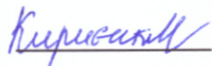


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології забезпечення
кібербезпеки з використанням Honeypot-систем»

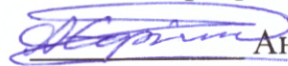
Виконав студент 2-го курсу групи КБм-24-1
спеціальності 125 «Кібербезпека та захист інформації»

 Євгеній КИРИЄНКО

Керівник доцент кафедри КІ та КБ, к.т.н.

 Олексій ШЕЛУХА

Рецензент доцент кафедри КІ та КБ, к.т.н., доцент

 Андрій ЄФІМЕНКО

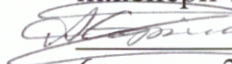
Житомир – 2025

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
6 жовтня 2025 р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу магістра

Студент: Кириєнко Євгеній Володимирович

Тема роботи: «Методи та технології забезпечення кібербезпеки з використанням Honeypot-систем»

затверджена Наказом університету від 6 жовтня 2025 р. № 566/с

Термін здачі студентом закінченої роботи 8 грудня 2025 р.

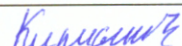
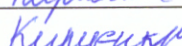
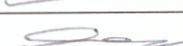
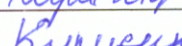
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

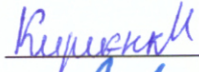
- методи та засоби створення, налаштування та використання Honeypot-системи для ідентифікації, аналізу та попередження кіберзагроз;
- процеси забезпечення кібербезпеки інформаційних систем у комп'ютерних мережах в умовах дії сучасних кіберзагроз;

Обладнання та програмне забезпечення:

1. VirtualBox
2. ОС Ubuntu / Kali Linux

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Росієнський Ю.М.	 6.10.25	 06.10.25
2	Росієнський Ю.М.	 6.10.25	 06.10.25
3	Росієнський Ю.М.	 6.10.25	 06.10.25

Студент  Євгеній КИРИЄНКО

Керівник  Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз завдання та формування структури роботи	06.10.2025	Виконано
2	Аналіз літературних джерел	23.10.2025	Виконано
3	Дослідження поняття та класифікації Honeypot-систем.	11.11.2025	Виконано
4	Вивчення принципів роботи Honeypot-систем	26.11.2025	Виконано
5	Огляд методів виявлення кіберзагроз із використанням Honeypot-систем	01.12.2025	Виконано
6	Формулювання постановки завдання дослідження	08.12.2025	Виконано
7	Вибір інструментів і технологій для реалізації Honeypot-системи.	10.12.2025	Виконано
8	Розгортання експериментального середовища.	12.12.2025	Виконано
9	Моделювання кібератак на сервіси віддаленого доступу з використанням атакуючого середовища Kali Linux.	14.12.2025	Виконано
10	Аналіз журналів подій Honeypot-системи.	17.12.2025	Виконано
11	Оформлення пояснювальної записки	18.12.2025	Виконано
12	Оформлення презентації	20.12.2025	Виконано
13	Захист	27.12.2025	Виконано

Студент Кириєнко Євгеній КИРИЄНКО
Керівник Шелуха Олексій ШЕЛУХА

АНОТАЦІЯ

Кваліфікаційна робота на тему «Методи та технології забезпечення кібербезпеки з використанням Honeypot-систем» складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури.

Текстова частина викладена на 55 сторінках. Пояснювальна записка містить 20 рисунків. Список використаних джерел містить 22 найменувань на 2 сторінках. Загальний обсяг роботи становить 55 сторінок.

Метою магістерської роботи є дослідження та практична реалізація методів і технологій забезпечення кібербезпеки інформаційних систем із використанням Honeypot-систем, а також оцінка їх ефективності для виявлення та аналізу кібератак.

У роботі розглянуто теоретичні основи Honeypot-систем, їх класифікацію та принципи функціонування. Зпроектовано та реалізовано Honeypot-систему на основі low-interaction підходу з використанням Honeypot-системи Cowrie та технології контейнеризації Docker. Створено експериментальне середовище для моделювання кібератак на сервіси віддаленого доступу та проведено аналіз журналів подій Honeypot-системи. За результатами дослідження оцінено ефективність застосування Honeypot-систем і сформульовано практичні рекомендації щодо їх використання у системах кібербезпеки.

Ключові слова: КІБЕРБЕЗПЕКА, HONEYPOT-СИСТЕМА, КІБЕРАТАКИ, ІНФОРМАЦІЙНІ СИСТЕМИ, МОНІТОРИНГ БЕЗПЕКИ, COWRIE, DOCKER, ВИЯВЛЕННЯ ЗАГРОЗ.

ANNOTATION

The qualification thesis entitled “Methods and Technologies for Ensuring Cybersecurity Using Honeypot Systems” consists of a list of abbreviations, an introduction, three chapters, conclusions, and a list of references.

The main text comprises 55 pages. The explanatory note contains 20 figures. The list of references includes 22 sources on 2 pages. The total volume of the thesis is 55 pages.

The aim of the master’s thesis is to study and practically implement methods and technologies for ensuring the cybersecurity of information systems using Honeypot systems, as well as to evaluate their effectiveness in detecting and analyzing cyberattacks.

The thesis examines the theoretical foundations of Honeypot systems, their classification, and principles of operation. A low-interaction Honeypot system was designed and implemented using the Cowrie Honeypot and Docker containerization technology. An experimental environment was created to simulate cyberattacks on remote access services, and the event logs of the Honeypot system were analyzed. Based on the results of the study, the effectiveness of Honeypot systems was evaluated, and practical recommendations for their use in cybersecurity systems were formulated.

Keywords: CYBERSECURITY, HONEYPOT SYSTEM, CYBERATTACKS, INFORMATION SYSTEMS, SECURITY MONITORING, COWRIE, DOCKER, THREAT DETECTION.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ HONEYROT-СИСТЕМ.....	9
1.1 Поняття та класифікація Honeypot-систем.....	9
1.2. Принципи роботи Honeypot-систем.....	15
1.3. Огляд методів виявлення кіберзагроз за допомогою Honeypot	19
1.4. Постановка завдання дослідження.....	21
Висновок до першого розділу:	23
РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ HONEYROT-СИСТЕМИ	24
2.1. Вибір архітектури Honeypot-системи	24
2.2. Інструменти та технології для реалізації Honeypot-систем.....	26
2.3. Процес налаштування Honeypot-системи.....	28
2.4. Оцінка видимості Honeypot-системи та її виявлення зловмисниками.....	34
2.5. Методи аналізу даних, отриманих з Honeypot-систем.....	36
Висновок до другого розділу:	38
РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ HONEYROT-СИСТЕМИ.....	39
3.1. Організація експериментального середовища	39
3.2. Моделювання кібератак та збір експериментальних даних	41
3.3. Аналіз отриманих результатів та виявлення ознак кібератак	45
Висновок до третього розділу:	50
ВИСНОВКИ	52
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	53

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SQL – Structured Query Language

ПЗ – програмне забезпечення

API – Application Programming Interface

DMZ – Demilitarized Zone

SSH – Secure Shell

POSIX – Portable Operating System Interface

LTS – Long-Term Support

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

SIEM – Security Information and Event Management

DevSecOps – Development, Security and Operations

VM – Virtual Machine

ВСТУП

Актуальність теми. У сучасних умовах розвитку інформаційних технологій зростає актуальність забезпечення кібербезпеки через збільшення кількості та складності кібератак. У зв'язку з обмеженими можливостями традиційних засобів захисту доцільним є використання Honeypot-систем для виявлення та дослідження атак у контрольованому середовищі.

Метою кваліфікаційної роботи є дослідження та практична реалізація методів і технологій забезпечення кібербезпеки з використанням Honeypot-систем, а також аналіз їх ефективності для виявлення та аналізу кібератак.

Визначена мета обумовлює наступні завдання:

- провести аналіз сучасних підходів до забезпечення кібербезпеки, зокрема дослідити можливості застосування Honeypot-систем для виявлення кібератак;
- розробити проєкт Honeypot-системи з урахуванням вимог безпеки та ізоляції, а також реалізувати модель такої системи для збору та журналювання даних про атакувальну активність;
- провести експериментальні дослідження з моделювання кібератак та проаналізувати отримані результати.

Об'єктом дослідження є процеси функціонування Honeypot-систем у складі систем кібербезпеки комп'ютерних мереж, зокрема процеси виявлення, моніторингу та аналізу атакувальної активності.

Предметом дослідження є методи та технології виявлення, моніторингу та аналізу кібератак із використанням Honeypot-систем.

Практичне значення полягає в тому, що наведені в роботі результати дослідження можуть бути використані фахівцями із адміністрування безпеки систем та мереж для впровадження Honeypot-систем, як додаткового інструмента підвищення ефективності моніторингу безпеки в корпоративних і навчальних мережах, зокрема для виявлення та аналізу кібератак в зазначених інформаційних системах.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ HONEYPOT-СИСТЕМ

1.1 Поняття та класифікація Honeypot-систем

У сучасних умовах забезпечення кібербезпеки інформаційних систем потребує комплексного підходу, який поєднує різні технічні та організаційні засоби захисту. Традиційні механізми безпеки, такі як міжмережеві екрани, системи виявлення та запобігання вторгненням, антивірусні засоби та системи моніторингу, спрямовані переважно на запобігання атакам і мінімізацію їх наслідків. Водночас Honeypot-системи виконують іншу, доповнювальну роль – вони орієнтовані на виявлення, спостереження та аналіз атакувальної активності.

Honeypot – це механізм кібербезпеки, що використовує штучну ціль для атак, щоб відволікти кіберзлочинців від реальних об'єктів. Водночас він збирає розвідувальні дані про особу, методи та мотивацію зловмисників. Honeypot може бути змодельований під будь-який цифровий актив, включаючи програмне забезпечення, сервери або саму мережу. Він навмисно створений таким чином, щоб виглядати як легітимна ціль, імітуючи її структуру, компоненти та вміст. Це необхідно для того, щоб переконати зловмисника у тому, що він отримав доступ до реальної системи, і спонукати його провести більше часу в контрольованому середовищі [1].

Honeypot діє як приманка, відволікаючи кіберзлочинців від справжніх цілей. Він також може використовуватися для збору даних про методи, можливості та рівень підготовки зловмисників. Зібрана інформація допомагає організаціям покращувати стратегію кібербезпеки, реагувати на реальні загрози та виявляти потенційні слабкі місця в архітектурі мережі та системах безпеки.

Honeynet – це мережа з кількох honeypot-систем, що виглядає як реальна мережа з різними системами, базами даних, серверами, маршрутизаторами та іншими цифровими активами. Оскільки honeynet імітує складність типової корпоративної мережі, він може утримувати кіберзлочинців у системі протягом тривалого часу. Завдяки розміру honeynet можна керувати середовищем, заманюючи зловмисників глибше в систему, щоб отримати більше інформації про їхні можливості або ідентичність. Основний принцип honeypot полягає в

тому, що він повинен виглядати як мережевий об'єкт, який організація намагається захистити.

Honeypot може бути змодельований під платіжний шлюз, оскільки він містить велику кількість конфіденційної інформації, наприклад, зашифровані номери кредитних карток або банківські рахунки. Він також може імітувати базу даних, щоб залучати зловмисників, які шукають інтелектуальну власність, комерційні таємниці або іншу цінну інформацію. Деякі honeypot-системи навіть створюються з виглядом потенційно компрометуючих файлів або зображень, щоб заманювати кіберзлочинців, які прагнуть шантажувати або завдавати репутаційної шкоди [3].

Перебуваючи в системі, можна відстежувати дії зловмисників, щоб краще розуміти їхні методи та мотивацію. Це допомагає організації адаптувати існуючі заходи безпеки та запобігати подібним атакам у майбутньому.

Щоб зробити honeypot привабливішим, у ньому можуть бути навмисно залишені вразливості, але вони не повинні бути надто очевидними. Досвідчені зловмисники можуть розпізнати погано захищену систему, внести в неї дезінформацію або навіть використати її у своїх цілях [2].

Honeypot є важливим елементом стратегії кібербезпеки, адже він допомагає:

- Виявляти вразливості в системі.
- Відволікати хакерів від реальних об'єктів.
- Збирати інформацію про методи та інструменти зловмисників.

Honeypot-системи посідають важливе місце серед сучасних засобів забезпечення кібербезпеки завдяки своїм унікальним функціональним можливостям. На відміну від традиційних механізмів захисту, які орієнтовані на запобігання атакам, Honeypot-системи зосереджені на виявленні, спостереженні та аналізі атакуювальної активності, що надає додаткові переваги для побудови комплексних систем кіберзахисту.

Однією з основних переваг використання Honeypot-систем є висока інформативність зібраних даних. Оскільки Honeypot не призначені для

легітимного використання, будь-яка зафіксована активність розглядається як потенційно зловмисна. Це дозволяє зменшити кількість хибнопозитивних спрацювань і зосередитися на реальних загрозах, що значно спрощує аналіз подій безпеки.

Важливою перевагою Honeypot-систем є можливість детального дослідження поведінки зловмисників. Honeypot дозволяють фіксувати не лише факт атаки, але й послідовність дій атакувальника, використані методи, інструменти та сценарії. Отримана інформація є цінним джерелом для аналізу сучасних кібератак і може бути використана для вдосконалення інших засобів кібербезпеки.

Ще однією перевагою є раннє виявлення нових або невідомих загроз. На відміну від сигнатурних систем захисту, Honeypot не залежать від попередньо відомих шаблонів атак. Це дозволяє виявляти нові техніки проникнення, автоматизовані сканування та нетипову атакувальну активність, що особливо актуально в умовах швидкої еволюції кіберзагроз [4].

Honeypot-системи також характеризуються відносною простотою розгортання та гнучкістю налаштування, особливо при використанні сучасних технологій віртуалізації та контейнеризації. Це дозволяє швидко адаптувати Honeypot до різних мережових середовищ, масштабувати рішення та використовувати їх як у дослідницьких, так і у виробничих умовах.

Окрему перевагу становить можливість інтеграції Honeypot-систем з іншими елементами кібербезпеки. Дані, отримані від Honeypot, можуть використовуватися у системах централізованого аналізу подій безпеки, для оновлення правил виявлення атак або формування індикаторів компрометації. Таким чином, Honeypot виступає важливим джерелом інформації для підвищення загального рівня захищеності інформаційних систем [5].

Крім того, Honeypot-системи мають значну навчальну та дослідницьку цінність. Вони можуть використовуватися для підготовки фахівців з кібербезпеки, аналізу реальних сценаріїв атак та проведення експериментальних досліджень у контрольованому середовищі без ризику для продуктивних систем.

Проте honeypot не є панацеєю. Якщо він використовується окремо без інших засобів безпеки, це не гарантує повного захисту від кібератак. Хакери також можуть використовувати honeypot. Якщо вони визначають, що система є пасткою, вони можуть перенаправити туди атаки, щоб відволікти увагу від справжніх загроз або внести дезінформацію. Також можливі випадки неправильного налаштування honeypot, через що досвідчені зловмисники можуть отримати доступ до інших частин мережі.

Honeypot-системи можуть бути класифіковані за різними ознаками залежно від їх призначення, рівня взаємодії зі зловмисником, способу розгортання та функціональних можливостей. Така класифікація дозволяє обрати оптимальний тип Honeypot-системи відповідно до цілей кібербезпеки та умов експлуатації.[6]

Одним із основних критеріїв класифікації Honeypot-систем є рівень взаємодії зі зловмисником (Рис.1.1).

