

Лабораторна робота №4

Захист від зміни бінарного файлу

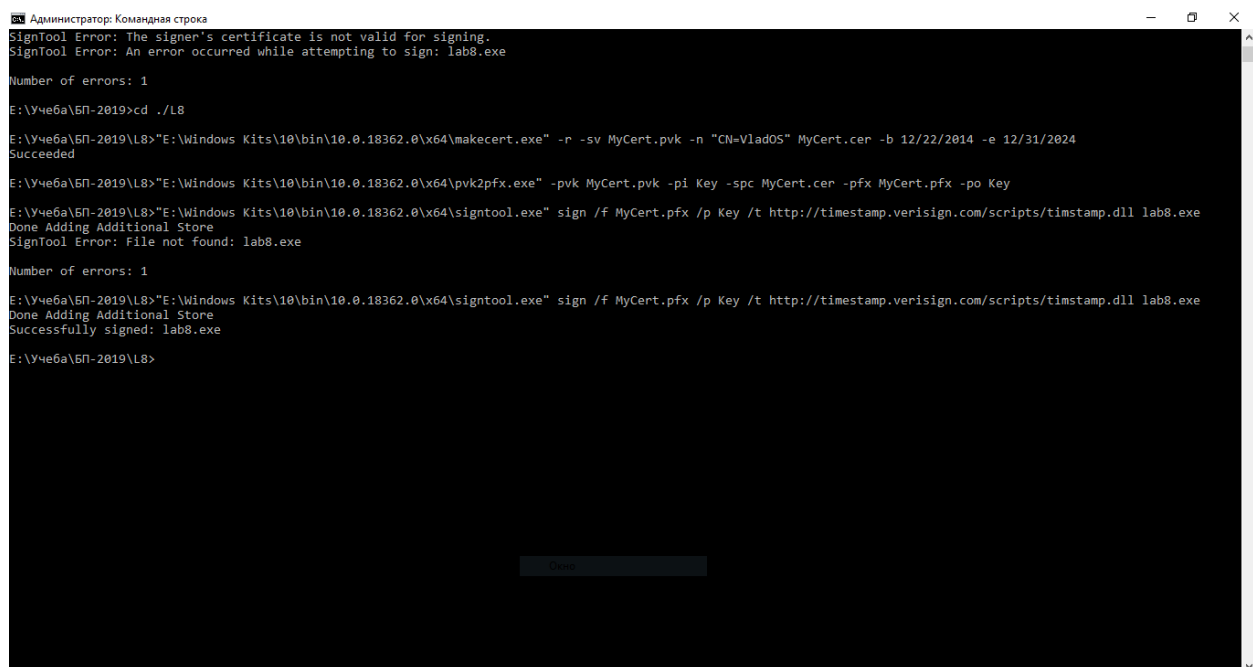
Мета: Навчитися підписувати виконувані файли.

Індивідуальне завдання:

Організувати підпис виконуваного файлу, написаного на мові С або С++ (і його верифікації на рівні коду) за допомогою утиліти SignTool.

Переконатися, що зміна підписаного файлу призводить до неможливості його виконання.

Створимо сертифікат і підпишемо будь яку програму.



```
Администратор: Командная строка
SignTool Error: The signer's certificate is not valid for signing.
SignTool Error: An error occurred while attempting to sign: lab8.exe

Number of errors: 1

E:\Учеба\БП-2019>cd ../L8

E:\Учеба\БП-2019\L8>"E:\Windows Kits\bin\10.0.18362.0\x64\makecert.exe" -r -sv MyCert.pvk -n "CN=VladOS" MyCert.cer -b 12/22/2014 -e 12/31/2024
Succeeded

E:\Учеба\БП-2019\L8>"E:\Windows Kits\bin\10.0.18362.0\x64\pvk2pfx.exe" -pvk MyCert.pvk -pi Key -spc MyCert.cer -pfx MyCert.pfx -po Key

E:\Учеба\БП-2019\L8>"E:\Windows Kits\bin\10.0.18362.0\x64\signtool.exe" sign /f MyCert.pfx /p Key /t http://timestamp.verisign.com/scripts/timestamp.dll lab8.exe
Done Adding Additional Store
SignTool Error: File not found: lab8.exe

Number of errors: 1

E:\Учеба\БП-2019\L8>"E:\Windows Kits\bin\10.0.18362.0\x64\signtool.exe" sign /f MyCert.pfx /p Key /t http://timestamp.verisign.com/scripts/timestamp.dll lab8.exe
Done Adding Additional Store
Successfully signed: lab8.exe

E:\Учеба\БП-2019\L8>
```

