

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ  
Кафедра кібербезпеки

**Звіт до лабораторної роботи № 14**  
**на тему “ Дослідження можливостей платформи Metasploit для тестування на**  
**проникнення ”**

**Виконав студент(ка)**

Борщ Дмитро

**Група**

КБ-01

**Перевірила**

Лаврик Т.В.

**«Дослідження можливостей платформи Metasploit для тестування на проникнення»**

**Завдання до роботи:**

**Завдання 1 (платформа Range Force).** Виконати модулі:

- Metasploit Basics
- Metasploit Overview

**Завдання 2.** Надати відповідь:

Які є способи завантаження Metasploit Framework в Kali Linux.

Існує два основні способи як відкрити *msfconsole*:

- за допомогою ярлику в лаунчері програм в секції «Exploitation tools»;
- написавши в терміналі *msfconsole*.

**Завдання 3.** Виписати основні команди, що дозволяють:

а) отримати інформаційну довідку про команду;

*help [команда]*

б) переглянути список експлойтів;

*show exploits*

в) знайти експлойт за ключовими словами, за типом модуля, за типом платформи (ОС);

*search [пошуковий паттерн]*

г) використати обраний експлойт;

*use [шлях експлойту | порядковий номер в після команди search]*

*Наприклад:*

```
msf6 > search wordpress database backup

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/multi/http/wp_db_backup_rce      2019-04-24      excellent Yes     WP Database Backup RCE
1  auxiliary/scanner/http/wp_total_upkeep_downloader 2020-12-12      normal  No      WordPress Total Upkeep Unauthenticated B
ackup Downloader

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/http/wp_total_upkeep_downloader

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/http/wp_db_backup_rce) > use exploit/multi/http/wp_db_backup_rce
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/http/wp_db_backup_rce) >
```

д) переглянути список доступних payloads для обраного експлойту;

*show payloads*

е) вивести інформацію про обраний payload із попереднього списку;

*info [шлях payload]*

є) встановити для експлойту обраний payload;

*set payload [шлях payload]*

ж) запустити експлойт з обраним payload.

*run або exploit*