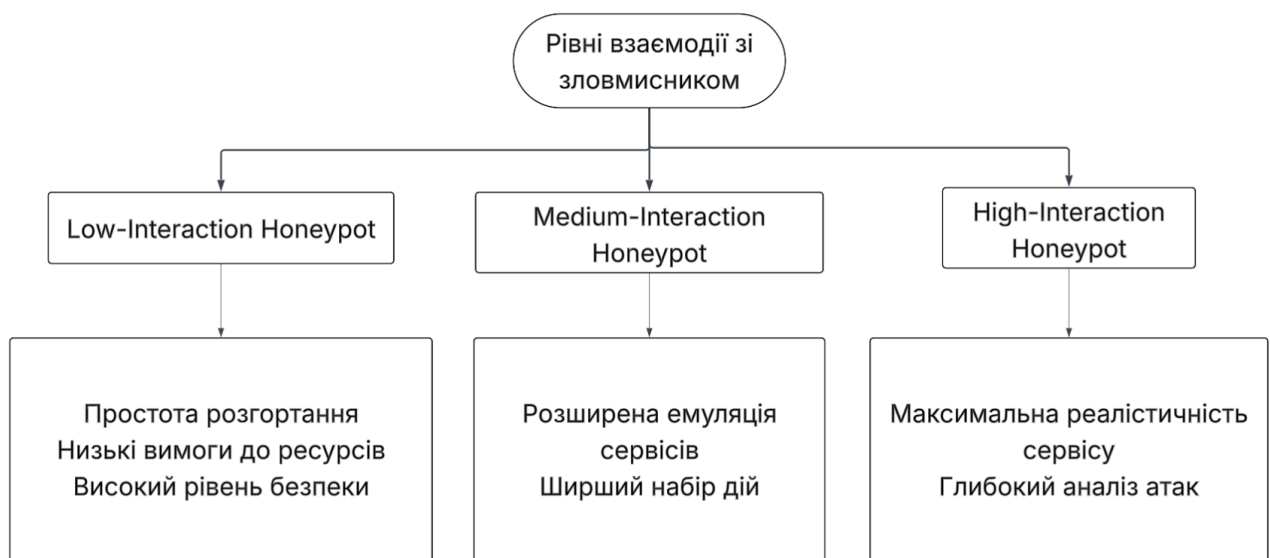


Рисунок 1.1 – Рівні взаємодії зі зловмисником

Low-interaction Honeypot імітують роботу окремих мережевих сервісів або протоколів без надання доступу до реальної операційної системи. Такі системи фіксують спроби підключення, автентифікації та базові дії атакувальника. Їх основними перевагами є простота розгортання, низькі вимоги до ресурсів і

високий рівень безпеки. Водночас вони обмежені в можливостях аналізу складних сценаріїв атак.

Medium-interaction Honeypot забезпечують розширену емуляцію сервісів і дозволяють зловмиснику виконувати ширший набір дій, однак без повного доступу до реального середовища. Вони надають більш детальну інформацію про поведінку атакувальника, зберігаючи при цьому прийнятний рівень безпеки.

High-interaction Honeypot являють собою повноцінні операційні системи або сервіси, що дозволяють зловмиснику здійснювати реальні дії в середовищі. Такі Honeypot-системи забезпечують максимальну реалістичність і глибокий аналіз атак, проте потребують значних ресурсів і підвищених заходів безпеки, оскільки існує ризик їх використання як плацдарму для подальших атак [12].

За функціональним призначенням Honeypot-системи поділяються на:

- Дослідницькі Honeypot, які використовуються для збору даних про нові типи атак, методи та інструменти зловмисників. Вони застосовуються переважно в наукових дослідженнях, аналітичних центрах і лабораторіях кібербезпеки.
- Виробничі Honeypot, які інтегруються в реальні інформаційні системи з метою підвищення рівня захищеності. Вони виконують роль додаткового механізму раннього виявлення атак і доповнюють традиційні засоби безпеки.

За способом розгортання Honeypot-системи можуть бути:

Окремі Honeypot, що функціонують як ізольовані вузли в мережі та імітують окремі сервіси або сервери [7].

Honeynet, які являють собою сукупність взаємопов'язаних Honeypot-систем і імітують фрагмент реальної мережевої інфраструктури. Honeynet дозволяють аналізувати складні сценарії атак і взаємодію зловмисника з декількома системами одночасно (Рис.1.2).

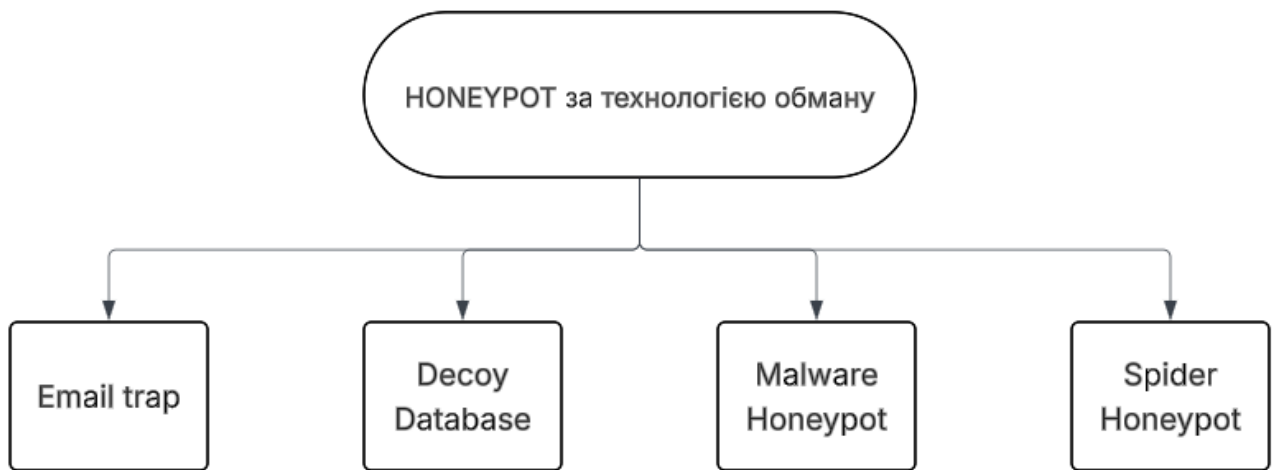


Рисунок 1.2 – Honeypot за технологією обману

За технологією обману Honeypot бувають:

- Email trap (пастка для електронної пошти) – впроваджує фіктивну email-адресу в прихованому полі, доступному лише для автоматизованих сканерів. Уся кореспонденція, що надходить на цю адресу, визначається як спам, а її джерела блокуються.
- Decoy Database (приманна база даних) – навмисно вразлива база даних для виявлення атак, зокрема SQL-ін'єкцій, викрадення облікових даних і зловживання привілеями. Зібрана інформація допомагає вдосконалювати системи безпеки.
- Malware Honeypot (пастка для шкідливого ПЗ) – імітує програму або API, щоб провокувати атаки шкідливого ПЗ. Це дає змогу аналізувати методи атак і покращувати антивірусні рішення.
- Spider Honeypot (пастка для веб-сканерів) – створює приховані вебсторінки, доступні лише для автоматизованих ботів. Дозволяє виявляти та блокувати шкідливі веб-сканери.

Таким чином, honeypot-системи є ефективним інструментом кібербезпеки, що дозволяє не лише захистити реальні цілі, а й досліджувати нові методи атак.

1.2. Принципи роботи Honeypot-систем

Honeypot-системи є спеціалізованими засобами кібербезпеки, принцип роботи яких ґрунтується на навмисному створенні привабливого, але контрольованого середовища для потенційних зловмисників.

Основною ідеєю Honeypot є імітація реальних інформаційних ресурсів з метою виявлення, спостереження та аналізу атакуючої активності без загрози для основної інфраструктури. На відміну від традиційних засобів захисту, які орієнтовані на блокування загроз, Honeypot-системи спрямовані на їх виявлення та дослідження [8].

Одним з ключових принципів роботи Honeypot-систем є принцип приманки. Honeypot навмисно позиціонується як потенційно вразливий або цінний ресурс, що може зацікавити зловмисника. Для цього використовуються відкриті мережеві порти, емуляція популярних сервісів, стандартні облікові записи або типові конфігурації. У нормальних умовах легітимні користувачі не взаємодіють із Honeypot-системою, тому будь-яка активність, зафіксована Honeypot, розглядається як потенційно зловмисна.

Другим фундаментальним принципом є ізоляція Honeypot-системи від реального середовища (Рис.1.3). Незважаючи на зовнішню подібність до реальних серверів або сервісів, Honeypot не повинен мати прямого доступу до критичних ресурсів мережі. Ізоляція досягається шляхом використання віртуалізації, контейнеризації або розміщення Honeypot у демілітаризованій зоні (DMZ).



Рисунок 1.3 – Ізоляція Honeypot-системи

Це забезпечує безпечне проведення експериментів навіть у разі активної взаємодії зловмисника з Honeypot-системою.

Важливим принципом роботи Honeypot-систем є контрольований рівень взаємодії зі зловмисником. Залежно від архітектури, Honeypot може надавати обмежену або розширену можливість взаємодії. Low-interaction Honeypot імітують лише окремі сервіси та команди, що дозволяє безпечно фіксувати спроби атак без реального виконання шкідливих дій. High-interaction Honeypot, навпаки, дозволяють повноцінну взаємодію з операційною системою, що підвищує реалістичність, але потребує посилення заходів безпеки. У межах даної роботи основна увага приділяється принципам low-interaction Honeypot, які є більш поширеними та безпечними для практичного застосування [11].

Наступним ключовим принципом є детальне журналювання та моніторинг подій. Honeypot-системи фіксують усі дії зловмисника, включаючи мережеві підключення, спроби автентифікації, введені команди, параметри сесій та часові мітки подій. Особливістю Honeypot-систем є те, що вони реєструють навіть ті дії, які в традиційних системах безпеки могли б залишитися непоміченими. Завдяки цьому Honeypot виступає цінним джерелом інформації для подальшого аналізу атак.

Наглядна схема підключення honeypot в корпоративну мережу:

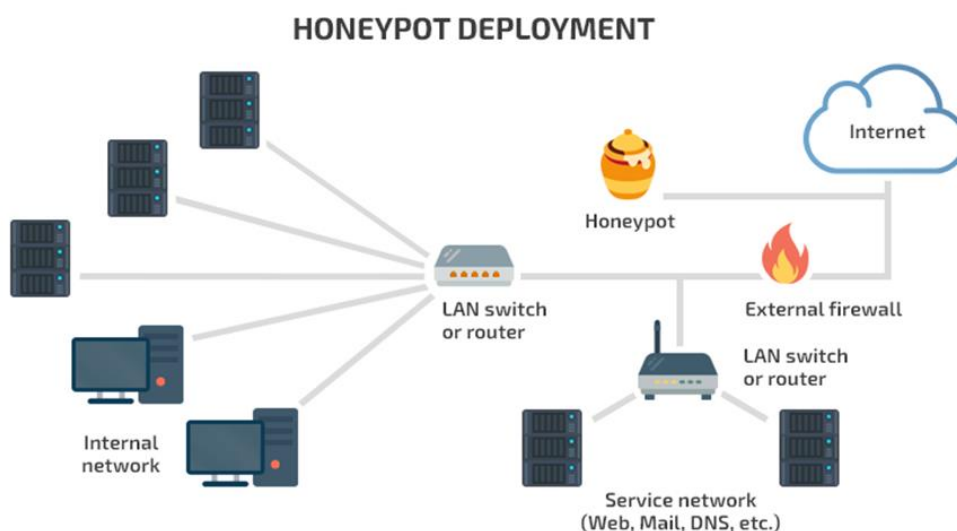


Рисунок 1.4 – Приклад використання Honeypot в корпоративній мережі

Принцип відсутності продуктивного навантаження також є важливим для Honeypot-систем. На відміну від реальних серверів, Honeypot не обслуговує легітимні запити користувачів і не виконує бізнес-функції. Це означає, що будь-яка активність у системі з високою ймовірністю є аномальною. Така особливість значно спрощує процес виявлення підозрілої поведінки та зменшує кількість хибнопозитивних спрацювань [10].

Окрему роль у принципах роботи Honeypot-систем відіграє адаптивність та масштабованість. Сучасні Honeypot-рішення можуть бути швидко розгорнуті, перевстановлені або масштабовані залежно від потреб середовища. Це дозволяє адаптувати систему до нових типів загроз, змінювати конфігурацію сервісів або розгортати декілька Honeypot-вузлів у різних сегментах мережі (Рис.1.4.).

Принцип аналітичної орієнтованості полягає в тому, що Honeypot-системи не обмежуються лише збором даних, а створюють основу для подальшого аналізу атак. Зібрані журнали подій можуть використовуватися для виявлення закономірностей, побудови поведінкових моделей зловмисників, формування індикаторів компрометації та вдосконалення інших засобів кібербезпеки. Саме цей принцип робить Honeypot важливим інструментом у дослідженнях і навчанні.

Таким чином, принципи роботи Honeypot-систем базуються на поєднанні привабливої імітації, ізоляції, контрольованої взаємодії та детального збору інформації. Завдяки цим принципам Honeypot-системи дозволяють не лише виявляти кібератаки, а й глибше досліджувати методи та поведінку зловмисників [9]. Це робить їх ефективним доповненням до традиційних засобів кібербезпеки та перспективним напрямом розвитку систем захисту інформації.

Існують honeypot, створені на виділених серверах, і програмно-емуляційні honeypot.

- Honeypot на виділеному сервері: цей тип дозволяє максимально наблизити honeypot до реального сервера, роль якого він виконує (наприклад, сервер даних, сервер додатків, проксі-сервер). Він працює в ізольованому

середовищі та має спеціально створені вразливості, що сприяють залученню злоумисників.

- Емульований honeypot: він швидко відновлюється після злому і чітко обмежується від основної операційної системи. Це дає йому можливість швидко реагувати на атаки і не спричиняти серйозних збитків. Цей тип можна реалізувати через віртуальні машини або за допомогою програмного забезпечення, як-от Honeyd.

Різниця між ними в масштабах мережі. Якщо це невелика офісна мережа, можна обмежитися емульованою системою або навіть окремими віртуальними сервісами [13]. Водночас для великих організацій з великими мережами використовуються саме виділені сервери, на яких повністю відтворюються мережеві служби, з помилками, щоб заманити злоумисників. Це дозволяє вивчати їхні методи атаки без ризику для реальних систем (Рис.1.5).

