

Міністерство освіти і науки України
Національний університет «Запорізька політехніка»

кафедра програмних засобів

ЗВІТ

з лабораторної роботи № 7

з дисципліни «Безпека та захист програм і даних» на тему:

**«ЗАХИСТ ПРОГРАМ ЗА ДОПОМОГОЮ ПРОГРАМ-
ПАКУВАЛЬНИКІВ»**

Виконав:

ст. гр. КНТ-113сп

Іван ЩЕДРОВСЬКИЙ

Прийняв:

доцент

Тетяна ЗАЙКО

1 Мета роботи

Дослідити роботу основних програм для захисту виконуваних файлів шляхом пакування. Ознайомитись на практиці з програмами для ідентифікації пакування. Дослідити програми-розпакувальники, які використовуються зламниками для зняття захистів

2 Завдання до лабораторної роботи

Навчитись використовувати базові функції запропонованих програм, і заповнити таблицю характеристик

3 Відповіді на контрольні питання

В чому різниця між архіваторами та пакувальниками?

Пакувальник це спеціалізований архіватор, що створює виконувані файли програм. При запуску такі програми автоматично розпаковуються

Який принцип дії програм-пакувальників?

Основний код програми посегментно запаковується тим чи іншим методом, а потім в початок додається процедура його розпакування перед виконанням

Які позитивні і негативні риси пакувальників?

Позитивні:

Програма повністю працює та займає менше місця

Програма більш захищена від не досвідченого хакера

Програма більш захищена від вірусу, оскільки її внутрішній код недоступний для модифікації вірусом

Недоліки:

Більший час завантаження, оскільки програма повинна ще розпакувати себе

Процедура розпакування займає пам'ять

Після розпакування програма завжди робить запит на нову пам'ять для своєї роботи, розмір якої завжди буде більший, ніж початково виділений даному процесу

Назвіть декілька програм для пакування виконуваних файлів

UPX, MPRESS, ASM Guard

Наведіть приклади програм для ідентифікації пакування файлів. Яке їх призначення?

Detect It Easy, PEId

Їх призначення визначити чи програма була запакована і якщо так, то яким інструментом

Яке програмне забезпечення виконує злам програмних продуктів, захищених пакувальниками?

Розпакувальники

Назвіть основні методи, що їх використовують розпакувальники

Це може бути виконання дій, протилежних до пакувальника. В такому випадку ми отримуємо програму, яка точно відповідає програмі до пакування. Але тут є недолік, оскільки розпакувальний прив'язаний до пакувальника та навіть до його версії

Другий підхід це трасування. Програма запускається та в режимі відлагодження і трасувальник намагається «засікти» той момент, коли розпаковка програми закінчилась і їх буде передане керування

4 Короткі відомості

Для виконання завдання потрібно підготувати три програми

Перша це виконуваний файл консольної програми малого розміру. Для цього було створено проєкт в Visual Studio 2022 з Hello world на C++.

Друга це виконуваний файл API-додатку під Windows. Для цього було створено проєкт Windows Desktop Application з Hello world

Третя це виконуваний файл MFC-додатку під Windows. Для цього було створено проєкт MFC App

Далі для кожного проєкту було взято виконуваний exe файл

Для виконання роботи було взято чотири пакери

Перший це «UPX, Ultimate Packer for eXecutables, 5.0.2». UPX вміє стискати виконувані файли, запаковувати файл без зовнішніх бібліотек, коли розпакування відбувається під час запуску програми. UPX не призначений для захисту від реверс-інжинірингу, а також деякі антивіруси можуть реагувати на нього

Другий «Alternate EXE Packer, 2.740, uses UPX». Цей застосунок використовує UPX 5.0.0, тому фактично має всі такі самі характеристики, як і UPX, але з GUI

Третій «Mpress 2.19». MPRESS вміє пакувати exe та dll файли, підтримує 32 та 64 біти, також має автоматичне розпакування і не потребує зовнішніх DLL або рантаймів. MPress не призначений для захисту від реверс-інжинірингу, а також може стискати менше, а ніж UPX в деяких випадках.

