Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:
«Модель атак на інформаційні ресурси кіберполігону»

Виконав: студент 2-го курсу, гр. 1БС-22м
спеціальності 125 Кібербезпека
_____ Ілля ТРИФАНЮК
Керівник: к.т.н., доцент каф. ЗІ
_____ Олеся ВОЙТОВИЧ
Опонент: к.т.н., доц., доц. каф . ПЗ
_____ Олександр ХОШАБА
«13» 12 2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д.т.н, проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«14» 12 2023 р.

Вінниця ВНТУ – 2023 рік

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II-й (магістерський)
Галузь знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека
Освітня програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д. т. н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«_19_» __09_____ 2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Трифанюку Іллі Сергійовичу

1. Тема роботи: «Модель атак на інформаційні ресурси кіберполігону», керівник роботи: Войтович Олеся Петрівна, к.т.н., доцент кафедри ЗІ затверджені наказом ректора ВНТУ від 18 вересня 2023 року, протокол №247.
2. Строк подання студентом роботи 13 грудня 2023 р.
3. Вихідні дані до роботи:
   - дані зібрані у матриці Mitre ATT&CK;
   - данні зібрані з веб-сайту Mitre CAPEC;
   - данні зібрані з OWASP TOP TEN.
4. Зміст текстової частини: Вступ. 1. Огляд предметної області. 2. Розробка моделей кібератак. 3. Розробка сценаріїв кібератак на кіберполігон. 4. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Локальний кіберполігон, апаратне забезпечення простого кіберполігону на базі університету (плакат А4). Реалізація апаратної моделі навчального кіберполігону на базі університету (плакат А4). Модель концепції Cyber-Kill Chain та розширена модель концепції Cyber-Kill Chain (плакат А4). Модель Diamond Model of Intrusion Analysis (плакат А4). Теоретико-множинна модель (плакат А4). Сценарій атаки на кіберполігон з розгалуженнями (плакат А4). Сценарій атаки на маршрутизатор кіберполігону (плакат А4). Лінійний сценарій атаки на кіберполігон (плакат А4).

. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанти	Підпис, дата	
		завдання видав	виконання прийняв
1	Олеся ВОЙТОВИЧ, к.т.н., доц. каф. ЗІ	19.09	25.09
2	Олеся ВОЙТОВИЧ к.т.н., доц. каф. ЗІ	19.09	30.09
3	Олеся ВОЙТОВИЧ к.т.н., доц. каф. ЗІ	19.09	10.10
4	Ольга РАТУШНЯК., к.т.н., доцент каф. ЕПВМ	19.09	11.11

7. Дата видачі завдання 1 вересня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Приміт
1	Аналіз завдання. Вступ	01.09.2023 – 10.09.2023	
2	Аналіз літературних джерел за напрямом магістерської кваліфікаційної роботи	10.09.2023 – 15.09.2023	
3	Науково-технічне обгрунтування	16.09.2023 – 22.09.2023	
4	Розробка технічного завдання	23.09.2023 – 29.09.2023	
5	Розробка рішень	30.09.2023 – 12.10.2023	
6	Практична реалізація, моделювання, експериментування, результати	14.10.2023 – 10.11.2023	
7	Розробка розділу економічного обгрунтування доцільності розробки	11.11.23 – 17.11.2023	
8	Аналіз виконання ТЗ, висновки	18.11.2023 – 24.11.2023	
9	Оформлення пояснювальної записки	25.11.2023 – 30.11.2023	
10	Попередній захист та доопрацювання МКР	28.11.2023 – 01.12.2023	
11	Перевірка магістерської роботи на наявність плагіату	02.12.2023 – 10.12.2023	
12	Представлення МКР до захисту	11.12.2023 – 14.12.2023	
13	Захист МКР	14.12.2023 – 21.12.2023	

Студент _____ Ілля ТРИФАН

Керівник роботи _____ Олеся ВОЙТОВ

АНОТАЦІЯ

УДК 004.056

Трифанюк І. Модель атак на інформаційні ресурси кіберполігону. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2023. 76 с.

Укр. мовою. Бібліогр.: 19 назв; рис.: 12; табл. 10.

Магістерська кваліфікаційна робота присвячена покращенню розуміння кібербезпеки, шляхом моделювання кібератак на інформаційні ресурси кіберполігону. Підготовлено науково-дослідне та техніко-економічне обґрунтування доцільності моделювання кібератак. У здійснено аналіз класифікації кібератак, розглянуто варіанти використання кіберполігону, розроблено структуру кіберполігону для університету. Розроблено теоретико-множинну модель для кібератак, розписано моделі кібератак та сценарії кібератак на інформаційні ресурси кіберполігону за цією моделлю.

В економічному розділі оцінено витрати на розробку.

Ілюстративна частина складається з плакатів з демонстрацією схеми алгоритму роботи системи та прикладами її використання.

Ключові слова: кіберполігон, кібератаки, моделі кібератак, сценарії кібератак, теоретико-множинна модель.

ABSTRACT

Trifaniuk I. Model of attacks on information resources of the cyber range. Master's qualification work in specialty 125 - Cybersecurity, educational program - Security of information and communication systems. Vinnytsia: VNTU, 2023. 76 c.

In Ukrainian. Bibliography: 19 titles; Figures: 12; Table 10.

The master's qualification work is devoted to improving the understanding of cybersecurity by modeling cyberattacks on the information resources of the cyber training ground. A research and feasibility study on the feasibility of modeling cyber attacks was prepared. The classification of cyberattacks was analyzed, the options for using the cyber range were considered, and the structure of the cyber range for the university was developed. A theoretical multiple model for cyberattacks is developed, cyberattack models and scenarios of cyberattacks on the information resources of the cyber range are described according to this model.

The economic section estimates the development costs.

The illustrative part consists of posters demonstrating the scheme of the system's algorithm and examples of its use.

Keywords: cyber training ground, cyberattacks, cyberattack models, cyberattack scenarios, theoretical set model.

ЗМІСТ

ВСТУП

В наш час стрімко відбувається процес цифровізації буденного життя, доказом цього є залежність від технологій у всіх сферах людської діяльності. Зараз важко уявити ефективний бізнес, адміністрування, буденність без використання технологій та інтернету [1].

Більшість організацій, магазинів, підприємств використовують веб-сайти, пошту та корпоративні додатки для ефективної роботи. Проте разом з прогресом, прогресують і шахраї та злочинці, тому наразі злочини в кіберпросторі не є рідкістю. Залежно від цілей злочинців та доступних їм способів, вони можуть завдати збитків тим чи іншим компаніям чи організаціям, використовуючи різноманітні методи, у результаті чого підприємства та організації несуть великі фінансові, ресурсні, репутаційні втрати, або навіть порушення національної безпеки. Ось чому, особливо зараз, дуже важливо забезпечувати повноцінну кібербезпеку, а це не можливо без наявності підготовлених фахівців у галузі кібербезпеки.

Через різний рівень володіння, отримання, обробки інформації, дуже багато компаній, установ, організацій нехтують кібербезпекою, за що досить часто отримують великі збитки. Але наявність фахівців не дає 100% захисту від кібератак, так як постійно розвивається як захист, так і способи обійти цей захист, тому постійно потрібно удосконалювати та оновлювати захист відповідно до сучасних викликів і потреб, також потрібно мати план реагування на такі інтенданти.

Для вивчення та вдосконалення навичок, спеціалістам з кібербезпеки допоможе кіберполігон, на якому вони зможуть потренуватись для відтворення кібератак та їх аналізу. У кіберполігоні можна відтворити системи, схожі на реальні для детального аналізу та тренувань, без реальних наслідків. Це допомагає організаціям і фахівцям з кібербезпеки готуватися до реагування на кібератаки та розробляти ефективні методи захисту від них.

Об’єкт дослідження – процес забезпечення кібербезпеки.

Предмет дослідження – методи моделювання кібератак на інформаційні ресурси кіберполігону.

Мета кваліфікаційної роботи – покращення обізнаності та навчання кібербезпеки шляхом побудови моделей кібератак, що можуть бути реалізовані на кіберполігоні з урахуванням відомих моделей.

Для досягнення мети необхідно:

– здійснити аналіз відомих кіберполігонів, що використовуються для навчання та покращення обізнаності;

– виконати аналіз літературних джерел щодо існуючих моделей кібератак;

– розробка моделей кібератак, що можуть бути реалізовані на кіберполігоні;

– розробити сценарії кібератак, що реалізовуються на кіберполігоні;

– виконати економічне обгрунтування доцільності розробки.

Елементи наукової новизна магістерської роботи полягають в тому, що подальшого розвитку набули моделі кібератак, які здійснюються на інформаційні ресурси кіберполігону, на відміну від відомих моделей, комбінує декілька відомих моделей, що дозволяє покращити техніки проведення атак на кіберполігоні.

Практична цінність полягає у розробці сценаріїв атак, що реалізуються на інформаційні ресурси кіберполігону під час навчання.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ДЖЕРЕЛ ЗА ТЕМОЮ ДОСЛІДЖЕННЯ

1.1 Потреби в моделюванні загроз і атак за допомогою кіберполігону

Щорічно у світі відбувається близько 800 тис кібератак, тобто кожні 39с відбувається 1 атака [2]. Швидкість еволюція кібератак є дуже високою і зростає з кожним роком. До причин такої еволюції можна віднести кількісну складову атак, частоту з якими вони відбуваються, приблизно 2222 атаки на день, та розвиток передових технологій, якими часто користуються кіберзлочинці.

Для протистояння швидкій еволюції кібератак, потрібно не тільки вчасно дізнаватись про нові атаки та методи їх реалізацій, а й регулярно тестувати систему для оцінки ризиків та навчання персоналу. Враховуючи постійний розвиток атак, ідеальним варіантом буде моделювання нових та існуючих атак і загроз на кіберполігоні. Цей метод дозволить постійно тестувати безпеку без загроз для основної системи, а головне такий метод тестування ніяк не випливає на бізнес процес у реальному часі, проте дає важливу інформацію про стан безпеки та захищеність від загроз.

Моделювання загроз і атак на кіберполігоні – це спосіб тестування кіберзахисту, схожий на тренування для команди кібербезпеки. Це допомагає виявити слабкі місця в системі та розробити ефективні заходи забезпечення безпеки. Такі тренування можуть включати в себе симуляцію різних видів атак, від фішингу до атак на програмне забезпечення, щоб підняти рівень готовності до потенційних загроз.

Важливість моделювання загроз на кіберполігоні полягає у:

1) Виявлення слабких місць – моделювання атак дозволяє ідентифікувати можливі слабкі місця в інфраструктурі та застосунках, які можуть бути використані зловмисниками.

2) Підготовка персоналу – команди кібербезпеки можуть отримати цінний досвід і тренування в реальних умовах, щоб краще розуміти, як реагувати на загрози та ефективно контролювати ситуацію.

3) Оцінка заходів безпеки – моделювання дозволяє оцінити ефективність вже встановлених заходів безпеки і внести відповідні поліпшення для запобігання майбутнім атакам.

4) Зниження ризику – шляхом імітації реальних загроз і атак.

5) На кіберполігоні можна відтворити точну копію робочої системи, що дозволить ефективно протестувати наявний рівень безпеки, готовність персоналу що-до виявлення та реагування на атаку, перевірити стійкість системи.

Технології та методи атак постійно змінюються, моделювання ж дозволяє підготувати персонал та систему до нових загроз та атак, ефективно оцінити та оптимізувати кількість витрат на кібербезпеку [3].

1.2 Кіберполігон основні відомості

Кіберполігон – це імітоване середовище або навчальний центр, призначений для навчання і вдосконалення навичок кібербезпеки, а також для імітації та аналізу кібератак. Кіберполігони використовуються для підготовки кіберзахисників, тестування стратегій і методів кіберзахисту, імітації кібератак та інших подібних ситуацій.

Кіберполігони можуть мати різну складність та рівень масштабованості. Залежно від мети їх створення можна поділити на:

Локальні кіберполігони – індивідуальні, розгорнуті на віртуальній машині, або окремому комп’ютері, на яких фахівець вивчає та тестує безпеку, проводить експерименти та навчається. Такі полігони є найпростішими та доступними (рисунок 1.1).

Місцеві кіберполігони для навчальних закладів – розгортаються у навчальних закладах, та тренувальних центрах для навчання студентів та досліджень у кібербезпеці.

Кіберполігони для підприємств – розгортаються на базі систем підприємства, для тестувань безпеки та навчання персоналу, вдосконалення системи захисту.

Кіберполігони національного рівня – розгортаються у тренувальних центрах, використовуються для тестування великих об’єктів інфраструктури, таких як системи зв’язку, енергетичні об’єкт тощо.

Міжнаціональні кіберполігони – розгортаються великими міжнародними організаціями партнерами для спільних тренувань та обміну знаннями у галузі.

Також на розміри та складність кіберполігону впливають наявність ресурсів, як технічних так і людських, залежно від розмірів кіберполігону обладнання може варіюватись, до основних ресурсів можна віднести:

- Комп’ютери та сервери.
- Відповідне програмне забезпечення.
- Мережеве обладнання.
- Засоби моніторингу та аналізу.
- Персонал.
- Навчальні програми та сценарії.

Рисунок 1.1 – Локальний кіберполігон

Локальний кіберполігон зображений на рисунку 1.1, є простою доступною версією для кожного, але використовувати такий кіберполігон зручно лише в індивідуальних цілях, через малу потужність та обмежену можливість тестування безпеки.

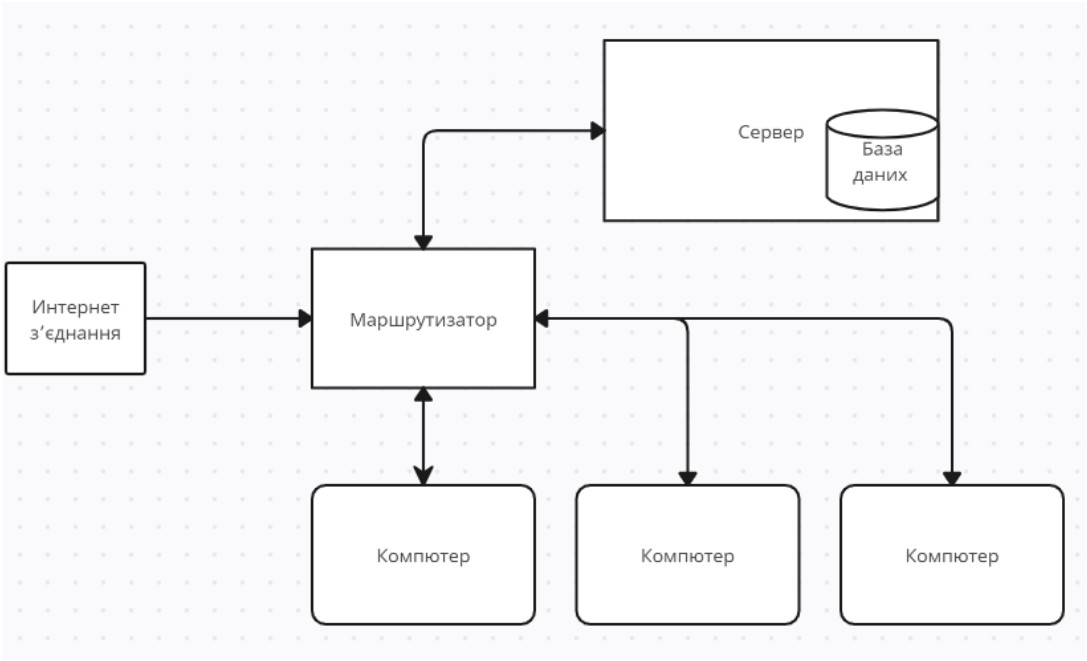


Рисунок 1.2 – Апаратне забезпечення простого кіберполігону на базі університету

На рисунку 1.2 зображений простий кіберполігон, який можна зробити враховуючи наявне апаратне забезпечення у вигляді 1 сервера, маршрутизатора та 3 комп'ютерів та мережевого кабелю.

Для мінімального захисту такого кіберполігону потрібно встановити антивірусне програмне забезпечення на всі комп'ютери та сервер для виявлення та блокування шкідливого програмного забезпечення, використати систему IDS/IPS для моніторингу мережевого трафіку, налаштувати фаервол на маршрутизаторі та комп'ютерах для фільтрації трафіку, встановити фаервол для захисту мережі.

Такий кіберполігон можна використовувати як імітаційну систему маленького бізнесу для тестування безпеки та навчання студентів.

В Україні здебільшого використовуються навчальні полігони, які створюють окремі освітні організації, найпоширеніші на базі університетів. Одним з найпопулярніших національних полігонів, є Unit Range, який має 150 сценаріїв атаки та захисту, та може використовуватись, як досвідченими спеціалістами з кібербезпеки так і студентами [4].

Cyber Ranges – офіційний кіберполігон Міжнародного союзу електрозв'язку ООН для проведення національних, регіональних і глобальних кібернавчань. Цей полігон налічує 88 безкоштовних та більше 500 платних сценаріїв атак(залежно від обраної підписки або конкретної покупки), також на цьому полігоні проводять кіберзмагання. Більшість сценаріїв відрізняються по своїй складності та типу завдань, є завдання для фахівців різного рівня від новачків до професіоналів. Тому такий кіберполігон є чудовим інструментом для навчальних цілей студентів та фахівців з різним рівнем знань(рисунок 1.3).

