**Міністерство освіти і науки України**

**Національний технічний університет України**

**«Київський політехнічний інститут імені Ігоря Сікорського»**

**Факультет інформатики та обчислювальної техніки**

**Кафедра обчислювальної техніки**

**Лабораторна робота № 3**

з дисципліни

«Системне програмування»

на тему

“Дослідження структури програм формату EXE”

Виконав:

Перевірив:

студент групи ІМ-22 доцент

Куц Іван Васильович Павлов В.Г.

Номер у списку групи: 12

номер залікової книжки: 9017

**Київ 2024**

**Мета:** Ознайомлення із специфікацією COFF (Common Object File

Format). Вивчення прийомів дослідження структури файлів PE-

формату.

**Інтерфейс програми**

Зображення, що містить текст, знімок екрана, Шрифт

Автоматично згенерований опис

Мал. 1. Вікно з полем для введення даних

Зображення, що містить текст, знімок екрана, монітор, мультимедіа

Автоматично згенерований опис

Мал. 2. Інформаційне вікно, яке сповіщає про неправильно введений пароль

Зображення, що містить текст, знімок екрана, Шрифт

Автоматично згенерований опис

Мал. 3. Інформаційне вікно, яке сповіщає про правильно введений пароль та дані студента

Дослідження файлу в HIEW32

Зображення, що містить електроніка, монітор, знімок екрана, комп’ютер

Автоматично згенерований опис

Зображення, що містить текст, монітор, знімок екрана, комп’ютер

Автоматично згенерований опис

Зображення, що містить знімок екрана, текст, програмне забезпечення, монітор

Автоматично згенерований опис

На першому скріншоті показано DOS Header та PE Header, DOS Header займає 64 байти

Зображення, що містить текст, знімок екрана, число, Шрифт

Автоматично згенерований опис

Скористаємося даною діаграмою для дослідження характеристик файлу

Спершу знайдемо адресу сигнатури (0x5045)

