Міністерство освіти і науки України
Вінницький національний технічний університет Факультет
інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Комплексна бакалаврська дипломна робота на тему:
«Кіберполігон для дослідження подій інформаційної безпеки. Частина 1. Модуль для імітації атак»

Виконав: студент 2 курсу групи 1БС – 21мс
спеціальності 125 Кібербезпека
_____Блоха А.О.

Керівник: к. т. н., доцент кафедри ЗІ
_____Войтович О. П.
«16» червня 2023 р.

Рецензент: к.т.н., доц., доцент кафедри ПЗ
_____Коваленко О. О.
«16» червня 2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____Лужецький В. А.
«16» червня 2023 р.

Вінниця ВНТУ – 2023 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти І (бакалаврський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо – професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Зав. кафедри ЗІ,
д. т. н., проф.
Володимир ЛУЖЕЦЬКИЙ
«20» березня 2023 р.

ЗАВДАННЯ
НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Блосі Андріану Олександровичу

1. Тема роботи: «Кіберполігон для дослідження подій інформаційної безпеки. Частина 1. Модуль для імітації атак»

керівник роботи: Войтович Олеся Петрівна, к. т. н., доцент кафедри ЗІ,

затверджені наказом ректора ВНТУ від 20 березня 2023 року №67.

2. Строк подання студентом роботи 16 червня 2023 р.

3. Вихідні дані до роботи:

– кіберполігон;

– попередній аналіз даних щодо різноманітних атак в ІКС;

– реалізація відомих методів атак;

– експериментальне дослідження запропонованих рішень.

4. Зміст текстової частини: Вступ. 1. Аналіз інформаційних джерел. 2. Розробка моделей атак для імітації. 3. Налаштування та реалізація модуля імітації атак. Висновки.

5. Перелік ілюстративного матеріалу: Потік активного розвідувального сканування (плакат А4). Модель циклу отримання доступу (плакат А4). Модель циклу підвищення привілеїв (плакат А4). Модель циклу підробки ідентифікатора батьківського процесу (PPID) (плакат А4). Модель циклу здійснення атаки на відмову в обслуговуванні (плакат А4). Процес виявлення інфраструктури IAAS (плакат А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання при
1	Войтович О. П., к.т.н., доц. каф.ЗІ	20.03.23	16.06.23
2	Войтович О. П., к.т.н., доц. каф.ЗІ	20.03.23	16.06.23
3	Войтович О. П., к.т.н., доц. каф.ЗІ	20.03.23	16.06.23

6. Дата видачі завдання 20 березня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

ч	Назва етапів комплексної бакалаврської дипломної роботи	Строк виконання етапів роботи	Прим
1	Аналіз завдання. Вступ	20.03.23 – 26.03.23	
2	Аналіз джерел за напрямком комплексної бакалаврської дипломної роботи	27.03.23 – 09.04.23	
3	Розробка архітектури та алгоритму засобу	10.04.23 – 23.04.23	
4	Програмна реалізація та тестування	24.04.23 – 21.05.23	
5	Аналіз результатів тестування, висновки	22.05.23 – 24.05.23	
6	Оформлення пояснювальної записки	25.05.23 – 31.05.23	
7	Попередній захист та доопрацювання БДР	01.06.23 – 15.06.23	
8	Представлення БДР на захист	16.06.23 – 19.06.23	
9	Захист БДР	20.06.23 – 23.06.23	

Студент _____ Андріан БЛО

Керівник роботи _____ Олеся ВОЙТОВИ

АНОТАЦІЯ

Бакалаврська кваліфікаційна робота складається з 61 сторінок формату А4, на яких є 18 рисунків, 1 таблиці, 7 схем, список використаних джерел містить 19 найменувань.

Бакалаврська робота присвячена розробці та реалізації кіберполігону з модулем для імітації атак у контексті дослідження подій інформаційної безпеки. Кіберполігон є симуляційною середовищем, яке дозволяє імітувати різноманітні кібератаки та вразливості, що можуть стати причиною порушення безпеки інформаційних систем. У роботі розглядаються основні аспекти побудови кіберполігону, включаючи архітектуру, компоненти та функціональні можливості. Основна увага приділяється модулю для імітації атак, який дозволяє створювати різноманітні типи кібератак, включаючи відомі вразливості та сценарії атак. Для реалізації модуля використовуються сучасні методи та інструменти кібербезпеки. Зокрема, використовується знання про вразливості систем, методи атак та захисту, а також використання сучасних інструментів для моделювання та імітації атак.

Ключові слова: кіберполігон, кібератака, модель, DoS, фішинг, інформаційно-комунікаційна система, програмний засіб.

ABSTRACT

The bachelor's thesis consists of 61 pages of A4 format, on which there are 18 figures, 1 table, 7 diagrams, the list of used sources contains 19 items.

The bachelor thesis is devoted to the development and implementation of a cyber polygon with a module for generating attacks in the context of information security event research. The cyber training ground is a simulation environment that allows you to simulate various cyber attacks and vulnerabilities that can cause a violation of the security of information systems. The paper examines the main aspects of building a cyber polygon, including architecture, components, and functionality. The main focus is on the attack generation module, which allows the creation of various types of cyber attacks, including known vulnerabilities and attack scenarios. Modern cyber security methods and tools are used to implement the module. In particular, knowledge about system vulnerabilities, methods of attacks and protection, as well as the use of modern tools for modeling and simulating attacks is used.

Keywords: cyber polygon, cyber attack, model, DoS, phishing, information and communication system, software.

ЗМІСТ

ВСТУП

У світі швидкого технологічного розвитку зростає потреба у захисті комп'ютерних систем від різних видів кібератак. З кожним роком злочинні елементи знаходять нові способи, якими можуть завдати шкоди електронним пристроям та інформаційним системам, що утримують важливу інформацію. Щоб відстояти вірогідність таких атак, необхідно розробляти та вдосконалювати методи захисту і тестування комп'ютерних систем. Один із способів тестування імітує кібератаки на власній системі. Це моделювання атак, яке дозволяє проводити випробування на проникнення, перевіряти стійкість систем до відповідних загроз та удосконалювати захист. Кіберполігон – це зручний інструмент для такого типу тестування.

Метою бакалаврської роботи є покращення захисту інформаційно комунікаційних систем за допомогою розробки моделей кібератак, які можуть бути використані в кіберполігонах для тестування захисту комп'ютерних систем.

Завданнями є проаналізувати відомі атаки для імітації; розробити моделі атак для імітації; налаштування та робробка атак для кіберполігону; протестувати отримані рішення.

Предметом дослідження є відомі атаки, які можна реалізувати в рамках кіберполігону для дослідження подій кібербезпеки.

Об’єктом дослідження є процес імітації атак на інформаційно-комунікаційну систему в рамках кіберполігону.

Результати проекту можуть бути використані для забезпечення високої стійкості інформаційно-комунікаційних систем до різних типів кібератак.

Проміжні результати бакалаврської роботи обговорювались на LII Науково-технічній конференції факультету інформаційних технологій та комп'ютерної інженерії (2023).

Блоха А. О. МОДУЛЬ ДЛЯ ГЕНЕРАЦІЇ АТАК [Електронний ресурс] / А. О. Блоха, О. П. Войтович // Матеріали Всеукраїнської науково-практичної інтернет-конференції [1].

1 АНАЛІЗ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1.1 Аналіз задач при імітації атак

У сучасному цифровому світі кібератаки стають не тільки все поширенішими, але й дедалі складнішими та швидкіше розвиваються. Кіберзлочинці постійно вдосконалюють свої методи, використовують нові технології та постійно адаптуються до заходів, прийнятих для їх запобігання.

Кібератаки стали настільки поширеними, що стало практично неможливо позбутися повністю ризику їх виникнення. Незалежно від розміру організації чи масштабу її мережі, ніхто не повністю захищеним до потенційних загроз. Кіберзлочинці спроможні атакувати різні цілі, включаючи урядові установи, корпорації, навчальні заклади, фінансові установи, медичні системи та приватних осіб. Залежно від мотивації кіберзлочинців, атаки можуть бути спрямовані на крадіжку фінансової інформації, розголошення конфіденційних даних, спричинення розладу в системах, шпигунство або політичні цілі.

Кібератаки швидко розвиваються, виробляючи нові методи та інструменти для зламування систем. Кіберзлочинці постійно оновлюють свої навички і засоби, використовують нові технології та розвивають складні атаки. Наприклад, з'явилися такі загрози, як розподілені атаки на відмову в обслуговуванні (DDoS), вимагання викупу, атаки на програмне забезпечення та використання штучного інтелекту для проведення цілеспрямованих атак.

Одним з основних факторів, що призводить до швидкого розвитку кібератак, є зростання кількості підключених пристроїв у мережі. Зростання кількості пристроїв, які можуть бути атаковані, створює нові можливості для злочинців.

Захист від кібератак стає невід'ємною частиною будь-якої організації або користувача. Регулярне оновлення програмного забезпечення, встановлення ефективних систем захисту, навчання персоналу та своєчасне виявлення

аномальної активності стають необхідними заходами для боротьби з кібератаками. Проте, розвиток технологій кібербезпеки не вистежує швидкого темпу зростання кіберзлочинності, що ставить під загрозу безпеку мережевих ресурсів.

У сучасних комп'ютерних мережах та цифровому середовищі відбувається надзвичайно велика кількість подій, пов'язаних з інформаційною безпекою. ІБ - події включають в себе різноманітні активності та події, які відбуваються в мережах, серверах, комп'ютерах, програмах та інших елементах інформаційної інфраструктури. Серед цих подій часто зустрічаються інциденти інформаційної безпеки, причиною яких є атаки. Сучасні статистичні дані свідчать про зростаючу кількість інцидентів інформаційної безпеки, пов'язаних з атаками. Наприклад, згідно з дослідженням, проведеним компанією Accenture, лише протягом одного року кількість виявлених ІБ - інцидентів зросла на 11%. Це свідчить про постійне зростання загроз та злочинної активності в кіберпросторі.

Статистика показує, що кібератаки широко поширені і постійно розвиваються. Ось кілька фактів.

За даними звіту "Verizon 2021 Data Breach Investigations Report", було виявлено більше 29 000 інцидентів безпеки та понад 5 200 підтверджених даних про порушення в 2020 році[2].

Загалом 85% розглянутих у звіті порушень так чи інакше пов’язані з людським фактором.

Фішинг (phishing) у 2021 р., як і раніше, був найпопулярнішою тактикою порушення безпеки даних. Порівняно з попереднім 2020 р. кількість інцидентів із застосуванням фішингу зросла ще на 11% та досягла 36% їх загальної кількості. Велику роль відіграло поширення COVID-19, що спричинило збільшення комунікацій та замовлень онлайн і дало зловмисникам нову тему для маніпуляцій.

Друге місце посіла компрометація корпоративних імейлів (Business Email Compromises – BECs). 2021 р. кількість випадків уведення в оману

(misrepresentation) користувачів виявилася в 15 разів більшою проти попереднього року.

Удвічі частіше (у 10% випадків), як порівняти з 2020 р., застосували програми-вимагачі (ransomware), що 2021 р. опинилися на третьому місці. Таке зростання зумовлено новими зловмисними тактиками, як-от викрадення даних під час їх шифрування.

Основним вектором хакерських атак досі є вебдодатки, причому 80 % таких атак спричиняють порушення безпеки даних. Так, на друге місце в Hacking vectors перемістилися програми шерингу робочого столу ПК (screensharing, desktop sharing).

Інциденти й порушення безпеки даних 2021 р. внаслідок компрометації активів організацій відбувалися в зовнішніх хмарних сховищах (external cloud assets) частіше, аніж на домашніх серверах у приміщеннях (on-premises assets). Отже, кількість скомпрометованих персональних пристроїв знизилася.

61 % порушень безпеки даних були пов’язані з обліковими даними.

Медіанне значення втрат від інцидентів 2021 р. склало $21659 при загальному діапазоні сум таких утрат від $826 до $653587.

За даними "Cybersecurity Ventures", вартість злочинів у сфері кібербезпеки може сягати 6 трільйонів доларів до 2021 року[3].

За дослідженням "Ponemon Institute's 2020 Cost of a Data Breach Report", середній витрати на розслідування та відновлення після кібератаки складають близько 3,86 млн доларів.

Згідно з дослідженням "CyberEdge Group's 2021 Cyberthreat Defense Report", 80% організацій зазнали принаймні однієї кібератаки в 2020 році[4].

За даними "Symantec's Internet Security Threat Report", кількість нових загроз безпеці збільшилась на 40% у 2020 році, досягнувши 5,6 мллрд.

1.2 Аналіз відомих атак

Зараз інформаційні системи та мережі стали невід'ємною частиною життя людей та організацій, тому їх вразливість до кібератак стала дуже великою.

Кібератаки можуть бути спрямовані на отримання фінансової вигоди, викрадення конфіденційної інформації, завдання шкоди репутації та інші цілі. Кіберзлочинці постійно вдосконалюють свої методи та техніки для злому та викрадення інформації, тому відомі методи та прийоми захисту можуть бути недостатніми для запобігання кібератакам.

Кібератаки можна класифікувати за різними критеріями. Наприклад, за видами злому, методами атак, метою та іншими параметрами. Розглянемо детальніше деякі типи кібератак, що найчастіше застосовуються злочинцями.

Існує низка моделей атак, які використовуються зловмисниками для злому комп'ютерних систем і мереж. Ось декілька найпоширеніших моделей атак.

1.2.1 Модель "Вторгнення в мережу"

Модель "Вторгнення в мережу" (Network Intrusion): Ця модель атаки передбачає незаконне проникнення до комп'ютерної мережі зловмисником з метою отримати доступ до системи, отримати конфіденційну інформацію або завдати шкоди мережевим ресурсам. Це може включати в себе сканування портів, використання вразливостей, введення зловмисного коду і зловживання привілеями.

Модель "Вторгнення в мережу" (Network Intrusion) є однією з найбільш складних і широко поширених форм кібератак. Ця атака полягає в незаконному проникненні зловмисника до комп'ютерної мережі з метою отримання доступу до системи, отримання конфіденційної інформації або завдання шкоди мережевим ресурсам [5].

Процес вторгнення в мережу може включати наступні етапи (рис 1.1):

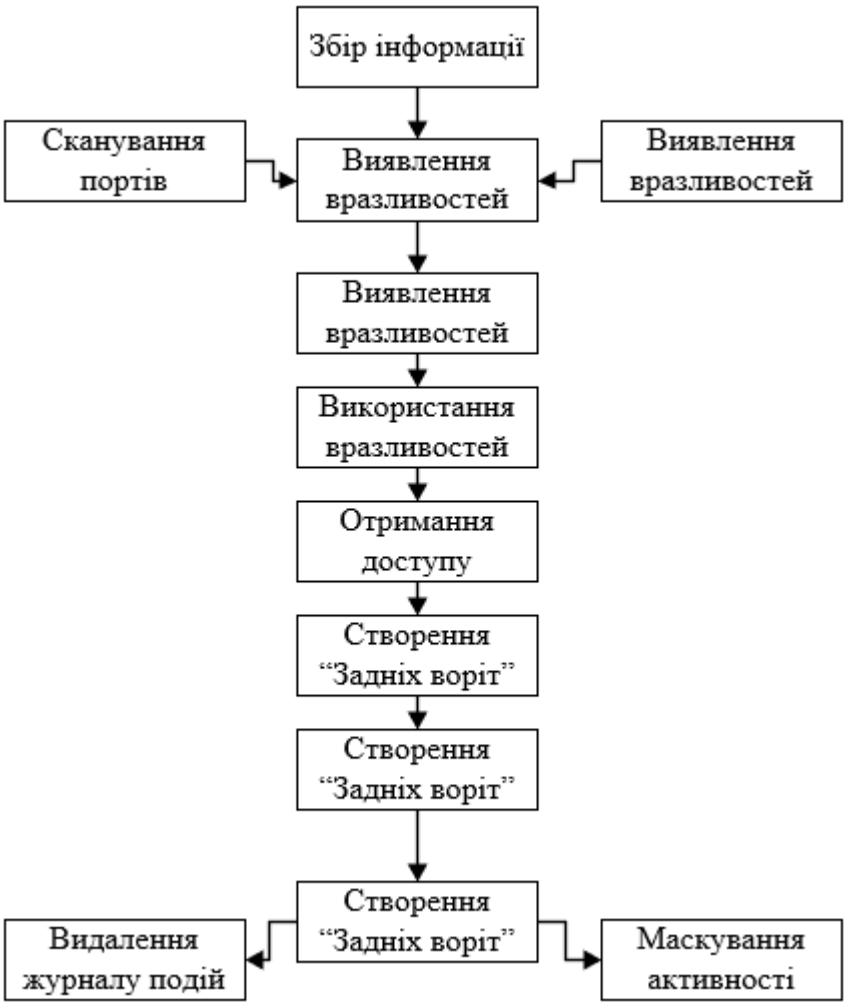


Рисунок 1.1- Процес вторгнення в мережу

Етап 1 - розвідка (Reconnaissance). Збір інформації: зловмисник здійснює пошук і збір інформації про цільову мережу. Це включає виявлення хостів, портів, служб, мережевих топологій та інших характеристик.