Існує три основні типи Honeypot систем:

- Honeypot з низьким рівнем взаємодії
- Honeypot середнього рівня взаємодії
- Honeypot високого рівня взаємодії

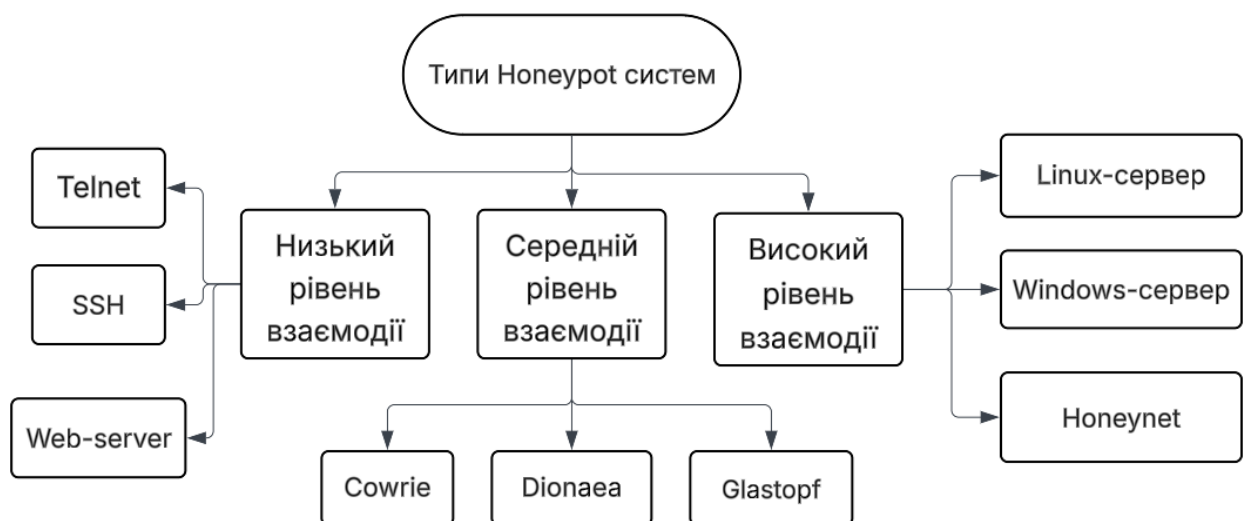


Рисунок 1.5 – Типи Honeypot систем

Honeypot з низьким рівнем взаємодії – ці системи імітують найпростіші сервіси, такі як Telnet, SSH або веб-сервери. Зловмисники можуть випадково сприйняти ці пастки за реальні вразливі системи та встановити шкідливе програмне забезпечення [15].

Honeypot середнього рівня взаємодії – більш функціональні пастки, ніж попередні. Вони можуть імітувати різноманітні вразливі системи, включаючи більшу кількість сервісів, але все одно обмежені в порівнянні з реальними системами.

Honeypot високого рівня взаємодії – це реальні системи, які вимагають додаткових заходів безпеки для запобігання компрометації інших пристроїв. Вони створюють найреалістичніші умови для атакуючих, а завдяки своїй складності можуть ідентифікувати методи, які ще не виявлені простими системами. Наприклад, вони можуть бути налаштовані на POSIX-сумісну операційну систему, що значно ускладнює зловмисникам виявлення пастки.

Honeypot-системи можуть бути використані не тільки для залучення і аналізу кібератак, а й для навчання персоналу. Вони можуть допомогти адміністраторам мережевої безпеки зрозуміти механізми атак і вдосконалити протипожежні стратегії для захисту реальних систем. Крім того, honeypot може виявляти не тільки зовнішні, але й внутрішні загрози, що часто є складними для виявлення звичайними системами безпеки.

1.3. Огляд методів виявлення кіберзагроз за допомогою Honeypot

Honeypot-системи є ефективним інструментом виявлення кіберзагроз, оскільки дозволяють фіксувати атакувальну активність без впливу на продуктивні інформаційні ресурси. На відміну від традиційних засобів захисту, які аналізують трафік реальних користувачів, Honeypot орієнтовані виключно на взаємодію зі зловмисниками, що значно спрощує ідентифікацію підозрілих дій. Методи виявлення кіберзагроз за допомогою Honeypot можуть бути класифіковані залежно від типу зібраних даних, характеру взаємодії та способів аналізу атакувальної активності [14].

Одним із базових методів виявлення загроз є аналіз спроб несанкціонованого доступу. Honeypot-системи фіксують усі спроби підключення до імітованих сервісів, зокрема спроби автентифікації з використанням типових або випадкових облікових даних. Повторюваність таких спроб, використання словникових паролів або велика кількість підключень з однієї IP-адреси розглядаються як ознаки автоматизованих атак типу brute-force. Даний метод дозволяє ефективно виявляти масові та цілеспрямовані атаки на сервіси віддаленого доступу.

Іншим важливим методом є виявлення автоматизованого мережевого сканування. Honeypot-системи здатні реєструвати спроби встановлення з'єднань з різними портами та сервісами, що характерно для початкового етапу атаки. Аналіз частоти та послідовності таких підключень дозволяє ідентифікувати використання сканерів мережі та підготовчі дії зловмисників перед здійсненням більш складних атак.

Значну роль у виявленні загроз відіграє аналіз поведінки зловмисника після встановлення з'єднання. У разі успішної автентифікації Honeypot-системи можуть фіксувати введені команди, спроби перегляду файлової системи, отримання інформації про систему або виконання розвідувальних дій. Така поведінка дозволяє визначити тип атаки, її цілі та рівень підготовки зловмисника. Поведінковий аналіз є особливо цінним для дослідження складних сценаріїв атак і формування моделей загроз.

Окрему групу методів становить аналіз часових і статистичних характеристик атакуючої активності. До таких характеристик належать час появи першої атаки після розгортання Honeypot, інтенсивність підключень, тривалість сесій та динаміка атак у часі. Аналіз цих показників дозволяє виявляти аномальні стани, масові кампанії атак або зміну тактик зловмисників.

Важливим методом виявлення загроз є також кореляція подій, зафіксованих Honeypot-системою, з іншими джерелами інформації. Журнали подій Honeypot можуть використовуватися для зіставлення з даними систем моніторингу, мережевих сенсорів або журналів безпеки інших компонентів

інфраструктури. Такий підхід дозволяє підвищити точність виявлення загроз і зменшити кількість хибних спрацювань.

З теоретичної точки зору, Honeypot-системи також можуть застосовуватися для виявлення нових або раніше невідомих типів атак. Оскільки Honeypot не залежать від сигнатур відомих загроз, вони здатні фіксувати нетипову або аномальну поведінку, яка не відповідає звичайним шаблонам. Це робить Honeypot-системи перспективним інструментом для дослідження сучасних кіберзагроз та адаптації систем захисту до нових умов.

Таким чином, методи виявлення кіберзагроз за допомогою Honeypot охоплюють аналіз спроб несанкціонованого доступу, автоматизованого сканування, поведінки зловмисників, статистичних характеристик атак та кореляцію подій. Комплексне використання цих методів дозволяє підвищити ефективність виявлення кібератак і забезпечити глибший аналіз загроз у системах кібербезпеки.

1.4. Постановка завдання дослідження

У комплексній системі захисту Honeypot-системи виконують роль додаткового сенсора безпеки, який дозволяє фіксувати спроби несанкціонованого доступу на ранніх етапах атаки. Оскільки Honeypot не призначені для легітимного використання, будь-яка взаємодія з ними розглядається як потенційно зловмисна, що забезпечує високу точність виявлення атак і суттєво зменшує кількість хибнопозитивних спрацювань. Крім того, Honeypot-системи відіграють важливу роль у зборі розвідувальної інформації про кіберзагрози, дозволяючи аналізувати тактики, техніки та процедури атак, а також виявляти нові або модифіковані методи проникнення.

Інтеграція Honeypot-систем з іншими компонентами кібербезпеки, зокрема із системами централізованого збору та аналізу журналів подій, сприяє підвищенню ефективності кореляції подій безпеки та формуванню комплексного уявлення про загрози в мережі. Отримані з Honeypot дані можуть використовуватися для вдосконалення правил виявлення атак, оновлення

політик безпеки та формування індикаторів компрометації. Окрім цього, Honeypot-системи мають значну навчальну й дослідницьку цінність, оскільки дозволяють моделювати реальні сценарії атак у контрольованому середовищі без ризику для продуктивних систем.

Разом із тим, Honeypot-системи не можуть розглядатися як самостійний засіб захисту. Їх ефективність значною мірою залежить від правильного проектування, налаштування та інтеграції з іншими елементами системи кібербезпеки. Тому доцільним є дослідження методів і технологій побудови Honeypot-систем, а також оцінка їх практичної ефективності в умовах, наближених до реальних.

На основі проведеного теоретичного аналізу Honeypot-систем, їх типів, принципів функціонування та методів виявлення кіберзагроз підтверджено актуальність теми магістерської роботи «Методи та технології забезпечення кібербезпеки з використанням Honeypot-систем». Метою даного дослідження є створення та дослідження ефективної Honeypot-системи, здатної забезпечити виявлення, аналіз і класифікацію кібератак, а також сприяти підвищенню загального рівня захищеності мережевих ресурсів.

Досягнення поставленої мети передбачає ґрунтовний аналіз існуючих Honeypot-систем і методів виявлення кіберзагроз, що дозволяє оцінити їхні можливості, переваги та обмеження. На основі цього здійснюється розробка концепції Honeypot-системи, яка відповідає вимогам безпеки, ізоляції та відтворюваності експериментального середовища, а також визначаються її архітектура, основні функціональні компоненти та інструменти реалізації. Завершальним етапом дослідження є тестування розробленої Honeypot-системи в умовах, наближених до реальних, з подальшим аналізом зібраних даних про атакувальну активність, оцінкою ефективності запропонованого рішення та формулюванням практичних рекомендацій щодо його використання у системах кібербезпеки.

Реалізація поставлених завдань дозволить створити надійну Honeypot-систему як ефективний інструмент виявлення та аналізу кібератак, що сприятиме

зниженню ризиків для комп'ютерних мереж і підвищенню загального рівня кібербезпеки організацій.

Висновок до першого розділу:

У даному розділі магістерської роботи було розглянуто теоретичні основи Honeypot-систем як одного з перспективних напрямів забезпечення кібербезпеки інформаційних систем. Проаналізовано сучасні підходи до захисту комп'ютерних мереж та обґрунтовано роль Honeypot-систем як ефективного доповнення до традиційних засобів безпеки, зокрема міжмережевих екранів, систем виявлення та запобігання вторгненням і засобів моніторингу.

У ході дослідження було розкрито поняття Honeypot та Honeynet, а також систематизовано класифікацію Honeypot-систем за рівнем взаємодії зі зловмисником, функціональним призначенням і способом розгортання. Детально розглянуто основні принципи роботи Honeypot-систем, зокрема ізоляцію, контрольовану взаємодію та детальне журналювання подій, що забезпечують безпечне виявлення та аналіз атакувальної активності.

Окрему увагу приділено огляду методів виявлення кіберзагроз за допомогою Honeypot-систем, включаючи аналіз спроб несанкціонованого доступу та поведінки зловмисників після встановлення з'єднання. Показано, що Honeypot-системи дозволяють виявляти як відомі, так і нові типи атак, зменшуючи кількість хибнопозитивних спрацювань та підвищуючи інформативність зібраних даних.

На основі проведеного теоретичного аналізу підтверджено актуальність теми магістерської роботи та сформульовано завдання подальшого дослідження. Отримані результати створили теоретичну основу для подальшого проєктування та практичної реалізації Honeypot-системи.

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ HONEYPOT-СИСТЕМИ

2.1. Вибір архітектури Honeypot-системи

Вибір архітектури Honeypot-системи є одним із ключових етапів її проектування, оскільки саме архітектурні рішення визначають рівень безпеки, гнучкість налаштування, можливості збору експериментальних даних та подальшого аналізу кібератак. Неправильно обрана архітектура може призвести як до недостатньої ефективності Honeypot, так і до підвищених ризиків компрометації реальної інфраструктури.

Honeypot-системи можуть реалізовуватися за різними архітектурними підходами, які умовно поділяються за рівнем взаємодії зі зловмисником, масштабом розгортання та ступенем ізоляції від основної мережі [16].

Найпоширенішою класифікацією є поділ на low-interaction, medium-interaction та high-interaction honeypot. Кожен із цих підходів має свої переваги та недоліки, які необхідно враховувати залежно від цілей дослідження.

High-interaction honeypot передбачають розгортання повноцінних операційних систем або сервісів, які дозволяють зловмиснику взаємодіяти з реальним середовищем. Такий підхід забезпечує максимальну реалістичність і дає змогу досліджувати складні сценарії атак, включаючи експлуатацію вразливостей і подальше поширення у мережі. Водночас high-interaction honeypot потребують значних обчислювальних ресурсів, складного адміністрування та постійного контролю, оскільки у разі успішної атаки вони можуть бути використані як плацдарм для подальших атак.

Low-interaction honeypot, навпаки, не надають зловмиснику доступу до реальної операційної системи, а лише імітують поведінку мережевих сервісів. Такі системи фокусуються на зборі інформації про спроби автентифікації, мережеву активність та початкові дії зловмисника. Основною перевагою цього підходу є високий рівень безпеки та простота розгортання, що робить його придатним для дослідницьких і навчальних цілей.

З огляду на мету даної магістерської роботи – дослідження методів забезпечення кібербезпеки з використанням Honeypot-систем – було обрано

архітектуру low-interaction honeypot. Такий вибір дозволяє зосередитися на аналізі типових кібератак на сервіси віддаленого доступу, зокрема SSH, які є одними з найпоширеніших цілей атак у сучасних мережах.(Рис.2.1)

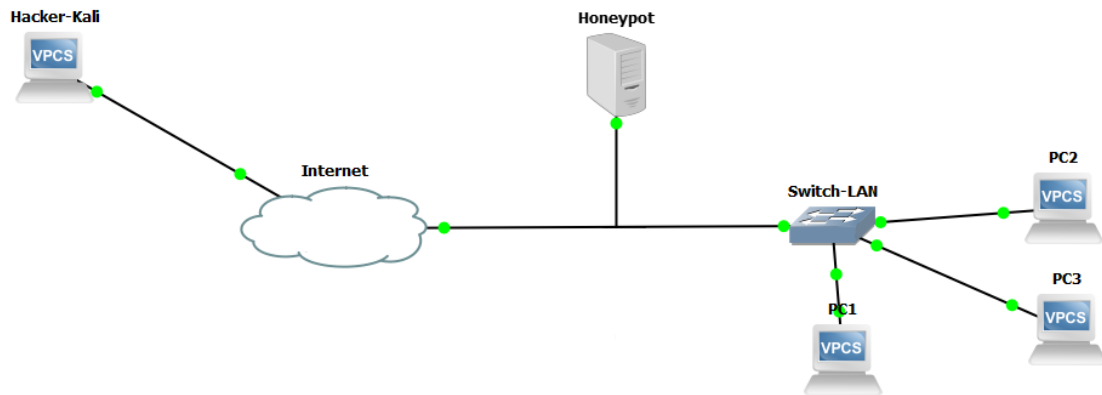


Рисунок 2.1 – Схема розробленої експериментальної мережі

Архітектура розроблюваної Honeypot-системи передбачає використання окремого серверного вузла, який виконує роль приманки для потенційних атакувальників. Цей вузол розміщується у віртуалізованому середовищі та не має прямого доступу до критичних ресурсів інформаційної системи. Такий підхід дозволяє мінімізувати ризики у разі активної взаємодії зловмисника з Honeypot-системою [17].

