

АВТОМАТИЗОВАНА СИСТЕМА ІЗОЛЬОВАНИХ ІМІТАЦІЙНИХ СЕРЕДОВИЩ ДЛЯ ДОСЛІДЖЕННЯ КІБЕРЗАГРОЗ

У статті розглянуто питання застосування технологій Cyber Deception для дослідження сучасних кіберзагроз та аналізу дій потенційних кіберзловмисників. Обґрунтовано актуальність використання систем-приманок (honeypot) як ефективного засобу збору інформації про спроби несанкціонованого доступу до інформаційних систем, дослідження сучасних методів проведення кібератак та вдосконалення механізмів забезпечення кібербезпеки. Показано, що застосування технологій кіберобману дозволяє створювати контрольовані імітаційні середовища, у яких можливо досліджувати поведінку потенційних зловмисників без ризику компрометації реальної інформаційної інфраструктури.

Метою дослідження є аналіз технологій побудови ізольованих імітаційних середовищ та розроблення лабораторної системи для дослідження кіберзагроз із використанням honeypot-технологій. У роботі проведено аналіз сучасних підходів до побудови систем Cyber Deception, класифікації honeypot за рівнем взаємодії із зловмисником, особливостей їх використання в системах кібербезпеки, а також можливостей застосування таких систем у дослідницькому та навчальному процесах. Запропоновано архітектуру лабораторного середовища на базі віртуальної інфраструктури з використанням системи Cowrie, реалізовано автоматизований збір журналів подій та забезпечено можливість моніторингу спроб несанкціонованого доступу, фіксації процесів автентифікації, виконуваних команд і подальшого аналізу дій потенційних кіберзловмисників.

За результатами експериментальних досліджень встановлено, що переважна більшість зафіксованих атак має автоматизований характер і реалізується шляхом використання типових сценаріїв компрометації інформаційних систем, зокрема словникового підбору паролів, застосування стандартних облікових записів та виконання команд після успішної автентифікації. Показано, що використання honeypot забезпечує накопичення експериментальних даних про сучасні методи проведення кібератак, дозволяє досліджувати тактики та інструменти, які застосовують потенційні кіберзловмисники, а також підвищує ефективність аналізу журналів подій інформаційної безпеки.

Практична цінність роботи полягає у створенні лабораторного середовища, яке може використовуватися для проведення наукових досліджень у сфері кібербезпеки, тестування засобів виявлення атак, накопичення даних для вдосконалення механізмів моніторингу та реагування на кіберінциденти, а також під час підготовки фахівців з кібербезпеки. Запропоноване рішення може слугувати основою для подальшої інтеграції із системами класу SIEM, розширення функціональних можливостей лабораторних стендів і розвитку сучасних засобів проактивного захисту інформаційних систем.

Ключові слова: кібербезпека, інформаційна безпека, Cyber Deception, honeypot, кіберзагрози, аналіз атак, імітаційне середовище.

Вступ та постановка проблеми. У сучасних умовах цифрової трансформації більшість організацій зберігає критично важливі дані на серверних платформах, що робить їх привабливими цілями для кіберзлочинців. Зростання кількості кібератак, поява нових інструментів компрометації та постійне ускладнення їх реалізації вимагають удосконалення підходів до забезпечення кібербезпеки та своєчасного виявлення потенційних загроз.

Дослідження сучасних кібератак неможливе лише на основі теоретичних моделей. Для розуміння механізмів їх реалізації необхідно аналізувати практичні сценарії поведінки зловмисників у контрольованому середовищі. Саме тому в наукових дослідженнях і

навчальному процесі широко використовуються спеціалізовані лабораторні стенди, які дають змогу відтворювати типові сценарії атак, досліджувати їх перебіг та оцінювати ефективність засобів захисту.

Одним із найбільш поширених інструментів такого дослідження є технологія *honeypot*, що являє собою спеціалізований програмно-апаратний ресурс, котрий виконує роль приманки для потенційних зломисників. Зовні *honeypot* імітує функціонування реального сервера або іншого мережевого сервісу, створюючи у нападника враження про наявність вразливої системи. Під час взаємодії із цією системою всі дії зломисника фіксуються та реєструються для подальшого аналізу.

Отримані дані дають можливість досліджувати тактики, техніки та процедури, які використовують атакуючі, виявляти нові тенденції розвитку кіберзагроз і вдосконалювати механізми захисту інформаційних систем. Такий підхід забезпечує перехід від реактивних методів захисту до проактивного аналізу загроз, що особливо важливо в умовах постійної еволюції кіберзлочинної діяльності.

Аналіз останніх досліджень і публікацій. Питання виявлення, аналізу та прогнозування кіберзагроз активно досліджуються як у вітчизняній, так і в зарубіжній науковій літературі. Значна увага приділяється розробленню методів моніторингу мережевої активності, аналізу кіберінцидентів, побудові систем раннього виявлення атак і використанню спеціалізованих середовищ для дослідження поведінки зломисників.

У працях [1, 2] розглянуто базові принципи захисту інформації в мережевих середовищах, зокрема методи виявлення кіберзагроз, аналізу атак, контролю доступу та моніторингу мережевої інфраструктури. Представлені підходи формують теоретичне підґрунтя сучасних систем забезпечення інформаційної безпеки, включаючи засоби моніторингу, аудиту та управління подіями безпеки. Окрему увагу автори приділяють аналізу дій зломисників як важливому джерелу даних для підтримки прийняття рішень у сфері кібербезпеки.