Четвертий «ASM Guard 2.9.4». Це не тільки пакувальник, а також протекторм коду. Він вміє додавати фейкові функції C++, додавати фейковий імпорт WinAPI, додавати «сміттєві» секції/розділи і приховані повідомлення, і також має імітацію виявлення як UPX в деяких сканерах. Але, звичайно, він не гарантує повної безпеки

Було взяти тільки 4 пакери замість 5-ти по завданню, оскільки всі інші пакери або не працюють на Windows 11 64bit, або ж мають віруси, або ж не правильно кодували файл, через що його не можна було запустити. Також є деякі пакери, які я не зміг знайти

В процесі пошуку пакерів було перевірено: ByteBoozer, ByteBoozer2, PEzor, squishy, UPXxShell, ерарк та aspack, але кожен з них мав проблеми

Спочатку було виконано пакування exe файлу з використанням оригінального UPX, а також виконано розпакування. Це показано на рисунку 4.1 та 4.1

```
C:\home\university-4\security\lb7\programs\upx-5.0.2-win64\upx-5.0.2-win64>upx -o ..\..\small-console-app-upx.exe ..\..\small-console-app.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2025
UPX 5.0.2      Markus Oberhumer, Laszlo Molnar & John Reiser   Jul 20th 2025

-----
File size      Ratio      Format      Name
-----
68608 ->      16384      23.88%      win64/pe      small-console-app-upx.exe

Packed 1 file.
```

Рисунок 4.1 – Пакування через UPX

```
C:\home\university-4\security\lb7\programs\upx-5.0.2-win64\upx-5.0.2-win64>upx -d -o ..\..\small-console-app-upx-d.exe ..\..\small-console-app-upx.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2025
UPX 5.0.2      Markus Oberhumer, Laszlo Molnar & John Reiser   Jul 20th 2025

-----
File size      Ratio      Format      Name
-----
68608 <-      16384      23.88%      win64/pe      small-console-app-upx-d.exe

Unpacked 1 file.
```

Рисунок 4.2 – Розпакування через UPX

Далі було виконано пакування та розпакування з використанням «Alternate EXE Packer (uses UPX 5.0.0)», це показано на рисунку 4.3