Для забезпечення додаткової ізоляції та керованості середовища виконання було застосовано контейнерну архітектуру. Контейнеризація дозволяє розгорнути Honeypot-систему у вигляді незалежного ізольованого середовища, яке працює поверх основної операційної системи. У разі виявлення нестабільної поведінки або необхідності відновлення системи контейнер може бути швидко перезапущений або перевстановлений без впливу на хостову систему.

Важливим аспектом вибору архітектури є також масштабованість та відтворюваність експериментів. Контейнеризований підхід дозволяє відтворити однакове експериментальне середовище на різних платформах без суттєвих змін у конфігурації. Це особливо важливо у контексті наукових досліджень, де необхідно забезпечити повторюваність результатів та можливість порівняльного аналізу.

Обрана архітектура також враховує можливість інтеграції Honeypot-системи з іншими елементами кібербезпеки. Завдяки використанню структурованих журналів подій та стандартних мережевих протоколів, зібрані дані можуть бути використані для подальшого аналізу, кореляції подій та побудови систем виявлення загроз. Таким чином, Honeypot-система розглядається не як ізольований експериментальний інструмент, а як складова частина комплексної системи кібербезпеки [18].

Отже, вибір архітектури low-interaction Honeypot-системи з використанням віртуалізації та контейнеризації є обґрунтованим з точки зору безпеки, ефективності збору даних та відповідності цілям дослідження. Така архітектура забезпечує оптимальний баланс між реалістичністю імітації атак та контролем над експериментальним середовищем, що створює надійну основу для подальшої реалізації та аналізу Honeypot-системи.

2.2. Інструменти та технології для реалізації Honeypot-систем

Реалізація Honeypot-системи вимагає ретельного вибору інструментів та технологій, які повинні забезпечувати стабільну роботу, безпеку експериментального середовища, а також можливість збору й подальшого аналізу даних про кібератаки. У межах даної магістерської роботи добір програмних засобів здійснювався з урахуванням сучасних підходів до побудови систем кібербезпеки, вимог до відтворюваності експериментів та практичної цінності отриманих результатів.

Основною платформою для розгортання Honeypot-системи було обрано серверну операційну систему Ubuntu Server 20.04 LTS. Дана операційна система є однією з найбільш поширених у серверних середовищах, має довгострокову

підтримку та стабільні оновлення безпеки. Використання Ubuntu Server дозволяє забезпечити надійне функціонування системи, а також відповідає практикам, які застосовуються в реальних корпоративних і хмарних інфраструктурах [19].

Ключовим програмним компонентом Honeypot-системи є Cowrie – спеціалізований low-interaction honeypot, призначений для емуляції сервісів віддаленого доступу, зокрема SSH та Telnet. Cowrie широко використовується у дослідницьких та практичних проєктах з кібербезпеки завдяки своїй здатності детально фіксувати дії потенційних зловмисників без надання доступу до реальних ресурсів системи. Система реєструє спроби автентифікації, параметри з'єднань, виконані команди, а також поведінкові характеристики сесій, що робить її ефективним інструментом для дослідження атак.

Важливою перевагою Cowrie є підтримка різних форматів журналювання, зокрема текстових логів та структурованих журналів у форматі JSON. Використання структурованих журналів значно спрощує подальший аналіз даних, автоматичну обробку подій та інтеграцію з іншими засобами кібербезпеки. Саме ці можливості були ключовими при виборі Cowrie як основи для реалізації Honeypot-системи у даній роботі.

Для розгортання Cowrie було застосовано технологію контейнеризації Docker. Docker дозволяє ізолювати середовище виконання Honeypot-системи від хостової операційної системи, що підвищує рівень безпеки та спрощує процес адміністрування. Контейнеризація також усуває проблеми сумісності програмних бібліотек та версій інтерпретатора Python, що є актуальним для складних програмних систем. Крім того, Docker забезпечує можливість швидкого розгортання, масштабування та повторного використання конфігурацій Honeypot-системи.

Використання Docker у поєднанні з Cowrie відповідає сучасним підходам DevSecOps, де безпека інтегрується безпосередньо у процеси розгортання та експлуатації систем. Такий підхід дозволяє розглядати Honeypot-систему не лише як експериментальний інструмент, а як компонент реальної інфраструктури кібербезпеки.

Для моделювання атакуючої активності у межах дослідження було використано операційну систему Kali Linux. Kali Linux є спеціалізованим дистрибутивом, що містить широкий набір інструментів для тестування безпеки, аналізу мережі та моделювання різних типів кібератак. Застосування Kali Linux дозволило імітувати як ручні спроби несанкціонованого доступу, так і автоматизовані атаки типу brute-force, що забезпечило отримання реалістичних експериментальних даних.

Мережеву взаємодію між Honeypot-сервером та атакуючою системою було організовано у межах віртуального середовища з використанням платформи віртуалізації. Це дозволило створити ізольовану експериментальну мережу, у якій можна безпечно проводити атаки без ризику впливу на зовнішні мережеві ресурси. Такий підхід відповідає принципам безпечного проведення досліджень у сфері кібербезпеки.

Додатковим технологічним аспектом реалізації Honeypot-системи є можливість подальшої інтеграції з аналітичними та моніторинговими інструментами. Структуровані журнали подій Cowrie можуть бути використані для подальшої обробки за допомогою мов програмування, таких як Python, або інтегровані з системами централізованого аналізу подій безпеки. Це відкриває можливості для застосування інтелектуальних методів аналізу даних та побудови моделей виявлення атак [20].

Отже, використаний набір інструментів і технологій – Ubuntu Server, Cowrie, Docker та Kali Linux – забезпечує комплексний підхід до реалізації Honeypot-системи. Вони дозволяють поєднати безпеку, стабільність та гнучкість експериментального середовища, а також створюють передумови для подальшого аналізу та практичного застосування результатів дослідження у сфері кібербезпеки.

2.3. Процес налаштування Honeypot-системи

Процес налаштування Honeypot-системи є критично важливим етапом її реалізації, оскільки від правильності конфігурації залежить коректність збору експериментальних даних, рівень безпеки середовища та можливість

подальшого аналізу кібератак. У межах даної магістерської роботи налаштування Honeypot-системи здійснювалося поетапно з урахуванням вимог до ізоляції, стабільності роботи та відтворюваності експериментів.

На першому етапі було підготовлено базове серверне середовище. Для цього у віртуальному середовищі було встановлено операційну систему Ubuntu Server 20.04 LTS. Вибір серверної операційної системи зумовлений її стабільністю, широкою підтримкою та можливістю використання у реальних виробничих середовищах. Після встановлення було виконано базове налаштування системи, включаючи оновлення програмних пакетів, налаштування користувацьких облікових записів та перевірку мережевої доступності.

Другим етапом стало налаштування мережевого середовища для Honeypot-системи. Було організовано ізольовану віртуальну мережу, у межах якої Honeypot-сервер та атаквальна система могли безпосередньо взаємодіяти між собою [21]. Такий підхід дозволив забезпечити безпечне проведення експериментів без ризику впливу на зовнішні мережеві ресурси або основну інфраструктуру. Мережеві параметри було налаштовано таким чином, щоб Honeypot-система приймала вхідні з'єднання на визначені порти, що імітують роботу сервісів віддаленого доступу.

Наступним етапом стало встановлення та налаштування платформи контейнеризації Docker. Використання Docker дозволило ізолювати Honeypot-систему від хостової операційної системи та забезпечити контрольоване середовище виконання. Після встановлення Docker було перевірено коректність його роботи, налаштовано служби автозапуску та права доступу, що дозволило стабільно запускати контейнеризовані сервіси.

Безпосереднє розгортання Honeypot-системи здійснювалося шляхом запуску контейнера Cowrie. Контейнер було налаштовано з пробросом мережевих портів, що дозволило приймати SSH-з'єднання з атаквальної системи. Такий підхід дозволяє емулювати поведінку реального сервера віддаленого доступу, не надаючи при цьому доступу до реальних ресурсів

операційної системи. Контейнеризований запуск також спростив керування життєвим циклом Honeypot-системи, зокрема її перезапуск та відновлення після завершення експериментів.

Окрему увагу було приділено налаштуванню механізмів журналювання подій. Honeypot-система Cowrie підтримує реєстрацію подій у різних форматах, що дозволяє здійснювати як оперативний перегляд активності, так і подальший детальний аналіз. Було забезпечено збереження структурованих журналів у форматі JSON, які містять інформацію про IP-адреси джерел атак, використані облікові записи, часові мітки подій та типи виконаних дій. Саме ці журнали стали основним джерелом експериментальних даних для аналізу у третьому розділі роботи.

Після завершення первинного налаштування Honeypot-системи було проведено тестування її працездатності. Контрольні підключення дозволили перевірити коректність прийому мережевих з'єднань, реєстрації спроб автентифікації та збереження лог-файлів. У результаті тестування було підтверджено, що Honeypot-система коректно імітує сервіс віддаленого доступу та забезпечує стабільний збір даних про атакувальну активність.

Завершальним етапом налаштування стала підготовка системи до проведення експериментів з моделювання кібератак. Honeypot-система була залишена у пасивному режимі очікування з'єднань, що дозволило фіксувати всі спроби доступу з атакувальної системи. Такий режим роботи відповідає реальним сценаріям використання Honeypot у мережевих середовищах та створює умови для збору репрезентативних експериментальних даних.

Таким чином, поетапний процес налаштування Honeypot-системи забезпечив створення стабільного, безпечного та функціонального експериментального середовища. Реалізована конфігурація дозволила не лише здійснювати моделювання кібератак, але й отримувати структуровані дані для подальшого аналізу та оцінки ефективності Honeypot-системи.

Honeypot-системи найбільш ефективні не як ізольовані рішення, а як складові комплексної системи забезпечення кібербезпеки. Інтеграція Honeypot із

іншими засобами захисту дозволяє підвищити рівень виявлення загроз, забезпечити кореляцію подій безпеки та сформувати цілісне уявлення про стан захищеності інформаційної системи. У межах даної магістерської роботи інтеграція Honeypot-системи розглядається як перспективний напрям підвищення ефективності кіберзахисту.

Одним з основних напрямів інтеграції Honeypot-систем є взаємодія з системами моніторингу та централізованого збору подій безпеки. Honeypot-система Cowrie формує детальні журнали подій, які містять інформацію про спроби несанкціонованого доступу, параметри з'єднань, облікові записи та поведінку зломисників. Ці дані можуть бути використані як джерело подій для систем класу SIEM, що дозволяє здійснювати кореляцію з іншими подіями безпеки, такими як спрацювання міжмережевих екранів або систем виявлення вторгнень.

Інтеграція Honeypot-системи з системами виявлення та запобігання вторгненням (IDS/IPS) відкриває можливості для підвищення точності виявлення атак. Інформація, зібрана Honeypot, може використовуватися для оновлення сигнатур атак або формування поведінкових правил виявлення підозрілої активності. Наприклад, повторювані спроби автентифікації або характерні команди, зафіксовані Honeypot-системою, можуть слугувати індикаторами компрометації для інших елементів системи безпеки.

Важливим аспектом інтеграції є використання Honeypot-системи у процесах аналізу загроз та реагування на інциденти. Дані, отримані від Honeypot, дозволяють фахівцям з кібербезпеки отримати уявлення про актуальні методи та інструменти атакувальників. Це, у свою чергу, сприяє вдосконаленню політик безпеки, налаштуванню правил доступу та підвищенню обізнаності персоналу щодо сучасних загроз.

Контейнеризована архітектура Honeypot-системи значно спрощує її інтеграцію у сучасні IT- та DevSecOps-середовища. Завдяки використанню Docker Honeypot може бути швидко розгорнутий у тестових або виробничих середовищах без значних змін у наявній інфраструктурі. Такий підхід дозволяє

масштабувати Honeypot-систему, розгортати декілька екземплярів для різних сегментів мережі та оперативно адаптувати систему до нових вимог безпеки.

Окрему роль Honeypot-системи відіграють у контексті інтелектуального аналізу даних та машинного навчання. Зібрані журнали подій можуть використовуватися як навчальні вибірки для побудови моделей виявлення аномалій або класифікації кібератак. Це дозволяє розглядати Honeypot не лише як інструмент спостереження, а як активне джерело даних для розвитку інтелектуальних систем кібербезпеки.

Також Honeypot-системи можуть бути інтегровані у процеси навчання та підготовки фахівців з кібербезпеки. Реалістичні журнали атак і змодельовані сценарії зловмисної активності можуть використовуватися для аналізу інцидентів, навчальних лабораторних робіт та підвищення практичних навичок персоналу. Це підкреслює універсальність Honeypot-систем як інструментів не лише захисту, але й навчання.

Таким чином, інтеграція Honeypot-системи з іншими елементами кібербезпеки дозволяє значно розширити її функціональні можливості. У комплексі з системами моніторингу, аналізу подій та реагування на інциденти Honeypot-система стає важливим джерелом інформації про загрози та ефективним інструментом підвищення загального рівня кіберзахисту інформаційних систем.

У реальних інформаційних системах Honeypot-системи рідко використовуються як одиничні ізольовані вузли. Для підвищення ефективності виявлення кібератак та збору репрезентативних даних доцільним є масштабування Honeypot-рішень і їх розгортання у різних сегментах мережевої інфраструктури. Масштабований підхід дозволяє охопити ширший спектр загроз і моделювати поведінку зловмисників у середовищах, наближених до реальних.

Одним із поширених підходів до масштабування є побудова Honeynet – сукупності взаємопов'язаних Honeypot-систем, які імітують фрагмент реальної мережі. Такий підхід дозволяє створити більш реалістичне середовище, у якому зловмисник може взаємодіяти з декількома сервісами або вузлами. Honeynet

підвищує цінність зібраних даних, оскільки дає змогу аналізувати не лише окремі атаки, а й сценарії поширення зловмисної активності.

Важливим аспектом масштабування Honeypot-систем є сегментація мережі. Розміщення Honeypot у різних мережевих зонах, таких як демілітаризована зона (DMZ), внутрішня мережа або окремі підмережі, дозволяє виявляти атаки на різних етапах проникнення. Такий підхід забезпечує раннє виявлення зовнішніх загроз і водночас дозволяє аналізувати внутрішню атакувальну активність.

Сучасні технології віртуалізації та контейнеризації значно спрощують масштабування Honeypot-систем. Використання контейнерних платформ дозволяє швидко розгортати декілька екземплярів Honeypot з однаковою або зміненою конфігурацією, мінімізуючи витрати на адміністрування. Контейнеризовані Honeypot можуть динамічно створюватися або видалятися залежно від потреб безпеки та навантаження на систему.

Окрему увагу при масштабуванні Honeypot-систем необхідно приділяти централізованому збору та аналізу даних. У реальних мережах з великою кількістю Honeypot важливим є агрегування журналів подій у єдине сховище, що дозволяє здійснювати кореляцію подій, виявляти масові атаки та аналізувати поведінкові патерни зловмисників. Централізований підхід підвищує ефективність аналізу та спрощує управління Honeypot-інфраструктурою.

Разом з тим, масштабування Honeypot-систем пов'язане з певними ризиками та обмеженнями. Зі збільшенням кількості Honeypot зростає ймовірність їх ідентифікації зловмисниками як пасток, що може зменшити ефективність збору даних. Крім того, неправильна конфігурація масштабованої Honeypot-інфраструктури може створювати додаткові ризики безпеки. Тому при розгортанні Honeypot у реальних мережах необхідно забезпечувати належний рівень ізоляції, контролю доступу та моніторингу.