У роботах [3, 4] досліджено питання управління ризиками, формування політик інформаційної безпеки, захисту мережевої інфраструктури, протидії кіберзагрозам, а також особливості побудови систем моніторингу та виявлення атак. Автори наголошують на доцільності постійного моніторингу дій зломисників з метою накопичення даних для вдосконалення механізмів виявлення та протидії сучасним кібератакам.

Праці [5, 6] присвячено комплексному дослідженню принципів побудови, впровадження та експлуатації систем виявлення і запобігання вторгненням (IDPS) у сучасних інформаційно-телекомунікаційних системах. У них наведено класифікацію IDPS за місцем розташування та способом аналізу подій, зокрема мережевих (NIDPS), хостових (HIDPS), бездротових (WIDPS) систем, а також систем аналізу поведінки мережі (NBA). Значну увагу приділено методам виявлення атак на основі сигнатурного аналізу, аналізу аномалій та специфікацій мережевих протоколів. Також у роботі наведено рекомендації щодо вибору архітектури системи з урахуванням особливостей інформаційної інфраструктури та вимог до забезпечення кібербезпеки.

У дослідженні [7] розглянуто проблему атрибуції кібератак, тобто визначення їхнього можливого джерела. Це завдання належить до найбільш складних у сфері кібербезпеки, оскільки сучасні кіберінциденти зазвичай характеризуються багаторівневою структурою та використанням різних механізмів приховування слідів атаки. Показано, що ефективне виявлення таких інцидентів і своєчасне реагування на них потребують комплексного аналізу даних із різних джерел, автоматизованої обробки подій безпеки та оцінювання ризиків у режимі реального часу.

У роботі [8] увагу зосереджено на використанні спеціалізованих систем-приманок (*honeypots*) для виявлення та дослідження дій потенційних зломисників. *Honeypot* розглядається як імітаційний інформаційний ресурс, який відтворює ознаки потенційно вразливої системи та стимулює взаємодію з боку атакуючих. Застосування таких рішень дає змогу не лише фіксувати факти несанкціонованої активності, а й отримувати детальну

інформацію про інструменти, тактики та методи, що використовуються під час проведення кібератак.

Незважаючи на значну кількість досліджень, присвячених системам виявлення вторгнень, платформам SIEM та технологіям honeypot, питання побудови комплексних лабораторних середовищ залишаються недостатньо висвітленими. Особливо це стосується рішень, які поєднують емуляцію кібератак, використання систем-приманок, централізований збір і кореляцію подій безпеки, а також їх подальший аналіз у навчальних і дослідницьких цілях. Саме ця обставина визначила напрям дослідження та обумовила необхідність розроблення відповідного лабораторного середовища.

Метою статті є дослідження технологій побудови ізольованих імітаційних середовищ та розроблення комплексної лабораторної системи для виявлення, моніторингу й аналізу кіберзагроз із використанням технології honeypot та засобів централізованого збору й аналізу подій інформаційної безпеки.

Виклад основного матеріалу. Сучасні інформаційні системи функціонують в умовах постійного зростання кількості та складності кіберзагроз. Зловмисники регулярно вдосконалюють інструменти та методи проведення атак, використовуючи нові способи отримання несанкціонованого доступу до інформаційних ресурсів, компрометації даних або порушення роботи цифрових сервісів. Різноманіття таких загроз охоплює кілька основних категорій, кожна з яких характеризується власними механізмами реалізації та потенційними наслідками для інформаційної безпеки.

Серед найбільш поширених загроз особливе місце займає шкідливе програмне забезпечення (Malware), до складу якого входять комп'ютерні віруси, троянські програми, шпигунське програмне забезпечення (Spyware) та програми-вимагачі (Ransomware). Функціональні можливості таких програм можуть істотно відрізнятися залежно від цілей атаки. Одні з них орієнтовані на викрадення облікових даних і конфіденційної інформації, інші забезпечують приховане керування скомпрометованою системою або порушують її нормальне функціонування. Окрему небезпеку становлять програми-вимагачі, які шифрують дані користувача та вимагають сплати викупу за відновлення доступу до них.

Окрему категорію кіберзагроз становлять розподілені атаки типу відмови в обслуговуванні (Distributed Denial of Service, DDoS), які є одними з найбільш поширених засобів порушення доступності інформаційних сервісів. Принцип їх реалізації полягає у формуванні великої кількості одночасних запитів до цільового ресурсу з множини скомпрометованих пристроїв. Унаслідок перевантаження обчислювальних і мережевих ресурсів сервер втрачає здатність обслуговувати легітимні запити користувачів, що призводить до часткового або повного припинення його функціонування.

Окрему групу загроз становлять вразливості програмного забезпечення, що виникають через помилки проектування, реалізації або налаштування інформаційних систем. Саме такі недоліки нерідко стають точкою входу для зловмисників. Їх експлуатація може призвести до отримання несанкціонованого доступу до ресурсів системи, виконання довільного програмного коду, розширення привілеїв користувача або порушення цілісності та доступності даних.