Сканування портів: зловмисник використовує спеціальні програми для сканування мережі на предмет виявлення відкритих портів. Це дозволяє зловмисникові встановити, які сервіси або протоколи доступні на хостах мережі.

Виявлення вразливостей: зловмисник використовує інструменти для виявлення вразливостей в мережевих системах та сервісах. Це допомагає встановити можливі шляхи атаки.

Етап 2 - експлуатація (Exploitation) – використання вразливостей: після знаходження вразливостей в мережевих системах або сервісах зловмисник

використовує їх для здійснення атаки. Вразливості можуть бути пов'язані з недостатньо захищеними паролями, слабою конфігурацією сервісів, використанням застарілих версій програмного забезпечення або відомих вразливостей.

Етап 3 - захоплення контролю (Control Acquisition) – отримання доступу: після успішної експлуатації вразливостей зловмисник отримує контроль над системою або мережею. Він може отримати привілейований доступ, створити облікові записи адміністратора або встановити шкідливе програмне забезпечення для забезпечення подальшого доступу.

Етап 4 - Забезпечення доступу (Access Maintenance) – створення "задніх воріт": зловмисник може створити "задні ворота" або інші механізми для збереження доступу до системи. Це дозволяє залишатися непоміченим і знову отримати доступ до системи навіть після виявлення та виправлення вразливостей.

Етап 5 - приховування слідів (Covering Tracks): видалення журналів подій - зловмисник може видаляти або модифікувати журнали подій, щоб приховати свої сліди в системі.

Етап 6 - маскування активності: зловмисник вживає заходів для маскування своєї активності в мережі, щоб уникнути виявлення його присутності.

Вторгнення в мережу може мати різноманітні наслідки, такі як втрата конфіденційної інформації, втрата контролю над системою, втрата доступу до мережевих ресурсів, втрата продуктивності та інші шкоди. Для захисту від таких атак необхідно використовувати ефективні механізми безпеки, такі як брандмауери, системи виявлення і запобігання вторгненням, регулярне оновлення програмного забезпечення, складні паролі та виправлення вразливостей.

1.2.2 Модель "Фішинг"

Модель "Фішинг" (Phishing): Фішинг – це соціально – інженерна атака, в якій зловмисник намагається обманути користувачів, щоб вони надали свої

конфіденційні дані, такі як паролі, номери кредитних карт або іншу особисту інформацію (рис 1.2). Це може бути здійснено шляхом підробки електронних повідомлень, веб – сайтів або соціальних мереж з метою виглядати як легітимні джерела[6].

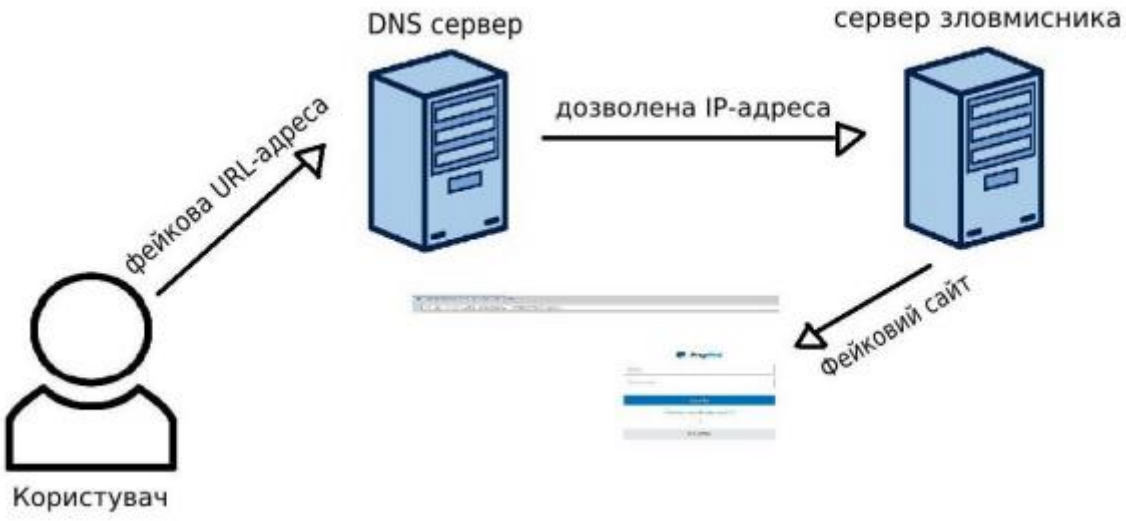


Рисунок 1.2 – Схема фішингу

Основний сценарій фішингу – атаки включає наступні етапи:

Етап 1 - підготовка. Створення підробленого джерела – зловмисники створюють виглядом схожий на офіційне джерело, таке як підроблений веб – сайт, електронне повідомлення, соціальна мережа або додаток. Вони можуть використовувати подібний дизайн, логотипи, інтерфейси та навіть доменні імена, щоб підштовхнути жертву довіритися їм.

Збір інформації – зловмисники можуть знаходити інформацію про потенційних жертв, таку як адреси електронної пошти, імена, контактні дані або інші деталі, для персоналізації атаки і зробити її більш переконливою.

Етап 2 - виклик до дії. Відправка фішингового повідомлення – зловмисники відправляють електронні листи або повідомлення через соціальні мережі, які здаватимуться легітимними. Ці повідомлення можуть містити підроблені логотипи, імена відомих компаній, спливаючі вікна або вимоги негайних дій.

Соціальний інженеринг – зловмисники використовують різні психологічні техніки, щоб заманити жертву до виконання певних дій. Наприклад, вони можуть створити вигадану нагороду, надати залякування про можливі наслідки або створити виглядом надзвичайної ситуації, що вимагає негайної уваги.

Етап 3 - збір інформації. Введення конфіденційних даних – зловмисники намагаються переконати жертву ввести свої особисті дані на підробленій сторінці або формі. Це може бути пароль, номер кредитної карти, дата народження або будь – яка інша конфіденційна інформація.

Зловживання даними – після отримання конфіденційних даних, зловмисники можуть використовувати їх для здійснення шахрайських дій, таких як крадіжка грошей, ідентичність або здійснення інших кримінальних діянь.

Етап 4 - приховування слідів. Закриття атаки – зловмисники можуть намагатися приховати свою активність, видаливши свої сліди, включаючи видалення фішингових повідомлень, знищення підроблених веб – сайтів або закриття спільного доступу до компрометованої інфраструктури.

Фішинг – атаки можуть мати серйозні наслідки для жертв, такі як фінансові втрати, викрадення особистих даних, шкода репутації або навіть правові проблеми. Для захисту від фішингу важливо бути обережними при взаємодії з електронними повідомленнями та веб – сайтами. Рекомендується уважно перевіряти посилання, використовувати сильні паролі, установлювати антивірусне програмне забезпечення, оновлювати програмне забезпечення та вести навчання щодо кібербезпеки.

1.2.3 Модель "Вірус"

Модель "Вірус" (Virus): Віруси – це шкідливі програми, які прикріплюються до існуючих файлів або програм і поширюються через інфіковані системи. Вони можуть розмножуватися і поширюватися на інші файли або системи, завдавати шкоди даним, перехоплювати інформацію або навіть призводити до зупинки системи[7].

Основні етапи роботи вірусу включають(рис 1.3):

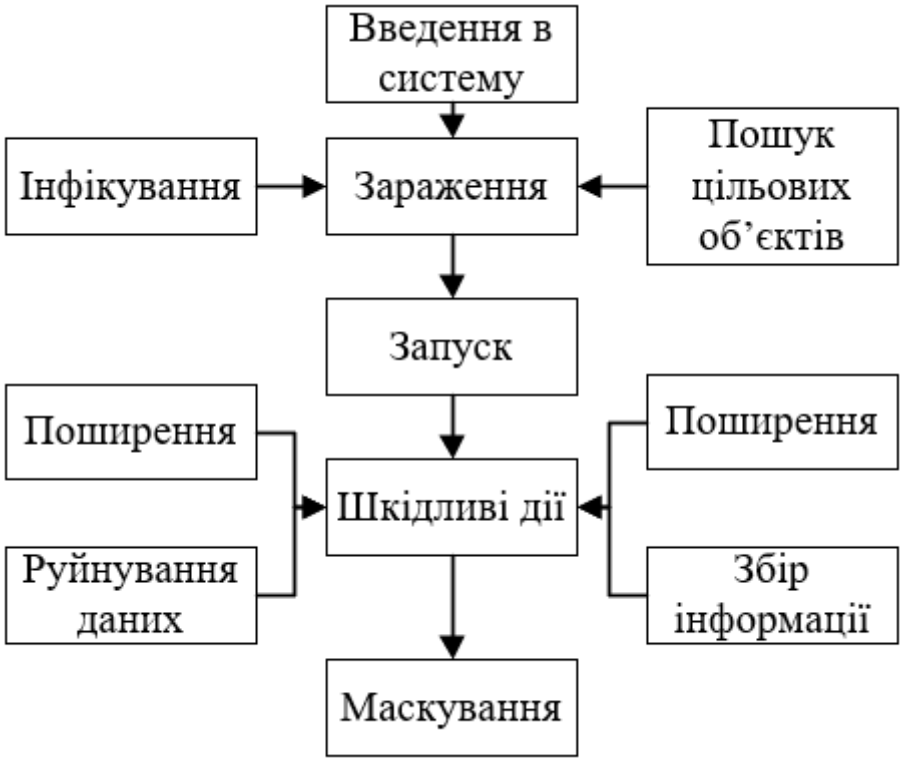


Рисунок 1.3 – Основні етапи моделі "Вірус"

Етап 1 - зараження. Введення в систему – віруси можуть потрапити на комп'ютер через інфіковані електронні листи, завантажені файли з ненадійних джерел, підроблені програми або вразливості в операційній системі або програмному забезпеченні.

Пошук цільових об'єктів – після потрапляння в систему, вірус починає пошук нових файлів або програм, які він може інфікувати. Вірус може сканувати диски, мережі або навіть пам'ять комп'ютера, щоб знайти підходящі цільові об'єкти.

Інфікування об'єктів – вірус вбудовує свій код в об'єкти, такі як виконувані файли, документи, архіви або розширення браузера. Це дозволяє вірусу розповсюджуватися і забезпечує йому можливість запускатися під час виконання інфікованого об'єкта.

Етап 2 - активація. Запуск вірусу – після інфікування об'єктів вірус очікує на активацію. Це може бути спеціальна дата, подія або виконання певних умов. Після активації вірус виконує свої шкідливі дії.

Етап 3 - шкідливі дії. Поширення – вірус може поширюватися шляхом інфікування інших файлів або програм в системі, а також через мережі або зовнішні пристрої. Він може створювати копії свого коду та розсилати їх по електронній пошті до контактів жертви або використовувати інші канали комунікації для розповсюдження.

Руйнування даних – вірус може знищувати, пошкоджувати або блокувати доступ до файлів, дисків або системних ресурсів. Він може стерти або змінити дані, що призводить до втрати інформації або некоректної роботи системи.

Збирання інформації – деякі віруси можуть збирати конфіденційні дані, такі як паролі, банківські реквізити або особисту інформацію. Вони можуть надсилати зібрані дані зловмисникам або використовувати їх для злочинних цілей.

Етап 4 - приховування. Маскування – вірус може приховувати свій код або діяльність, щоб уникнути виявлення антивірусним програмним забезпеченням або системними механізмами безпеки. Він може зашифровувати свій код, використовувати методи обфускації або модифікувати себе для унікальності.

Віруси можуть завдати серйозних шкідливих наслідків, таких як втрата даних, некоректна робота системи, крадіжка конфіденційної інформації або збитки в бізнесі. Для запобігання вірусним атакам рекомендується використовувати актуальне антивірусне програмне забезпечення, оновлювати системне програмне забезпечення, оберігати відкривати невідомі або підозрілі файли, а також вести постійний моніторинг та бекапування даних.

1.2.4 Модель "Відмова в обслуговуванні"

Модель "Відмова в обслуговуванні" (Denial of Service DoS): В атаках DoS зловмисники спробують перенаситити цільову систему або ресурси, такі як мережеві пропускні здатності або серверні потужності, шляхом надсилання

великого обсягу запитів або заборонених даних. Це призводить до перевантаження ресурсів і зниження доступності для легітимних користувачів[8].

Основні етапи роботи атаки DoS включають:

Етап 1 - ідентифікація цілі. Визначення цілі – зловмисники визначають цільову систему або сервіс, до якого вони планують здійснити атаку. Це може бути веб – сайт, мережевий сервер, електронна пошта або будь – який інший сервіс, доступ до якого вони хочуть припинити.

Збір інформації – зловмисники здійснюють дослідження цільової системи, її інфраструктури та вразливостей. Вони можуть використовувати автоматизовані інструменти для сканування мережі або відкритих портів, аналізувати конфігурацію системи та встановлені служби.

Етап 2 - підготовка атаки. Вибір методу атаки – зловмисники вибирають метод атаки DoS, який найбільше підходить для цільової системи. Це може бути "напад на перенавантаження мережі" (Network Flooding), "напад на затрати обчислювальних ресурсів" (Resource Consumption), "напад на вразливості програмного забезпечення" (Software Vulnerability), "напад на протоколи комунікації" (Protocol Exploitation) та інші.

Конфігурація інструментів – зловмисники налаштовують спеціальні інструменти або програми, які допомагають в реалізації атаки. Ці інструменти можуть бути здатні генерувати великий обсяг трафіку, створювати фальшиві запити або використовувати ресурси системи неефективним чином.

Етап 3 - здійснення атаки. Запуск атаки – зловмисники запускають атаку, використовуючи підготовлені інструменти. Вони намагаються перевантажити цільову систему, направляючи на неї великий обсяг трафіку або використовуючи вразливості для споживання ресурсів.

Відмова в обслуговуванні – в результаті атаки ресурси цільової системи стають перевантаженими або вичерпані, що призводить до відмови в обслуговуванні законних користувачів. Система може стати недоступною, повільною або некоректною у своїй роботі.

Етап 4 - приховування слідів. Маскування атаки – зловмисники можуть приховувати свою активність або походження атаки, використовуючи проксі – сервери, анонімізуючі сервіси або інші техніки. Вони можуть намагатись залишити мінімальні сліди, щоб ускладнити виявлення та відслідковування.

Атаки DoS можуть призвести до серйозних наслідків, таких як втрата продуктивності бізнесу, втрати даних або недоступність сервісів для користувачів. Для захисту від таких атак рекомендується використовувати заходи безпеки, такі як фільтрація трафіку, виявлення та блокування ненормальних запитів, а також масштабованість ресурсів для впорядкування збільшення навантаження.

1.2.5 Модель "Злом паролю"

Модель "Злом паролю" (Password Cracking): В атаках на злом паролю зловмисники намагаються отримати несанкціонований доступ до системи або акаунту, вгадуючи, перебираючи або використовуючи викрадені паролі. Вони можуть використовувати програми для перебору паролів або використовувати словникові атаки, спираючись на загальні або поширені паролі[9].

Основні методи злому паролю включають наступне.

Словникова атака (Dictionary Attack): зловмисники використовують заранее підготовлені словники, які містять потенційні паролі, поширені слова, комбінації символів та інші варіанти. Вони перебирають ці слова один за одним, спробуючи знайти збіг зі значенням пароля.

Атака грубою силою (Brute Force) – зловмисники систематично перебирають всі можливі комбінації символів, починаючи з коротких і простих паролів і закінчуючи довгими та складними. Вони спробують всі можливі варіанти, поки не знайдуть правильний пароль.

Геш – атака (Hash Attack) – зловмисники використовують хеш – функції для створення хеш – значень паролів, які зберігаються в системі або базі даних. Вони обчислюють хеш – значення для потенційних паролів і порівнюють їх зі збереженими хешами для знаходження збігу.

Райдужні – таблиці (Rainbow Tables) – зловмисники використовують рейнбоу – таблиці, які містять заздалегідь обчислені хеш – значення для великої кількості можливих паролів. Вони швидко шукають збіг між гешами з бази даних та рейнбоу – таблицями для відновлення оригінальних паролів.