Таким чином, масштабування та розгортання Honeypot-систем у реальних мережах є важливим етапом підвищення ефективності їх використання. Поєднання декількох Honeypot, сегментація мережі та застосування сучасних

технологій контейнеризації дозволяють створити гнучку та адаптивну Honeypot-інфраструктуру, яка може бути ефективно інтегрована у комплексні системи кібербезпеки.

2.4. Оцінка видимості Honeypot-системи та її виявлення зловмисниками

Одним із важливих аспектів ефективності Honeypot-систем є рівень їх «видимості» для потенційних зловмисників та тривалість періоду, протягом якого система сприймається як реальний мережевий ресурс. (Рис.2.2.) З часом Honeypot може бути ідентифікований як пастка, що призводить до зменшення кількості атак або повної втрати інтересу з боку зловмисників. Тому доцільним є дослідження показників, які дозволяють оцінити, наскільки швидко Honeypot-система стає відомою в публічних джерелах або серед атакувальної спільноти. (Рис.2.2)

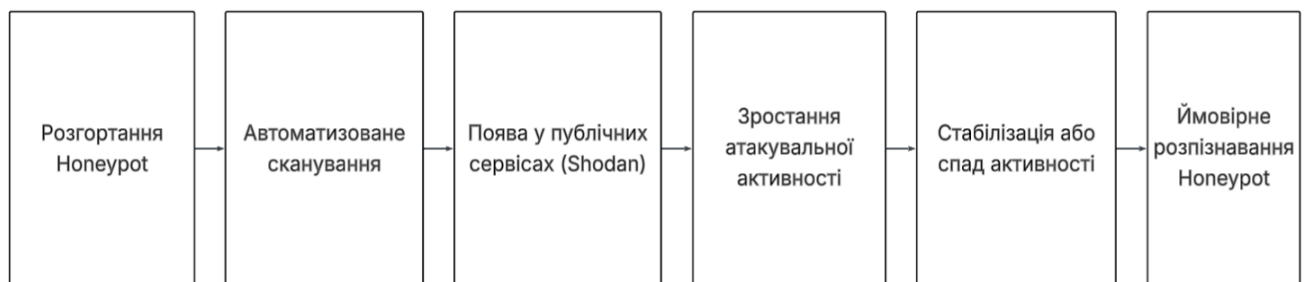


Рисунок 2.2 – Часова модель виявлення Honeypot-системи зловмисниками

Одним із індикаторів видимості Honeypot-системи є поява інформації про неї у відкритих сервісах збору даних про мережеві вузли, таких як пошукові системи мережевих сервісів (наприклад, сервіси типу Shodan або подібні платформи). (Рис.2.2) Такі сервіси здійснюють автоматизоване сканування глобальної мережі та формують бази даних відкритих портів, сервісів і банерів. Потрапляння Honeypot-системи до таких баз даних може свідчити про її зовнішню доступність та потенційну зацікавленість з боку зловмисників.

З теоретичної точки зору, процес «виявлення» Honeypot-системи можна розглядати як часовий інтервал між моментом її розгортання та моментом першої зафіксованої зовнішньої атакуючої активності або появи інформації про систему в публічних джерелах. Чим коротшим є цей інтервал, тим швидше система стає доступною для автоматизованих сканерів та потенційних зловмисників. Водночас надмірно швидке зростання кількості атак може свідчити про агресивне сканування або характерні ознаки Honeypot-системи, які привертають увагу.[21]

Іншим важливим показником є динаміка атакуючої активності у часі. На початковому етапі розгортання Honeypot зазвичай спостерігається поступове зростання кількості підключень, спроб автентифікації та автоматизованих атак. Зниження інтенсивності атак або різке припинення взаємодії з системою може свідчити про те, що Honeypot був ідентифікований як пастка або втратив привабливість для зловмисників. Таким чином, тривалість активної взаємодії може розглядатися як непрямий показник ефективності маскуванню Honeypot-системи.

З позиції теорії кібербезпеки, важливим фактором є також реалістичність емульованих сервісів. Honeypot-системи, які використовують типові конфігурації, стандартні банери або характерні відповіді сервісів, можуть бути швидше ідентифіковані автоматизованими інструментами. Натомість системи з більш гнучкою конфігурацією та поведінкою, наближеною до реальних серверів, здатні зберігати інтерес зловмисників протягом тривалішого часу.

Таким чином, у теоретичному аспекті оцінка ефективності Honeypot-системи може включати аналіз часу її виявлення, динаміки атакуючої активності та тривалості періоду взаємодії зі зловмисниками. Дослідження цих показників дозволяє зробити висновки щодо ступеня «привабливості» Honeypot-системи та її здатності залишатися непоміченою як пастка, що є важливим фактором для практичного використання Honeypot у системах кібербезпеки.

2.5. Методи аналізу даних, отриманих з Honeypot-систем

Honeypot-системи забезпечують збір великого обсягу даних про атакувальну активність, що потребує застосування різноманітних методів аналізу для отримання корисної інформації про характер і джерела кіберзагроз. Дані, отримані з Honeypot, можуть включати журнали підключень, спроби автентифікації, виконані команди, мережеві параметри та часові характеристики атак. Ефективний аналіз таких даних є ключовим етапом у процесі виявлення, класифікації та дослідження кібератак [22].

Одним із базових підходів є журнальний (лог-аналіз). Він полягає у вивченні журналів подій, що фіксують спроби підключення, використані облікові дані, IP-адреси, часові мітки та результати автентифікації. Аналіз логів дозволяє виявляти повторювані шаблони атак, частоту спроб доступу, використання словникових паролів і типові ознаки автоматизованих атак. (Рис.2.3) Даний метод є основою для більш складних підходів до аналізу даних Honeypot-систем.

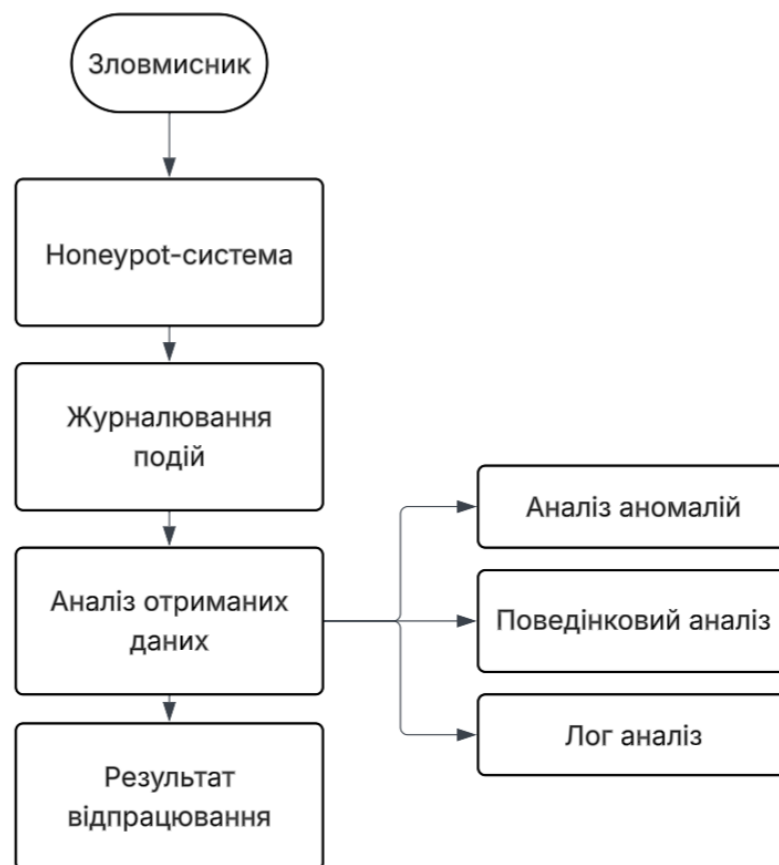


Рисунок 2.3 – Загальний процес аналізу зібраних даних

Важливе місце займає статистичний аналіз отриманих даних. До статистичних показників належать кількість атак за одиницю часу, розподіл атак за джерелами, середня тривалість сесій та інтенсивність спроб автентифікації. Аналіз цих параметрів дозволяє виявляти аномальні стани, пікові навантаження та масові кампанії атак. Статистичні методи також використовуються для порівняння ефективності Honeypot-систем у різні періоди часу.

Окрему групу методів становить поведінковий аналіз. Він базується на дослідженні дій зловмисників після встановлення з'єднання з Honeypot-системою. Аналіз введених команд, послідовності дій та спроб доступу до ресурсів дозволяє визначити наміри атакувальника, рівень його підготовки та тип атаки. Поведінковий підхід є особливо корисним для виявлення складних або цілеспрямованих атак.

Для підвищення точності виявлення загроз застосовується кореляційний аналіз. Він полягає у зіставленні даних Honeypot із подіями, зафіксованими іншими компонентами системи кібербезпеки, такими як мережеві сенсори, системи моніторингу або журнали серверів. Кореляція подій дозволяє виявляти взаємозв'язки між окремими атаками та ідентифікувати координовану або розподілену атакувальну активність.

Перспективним напрямом є аналіз аномалій, що ґрунтується на виявленні відхилень від типового профілю атакувальної активності. У рамках цього підходу визначаються характерні параметри нормальної поведінки, після чого фіксуються нетипові зміни у частоті, тривалості або характері атак. Даний метод дозволяє виявляти нові або раніше невідомі типи кібератак.

Також застосовується класифікація атак, яка передбачає групування за типами, методами проникнення або рівнем складності. Класифікаційний підхід дозволяє структурувати зібрані дані та спрощує подальший аналіз загроз. У теоретичному аспекті класифікація може базуватися на правилах, статистичних характеристиках або комбінованих підходах.

Таким чином, аналіз даних, отриманих з Honeypot-систем, ґрунтується на поєднанні журнального, статистичного, поведінкового, кореляційного та

аномального аналізу. Комплексне застосування цих методів дозволяє отримати глибоке уявлення про характер сучасних кібератак і підвищити ефективність використання Honeypot-систем у комплексних системах кібербезпеки.

Висновок до другого розділу:

У другому розділі було спроектовано та реалізовано Honeypot-систему з урахуванням сучасних вимог до безпеки, ізоляції та відтворюваності експериментального середовища. Обґрунтовано вибір архітектури low-interaction Honeypot-системи, що забезпечує безпечне моделювання кібератак та ефективний збір експериментальних даних.

Розглянуто інструменти й технології, використані для реалізації системи, зокрема операційну систему Ubuntu Server, Honeypot-систему Cowrie, контейнеризацію Docker та атакувальне середовище Kali Linux. Детально описано процес налаштування Honeypot-системи та окреслено можливості її інтеграції з іншими елементами кібербезпеки.

Окрему увагу приділено теоретичним аспектам оцінки видимості Honeypot-системи та можливості її ідентифікації зломисниками у відкритих мережеских середовищах, що дозволяє враховувати фактор тривалості ефективної роботи Honeypot як приманки.

Отримані результати створили технічну та методологічну основу для проведення експериментальних досліджень і аналізу ефективності Honeypot-системи, реалізованих у наступному розділі роботи.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ HONEYPOT-СИСТЕМИ

3.1. Організація експериментального середовища

Для проведення дослідження ефективності Honeypot-системи було організовано експериментальне середовище, яке дозволяє моделювати реальні сценарії кібератак у контрольованих та безпечних умовах. Основною вимогою до середовища була можливість ізольованого розгортання Honeypot-системи, стабільної фіксації подій безпеки та відтворюваності експериментів.

Експериментальне середовище реалізовано з використанням технологій віртуалізації та контейнеризації. Як платформа віртуалізації було використано Oracle VM VirtualBox, у межах якої розгорнуто серверну операційну систему Ubuntu Server 20.04 LTS. Застосування віртуального середовища дозволило ізольовати експериментальну інфраструктуру від основної системи та уникнути ризиків для реальної мережі.

У межах дослідження було розгорнуто дві віртуальні машини, кожна з яких виконувала чітко визначену функціональну роль. Перша віртуальна машина використовувалася як Honeypot-сервер та функціонувала під керуванням операційної системи сімейства Linux (Ubuntu Server).

Для підвищення стабільності та усунення проблем сумісності програмних бібліотек Honeypot-система була розгорнута у вигляді Docker-контейнера. Контейнеризація дозволяє ізольовати програмне середовище виконання, спростити процес розгортання та забезпечити однакову конфігурацію системи незалежно від версій операційної системи та інтерпретатора Python. Такий підхід широко використовується у сучасних системах кібербезпеки та відповідає практикам DevSecOps.

У якості Honeypot-системи було використано Cowrie – low-interaction honeypot, призначений для емуляції сервісів віддаленого доступу, зокрема SSH та Telnet. Cowrie не надає зловмиснику доступу до реальної операційної системи, проте імітує поведінку сервера та фіксує всі дії потенційного атакувальника. Це дозволяє безпечно збирати експериментальні дані про спроби несанкціонованого доступу та поведінку зловмисників.

Архітектура експериментального середовища передбачала використання двох логічних компонентів. Першим компонентом був Honeypot-сервер на базі Ubuntu Server з розгорнутим Docker-контейнером Cowrie. Другим компонентом виступала атакувальна система на базі Kali Linux, яка використовувалася для моделювання кібератак. Обидві системи були підключені до однієї ізольованої віртуальної мережі VirtualBox, що забезпечувало можливість прямої мережевої взаємодії між ними та водночас виключало доступ до зовнішніх мережевих ресурсів.(Рис.3.1)

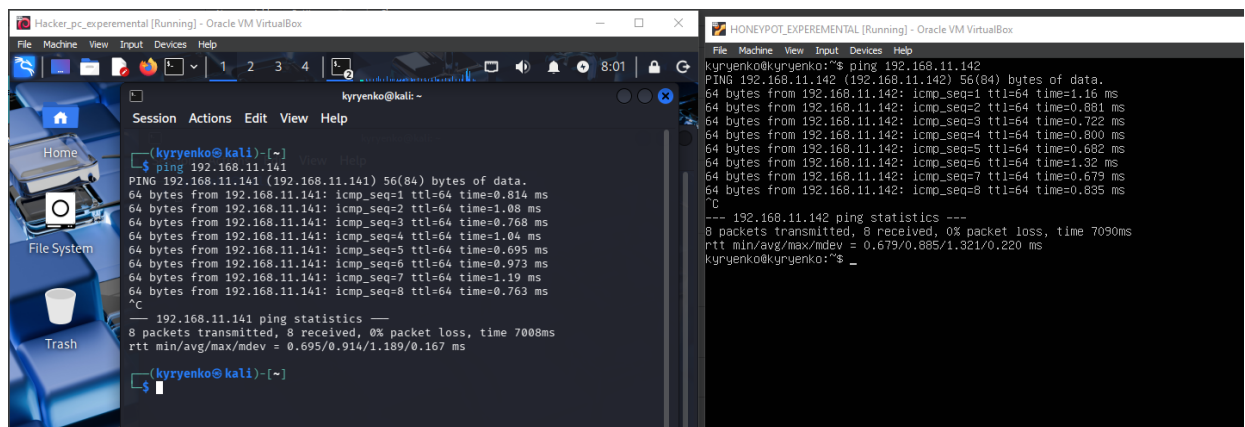


Рисунок 3.1 – Встановлення зв'язку між сервером та атакувальником

Docker-контейнер Cowrie було налаштовано з пробросом мережевих портів, що дозволило приймати вхідні SSH-з'єднання з атакувальної системи. Усі спроби автентифікації, відкриття сесій та виконання команд автоматично реєструвалися Honeypot-системою.(Рис.3.2) Журнали подій містили інформацію про IP-адреси джерел атак, облікові записи, часові мітки, параметри термінального середовища та послідовність дій злоумисника.