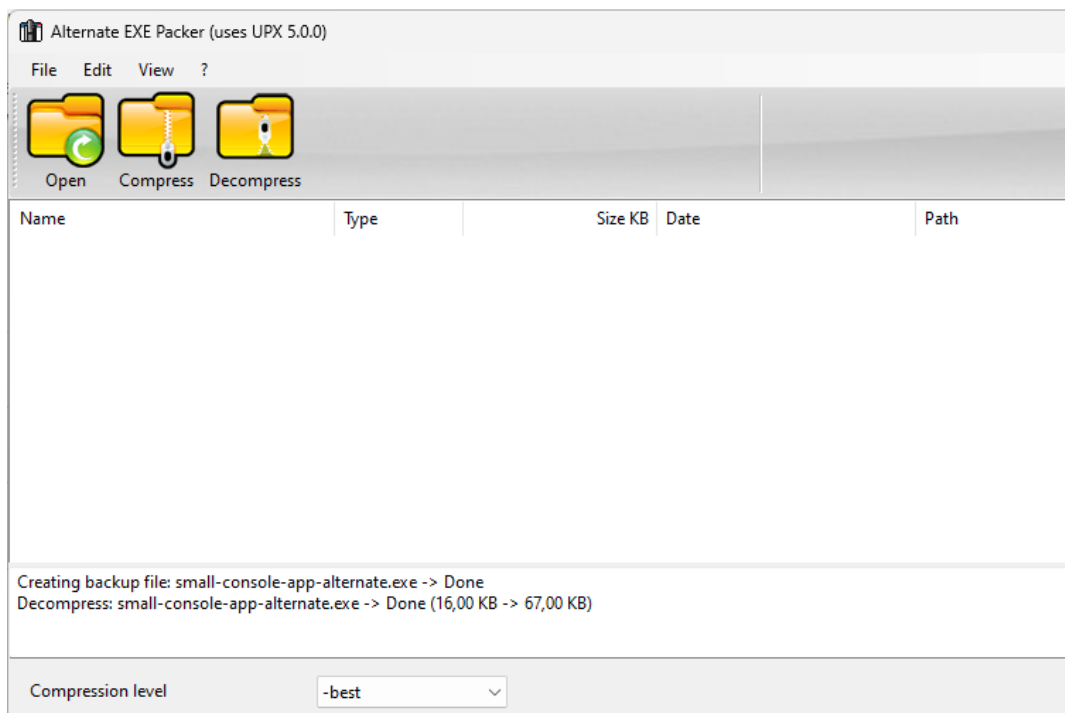


Рисунок 4.3 – Пакування з використанням Alternate EXE Packer

Наступним пакером було використано MPRESS, це показано на рисунку 4.4

```
C:\home\university-4\security\lb7\programs>mpress.exe ..\small-console-app.exe
```

```
    MATCODE compRESSor for executables
    Copyright (C) 2007-2012, MATCODE Software, MPRESS v2.19
```

```
<< small-console-app.exe >>
PE32+/x64 67.0kB |-> 16.0kB  Ratio: 23.8%
```

```
MPRESS: Warning! Module probably was already packed or modified by
some other tool.
```