Соціальна інженерія (Social Engineering) – зловмисники використовують методи соціальної інженерії, щоб отримати пароль безпосередньо від користувача. Це може включати відправку фішингових повідомлень, підбор інформації про користувача або психологічне впливання на них.

Для захисту від атак злому паролю рекомендується використовувати наступні практики.

Використання сильних паролів – потрібно використовувати довгі паролі, що складаються з різних символів, цифр та різного регістру.

Багаторазове використання паролів – не можна використовувати один і той самий пароль для різних облікових записів.

Використання двохфакторної автентифікації – потрібно вмикати додатковий рівень захисту, який вимагає додаткового підтвердження при вході.

Шифрування паролів – рекомендується зберігати паролі в зашифрованому вигляді, використовуючи сучасні алгоритми хешування.

Регулярна зміна паролів – також рекомендується змінювати свої паролі періодично, особливо для важливих облікових записів.

Враховуючи ці рекомендації, користувачі можуть знизити ризик злому паролю і зберегти свою конфіденційність та безпеку своїх облікових записів.

Модель "Кібершпигунство" (Cyber Espionage): Кібершпигунство передбачає незаконне отримання конфіденційної інформації або розробку засобів для здобуття переваги в політичних, економічних або військових сферах[10].

Основні аспекти кібершпигунства включають наступне.

Цільова інформація. Конфіденційні дані – кібершпигуни спрямовують свої зусилля на отримання конфіденційних даних, таких як таємниці компаній,

державні секрети, технологічні розробки, плани військових операцій і політичні стратегії.

Інтелектуальна власність – кібершпигуни намагаються отримати доступ до цінних технологічних розробок, винаходів, патентів або комерційних секретів, які можуть дати їм перевагу в галузі конкуренції.

Методи кібершпигунства. Вторгнення в мережі – кібершпигуни здійснюють атаки на комп'ютерні системи та мережі, використовуючи шкідливі програми, вразливості або соціальну інженерію, щоб отримати несанкціонований доступ до системи.

Фішинг та спам – кібершпигуни використовують фішингові атаки та надсилають шкідливі спам – повідомлення для отримання доступу до облікових записів та розповсюдження шкідливих програм.

Викрадення ідентифікації – кібершпигуни використовують методи для викрадення ідентифікаційних даних, таких як логіни та паролі, для незаконного доступу до систем та облікових записів.

Використання шпигунського програмного забезпечення – кібершпигуни розробляють та розповсюджують шпигунське програмне забезпечення, яке дозволяє віддалено перехоплювати, слідкувати та викрадати інформацію з заражених систем.

Наслідки кібершпигунства. Втрата конфіденційності – кібершпигунство може призвести до витоку конфіденційної інформації, що може завдати значних збитків компаніям або державам.

Порушення приватності – особиста інформація та дані користувачів можуть бути скомпрометовані кібершпигунами, що призводить до порушення приватності та можливого зловживання цими даними.

Економічна шкода – крадіжка комерційних секретів і технологічних розробок може вразити економіку країни або конкретні компанії, зменшуючи їхню конкурентоспроможність.

Для захисту від кібершпигунства необхідно вживати наступні заходи[11]:

– Регулярне оновлення програмного забезпечення та патчів систем для заповнення вразливостей.

– Використання сильних паролів та багатофакторної аутентифікації. Використання ефективного антивірусного програмного забезпечення та брандмауерів.

– Контроль за вхідними та вихідними мережевими з'єднаннями та моніторинг активності мережі.

– Навчання користувачів про фішингові атаки та інші методи соціальної інженерії.

– Застосування шифрування для захисту конфіденційної інформації.

– Регулярні аудити безпеки та перевірки на наявність зловмисного програмного забезпечення.

Враховуючи ці заходи, організації та користувачі можуть знизити ризик кібершпигунства та зберегти конфіденційність своїх даних та інформацію.

Зловмисники можуть використовувати різні методи, такі як вторгнення до комп'ютерних систем, перехоплення комунікацій або викрадення даних, для отримання цієї інформації. Ці моделі атак є лише деякими прикладами існуючих загроз у кіберпросторі. Зловмисники постійно розвивають нові та вдосконалюють існуючі методи атак, тому важливо підтримувати свої системи оновленими і приймати відповідні заходи безпеки для захисту від цих загроз.

1.3 Актуальність використання кіберполігону

Кіберполігон (Cyber Range) є інноваційною платформою, яка дозволяє проводити імітаційні та навчальні сесії для тестування, тренування та вдосконалення навичок з кібербезпеки(рис. 1.4). У рамках кіберполігону проводяться різноманітні симуляції кібератак, що дає змогу організаціям та кіберспеціалістам реалістично вивчити та протистояти загрозам кібербезпеки. Необхідність проведення атак в рамках кіберполігону випливає з декількох

факторів таких як тренування та навички – кібератаки є складними і динамічними, і вони постійно еволюціонують[12].

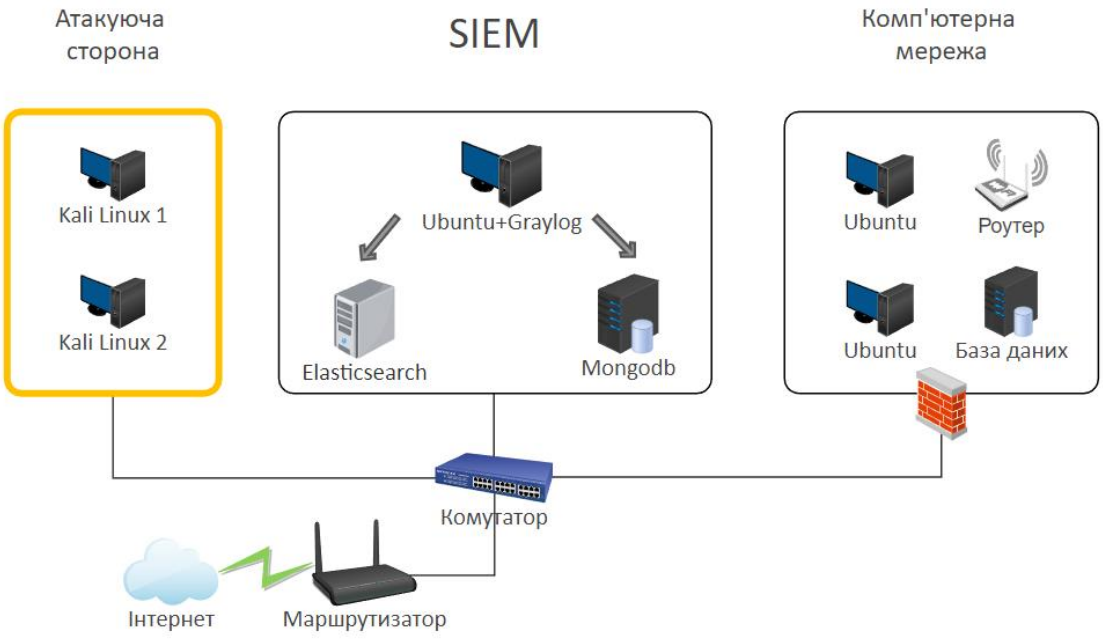


Рисунок 1.4 – Схема кіберполігону

Проведення атак у контрольованому середовищі кіберполігону дозволяє тренувати кіберспеціалістів та організації, набувати нових навичок, вчитися реагувати на кіберзагрози та вдосконалювати стратегії захисту.

Виявлення вразливостей – проведення атак дозволяє виявити слабкі місця в системах та мережах. Шляхом симуляції реальних кібератак можна виявити потенційні вразливості, помилки в конфігурації, недостатні заходи безпеки та інші слабкі місця, які можуть бути використані зловмисниками.

Тестування та оцінка систем безпеки – кіберполігон дає можливість тестувати ефективність заходів безпеки, виявляти їхню ефективність та оцінювати рівень готовності систем до реальних кібератак. Це дозволяє виявити потенційні проблеми та удосконалити заходи безпеки перед їх застосуванням в реальному середовищі.

Розробка та вдосконалення стратегій захисту – проведення атак допомагає в розробці та вдосконаленні стратегій захисту. Аналізуючи результати симуляції атак, організації можуть ідентифікувати слабкі місця, розробити стратегії та політики безпеки, покращити реагування на інциденти та підвищити загальний рівень кібербезпеки.

Оцінка впливу – проведення атак в рамках кіберполігону дозволяє оцінити потенційний вплив кібератак на організацію. Це дозволяє визначити можливі наслідки, втрати даних, порушення бізнес – процесів та інші шкодливі наслідки, що можуть виникнути внаслідок реальних кібератак. Така оцінка допомагає організаціям виявити слабкі місця та розробити стратегії для мінімізації ризиків та підвищення стійкості до кіберзагроз.

Підготовка кадрів – кіберполігон надає можливість тренувати та підготувати нових кіберспеціалістів. Симуляція різних видів кібератак допомагає зрозуміти їх характеристики, методи та техніки, що дозволяє кадрам з кібербезпеки набувати практичного досвіду та вмінь. Це особливо корисно для молодих спеціалістів, які можуть навчитися аналізувати, реагувати та вирішувати загрози.

Співпраця та обмін даними – кіберполігон створює сприятливу платформу для співпраці та обміну даними між організаціями, кіберспеціалістами та іншими зацікавленими сторонами. Це дозволяє спільно вивчати нові види кіберзагроз, обговорювати стратегії захисту, ділитися навичками та кращими практиками.

Такий обмін даними сприяє підвищенню рівня кібербезпеки загалом та ефективному протистоянню загрозам.

Переваги та недоліки використання кіберполігону приведені у таблиці 1.

Таблиця 1 – Переваги та недоліки використання кіберполігону.

	Переваги	Недоліки
1	Можливість навчання та тестування на живих сценаріях кібератак.	Вартість налагодження та підтримки кіберполігону.

2	Збільшення ефективності виявлення та реагування на кібератаки.	Обмежена реальність тестування, оскільки кіберполігон може не повністю відображати умови реального виробничого середовища.
3	Створення контрольованого середовища для аналізу середовища та ризиків.	Можлива страта конфіденційності у разі використання зовнішніх кіберполігонів.
4	Тренування персоналу з кібербезпеки.	Можливість некоректного інтерпретування результатів тестування.
5	Відсутність реальних наслідків та пошкоджень у виробничому середовищі.	Відсутність фактора невизначенності, який присутній у реальній кібератаці.
6	Можливість створення різних сценаріїв та умов для тестування	

До інших переваг використання кіберполігону для тестування захисту комп'ютерних систем можна віднести[13].

Симулювання реальних атак. Кіберполігон може відтворювати сценарії атак, які відбуваються в реальному світі, що дозволяє протестувати захист комп'ютерних систем у реалістичних умовах.

Можливість оцінювання рівня захищеності. Кіберполігон дозволяє оцінювати рівень захисту комп'ютерної системи, виявляти слабкі місця та розробляти стратегії підвищення рівня захищеності.

Відсутність ризику втрати даних. Тестування захисту комп'ютерної системи за допомогою кіберполігону не пов'язане з ризиком втрати даних або порушенням їх конфіденційності, що є важливим фактором для бізнесу та інших організацій.

Економічна ефективність. Використання кіберполігону може бути більш економічно вигідним способом тестування захисту комп'ютерних систем, порівняно з наймом професійних хакерів або проведенням реальних тестів з використанням живих атак[14].

Щодо недоліків кіберполігону, слід зазначити, що його ефективність може бути обмеженою, якщо він не відповідає конкретним потребам тестування

системи. Наприклад, якщо кіберполігон не враховує конфігурацію системи чи неможливість відтворити окремі атаки, то результати його роботи можуть бути неповними або недостовірними.

Також важливо враховувати те, що кіберполігон може бути використаний лише для тестування імітованих середовищ, що може відрізнятися від реальних умов експлуатації системи. Це означає, що результати тестування можуть бути не зовсім релевантними реальному стану захисту системи.

Ще одним недоліком використання кіберполігону може бути складність використання і обмежені можливості налаштування. Деякі інструменти для створення кіберполігону можуть бути складними у використанні, що може знизити продуктивність тестування та збільшити час на налаштування середовища.

Отже, кіберполігон – це потужний інструмент для тестування захисту комп'ютерних систем, який дозволяє моделювати різні типи атак та перевіряти ефективність захисту системи. Однак, перед його використанням, необхідно ретельно зважити на переваги та недоліки, що він пропонує, і забезпечити правильне налаштування тестування, щоб отримати найбільш точні результати.

1.4 Атакуюча сторона Red team

Red team в кіберполігоні – це команда спеціалістів, яка виконує роль потенційного зловмисника з метою виявлення та вирішення вразливостей в інформаційній системі або мережі. Red team працює в опозиції до Blue team, яка відповідає за захист та безпеку системи.

Детальний опис роботи Red team в кіберполігоні включає наступні етапи та дії.

Етап 1 - планування та підготовка: Red team визначає цілі атаки та об'єкти, які підлягають перевірці в кіберполігоні.

Етап 2 - збір інформації: команда збирає дані про цільову систему або мережу, включаючи топологію, архітектуру, слабкі місця та вразливості.

Етап 3 - розробка плану атаки: Red team розробляє детальний план атаки, включаючи вибір методів, інструментів та технік, які використовуються під час симуляції атак.

Етап 4 - виконання атак: Red team намагається отримати несанкційний доступ до системи або мережі, використовуючи різноманітні методи, такі як фішинг, використання вразливостей, перехоплення аутентифікаційних даних тощо.

Етап 5 - підвищення привілеїв: після отримання початкового доступу, Red team використовує методи та експлойти для підвищення свого рівня привілеїв в системі або мережі.

Етап 6 - збір інформації та розвідка: Red team активно сканує та аналізує цільову систему, виявляє активні порти, служби, вразливості, збирає конфіденційну інформацію та виконує розвідку.

Етап 7 - розповсюдження: після отримання контролю над системою або мережею, Red team розповсюджується, поширює свій доступ і намагається збільшити свою впливову зону.

Етап 8 - збір і аналіз результатів: Red team збирає дані про всі дії, виконані під час атаки, включаючи логи подій, пакети мережевого трафіку та інші відомості.

Етап 9 - аналіз вразливостей: команда проводить детальний аналіз вразливостей, використаних під час атаки, та визначає, які заходи захисту були обходяться.

Етап 10 - оцінка ризиків: Red team оцінює ризики, пов'язані з виявленими вразливостями, і надає рекомендації щодо виправлення проблем та підвищення рівня безпеки.

Етап 11 - звітність та рекомендації: Red team складає детальний звіт про виявлені вразливості, успішно виконані атаки, отриману інформацію та рекомендації щодо поліпшення безпеки системи.

Етап 12 - презентація результатів: команда представляє свої результати, звіт та рекомендації відповідним зацікавленим сторонам.

Важливо відзначити, що Red team проводить свою роботу у контрольованому середовищі кіберполігону, з використанням заздалегідь узгоджених процедур та зі згоди власника системи або мережі. Метою Red team є виявлення слабких місць і підвищення рівня безпеки шляхом виявлення і усунення вразливостей та недоліків в інформаційній системі або мережі.

1.5 Постановка завдання

Постановка завдання для побудови модуля імітації атак на кіберполігоні включатиме наступні етапи.

Вибір технологій і інструментів: обераються підходящі технології та інструменти для реалізації модуля імітації атак.

Визначення типів атак: потрібно розглянути різні типи атак, які будуть генеруватись на кіберполігоні. Це можуть бути наприклад DDoS-атаки, атаки на проникнення, фішинг, використання вразливостей програм тощо.

Визначення сценаріїв атак: розробляються конкретні сценарії атак для кожного типу атаки, враховуючи їх характеристики, цілі і можливі наслідки. Потрібно встановити параметри атак, такі як інтенсивність, тривалість, цільові об'єкти і методи.

Реалізація атак: потрібно написати код для імітації атак, використовуючи визначені сценарії. Забезпечити, реалістичність та відповідність вимогам кіберполігону.

Тестування та налагодження: потрібно виконати тестування модуля імітації атак, перевірити його працездатність та ефективність. Виправити помилки та вдосконалити модуль, якщо потрібно.

Документація та звітність: підготувати документацію для модуля імітації атак, включаючи опис функціональності, використання, параметрів атак, залежностей від інших модулів і технологій. Зробити звіт про реалізацію та тестування модуля.