Рисунок 1 – Результат

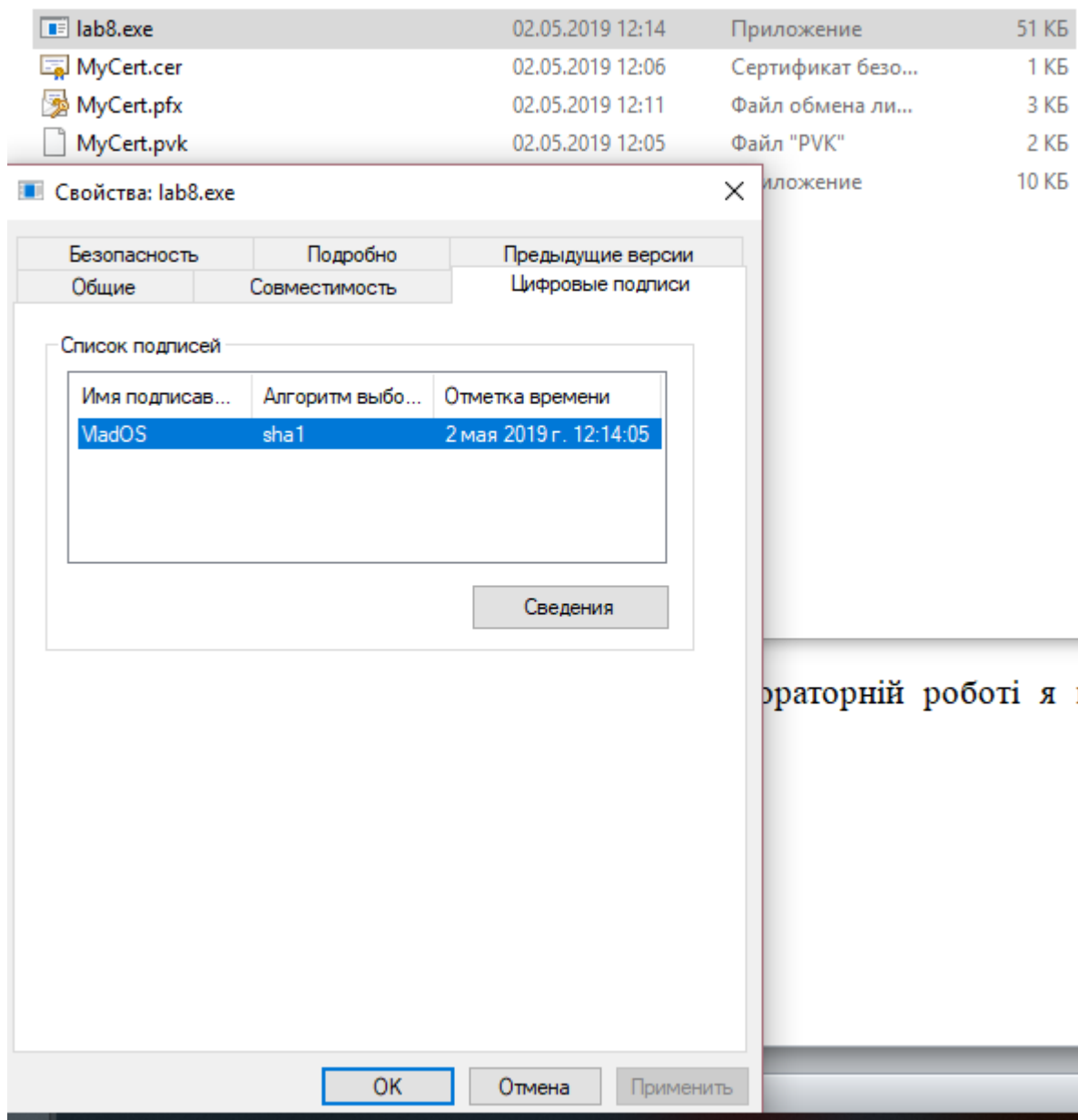


Рисунок 2 – Результат

Для простоти перевіримо на програмі написаній мовою Assembler. Підпишемо програму «vlad1.exe» тим же сертифікатом, а потім замінимо дані в налагоджувачі:

	Шестнадцатеричное																ASCII
0000	49	6E	70	75	74	20	70	61	73	73	77	6F	72	64	3A	2A	Input password:*
0010	2A	2A	2A	2A	2A	2A	2A	0A	00	4B	6F	76	61	6C	65		*****.Kovale
0020	6E	68	6F	00	C2	F8	20	E2	E2	E5	E8	E8	20	EA	EE	F0	nko.Au aaaaa eib
0030	F0	E5	EA	F2	ED	F8	E9	20	EF	E0	F0	EE	E8	FC	2E	20	0a00iue iadiu.
0040	CF	EE	E7	E4	F0	E0	E2	E8	FF	E5	EC	21	00	C2	F8	20	Iicadaaeyai!.Au
0050	E2	E2	E5	E8	E8	20	ED	E5	EF	F0	E0	E2	E8	E8	FC	ED	aaaae iai0aaeeui
0060	FB	E9	20	EF	E0	F0	EE	E8	FC	2E	00	0A	00	00	00	00	ue iadiu.....
0070	00	00	00	1A	00	00	00	00	00	00	00	00	00	00	00	00YeaiA
0080	ED	F2	E0	F0	ED	E0	FF	20	EA	EE	ED	F1	EE	E8	FC	ED	i0adiay einiueui
0090	E0	FF	20	EF	F0	EE	E3	F0	E0	EC	EC	E0	20	E2	E2	EE	ay i0iadaiaa aai
00A0	E4	E0	20	EF	E0	F0	EE	E8	FF	00	D0	E5	E7	F3	E8	FC	aa iadiu.0a00eu
00B0	F2	E0	F2	20	EF	F0	EE	E3	F0	E0	EC	EC	F8	00	00	00	0a0 i0iadaiaiu...