Практика останніх років свідчить, що зі зростанням складності кібератак традиційні засоби захисту вже не завжди здатні забезпечити необхідний рівень безпеки. Навіть за наявності антивірусного програмного забезпечення та мережевих засобів фільтрації частина атак залишається непоміченою або виявляється вже після компрометації системи. Тому дедалі більшого значення набувають проактивні підходи, орієнтовані не лише на виявлення та блокування загроз, а й на вивчення поведінки самих атакуючих. Дослідження тактик, технік і процедур, які використовуються під час атак, дає змогу краще розуміти механізми їх реалізації, своєчасно виявляти нові вектори компрометації та вдосконалювати засоби захисту.

У цьому контексті особливий інтерес становлять технології Cyber Deception (кіберобману), які дають можливість досліджувати дії потенційних зловмисників у контрольованому середовищі. На відміну від традиційних засобів захисту, основною метою

яких є запобігання несанкціонованому доступу, технології кіберобману створюють спеціально підготовлені об'єкти, що зовні не відрізняються від реальних серверів, сервісів або інформаційних ресурсів. Взаємодіючи з такими об'єктами, атакуючий фактично розкриває свої наміри, інструменти та методи роботи. Це дозволяє отримувати цінні дані про сценарії атак без ризику для реальної інформаційної інфраструктури.

Одним із найпоширеніших практичних інструментів реалізації концепції Cyber Deception є технологія honeypot. Такі системи виконують роль приманки, привертаючи увагу потенційних зломисників і фіксуючи їхню активність. Зібрані журнали подій та результати спостережень можуть використовуватися для вдосконалення механізмів виявлення атак, підвищення ефективності реагування на кіберінциденти, а також для навчання та підготовки фахівців у сфері кібербезпеки.

На сьогодні технології Cyber Deception реалізуються за допомогою кількох основних засобів (рис. 1):

- *Honeypot* – окремий інформаційний ресурс або сервер-приманка, призначений для виявлення та аналізу дій потенційних кіберзломисників.
- *Honeynet* – сукупність взаємопов'язаних систем-приманок, що імітують функціонування реального сегмента мережі та забезпечують дослідження складних сценаріїв кібератак.
- *Honeytokens* – спеціально створені цифрові артефакти (облікові записи, паролі, документи, ключі доступу тощо), використання яких свідчить про несанкціонований доступ до інформаційної системи.
- *Deception Files* (файли-приманки) – спеціально сформовані файли та каталоги, що імітують конфіденційну інформацію і призначені для виявлення несанкціонованих спроб доступу.



Рисунок 1 – Класифікація імітаційних систем у кібербезпеці

Основне призначення технологій кіберобману полягає у відверненні уваги потенційного зломисника від реальних інформаційних ресурсів і спрямуванні його дій до спеціально підготовленого контрольованого середовища. Такий підхід дає можливість простежити перебіг атаки на всіх її етапах, дослідити інструменти та методи, які використовує атакуючий, а також накопичити дані, необхідні для вдосконалення механізмів захисту інформаційних систем.

Серед рішень, що реалізують концепцію Cyber Deception, найбільш поширеними є системи *honeypot*. Вони широко застосовуються як у наукових дослідженнях, так і в практиці забезпечення кібербезпеки. Принцип їх роботи ґрунтується на створенні середовища, яке зовні

нагадує реальну інформаційну систему та спонукає атакуючого до активних дій. Будь-яка взаємодія з таким ресурсом реєструється, що створює можливість для подальшого аналізу застосованих інструментів, способів компрометації та характерних сценаріїв проведення атак.

Однією з ключових переваг honeypot є можливість спостерігати за діями зловмисника після проникнення до імітованого середовища. Якщо традиційні засоби захисту переважно орієнтовані на попередження або блокування атаки, то системи-приманки дозволяють вивчати весь ланцюг подій від моменту отримання доступу до виконання подальших дій у скомпрометованій системі. Завдяки цьому можна досліджувати використовувані інструменти, способи експлуатації вразливостей та логіку розвитку кіберінциденту.

Залежно від рівня взаємодії з атакуючим honeypot традиційно поділяють на дві основні категорії: системи низької взаємодії (Low-Interaction Honeypots) і системи високої взаємодії (High-Interaction Honeypots). Перший тип забезпечує емуляцію окремих сервісів або мережних протоколів і використовується переважно для виявлення масових та типових атак. Другий тип відтворює повноцінне програмне середовище, що дозволяє отримувати значно більше інформації про поведінку зловмисника та досліджувати складні сценарії компрометації. Водночас такі рішення потребують ретельнішої ізоляції та контролю через підвищений рівень ризику.

Системи низької взаємодії відтворюють лише окремі мережеві служби або протоколи, не надаючи зловмиснику доступу до повноцінного операційного середовища. Завдяки цьому вони залишаються відносно простими в розгортанні та супроводі, а також характеризуються нижчим рівнем ризику порівняно з рішеннями високої взаємодії.

Системи високої взаємодії імітують повноцінні операційні системи та дозволяють атакуючому взаємодіяти з ними майже так само, як із реальною системою. Такі системи дають можливість отримувати більш детальну інформацію про методи атак, але водночас потребують більш складного адміністрування.