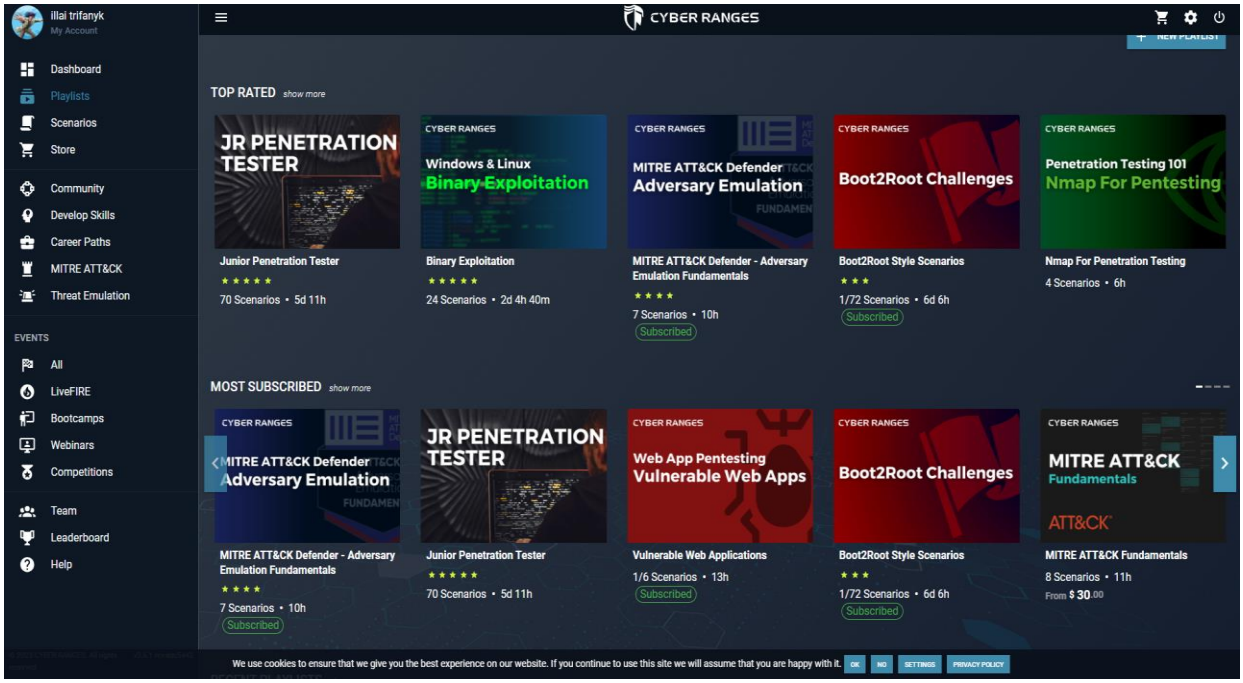


Рисунок 1.3 – Доступні сценарії атак на міжнародному кіберполігоні Cyber Range

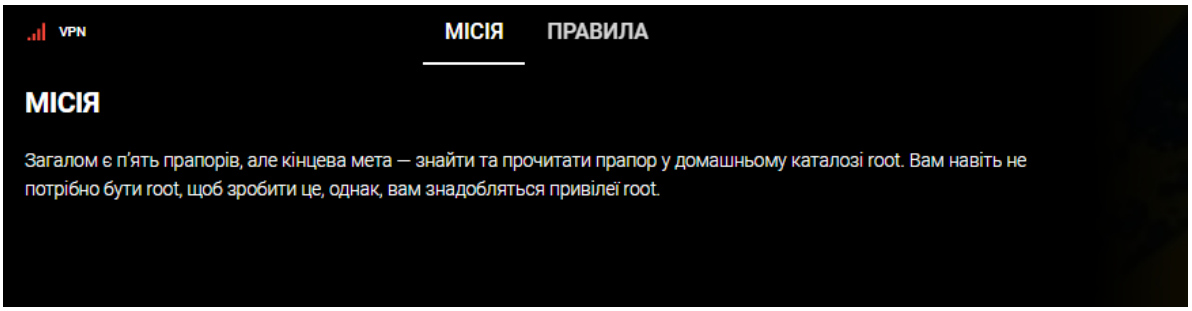


Рисунок 1.4 – Приклад сценарію атаки на міжнародному кіберполігоні Cyber Range

Загалом більшість завдань на цьому полігоні розроблені у форматі CTF для 1 людини, такий вид навчання допоможе фахівцям покращити свої практичні навички з атак для подальшого тестування реальних додатків.

1.3 Тестування безпеки на кіберполігоні

Часто кіберполігон використовують для тестування у форматі «Red, Blue та Purple team». Цей вид змагання схожий на гру-змагання, у якій Red team виступає у ролі хакера, який атакує кіберполігон, Blue team виступає у ролі спеціалістів, які повинні реагувати на атаку та захищатися від Red team, Purple team виступає у ролі координатора, який забезпечує максимальну ефективність команд, покращує роботу та забезпечує максимальний результат тестування.

Red tema – це група професіоналів або етичних хакерів, які моделюють атаки на комп'ютерну систему, мережу або організацію для виявлення вразливостей і слабкостей. Мета - оцінити заходи безпеки організації та покращити її захист [5].

Фактично Red tema зазвичай має такий сценарій тестування:

1) планування;
2) відкрита атака з використанням наявної інформації;
3) збір інформації;
4) аналіз та звітність;
5) співпраця з командою синіх.

На етапі планування команда розробляє план атаки або групи сценаріїв, щоб симулювати різні види атак, які можуть бути використані шахраями. Це може включати тестування фізичних, мережевих, програмних та соціальних вразливостей. Після чого команда проводить ряд атак, визначених у плані. Під час цих атак команда збирає інформацію про те, як команда синіх реагує на їхні атаки. Оцінюється реакція оборони на інциденти та зусилля зловмисників у боротьбі з заходами безпеки. Після чого отримана інформація детально аналізується, обговорюється з командою синіх для покращення заходів безпеки та реагування на інциденти, формується детальний звіт з виявленими вразливостями та рекомендаціями щодо покращення системи захисту.

Blue team – це команда, яка відповідає за захист та безпеку інформаційних ресурсів організації. Основними задачами цієї команди є виявлення атак та реагування на них, моніторинг безпеки, покращення заходів безпеки та аналіз інцидентів.

Ще одним видом використання кіберполігону є CTF-змагання.

"CTF" - це абревіатура, яка означає "Capture The Flag" (захоплення прапорця). Це формат змагань у галузі кібербезпеки, де учасники використовують свої навички, щоб вирішити різні завдання та завдання, які створені для тестування їх знань і навичок в сфері інформаційної безпеки. В ході CTF змагань учасники шукають прапорці (флаги), які представляють собою секретні рядки або символи, що підтверджують їх успіх [6].

CTF-завдання можуть варіюватися від технічних до креативних, і вони можуть охоплювати різні аспекти кібербезпеки, включаючи:

1) Криптографія. Завдання, пов'язані з розшифруванням або створенням криптографічних алгоритмів.

2) Заповнення сторінки пам'яті (Buffer Overflow). Використання багів програмного забезпечення для введення зловмисного коду та отримання контролю над системою.

3) Веб-безпека. Виявлення вразливостей в веб-додатках, таких як SQL-ін'єкції, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery).

4) Використання послуг. Розв'язання завдань, які вимагають знаходження вразливостей в сервісах (наприклад, веб-сервісах, FTP-серверах тощо).

5) Аналіз мережі. Розгадування заголовків пакетів, отримання доступу до внутрішніх мереж, знаходження портів і служб, які працюють на серверах.

Ключові аспекти CTF:

1) Завдання та прапорці. Організатори CTF створюють різні завдання, які включають в себе вимоги для розв'язання або взяття прапорця. Прапорці – це секретні рядки або символи, які гравці повинні знайти або здобути.

2) Часові обмеження. Більшість CTF мають часові обмеження. Учасники мають обмежений час для розв'язання завдань і здобуття прапорців.

3) Множина завдань. Зазвичай CTF мають різні категорії завдань, що вимагають різних навичок. Гравці можуть вибирати, які завдання їм цікаво розв'язати.

4) Команди індивідуальні або групові. Гравці можуть брати участь в CTF індивідуально або у командах. Групи спільно працюють, щоб розв'язати завдання.

5) Підсумкова оцінка. Після завершення CTF гравці або команди отримують оцінку на основі кількості розв'язаних завдань та швидкості їх розв'язання.

6) Багатофакторна навчальна діяльність. CTF на кіберполігоні сприяють навчанню та підвищенню кваліфікації в галузі кібербезпеки, а також розвивають навички аналізу, рішення проблем та командної роботи.

1.4 Класифікація кібератак

Класифікація кібератак полягає у групуванні на основі різних характеристик, залежно від типу, методів, мети та багатьох інших факторів. Розглянемо декілька загальних критеріїв класифікації:

1) За типом атаки:

- Фішинг – атаки, які використовують соціальну інженерію для отримання конфіденційних інформації.
- Злам паролів – вгадування чи обчислення паролю, для несанкціонованого доступу до системи**.**
- Атака з використанням вразливостей в програмному забезпеченні – використання вразливостей у системі, для отримання доступу до системи
- Атака на відмову в обслуговуванні (DoS) – перевантаження ресурсів системи для запобігання її роботи.
- Розподілена атака на відмову в обслуговуванні (DDoS) – використання багатьох комп'ютерів для підсилення DoS атаки.
- Malware – використання шкідливого програмного забезпечення для доступу або збору інформації.

2) За метою атаки:

- Шпигунство – атаки, спрямовані на отримання конфіденційної інформації, які можуть включати шпигунство державної та комерційної інформації.
- Саботаж – атаки з метою завдання шкоди або руйнування систем, наприклад, атаки на критичну інфраструктуру.
- Викуп від атаки (Ransomware) – атаки, які блокують доступ до даних та вимагають викуп за їх відновлення.
- Недекларований доступ (Backdoor) – використання вразливостей для створення прихованих шляхів доступу до системи.

3) За джерелом атаки:

- Внутрішня атака – атака, яка виходить від внутрішнього користувача чи співробітника організації.
- Зовнішня атака – атака, яка походить з поза організації.

Для аналізу та класифікації атак можна використовувати MITRE CAPEC та MITRE ATT&CK.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – це система, розроблена MITRE Corporation, яка надає вичерпний опис тактик, методів та загальних знань, які використовують кіберзлочинці та загрози для вторгнення в комп'ютерні системи та мережі. MITRE ATT&CK допомагає спільноті кібербезпеки краще розуміти різноманітні атаки та техніки, які можуть бути використані в кібератаках, а також розробляти заходи для їх запобігання та виявлення [7].

MITRE ATT&CK складається з таких компонентів:

1) Матриця ATT&CK – Матриця ATT&CK поділена на тактики, які описують загальні цілі атак, і методи, які описують конкретні техніки. Матриця містить десятки тактик і сотні методів (рисунок 1.5).

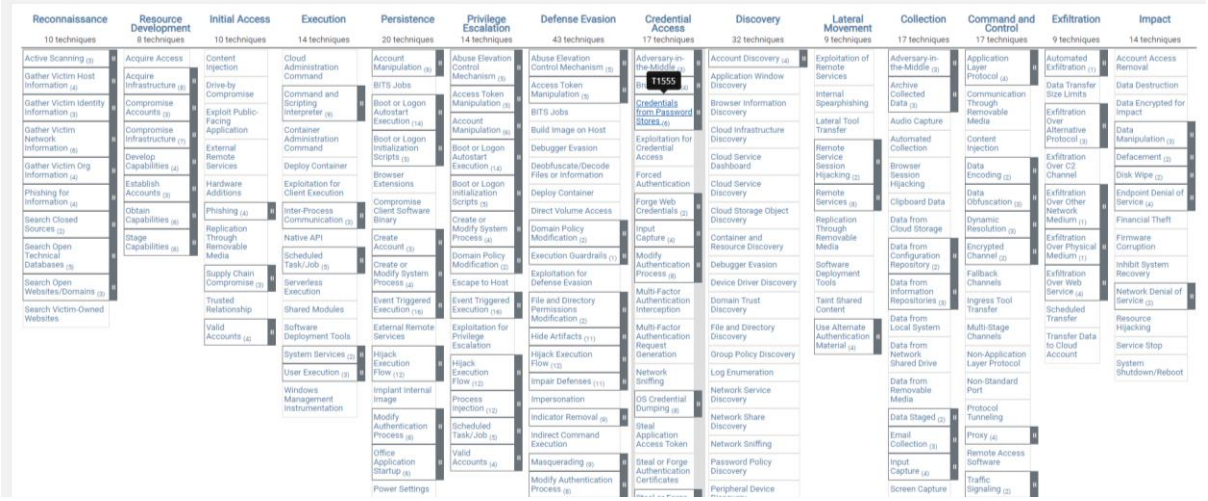


Рисунок 1.5 – Фрагмент матриці MITRE ATT&CK

Як видно з рисунка 1.5, у матриці MITRE ATT&CK досить зручно класифіковані атаки, тактики та способи їх проведення, тому цю матрицю зручно використовувати для планування атак та захисту від них, відкривши необхідну атаку можна отримати загальну характеристику атака та вразливість

на яку ця атака направлена, таким чином можна покращити захист або спланувати тест системи за допомогою цього ресурсу.

1) Підкомпоненти: В додаток до основної матриці ATT&CK, існують різні додаткові підкомпоненти та додатки, такі як «ATT&CK для мобільних пристроїв», «ATT&CK для хмарних середовищ».

2) Офіційний сайт та інструменти: MITRE публікує офіційний сайт ATT&CK, де можна знайти весь матеріал, включаючи матрицю та додаткові ресурси. Також, на сайті доступні інструменти, які допомагають аналізувати та використовувати дані з матриці ATT&CK.

3) Додаткові ресурси і документація: MITRE надає документацію, яка допомагає розуміти та використовувати ATT&CK, а також інші ресурси, такі як блоги, вебінари та інші матеріали.

MITRE CAPEC (Common Attack Pattern Enumeration and Classification) – це інша система, розроблена MITRE Corporation, яка служить для описування та класифікації загальних шаблонів атак. У відміну від MITRE ATT&CK, яка акцентується на тактиках та конкретних техніках, MITRE CAPEC допомагає ідентифікувати загальні маловідомі шаблони атак та побудувати класифікацію цих атак для кращого їх розуміння та захисту [8].

Основні компоненти MITRE CAPEC включають:

1) Записи атак – кожна атака описується в окремому записі, де надаються деталі щодо методів та технік, використовуваних у конкретній атаці.

2) Класифікація – MITRE CAPEC класифікує атаки згідно з різними аспектами, такими як типи вразливостей, типи шкодливого коду, типи атак, тощо.

3) Зв’язок з іншими системами – MITRE CAPEC пов’язана з іншими системами, такими як CWE (Common Weakness Enumeration) і ATT&CK, що дозволяє збагачувати знання про атаки та вразливості.

4) Офіційний сайт та інструменти – MITRE надає офіційний сайт для доступу до деталей про атаки та інші ресурси для спільноти кібербезпеки.

Отже, використавши MITRE CAPEC та MITRE ATT&CK, можна зручно знайти потрібну атаку та отримати інформацію про тактику, методи та детальний опис атаки. Цю інформацію можна використати у плануванні тесту для покращення тестування системи або ж навчальних цілях при роботі з кіберполігоном. Також ці ресурси містять інформацію про те, як виявити атаку та пом’якшити її вплив на систему.

1.5 Топ-10 актуальних вразливостей від OWASP

OWASP Топ-10 – є визнаною світовою методологією оцінки вразливостей веб-додатків у всьому світі і відображає сучасні тренди безпеки веб-додатків, є першим кроком організації до створення культури більш безпечного коду програмного забезпечення.

1) Injection, Injection flaws, SQL, NoSQL, OS, LDAP – ін’єкції коду, недоліки управління та зберігання сеансів, міжсайтовий скриптинг виникають, коли недовірливі дані передають інтерпретатору як частину команди чи запиту, проблеми, які виникають під час передавання інтерпретатору недовірливих даних у складі команди чи запиту, не змінювалися впродовж багатьох років. На жаль, введення різних токенів і використання хешів не робить веб-додатки більш захищеними.

2) Broken Authentication– функції додатків, пов’язані з автентифікацією та управлінням сеансами, часто реалізуються зловмисниками. Це дозволяє зловмисникам перехоплювати паролі, ключі і токени та ідентифікувати себе як користувачів системи.

3) Sensitive Data Exposure – існує багато веб-додатків та API, які не захищають належним чином конфіденційні дані, зокрема соціальні, фінансові та медичні. Зловмисники можуть викрасти або змінити такі погано захищені дані, щоб вчинити шахрайство з кредитними картками, крадіжку особистих даних та інші злочини. Існує також можливість неналежної передачі

конфіденційних даних без шифрування або без дотримання спеціальних заходів безпеки при обміні в браузері.

4) XML External Entities (XXE) – існує багато веб-додатків та API, які не захищають належним чином конфіденційні дані, включаючи соціальні, фінансові та медичні дані. Зловмисники можуть викрасти або змінити такі погано захищені дані для вчинення злочинів, таких як шахрайство з кредитними картками або крадіжка особистих даних. Конфіденційні дані також можуть передаватися неналежним чином через відсутність шифрування або спеціальних заходів безпеки при обміні в браузері.

5) Broken Access Control – Зловмисники можуть скористатися цими уразливостями, щоб отримати доступ до несанкціонованих функцій частин програми та/або даних, таких як доступ до облікових записів інших користувачів, перегляд конфіденційних файлів, модифікація даних інших користувачів або зміна прав доступу.

6) Security Misconfiguration – Неправильні налаштування безпеки є поширеною помилкою. Це пов’язано з використанням налаштувань безпеки за замовчуванням, відсутніми або користувацькими налаштуваннями, відкритими хмарними сховищами, неправильними заголовками HTTP і повідомленнями про помилки з критичними даними. Всі операційні системи, фреймворки, бібліотеки та додатки повинні бути належним чином налаштовані та оновлені, а також завантажені з надійних репозиторіїв.

7) Cross-Site Scripting (XSS) – виникає, коли програма додає дані на сторінку з неперевіреного джерела без будь-якої перевірки або перетворення. Крім того, вона використовує API-інтерфейси браузера, які дозволяють створювати HTML і JavaScript для оновлення існуючих веб-сторінок за допомогою даних, наданих користувачем. XSS дозволяє зловмисникам запускати скрипти в браузері жертви, перехоплювати сеанси користувачів, знищувати веб-сайти і перенаправляти користувачів на шкідливі сайти.

8) Insecure Deserialization – небезпечна десеріалізація часто призводить до віддаленого виконання коду. Помилки десеріалізації, що не

приводять до віддаленого виконання коду, можуть бути використані для атак з повторним відтворенням, впровадженням і підвищенням привілеїв.

9) Using Components with Known Vulnerabilities – використання компонентів з відомими вразливостями може призвести до втрати даних і серйозних наслідків для керування сервером.

10) Insufficient Logging & Monitoring – Неналежний облік і моніторинг, відсутність або неефективне використання систем реагування на інциденти дозволяє зловмисникам організовувати атаки, приховувати свою присутність і модифікувати, вилучати або знищувати дані. Вторгнення зазвичай виявляються через 200 днів і, як правило, не в рамках внутрішнього аудиту або моніторингу, а сторонніми розслідувачами [9].

1.6 Висновки до розділу 1

Виконано аналіз кібератак та освітлення вразливостей веб-додатків через призму OWASP Топ-10 разом із використанням MITRE ATT&CK та MITRE CAPEC підкреслює критичну важливість адекватного моделювання атак для сучасних організацій.

MITRE ATT&CK виступає як невід'ємний інструмент для розуміння тактик і методів кіберзлочинців, допомагаючи ефективно аналізувати та розробляти стратегії захисту. Це стає ключовим елементом готовності до ризиків та визначення заходів безпеки.

Активне моделювання атак, засноване на детальному вивченні класифікації та використанні доступних інструментів, виступає як невід'ємна складова стратегії кіберзахисту. Цей підхід допомагає не лише розуміти потенційні загрози, але і ефективно реагувати на них, підвищуючи рівень безпеки та готовності організацій до викликів сучасного кіберпростору.