Особливу увагу було приділено механізмам збору та збереження експериментальних даних. Cowrie здійснює журналювання у текстовому та структурованому форматах, що забезпечує можливість подальшого аналізу подій, їх класифікації та виявлення характерних ознак кібератак. Зібрані лог-файли використовувалися як основне джерело даних для аналізу в наступних підрозділах даного розділу.

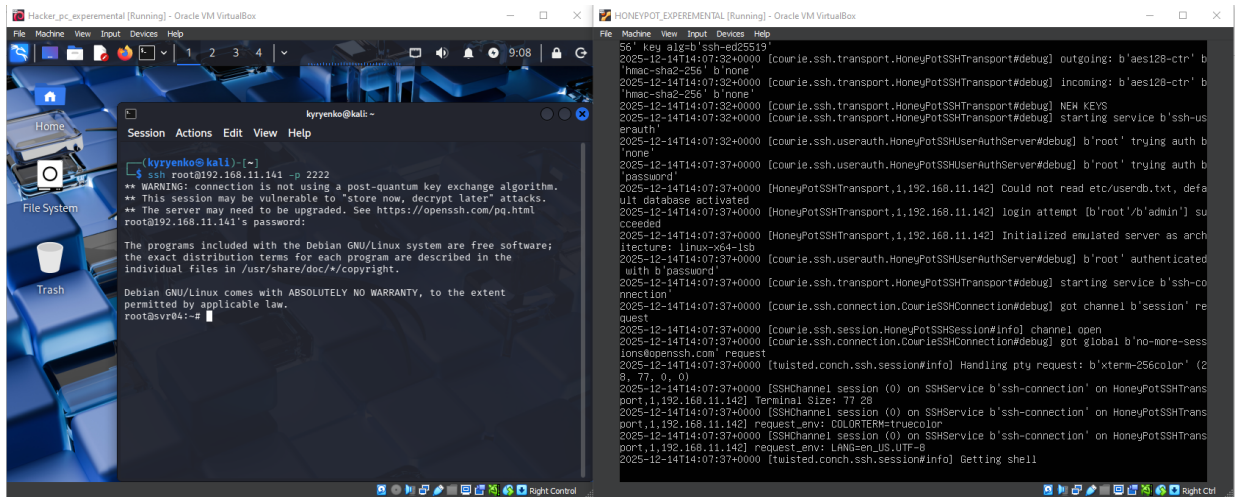


Рисунок 3.2 – Перше підключення до Honeypot-системи

Таким чином, створене експериментальне середовище забезпечує безпечне та стабільне функціонування Honeypot-системи, дозволяє моделювати типові сценарії атак на сервіси віддаленого доступу та формує повноцінну базу експериментальних даних. Отримане середовище стало основою для моделювання кібератак, аналізу отриманих результатів та оцінки ефективності Honeypot-системи, що розглядається у наступних підрозділах розділу.

Для підвищення реалістичності експериментального середовища передбачено можливість моделювання автоматизованих атак типу brute-force з використанням спеціалізованих інструментів. Це дозволяє імітувати поведінку зловмисників та шкідливих ботів, характерну для сучасних мережевих атак.

3.2. Моделювання кібератак та збір експериментальних даних

З метою оцінки працездатності Honeypot-системи та перевірки її здатності фіксувати дії потенційних зловмисників було проведено моделювання типових кібератак на сервіси віддаленого доступу. Експерименти здійснювалися у межах підготовленого віртуального середовища з використанням атакуючої системи на базі операційної системи Kali Linux [15].

На першому етапі було змодельовано початкову активність зловмисника, характерну для етапу розвідки та перевірки доступності сервісів. З атакуючої

системи виконувалися спроби встановлення SSH-з'єднання з Honeypot-сервером. (Рис.3.3) Під час цих спроб використовувалися різні облікові записи та паролі, що імітує ручні спроби несанкціонованого доступу. (Рис.3.4)

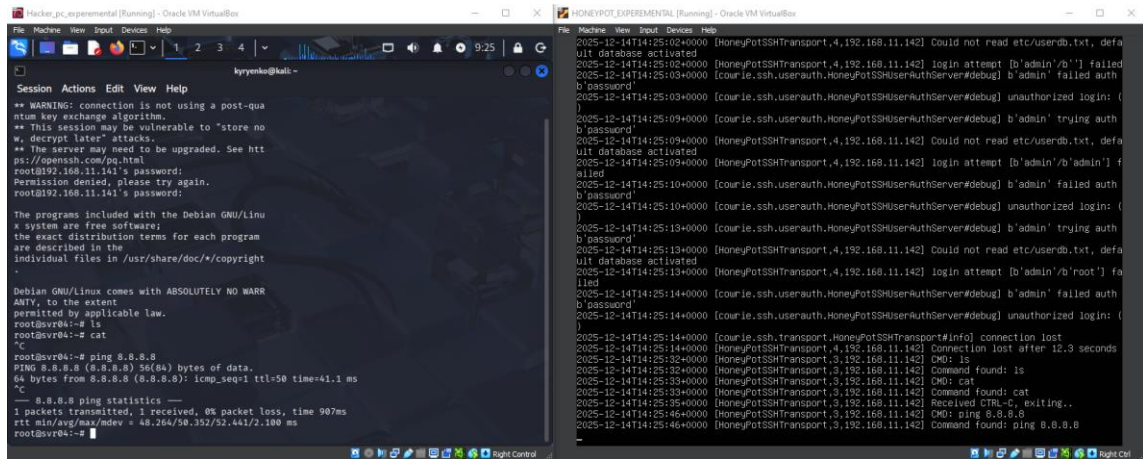


Рисунок 3.3 – Імітація несанкціонованого доступу

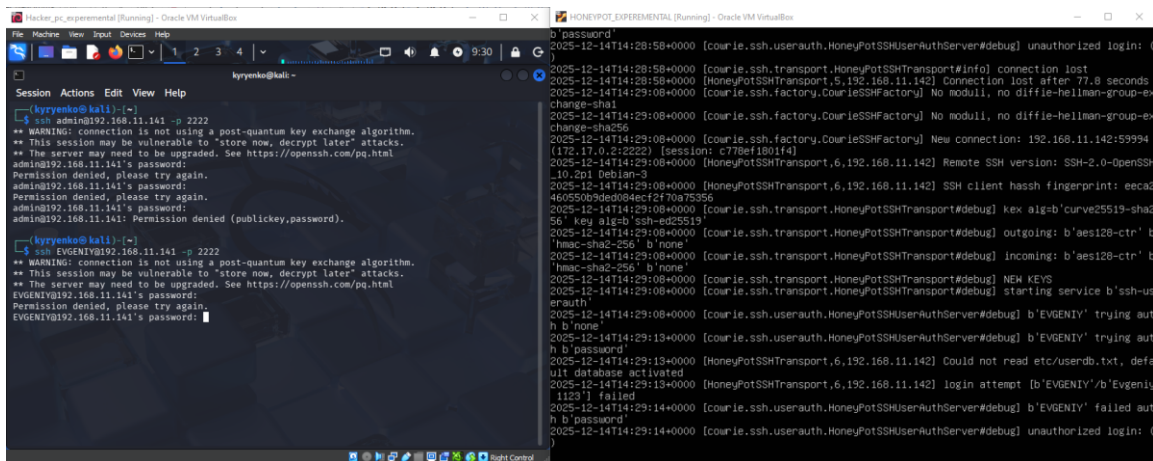


Рисунок 3.4 – Імітація несанкціонованого доступу

Другим етапом експерименту стало моделювання повторюваних спроб автентифікації, які відповідають атакам типу brute-force. Було виконано серію послідовних SSH-підключень до Honeypot-системи з одного джерела за короткий проміжок часу. Така активність дозволила оцінити здатність Honeypot-системи фіксувати масові спроби доступу та накопичувати відповідні журнали подій.

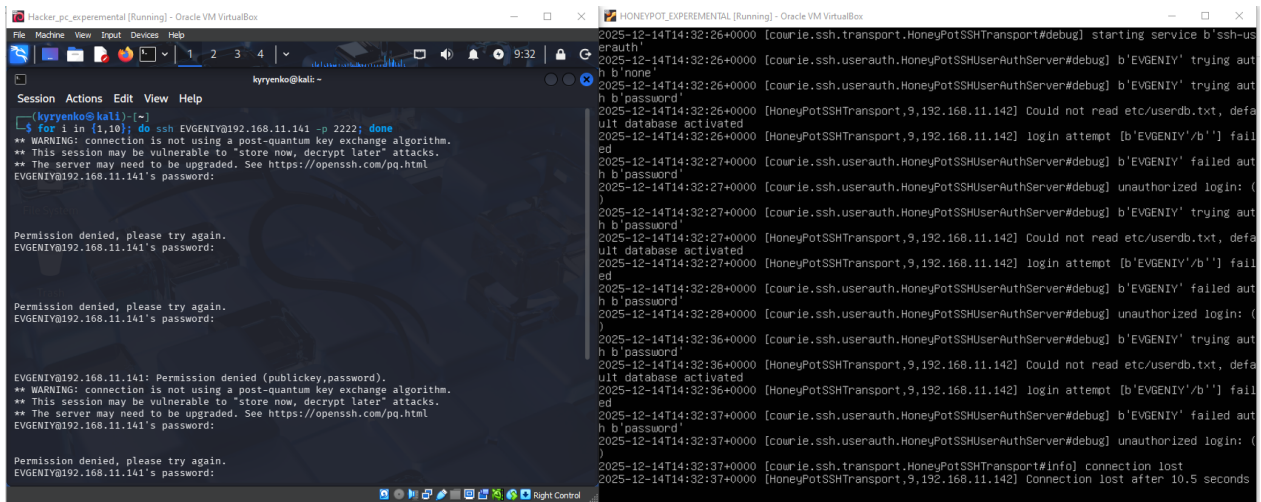


Рисунок 3.5 – Моделювання повторюваних спроб автентифікації

На третьому етапі здійснювалася взаємодія з емуляваним shell-оточенням Honeypot-системи. (Рис.3.6) Після встановлення з'єднання виконувалися базові системні команди, характерні для початкового етапу роботи зломисника після компрометації сервера. Усі введені команди та параметри сесії автоматично реєструвалися Honeypot-системою.

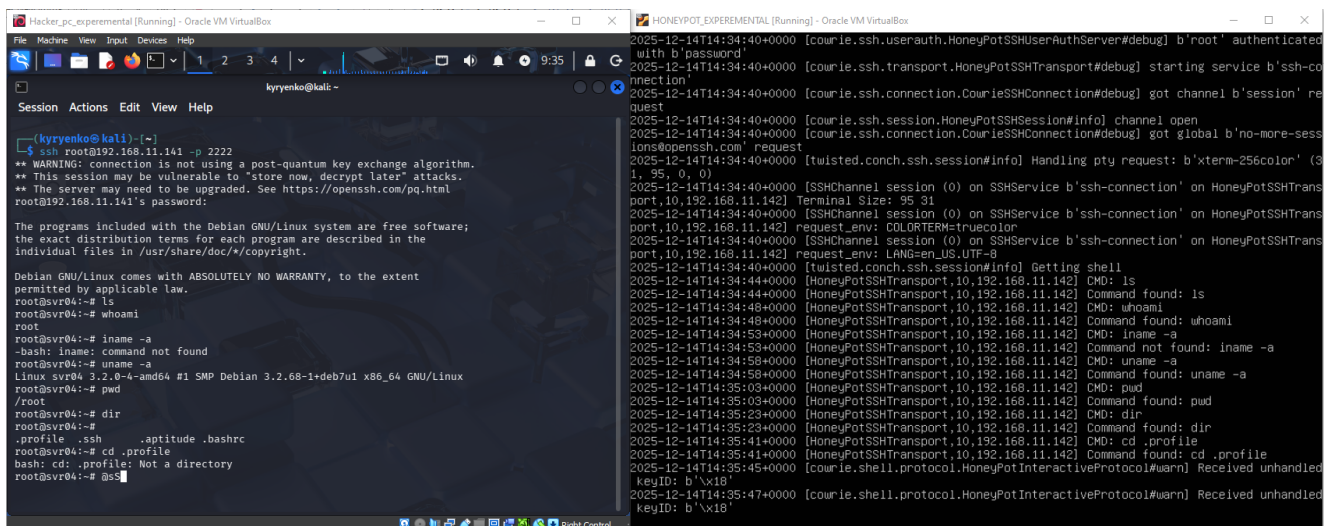


Рисунок 3.6 – Взаємодія з емуляваним shell-оточенням Honeypot-системи

У процесі експериментів Honeypot-система Cowrie коректно фіксувала всі спроби підключення, незалежно від їх результату. До зібраних експериментальних даних увійшли IP-адреси джерел атак, використані облікові

записи, часові мітки подій, факти відкриття сесій та послідовності виконаних команд. Отримані журнали подій сформували базу експериментальних даних для подальшого аналізу та виявлення характерних ознак кібератак.

Для моделювання більш складного сценарію атаки було реалізовано автоматизовану атаку типу brute-force з використанням інструмента Hydra.(Рис.3.7) Атака полягала у багаторазових спробах автентифікації до SSH-сервісу Honeypot-системи з використанням набору типових облікових записів і паролів. Такий тип атак є характерним для ботнетів та автоматизованих шкідливих скриптів.

У ході експерименту Honeypot-система Cowrie коректно фіксувала кожну спробу автентифікації, зберігаючи інформацію про використані облікові дані, часові мітки та джерело атаки. Після імітації успішного доступу було змодельовано базову поведінку зловмисника шляхом виконання типових системних команд, що дозволило дослідити можливості Honeypot-системи щодо реєстрації post-login активності.