Метою розроблення є створення автоматизованої системи ізольованих імітаційних цільових середовищ, призначеної для дослідження різних типів кіберзагроз у контрольованих умовах. Така система повинна відтворювати окремі елементи реальної інформаційної інфраструктури та забезпечувати реєстрацію дій потенційних зловмисників під час взаємодії з імітованими ресурсами.

Архітектура системи передбачає використання кількох взаємопов'язаних компонентів, які функціонують у межах ізольованої мережі. Такий підхід дає змогу безпечно відтворювати сценарії кібератак, спостерігати за поведінкою атакуючих та аналізувати наслідки їхніх дій без загрози для реальної інформаційної інфраструктури. Ізоляція середовища забезпечує контроль над перебігом експериментів і створює умови для дослідження як типових, так і більш складних сценаріїв компрометації інформаційних систем.

Основними компонентами запропонованої системи є:

- система віртуалізації;
- honeypot-сервер;
- система генерації атак;
- сервер збору логів;
- система аналізу отриманих даних.

Система віртуалізації використовується для створення лабораторного середовища, у якому розгортаються всі компоненти системи. Наприклад, можна використовувати платформу Oracle VirtualBox, яка дозволяє створювати віртуальні машини та налаштовувати ізольовані мережі [9].

Honeypot-сервер – це приманка. Він імітує реальний сервер і має виглядати для кіберзловмисника максимально цікавою здобиччю. Завдання такого сервера – заманити зловмисника і записувати кожен його крок.

Система генерації атак – це тестова система для перевірки захисту. Для цієї ролі була обрана система Kali Linux [10]. Вона стандартно містить доволі широкий набір інструментів для проведення тестів на проникнення.

Сервер збору логів (Log Server) – це таке собі сховище дій зловмисника. Сюди стікається вся інформація про те, що відбувалося під час атак. По суті, це база для подальшого аналізу: хто заходив, які команди вводив і що намагався зламати [11].

Таким чином, запропонована архітектура автоматизованої системи для створення контрольованого середовища базується на використанні ізольованої мережі, у якій всі компоненти взаємодіють між собою (рис. 2).

На рисунку показана загальна схема: тут є вузол для атак на базі Kali Linux, сам Honeypot, сервер для логів (Log Server) і окрема частина для аналізу отриманих даних. У цій архітектурі honeypot-сервер – це центр усієї системи. Саме він приймає на себе всі з'єднання і фіксує, що там робить кіберзловмисник. Kali Linux виступає в ролі агресора і проводить тестові атаки на honeypot-сервер, а в цей час сервер логування "тихо" збирає та фіксує всі події, що відбуваються в мережі.

Для реалізації сервера-приманки був обраний Honeypot-сервер Cowrie. Він добре імітує SSH та Telnet сервіси і дозволяє повністю записувати все, що робить атакуючий у системі [12].

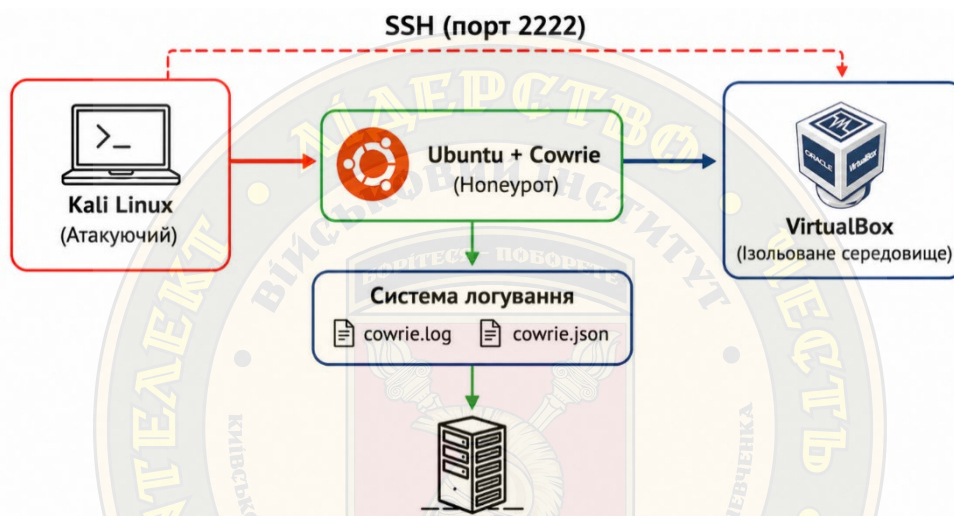


Рисунок 2 – Архітектура автоматизованої honeypot-системи

Встановлення та налаштування honeypot-системи [13].

Спочатку було встановлено ізольоване середовище Python (venv), що дозволило уникнути конфліктів пакетів. Процес встановлення:

```
git clone https://github.com/cowrie/cowrie
cd cowrie
```

```
python3 -m venv cowrie-env
source cowrie-env/bin/activate
pip install -upgrade pip
pip install -r requirements.txt
```

Після цього було встановлено тестові залежності за допомогою стандартного шаблону конфігурації: `cp etc/cowrie.cfg.dist etc/cowrie.cfg`.