2 РОЗРОБКА МОДЕЛЕЙ КІБЕРАТАК

2.1 Модель кібератак

Модель атаки – це стриктурний підхід до опису і аналізу вразливостей, які можуть погрожувати безпеці системи. В рамках моделі визначаються потенційні зловмисники та їх мотиви, способи а також види атак, які вони можуть здійснити.

Процес може включати в себе різні аспекти, такі як:

1) Модель загроз – визначає потенційного зловмисника, наприклад хакера чи незадоволеного працівника, їх мотиви та ресурси.

2) Модель сценаріїв – описує конкретні способи вторгнення, від простих атак по типу підбору паролів до складних атак на рівні додатків з використанням шкідливого ПЗ.

3) Модель поведінки – аналізує дії зловмисники до та після проникнення, визначає як зловмисник буде керувати зламаними системами та приховувати сліди проникнення.

Моделювання атаки є важливою складовою в процесі розробки політики безпеки та оцінки ризиків.

Загалом немає загальної моделі атак, які б підходили усім атакам, але для більшості атак можна застосувати модель:

1) Збір інформації – збір інформації про цільову систему. Отримання IP-адреси, доменів, мережевої інфраструктури та інших видів відкритих даних.

2) Визначення вразливостей – пошук та аналіз потенційних вразливостей в системі, такі як сканер вразливостей і ручний аналіз коду.

3) Отримання доступу – отримання несанкціонованого доступу до системи, за рахунок виявлених вразливостей. Це може включати злам паролів, маніпуляцію сесіями, використання слабких точок автентифікації тощо.

4) Ескалація привілеїв – після отримання обмеженого доступу, підвищення своїх прав у системі для отримання більшої можливості для проведення атак.

5) Виконання атаки – використовуючи доступ, який був отриманий у попередніх етапах, виконується атака.

6) Приховування слідів – щоб не бути виявленим, зловмисник намагається стерти свої сліди, видаляючи журнали подій, змінюючи файли журналів та інші заходи.

7) Постексплуатація – після проведення атаки, залежно від одержаних результатів злочинець може використати отримані данні або доступ для подальших дій, таких як викрадення інформації або шантаж, розкриття конфіденційних даних, розміщення шкідливого коду тощо.

2.2 Концепція Cyber-Kill Chain

Концепція Cyber-Kill Chain визначає різні етапи, які зловмисники проходять при виконанні кібератаки. Цей термін був вперше введений компанією Lockheed Martin як частина їхнього підходу до кібербезпеки.

Модель Cyber-Kill Chain вказує на те, що для здійснення своїх злочинів хакери завжди повинні пройти такі основні етапи [10] (рисунок 2.1).

Рисунок 2.1 – Кроки моделі Cyber-Kill Chain

Етап 1 – зовнішня розвідка, визначається як фаза вибору мети, виявлення особливостей організації, вибір технологій, вивчення активності компанії у соціальних мережах.

Етап 2 – озброєння та упаковка. Можливі різні форми: експлуатація веб-додатків, стандартні або спеціально виготовлені шкідливі програми, уразливості у різних документах (PDF, Office або інші формати документів) або атаки типу watering hole. Зазвичай вони готуються з дуже конкретними знаннями про мету.

Етап 3 – доставка. Передача необхідного шкідливого контенту з ініціативи жертви через шкідливий сайт або шкідливий PDF-файл, або з ініціативи хакера – SQL-ін'єкція.

Етап 4 – зараження. Після доставки на комп'ютери користувача, шкідливий контент розгортається, встановлюючись в середовище. Як правило, це відбувається при використанні відомої вразливості, для якої раніше був доступний патч.

Етап 5 – установка. Часто установка відбувається на фоні якихось зовнішніх з'єднань, ховаючись у цих операціях, непомітно проникаючи на кінцеві точки до яких можна отримати доступ. Потім зловмисник може контролювати цю програму без відома жертви.

Етап 6 – отримання керування. На цьому етапі зловмисники починають контролювати жертв за допомогою віддалених методів, таких як DNS, Internet Control Message Protocol (ICMP). В результаті хакер передає на контрольовані «активи» необхідні команди: що робити далі і яку інформацію збирати. Методи, що використовуються для збору даних: знімки екрана, контроль натискання клавіш, злом паролів, моніторинг мережі на облікові дані, збір критичного контенту та документів. Часто призначається проміжний хост, куди копіюються всі дані, а потім стискаються/шифруються для подальшого відправлення.

Етап 7 – виконання дій у жертви. Фінальний етап, на якому хакер відправляє зібрані данні або виводить з ладу IT- активи під час свого перебування в мережі жертви, проводяться заходи для виявлення інших цілей, розширення своєї присутності всередині та вилучення даних.

Після 7 етапу зазвичай ланцюжок повторюється у середині мереж.

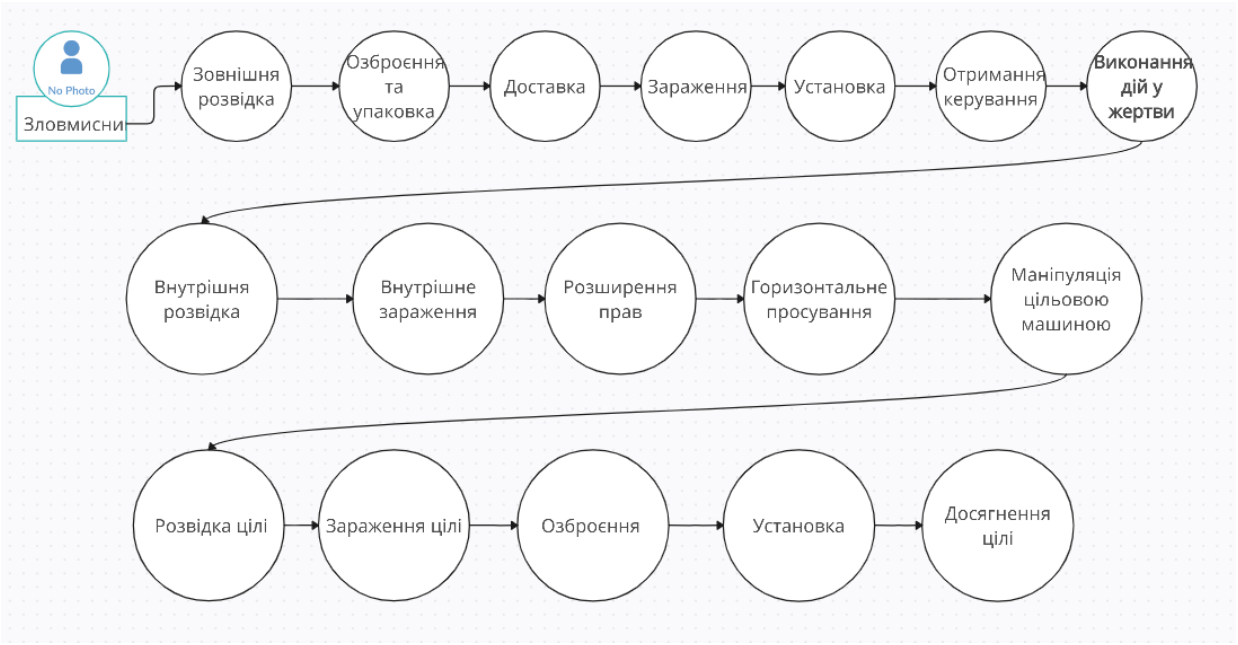


Рисунок 2.2 – Розширена модель Cyber-Kill Chain

Сукупність зовнішньої та внутрішньої моделі Cyber-Kill Chain називається розширена модель Cyber-Kill Chain, фактично це та сама модель Cyber-Kill Chain, яка має схожі кроки, але вже внутрішні. Кожен крок просуває злочинця в глиб системи, це може займати від кількох хвилин до кількох місяців, включно з часом остаточного вичікування моменту для атаки. Атака запускається в оптимальний для цього час для отримання максимального профіту, так як деякі кроки, зокрема розвідка та озброєння можуть займати по декілька місяців.

На етапі внутрішньої розвідки хакери мають доступ до робочої станцій одного користувача, з якої будуть отримуватись данні з локальних файлів, мережевих папок, історій браузера та данні про підключення до Wiki та SharePoint. Головна ціль – з’ясувати, як ця машина може допомогти у вивчені мережі та вийти на більш корисні активи.

Кінцевою ціллю хакерів, як правило, є отримання доступу до серверів, при отриманні доступу до сервера, порушаються головні принципи кібербезпеки такі як: конфіденційність, цілісність, доступність, що призведе

до репутаційних та фінансових втрат, можливо навіть втрати контролю над системою, що може призвести до подальших кібератак на інші системи та юридичних наслідків.

2.3 Модель Diamond Model of Intrusion Analysis

Модель Diamond Model of Intrusion Analysis розглядає кібератаку через призму чотирьох основних компонентів: Adversary (Супротивник), Victim (Жертва), Infrastructure (Інфраструктура) та Capability (Здібність) [11] (рисунок 2.3).

1) Adversary (Супротивник):

- Характеристики – описують, хто чи що виконує атаку - фізична особа, група чи організація.
- Мотивація вказує на цілі та мотивації супротивника в проведенні атаки.
- Тактика описує, як саме супротивник здійснює атаку та досягає своїх цілей.
- Ідентифікація визначає, як можна ідентифікувати супротивника та визначити його особливості.

2) Victim (Жертва):

- Характеристики описують особливості та атрибути об'єкта атаки (жертви).
- Цінність для супротивника вказує на те, чому саме обрана ця жертва для атаки.
- Ідентифікація визначає, як можна ідентифікувати жертву та зрозуміти її роль в контексті атаки.

3) Infrastructure (Інфраструктура):

- Технічні складові – включає сервери, мережеві ресурси, програмне забезпечення та інші технічні аспекти.
- Організаційні елементи включає людей, процеси, структури та інші організаційні аспекти, які підтримують атаку.

4) Capability (Здібність):

- Технічні засоби – описує конкретні технічні аспекти, використовувані для атаки.
- Експлоіти та інструменти вказують на конкретні експлоіти, інструменти чи методи, що використовуються супротивником.
- Компетенції та навички описують навички та здібності супротивника для впровадження атак.

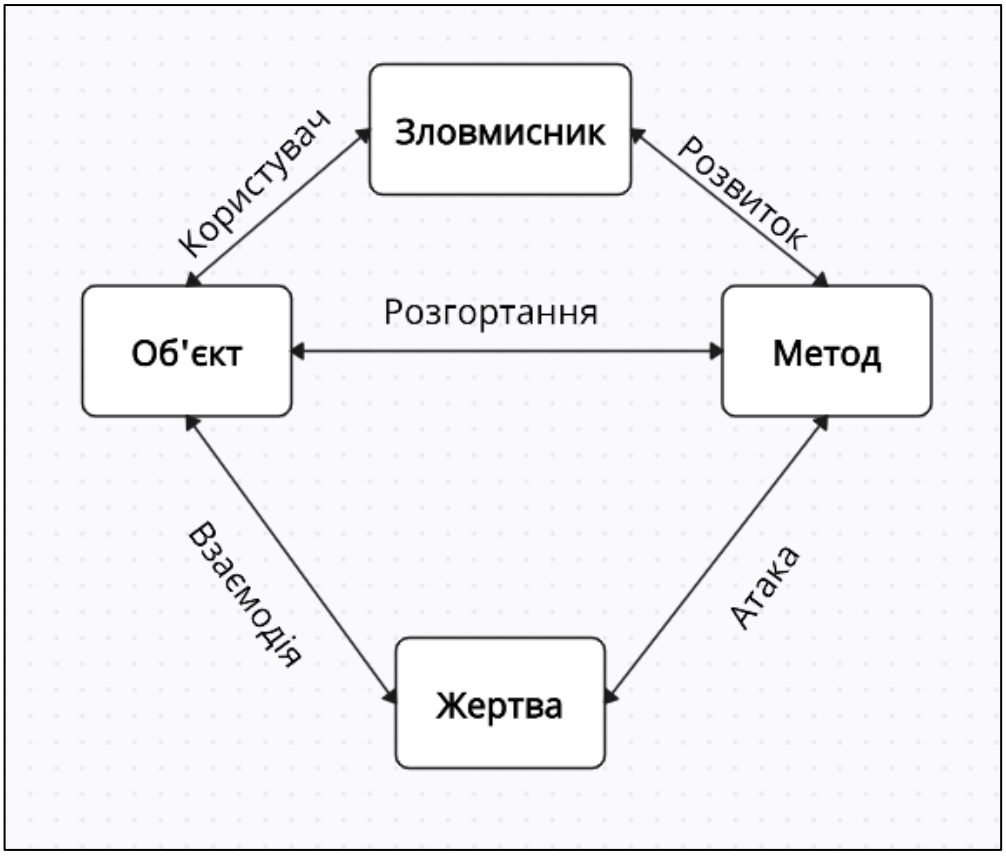


Рисунок 2.3 – Модель Diamond Model of Intrusion Analysis

Модель Diamond дозволяє більш глибоко розібратися в динаміці та елементах кібератак, забезпечуючи комплексний погляд на події та взаємодію учасників атаки.

2.4 Розробка теоретико-множинної моделі кібератак

2.4.1 Постановка задачі

Виходячи з концепції Cyber-Kill Chain та модель Diamond Model of Intrusion Analysis при моделюванні атак потрібно врахувати такі фактори : об’єкт атаки, інформацію яку може використати хакер, вразливість, техніку та тактику кібератаки та наслідки.

Нехай:

Хакери – множина хакерів.

Цілі – множина цілей атак.

Інформація – множина інформації, яку хакер може збирати.

Вразливості – множина вразливостей.

Аналіз – множина результатів аналізу вразливостей.

Тактики – множина тактик атак.

Техніки – множина технік атак.

ВиконаніАтаки – множина виконаних атак.

Наслідки – множина наслідків атак.

Тоді отримаєм таку функція:

1. Розвідка – Хакери × Цілі → Інформація.

2. Пошук вразливостей – Інформація→Вразливості.

3. Аналіз вразливостей – Вразливості→Аналіз.

4. Використання MITRE – Аналіз→Тактики×Техніки.

5. Виконання атаки – Тактики×Техніки→ВиконаніАтаки.

6. Пост-експлуатація – ВиконаніАтаки→Наслідки.

2.4.2. Отже отримаємо модель, яка буде мати вигляд[12]:

$$S=\{S1(a1,a2,\ldots an);\ S2(b1,b2\ldots bn);\ S3(c1,c2,\ldots cn);\ S4(d1,d2,\ldots dn);\ S5(e1,e2\ldots en);\ S6(f1,f2,...fn);\ S7(g1,g2\ldots gn)\},$$

де

S1 – Визначення цілей.

Цілі={система, база даних, сервер,...}

- конкретні об'єкти або ресурси, які можуть бути цілями;

S2 – Розвідка.

Інформація={дані1,дані2,...,дані*n*}

- конкретні дані, які можна збирати про цілі.

S3 – Пошук вразливостей.

Вразливості={паролі, застарілі програми, конфігураційні помилки,...}

- конкретні вразливості, які можуть бути використані для атаки.

S4 – Аналіз вразливостей:

Аналіз={атака1,атака2,...,атака n}

- конкретні аналізи, які допомагають визначити, які атаки можуть бути ефективними.

S5–Використання MITRE:

Тактики={соціальна інженерія, використання вразливостей,...}

- конкретні тактики атак.

Техніки={Фішінг, SQLInjection,...}

- конкретні техніки атаки.

S6–Виконання атаки:

Виконані атаки={атака1, атака2,..., атака n}

- відображає виконані атаки на основі використання певних тактик та технік.

S7–Пост-експлуатація:

Наслідки={отримання доступу, крадіжка даних, розповсюдження ШПЗ,...}

- конкретні наслідки виконаних атак.

Побудуємо моделі деяких кібератак на основі виведеної теоретико-множинної моделі:

2.4.3 Фішингові атаки[13].

1) Визначення цілей S1{a1,a2,a3}:

a1 - Вибір цілей фішинг-атаки (наприклад, працівників кіберполігону);

a2 - Аналіз доступних цілей серед працівників та їх звичок безпеки;

a3 - Вибір конкретної особи для фішинг-атаки.

2) Розвідка S2{b1,b2,b3}:

b1 - Збір інформації про працівників, їхній статус та обов'язки;

b2 - Вивчення графіка роботи та звичок працівників;

b3 - Аналіз внутрішньої та зовнішньої комунікації працівників.

3) Пошук вразливостей S3{c1,c2,c3}:

c1 - Визначення точок введення для фішинг-атаки, наприклад, електронна пошта чи соціальні мережі;

c2 - Виявлення слабких місць в безпеці працівників, таких як низький рівень обізнаності з фішинговими загрозами;

c3 - Аналіз можливостей обхіду захисту та соціального інженерінгу.

4) Аналіз вразливостей S4{d1,d2,d3}:

d1 - Визначення категорій фішинг-атак, таких як електронна пошта, соціальні мережі, або телефонний фішинг;

d2 - Вибір методу фішингу, який найефективніше пройде через захист;

d3 - Розробка плану фішинг-атаки для вибраного працівника.

5) Використання MITRE S5{e1,e2,e,3}:

e1 - Визначення тактик фішинг-атаки на основі MITRE ATT&CK;

e2 - Вибір конкретних методів фішинг-атаки, таких як відправка шахрайських листів чи створення підроблених веб-сайтів;

e3 - Адаптація методів атаки до характеристик та поведінки обраного працівника.

6) Виконання атаки S6{f1,f2,f3}:

f1 - Відправка фішингового листа, що містить шахрайське повідомлення або веб-посилання;

f2 - Використання соціального інженерінгу для отримання конфіденційної інформації або викликання працівника до дій, що порушують безпеку;

f3 - Моніторинг реакції та взаємодії працівника з фішинговим матеріалом;

7) Пост-експлуатація S7{g1,g2,g3}:

g1 - Використання отриманої конфіденційної інформації для подальших атак або доступу до системи;

g2 - Розповсюдження інформації про успіх фішинг-атаки для створення враження небезпеки та ризику для інших працівників;

g3 - Видалення слідів атаки та уникнення виявлення.

У фішинг-атаках, визначення цілей, розвідка, пошук вразливостей та аналіз вразливостей є ключовими етапами. Використання MITRE дозволяє адаптувати методи атаки до характеристик конкретного працівника. Під час виконання атак та пост-експлуатації, хакери стежать за реакцією та взаємодією з фішинговим матеріалом, використовуючи отриману інформацію для подальших атак або доступу.

2.4.4 DDoS-атаки[14].

1) Визначення цілей S1{a1,a2,a3}:

a1 - Вибір цілей атаки (наприклад, веб-сайту кіберполігону);

a2 - Аналіз доступних цілей серед веб-ресурсів;

a3 - Вибір конкретного веб-ресурсу.

2) Розвідка S2{b1,b2,b3}:

b1 - Визначення структури веб-сайту та серверної інфраструктури;

b2 - Збір інформації про захист веб-ресурсу від DDoS-атак;

b3 - Аналіз слабких місць існуючого захисту.

