה והתיבה שתיפתח:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

ואז יופיע התיבה המקורית אחרי שנלחץ על אישור.

תמונה שמכילה טקסט, שעון, צילום מסך

התיאור נוצר באופן אוטומטי

הסוף!