



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ

СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

## **Технічний аудит**

### **Лабораторна робота №5**

#### **Атака на рівні додатків**

Перевірив:

Котов Д. О.

Виконав:

студент IV курсу

групи ФБ-01

Сахній Н. Р.

Приходько І. Ю.

Корабельський Т. Б.

Київ 2023

## **1. Документ з макросом, який завантажує ресурс з мережі**

**Мета:** Зрозуміти методи атаки на рівні додатків

**Після роботи студент повинен**

- **знати:** типи атак на рівні додатків;
- **вміти:** проводити атаки на рівні додатків.

**Завдання:**

- Встановити віртуальну машину Kali Linux VM;
- Встановити віртуальну машину Windows 7 VM;
- Виконати щонайменше одне з вказаних завдань.

**Технічне оснащення робочого місця:**

- Kali Linux VM (Kali)
- Windows 7 VM (target)
- Microsoft Word (встановити на Windows 7)
- Веб-сервер Apache (встановлено в Kali)
- Metasploit Framework (встановлено в Kali)

### **ЗАВДАННЯ 1**

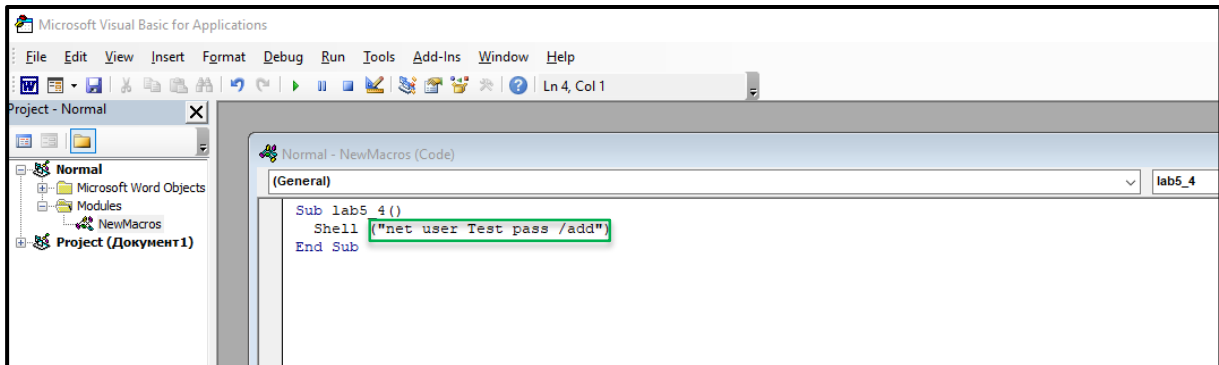
Виконати щонайменше одне з вказаних завдань: **(було зроблено три із них)**

1. Створити сервіс, та поставити його на автозапуск
2. Створити заплановане завдання у планувальнику
3. Додати файл, що виконується, в автозапуск через реєстр
4. Створити додаткового користувача та поставити йому пароль
5. Запустити SMB/RDP та поставити всі налаштування для віддаленого доступу.

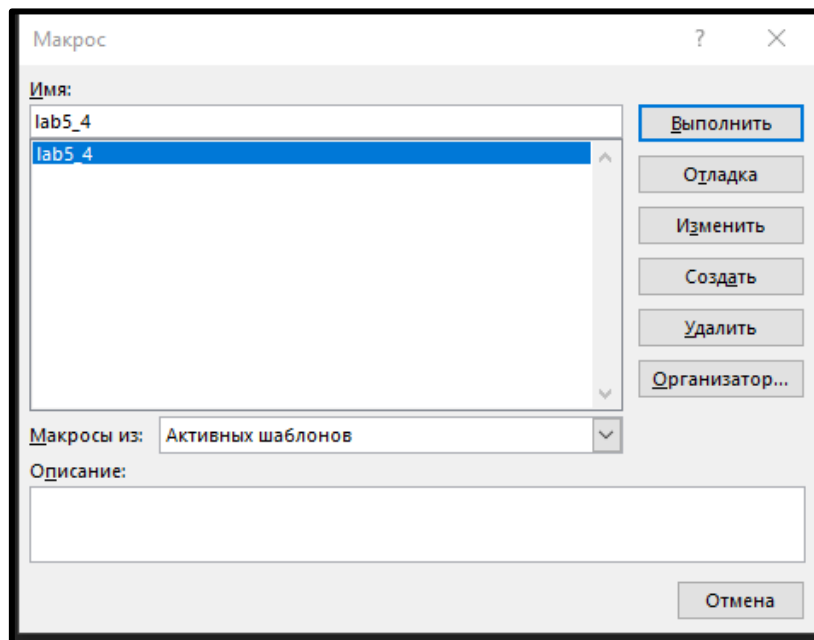
Доведіть це за допомогою скріншотів.