2 РОЗРОБКА МОДЕЛЕЙ АТАК ДЛЯ ІМІТАЦІЇ

На інформаційно-комунікаційні системи (ІКС) можуть бути спрямовані різноманітні атаки, які можна класифікувати за різними критеріями. Ось деякі типи атак, які можуть відбуватись на ІКС:

Спам та фішинг: атаки спаму та фішингу полягають у відправці небажаних повідомлень або масової розсилці електронних листів, які містять шкідливі посилання або вкладення. Метою таких атак є виведення користувачів з ладу або отримання їхніх особистих даних.

Шкідливі програми: шкідливі програми можуть бути розповсюджені через ІКС з метою нанесення шкоди. Троянські програми, черв'яки та інші види шкідливого програмного забезпечення можуть поширюватись інфікованими файлами, електронною поштою, вразливостями програм і т. д.

Відома в обслуговуванні (DDoS): атаки типу DDoS (розподілена атака з обмеженням доступу до сервісу) спрямовані на перевантаження серверів, мережевих ресурсів або програм, завдяки чому легітимні користувачі не зможуть отримати доступ до ІКС.

Витік інформації: це атаки, спрямовані на викрадення конфіденційної або чутливої інформації з ІКС. Наприклад, хакер може скористатись вразливістю в системі і отримати доступ до даних, які мають бути обмежені для певних користувачів.

Формування ботнетів: хакери можуть намагатись створити ботнет, тобто мережу комп'ютерів або пристроїв, які були заражені шкідливим програмним забезпеченням, щоб використовувати їх для злочинних цілей, наприклад, відправляти спам, проводити DDoS – атаки або здійснювати крадіжку обчислювальних ресурсів.

Використання вразливостей: хакери можуть експлуатувати вразливості в програмах або операційних системах, які використовуються в ІКС. Вони можуть застосовувати відомі уразливості для здійснення несанкціонованого доступу, виконання коду або інших шкідливих дій.

Це лише декілька прикладів атак, які можуть відбуватись на ІКС. Захист ІКС вимагає комплексного підходу, який включає в себе застосування безпечних практик програмування, регулярне оновлення програмного забезпечення, встановлення ефективної системи виявлення і запобігання вторгненням (IDS/IPS), використання міцних паролів та шифрування даних, а також навчання користувачів у питаннях кібербезпеки.

2.1 Розробка моделі “Розвідка”

Противники можуть виконувати активне розвідувальне сканування, щоб зібрати інформацію, яку можна використовувати під час націлювання[15].

Активне сканування – це сканування, під час якого зловмисник досліджує інфраструктуру жертви через мережевий трафік, на відміну від інших форм розвідки, які не передбачають прямої взаємодії (рис 2.1). Зловмисники можуть виконувати різні форми активного сканування залежно від того, яку інформацію вони прагнуть зібрати.

Ці сканування також можна виконувати різними способами, зокрема за допомогою власних функцій мережевих протоколів, таких як ICMP.

Інформація з цих сканувань може виявити можливості для інших форм розвідки (наприклад: Пошук відкритих веб – сайтів/доменів або Пошук відкритих технічних баз даних), створення оперативних ресурсів (наприклад: розвиток можливостей або Отримання можливостей) та/або початкове доступ (наприклад: зовнішні віддалені служби або Експлойти загальнодоступної програми).

Зловмисники можуть сканувати IP – блоки, щоб зібрати інформацію про мережу жертви , наприклад, які IP – адреси активно використовуються, а також більш детальну інформацію про хости, яким призначено ці адреси.

Сканування може варіюватися від простих запитів ping (запити та відповіді ICMP) до більш тонких сканувань, які можуть виявити програмне забезпечення/версії хоста через банери сервера чи інші мережеві артефакти.

Інформація з цих сканувань може виявити можливості для інших форм розвідки (наприклад: Пошук відкритих веб – сайтів/доменів або Пошук відкритих технічних баз даних), встановлення оперативних ресурсів (наприклад: Розвиток можливостей або Отримання можливостей) та/або початковий доступ (наприклад : зовнішні віддалені служби).

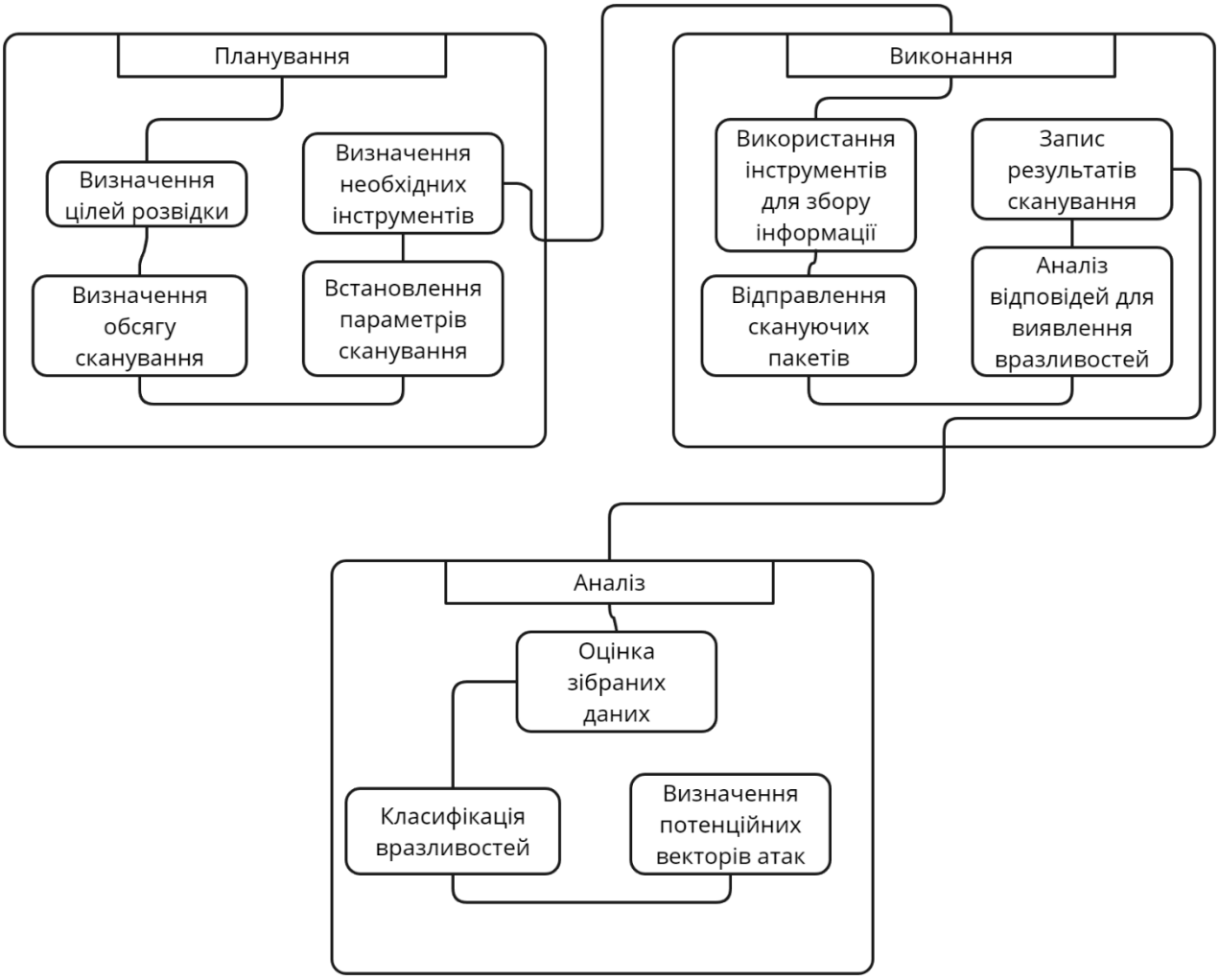


Рисунок 2.1 – Потік активного розвідувального сканування

Зловмисники можуть сканувати жертви на наявність вразливостей, які можна використовувати під час націлювання.

Сканування вразливостей зазвичай перевіряє, чи конфігурація цільового хоста/програми (наприклад, програмне забезпечення та версія) потенційно відповідає цілі конкретного експлойту, який може спробувати використати

зловмисник. Ці сканування можуть також включати більш широкі спроби зібрати інформацію про хост-жертву , яка може бути використана для виявлення більш загальновідомих вразливостей, які можна використовувати.

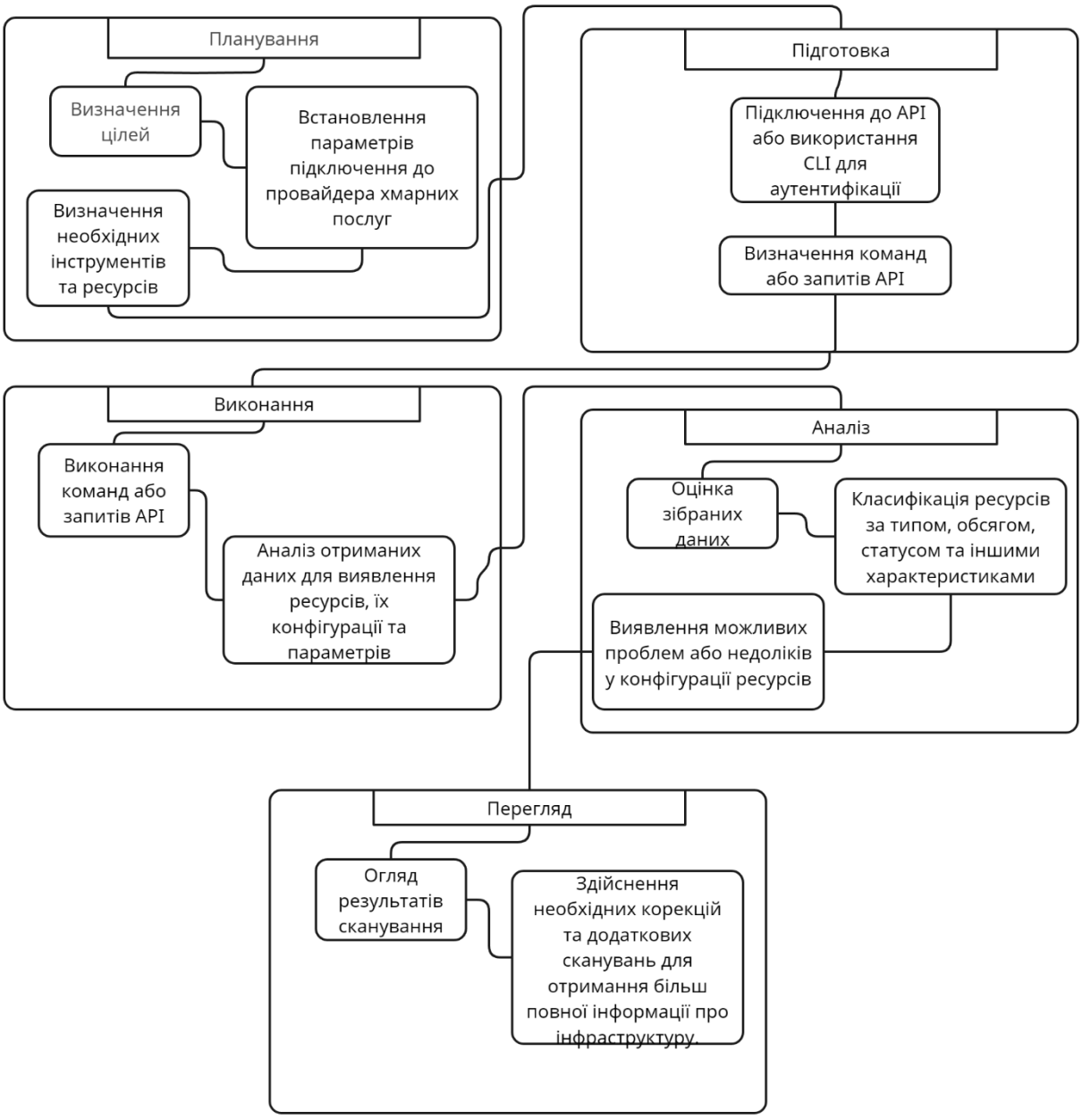


Рисунок 2.2 – Процес виявлення інфраструктури IaaS

Сканування вразливостей зазвичай збирає запущене програмне забезпечення та номери версій через банери сервера, порти прослуховування або інші мережеві артефакти. Інформація з цих сканувань може виявити можливості для інших форм розвідки (наприклад: пошук відкритих веб – сайтів/доменів або

Пошук відкритих технічних баз даних), створення оперативних ресурсів та/або початковий доступ.

Зловмисник може спробувати виявити інфраструктуру та ресурси, доступні в середовищі інфраструктури як послуги (IaaS) (рис 2.2). Це включає ресурси обчислювальної служби, такі як екземпляри, віртуальні машини та знімки, а також ресурси інших служб, включаючи служби зберігання даних і бази даних.

Постачальники хмарних послуг пропонують такі методи, як API та команди, що видаються через CLI, для надання інформації про інфраструктуру.

Окрім команд API, зловмисники можуть використовувати інструменти з відкритим кодом, щоб виявити інфраструктуру хмарних сховищ за допомогою сканування списку слів. Зловмисник може перерахувати ресурси, використовуючи ключі доступу зламаного користувача, щоб визначити, які доступні цьому користувачеві.

2.2 Розробка моделі “Отримання доступу”

Зловмисники можуть придбати або іншим чином отримати існуючий доступ до цільової системи чи мережі. Для продажу доступу до раніше скомпрометованих систем доступні різноманітні онлайн – сервіси та мережі посередників початкового доступу. У деяких випадках групи супротивників можуть створювати партнерства для спільного використання скомпрометованих систем одна з одною.

Точка опори для скомпрометованих систем може мати різні форми, наприклад доступ до встановлених бекдорів (наприклад, Web Shell) або встановлений доступ через зовнішні віддалені служби . У деяких випадках брокери доступу імплантують скомпрометовані системи з «навантаженням», яке можна використовувати для встановлення додаткового шкідливого програмного забезпечення для клієнтів, які платять.

Використовуючи існуючі мережі посередників доступу, а не розробляючи або отримуючи власні початкові можливості доступу, зловмисник потенційно може зменшити ресурси, необхідні для закріплення в цільовій мережі, і зосередити свої зусилля на наступних етапах компрометації. Зловмисники можуть пріоритетно отримати доступ до систем, які, як було визначено, не мають моніторингу безпеки або мають високі привілеї, або систем, які належать організаціям у певному секторі.

У деяких випадках придбання доступу до організації в таких секторах, як IT-підряди, розробка програмного забезпечення або телекомунікації, може дозволити зловмиснику скомпрометувати додаткові жертви через довірені стосунки, перехоплення багатофакторної автентифікації або навіть компрометацію ланцюга постачання .

2.3 Розробка моделі “Початковий доступ”

Зловмисники можуть отримати доступ до системи, якщо користувач відвідує веб-сайт під час звичайного перегляду (рис 2.3). За допомогою цієї методики веб-браузер користувача зазвичай є ціллю для експлуатації, але зловмисники також можуть використовувати скомпрометовані веб-сайти для неексплуатаційної поведінки, наприклад для отримання маркера доступу до програми.

Існує кілька способів доставки коду експлойту в браузер (наприклад, Drive – by Target), зокрема, законний веб-сайт скомпрометовано, якщо зловмисники ввели певну форму шкідливого коду, наприклад JavaScript, iFrames і міжсайтовий сценарій.