У самому файлі `cowrie.cfg` було змінено кілька основних моментів – ім'я хосту, щоб сервер виглядав звичайно, а не як незвичайний або небезпечний. Також було зроблено налаштування параметрів емуляції SSH та перевірка запису логів, щоб їх було зручно переглядати та аналізувати. Сам сервер запускається через скрипт `bin/cowrie start`. За замовчуванням, він працює на порті 2222, тому була створена служба `systemd`, щоб система працювала автономно у фоні. Це усуває необхідність кожного разу запускати службу вручну після перезавантаження.

```
sudo systemctl daemon-reload
sudo systemctl enable cowrie
sudo systemctl start cowrie
```

Перевірка через `systemctl status cowrie` показала, що все поєдналось нормально, служба активна і працює у фоновому режимі.

Проведення тестових атак (рис. 3).

Для перевірки працездатності honeypot-системи були проведені тестові атаки з використанням Kali Linux. На першому етапі дослідження за допомогою Nmap були проскановані відкриті порти:

```
nmap -p 2222 <IP-адреса honeypot>
```

Результат сканування підтвердив наявність відкритого SSH-порту, що імітується honeypot-системою.

Далі було виконано атаку типу *brute-force* за допомогою утиліти Hydra:

```
hydra -l root -P passwords.txt ssh://<IP>:2222
```

Під час атаки виконувалися спроби підбору паролів із використанням словника. Honeypot-система не блокує доступ, а навпаки, дозволяє атакуючому "успішно" увійти в систему, імітуючи роботу реального сервера.

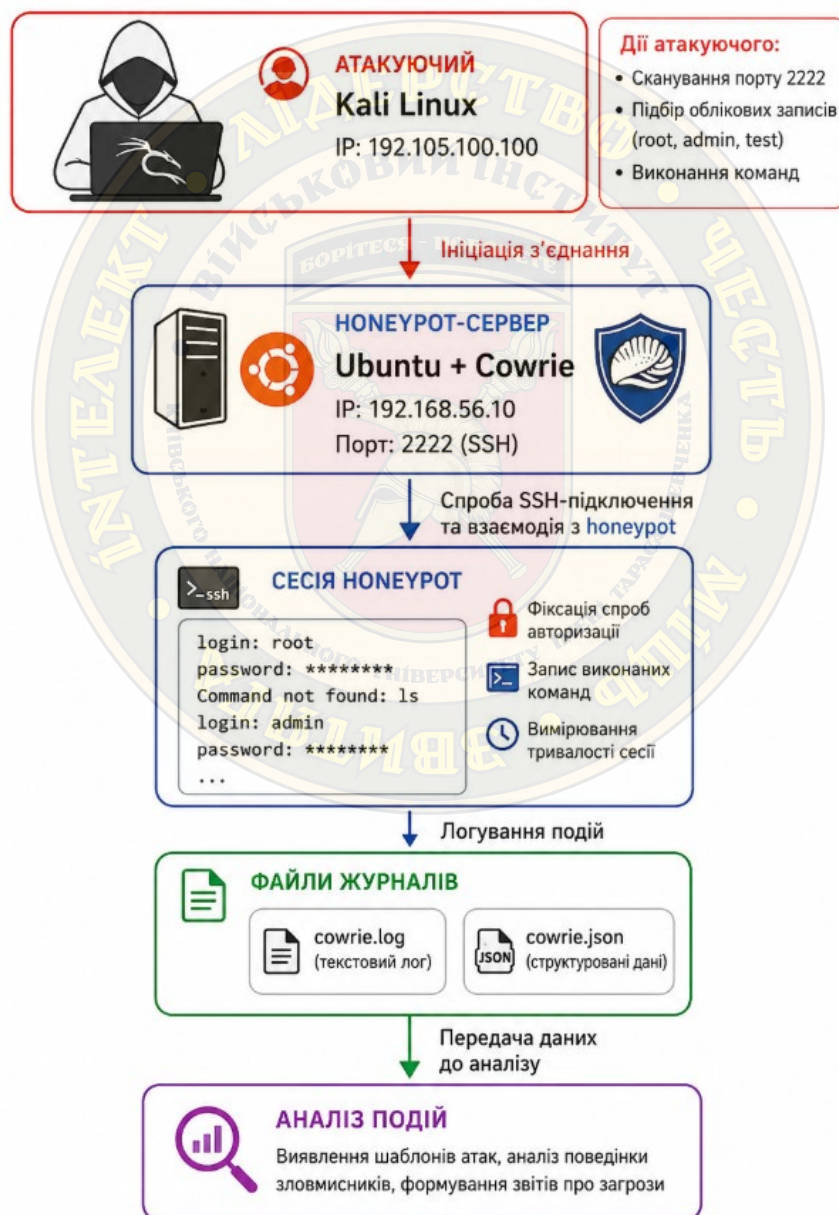


Рисунок 3 – Схема проведення тестової атаки та фіксації подій у honeypot-системі

Збір та аналіз журналів подій (рис. 4).

Однією з ключових функцій honeypot-системи є збір інформації про дії атакуючого. У системі Cowrie всі події записуються до двох основних журналів:

- cowrie.log – текстовий лог;
- cowrie.json – структурований лог у форматі JSON.