3) Пошук вразливостей S3{c1,c2,c3}:

c1 - Оцінка пропускної спроможності веб-сайту та серверів;

c2 - Виявлення можливих вразливостей в мережевій інфраструктурі;

c3 - Створення списку потенційних точок атаки.

4) Аналіз вразливостей S4{d1,d2,d3}:

d1 - Категоризація можливих вразливостей, які можна використовувати для DDoS-атаки;

d2 - Аналіз можливих видів DDoS-атак, таких як SYN flood, HTTP flood тощо;

d3 - Розробка стратегії DDoS-атаки на основі знайдених вразливостей.

5) Використання MITRE S5{e1,e2,e,3}:

e1 - Визначення тактик атак на основі визначених вразливостей та видів DDoS-атак;

e2 - Вибір конкретних технік DDoS-атаки, таких як змінення частоти запитів чи розподілення атак з великої кількості джерел;

e3 - Адаптація методів атаки до структури веб-сайту та серверної інфраструктури.

6) Виконання атаки S6{f1,f2,f3}:

f1 - Запуск DDoS-атаки на веб-сайт кіберполігону, використовуючи інфраструктуру, яка раніше була зібрана під час розвідки;

f2 - Використання різних видів DDoS-атак для подолання захисту веб-ресурсу;

f3 - Моніторинг та налаштування атаки для уникнення виявлення та заходів відновлення.

7) Пост-експлуатація S7{g1,g2,g3}:

g1 - Оцінка успішності DDoS-атаки шляхом вимірювання часу відновлення веб-сайту та його доступності;

g2 - Поширення результатів атаки для привертання уваги та створення враження нестабільності ресурсу;

g3 - Використання отриманої інформації для планування подальших атак.

У DDoS-атаках, визначення цілей, розвідка та пошук вразливостей фокусуються на виявленні слабких місць існуючого захисту веб-ресурсу. Використання MITRE дозволяє визначити тактики та техніки, які найефективніше пройдуть через захист. Виконання атак та пост-експлуатація включають у себе ефективні методи, спрямовані на подолання захисту та використання отриманої інформації для подальших атак.

2.4.5 XSS-атаки[15].

1) Визначення цілей S1{a1,a2,a3}:

a1 - Вибір цілей атаки (наприклад, сторінок веб-сайту кіберполігону, які обробляють користувацький ввід);

a2 - Аналіз доступних цілей серед веб-ресурсів;

a3 - Вибір конкретної веб-сторінки з уразливими місцями.

2) Розвідка S2{b1,b2,b3}:

b1 - Визначення структури та обробки введення на вибраній веб-сторінці;

b2 - Збір інформації про використані технології та фреймворки;

b3 - Аналіз можливих точок введення та вразливостей в обробці користувацького вводу.

3) Пошук вразливостей S3{c1,c2,c3}:

c1 - Визначення точок введення, де можна впровадити XSS-код;

c2 - Пошук інших вразливостей, які можна використовувати для обхіду захисту;

c3 - Виявлення можливостей для введення користувацького коду без фільтрації.

4) Аналіз вразливостей S4{d1,d2,d3}:

d1 - Категоризація вразливостей, таких як persistent або non-persistent XSS;

d2 - Визначення потенційних атак та їх вплив на користувачів;

d3 - Розробка плану XSS-атаки для вибраної веб-сторінки.

5) Використання MITRE S5{e1,e2,e,3}:

e1 - Визначення тактик атаки XSS на основі MITRE ATT&CK;

e2 - Вибір конкретних технік XSS-атаки, таких як внедрення скриптів чи використання маскування коду;

e3 - Адаптація методів атаки до структури та технологій, використаних на вибраній веб-сторінці.

6) Виконання атаки S6{f1,f2,f3}:

f1 - Введення XSS-коду через знайдені точки введення;

f2 - Використання XSS-атаки для здійснення атак на користувачів, використовуючи їх сесійні дані;

f3 - Збір інформації, отриманої через XSS-атаку, такої як сесійні ключі або конфіденційна інформація;

7) Пост-експлуатація S7{g1,g2,g3}:

g1 - Використання отриманих сесійних даних для отримання доступу до інших ресурсів;

g2 - Розповсюдження посилань або коду з XSS-вразливістю для впливу на інших користувачів;

g3 - Видалення слідів атаки та уникнення виявлення.

У моделі атаки XSS, визначення цілей, розвідка та пошук вразливостей фокусуються на ідентифікації слабких місць у веб-сторінках, де можливе впровадження вредоносного коду. Використання MITRE ATT&CK дозволяє краще адаптувати методи атаки до конкретних технологій та фреймворків. Виконання атаки та пост-експлуатація передбачають використання XSS для здійснення атак на користувачів та збір конфіденційної інформації.

2.4.6 SQL-ін'єкції[16].

1) Визначення цілей S1{a1,a2,a3}:

a1 - Вибір цілей SQL-ін'єкції (наприклад, веб-додатків або баз даних кіберполігону);

a2 - Аналіз доступних цілей серед баз даних та веб-додатків;

a3 - Вибір конкретної цілі для SQL-ін'єкції.

2) Розвідка S2{b1,b2,b3}:

b1 - Вивчення структури баз даних та логіки веб-додатків, які використовуються на кіберполігоні;

b2 - Збір інформації про типи баз даних та їх конфігурацію;

b3 - Аналіз можливостей SQL-ін'єкції в параметрах веб-запитів.

3) Пошук вразливостей S3{c1,c2,c3}:

c1 - Визначення параметрів веб-запитів, де можна впровадити SQL-ін'єкційний код;

c2 - Виявлення слабких місць в безпеці, які можна використати для обходу захисту від SQL-ін'єкцій;

c3 - Пошук інших можливостей впровадження SQL-ін'єкційного коду.

4) Аналіз вразливостей S4{d1,d2,d3}:

d1 - Визначення категорій SQL-ін'єкцій, таких як UNION-based, Error-based або Blind SQL-ін'єкції;

d2 - Вибір методу SQL-ін'єкції, який найефективніше обходить захист;

d3 - Розробка плану SQL-ін'єкційної атаки для вибраної цілі.

5) Використання MITRE S5{e1,e2,e,3}:

e1 - Визначення тактик атаки SQL-ін'єкції на основі MITRE ATT&CK;

e2 - Вибір конкретних технік SQL-ін'єкції, таких як використання UNION запитів або впровадження коду в параметрах;

e3 - Адаптація методів атаки до структури та технологій, використованих на вибраній цілі.

6) Виконання атаки S6{f1,f2,f3}:

f1 - Впровадження SQL-ін'єкційного коду через визначені параметри веб-запитів;

f2 - Використання SQL-ін'єкції для отримання несанкціонованого доступу до даних в базі даних;

f3 - Збір конфіденційної інформації або впровадження змін у базу даних.

7) Пост-експлуатація S7{g1,g2,g3}:

g1 - Використання отриманих даних для подальших атак або доступу до системи;

g2 - Розповсюдження інформації про успіх SQL-ін'єкції для створення загрози та ризику для інших частин системи;

g3 - Видалення слідів атаки та уникнення виявлення.

У моделі атаки SQL-ін'єкції, фокус знову спрямований на визначення цілей, розвідку та пошук вразливостей, зокрема в параметрах веб-запитів. Класифікація вразливостей та вибір методів атаки спрощують розробку плану ін'єкційної атаки. Використання MITRE ATT&CK допомагає визначити тактики та техніки атаки на основі конкретних характеристик цільової системи. Виконання атаки та пост-експлуатація передбачають впровадження ін'єкційного коду, отримання доступу до даних та подальше використання отриманої інформації.

2.4.7 Атаки Server-Side Request Forgery(SSRF)[17].

1) Визначення цілей S1{a1,a2,a3}:

a1 - Вибір цілей атаки SSRF (наприклад, внутрішніх ресурсів або служб на сервері кіберполігону);

a2 - Аналіз доступних цілей серед внутрішніх ресурсів та служб;

a3 - Вибір конкретної цілі для атаки SSRF.

2) Розвідка S2{b1,b2,b3}:

b1 - Збір інформації про серверну інфраструктуру та доступні служби;

b2 - Вивчення мережевої топології та конфігурації серверів;

b3 - Аналіз можливих шляхів взаємодії між серверами.

3) Пошук вразливостей S3{c1,c2,c3}:

c1 - Визначення можливих точок введення, які можна використати для атаки SSRF;

c2 - Знаходження слабких місць у фільтрації вхідних даних та управлінні обмеженнями;

c3 - Пошук інших можливостей для використання SSRF.

4) Аналіз вразливостей S4{d1,d2,d3}:

d1 - Визначення категорій SSRF-вразливостей, таких як використання ненадійних URL-параметрів або обхід захисту;

d2 - Вибір методів атаки, таких як відправка зловмисних запитів на внутрішні ресурси;

d3 - Розробка плану SSRF-атаки на вибрану ціль.

5) Використання MITRE S5{e1,e2,e,3}:

e1 - Визначення тактик SSRF-атаки на основі MITRE ATT&CK;

e2 - Вибір конкретних технік SSRF-атаки, таких як використання ненадійних URL або зловмисних HTTP-запитів;

e3 - Адаптація методів атаки до конкретних властивостей серверної інфраструктури.

6) Виконання атаки S6{f1,f2,f3}:

f1 - Використання SSRF для відправки зловмисних запитів на внутрішні ресурси, такі як файлові системи або служби на інших серверах;

f2 - Отримання конфіденційної інформації або викликання дій на внутрішніх серверах;

f3 - Моніторинг реакції системи та аналіз результатів атаки.

7) Пост-експлуатація S7{g1,g2,g3}:

g1 – Використання отриманої інформації для подальших атак або доступу до внутрішніх ресурсів;

g2 – Розповсюдження інформації про успіх SSRF-атаки для створення загрози та ризику для інших частин системи;

g3 – Видалення слідів атаки та уникнення виявлення.

У моделі атаки SSRF, визначення цілей, розвідка, пошук вразливостей та аналіз вразливостей є ключовими етапами. Використання MITRE дозволяє адаптувати методи атаки до конкретних властивостей серверної інфраструктури. Під час виконання атак та пост-експлуатації, зловмисники використовують отриману інформацію для подальших атак або доступу до внутрішніх ресурсів.

2.4.8. Security Logging and Monitoring Failures (помилки ведення журналу та моніторингу безпеки)[18].

1) Визначення цілей S1{a1,a2,a3}:

a1 - Визначення цілей атаки на Security Logging and Monitoring (наприклад, вибір конкретних механізмів моніторингу та журналювання);

a2 - Аналіз доступних цілей серед систем моніторингу та журналювання;

a3 - Вибір конкретної системи або механізму моніторингу та журналювання для атаки.

2) Розвідка S2{b1,b2,b3}:

b1 - Збір інформації про системи моніторингу та журналювання, їх конфігурацію та обмеження;

b2 - Вивчення процесів моніторингу та ведення журналу безпеки на кіберполігоні;

b3 - Аналіз можливих слабких місць у механізмах моніторингу та журналювання.

3) Пошук вразливостей S3{c1,c2,c3}:

c1 - Визначення точок введення для атаки на системи моніторингу та журналювання;

c2 - Знаходження можливих помилок конфігурації або вразливостей у програмному забезпеченні систем моніторингу та журналювання;

c3 - Пошук інших можливостей впровадження атаки на моніторинг та журналювання;

4) Аналіз вразливостей S4{d1,d2,d3}:

d1 - Визначення категорій вразливостей моніторингу та журналювання, таких як недостатність журналювання, недостатня захист від видалення логів тощо;

d2 - Вибір методів атаки, які найефективніше використовують знайдені вразливості;

d3 - Розробка плану атаки на системи моніторингу та журналювання.

5) Використання MITRE S5{e1,e2,e,3}:

e1 - Визначення тактик атаки на моніторинг та журналювання на основі MITRE ATT&CK.

e2 - Вибір конкретних технік атаки, таких як видалення логів, обхід захисту журнальних файлів тощо.

e3 - Адаптація методів атаки до конкретних систем моніторингу та журналювання.

6) Виконання атаки S6{f1,f2,f3}:

f1 - Здійснення атак на системи моніторингу та журналювання, наприклад, видалення журнальних файлів, обхід захисту, або перехоплення логів;

f2 - Зміна чи видалення журнальних записів для приховування атаки або слідів дій;

f3 - Моніторинг реакції системи на атаку та аналіз результатів.

7) Пост-експлуатація S7{g1,g2,g3}:

g1 - Використання успіхів атаки для подальших дій або отримання доступу до системи;

g2 - Розповсюдження інформації про успіх атаки на моніторинг та журналювання для створення загрози та ризику для інших частин системи;

g3 - Видалення слідів атаки та уникнення виявлення.

У моделі атаки на помилки ведення журналу та моніторинг безпеки, визначення цілей, розвідка та пошук вразливостей фокусуються на ідентифікації слабких місць у механізмах моніторингу та журналювання. Використання MITRE дозволяє визначити тактики та техніки, які

найефективніше використовують знайдені вразливості. Виконання атак та пост-експлуатація включають в себе ефективні методи, спрямовані на обхід захисту та використання отриманої інформації для подальших атак.

2.5 Висновки до 2 розділу

Модель атаки визначає стриктурний підхід до аналізу та визначення потенційних загроз безпеці системи. Цей процес включає в себе модель загроз, яка ідентифікує потенційних зловмисників, їх мотиви та ресурси; модель сценаріїв, яка описує конкретні способи вторгнення; та модель поведінки, яка аналізує дії зловмисників до та після проникнення.

Більшість спланованих кібератак відбуваються за схожим сценарієм, відрізняються лише методами досягнення цілей, які залежать від вразливостей та захисту системи . Збір інформації, визначення вразливостей, отримання доступу, ескалація привілеїв, виконання атаки приховування слідів, постексплуатація - усі ці кроки проходь зловмисники для досягнення цілей, можливо навіть декілька разів.

Розроблена теоретико-множинна модель для аналізу кібератак на основі концепції Cyber-Kill Chain та моделі Diamond Model of Intrusion Analysis дозволяє систематизувати та узагальнити різноманітні етапи та компоненти, що визначають процеси кібератаки. В даній моделі враховуються об'єкти атаки, інформація, яку хакер може використовувати, вразливості, тактика та техніка атаки, а також наслідки.

Модель дозволяє визначити цілі атаки, провести розвідку для отримання необхідної інформації, визначити вразливості, провести аналіз та вибрати техніку та тактику для виконання атаки. Використовуючи MITRE, хакери можуть визначити конкретні тактики та техніки, що відповідають їхнім цілям. Після виконання атаки настає етап пост-експлуатації, де визначаються конкретні наслідки вдалого вторгнення.

Застосування такої моделі дозволяє не лише аналізувати існуючі кібератаки, але і ефективно моделювати та передбачати можливі сценарії атак, що сприяє розробці більш ефективних заходів кібербезпеки та підвищенню стійкості інформаційних систем.

Представлені моделі фішинг-атак та DDoS-атак на основі теоретико-множинного підходу надають систематичний огляд етапів та компонентів цих типів кібератак. Аналізуючи різні аспекти атак, від визначення цілей до пост-експлуатації, можна ефективно моделювати та аналізувати ці процеси для розробки ефективних заходів кібербезпеки.

Розглянуті моделі атак, такі як Cross-Site Scripting (XSS), SQL-ін'єкції та Server-Side Request Forgery (SSRF), дозволяють структурувати процеси атаки від визначення цілей до пост-експлуатації, спрощуючи розробку ефективних заходів кібербезпеки.

3 РОЗРОБКА СЦЕНАРІЇВ КІБЕРАТАК НА КІБЕРПОЛІГОН

3.1 Навчальний кіберполігон

Кіберполігон на базі навчального закладу, для студентів не потребує досить великої кількості апаратного забезпечення, враховуючи середню кількість студентів у групах 15-20 чоловік.

Тому для такого кіберполігону нам потрібно : 2 сервери, маршрутизатор, wifi-роутер + маршрутизатор та 5 комп’ютерів. Якщо використовувати таку мінімальну кількість апаратного забезпечення , можна розгорнути архітектуру, для конкретного проєкту, використавши різні варіанти підключень та архітектуру для урізноманітнення можливих сценаріїв атаки на такий полігон.

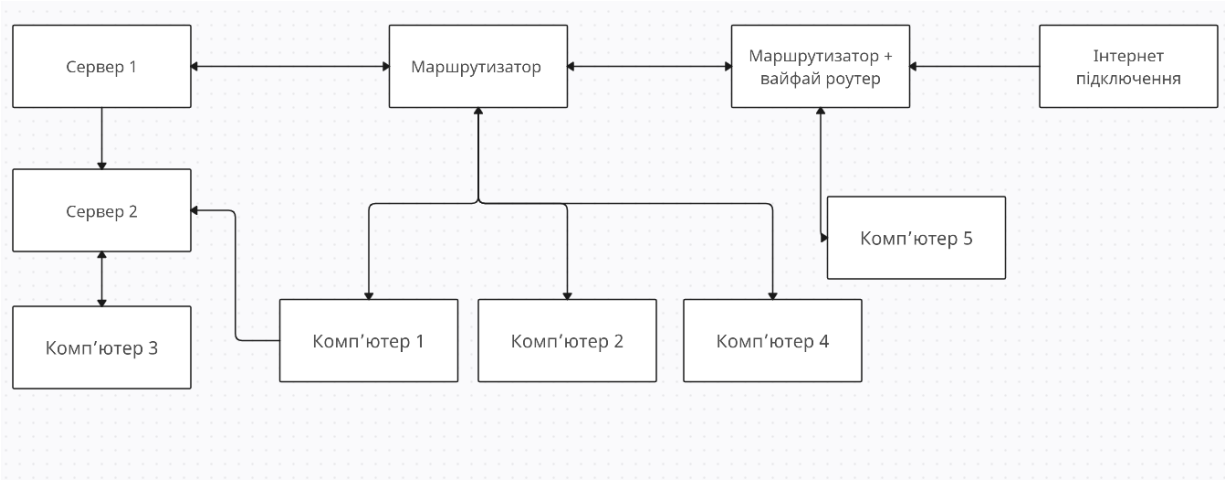


Рисунок 3.1 – Реалізація апаратної моделі навчального кіберполігону на базі університету

Вразливості кіберполігону з рисунка 3.1:

1) Слабке забезпечення мережі Wi-Fi:

- Якщо настройки бездротової мережі недостатньо захищені (наприклад, використання слабкого пароля чи захисту), це може призвести до несанкціонованого доступу до мережі через Wi-Fi.

2) Недостатня безпека маршрутизатора 2:

- Якщо маршрутизатор 2 має слабкі налаштування безпеки, це може призвести до несанкціонованого доступу чи атак на сам маршрутизатор.

3) Можливість атаки на сервери:

- Якщо сервери (Server 1 і Server 2) не належним чином захищені, це може призвести до атак, таких як SQL-ін'єкції або неправомірного доступу до серверів.