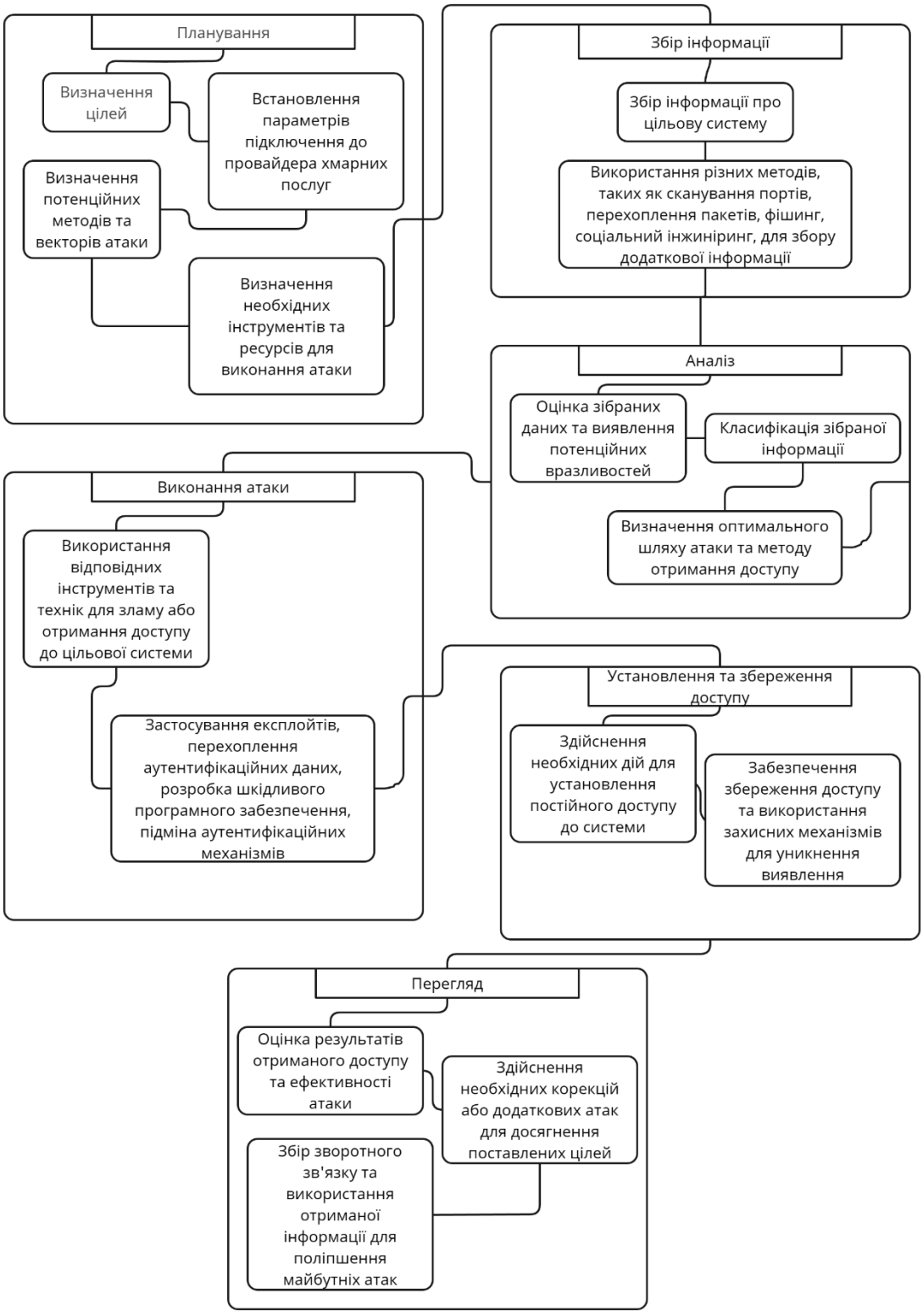


Рисунок 2.3 – Схема моделі циклу отримання доступу

Зловмисник змінює файли сценаріїв, які надаються законному веб-сайту з відкритого для запису відра хмарного сховища.

Шкідлива реклама оплачується та розміщується через законних постачальників реклами (наприклад, шкідлива реклама).

Вбудовані інтерфейси веб-додатків використовуються для вставки будь-яких інших типів об’єктів, які можна використовувати для відображення веб-вмісту або містять сценарій, який виконується на відвідувачі клієнта (наприклад, дописи на форумі, коментарі та інший контрольований користувачем веб-вміст).

Часто веб-сайт, який використовує зловмисник, відвідує певна спільнота, наприклад уряд, певна галузь чи регіон, де метою є скомпрометувати певного користувача або групу користувачів на основі спільних інтересів. Такий вид цільової кампанії часто називають стратегічним компромісом у мережі або атакою на водопою. Відомо кілька прикладів цього.

Типовий процес компромісу:

користувач відвідує веб-сайт, який використовується для розміщення контрольованого зловмисником вмісту.

Сценарії виконуються автоматично, зазвичай шукаючи потенційно вразливу версію браузера та плагінів. Від користувача може знадобитися допомогти в цьому процесі, увімкнувши сценарії або активні компоненти веб-сайту та ігноруючи діалогові вікна попереджень.

При виявленні вразливої версії код експлойту доставляється в браузер.

Якщо експлуатація буде успішною, це забезпечить виконання коду зловмисника в системі користувача, якщо немає інших засобів захисту. У деяких випадках перед доставкою коду експлойту потрібне повторне відвідування веб-сайту після початкового сканування.

На відміну від відкритої програми Exploit, ця техніка спрямована на використання програмного забезпечення на кінцевій точці клієнта під час відвідування веб-сайту. Зазвичай, це надає зловмиснику доступ до систем у внутрішній мережі замість зовнішніх систем, які можуть бути в DMZ.

Зловмисники також можуть використовувати скомпрометовані веб-сайти, щоб доставити користувача до зловмисної програми, призначеної для викрадення маркерів доступу до програми , як-от маркерів OAuth, щоб отримати

доступ до захищених програм та інформації. Ці шкідливі програми були доставлені через спливаючі вікна на законних веб-сайтах.

2.4 Розробка моделі “Підвищення привілеїв”

Зловмисники можуть змінювати маркери доступу для роботи в іншому контексті безпеки користувача або системи, щоб виконувати дії та обходити засоби контролю доступу (рис 2.4).

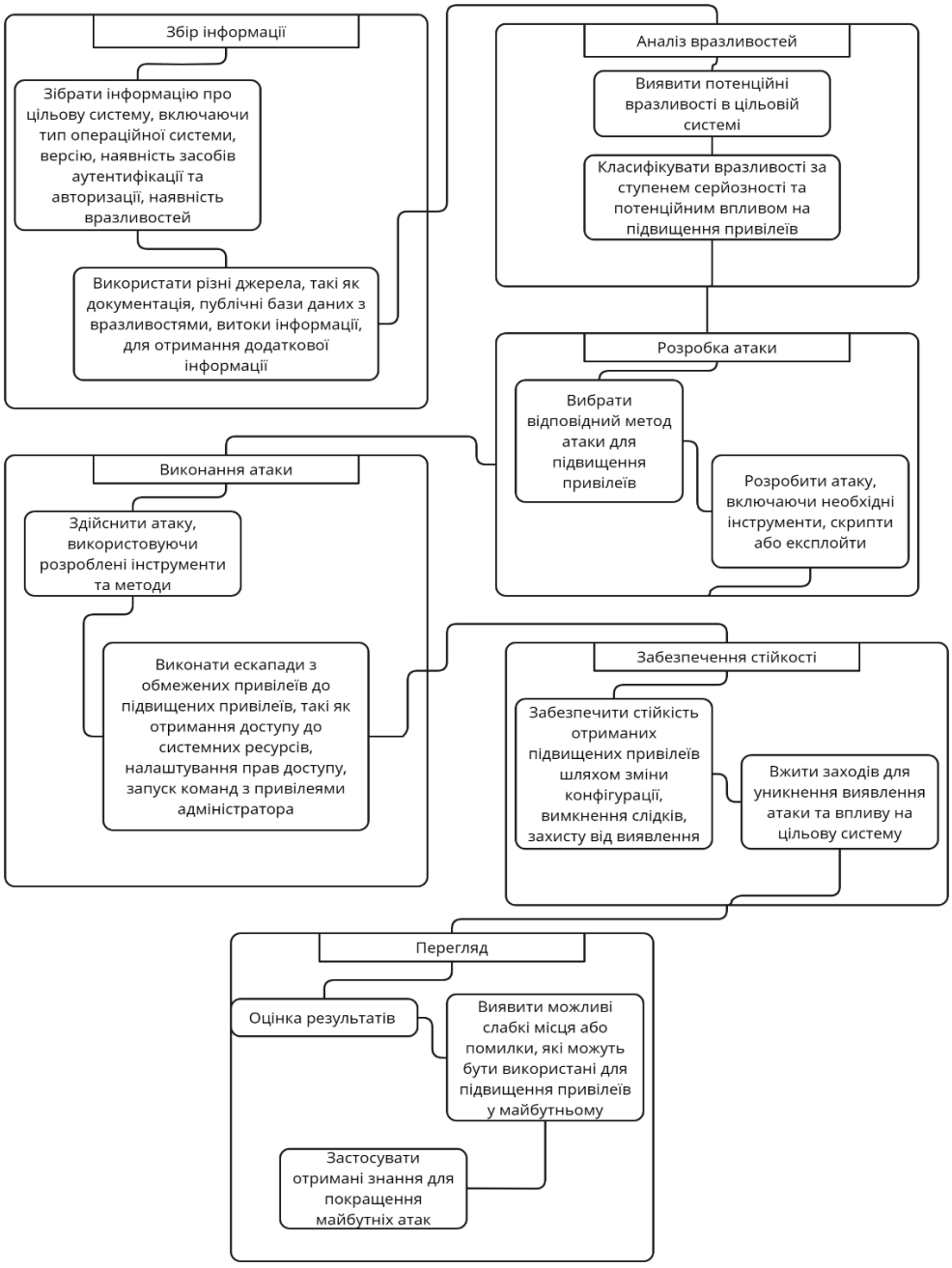


Рисунок 2.4 – Модель циклу підвищення привілеїв

Windows використовує маркери доступу для визначення права власності на запущений процес. Користувач може маніпулювати маркерами доступу, щоб запущений процес виглядав так, ніби він є дочірнім процесом іншого процесу або належить комусь іншому, ніж користувач, який запустив процес. Коли це відбувається, процес також приймає контекст безпеки, пов’язаний з новим маркером.

Зловмисник може використовувати вбудовані функції Windows API для копіювання маркерів доступу з існуючих процесів; це відоме як крадіжка токенів. Потім ці маркери можна застосувати до існуючого процесу (тобто імітація/викрадення маркера) або використати для створення нового процесу (тобто створити процес із маркером). Щоб вкрасти токен, зловмисник уже має бути в контексті привілейованого користувача (тобто адміністратора). Однак зловмисники зазвичай використовують крадіжку маркерів, щоб підняти свій контекст безпеки з рівня адміністратора до рівня системи. Потім зловмисник може використовувати маркер для автентифікації у віддаленій системі як обліковий запис для цього маркера, якщо обліковий запис має відповідні дозволи на віддалену систему.

Будь-який звичайний користувач може використовувати runas-команду та функції Windows API для створення токенів уособлення; для цього не потрібен доступ до облікового запису адміністратора. Існують також інші механізми, наприклад поля Active Directory, які можна використовувати для зміни маркерів доступу.

Зловмисники можуть підробити ідентифікатор батьківського процесу (PPID) нового процесу, щоб уникнути захисту від моніторингу процесу або підвищити привілеї (рис 2.5).

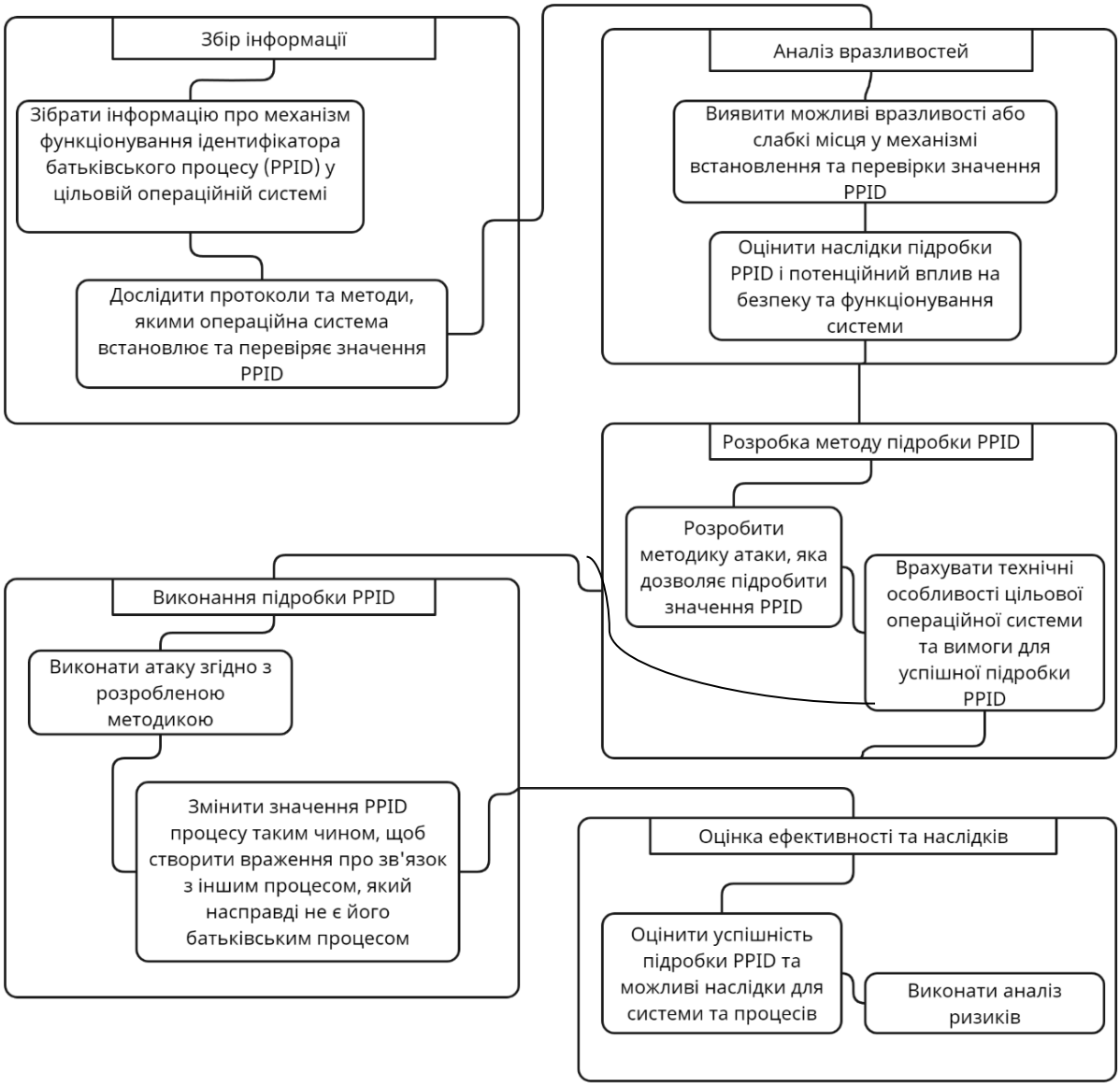


Рисунок 2.5 – Модель циклу підробки ідентифікатора батьківського процесу (PPID)

Нові процеси зазвичай породжуються безпосередньо з батьківського або викликаючого процесу, якщо це явно не вказано. Одним із способів явного призначення PPID нового процесу є CreateProcessвиклик API, який підтримує параметр, який визначає PPID для використання. Ця функція використовується такими функціями Windows, як «Контроль облікових записів користувачів» (UAC), щоб правильно встановити PPID після того, як запитаний процес з підвищеними правами створюється SYSTEM (зазвичай через svchost.exeабо consent.exe), а не поточним контекстом користувача.

Зловмисники можуть зловживати цими механізмами, щоб уникнути засобів захисту, як-от блокування процесів, що створюються безпосередньо з документів Office, і аналізу, націленого на незвичайні/потенційно зловмисні зв’язки батьківського й дочірнього процесів, як-от підробка PPID PowerShell / Rundll32 для доставки документа Office, а не документа Office explorer.exe. як частину Spearphishing Attachment . Цей спуфінг може бути виконано через Visual Basic у шкідливому документі Office або будь-якому коді, який може виконувати Native API.

Явне призначення PPID може також увімкнути підвищені привілеї з відповідними правами доступу до батьківського процесу. Наприклад, зловмисник у контексті привілейованого користувача (тобто адміністратор) може створити новий процес і призначити батьківський процес як процес, що виконується як SYSTEM (наприклад,), спричиняючи lsass.exe підвищення прав нового процесу через успадкований маркер доступу.

2.5 Розробка моделі “Відмова в обслуговуванні”

Зловмисники можуть здійснювати атаки на відмову в обслуговуванні (DoS), щоб погіршити або заблокувати доступність послуг для користувачів. Кінцева точка DoS може бути виконана, вичерпавши системні ресурси, на яких розміщено ці служби, або використовуючи систему, щоб викликати постійний збій (рис 2.6). Приклади послуг включають веб – сайти, служби електронної пошти, DNS і веб – додатки. Було помічено, що зловмисники проводять DoS – атаки в політичних цілях і для підтримки інших зловмисних дій, включаючи відволікання , хактивізм і вимагання.

Кінцева точка DoS забороняє доступність служби, не насичуючи мережу, яка використовується для надання доступу до служби. Зловмисники можуть націлитися на різні рівні стека програм, які розміщені в системі, яка використовується для надання послуги. Ці рівні включають операційні системи (ОС), серверні програми, такі як веб – сервери, DNS – сервери, бази даних і (як

правило, веб – додатки), які розташовані поверх них. Атака на кожен рівень вимагає різних методів, які використовують вузькі місця, унікальні для відповідних компонентів. DoS – атака може бути згенерована однією системою або декількома системами, поширеними в Інтернеті, що зазвичай називають розподіленим DoS (DDoS).