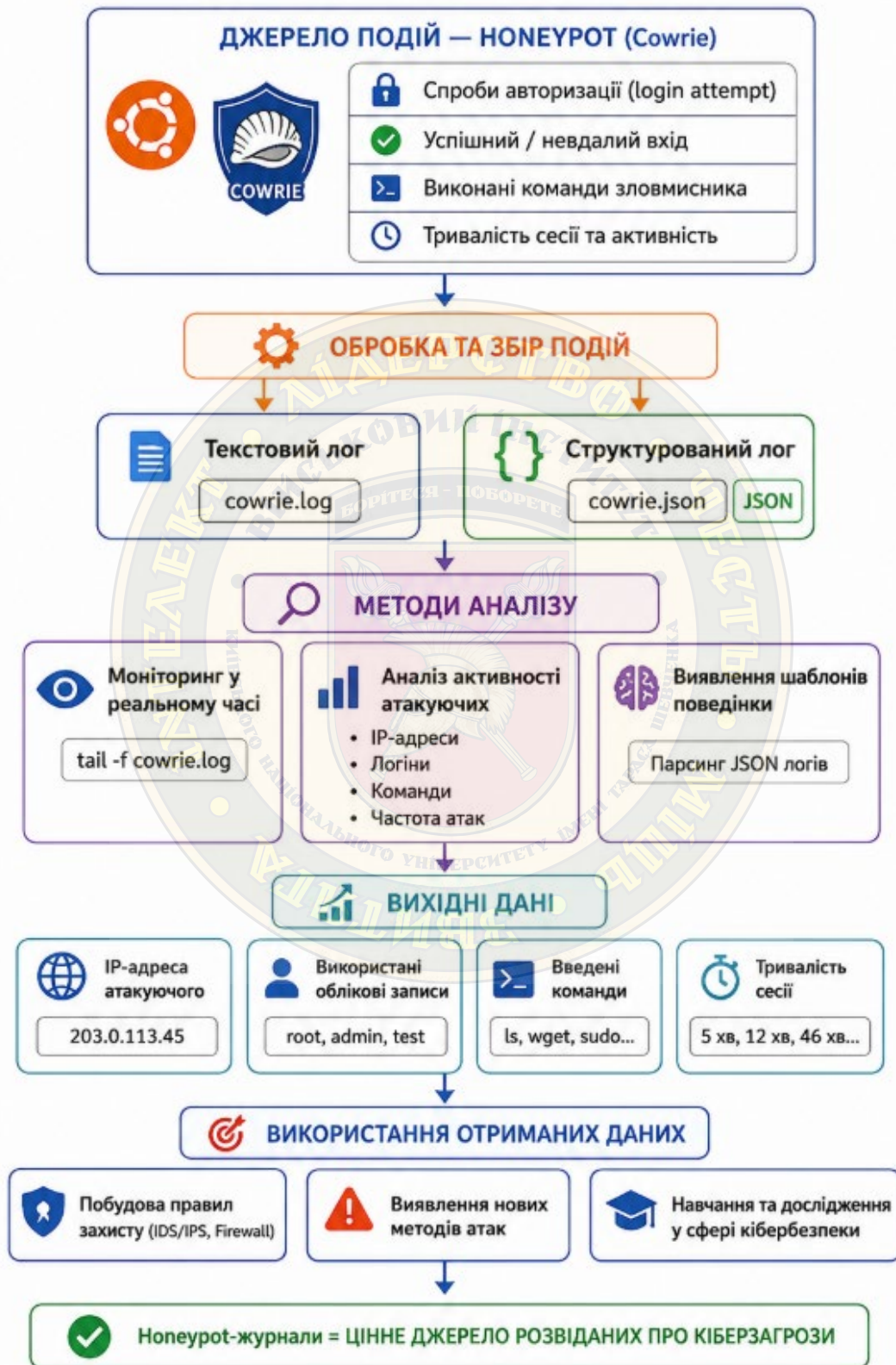


Рисунок 4 – Структура збору та аналізу журналів подій honeypot-системи

Для перегляду журналів у реальному часі використовується команда:

```
tail -f ~/cowrie/var/log/cowrie/cowrie.log
```

У журналах фіксуються такі події:

- IP-адреса атакуючого;
- спроби авторизації;
- використані логіни та паролі;
- введені команди;
- тривалість сесії;
- мережеві параметри підключення.

Завдяки цьому можна побачити повну картину дій зловмисника у системі.

Аналіз результатів експерименту.

У результаті проведених експериментальних досліджень було отримано інформацію про спроби несанкціонованого доступу до лабораторної honeypot-системи та особливості поведінки потенційних кіберзловмисників.

Аналіз зареєстрованих подій дав змогу встановити:

- наявність значної кількості спроб підключення до сервісу **SSH**;
- використання типових облікових записів, зокрема *root* та *admin*, під час спроб автентифікації;
- застосування словникових атак (Dictionary Attack) для автоматизованого підбору паролів;
- виконання команд операційної системи після успішної автентифікації, що свідчить про спроби подальшої компрометації інформаційної системи.

Отримані результати підтверджують, що більшість зафіксованих атак є автоматизованими та розгортаються за типовими сценаріями компрометації інформаційних систем. Завдяки honeypot вдалося детально зареєструвати кожен етап взаємодії зловмисника із системою – від спроб автентифікації та використаних облікових записів до виконаних команд і послідовності дій.

Дослідження довело ефективність honeypot як інструмента збору даних про сучасні кіберзагрози. Отримані експериментальні дані придатні для вдосконалення механізмів виявлення атак, розробки правил кореляції подій у SIEM-системах, посилення засобів захисту інформації та підготовки фахівців з кібербезпеки.