4) Одна точка відмови (Single Point of Failure):

- Якщо маршрутизатор 1 вийде з ладу, вся мережа може втратити доступ до Інтернету, що робить його однією точкою відмови.

5) Незахищені з'єднання:

- Якщо з'єднання між маршрутизатором 1 та маршрутизатором 2 не зашифровані, це може призвести до можливості перехоплення та читання чутливої інформації.

6) Недостатня захист бази даних і веб-сайту:

- Якщо база даних та веб-сайт не належним чином захищені, це може призвести до атак, таких як SQL-ін'єкції або атак на веб-додаток.

7) Недостатня кількість мережевих сегментів:

- Всі комп'ютери підключені до одного маршрутизатора 2, що може виникнути проблемами з безпекою, оскільки всі вони знаходяться в одній мережі.

Розміщення баз даних теж варіюється для кожного проєкту індивідуально, в даній конфігурації її можна розмістити на 2 серверах та будь-якому комп’ютері, залежно від потреби.

Якщо додати до такої конфігурації базу даних та веб-сайт, ми отримаємо готовий кіберполігон, з імітацією роботи підприємства, на якому студенти зможуть практикуватись у атаках та захисту такого підприємства для покращення практичних навичок.

3.2 Розвідка, інструменти для розвідки

Етап розвідки є одним із найважливіших етапів для проведення кібератак. На цьому етапі зловмисник збирає всю доступну відкриту або викрадену інформацію в інтернеті, на форумах, в дакрнеті, використовуючи різні інструменти пошуку та доступні ресурси. Шукають будь-яку інформацію яку можна використати у подальшому для досягнення цілей, найчастіше це:

1) Загальна інформація про компанію: офіційні e-mail адреси компанії та служби підтримки, веб сайти, форуми, додатки.

2) Інформація про технічні параметри: IP-адреси веб сайтів, інформацію про наявні сервери, домені імена пов’язані з організацією, інформацію про реєстраторів доменних імен, відомості про налаштування маршрутизаторів, комутаторів та інших мережевих пристроїв, файрволи та інші наявні засоби безпеки, відкриті порти, активні сервіси та їх версії, данні про хостинг-провайдерів, хмарні сервіси, топології мереж, підключені пристрої та їх розташування.

3) Персональна інформація працівників: e-mail адреси як корпоративні так і персональні, сторінки в соціальних мережах, номера телефонів, посади, емоційний стан та зв’язки працівників, інтереси, будь-яка інша інформація яку можна використати для методів соціальної інженерії.

4) Індустріальна інформація: про сферу діяльності, продукт, конкурентів, партнерів, постачальників, тенденції та політику компанії.

5) Інформація про відгуки та вразливості: наявні звіти про стан безпеки та захист, результати тестувань та виявлених вразливостей, інформацію про попередні кібератаки або інтенданти.

На цьому етапі злочинці можуть використати різноманітні інструменти, такі як Nmap, Wireshark, TheHavester, Shodan, OpenVas, Nessus, OWASP ZAP (Zed Attack Proxy), dnsenum, Masscan, Burp Suite, Maltego, інструменти пошуку WHOIS.

Nmap – сканер безпеки мережі, який виявляє активні пристрої та їх відкриті порти у мережі. Функціонал: визначення операційних систем, сканування портів, визначення версій програмного забезпечення.

Maltego – інструмент, для аналізу зав'язків між інформацією, дозволяє візуалізувати дані та зв'язки між даними. Функціонал: пошук відкритої інформації, аналіз зав'язків між об'єктами.

Burp Suite – інструмент, який має широкий спектр можливостей для виконання атак, використовується для тестування на проникнення, але у контексті розвідки можна використати інструмент для виявлення вразливостей для подальших дій. Функціонал: проксі, сканер вразливостей, інтерсептор, аналізу трафіку.

Shodan – інструмент для пошуку підключених пристроїв та ресурсів в інтернеті. Функціонал: пошук відео камер, пристроїв інтернету речей, відкритих портів та інше.

OWASP ZAP (Zed Attack Proxy) – безкоштовний інструмент від OWASP для тестування безпеки веб-додатків, що надає автоматизовані та ручні методи аналізу вразливостей. Функціонал: активне та пасивне сканування, аналіз вразливостей, перехоплення трафіку.

Masscan – високошвидкісний сканер портів у квеликих мережах. Функціонал: швидке сканування портів, пошук активних хостів.

Dnsenum – сканування DNS-записів, виявлення інформації про домени, виявлення піддоменів.

WHOIS – протокол для отримання інформації про власників доменів та їх контактні дані.

Етап розвідки є частиною більшості кібератак, особливо тих які спрямовані на конкретні цілі, виключення лише кібератаки які поширюються інтернетом та намагаються інфікувати якомога більше систем.

3.3 Сценарії кібератак на веб-сайт

Побудуємо декілька сценаріїв атак різного виду, 1 з розгалуженнями, 2 – лінійний, на основі виведеної у 2 розділі теоретико множинної моделі.

3.3.1 Сценарій 1 побудуємо за допомогою технік MITRE ATT&CK, який буде мати розгалуження (рисунок 3.2).

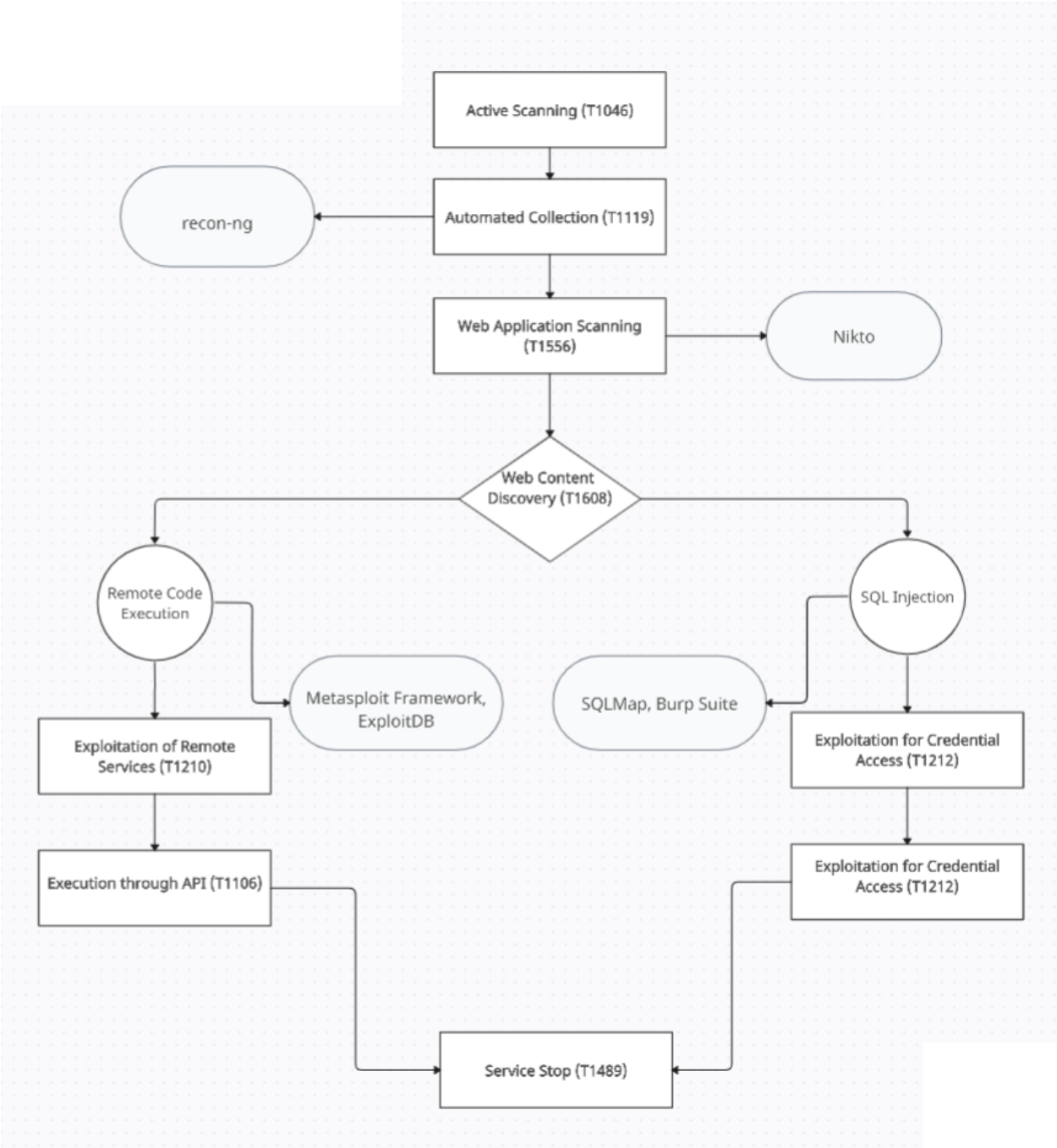


Рисунок 3.2 – Сценарій атаки на кіберполігон з розгалуженнями

У цьому сценарії будуть використані 2 вразливості, тому користувач зможе обирати яким шляхом рухатись.

Вразливості:

1) Вразливість А (веб-сервер):

Тип вразливості: Remote Code Execution (Віддалене виконання коду)

Деталі вразливості: Недолік у реалізації обробки HTTP-запитань.

Використані інструменти: Metasploit Framework, ExploitDB.

2) Вразливість В (база даних):

Тип вразливості: SQL Injection (SQL-ін'єкція)

Деталі вразливості: Недостатні фільтризація введених даних, що дозволяє виконання SQL-коду.

Використані інструменти: SQLMap, Burp Suite.

1) Визначення цілей (Етап 1):

MITRE ATT&CK тактика – Reconnaissance (Розвідка):

Техніка – Active Scanning (T1046). Атакуючий використовує спеціалізовані сканери для активного визначення активних IP-адрес веб-сайтів на кіберполігоні.

2) Розвідка (Етап 2):

MITRE ATT&CK тактика – Reconnaissance (Розвідка):

Техніка – Automated Collection (T1119). Атакуючий використовує потужні інструменти розвідки, такі як recon-ng, для аналізу веб-сайтів та отримання детальної інформації про їх конфігурацію та можливі вразливості.

Тактика – Web Application Profiling (Профілювання веб-застосунка). Атакуючий спрямовується на збір інформації про веб-сайт, його архітектуру та можливі точки входу.

Результат: отримана інформація про веб-сайт, включаючи його технічні характеристики, використовувані технології та слабкі місця.

3) Пошук вразливостей (Етап 3):

MITRE ATT&CK тактика – Discovery (Виявлення):

Техніка – Web Application Scanning (T1556). Атакуючий використовує інструменти, такі як Nikto чи OWASP Zap, для сканування веб-сайту та виявлення вразливостей в веб-застосунках.

Тактика – Web Vulnerability Scanning (Сканування вразливостей веб-застосунків). Атакуючий шукає слабкі місця в різних компонентах веб-сайту, таких як веб-застосунки, бази даних та інші.

Результат: виявлені вразливості в різних частинах веб-сайту, такі як непоновлені версії програм, недостатні обмеження доступу та інші.

4) Аналіз вразливостей (Етап 4):

Discovery (Виявлення):

Техніка – Web Content Discovery (T1608). Атакуючий аналізує знайдені вразливості для визначення структури веб-сайту та можливих точок атаки.

Тактика – Web Application Analysis (Аналіз веб-застосунків). Атакуючий спрямовується на ретельний аналіз вразливостей для ідентифікації потенційних точок входу.

Результат: Здобута детальна інформація про структуру веб-сайту та можливі шляхи атаки.

5) Використання MITRE (Етап 5):

MITRE ATT&CK тактика – Execution (Виконання):

Техніка – Exploitation of Web Servers (T1210). Атакуючий має вибір між двома вразливостями для експлуатації.

Тактика 1 – Web Server Exploitation (Експлуатація веб-сервера):

Техніка – Exploitation of Remote Services (T1210). Атакуючий обирає вразливість A для експлуатації веб-сервера.

Тактика 2 – Database Exploitation (Експлуатація бази даних):

Техніка – Exploitation for Credential Access (T1212). Атакуючий обирає вразливість B для експлуатації бази даних веб-сайту.

Результат (Тактика 1):

- Атака на веб-сервер використовуючи вразливість A.

- Отримання контролю над веб-сервером та можливість виконання коду на сервері.

Результат (Тактика 2):

- Атака на базу даних використовуючи вразливість B.
- Здобуття облікових даних та можливість використання їх для подальших атак або отримання доступу до конфіденційної інформації.

6) Виконання атаки (Етап 6):

MITRE ATT&CK тактика – Execution (Виконання):

Техніка (Тактика 1) – Execution through API (T1106):

Атакуючий використовує виклики до API веб-сайту для виконання власного коду та отримання додаткового доступу.

Техніка (Тактика 2) – Exploitation for Credential Access (T1212):

Атакуючий використовує отримані облікові дані для отримання доступу до систем та служб.

Тактики – API-based Execution (Виконання через API) та Credential Access (Отримання облікових даних):

Атакуючий взаємодіє з API веб-сайту та використовує отримані облікові дані для отримання додаткового доступу.

Результат: отримання додаткового доступу та можливість впровадження шкідливого коду через API веб-сайту.

7. Пост-експлуатація (Етап 7):

MITRE ATT&CK тактика – Defense Evasion (Ухилення від захисту):

Техніка – Service Stop (T1489):

Атакуючий використовує вразливості або отримані права для зупинки важливих служб на веб-сервері чи інших системах.

Тактика – Service Stop (Зупинка служб). Атакуючий використовує отримані права або експлуатує вразливості для зупинки важливих служб на веб-сервері.

Результат: зупинка важливих служб, що може призвести до відмови в обслуговуванні (DoS) та погіршення функціональності веб-сайту чи пов'язаних сервісів.

У цьому сценарії атаки на веб-сайт, атакуючий розпочинає з активного сканування для визначення активних веб-сайтів на кіберполігоні. Після отримання списку цільових ресурсів, він використовує інструменти розвідки для аналізу структури та конфігурації веб-сайтів.

Далі, атакуючий використовує інструменти сканування вразливостей для виявлення слабких місць у веб-застосунках. Після знаходження вразливостей, аналізує їх, щоб визначити можливі точки атаки.

На етапі використання MITRE ATT&CK, атакуючий обирає вразливість для експлуатації. У нашому сценарії є дві тактики: експлуатація веб-сервера та експлуатація бази даних. Кожна тактика має свою конкретну мету та наслідки. Наприклад, експлуатація веб-сервера може призвести до отримання контролю над сервером, тоді як експлуатація бази даних може дозволити здобуття облікових даних.

Наприкінці, на етапі виконання атаки, атакуючий використовує техніки виконання через API та отримання облікових даних. Завершальним етапом є пост-експлуатація, де атакуючий може використовувати ухилення від захисту та, наприклад, зупиняти важливі служби веб-сервера.

3.3.2 Сценарій 2 атаки на веб ресурси кіберполігону (рисунок 3.3).

1) Визначення цілей (Етап 1):

Опис: Атакуючий використовує активний перехідний аналіз для ідентифікації можливих цілей на кіберполігоні.

Результат: Виявлення веб-сайтів, що використовують застарілі версії веб-серверів.

Атака: Active Reconnaissance.

Інструменти: PassiveTotal, Shodan.

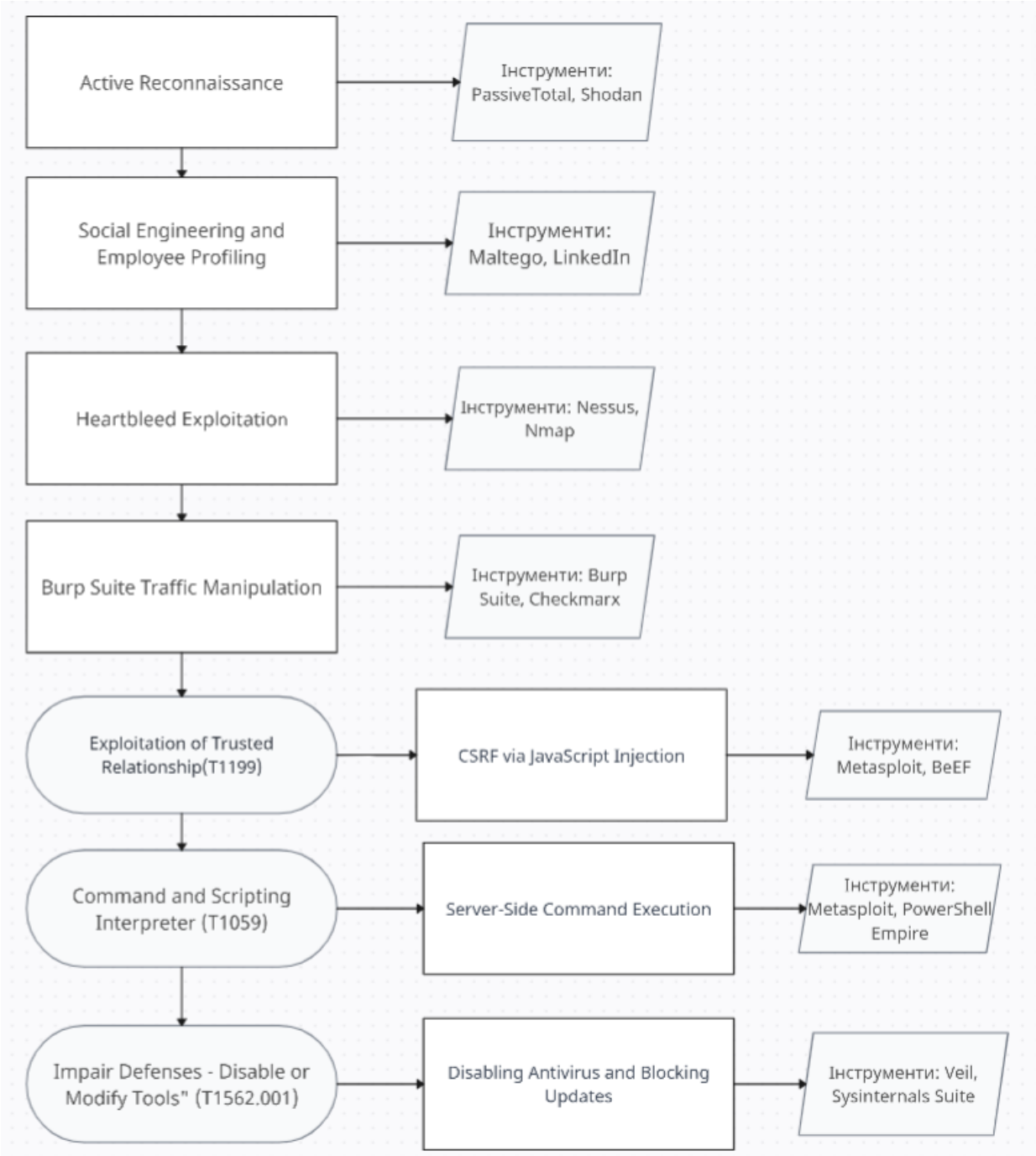


Рисунок 3.3 – Лінійний сценарій атаки на кіберполігон

2) Розвідка (Етап 2):

Опис: За допомогою соціальної інженерії та вивчення внутрішньої корпоративної структури, атакуючий визначає ключових працівників та їх роль в організації.