Рисунок 4.4 – Пакування з використанням MPRESS

І останнім пакером було використано ASM Guard 2.9.4, це показано на рисунку

4.5

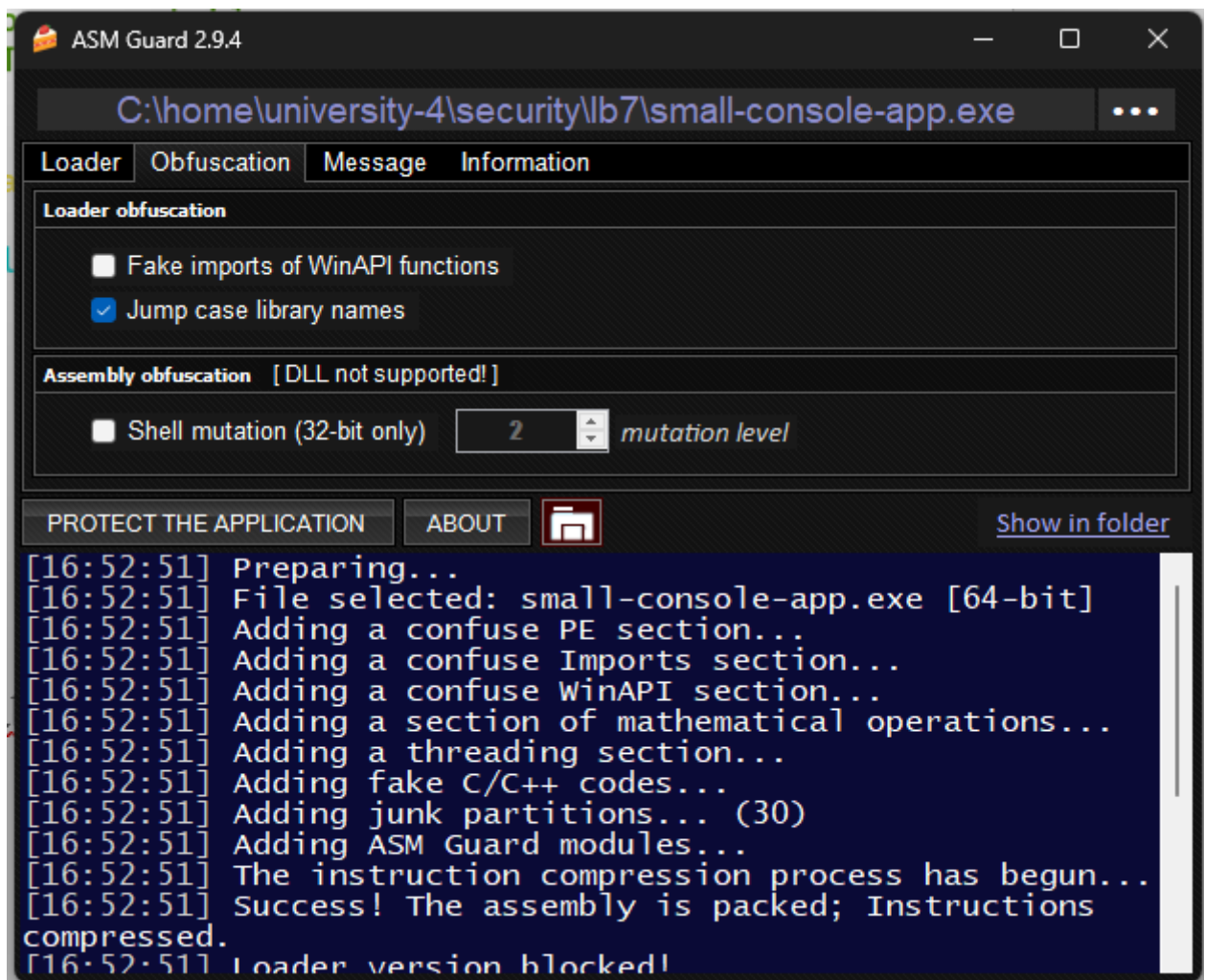


Рисунок 4.5 – Пакування з використанням ASM Guard

Таким самим чином було виконано пакування інших двох програм

Для ідентифікації було використано два ідентифікатора, а саме «PEId 0.95» та «DiE, Detect It Easy 3.10». Результати з PEId наводитись не будуть, оскільки в усіх програмах він нічого не знайшов, це показано на рисунку 4.6

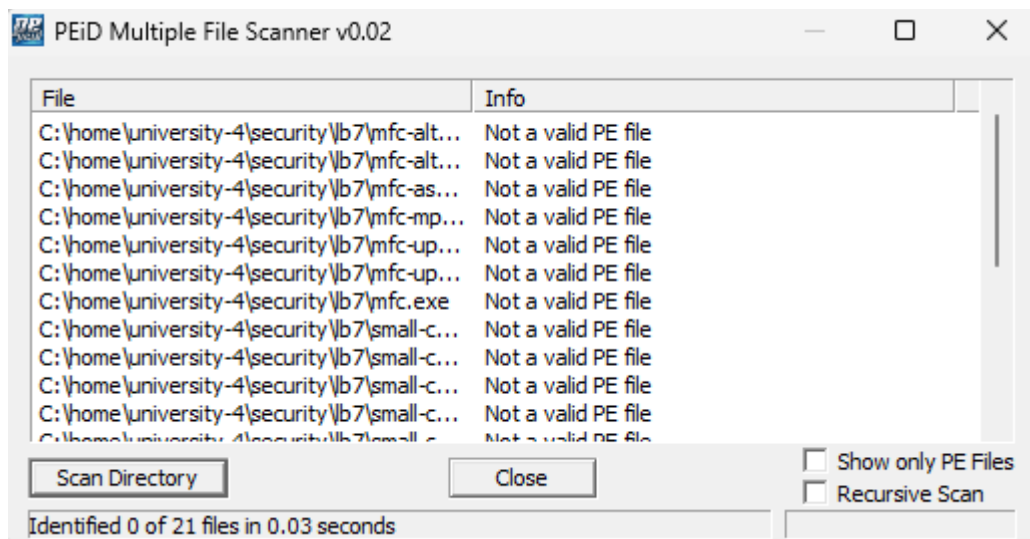


Рисунок 4.6 – Ідентифікація через PEiD

Тому далі використовується тільки DiE, приклад його використання показаний на рисунку 4.7