Автоматизація збору та аналізу журналів подій (рис. 5).

Щоб підвищити ефективність лабораторної системи, було налаштовано автоматизований збір і збереження журналів подій honeypot-системи Cowrie. Під час роботи система автоматично реєструє спроби несанкціонованого доступу, автентифікації, виконання команд та інші дії потенційних зловмисників.

Автоматизований збір логів дає змогу моніторити події в режимі реального часу, накопичувати історію кібератак та аналізувати поведінку нападників. Це створює підґрунтя для дослідження сучасних сценаріїв атак, виявлення індикаторів компрометації інформаційних систем і формування бази даних для подальших розробок.

Для забезпечення безперервного функціонування лабораторної системи використано механізми служби systemd, що дозволяють автоматизувати запуск сервісів, контролювати їх працездатність та забезпечувати автоматичне відновлення роботи після можливих збоїв.

Зібрані журнали подій слугують цінним джерелом даних для побудови систем виявлення кібератак, дослідження методів проникнення, удосконалення правил кореляції в SIEM-системах і навчання моделей кіберзахисту. Узагальнення та аналіз цих даних дають змогу своєчасно виявляти нові тенденції розвитку кіберзагроз і підвищувати ефективність захисних механізмів.

Отже, розроблена лабораторна система не лише автоматизує збір і реєстрацію подій інформаційної безпеки, а й створює основу для комплексного аналізу кібератак, удосконалення засобів виявлення загроз та розвитку технологій захисту.

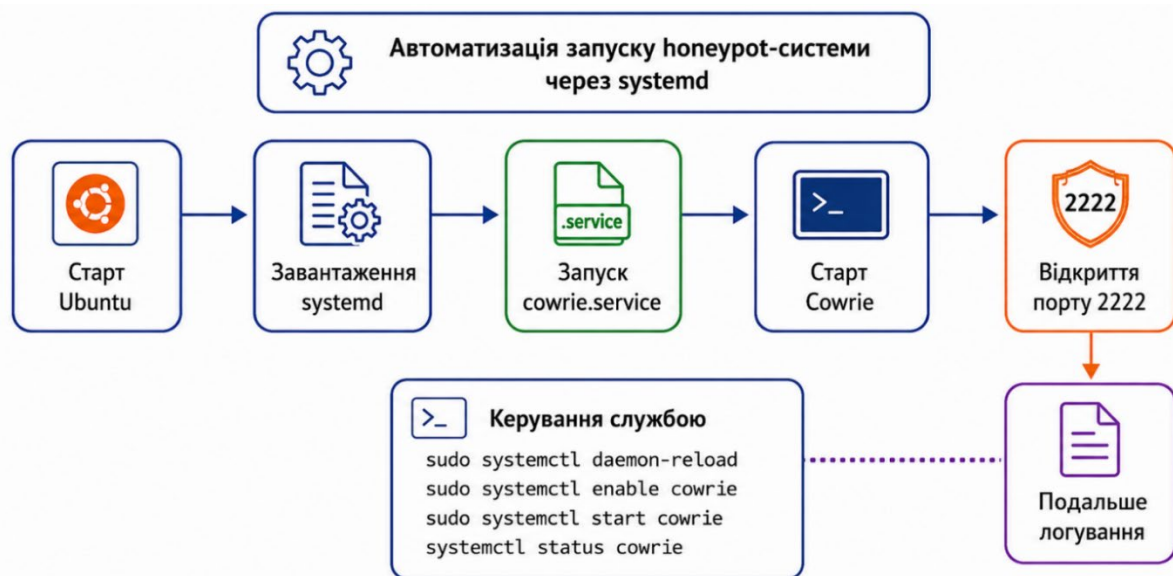


Рисунок 5 – Схема автоматизованого запуску honeypot-системи через *systemd*

Висновки. У роботі досліджено сучасні підходи до побудови ізольованих імітаційних середовищ для аналізу кіберзагроз, а також особливості застосування технологій Cyber Desorption у системах забезпечення кібербезпеки. Аналіз показав, що системи-приманки (honeypot) є ефективним інструментом проактивного виявлення та дослідження сучасних кібератак, що дає змогу збирати достовірні дані про тактики, техніки й процедури кіберзловмисників без ризику для реальної інформаційної інфраструктури.

У межах дослідження розроблено та реалізовано лабораторну систему на основі honeypot Cowrie, яка моделює мережеві сервіси, автоматизовано збирає журнали подій і дозволяє досліджувати поведінку потенційних зловмисників. Реалізована система реєструє спроби несанкціонованого доступу, фіксує процеси автентифікації, виконані команди та інші дії, характерні для розвитку кібератаки.

Експериментальні дослідження підтвердили працездатність запропонованого рішення. Переважна більшість зафіксованих атак має автоматизований характер і здійснюється за типовими сценаріями компрометації інформаційних систем – насамперед шляхом словникового підбору паролів та використання стандартних облікових записів. Отримані результати демонструють ефективність honeypot для дослідження сучасних методів несанкціонованого доступу та накопичення експериментальних даних про кіберінциденти.

Практична цінність роботи полягає у створенні лабораторного середовища, придатного для дослідження нових кіберзагроз, тестування засобів виявлення атак, удосконалення правил кореляції подій у SIEM-системах, а також для використання у навчальному процесі під час підготовки фахівців з кібербезпеки.