Результат: Виявлення адміністраторів веб-сайтів та їхніх обов'язків.

Атака: Social Engineering and Employee Profiling.

Інструменти: Maltego, LinkedIn.

3) Пошук вразливостей (Етап 3):

Опис: Атакуючий використовує інструментарій для аналізу мережі та знаходить вразливість в розташуванні серверів, таку як неправильна конфігурація SSL.

Результат: Виявлення уразливості Heartbleed на веб-сервері.

Атака (SSL/TLS Vulnerability Scan – Heartbleed Exploitation): Використання Heartbleed для отримання конфіденційної інформації з пам'яті сервера.

Інструменти: Nessus, Nmap.

4) Аналіз вразливостей (Етап 4):

Опис: Атакуючий використовує інструменти аналізу коду, такі як static analysis tools, для виявлення можливих точок атаки на веб-сайті.

Результат: Виявлення вразливостей в коді веб-застосунку.

Атака (Code Analysis for Web Application Security – Burp Suite Traffic Manipulation): Використання Burp Suite для перехоплення та зміни трафіку між користувачем та сервером для отримання доступу до адміністративного розділу.

Інструменти: Burp Suite, Checkmarx.

5) Використання MITRE (Етап 5):

Опис: Атакуючий використовує техніку "Exploitation of Trusted Relationship" (T1199) для введення зловмисного коду в довірені скрипти на веб-сайті.

Результат: Введення шкідливого JavaScript-коду через XSS-атаку.

Атака (Cross-Site Scripting (XSS) Attack – CSRF via JavaScript Injection) Впровадження JavaScript-коду, який використовує CSRF-атаку для зміни облікових даних адміністратора.

Інструменти: Metasploit, BeEF.

6) Виконання атаки (Етап 6):

Опис: Після успішного введення коду атакуючий отримує доступ до внутрішніх ресурсів, використовуючи техніку "Command and Scripting Interpreter" (T1059).

Результат: Здобуття доступу до файлів та бази даних веб-сайту.

Атака (Remote Code Execution (RCE) – Server-Side Command Execution): Використання RCE-атаки для виконання команд на сервері та отримання повного контролю над системою.

Інструменти: Metasploit, PowerShell Empire.

7) Пост-експлуатація (Етап 7):

Опис: Використовуючи техніку "Impair Defenses - Disable or Modify Tools" (T1562.001), атакуючий вимикає системні інструменти моніторингу та виявлення, щоб уникнути виявлення його присутності.

Результат: Приховане утримання доступу та ухилення від систем моніторингу.

Атака (Anti-Forensics and Defensive Evasion – Disabling Antivirus and Blocking Updates): Вимкнення антивірусного програмного забезпечення на сервері та блокування оновлень для уникнення виявлення.

Інструменти: Veil, Sysinternals Suite.

Атака на веб-сайт розпочалась з активного розвідування, де атакуючий використовував інструменти, такі як PassiveTotal та Shodan, для виявлення веб-сайтів з застарілими версіями веб-серверів. Після ідентифікації цілей, атакуючий проводив соціальну інженерію та вивчав корпоративну структуру через інструменти, такі як Maltego та LinkedIn, для визначення адміністраторів веб-сайтів та їхніх обов'язків.

Знаючи ключових гравців, атакуючий переходив до пошуку вразливостей, використовуючи інструменти Nessus та Nmap для виявлення уразливості Heartbleed на веб-сервері. Ця уразливість була використана атакуючим для отримання конфіденційної інформації з пам'яті сервера.

Аналізуючи вразливості коду веб-застосунку за допомогою інструментів, таких як Burp Suite та Checkmarx, атакуючий виявляв можливі точки атаки. Наприклад, використовуючи Burp Suite, атакуючий змінював трафік між користувачем та сервером для отримання доступу до адміністративного розділу.

Використовуючи MITRE ATT&CK, атакуючий впроваджував XSS-атаку для введення шкідливого JavaScript-коду на веб-сайті. Це дозволяло атакуючому використовувати CSRF-атаку для зміни облікових даних адміністратора.

Далі, атакуючий використовував RCE-атаку за допомогою Metasploit та PowerShell Empire для виконання команд на сервері та отримання повного контролю над системою.

На завершальному етапі пост-експлуатації, атакуючий вимикає системні інструменти моніторингу та виявлення, використовуючи Veil та Sysinternals Suite, для ухилення від виявлення його присутності. Атакуючий вимикає антивірусне програмне забезпечення та блокує оновлення для уникнення виявлення.

3.4 Сценарій атаки на маршрутизатор кіберполігону

Побудуємо сценарій атаки на маршрутизатор кіберполігону, так як в наявному полігоні це дуже критична вразливість(рисунок 3.4).

Цей сценарій атаки на маршрутизатор кіберполігону включає кілька етапів, спрямованих на активне визначення цілей, розвідку, пошук та аналіз вразливостей, використання MITRE ATT&CK для виконання атак та подальшу пост-експлуатацію. Атакуючий використовує інструменти, такі як nmap та recon-ng, для активного сканування та автоматизованого збору інформації про маршрутизатори. На етапі пошуку вразливостей використовується Nessus для виявлення слабких місць. Після аналізу вразливостей, атака використовує Metasploit для експлуатації мережевих протоколів та компрометації маршрутизаторів. У кінцевому етапі пост-експлуатації, атакуючий використовує Cisco IOS Commands для маніпулювання конфігурацією мережевих пристроїв, забезпечуючи постійний контроль та можливість подальших атак.

Сценарій ставить під загрозу безпеку інфраструктури кіберполігону, дозволяючи атакуючому отримати контроль над мережевими пристроями та маніпулювати їх конфігурацією.

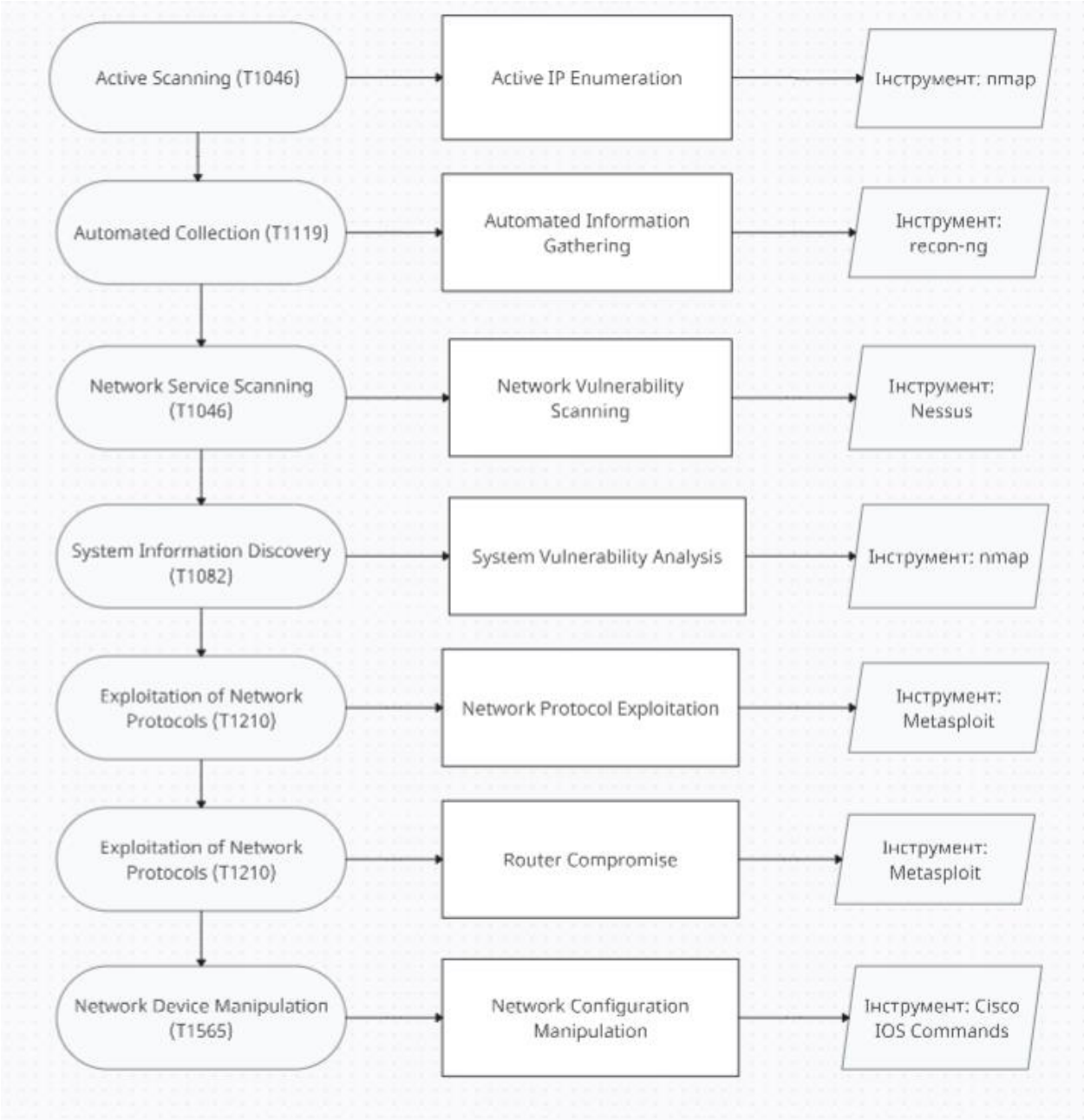


Рисунок 3.4 – Сценарій атаки на маршрутизатор кіберполігону

1) Визначення цілей (Етап 1):

MITRE ATT&CK тактика: Reconnaissance

Техніка: Active Scanning (T1046)

Атака: Active IP Enumeration

Інструмент: nmap

Результат: Знайдені активні IP-адреси маршрутизаторів.

Мета: Визначення потенційних цілей для подальших атак.

Розвідка (Етап 2):

MITRE ATT&CK тактика: Reconnaissance

Техніка: Automated Collection (T1119)

Атака: Automated Information Gathering

Інструмент: recon-ng

Результат: Збір деталізованої інформації про маршрутизатори, включаючи власників та адміністраторів.

Мета: Підготовка до наступних етапів атаки, включаючи ідентифікацію слабкіх місць.

3) Пошук вразливостей (Етап 3):

MITRE ATT&CK тактика: Discovery

Техніка: Network Service Scanning (T1046)

Атака: Network Vulnerability Scanning

Інструмент: Nessus

Результат: Виявлені вразливості мережевих служб на маршрутизаторах.

Мета: Визначення точок входу для подальшої експлуатації.

4) Аналіз вразливостей (Етап 4):

MITRE ATT&CK тактика: Discovery

Техніка: System Information Discovery (T1082)

Атака: System Vulnerability Analysis

Інструмент: nmap

Результат: Детальний аналіз виявлених вразливостей та визначення можливих шляхів атаки.

Мета: Підготовка до вибору конкретної атаки на основі вразливостей.

5) Використання MITRE (Етап 5):

MITRE ATT&CK тактика: Execution

Техніка: Exploitation of Network Protocols (T1210)

Атака: Network Protocol Exploitation

Інструмент: Metasploit

Результат: Компрометація мережевих протоколів маршрутизаторів.

Мета: Отримання доступу та підготовка до подальших етапів атаки.

6) Виконання атаки (Етап 6):

MITRE ATT&CK тактика: Execution

Техніка: Exploitation of Network Protocols (T1210)

Атака: Router Compromise

Інструмент: Metasploit

Результат: Компрометація маршрутизаторів, можливість контролю та внесення змін у їх конфігурацію.

Мета: Отримання контролю над мережевою інфраструктурою для подальших дій.

7) Пост-експлуатація (Етап 7):

MITRE ATT&CK тактика: Impact

Техніка: Network Device Manipulation (T1565)

Атака: Network Configuration Manipulation

Інструмент: Cisco IOS Commands

Результат: Зміна конфігурації мережевих пристроїв.

Мета: Забезпечення постійного контролю та можливості подальших маніпуляцій у мережі.

3.5 Сценарій атаки на виведення з ладу мережі кіберполігону

1) Визначення цілей: Атакуючий використовує Shodan для ідентифікації всіх пристроїв у мережі кіберполігону та їхніх служб.

Назва атаки: Automated Collection (T1119)

Результат: Повний список пристроїв та їхні служби в мережі.

2) Розвідка: За допомогою Wireshark атакуючий перехоплює та аналізує мережевий трафік, визначає структуру мережі та ключові вузли.

Атака: Packet Sniffing (T1040).

Додаткова тактика: Network Mapping (Мапування мережі).

Результат: Детальна інформація про структуру мережі та ключові вузли.

3) Пошук вразливостей: Атакуючий використовує Nmap для активного сканування пристроїв у мережі та виявлення вразливостей.

Атака: Active Scanning (T1046).

Додаткова тактика: Host Discovery (Виявлення хостів).

Результат: Виявлення вразливостей на пристроях у мережі.

4) Аналіз вразливостей: Застосунок OpenVAS використовується для аналізу виявлених вразливостей та ідентифікації потенційних атак.

Назва атаки: Vulnerability Analysis (Аналіз вразливостей).

Результат: Здобута детальна інформація про вразливості в мережі.

5) Використання MITRE: Атакуючий обирає тактику Impact та використовує техніку Network Denial of Service (DoS) (T1498), використовуючи вразливості, знайдені на етапах 3-4.

Назва атаки: Network Denial of Service (DoS) (T1498).

Результат: Виведення з ладу ключових сервісів та пристроїв.

6) Виконання атаки: Атакуючий використовує hping для виготовлення великого обсягу мережевого трафіку, спрямованого на ключові сервери та мережеві пристрої.

Назва атаки: Amplification Attack (Атака з використанням ампліфікації).

Результат: Перенавантаження мережі, відмова в обслуговуванні (DoS) ключових сервісів.

7) Пост-експлуатація: Атакуючий використовує Scapy для створення фальшивих пакетів, що спрямовуються на мережеві пристрої з метою подальшого зниження їхньої ефективності.

Назва атаки: Packet Flooding (Затоплення мережі пакетами).

Результат: Зниження ефективності мережевих пристроїв та подальше ускладнення відновлення мережі.

В цьому сценарії атаки атакуючий спершу використовує Shodan для ідентифікації всіх пристроїв у мережі кіберполігону та їхніх служб. За допомогою Wireshark проводить аналіз мережевого трафіку та визначає структуру мережі, використовуючи атаку Packet Sniffing та додаткову тактику Network Mapping. Після цього атакуючий виявляє вразливості на пристроях у мережі за допомогою Nmap та активного сканування (Active Scanning). Використовуючи OpenVAS, атакуючий аналізує вразливості та визначає можливі атаки на пристрої. На етапі використання MITRE атакуючий вибирає тактику Impact та запускає атаку Network Denial of Service (DoS) з використанням виявлених вразливостей, виводячи з ладу ключові сервіси та пристрої. Далі він використовує hping для проведення атаки з використанням ампліфікації, перенавантажуючи мережу та спричиняючи відмову в обслуговуванні (DoS) ключових сервісів. На завершальному етапі пост-експлуатації атакуючий використовує Scapy для створення фальшивих пакетів, спрямованих на мережеві пристрої з метою подальшого зниження їхньої ефективності, використовуючи атаку Packet Flooding. Це призводить до зниження ефективності мережевих пристроїв та ускладнює відновлення мережі.

3.6 Висновки до розділу 3

Розгорнута архітектура кіберполігону надає ефективні умови для практичного навчання студентів у сфері кібербезпеки. Аналіз вразливостей вказує на необхідність удосконалення заходів безпеки, щоб гарантувати надійний захист системи від потенційних атак. Такий підхід сприяє формуванню висококваліфікованих фахівців у галузі кібербезпеки, готових ефективно впроваджувати заходи захисту в реальних умовах.

Етап розвідки є критично важливим для проведення кібератаків і включає збір різноманітної інформації, яка дозволяє зловмисникам краще

підготувати до атаки та здійснити її з більшою ефективністю. Збір інформації розпочинається із загальних даних про компанію та завершується детальним аналізом технічних параметрів і особистої інформації працівників. Отримана інформація може використовуватися для різних цілей, включаючи соціальну інженерію, тестування на проникнення та інші види кібератак.

Застосування різноманітних інструментів, таких як Nmap, Maltego, Burp Suite, Shodan, OWASP ZAP, Masscan, dnsenum, WHOIS, дозволяє здійснити широкий спектр дій для збору інформації. Наприклад, Nmap визначає активні пристрої та їх порти, Maltego аналізує зв’язки між об’єктами, а Shodan шукає підключені пристрої в Інтернеті.

Також створено 4 сценарія атаки на інформаційні ресурси кіберполігону які націлені на різні його частини, такі як маршрутизатор, базу даних, сервер, веб-сайт, що дасть змогу студентам удосконалити практичні та теоретичні навички у різних ситуаціях, і більш глибоко розібратись у різних техніках і тактиках кібератак.

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Оцінювання наукового ефекту

Основними ознаками наукового ефекту науково-дослідної роботи є новизна роботи, рівень її теоретичного опрацювання, перспективність, рівень розповсюдження результатів, можливість реалізації . Науковий ефект НДР на тему «Модель атак на інформаційні ресурси кіберполігону» можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Значення показників ступеня новизни і рівня теоретичного опрацювання науково-дослідної роботи в балах наведені в табл. 4.1 та 4.2.

Таблиця 4.1 – Показники ступеня новизни науково-дослідної роботи виставлені експертами

Ступінь новизни	Характеристика ступеня новизни	Значення ступеня новизни, бали		
		Експерти (ПІБ, посада)		
		1	2	3
Принципово нова	Робота якісно нова за постановкою задачі і ґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отримані принципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод	0	0	0
Нова	Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів	0	0	0

Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв'язок (або знайдено новий зв'язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об'єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональна модифікація (з ознаками новизни)	54	58	60
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим	0	0	0
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам	0	0	0
Середнє значення балів експертів		57,3		

Згідно отриманого середнього значення балів експертів ступінь новизни характеризується як відносно нова, тобто отримана нова інформація, яка систематизує та узагальює наявну інформаці..

Таблиця 4.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи виставлені експертами

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Експерт (ПІБ, посада)		
	1	2	3
Відкриття закону, розробка теорії	0	0	0
Глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	0	0	0
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	0	0	0
Елементарний аналіз зв'язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо	63	59	58
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	0	0	0
Середнє значення балів експертів	60		

Згідно отриманого середнього значення балів експертів рівень теоретичного опрацювання науково-дослідної роботи характеризується як глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу.