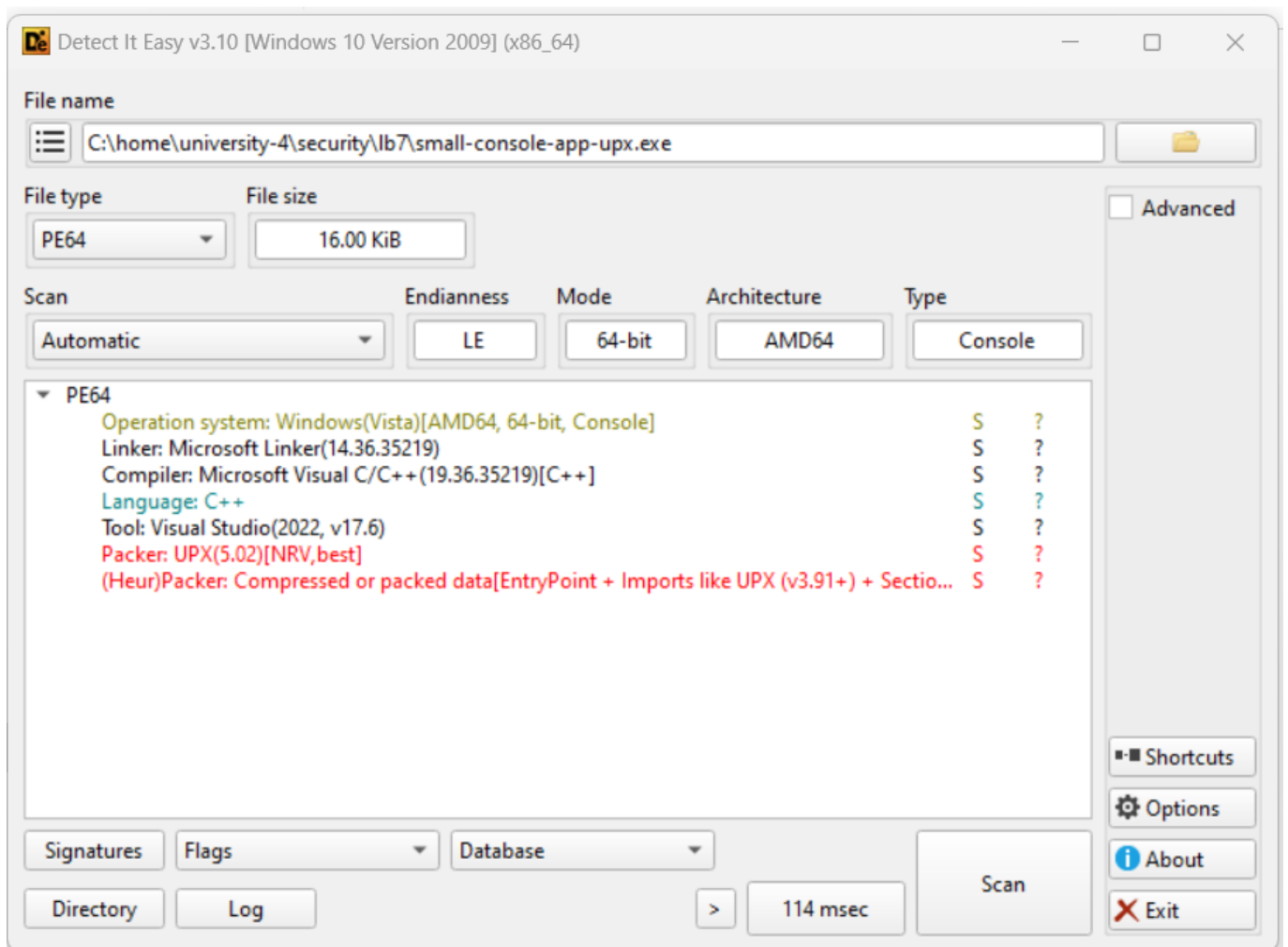


Рисунок 4.7 – Використання Detect It Easy 3.10

Також ця програма надає можливість сканування директорії, це показано на рисунку 4.8