**Відповідь:**

**1. Створення додаткового користувача та встановлення для нього паролю ↓**



Після написання відповідного VBA-скрипта одразу виконаємо його:



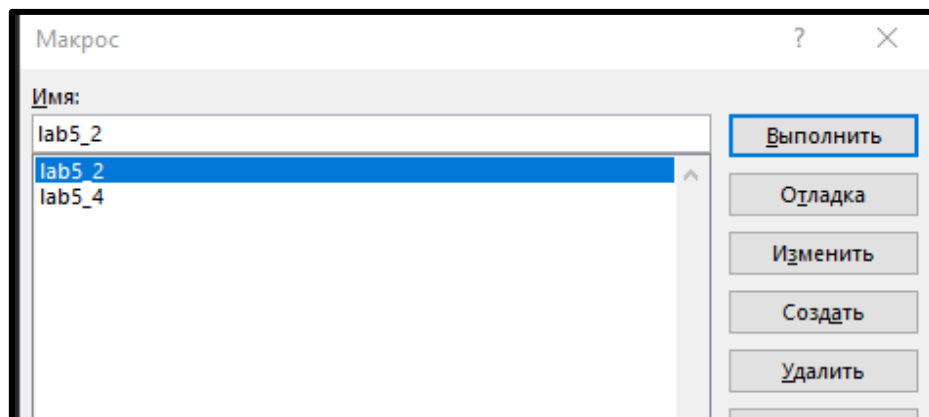
Отже, впевнимось за допомогою команди “net user”, що було створено:

```
C:\Users\admin>net users  
  
Учетные записи пользователей для \\DESKTOP-PM4UH62  
  
-----  
admin                DefaultAccount      Test  
WDAGUtilityAccount   Администратор      Гость  
Команда выполнена успешно.
```

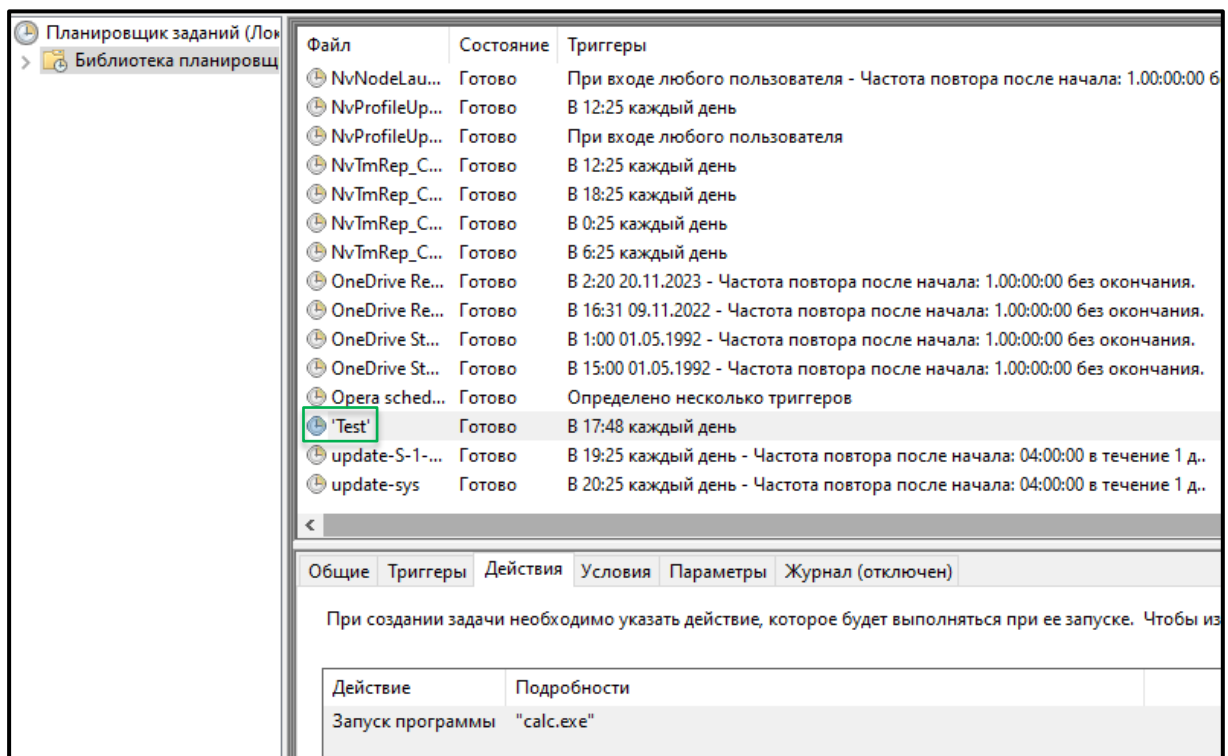
## 2. Створення запланованого завдання у планувальнику ↓

```
Sub lab5_2()  
Shell ("schtasks /create /tn 'Test' /tr 'calc.exe' /sc daily /st 17:48")  
End Sub
```