Показник, який характеризує рівень наукового ефекту, визначаємо за формулою [22]:

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор}, \quad (4.1)$$

де $k_{нов}, k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{нов} = 57,3, k_{теор} = 60$ балів;

0,6 та 0,4 – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор} = 0,6 \cdot 57,3 + 0,4 \cdot 60 = 58,38 \text{ балів.}$$

Визначення характеристики показника $E_{нау}$ проводиться на основі висновків експертів виходячи з граничних значень, які наведені в табл. 4.3.

Таблиця 4.3 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Відповідно до визначеного рівня наукового ефекту проведеної науково-дослідної роботи на тему «Модель атак на інформаційні ресурси кіберполігону», даний рівень становить 58,38 балів і відповідає статусу -

середній рівень. Тобто у даному випадку можна вести мову про потенційну фактичну ефективність науково-дослідної роботи.

4.2 Розрахунок витрат на впровадження МКР на тему «Модель атак на інформаційні ресурси кіберполігону»

Основні витрати потрібно розрахувати за такими статями:

− витрати на оплату праці;

− відрахування на соціальні заходи;

− паливо та енергія для науково-виробничих цілей;

− витрати на службові відрядження;

− спецустаткування для наукових (експериментальних) робіт;

− програмне забезпечення для наукових (експериментальних) робіт;

− витрати на роботи, які виконують сторонні підприємства, установи і організації;

− інші витрати;

− накладні (загальновиробничі) витрати.

4.2.1 Витрати на оплату праці

Основна заробітна плата дослідників.

Витрати на основну заробітну плату дослідників ($З_о$) розраховують відповідно до посадових окладів працівників, за формулою:

$$З_о = \sum ((М_{пі} \times t_і) / Т_р), \quad (4.2)$$

де k – кількість посад дослідників, залучених до процесу досліджень;

$М_{пі}$ – місячний посадовий оклад конкретного дослідника, грн;

$t_і$ – кількість днів роботи конкретного дослідника, дн.;

$Т_р$ – середня кількість робочих днів в місяці, $Т_р$=21.

$$З_о = 17000 \cdot 21 / 21 = 17000 \text{ грн.}$$

Таблиця 4.4 – Витрати на заробітну плату дослідників:

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Кількість днів роботи	Витрати на заробітну плату, грн.
Адміністратор	17000	809,5	21	17000
Аспірант	6700	319,04	11	3509,44
Лаборант	6700	319,04	11	3509,44
Всього				24018,88

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i \quad , \tag{4.3}$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} \quad , \tag{4.4}$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду ;

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих

об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

$T_р$ – середнє число робочих днів в місяці, приблизно $T_р$ = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$$C_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}65 / (21 \cdot 8) = 72{,}38 \text{ грн.}$$

$$З_{р1} = 72{,}38 \cdot 5 = 361{,}9 \text{ грн.}$$

Таблиця 4.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Збір ПК	5	2	1.1	72,38	361,9
Підключення та налаштування всіх аппаратних засобів	16	3	1.35	88,83	1421,28
Встановлення ПЗ	8	2	1.1	72,38	579,04
Налаштування мережі	4	4	1.5	98,7	394,8
Налаштування бази данних	4	4	1.5	98,7	394,8
Всього					3151,82

Додаткова заробітна плата дослідників та робітників.

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.5)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$$З_{дод} = (24018,88+3151,82) \cdot 11 / 100\% = 2988,7 \text{ грн.}$$

4.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad , \tag{4.6}$$

де $Н_{зп}$ – норма нарахування на заробітну плату. де $Н_{зп}$ = 22%.

$З_н = (24018,88+3151,82 + 2988,7) \cdot 22 / 100\% = 6635,06$ грн.

4.1.3 Сировина та матеріали

Майже всі процеси відбуваються електронно, але є деяка необхідність у папері для записів, моделювання та друку.

Витрати на матеріали ($М$), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$М = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц_{вj} , \tag{4.7}$$

де $Н_j$ – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = 1,1 ... 1,15);

$В_j$ – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів j-го найменування, грн/кг.

$М_1 = 2,0 \cdot 172,00 \cdot 1,1 - 0 \cdot 0 = 378,4$ грн.

Таблиця 4.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг,шт/грн	Норма витрат, кг,шт	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн

Папір канцелярський офісний (500шт)(А4)	172,00	2,0	0	0	378,4
Стартовий набір в картонній коробці AS111/M	1389,00	1	0	0	1527,9
Настільний набір	378,00	2	0	0	831,6
Картридж для принтера	800	1,0	0	0	880,00
Всього					3617,9

4.2.4 Розрахунок витрат на комплектуючі

Залежно від потреби, кількість комплектуючих кіберполігону може суттєво відрізнятись, для навчального кіберполігону на рівні університету або невеликого комерційного кіберполігону не потрібно досить серйозних затрат, проте деякі комплектючі можуть обійтись доволі дорого, розрахуємо їх за формулою[19]:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (4.8)$$

де $Н_j$ – кількість комплектуючих *j*-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих *j*-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ *= 1,1 ... 1,15*).

$К_в = 1 \cdot 56\ 585 \cdot 1,1 = 62243.5$ *грн*

Таблиця 4.7 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Вартість, грн

Сервер HPE ProLiant DL380 Gen10 (868706-B21/v16)	1	56 585	62243,5
Сервер ARTLINE Business R27 v07 (R27v07)	1	72 344	79578,4
Маршрутизатор TP-LINK Archer AX1500 дводіапазонний WiFi 6	1	2 000	2200
Маршрутизатор TP-LINK TL-R480T+	1	2 029	2231,9
Комплект (ПК+Монітор) ARTLINE Business B27+B24F75plus-IPS (B27v37+B24F75plus-IPS)	5	15 429	84859,5
Кабель LAN CAT 5E(10м) синій	10	153	1683
Конектор Cablexpert Cat.5e 8P8C LC-8P8C-001/10 10 шт.	10	55	605
Клавіатура дротова Vinga KB110BK USB	5	129	709,5
Миша RZTK MR 120 USB Black	5	100	550
Принтер HP Laser 107a	6499	1	7148,9
Всього:			241809,7

4.1.5 Спецустаткування для наукових (експериментальних) робіт

Витрати на спец устаткування відсутні, тому $B_{спец} = 0$.

4.2.6 Програмне забезпечення для наукових (експериментальних) робіт

Балансову вартість програмного забезпечення розраховують за формулою:

$$В_{прг} = \sum Ц_{іпрг} \times С_{пргі} \times К_і, \quad (4.9)$$

де $Ц_{іпрг}$ – ціна придбання одиниці програмного засобу цього виду, грн;

$С_{пргі}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

$К_і$ – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, (Кі = 1,10…1,12);

k – кількість найменувань програмних засобів.

$В_{прг} = 6590 \cdot 5 \cdot 1,1 = 36245$

Таблиця 4.8 Витрати на придбання програмних засобів по кожному виду:

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн.	Вартість, грн
Windows 10	5	6590	36245
Всього			36245

4.2.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою[19]

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.10)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (62243,5 \cdot 1) / (2 \cdot 12) = 2593,47$ *грн.*

Таблиця 4.9 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Сервер HPE ProLiant DL380 Gen10 (868706-B21/v16)	62243,5	2	1	2593,47
Сервер ARTLINE Business R27 v07 (R27v07)	79578,4	2	1	3315,76
Маршрутизатор TP-LINK Archer AX1500 дводіапазонний WiFi 6	2200	2	1	91,6
Маршрутизатор TP-LINK TL-R480T+	2231,9	2	1	92,9
Комплект (ПК+Монітор) ARTLINE Business B27+B24F75plus-IPS (B27v37+B24F75plus-IPS)	84859,5	2	1	3535,81
Принтер HP Laser 107a	7148,9	2	1	297,87
Всього				9927,41

4.2.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою[19]:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.11)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), $Ц_е$ = 7,20 грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 1{,}4 \cdot 168 \cdot 7{,}20 \cdot 0{,}95 / 0{,}97 =$ 230,35*грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.10 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Сервер HPE ProLiant DL380 Gen10 (868706-B21/v16)	1.4	168	230,35
Сервер ARTLINE Business R27 v07 (R27v07)	0,48	168	78,9
Комплект (ПК+Монітор) ARTLINE Business B27+B24F75plus-IPS (B27v37+B24F75plus-IPS)	0,4	168*5	473,86
Маршрутизатори	0,012	168	19,7
Принтер HP Laser 107a	0,2	10	14,1
Всього			816,95

4.2.9 Службові відрядження

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \quad (4.12)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», $Н_{св}$ = 20%.

$$B_{св} = (24018,88+3151,82) \cdot 20 / 100\% = 5434,14 \text{ грн.}$$

4.2.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» відсутні.

4.2.11 Інші витрати.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.13)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 75%.

$$I_в = (24018,88+3151,82) \cdot 75 / 100\% = 20378,02 \text{ грн.}$$

4.2.12 Накладні (загальновиробничі) витрати

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.14)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», $Н_{нзв}$ = 100%.

$$B_{нзв} = (24018,88+3151,82) \cdot 100 / 100\% = 27170,7 \text{ грн.}$$

Витрати на проведення науково-дослідної роботи розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}. \quad (4.15)$$

$B_{заг}$= 24018,88 + 3151,82 +2988,7+6635,06+3617,9+241809,7+0+36245+ +9927,41+816,95+5434,14+0+20378,02+27170,7=382194,28 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.16)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,5

ЗВ=382194,28/0.5=764388,56

4.3 Оцінювання важливості та наукової значимості науково-дослідної роботи

Оцінювання та доведення ефективності виконання науково-дослідної роботи фундаментального чи пошукового характеру є достатньо складним процесом і часто базується на експертних оцінках, тому має вірогідний характер.

Для обґрунтування доцільності виконання науково-дослідної роботи на тему «Модель атак на інформаційні ресурси кіберполігону» використовується спеціальний комплексний показник, що враховує важливість, результативність роботи, можливість впровадження її результатів у виробництво, величину витрат на роботу.

Комплексний показник K_P рівня науково-дослідної роботи може бути розрахований за формулою:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \quad (4.17)$$

де I – коефіцієнт важливості роботи. $I = 3$;

n – коефіцієнт використання результатів роботи; $n = 0$, коли результати роботи не будуть використовуватись; $n = 1$, коли результати роботи будуть використовуватись частково; $n = 2$, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках; $n = 3$, коли результати можуть використовуватись навіть без проведення дослідно-конструкторських розробок. $n = 2$;

T_C – коефіцієнт складності роботи. $T_C = 3$;

R – коефіцієнт результативності роботи; якщо результати роботи плануються вище відомих, то $R = 4$; якщо результати роботи відповідають відомому рівню, то $R = 3$; якщо нижче відомих результатів, то $R = 1$. Приймемо $R = 4$;

B – вартість науково-дослідної роботи, тис. грн. *B = 382194,28* грн;

t – час проведення дослідження. t = 0,08 років, (1 міс.).

Визначення показників *I, n, T_C, R, B, t* здійснюється експертним шляхом або на основі нормативів .

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t} = 3^2 \cdot 3 \cdot 4 / 382{,}1 \cdot 0{,}08 = 3{,}53.$$

Якщо $K_P > 1$, то науково-дослідну роботу на тему «Модель атак на інформаційні ресурси кіберполігону» можна вважати ефективною з високим науковим, технічним і економічним рівнем.

Витрати на проведення науково-дослідної роботи на тему «Модель атак на інформаційні ресурси кіберполігону» складають *382194,28* грн. Відповідно до проведеного аналізу та розрахунків рівень науково-економічного ефекту проведеної науково-дослідної роботи на тему «Модель атак на інформаційні ресурси кіберполігону» є середній, а дослідження актуальними, рівень доцільності виконання науково-дослідної роботи $K_P > 1$, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

ВИСНОВКИ

В магістерській кваліфікаційній роботі проведено моделювання кібератак за допомогою розробленої моделі, розроблено сценарії кібератак на інформаційні ресурси кіберполігону що дозволить покращити обізнаність у кібербезпеці для студентів, які зможуть використати ці сценарії та модель для моделювання атак на інформаційні ресурси кіберполігону.

У 1 розділі розглянуто потребу в моделюванні кібератак на інформаційних ресурсах кіберполігону, проаналізовану існуючі кіберполігони, розглянуто методи тестування безпеки у форматі CTF та Red/Blue team на кіберполігоні, зроблено класифікацію кібератак та розглянуто топ 10 OWASP вразливостей.

У 2 розділі розглянуто які бувають моделі кібератак, а саме модель сценаріїв, модель поведінки та модель загроз, розглянуто концепцію Cyber-kill chain та модель Diamond Model of Intrusion Analysis на освнові яких створена теоретико-множинна модель для моделювання кібератак, за якою проведено моделювання деяких кібератак.

У 3 розділі створений можливий варіант практичної реалізації кіберполігону на базі університету, розглянуто найважливійши етап розвідки, та побудовано декілька видів сценаріїв атак, які направленні на різні частини та ресурси кіберполігону.

У 4 розділі проведенні розрахунки, що-до вартості дослідження та практичної користі.

Результатом роботи є сценарії кібератак, які можна впровадити для навчання студентів, щоб покращити обізнаність з кібербезпеки та практичні навички

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цифровізація суспільства : веб-сайт. URL: https://newacropolis.org.ua /articles/tsyfrovizatsiya-suspilstva (дата звернення: 08.11.2023).

2. 160 Cybersecurity Statistics 2023 **:** веб-сайт. URL: https://www.getastra.com /blog/security-audit/cyber-security-statistics/. (дата звернення: 08.11.2023).

3. Cyber Range Simulator : The Ultimate Test for Cybersecurity Professionals: веб-сайт. URL: https://www.simspace.com/blog/what-to-know-entering-cyber-range-simulation. (дата звернення: 08.11.2023).

4. Dev.ua : веб-сайт. URL: https://dev.ua/news/v-ukraini-zapustyly-kiberpolihon-dlia-praktychnoho-trenuvannia-spetsialistiv-vin-maie-150-stsenariiv-1686759364 (дата звернення: 08.11.2023).

5. Cranford J.J RED TEAM VS BLUE TEAM IN CYBERSECURITY : веб-сайт URL: https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/ (дата звернення: 08.11.2023).

6. Кращі онлайн CTF для хакерів-початківців : веб-сайт. URL: https://spy-soft.net/ctf-online-for-beginners/ (дата звернення: 08.11.2023).

7. Mitre.att&ck : веб-сайт. URL: https://attack.mitre.org/ (дата звернення: 08.11.2023).

8. Mitre.capec : веб-сайт .URL: https://capec.mitre.org/ (дата звернення: 08.11.2023).

9. OWASP : веб-сайт .URL: https://owasp.org/ (дата звернення: 08.11.2023).

10. E. M. Hutchins, M. J. Clopperty, and R. M. Amin, Ph.D. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2010.

11. S. Caltagirone, A. Pendergast, and C. Betz, “Diamond Model of Intrusion Analysis”, Center for Cyber Threat Intelligence and Threat Research, Hanover, MD, Technical Report ADA586960, 05 July 2013.

12. Томашевський В.М. Моделювання систем: навч. посіб. Київ: Видавнича група BHV,2005 – 352с. (с37-44).

13. Фішинг : веб-сайт URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/ (дата звернення: 08.11.2023).

14. What is a DDoS Attack? : веб-сайт URL: https://sucuri.net/guides/what-is-a-ddos-attack/ (дата звернення: 08.11.2023).

15. Cross Site Scripting (XSS) : веб-сайт URL: https://owasp.org/www-community/attacks/xss/ (дата звернення: 08.11.2023).

16. Підручник з SQL веб-сайт URL: https://www.w3schools.com/sql/default.asp (дата звернення: 08.11.2023).

17. SSRF (SERVER-SIDE REQUEST FORGERY) : веб-айт URL: https://cqr.Company/web-vulnerabilities/ssrf/ (дата звернення: 08.11.2023).

18. Security Logging and Monitoring Failures OWASP: веб-айт URL:https://hostsailor.com/blog/security_logging_and_monitoring_failures_owasp/(дата звернення: 08.11.2023).

19. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

ДОДАТКИ

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ
МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Модель атак на інформаційні ресурси кіберполігону
Автор роботи: Трифанюк Ілля Сергійович
Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 95,9 %. Схожість – 4,1 %.
Аналіз звіту подібності (відмітити потрібне):

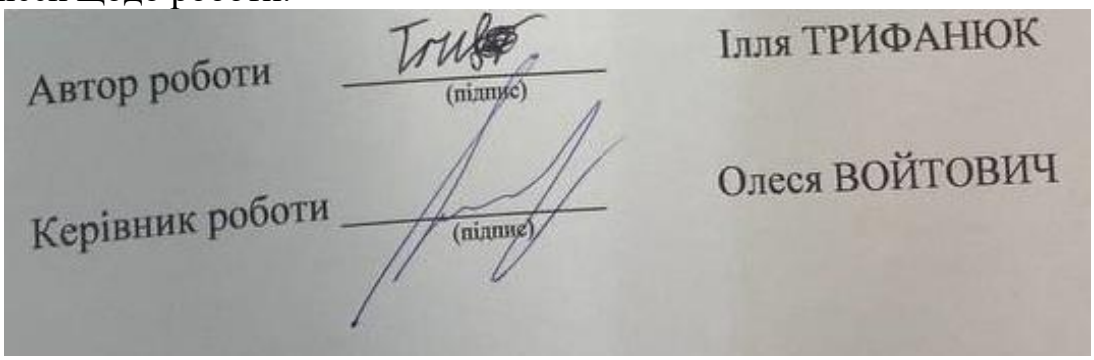
√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Валентина КАПЛУН
(підпис)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.