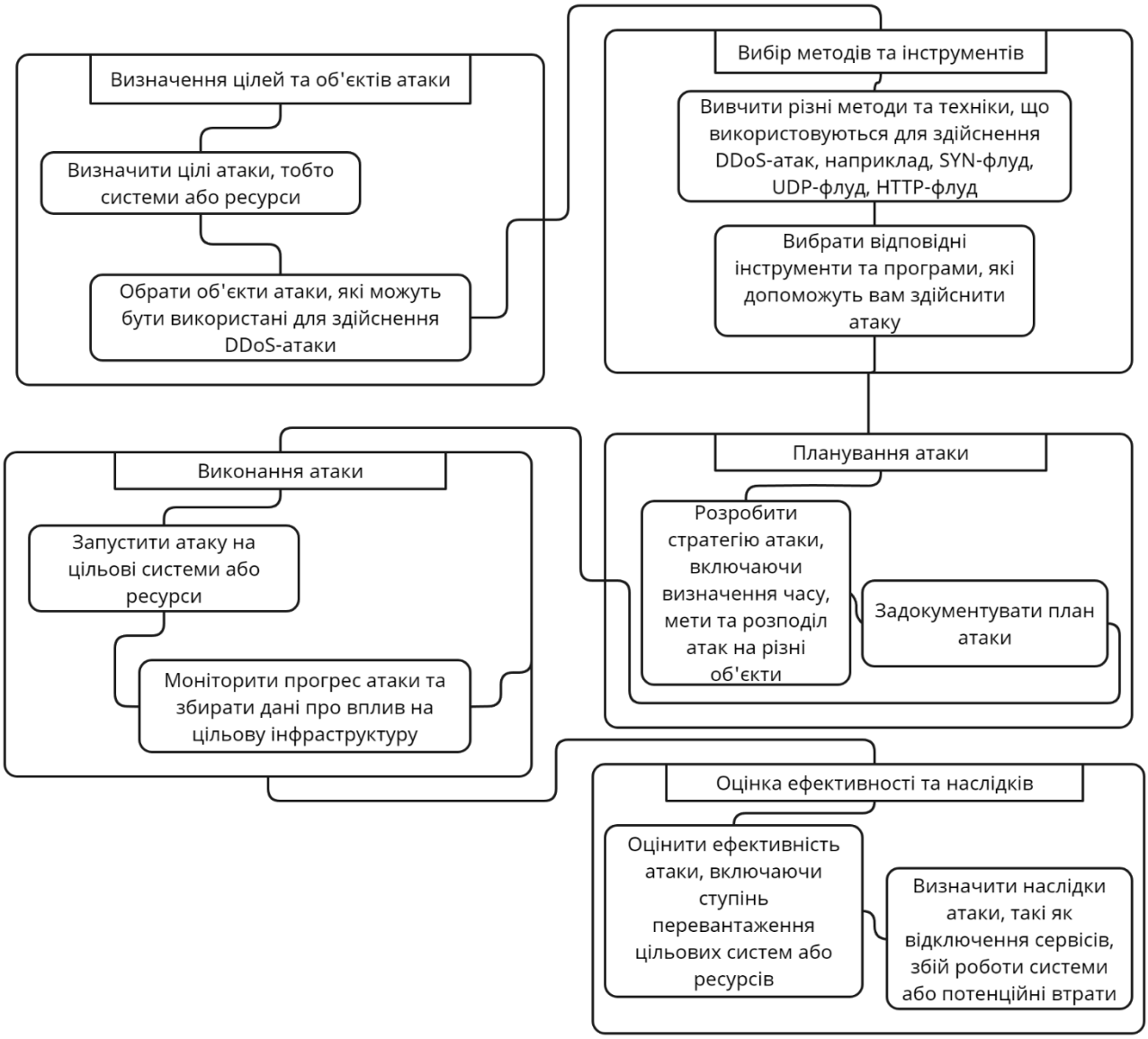


Рисунок 2.6 – Модель циклу здійснення атаки на відмову в обслуговуванні

Для здійснення DoS-атак на ресурси кінцевих точок застосовуються кілька аспектів, включаючи підміну IP-адрес і ботнети.

Зловмисники можуть використовувати оригінальну IP-адресу системи – атаки або підробити IP-адресу джерела, щоб ускладнити відстеження трафіку атаки до системи – атаки або забезпечити відображення. Це може збільшити труднощі, які мають захисники під час захисту від атаки, зменшуючи або усуваючи ефективність фільтрації за адресою джерела на пристроях захисту мережі.

Ботнети зазвичай використовуються для проведення DDoS-атак на мережі та служби. Великі ботнети можуть генерувати значну кількість трафіку від систем, поширених у глобальній мережі Інтернет. Зловмисники можуть мати ресурси для створення та контролю власної інфраструктури бот-мережі або можуть орендувати час у існуючій бот-мережі для проведення атаки. У деяких із найгірших випадків для DDoS-атак для створення запитів використовується так багато систем, що кожній із них потрібно лише надіслати невелику кількість трафіку, щоб отримати достатній обсяг, щоб вичерпати ресурси цілі. За таких обставин відрізнити трафік DDoS від легальних клієнтів стає надзвичайно складно.

У випадках, коли використовується маніпулювання трафіком, у глобальній мережі можуть існувати точки (наприклад, маршрутизатори шлюзу з високим трафіком), де пакети можуть бути змінені та змусити легітимних клієнтів виконувати код, який спрямовує мережеві пакети до цілі у великій кількості. Цей тип можливостей раніше використовувався для цілей веб – цензури, коли HTTP-трафік клієнта було змінено, щоб включити посилання на JavaScript, який генерував код DDoS для перевантаження цільових веб-серверів.

Зловмисники можуть розпочати атаку на відмову в обслуговуванні (DoS), спрямовану на операційну систему (ОС) кінцевої точки. ОС системи відповідає за керування обмеженими ресурсами, а також за запобігання перевантаження всієї системи через надмірні вимоги до її потужності. Ці атаки не потребують виснаження фактичних ресурсів системи; атаки можуть просто вичерпати обмеження та доступні ресурси, які ОС сама нав’язує.

Існують різні способи досягти цього, включаючи атаки виснаження стану TCP, такі як SYN-флуди та ACK-флуди. Під час SYN-флудів надсилається надмірна кількість SYN-пакетів, але тристороннє зв'язування TCP ніколи не завершується. Оскільки кожна ОС має максимальну кількість одночасних TCP-з'єднань, які вона дозволяє, це може швидко вичерпати здатність системи отримувати нові запити на TCP-з'єднання, таким чином запобігаючи доступ до будь-якої служби TCP, що надається сервером.

Потоки ACK використовують природу протоколу TCP із збереженням стану. Потік пакетів ACK надсилається до цілі. Це змушує ОС шукати в таблиці станів пов'язане TCP-з'єднання, яке вже було встановлено. Оскільки пакети ACK призначені для неіснуючих з'єднань, ОС буде шукати всю таблицю станів, щоб підтвердити відсутність відповідності. Коли це необхідно зробити для великого потоку пакетів, вимоги до обчислень можуть призвести до того, що сервер стане млявим і/або не відповідає на запити через роботу, яку він повинен виконати, щоб усунути фальшиві пакети ACK. Це значно зменшує ресурси, доступні для надання цільової послуги.

2.6 Висновки до розділу

У цьому розділі було проведено огляд і опис відомих атак, що виникають у сфері кібербезпеки. Аналіз відомих атак є важливою складовою частиною дослідження і розробки кіберполігону для дослідження подій інформаційної безпеки.

На основі проведеного огляду було виявлено, що кібератаки можуть бути дуже різноманітними за своїми характеристиками та механізмами дії. Вони можуть включати атаки на різні рівні інфраструктури, такі як мережеві атаки, атаки на додатки, соціально-інженерні атаки та інші.

Аналіз відомих атак дозволив ідентифікувати основні методи та техніки, які використовуються зловмисниками для здійснення атак. Це може бути експлуатація вразливостей систем, використання шкідливих програм, фішингові атаки, DDoS атаки та інші.

Опис відомих атак є важливим для розробки ефективних захисних стратегій і механізмів протидії. Він надає уявлення про типові сценарії атак, а також допомагає виявити уразливості системи та розробити заходи щодо їх запобігання та виявлення.

Цей аналіз допомагає виявити потенційні уразливості в системі та розуміти, яким чином зловмисники можуть їх використати.

На основі опису відомих атак можна розробити ефективні стратегії протидії. Враховуючи типові сценарії, можна розробити відповідні захисні механізми та контрмери, що допоможуть запобігти атакам або виявити їх на ранніх стадіях. Наприклад, якщо відомо, що фішинг-атаки є поширеними, можна розробити навчальні програми для підвищення обізнаності користувачів та встановити фільтри для виявлення шахрайських листів.

Опис відомих атак також допомагає вдосконалювати процес виявлення та реагування на інциденти. Аналізуючи попередні атаки, можна виявити спільні ознаки та моделі поведінки зловмисників, що дозволить розробити ефективні механізми виявлення та аналізу подій в реальному часі.

Далі в роботі будуть розглянуті інструменти та методи для моделювання атак у рамках кіберполігону, що дозволить більш детально вивчити та аналізувати характеристики цих атак. Це допоможе в розробці більш ефективних захисних стратегій та підготовці фахівців з кібербезпеки до реальних загроз.

Загалом, аналіз відомих атак є важливим етапом у дослідженні кібербезпеки, оскільки він допомагає розуміти сучасні загрози та розробляти ефективні заходи для їх протидії.

3 НАЛАШТУВАННЯ ТА РЕАЛІЗАЦІЯ МОДУЛЯ ІМІТАЦІЇ АТАК

3.1 Моделювання атаки “Розвідка”

Nmap (Network Mapper) - це потужний сканер мережі, який надає можливості сканування, виявлення топології мережі, визначення доступних хостів, сканування портів та інше.

Для сканування засобами Nmap можна використовувати різні параметри, які впливають на різні аспекти сканування. Ось кілька основних параметрів сканування у Nmap:

-sS або --syn: виконує TCP SYN сканування, що дозволяє виявляти відкриті порти на хості.

-sT або --connect: виконує повне TCP-з'єднання з кожним портом, що дозволяє виявляти відкриті порти та встановлення з'єднання з сервісом.

-sU або --udp: виконує UDP-сканування для виявлення відкритих UDP-портів.

-p <порти>: визначає діапазон портів, які будуть скануватись. Наприклад, -p 1-100 скануватиме порти від 1 до 100.

-O або --osscan-guess: виконує вгадування операційної системи (OS fingerprinting) на основі відповідей на сканування.

-A або --all: виконує розширений скан, включаючи виявлення версій сервісів, детальну інформацію про ОС, трасування шляху до хоста та іншу інформацію.

-v або --verbose: ввімкнути режим докладного виводу, що надає більше інформації про хід сканування.

-oN <файл>: записує результати сканування у вказаний файл в форматі "нормального" тексту.

-sP: виконує сканування присутності (Ping scan) для визначення доступних хостів, не проводячи сканування портів.

-sV: виконує сканування версій сервісів для визначення версій програмного забезпечення, які працюють на відкритих портах.

-sN, -sF, -sX: виконують сканування неповних TCP-пакетів, таких як NULL, FIN, Xmas, відповідно. Вони використовуються для тестування специфічних вразливостей.

-sA: виконує сканування ACK для визначення фільтрації портів брандмауером.

--script <скрипти>: дозволяє виконувати спеціальні скрипти Nmap для виявлення вразливостей, автоматизації завдань аналізу та отримання додаткової інформації про цільову мережу.

--traceroute: Виконує трасування шляху до цільового хоста, відображаючи проміжні маршрути та їх затримки.

-T<число>: Встановлює рівень інтенсивності сканування (1-5), де 1 - найповільніше, а 5 - найшвидше.

--scan-delay <час>: Встановлює затримку між скануванням портів (у мілісекундах), що допомагає уникнути виявлення аномальної активності.

--randomize-hosts: Випадковим чином змінює порядок сканування хостів.

Отже для запуску сканування потрібно вибрати параметри –traceroute, -T, -A, -sS, -sU, -p(рис 3.1).

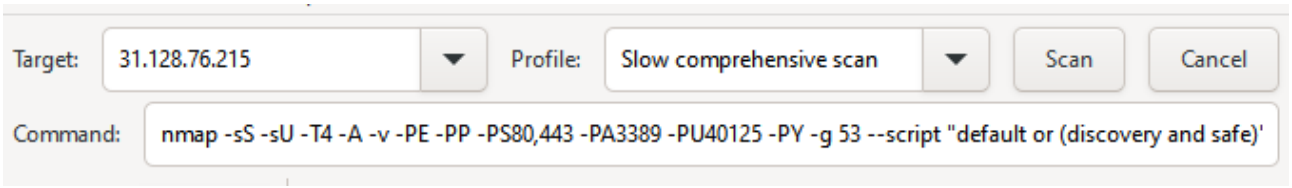


Рисунок 3.1 – Параметри сканування Nmap

Після виконання сканування можна отримати результат у вигляді топології мережі(рис 3.2). За допомогою цього можна дізнатись через які вузли проходить трафік.

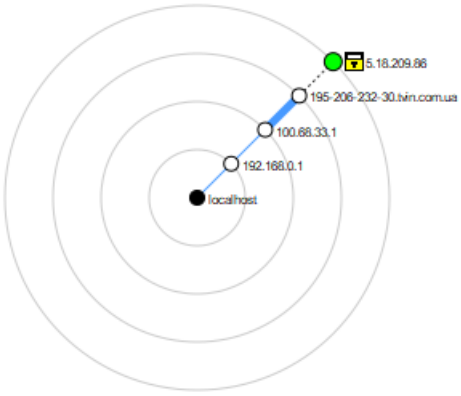


Рисунок 3.2 – Топологія мережі

Серед результатів можна дізнатись ім’я активного користувача, список всіх користувачів, мак адресу пристрою. Знаючи MAC-адресу чужого пристрою, можна спробувати виконати атаку з підміною. Також серед результатів можна дізнатись версію операційної системи(рис 3.3).

```
Host script results:
| smb2-time:
|   date: 2023-06-11T10:29:29
|_  start_date: N/A
| nbstat: NetBIOS name: JAGA, NetBIOS user: <unknown>, NetBIOS MAC:
02:50:93:d2:fc:01 (unknown)
| Names:
|   JAGA<00>             Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  JAGA<20>             Flags: <unique><active>
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT      ADDRESS
1   21.76 ms 26.245.43.151
```

Рисунок 3.3 – Інформація про ОС

Багато атак з підміною використовують протокол ARP (Address Resolution Protocol), що відповідає за відповідність IP-адрес і MAC-адрес. Наприклад, атака MITM (Man-in-the-Middle) може використовувати підроблені ARP-відповіді для перенаправлення мережевого трафіку через атакуючий пристрій.

Також при розвідці цільової системи потрібно провести всі можливі сканування портів (рис. 3.4, 3.5).

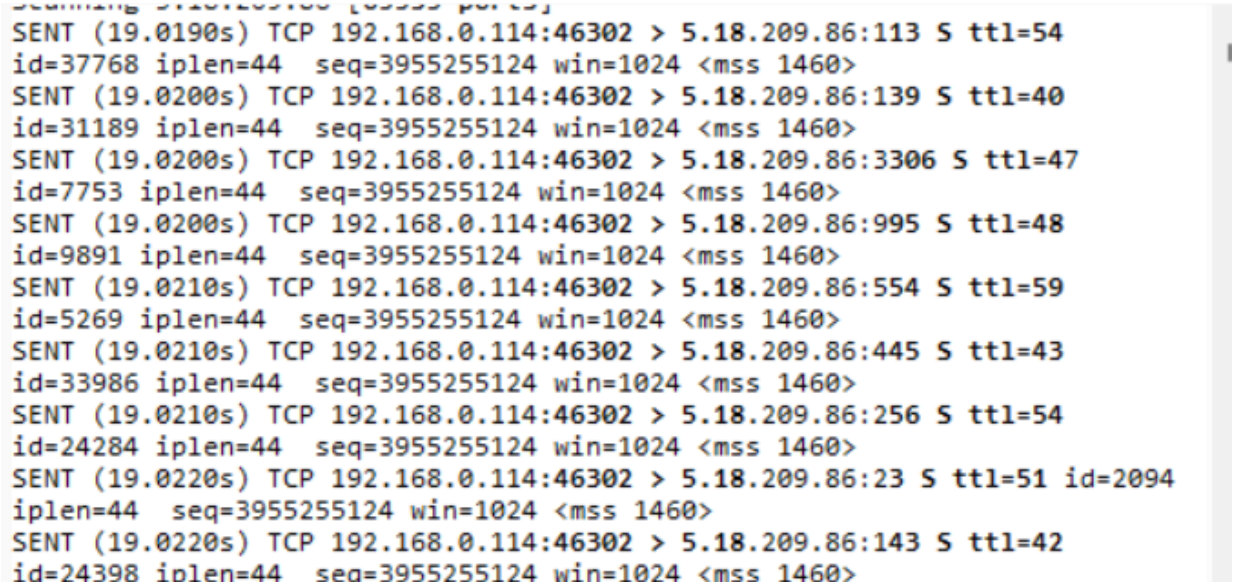


Рисунок 3.4 – TCP-сканування

Тут можна побачити адресу та порт з якої відбувається атака, також IP адресу цільової мережі та порт, який перевіряється. Також показується TTL (Time to Live) - це поле в заголовку IP-пакета, яке використовується для визначення максимальної кількості маршрутизаторів (хопів), які можуть бути пройдені пакетом, перш ніж він буде відкинутий або повернений назад.