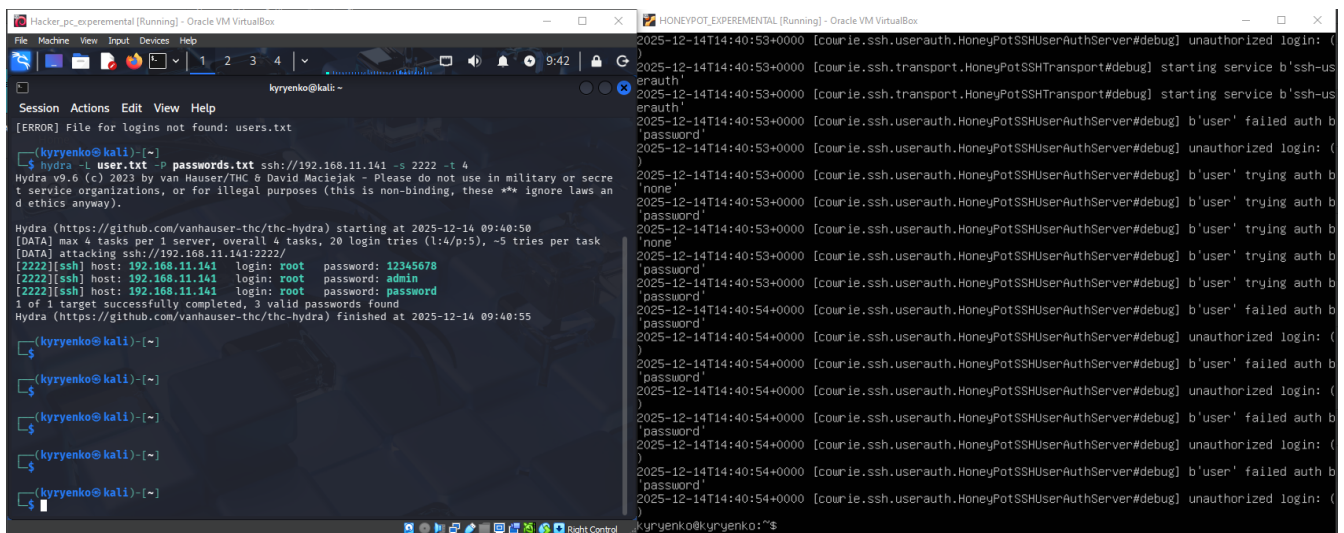


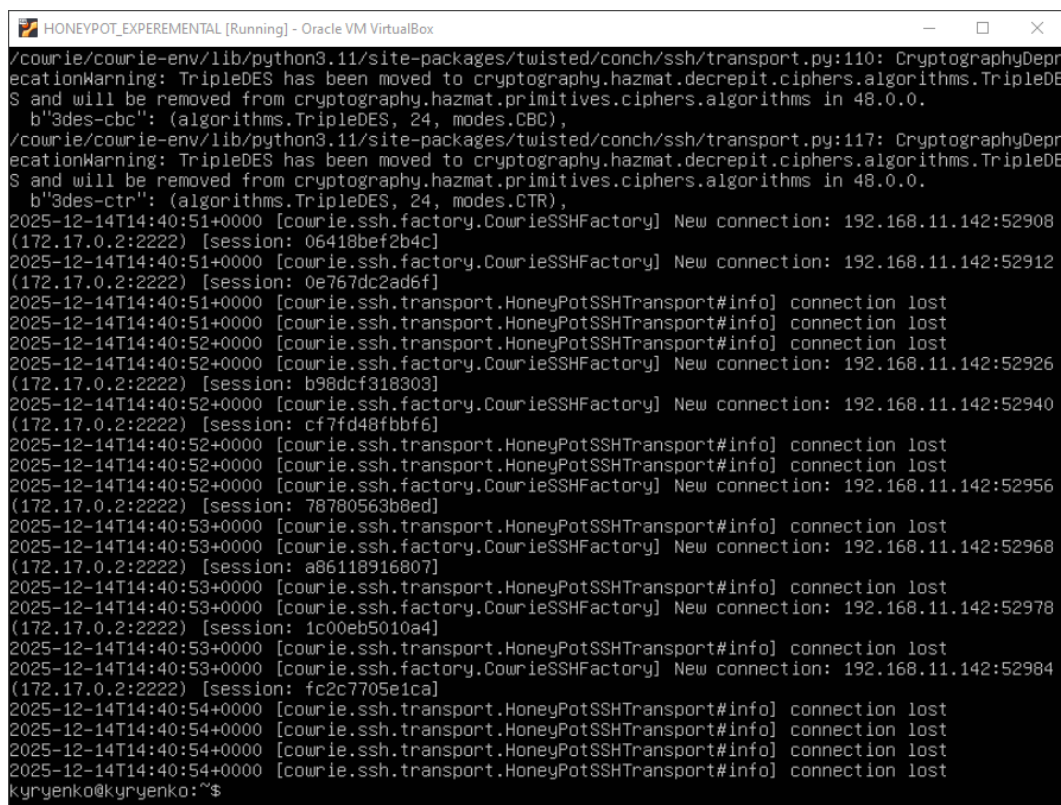
Рисунок 3.7 – Атака brute-force з використанням інструмента Hydra

Таким чином, проведене моделювання кібератак підтвердило здатність Honeypot-системи ефективно імітувати мережеві сервіси та забезпечувати детальний збір даних про дії потенційних зловмисників у реальному часі.

3.3. Аналіз отриманих результатів та виявлення ознак кібератак

Після проведення експериментів із моделювання кібератак було здійснено аналіз зібраних даних з метою виявлення характерних ознак несанкціонованої активності та оцінки аналітичних можливостей Honeypot-системи. Джерелом експериментальних даних слугували журнали подій Honeypot-системи Cowrie, які містять детальну інформацію про спроби підключення, автентифікації та взаємодію з емульованим середовищем.

На першому етапі аналізу було виконано попередній перегляд лог-файлів з метою ідентифікації ключових параметрів подій. (Рис.3.8) До таких параметрів належать IP-адреси джерел атак, облікові записи, що використовувалися під час спроб входу, часові мітки подій, а також типи дій, виконаних у межах SSH-сесій. (Рис.3.9) Додатково було проаналізовано частоту та повторюваність спроб автентифікації, що дозволило виявити ознаки автоматизованих атак типу brute-force. Отримані дані стали основою для подальшого статистичного та поведінкового аналізу атакуючої активності з метою класифікації загроз та оцінки ефективності Honeypot-системи.



```
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:117: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
2025-12-14T14:40:51+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.11.142:52908 (172.17.0.2:2222) [session: 06418bef2b4c]
2025-12-14T14:40:51+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.11.142:52912 (172.17.0.2:2222) [session: 0e767dc2ad6f]
2025-12-14T14:40:51+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:51+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:52+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:52+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.11.142:52926 (172.17.0.2:2222) [session: b98dcf318303]
2025-12-14T14:40:52+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.11.142:52940 (172.17.0.2:2222) [session: cf7fd48fbbf6]
2025-12-14T14:40:52+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:52+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:52+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.11.142:52956 (172.17.0.2:2222) [session: 78780563b8ed]
2025-12-14T14:40:53+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:53+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.11.142:52968 (172.17.0.2:2222) [session: a86118916807]
2025-12-14T14:40:53+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:53+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.11.142:52978 (172.17.0.2:2222) [session: 1c00eb5010a4]
2025-12-14T14:40:53+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:53+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.11.142:52984 (172.17.0.2:2222) [session: fc2c7705e1ca]
2025-12-14T14:40:54+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:54+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:54+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:40:54+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
kyryenko@kyryenko:~$
```

Рисунок 3.8 – Аналіз основних параметрів атакуючого

```
2025-12-14T14:34:40+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated
with b'password'
2025-12-14T14:34:40+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-co
nnection'
2025-12-14T14:34:40+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' re
quest
2025-12-14T14:34:40+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2025-12-14T14:34:40+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sess
ions@openssh.com' request
2025-12-14T14:34:40+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (3
1, 95, 0, 0)
2025-12-14T14:34:40+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTrans
port,10,192.168.11.142] Terminal Size: 95 31
2025-12-14T14:34:40+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTrans
port,10,192.168.11.142] request_env: COLORTERM=truecolor
2025-12-14T14:34:40+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTrans
port,10,192.168.11.142] request_env: LANG=en_US.UTF-8
2025-12-14T14:34:40+0000 [twisted.conch.ssh.session#info] Getting shell
2025-12-14T14:34:44+0000 [HoneyPotSSHTransport,10,192.168.11.142] CMD: ls
2025-12-14T14:34:44+0000 [HoneyPotSSHTransport,10,192.168.11.142] Command found: ls
2025-12-14T14:34:48+0000 [HoneyPotSSHTransport,10,192.168.11.142] CMD: whoami
2025-12-14T14:34:48+0000 [HoneyPotSSHTransport,10,192.168.11.142] Command found: whoami
2025-12-14T14:34:53+0000 [HoneyPotSSHTransport,10,192.168.11.142] CMD: uname -a
2025-12-14T14:34:53+0000 [HoneyPotSSHTransport,10,192.168.11.142] Command not found: uname -a
2025-12-14T14:34:58+0000 [HoneyPotSSHTransport,10,192.168.11.142] CMD: uname -a
2025-12-14T14:34:58+0000 [HoneyPotSSHTransport,10,192.168.11.142] Command found: uname -a
2025-12-14T14:35:03+0000 [HoneyPotSSHTransport,10,192.168.11.142] CMD: pwd
2025-12-14T14:35:03+0000 [HoneyPotSSHTransport,10,192.168.11.142] Command found: pwd
2025-12-14T14:35:23+0000 [HoneyPotSSHTransport,10,192.168.11.142] CMD: dir
2025-12-14T14:35:23+0000 [HoneyPotSSHTransport,10,192.168.11.142] Command found: dir
2025-12-14T14:35:41+0000 [HoneyPotSSHTransport,10,192.168.11.142] CMD: cd .profile
2025-12-14T14:35:41+0000 [HoneyPotSSHTransport,10,192.168.11.142] Command found: cd .profile
2025-12-14T14:35:45+0000 [cowrie.shell.protocol.HoneyPotInteractiveProtocol#warn] Received unhandled
keyID: b'\xx18'
2025-12-14T14:35:47+0000 [cowrie.shell.protocol.HoneyPotInteractiveProtocol#warn] Received unhandled
keyID: b'\xx18'
```

Рисунок 3.9 – Аналіз основних параметрів атакуючого

Аналіз цих параметрів дозволив сформуванати загальне уявлення про інтенсивність та характер атакуючої активності.

Подальший аналіз показав наявність повторюваних спроб автентифікації з використанням різних комбінацій логінів і паролів за короткі проміжки часу. Така поведінка є типовою ознакою атак типу brute-force та credential stuffing, які широко застосовуються автоматизованими шкідливими скриптами та ботнетами.

Повторюваність подій та їх висока частота свідчать про неінтерактивний, автоматизований характер атак.

Окрему увагу було приділено аналізу post-login активності, зафіксованої HoneyPot-системою (Рис.3.10). У журналах подій виявлено виконання типових системних команд, спрямованих на отримання інформації про середовище, облікові записи та параметри операційної системи (Рис.3.11). Така поведінка є характерною для початкового етапу компрометації та свідчить про намагання зловмисника оцінити подальші можливості атаки.

```
HONEYPOT_EXPERIMENTAL [Running] - Oracle VM VirtualBox
b 'password'
2025-12-14T14:28:58+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
2025-12-14T14:28:58+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:28:58+0000 [HoneyPotSSHTransport,5,192.168.11.142] Connection lost after 77.8 seconds
2025-12-14T14:29:08+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-ex
change-sha1
2025-12-14T14:29:08+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-ex
change-sha256
2025-12-14T14:29:08+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.11.142:59994
(172.17.0.2:2222) [session: c778ef1801f4]
2025-12-14T14:29:08+0000 [HoneyPotSSHTransport,6,192.168.11.142] Remote SSH version: SSH-2.0-OpenSSH
_10.2p1 Debian-3
2025-12-14T14:29:08+0000 [HoneyPotSSHTransport,6,192.168.11.142] SSH client hassh fingerprint: eeca2
460550b9ded084ecf2f70a75356
2025-12-14T14:29:08+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha2
56' key alg=b'ssh-ed25519'
2025-12-14T14:29:08+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b
'hmac-sha2-256' b'none'
2025-12-14T14:29:08+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b
'hmac-sha2-256' b'none'
2025-12-14T14:29:08+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2025-12-14T14:29:08+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-us
erauth'
2025-12-14T14:29:08+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'EVGENIY' trying aut
h b'none'
2025-12-14T14:29:13+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'EVGENIY' trying aut
h b'password'
2025-12-14T14:29:13+0000 [HoneyPotSSHTransport,6,192.168.11.142] Could not read etc/userdb.txt, defa
ult database activated
2025-12-14T14:29:13+0000 [HoneyPotSSHTransport,6,192.168.11.142] login attempt [b'EVGENIY'/b'Evgeniy
1123'] failed
2025-12-14T14:29:14+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'EVGENIY' failed aut
h b'password'
2025-12-14T14:29:14+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
```

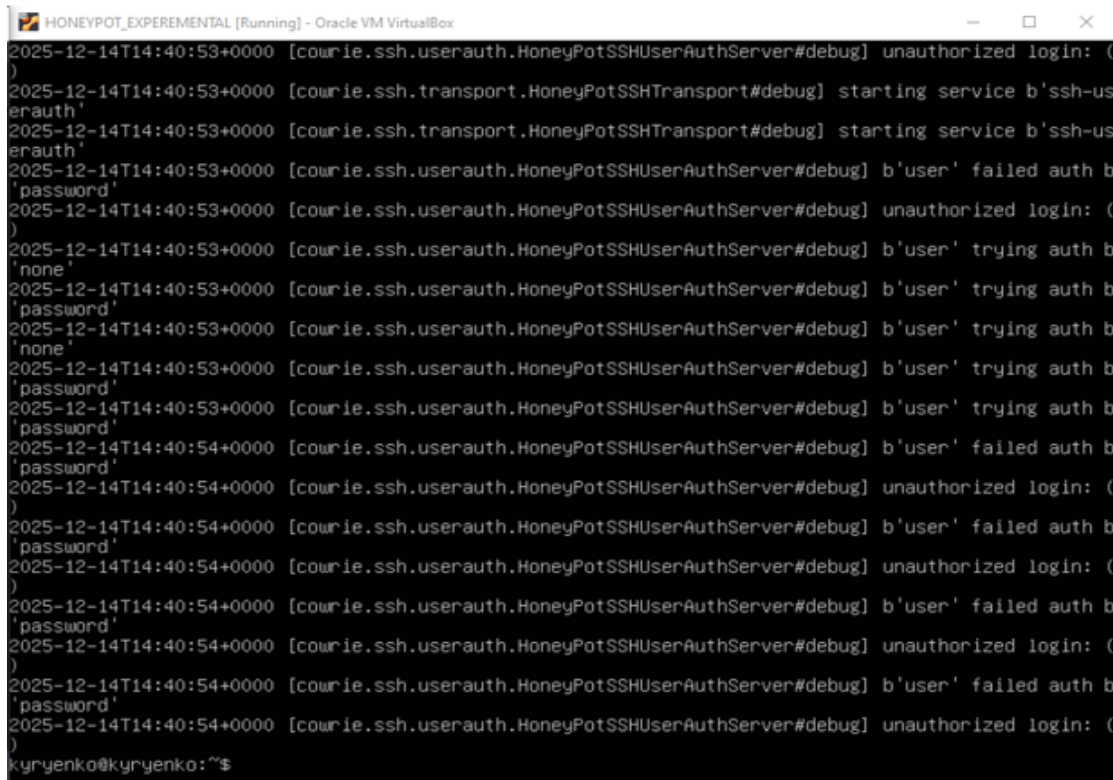
Рисунок 3.10 – Аналіз повторювальних подій атакуючого

```
HONEYPOT_EXPERIMENTAL [Running] - Oracle VM VirtualBox
2025-12-14T14:32:26+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-us
erauth'
2025-12-14T14:32:26+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'EVGENIY' trying aut
h b'none'
2025-12-14T14:32:26+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'EVGENIY' trying aut
h b'password'
2025-12-14T14:32:26+0000 [HoneyPotSSHTransport,9,192.168.11.142] Could not read etc/userdb.txt, defa
ult database activated
2025-12-14T14:32:26+0000 [HoneyPotSSHTransport,9,192.168.11.142] login attempt [b'EVGENIY'/b''] fail
ed
2025-12-14T14:32:27+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'EVGENIY' failed aut
h b'password'
2025-12-14T14:32:27+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
2025-12-14T14:32:27+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'EVGENIY' trying aut
h b'password'
2025-12-14T14:32:27+0000 [HoneyPotSSHTransport,9,192.168.11.142] Could not read etc/userdb.txt, defa
ult database activated
2025-12-14T14:32:27+0000 [HoneyPotSSHTransport,9,192.168.11.142] login attempt [b'EVGENIY'/b''] fail
ed
2025-12-14T14:32:28+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'EVGENIY' failed aut
h b'password'
2025-12-14T14:32:28+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
2025-12-14T14:32:36+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'EVGENIY' trying aut
h b'password'
2025-12-14T14:32:36+0000 [HoneyPotSSHTransport,9,192.168.11.142] Could not read etc/userdb.txt, defa
ult database activated
2025-12-14T14:32:36+0000 [HoneyPotSSHTransport,9,192.168.11.142] login attempt [b'EVGENIY'/b''] fail
ed
2025-12-14T14:32:37+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'EVGENIY' failed aut
h b'password'
2025-12-14T14:32:37+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
2025-12-14T14:32:37+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-12-14T14:32:37+0000 [HoneyPotSSHTransport,9,192.168.11.142] Connection lost after 10.5 seconds
```