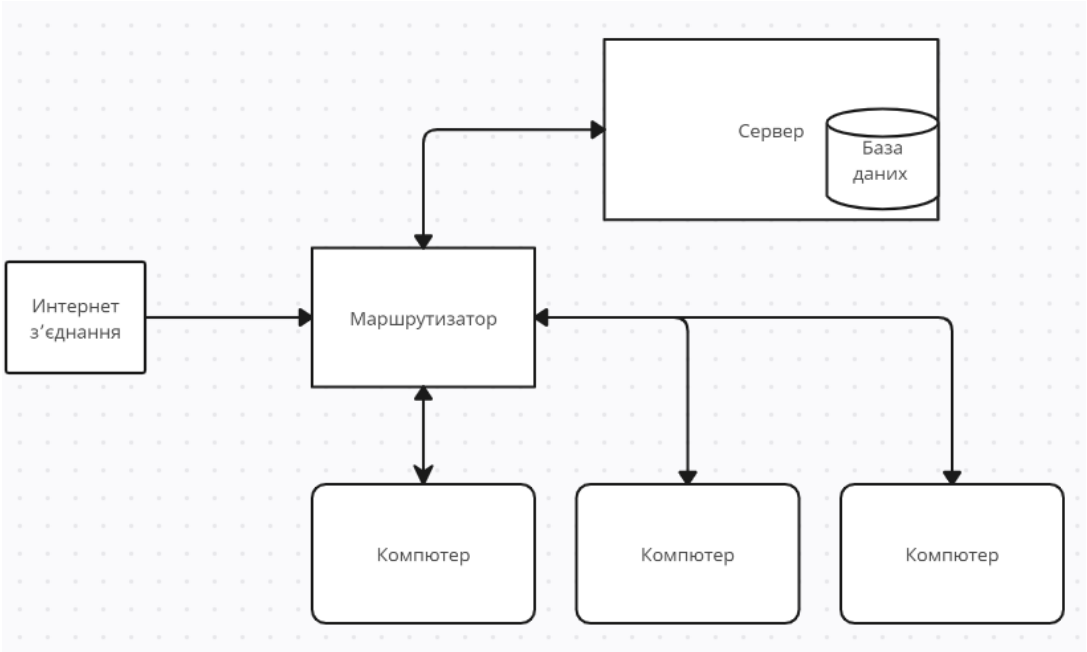
Додаток Б

ІЛЮСТРАТИВНА ЧАСТИНА

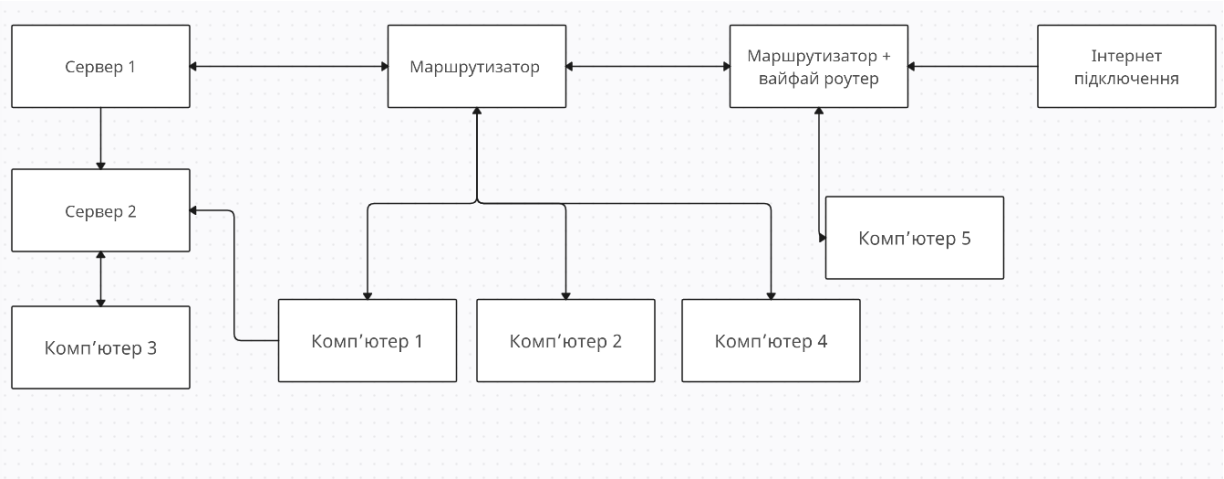
МОДЕЛЬ АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ КІБЕРПОЛІГОНУ

Локальний кіберполігон

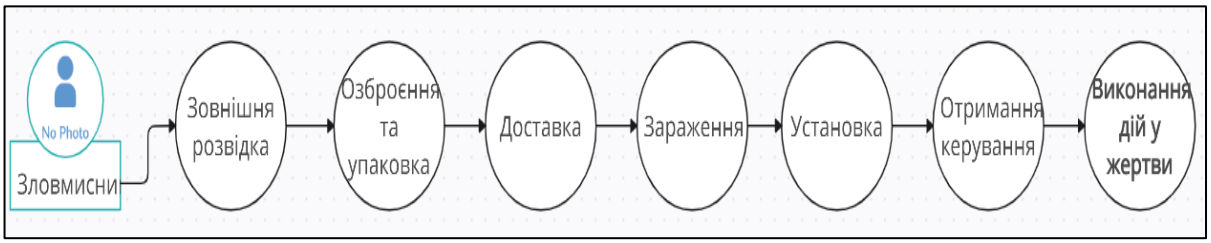
Апаратне забезпечення простого кіберполігону на базі університету



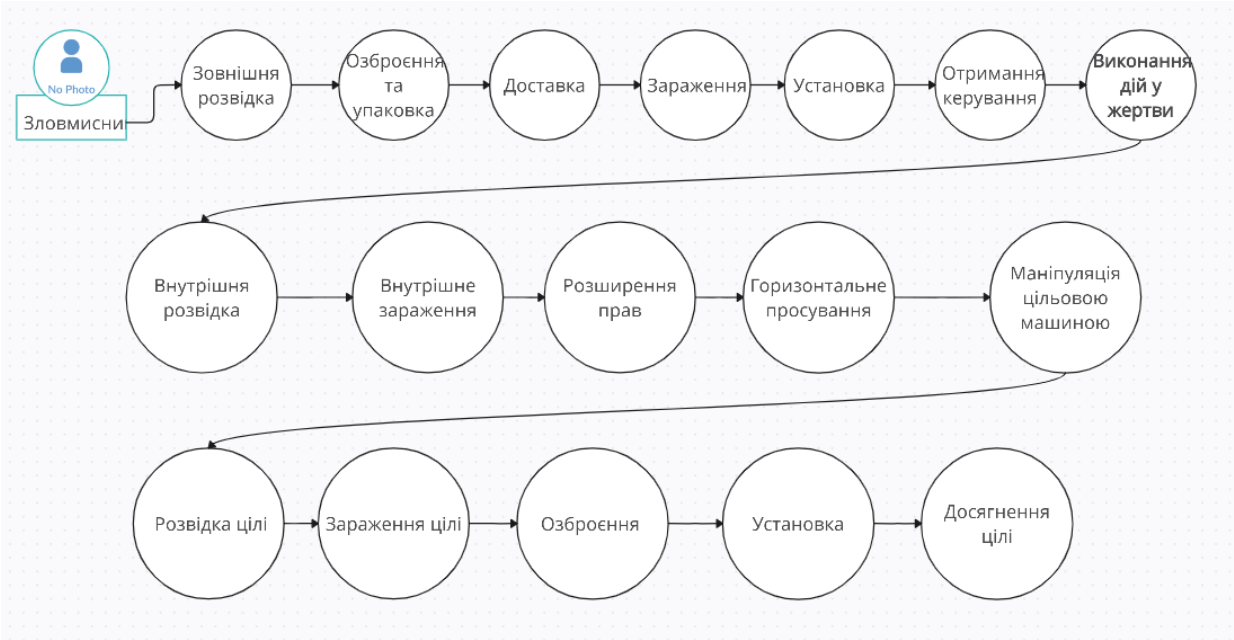
Реалізація апаратної моделі навчального кіберполігону на базі університету



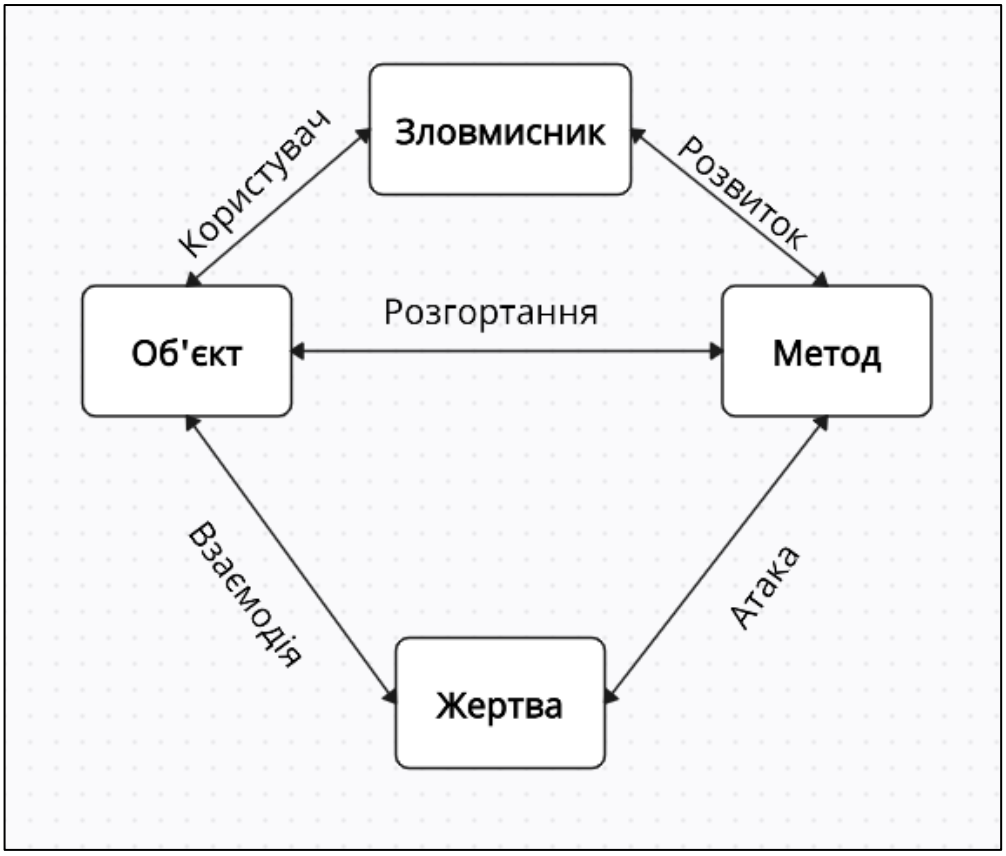
Модель концепції Cyber-Kill Chain



Розширена модель концепції Cyber-Kill Chain



Модель Diamond Model of Intrusion Analysis



Теоретико-множинна модель

S={S1(a1,a2,…an); S2(b1,b2…bn); S3(c1,c2,…cn); S4(d1,d2,…dn);
S5(e1,e2…en); S6(f1,f2,...fn); S7(g1,g2…gn)},

де
S1 – Визначення цілей.

Цілі={система, база даних, сервер,...}

- конкретні об'єкти або ресурси, які можуть бути цілями;
S2 – Розвідка.

Інформація={дані1,дані2,...,дані*n*}

- конкретні дані, які можна збирати про цілі.
S3 – Пошук вразливостей.

Вразливості={паролі, застарілі програми, конфігураційні помилки,...}

- конкретні вразливості, які можуть бути використані для атаки.
S4 – Аналіз вразливостей:

Аналіз={атака1,атака2,...,атака n}

- конкретні аналізи, які допомагають визначити, які атаки можуть бути ефективними.
S5–Використання MITRE:

Тактики={соціальна інженерія, використання вразливостей,...}

- конкретні тактики атак.

Техніки={Фішінг, SQLInjection,...}

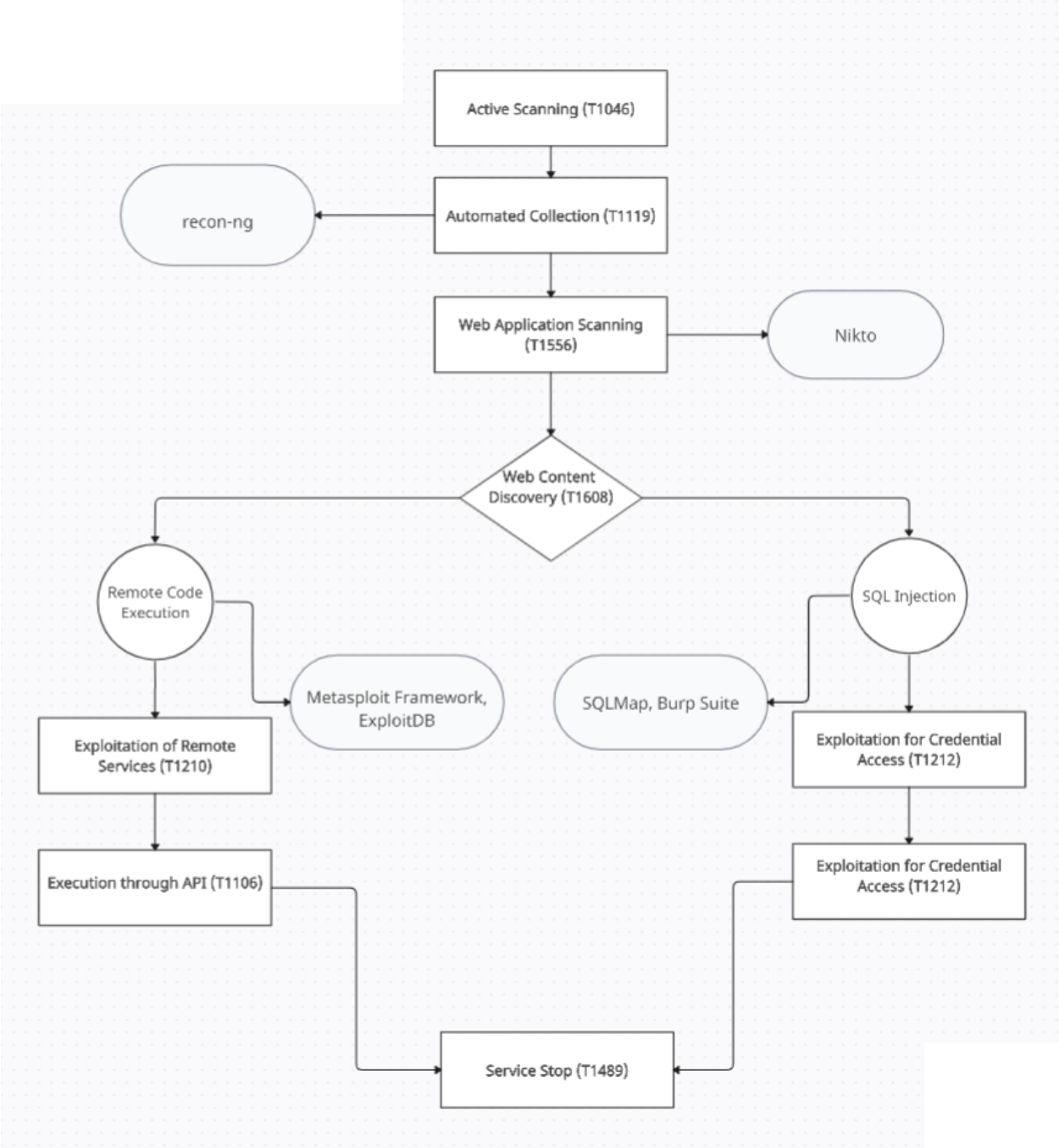
- конкретні техніки атаки.
S6–Виконання атаки:

Виконані атаки={атака1, атака2,..., атака n}

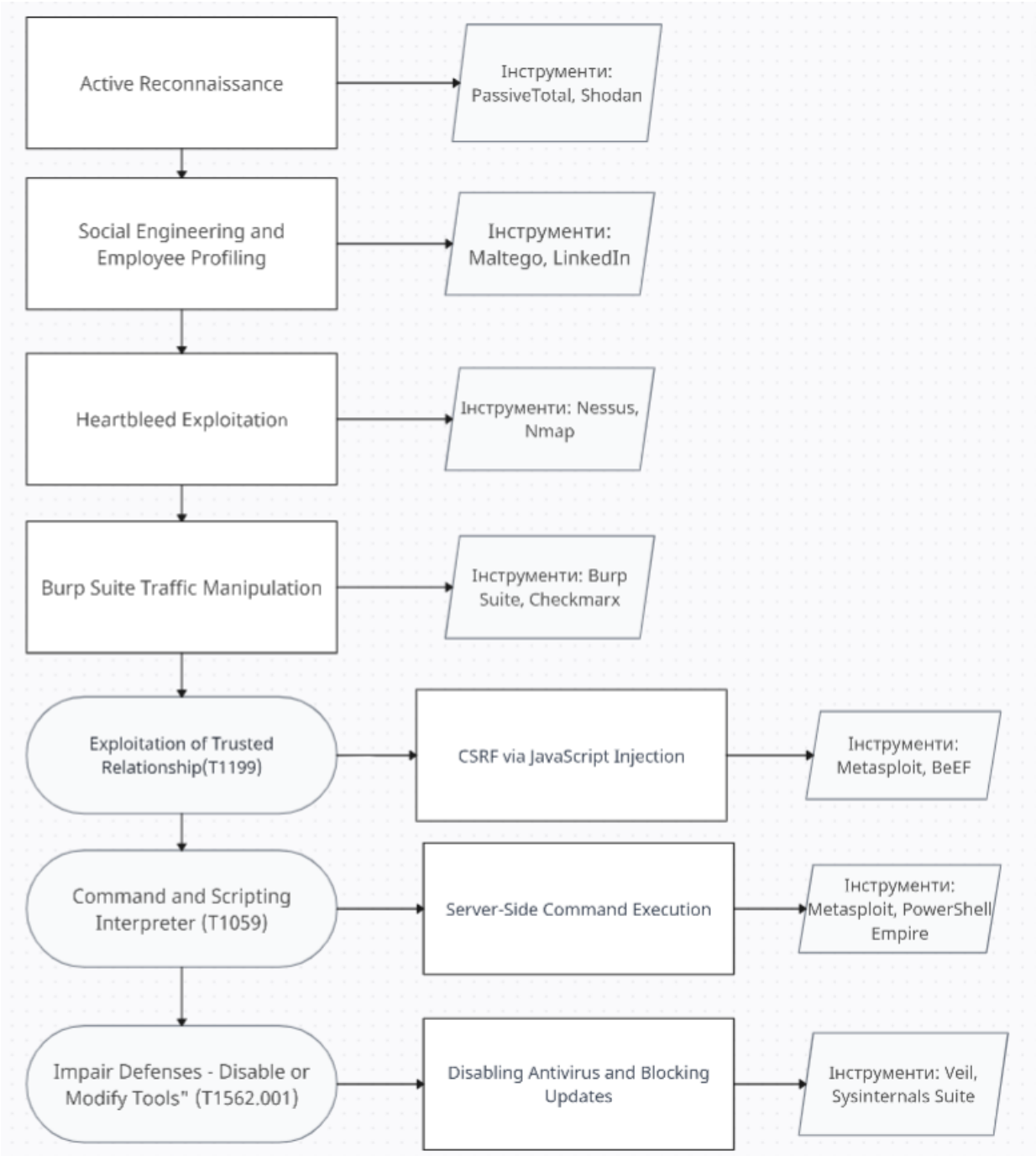
- відображає виконані атаки на основі використання певних тактик та технік.
S7–Пост-експлуатація:

Наслідки={отримання доступу, крадіжка даних, розповсюдження ШПЗ,...}
- конкретні наслідки виконаних атак.

Сценарій атаки на кіберполігон з розгалуженнями



Лінійний сценарій атаки на кіберполігон



Сценарій атаки на маршрутизатор кіберполігону