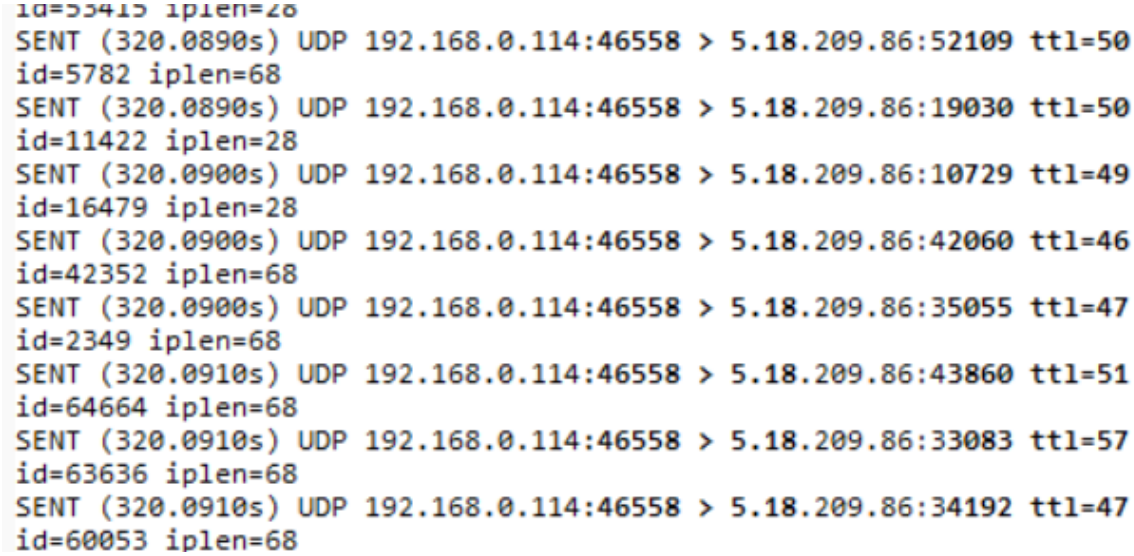


Рисунок 3.5 – UDP-сканування

У контексті сканування з використанням Nmap, поле TTL використовується для виявлення живих хостів та визначення їх оптимального шляху в мережі. Nmap використовує це поле для надсилання спеціально сформованих пакетів з різними значеннями TTL і вимірювання часу, який потрібен для отримання відповіді від хоста.

Після завершення сканування отримується результат з портами, які використовуються (рис. 3.6), та інформацію про те, що на них знаходиться(рис. 3.7).

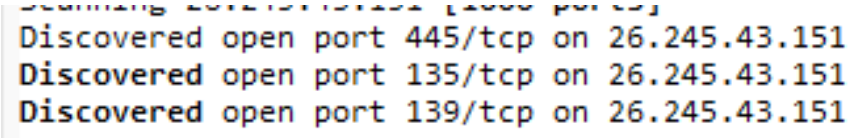


Рисунок 3.6 – Активні порти.

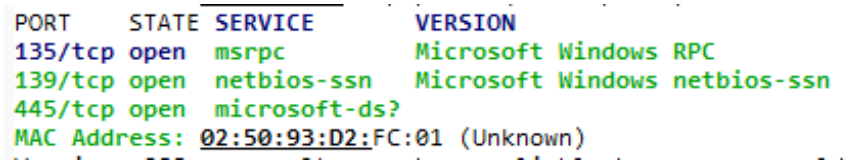


Рисунок 3.7 – Інформація про активні порти

3.2 Моделювання атак за допомогою Owasp ZAP

OWASP ZAP (Zed Attack Proxy) - це безкоштовний і відкритий інструмент для тестування на проникнення та роботи з веб-додатками. Він розроблений спільнотою OWASP (Open Web Application Security Project) і надає широкий функціонал для виявлення потенційних вразливостей в веб-додатках. Основні функції OWASP ZAP включають:

Активне сканування вразливостей: ZAP пропонує можливість активного сканування веб-додатків з метою виявлення потенційних вразливостей, таких як перехоплення сесій, вразливості введення даних, відмова в обслуговуванні, XSS (міжсайтовий скриптинг) та інші. Він може автоматично виконувати різні тестові сценарії та знаходити вразливості на основі виявлених аномалій.

Перехоплення та перевірка запитів: ZAP дозволяє перехоплювати та змінювати HTTP-запити та відповіді між клієнтом і сервером. Це дозволяє розробникам аналізувати веб-трафік, виконувати тестування на проникнення та перевіряти безпеку веб-додатків. Також можна використовувати цей інструмент для перевірки дії захисних механізмів, наприклад, фільтрації та підтвердження даних.

Аналіз вразливостей: ZAP надає зручні інструменти для аналізу знайдених вразливостей. Він генерує детальні звіти, які містять опис вразливостей, поради щодо виправлення проблеми та іншу корисну інформацію. Також можна налаштовувати правила сканування та фільтрувати результати з метою спрощення аналізу.

Автоматизація та інтеграція: ZAP надає можливості автоматизації тестування на проникнення шляхом використання API та скриптів. Він також підтримує інтеграцію з іншими інструментами, такими як CI/CD системи, для автоматичного тестування безпеки під час розробки і випуску веб-додатків.Для проведення сканування вразливостей обирається ціль, після чого URL цілі вводиться в відповідне поле, та обираються параметри сканування та атаки (рис 3.8). Для того щоб працювала атака, потрібно перевести ZAP у режим атаки, інакше програмне забезпечення не дозволяє проводити атаки, а тільки розвідку.

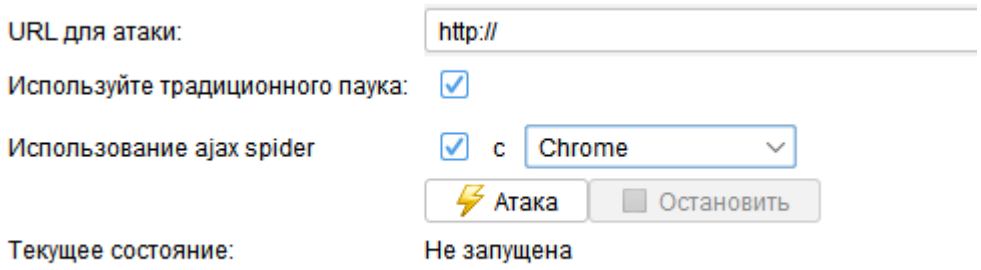


Рисунок 3.8 – Вікно запуску атаки

У результаті ПЗ видає інформацію про перебіг сканування та атаки. У процесі можна побачити стан сервісів, які ПЗ сканує, та їх доступність.

У процесі аналізу результатів сканування, можна побачити можливі вразливості. У цьому вікні приведені типи вразливості, їх рівень, що приведений у 4 рівнях.

Червоний прапорець вказує на те, що ці вразливості критично важливі для системи. Таких вразливостей було знайдено 1 тип та 13 вразливих ресурсів.

Оранжевий прапорець вказує на ті вразливості, що мають помірний рівень небезпеки. Такі помилки також можуть бути використані для потенційних атак на ресурс. Їх було знайдено 6 типів та більше 3 тисяч ресурсів.

Далі йдуть жовті прапорці, що вказують на слабкі вразливості, що майже не можуть вплинути на роботоздатність системи, але можуть бути використані для атак типу фішинг.

Синій прапорець вказує на те, що потрібно виправити, але ці помилки не можуть мати наслідків у вигляді кібератак.

Також під час всі сканування всі ресурси серверу показані у вікні посилань на скановані сайти, де можна їх переглянути. У цьому вікні можна побачити конкретний ресурс, рівень вразливості та іконку засобу, за допомогою якого було отримано ресурс.

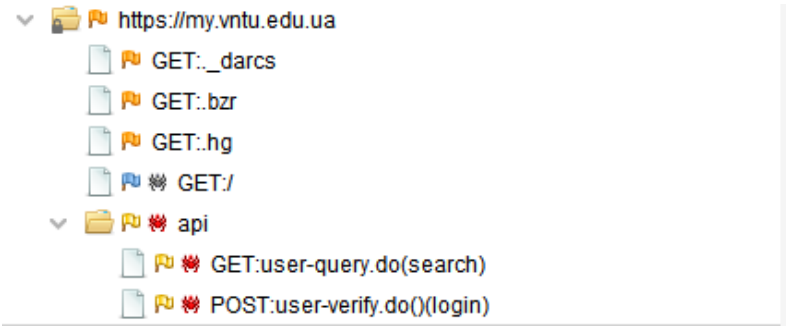


Рисунок 3.9 – Вікно ресурсів серверу

Далі ZAP дозволяє провести атаку, яка дозволяє скопіювати всі отримані ресурси веб-серверу. Також він дозволяє отримати інформацію про сервер, статус сторінки, на якому саме веб-сервері працює веб-ресурс. Також видно чи працює він в даний момент та розмір контенту.

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 13 Jun 2023 12:01:17 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Last-Modified: Tue, 13 Jun 2023 12:01:17 GMT
Vary: Accept-Encoding
Content-Length: 51395
```

Рисунок 3.10 – Отримана відповідь від серверу

Також серед відповідей можна знайти HTML та CSS код сторінок сайту (рис 3.11). Надалі цю інформацію можна використати для атак клікджекінгу та фішингу.