Зображення, що містить знімок екрана, комп’ютер, монітор, текст

Автоматично згенерований опис



Після чого, скориставшись діаграмою, перейдемо до пошуку характеристик

Таблиця параметрів файлу

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Значення | Опис поля | Опис значення поля |
| Machine type | 4C 01 | Тип машини (CPU) | Intel 386 або пізніша, та інші схожі процесори |
| Optional Header Standard Fields | | | |
| Magic | 0B01 | Число типу unsigned integer, що ідентифікує стан файлу | Ідентифікатор нормального файлу типу .ехе |
| Major linker version | 0E | Номер версії основного лінкера | |
| Minor linker version | 00 | Номер версії меншого лінкера | |
| Size Of Code | 00040000 | Розмір секції коду | |
| Size Of Initialized Data | 00060000 | Розмір секції ініціалізованих змінних | |
| Size Of Initialized Data | 00000000 | Розмір секції неініціалізованих змінних | |
| Address Of Entry Point | A5100000 | Адреса вхідної точки в програму, початкова адреса програми | |
| Base Of Code | 00 10 00 00 | Адреса початку секції коду при завантаженні в пам’ять | |
| Base Of Data | 00 20 00 00 | Адреса початку секції змінних при завантаженні в пам’ять | |
| Optional Header Windows NT-Specific fields | | | |
| Image Base | 00 00 40 00 | Адреса першого байту при завантаженні в пам`ять | |
| SectionAlignment | 00 10 00 00 | Вирівнювання (в байтах) розділів при завантаженні в пам'ять | |
| FileAlignment | 00 02 00 00 | Коефіцієнт вирівнювання (у байтах), який використовується для вирівнювання необроблених даних розділів у файлі зображення | |
| MajorOperatingSystem Version | 06 00 | Номер основної версії необхідної ОС | |
| MinorOperatingSystem Version | 00 00 | Номер другорядної версії необхідної ОС | |
| MajorImageVersion | 00 00 | Номер основної версії образу | |
| MinorImageVersion | 00 00 | Номер другорядної версії образу | |
| MajorSubsystemVersion | 06 00 | Номер основної версії підсистеми | |
| MinorSubsystemVersion | 00 00 | Номер другорядної версії підсистеми | |
| SizeOfImage | 00 50 00 00 | Розмір образу в байтах, включаючи всі заголовки | |
| SizeOfHeaders | 00 04 00 00 | Комбінований розмір заглушки MS-DOS, заголовка PE та заголовків розділів, округлених до кратного FileAlignment | |
| CheckSum | 00 00 00 00 | Контрольна сума файлу образу | |
| Subsystem | 03 00 | Підсистема, потрібна для запуску цього образу | |
| DLL Characteristics | 40 81 |  | |
| SizeOfStackReserve | 00 00 10 00 | Розмір стеку для резервування | |
| SizeOfStackCommit | 00 10 00 00 | Розмір стека для фіксації | |
| SizeOfHeapReserve | 00 00 10 00 | Розмір локальної купи для резервування | |
| SizeOfHeapCommit | 00 10 00 00 | Розмір локальної купи для фіксації | |
| LoaderFlags | 00 00 00 00 |  | |
| NumberOfRvaAndSizes | 10 00 00 00 | Кількість записів словника даних у решті необов’язкового заголовка. Кожен описує розташування та розмір. | |
| Virtual Size | 2E 74 65 78 | Розмір секції, завантаженої в пам’ять | |
| Virtual Address | 74 00 00 00 | Адреса першого байту секції | |
| Size Of Raw  Data | 98 02 00 00 | Розмір секції | |
| Pointer To  Relocations | 00 04 00 00 | Пойнтер до початку входжень релокацій в секцію (для файлів .ехе рівний 0) | |
| Number Of  Relocations | 00 00 | Кількість релокаційних входжень в секцію (для файлів .ехе рівний 0) | |
| Characteristics | 00 00 00 00 | Прапори опису характеристики секції | |

Дослідження в PE Editor

Зображення, що містить текст, знімок екрана, число, Шрифт

Автоматично згенерований опис

Зображення, що містить текст, Шрифт, число, ряд

Автоматично згенерований опис

Зображення, що містить текст, знімок екрана, число, Шрифт

Автоматично згенерований опис

Зображення, що містить текст, знімок екрана, монітор, Шрифт

Автоматично згенерований опис

Таблиці імпорту

У даній програмі використовувалося дві бібліотеки, нижче можемо побачити, список функцій з цих бібліотек, які були використані у програмі

user32.dll

Зображення, що містить текст, знімок екрана, програмне забезпечення, монітор

Автоматично згенерований опис

kernel32.dll

Зображення, що містить текст, знімок екрана, монітор, число

Автоматично згенерований опис

За Зараз наш пароль можна напряму побачити у коді

Зображення, що містить текст, знімок екрана, програмне забезпечення, монітор

Автоматично згенерований опис

Щоб запобігти цьому зашифруємо пароль за допомогою операції XOR, оберемо якийсь ключ, наприклад,

1234qw

A XOR 1 = p

A XOR 2 = a

S XOR 3 = `

M XOR 4 = y

3 XOR q = B

2 XOR w = E

Отриманий пароль – pa`yBE

Створимо нову програму, модифікуємо код та знайдемо зашифрований пароль у програмному коді

HEX режим

Зображення, що містить електроніка, текст, знімок екрана, комп’ютер

Автоматично згенерований опис

Текстовий режим Зображення, що містить текст, електроніка, знімок екрана, комп’ютер

Автоматично згенерований опис

**Висновок**

У даній лабораторній роботі я дослідив структура .EXE файлу, те що він складається з кількох секцій (DOS header, PE header І section headers), я написав 2 програми, в одній з яких провів шифрування паролю, хоч це й далеко недосконале шифрування, адже студент, який не прогулював пари з “Системного програмування” з легкістю зможе його розшифрувати