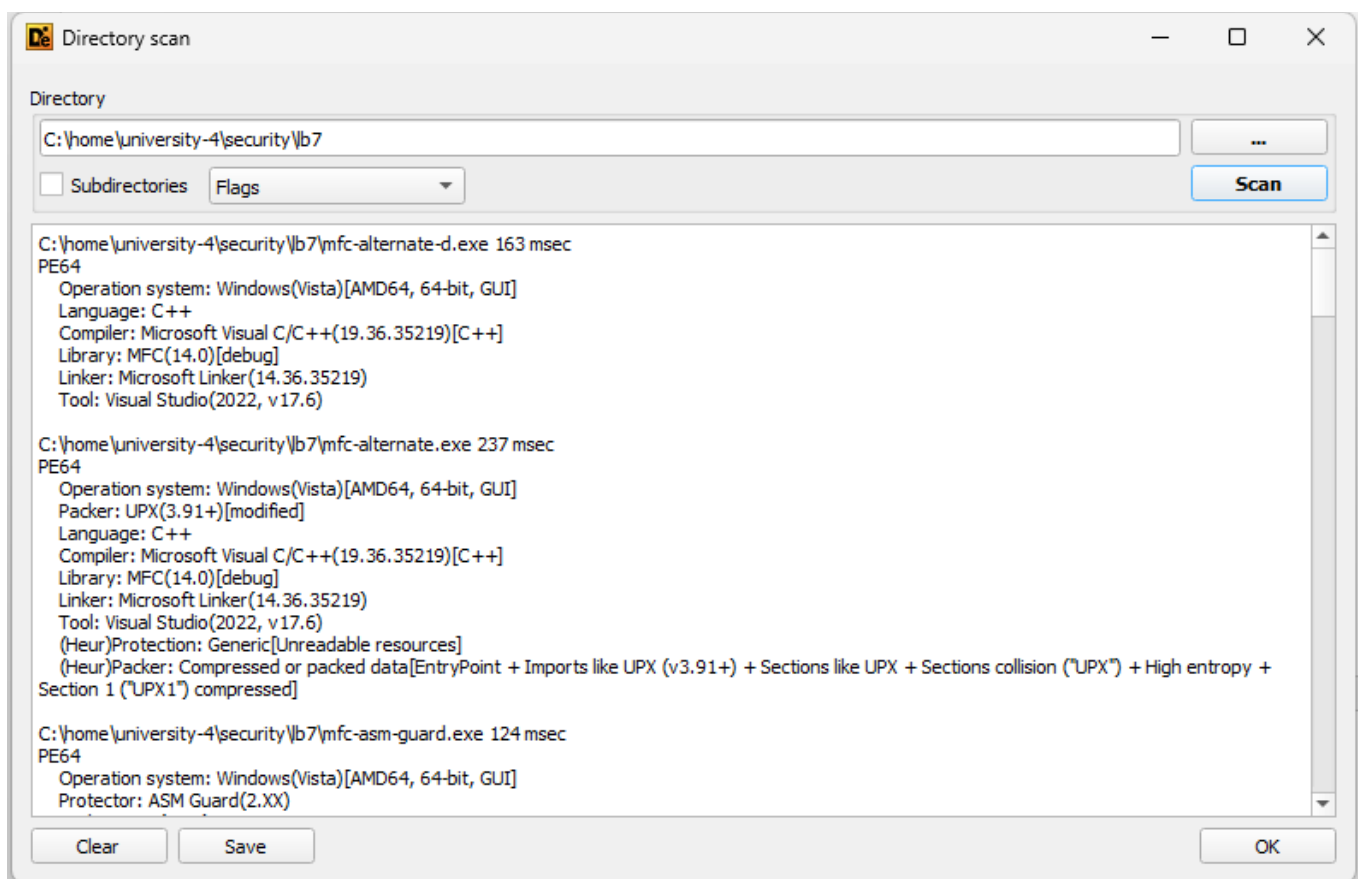


Рисунок 4.8 – Сканування директорії через Detect It Easy

5 Таблиця з результатами

Важливо зазначити, що описи пакерів були надані в попередньому блоці звіту, щоб уникнути дублювання тексту в таблиці