00C0	00	00	00	00	00	00	05	00	00	00	00	00	00	00	00	00
00D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Рисунок 3 – Було

Дамп 5		Просмотр 1		Структура		
ASCII						
73	77	6F	72	64	3A 2A	Input password:*
00	4B	6A	76	61	6C 65	*****.Kjvale
E5	E8	E8	20	EA	EE F0	nko.Âû ââââê êîð
E0	F0	EE	E8	FC	2E 20	ðâëðîüé îäîîü.
E5	EC	21	00	C2	FB 20	îîçäðââëÿâî!.Âû
F0	E0	E2	E8	E8	FC ED	ââââëë îäîðââëëüí
2E	00	0A	00	00	00 00	üé îäîîüü.....

Рисунок 4 – Стало

Зберігаємо зміни в файл lab2.exe. А тепер перевіримо цифрові підписи цих 2х програм:

```
D:\Windows Kits\10\bin\10.0.17763.0\x64>signtool verify /pa C:/lab1.exe
File: C:/Users/Index Algorithm Timestamp
*****
Successfully verified: C:/Users//Desktop/lab1.exe

D:\Windows Kits\10\bin\10.0.17763.0\x64>signtool verify /pa C:/lab2.exe
File: C:/Users/Index Algorithm Timestamp
*****
SignTool Error: WinVerifyTrust returned error: 0x80096010
.
Number of errors: 1
D:\Windows Kits\10\bin\10.0.17763.0\x64>
```

Рисунок 5 – Результат

Висновок: на цій лабораторній роботі навчилися підписувати виконувані файли.