Перспективним напрямом подальших досліджень вважаємо інтеграцію розробленої honeypot-системи із сучасними платформами моніторингу та управління подіями інформаційної безпеки (SIEM), застосування методів машинного навчання для автоматичного аналізу журналів подій, а також розширення функціональних можливостей лабораторного середовища шляхом реалізації багаторівневої архітектури.

ЛІТЕРАТУРА:

1. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. New York : Pearson, 2017. 456 p.
2. Bishop M. Computer Security: Art and Science. 2nd ed. Boston : Addison-Wesley, 2019. 1312 p.
3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis : John Wiley & Sons, 2020. 1200 p.

4. Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5): National Institute of Standards and Technology. 2020. 492 p.
5. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS): NIST Special Publication 800-94. Gaithersburg: National Institute of Standards and Technology, 2007. 127 p.
6. Skoudis E., Liston T. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. 2nd ed. Upper Saddle River: Prentice Hall, 2005. 784 p.
7. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2014. 320 p.
8. Spitzner L. Honeypots: Tracking Hackers. Boston: Addison-Wesley, 2002. 480 p.
9. Oracle VM VirtualBox User Manual: official documentation. URL: <https://www.virtualbox.org/manual/>.
10. Kali Linux Documentation: official website. URL: <https://www.kali.org/docs/>.
11. Lyon G. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. URL: <https://nmap.org>.
12. Cowrie Honeypot Documentation: documentation project. URL: <https://cowrie.readthedocs.io>.
13. OWASP Foundation. Web Security Testing Guide (WSTG): official project page. URL: <https://owasp.org/www-project-web-security-testing-guide/>.

REFERENCES:

1. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. New York : Pearson, 2017. 456 p.
2. Bishop M. Computer Security: Art and Science. 2nd ed. Boston : Addison-Wesley, 2019. 1312 p.
3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis : John Wiley & Sons, 2020. 1200 p.
4. Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5): National Institute of Standards and Technology. 2020. 492 p.
5. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS): NIST Special Publication 800-94. Gaithersburg: National Institute of Standards and Technology, 2007. 127 p.
6. Skoudis E., Liston T. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. 2nd ed. Upper Saddle River: Prentice Hall, 2005. 784 p.
7. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2014. 320 p.
8. Spitzner L. Honeypots: Tracking Hackers. Boston: Addison-Wesley, 2002. 480 p.
9. Oracle VM VirtualBox User Manual: official documentation. URL: <https://www.virtualbox.org/manual/>.
10. Kali Linux Documentation: official website. URL: <https://www.kali.org/docs/>.
11. Lyon G. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. URL: <https://nmap.org>.
12. Cowrie Honeypot Documentation: documentation project. URL: <https://cowrie.readthedocs.io>.
13. OWASP Foundation. Web Security Testing Guide (WSTG): official project page. URL: <https://owasp.org/www-project-web-security-testing-guide/>.

PhD Hakhovych S., Babuch T., PhD Savchenko T., Derkach E.

AUTOMATED SYSTEM OF ISOLATED EMULATION ENVIRONMENTS FOR CYBER THREAT RESEARCH

The article examines the application of Cyber Deception technologies for the investigation of modern cyber threats and the analysis of the behavior of potential cyber attackers. The relevance of using honeypot systems as an effective tool for collecting information on unauthorized access attempts, studying contemporary cyberattack techniques, and improving cybersecurity mechanisms is substantiated. It is demonstrated that Cyber Deception technologies enable the creation of controlled emulation environments in which the behavior of potential attackers can be investigated without compromising real information infrastructure.

The purpose of this study is to analyze technologies for constructing isolated emulation environments and to develop a laboratory system for cyber threat research based on honeypot technologies. The paper presents an analysis of current approaches to the development of Cyber Deception systems, the classification of honeypots according to the level of attacker interaction, the specific features of their application in cybersecurity systems, and their potential use in research and educational activities. An architecture of a laboratory environment based on a virtual infrastructure using the Cowrie honeypot system is proposed. The developed solution provides automated event log collection and enables continuous monitoring of unauthorized access attempts, authentication processes, executed commands, and subsequent analysis of attacker activities.

Experimental evaluation demonstrated that the vast majority of recorded attacks were automated and followed common compromise scenarios, including dictionary-based password guessing, the use of default user accounts, and command execution after successful authentication. The results confirm that the proposed honeypot environment effectively accumulates experimental data on contemporary cyberattack techniques, facilitates the investigation of attacker tactics and tools, and improves the efficiency of security event log analysis. The collected data provide valuable information for understanding attacker behavior and identifying emerging attack patterns that can be used to enhance cybersecurity strategies.

The practical significance of the proposed approach lies in the development of a laboratory environment suitable for cybersecurity research, evaluation of attack detection mechanisms, accumulation of experimental datasets for improving security monitoring and incident response processes, and practical training of cybersecurity specialists. Furthermore, the proposed solution can serve as a foundation for future integration with Security Information and Event Management (SIEM) platforms, expansion of laboratory cyber ranges, and further development of proactive information security technologies.

Keywords: cybersecurity, information security, Cyber Deception, honeypot, cyber threats, attack analysis, emulation environment.