№	Назва програми та її обсяг	Пакувальник	Результати пакування		Результати ідентифікації	Розпакувальник	Результати розпакування	
			Обсяг %	Зменшення %			Обсяг %	Працює
1	2	3	5		6	7	8	
1	small-console-app.exe 67 kB	UPX 5.0.2	23.88% 16 kB	76.12 %	DiE ідентифікував імпорти, section 1 та sections і sections collision як UPX v3.91+	UPX 5.0.2	318% 67 kB	Так
2	small-console-app.exe, 67 kB	Alternate EXE Packer (uses UPX 5.0.0)	23.88% 16 kB	76.12 %	DiE ідентифікував імпорти, section 1 та sections і sections collision як UPX v3.91+	Alternate EXE Packer (uses UPX 5.0.0)	318% 67 kB	Так
3	small-console-app.exe, 67 kB	MPRESS v2.19	23.88% 16 kB	76.12 %	DiE ідентифікував імпорти та секції як MPRESS, а також секцію 0 як .MPRESS1	-	-	-
4	small-console-app.exe, 67 kB	ASM Guard 2.9.4	44.8%, 30 kB	55.2%	DiE ідентифікував імпорти як ASM Guard (v2.XX+)	-	-	-
5	windows-api.exe 175 kB	UPX 5.0.2	37.57% 68 kB	61.1%	DiE ідентифікував імпорти, section 1 та sections і sections collision як UPX v3.91+	UPX 5.0.2	175 kB	Так

6	windows-api.exe 175 kB	Alternate EXE Packer (uses UPX 5.0.0)	38.8%, 68 kB	61.1%	DiE ідентифікував імпорти, section 1 та sections і sections collision як UPX v3.91+	Alternate EXE Packer (uses UPX 5.0.0)	175 kB	Так
7	windows-api.exe 175 kB	MPRESS v2.19	61.7%, 108 kB	38.2%	DiE ідентифікував імпорти та секції як MPRESS, а також секцію 0 як .MPRESS1	-	-	-
8	windows-api.exe 175 kB	ASM Guard 2.9.4	45.7%, 80 kB	54.3%	DiE ідентифікував імпорти як ASM Guard (v2.XX+)	-	-	-
9	mfc.exe, 524 kB	UPX 5.0.2	31.6%, 166 kB	68.3%	DiE ідентифікував імпорти, section 1 та sections і sections collision як UPX v3.91+	UPX 5.0.2	524 kB	Так
10	mfc.exe, 524 kB	Alternate EXE Packer (uses UPX 5.0.0)	31.2%, 164 kB	68.7%	DiE ідентифікував імпорти, section 1 та sections і sections collision як UPX v3.91+	Alternate EXE Packer (uses UPX 5.0.0)	524 kB	Так
11	mfc.exe, 524 kB	MPRESS v2.19	30.7%, 161 kB	69.2%	DiE ідентифікував імпорти та секції як MPRESS, а також секцію 0 як .MPRESS1	-	-	-
12	mfc.exe, 524 kB	ASM Guard 2.9.4	33.2%, 174 kB	66.7%	DiE ідентифікував імпорти як ASM Guard (v2.XX+)	-	-	-

6 Висновки

Я ознайомився на практиці з основними програмними засобами, що використовуються зламниками для аналізу роботи захищеного програмного забезпечення. Навчився обирати програмні засоби для аналізу системи захисту програм