פיתוח shellcode

בתרגיל זה נפתח shellcode אשר ידפיס למסך את השנה הנוכחית. יכולת קבלת תאריך/שעה חשובות ביותר עבור פיתוח נוזקות שכן חלקן פועל רק בטווח זמן נתון. כדי לקבל את הזמן הנוכחי נשתמש בפונקציית הספרייה הבאה:

```
NTSTATUS NtQuerySystemTime(PLARGE_INTEGER SystemTime);
```

הפונקציה מקבלת פרמטר בודד – מצביע לחתיכת זיכרון בגודל 8 בית. בזיכרון זה הפונקציה שומרת מספר X כך ש-X כפול 100 הוא מספר הננו-שניות שעברו מאז החצות של ה-1 בינואר 1601 (ברצועת זמן 0). ניתן לקרוא עוד על הפונקציה הזו בקישור הבא:

https://docs.microsoft.com/en-us/windows/win32/api/winternl/nf-winternl-ntquerysystemtime

לאחר חישוב השנה הנוכחית, יש להדפיסה באמצעות קריאה לפונקציה printf עם התבנית "%d". שימו לב כי מיקום הפונקציה printf קבוע.

ה-shellcode אשר אתם מפתחים צריך לעבוד כראוי גם במחשב אחר/אחרי הפעלה מחדש, כלומר הוא צריך להיות חסין ASLR.

דגשים:

1. חשוב לציין, ש<u>בשונה</u> מהפונקציה WinExec אשר שייכת ל-kernel32.dll, הפונקציה שלנו שייכת ל-ntdll.dll. נזכיר, כי סדר הDLLים ברשימה שמוצבעת ע"י הPEB הוא:

demo.exe → ntdll.dll → kernel32.dll

1. הפונקציות ב-ntdll.dll משחררות את הפרמטרים מהמחסנית בעצמן. כלומר, אין צורך לבצע את ההוראה ADD ESP, 4 אחרי הקריאה לפונקציה שלנו.
2. כדי לחלק מספר במספר יש לטעון את המחולק לאוגרים EDX ו-EAX ואת המחלק לאוגר כלשהו, נניח ECX. לאחר מכן יש לבצע את ההוראה DIV ECX. שימו לב כי ההוראה DIV שומרת באוגר EDX את שארית החלוקה. כדי לאפס את האוגר EDX ניתן לבצע את ההוראה XOR EDX,EDX.
3. כדי לתרגם את המספר X אשר מוחזר ע"י הפונקציה שלנו לשנה הנוכחית, נחלק תחילה את X ב-600000000 (8 אפסים), את התוצאה נחלק ב-525600 (=60*24*365) ולבסוף נוסיף 1601.
4. במידה וההוראה אשר טוענת מספר/כתובת לאוגר מכילה אפסים, ניתן להיעזר בהוראות bswap,inc,dec או בטעינה רק לחלקו התחתון של האוגר.