Рисунок 3.11 – Аналіз повторювальних подій атакуючого

На основі проведеного аналізу було виокремлено основні ознаки кібератак у мережевій взаємодії з Honeypot-системою. До таких ознак належать багаторазові невдалі спроби автентифікації, використання стандартних або поширених облікових записів, висока інтенсивність підключень з одного джерела, а також виконання інформаційно-розвідувальних команд після

встановлення сесії. Сукупність цих ознак дозволяє з високою ймовірністю ідентифікувати атакуючу активність та відрізнити її від легітимних дій користувачів.



```
HONEYPOT_EXPERIMENTAL [Running] - Oracle VM VirtualBox
2025-12-14T14:40:53+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
2025-12-14T14:40:53+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-us
erauth'
2025-12-14T14:40:53+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-us
erauth'
2025-12-14T14:40:53+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' failed auth b
'password'
2025-12-14T14:40:53+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
2025-12-14T14:40:53+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b
'none'
2025-12-14T14:40:53+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b
'password'
2025-12-14T14:40:53+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b
'none'
2025-12-14T14:40:53+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b
'password'
2025-12-14T14:40:53+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' trying auth b
'password'
2025-12-14T14:40:54+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' failed auth b
'password'
2025-12-14T14:40:54+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
2025-12-14T14:40:54+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' failed auth b
'password'
2025-12-14T14:40:54+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
2025-12-14T14:40:54+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' failed auth b
'password'
2025-12-14T14:40:54+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
2025-12-14T14:40:54+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'user' failed auth b
'password'
2025-12-14T14:40:54+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: (
)
kyryenko@kyryenko:~$
```

Рисунок 3.12 – Аналіз введених даних від атакуючого

Результати аналізу підтвердили, що Honeypot-система Cowrie забезпечує ефективний збір та структурування даних про дії потенційних злоумисників. Отримані журнали подій можуть використовуватися для формування правил виявлення атак, побудови профілів поведінки злоумисників та інтеграції з іншими засобами моніторингу й аналізу безпеки (Рис.3.12).

Таким чином, проведений аналіз експериментальних даних засвідчив доцільність використання Honeypot-систем для виявлення та дослідження кібератак. Зібрані та проаналізовані дані створюють основу для подальшого вдосконалення механізмів виявлення загроз та підвищення рівня кібербезпеки інформаційних систем.

На завершальному етапі дослідження було здійснено оцінку ефективності розгорнутої Honeypot-системи з точки зору її здатності виявляти, фіксувати та

аналізувати кібератаки у мережевому середовищі. Оцінювання базувалося на результатах експериментів, проведених у попередніх підрозділах, а також на аналізі зібраних журналів подій Honeypot-системи Cowrie.

Результати експериментів показали, що Honeypot-система забезпечує стабільний та безперервний збір даних про спроби несанкціонованого доступу до сервісів віддаленого адміністрування. Система коректно реєструвала спроби автентифікації, включаючи використані облікові записи, паролі, часові мітки та IP-адреси джерел атак. Це дозволяє з високою точністю ідентифікувати джерела та характер атакуючої активності.

Важливою перевагою використаної Honeypot-системи є можливість аналізу поведінки зломисника після встановлення з'єднання. Реєстрація post-login активності, зокрема виконання інформаційно-розвідувальних команд, дає змогу не лише виявляти факт атаки, а й аналізувати подальші наміри атакуюльника. Такий підхід є особливо цінним для дослідження сценаріїв компрометації систем та побудови поведінкових моделей загроз.

Контейнеризоване розгортання Honeypot-системи за допомогою Docker забезпечило додатковий рівень ізоляції та безпеки експериментального середовища. Використання контейнерів дозволило уникнути проблем сумісності програмних компонентів, спростити процес розгортання та підвищити відтворюваність експериментів. З точки зору практичного застосування, такий підхід є доцільним для впровадження Honeypot-систем у корпоративних та хмарних середовищах.

Разом з тим, Honeypot-системи мають і певні обмеження. Вони не призначені для безпосереднього блокування атак та не замінюють традиційні засоби захисту, такі як міжмережеві екрани або системи запобігання вторгненням. Основна цінність Honeypot-систем полягає у зборі та аналізі інформації про загрози, що потребує подальшої обробки та інтеграції з іншими засобами кібербезпеки.

На основі проведеного дослідження можна сформулювати практичні рекомендації щодо використання Honeypot-систем у системах кібербезпеки:

- доцільним є застосування Honeypot-систем як додаткового інструмента моніторингу та раннього виявлення загроз;
- ефективність використання Honeypot значно зростає при інтеграції з системами централізованого збору та аналізу подій безпеки (SIEM);
- зібрані журнали подій можуть бути використані для формування правил виявлення атак та навчання аналітичних моделей;
- контейнеризація Honeypot-систем є рекомендованим підходом для забезпечення ізоляції та спрощення розгортання.

Таким чином, результати дослідження підтверджують, що Honeypot-система Cowrie є ефективним інструментом для виявлення та дослідження кібератак на сервіси віддаленого доступу. Її використання дозволяє отримувати цінну інформацію про методи та поведінку зловмисників, що може бути використано для підвищення рівня захищеності інформаційних систем та вдосконалення існуючих механізмів кібербезпеки.

Висновок до третього розділу:

У третьому розділі магістерської роботи було реалізовано практичну частину дослідження, спрямовану на оцінку ефективності Honeypot-системи в умовах, наближених до реальних. Для цього було розгорнуто експериментальне середовище на основі контейнеризованого Honeypot-рішення Cowrie, що забезпечило ізоляцію, відтворюваність експериментів та безпечне моделювання атакуючої активності. У межах проведених експериментів здійснено моделювання типових кібератак на сервіси віддаленого доступу, що дозволило дослідити реакцію Honeypot-системи на реальні сценарії несанкціонованого доступу.

Під час експериментальних досліджень Honeypot-система продемонструвала здатність до стабільного збору та детального журналювання даних про атакуючу активність. Було зафіксовано багаторазові спроби автентифікації, автоматизовані атаки типу brute-force, а також post-login активність зловмисників, що включала виконання розвідувальних команд та

спроби отримання інформації про систему. Це підтвердило ефективність використаного Honeypot-рішення для збору репрезентативних даних про поведінку атакувальників.

Аналіз отриманих журналів подій дозволив виокремити характерні ознаки кібератак, зокрема високу інтенсивність підключень, повторюваність використаних облікових даних, часові закономірності атак та типові сценарії дій злоумисників після успішної автентифікації. Отримані результати засвідчили можливість застосування статистичного, поведінкового та кореляційного аналізу для виявлення та класифікації атакувальної активності на основі даних Honeypot-системи.

Таким чином, у межах третього розділу було виконано завдання з організації експериментального середовища, моделювання кібератак, збору та аналізу експериментальних даних, а також оцінки аналітичних можливостей Honeypot-системи. Проведене дослідження підтвердило доцільність використання Honeypot-систем як ефективного інструмента виявлення, аналізу та дослідження кібератак, а також обґрунтувало можливість їх практичного застосування у комплексних системах кібербезпеки для підвищення рівня захищеності інформаційних ресурсів.

ВИСНОВКИ

У процесі виконання магістерської роботи досягнуто поставленої мети та повністю виконано визначені завдання, пов'язані з дослідженням і практичним застосуванням Honeypot-систем у сфері кібербезпеки.

Проведено аналіз сучасних підходів до забезпечення кібербезпеки, зокрема досліджено можливості застосування Honeypot-систем для виявлення кібератак. Встановлено, що Honeypot-системи є ефективним інструментом доповнення традиційних засобів захисту, оскільки дозволяють здійснювати цілеспрямований збір інформації про атакувальну активність, методи та поведінку зловмисників, а також сприяють виявленню нових і прихованих загроз.

Розроблено проєкт Honeypot-системи з урахуванням вимог безпеки та ізоляції й реалізовано модель такої системи для збору та журналювання даних про атакувальну активність. Реалізоване рішення забезпечує імітацію мережевих сервісів, контрольований рівень взаємодії зі зловмисником та ізоляцію від продуктивного середовища, що створює безпечні умови для накопичення та подальшого аналізу даних про кібератаки.

Проведено експериментальні дослідження з моделювання кібератак і аналізу отриманих результатів. Honeypot-система забезпечила стабільний збір та детальне журналювання інформації про спроби несанкціонованого доступу й автоматизовані атаки. Аналіз отриманих даних дозволив виокремити характерні ознаки кібератак, зокрема високу інтенсивність підключень, повторюваність використаних облікових даних, часові закономірності та типові сценарії поведінки зловмисників.

Отримані результати підтверджують доцільність використання Honeypot-систем у комплексних системах кібербезпеки. Практична цінність роботи полягає в можливості застосування розробленої моделі для підвищення рівня захищеності інформаційних систем, удосконалення процесів виявлення кібератак та використання в навчальних, корпоративних і дослідницьких середовищах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. AppinLab. (2025). What is HoneyPot in Cybersecurity? How it protects against cyber-attacks. AppinLab. URL: <https://appinindore.com/blogs/what-is-a-honeypot-in-cybersecurity-how-does-it-protect-against-cyber-attacks/> (веб-ресурс, дата звернення: 18.03.2025)
2. Fan, W., Du, Z., Fernández, D. (2015). Taxonomy of honeynet solutions. In: 2015 SAI Intelligent Systems Conference (IntelliSys), 1002–1009. doi:10.1109/IntelliSys.2015.7361266. (наукова стаття)
3. Franco, J., Aris, A., Canberk, B., Uluagac, A. S. (2021). A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems. IEEE Communications Surveys & Tutorials, 23, 2351–2383. doi:10.1109/COMST.2021.3106669. (наукова стаття)
4. HackYourMom. (2025). Посібники про HoneyPot. Від А до Я. URL: <https://hackyourmom.com/kibervijna/posibnyky-pro-honeypot-vid-a-do-ya/> (веб-ресурс, дата звернення: 18.03.2025)
5. Ionescu, S., & Chitea, R. (2019). A comprehensive review of honeypot technologies. International Journal of Computer Science and Information Security, 17(7), 29-41. (наукова стаття)
6. Matherly, J. (2022). HoneyPot or Not? URL: <https://honeyscore.shodan.io/> (веб-ресурс)
7. Pa, Y. M. P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., Rossow, C. (2016). IoT POT: A Novel HoneyPot for Revealing Current IoT Threats. Journal of Information Processing, 24, 522-533. doi:10.2197/ipsjip.24.522. (наукова стаття)
8. Pashaei, A., Akbari, M. E., Zolfy Lighvan, M., Charmin, A. (2022). Early Intrusion Detection System using honeypot for industrial control networks. Results in Engineering, 16, 100576. doi:10.1016/j.rineng.2022.100576. (наукова стаття)
9. Spitzner, L. (2003). HoneyPots: Tracking Hackers. Addison-Wesley Professional. ISBN 978-0321223645 (книга)

10. Tsikerdekis, M., Zeadally, S., Schlesener, A., Sklavos, N. (2018). Approaches for Preventing Honey-pot Detection and Compromise. In: 2018 Global Information Infrastructure and Networking Symposium (GIIS), 1–6. doi:10.1109/GIIS.2018.8635603. (наукова стаття)
11. Xiph Cyber. (2025). How honeypots enhance cyber security. Xiph Cyber - Smart. Safe. Secure. URL: <https://xiphcyber.com/articles/honeypots> (веб-ресурс, дата звернення: 18.03.2025)
12. Буряк, О. В., & Шеремет, І. В. (2016). Захист інформаційних систем за допомогою технологій Honey-pot. Збірник наукових праць "Безпека та захист інформації", 2, 33-42. (стаття в збірнику наукових праць)
13. Колеснікова, Н. А. (2017). Основи кібербезпеки в комп'ютерних мережах. Харків: ХНУРЕ, 2017. 215 с. ISBN 978-617-7027-29-2 (книга)
14. Ковальчук, А. С., & Рибалка, М. І. (2015). Технології кібербезпеки та захисту інформації. Київ: Наукова думка, 2015. 312 с. ISBN 978-966-00-2045-5 (книга)
15. Коваленко, О. В., & Макарова, О. М. (2021). Моделювання атак в інформаційних системах за допомогою honeypot-систем. Науковий вісник НТУУ «КПІ». Київ, 22(3), 88-97. (стаття в збірнику наукових праць)
16. A Practical Guide to Honey-pots. URL: <https://www.cs.wustl.edu/~jain/cse571-09/ftp/honey.pdf> (веб-ресурс)
17. Behl, A., & Behl, K. (2017). Cyberwar: The Next Threat to National Security and What to Do About It. Oxford University Press. ISBN 978-0190654957. (книга)
18. Krawetz, N. (2004). Anti-Honey-pot Technology. IEEE Security & Privacy, 2(1), 76–79. doi:10.1109/MSECP.2004.1264565. (наукова стаття)
19. Provos, N., & Holz, T. (2007). Virtual Honey-pots: From Botnet Tracking to Intrusion Detection. Addison-Wesley Professional. ISBN 978-0321336321. (книга)
20. Plohmann, D., Yakdan, K., Klatt, M., Bader, J., & Gerhards-Padilla, E. (2013). A Comprehensive Measurement Study of Malware. In: Detection of Intrusions

and Malware & Vulnerability Assessment (DIMVA). Springer. doi:10.1007/978-3-642-37300-8_2.

21. Zhang, Y., Xiao, Y., Chen, H., & Li, Y. (2014). A Survey of Honeypot Technologies. *International Journal of Computer Network and Information Security*, 6(8), 1–10. doi:10.5815/ijcnis.2014.08.01. (наукова стаття)

22. Cisco Systems. (2023). Deception Technologies and Honeypots in Modern Networks. Cisco Security White Paper. URL: <https://www.cisco.com> (веб-ресурс, дата звернення: 18.03.2025)