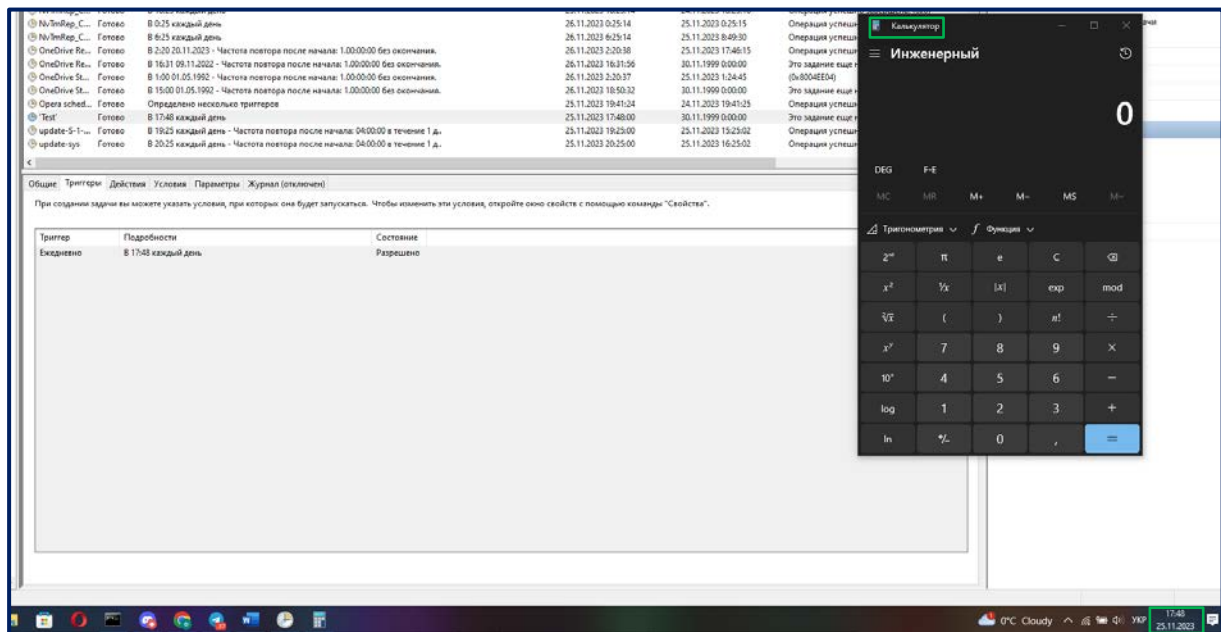
Аналогічно після збереження написаного скрипта, запусимо на виконання:



Отже, переглянемо відповідні зміни в планувальнику завдань:

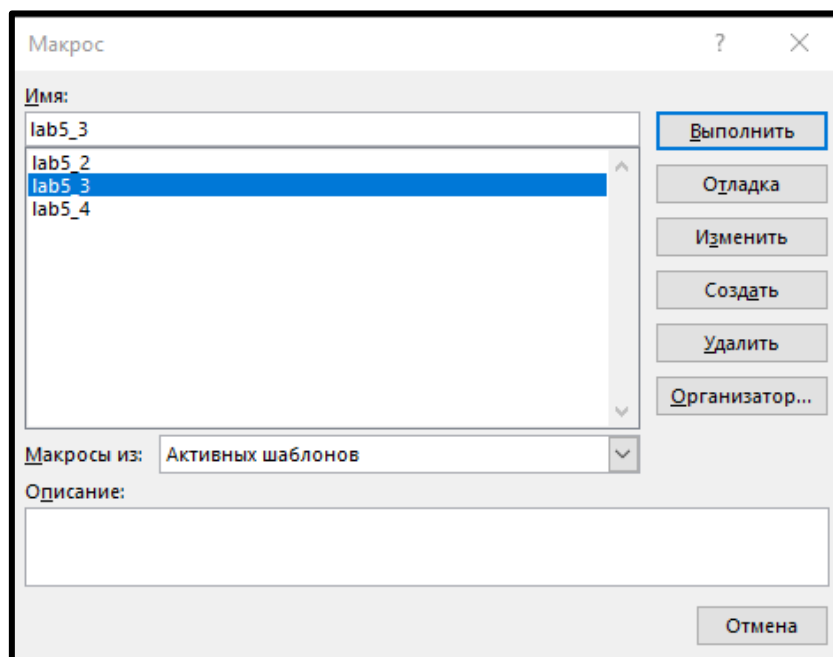


О 17:48, як було й налаштовано, система самостійно відкрила калькулятор:

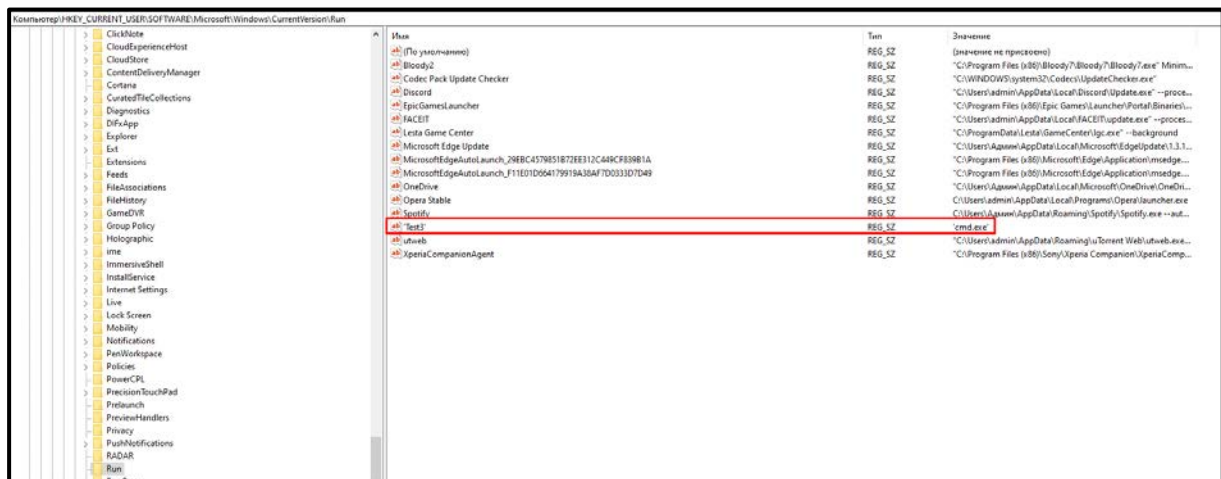


### 3. Додавання виконуваного файлу в автозапуск через реєстр ↓

```
Sub lab5_3()  
Shell("reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v 'Test3' /t REG_SZ /d 'cmd.exe' /f")  
End Sub
```

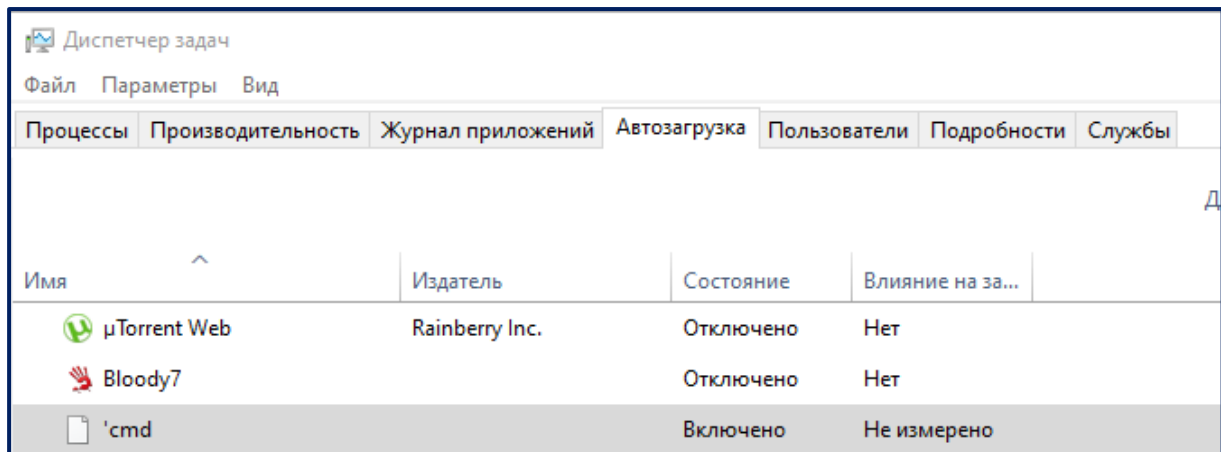


Виконавши скрипт, було помічено очікувані зміни в системного реєстрі:



Имя	Тип	Значение
(To uninstall)	REG_SZ	(значение не присвоено)
Bloody2	REG_SZ	"C:\Program Files (x86)\Bloody7\Bloody7.exe" Minim...
Code: Pack Update Checker	REG_SZ	"C:\WINDOWS\system32\Codecs\UpdateChecker.exe"
Discord	REG_SZ	"C:\Users\admin\AppData\Local\Discord\Updater.exe" --proc...
Epic Games Launcher	REG_SZ	"C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\...
FACEIT	REG_SZ	"C:\Users\admin\AppData\Local\FACEIT\update.exe" --proces...
Lesta Game Center	REG_SZ	"C:\ProgramData\Lesta\GameCenter\lgc.exe" --background
Microsoft Edge Update	REG_SZ	"C:\Users\Aqame\AppData\Local\Microsoft\Edge\update\1.3.1...
MicrosoftEdgeAutoLaunch_28BC457851872E312C44CF83981A	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge...
MicrosoftEdgeAutoLaunch_F11E07D064179919A38AF7D033D7D49	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge...
OneDrive	REG_SZ	"C:\Users\Aqame\AppData\Local\Microsoft\OneDrive\OneDri...
Opera Stable	REG_SZ	"C:\Users\admin\AppData\Local\Programs\Opera\launcher.exe
Spotify	REG_SZ	"C:\Users\Aqame\AppData\Roaming\Spotify\Spotify.exe --aut...
Test	REG_SZ	cmd.exe
utweb	REG_SZ	"C:\Users\admin\AppData\Roaming\utweb\utweb.exe...
Xperia Companion Agent	REG_SZ	"C:\Program Files (x86)\Sony\Xperia Companion\XperiaComp...

Як можна помітити нижче на зображенні, файл був доданий до автозапуску:



Имя	Издатель	Состояние	Влияние на за...
µTorrent Web	Rainberry Inc.	Отключено	Нет
Bloody7		Отключено	Нет
'cmd'		Включено	Не измерено