```
<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Вхід у персональний кабінет</title>
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <link rel="shortcut icon" href="/style/favicon.ico" type="image/x-icon">
    <link rel="stylesheet" href="/style/vendor/bootstrap-4.5.2/css/bootstrap.min.css" type='text/css' media='all' />
    <link rel='stylesheet' href='/style/font/ProbaPro.css' type='text/css' media='all' />
    <link rel="stylesheet" href="/style/style.css?ver=0.1.1" type='text/css' media='all' />
  </head>
  <body>
    <div class="background-tiles"></div>
    <div class="head-links d-none d-sm-block">
      <div style="float: right"><a href="/user/help/">Не можете увійти?</a></div>
```

Рисунок 3.11 - HTML та CSS код сторінок сайту

Серед вразливостей можна знайти такі:

Політика безпеки вмісту (CSP) – це додатковий рівень безпеки, який допомагає виявляти та пом'якшувати певні типи атак, включаючи міжсайтові сценарії (XSS) та атаки з впровадженням даних. Ці атаки використовуються для всього: від крадіжки даних до псування сайту або розповсюдження шкідливих програм. CSP надає набір стандартних HTTP заголовків, які дозволяють власникам веб-сайтів оголошувати затверджені джерела контенту, які браузери повинні дозволити завантажувати на цю сторінку. Типи, що охоплюються, включають JavaScript, CSS, HTML-фрейми, шрифти, зображення та об'єкти, що вбудовуються, такі як аплети Java. ActiveX, аудіо та відео файли.

Неправильна конфігурація CORS на веб-сервері дозволяє міждоменні запити читання з довільних сторонніх доменів з використанням неавтентифікованих API у цьому домені. Однак, реалізації веб-браузера не дозволяють довільним третім сторонам читати відповідь від автентифікованих API. Це дещо знижує ризик. Ця неправильна конфігурація може бути використана зловмисником для доступу до даних, які доступні без автентифікації, але які використовують іншу форму безпеки, як білий список IP-адрес.

Токени для знешкодження атак CSRF не були виявлені у формі надсилання на сторінці HTML. Підробка міжсайтового запиту - це атака, яка включає примус жертви до відправки HTTP-запиту в цільовий пункт призначення без її відома або наміру, щоб виконати дію як жертву. Основна причина - функціональність програми, що використовує передбачувані дії URL/форми повторюваним чином. Суть атаки полягає в тому, що CSRF використовує довіру, яку має веб-сайт до користувача. Навпаки, міжсайтовий скриптинг (XSS) використовує довіру користувача до веб-сайту. Як і XSS, CSRF-атаки не обов'язково є міжсайтовими, але можуть бути. Підробка міжсайтових запитів також відома як CSRF, XSRF, атака в один клік, сесійна атака, спантеличений помічник і морський серфінг.

CSRF-атаки ефективні у низці ситуацій, у тому числі:

У жертви активний сеанс на цільовому сайті.

Жертва аутентифікується через HTTP-аутентифікацію на цільовому сайті.

Жертва знаходиться в тій же локальній мережі, що й цільовий сайт.

CSRF в основному використовувався для виконання дії проти цільового сайту з використанням привілеїв жертви, але нещодавно було виявлено методи розкриття інформації шляхом отримання доступу до відповіді. Ризик розкриття інформації різко зростає, коли цільовий сайт вразливий для XSS, тому що XSS може використовуватися як платформа для CSRF, дозволяючи атаці діяти в рамках політики одного і того ж походження.

3.3 Моделювання атаки “Відмова в обслуговуванні”

Для початку можна обрати для атаки LOIC (Low Orbit Ion Cannon) — програма з відкритим вихідним кодом для здійснення мережевих атак, написана мовою програмування C#. Спочатку розроблена компанією Praetox Technologies, але пізніше була опублікована як суспільне надбання. Програма виконує розподілену атаку «відмова в обслуговуванні» (англ. Denial of Service — DoS) шляхом постійного відправлення на потрібний сайт або сервер TCP-, UDP-пакетів або HTTP-запитів з метою появи збоїв в функціонуванні певного хоста.

Для початку потрібно налаштувати її. Обрати тип атаки звичайну або розподілену атаку. Далі потрібно ввести посилання або IP адресу цілі(рис 3.12).

Рисунок 3.12 – Вікно з налаштуванням цілі

Далі потрібно обрати повідомлення, що буде надсилатись на сервер, швидкість атаки, метод TCP, UDP, HTTP. Також потрібно обрати порт та кількість пакетів (рис 3.13).

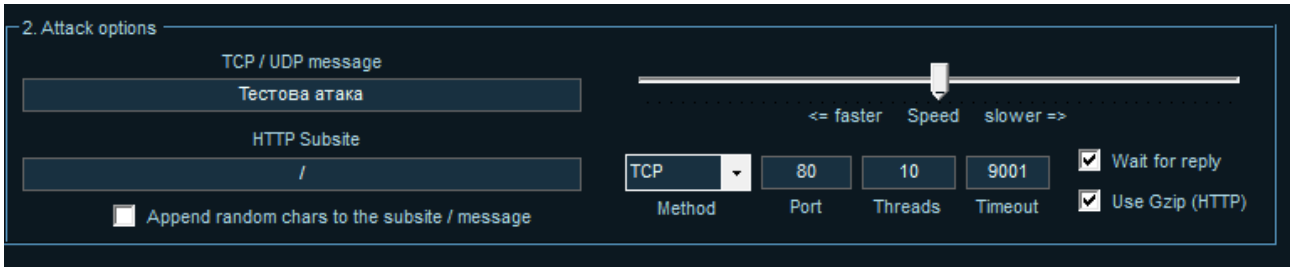


Рисунок 3.13 – Вікно налаштувань

Після чого потрібно запустити атаку та отримати результати моніторингу. Де можна бачити кількість відправлених запросів на цей момент, та кількість отриманих відповідей. Також можна побачити кількість пакетів з помилками (рис 3.14).

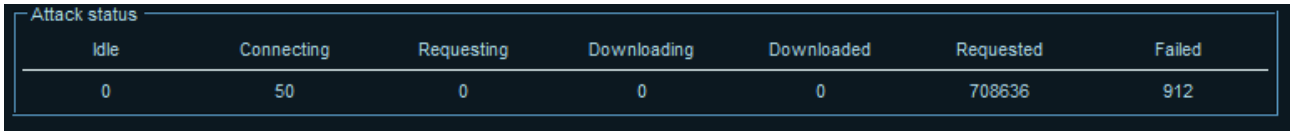


Рисунок 3.14 – Результат атаки

Також хід атаки можна промоніторити за допомогою додатку у консолі, для кращого розуміння результатів (рис.3.15).

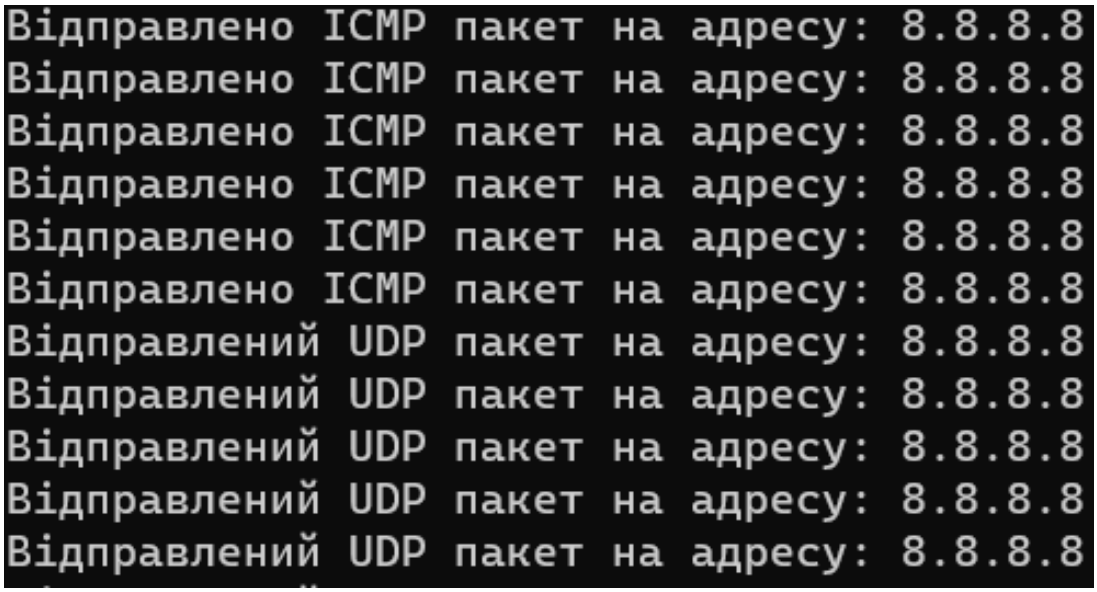


Рисунок 3.15 - Результат виконання у консолі

3.4 Висновок до розділу

Сканування за допомогою Nmap дозволяє виявити активні хости, відкриті порти та сервіси в мережі. Це допомагає збільшити розуміння структури мережі та виявити потенційні вразливості.

Використання Owasp ZAP для сканування додатків дозволяє виявити вразливості веб-додатків, такі як SQL-ін'єкція, XSS атаки, недостатній контроль доступу та інші. Це дозволяє розробникам та адміністраторам виявляти та виправляти потенційні проблеми безпеки.

DoS атаки демонструють можливості перевантаження цільової системи або мережі, забезпечуючи велике навантаження та перешкоджаючи нормальному функціонуванню. Це важливий аспект тестування стійкості та виявлення проблем з пропускною здатністю та надійністю.

Практична реалізація цих методів дозволяє практикуючим фахівцям та студентам набути практичний досвід у проведенні аналізу безпеки мережі та додатків. Це допомагає розширити їх знання та навички у сфері кібербезпеки. Важливо пам'ятати, що ці методи повинні використовуватися в етичних цілях та з дозволу власників системи. При їх використанні слід дотримуватись законодавства та враховувати можливі наслідки для системи та мережі.

В цілому, практична реалізація сканування та атак дозволяє покращити розуміння проблем безпеки та забезпечити більш ефективний захист інформаційних систем та мереж.

ВИСНОВОК

У результаті виконання комплексної бакалаврьскої дипломної роботи було спроектовано і побудовано кіберполігон на базі кафедри захисту інформації та впроваджено модуль імітації атак. Також було встановлено та налаштовано всі необхідні компоненти для коректного запуску модуля.

Проведений аналіз задач при імітації атак та вивчено відомі моделі атак, такі як "Вторгнення в мережу", "Фішинг", "Вірус", "Відмова в обслуговуванні" та "Злом паролю". Також встановлено актуальність використання кіберполігону в контексті дослідження інформаційної безпеки. Виконано аналіз атакуючої сторони (Red team).

Розроблено моделі атак, які використовуються для імітації атак на кіберполігоні. Розглянуті моделі включають "Розвідка", "Отримання доступу", "Початковий доступ", "Підвищення привілеїв" та "Відмова в обслуговуванні". Також було проведено детальний огляд кожної моделі атаки з описом їх характеристик.

Було проведено моделювання атаки "Розвідка" та "Відмова в обслуговуванні" і використано інструмент Owasp ZAP для моделювання атак. Описано технічні аспекти розробки модуля та його функціональні можливості.

У цілому, комплексна бакалаврська дипломна робота є комплексним дослідженням в галузі інформаційної безпеки та кібербезпеки. Було виконано аналіз і вивчення відомих атак, розроблено моделі атак для імітації, налаштування та реалізацію модуля імітації атак.

Результати цієї роботи можуть бути використані для покращення захисних стратегій та механізмів протидії в галузі кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Блоха А. О. МОДУЛЬ ДЛЯ ГЕНЕРАЦІЇ АТАК [Електронний ресурс] / А. О. Блоха, О. П. Войтович // Матеріали Всеукраїнської науково-практичної інтернетконференції "Молодь в науці: дослідження, проблеми, перспективи (МН-2023)", Вінниця, 22-23 червня 2023 р. Електрон. текст. дані. – 2023. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2023/paper/view/18298

2. 2023 Data Breach Investigations Report [Електронний ресурс] https://www.verizon.com/business/resources/reports/dbir/

3. Cybersecurity Ventures [Електронний ресурс] https://cybersecurityventures.com/

4. CyberEdge Group's 2021 Cyberthreat Defense Report [Електронний ресурс] https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1.pdf

5. Outsmarting the Super-Hackers By Securing Smart Autonomous Systems [Електронний ресурс] https://partners.wsj.com/tii/catalyzing-change/outsmarting-the-super-hackers/?utm_medium=content_discovery&utm_source=google-search&gclid=CjwKCAjws7WkBhBFEiwAIi168ydBZdSV_003JglJmcm5_DjCLoNLvatuCG9UX-JrZAfaac5T1V7n6xoC_rMQAvD_BwE

6. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy [Електронний ресурс]https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full.

7. Дослідження моделі поширення вірусу [Електронний ресурс] https://phm.cuspu.edu.ua/ojs/index.php/SNYS/article/view/1975.

8. Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks [Електронний ресурс] https://www.sciencedirect.com/science/article/pii/S0167404821001760.

9. A survey exploring open source Intelligence for smarter password cracking [Електронний ресурс] https://www.sciencedirect.com/science/article/pii/S2666281720303723.

10. Cyber espionage through Botnets [Електронний ресурс] https://link.springer.com/article/10.1057/s41284-019-00194-6.

11. Кібербезпека україни і засоби її реалізації [Електронний ресурс] https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/48191/1/%D0%A2%D0%B5%D0%B7%D0%B8%20%D0%9B%D1%8C%D0%B2%D1%96%D0%B2.pdf#page=545.

12. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture [Електронний ресурс] https://www.sciencedirect.com/science/article/abs/pii/S0167404819301804.

13. Особливості створення кіберполігонів для підготовки фахівців з кібербезпеки [Електронний ресурс] https://academy.ssu.gov.ua/uploads/p_57_54325835.pdf#page=204.

14. Інформаційно-комунікаційна технологія керування навчальним центром кібербезпеки з функціональністю симуляційного кіберполігону [Електронний ресурс] https://essuir.sumdu.edu.ua/bitstream-download/123456789/91126/1/Koval_mag_rob.pdf;jsessionid=B826B647E1486F46A80ED0027164A95A.

15. Ahmed M. Detecting Rare and Collective Anomalies in Network Traffic Data using Summarization [Електронний ресурс] / Mohiuddin Ahmed // School of Engineering and Information Technology The University of New South Wales Australia. – 2016. – Режим доступу до ресурсу: http://unsworks.unsw.edu.au/fapi/datastream/unsworks:42253/SOURCE02?view=true.

16. A Cyber Kill Chain Based Analysis of Remote Access Trojans [Електронний ресурс] https://link.springer.com/chapter/10.1007/978-3-030-10543-3_12.

17. Investigation of Cyber Situation Awareness via SIEM tools: a constructive review [Електронний ресурс] https://ieeexplore.ieee.org/abstract/document/9558964.

18. Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture [Електронний ресурс] https://ieeexplore.ieee.org/abstract/document/8551383.

19. Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures [Електронний ресурс] http://xml.jips-k.org/full-text/view?doi=10.3745/JIPS.03.0126.

20. Nmap: the Network Mapper - Free Security Scanner [Електронний ресурс] https://nmap.org/.

21. OWASP ZAP [Електронний ресурс] https://www.zaproxy.org/.

22. Hive Mind LOIC [Електронний ресурс] https://sourceforge.net/projects/hivemindloic/.

ДОДАТКИ

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ
БАКАЛАВРСЬКОЇ ДИПЛОМНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Кіберполігон для дослідження подій інформаційної безпеки. Частина 1. Модуль для імітації атак

Автор роботи: Блоха Андріан Олександрович

Тип роботи: бакалаврська дипломна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 99,0% Схожість – 1,0%.

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 _____ Каплун В. А.
(підпис) (прізвище, ініціали)

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

Автор роботи _____ Блоха А. О.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Войтович О. П.
(підпис) (прізвище, ініціали)

Додаток Б

Методичні вказівки

Мета роботи: Ознайомитися з процесом встановлення та налаштування програмного забезпечення для імітації атак.

Порядок виконання:

Крок 1 : оновлення системи.

Першим кроком перед встановленням програмного забезпечення потрібно провести оновлення операційної системи. Для того, щоб виконати цей крок необхідно виконати наступні команди:

```
sudo apt update && apt upgrade
```

Крок 2: Встановлення Nmap

Після оновлення списку пакетів введи команду для встановлення Nmap.

```
sudo apt install nmap
```

Система попросить підтвердити встановлення пакету Nmap.

Потрібно натиснути "Y" або "Так" та натиснкти Enter. Встановлення розпочнеться і може зайняти кілька хвилин, залежно від швидкості з'єднання та продуктивності системи.

Після завершення встановлення Nmap буде доступний в системі. Тепер можна використовувати його, запускаючи команду nmap в терміналі.

Для перевірки роботоздатності потрібно ввести `nmap –version`.

Крок 3: Встановлення Owasp ZAP

Потрібно переконатись що у системі є Java Development Kit (JDK). Потрібно ввести наступну команду, щоб перевірити наявність JDK.

```
java -version
```

Якщо пакет відсутній, потрібно його встановити командами:

```
sudo apt update
sudo apt install default-jdk
```

Далі потрібно відкрити веб-браузер і перейди на сторінку завантаження OWASP ZAP за посиланням: https://www.zaproxy.org/download/.

На сторінці завантаження знайти останню стабільну версію OWASP ZAP для Linux і вибрати відповідний пакет для своєї архітектури (32-біт або 64-біт).

Завантажити відповідний архів ZIP-файлу OWASP ZAP для Linux.

Перейти до папки, куди було завантажено архів OWASP ZAP.

Розпакувати архів за допомогою наступної команди:

```
unzip [запакований_файл]
```

Після розпакування архіву перейди до каталогу OWASP ZAP:

```
cd [назва_каталогу]
```

Запустити OWASP ZAP, виконавши наступну команду:

```
./zap.sh
```

OWASP ZAP запуститься і відкриє графічний інтерфейс користувача. За замовчуванням OWASP ZAP запуститься з використанням вбудованого проксі-сервера. Можеш налаштувати свій веб-браузер на використання проксі-сервера OWASP ZAP для перехоплення та аналізу HTTP-запитів.

ІЛЮСТРАТИВНА ЧАСТИНА

Кіберполігон для дослідження подій інформаційної безпеки. Частина 1. Модуль для імітації атак

(Назва бакалаврської дипломної роботи)

Виконав: студент 2 курсу групи 1БС-21мс
спеціальності 125 Кібербезпека
_____ Андріан БЛОХА
_____ 2023 р.

Керівник: к. т. н., доцент каф. ЗІ
_____Олеся ВОЙТОВИЧ
_____ 2023 р.

ПОТІК АКТИВНОГО РОЗВІДУВАЛЬНОГО СКАНУВАННЯ

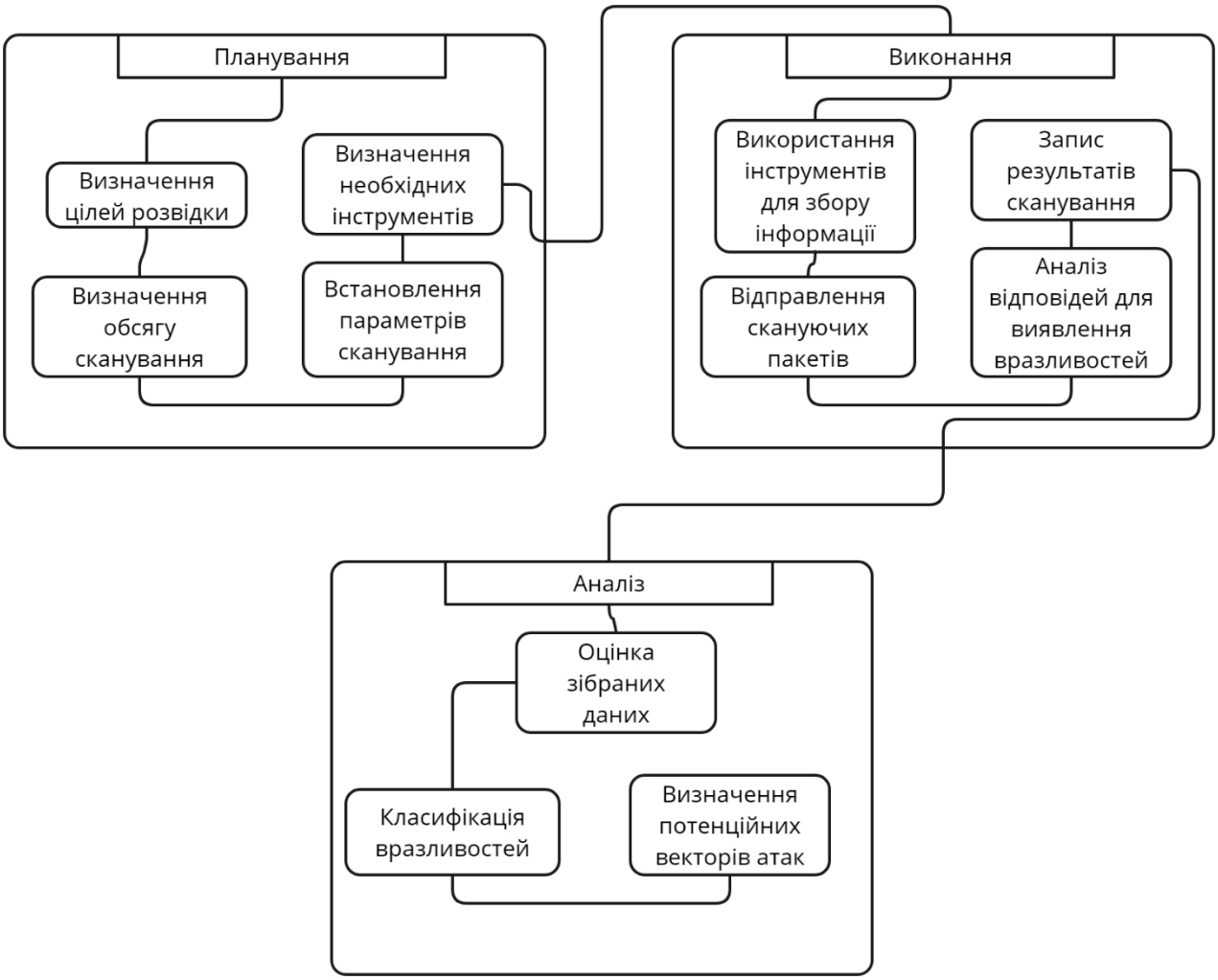
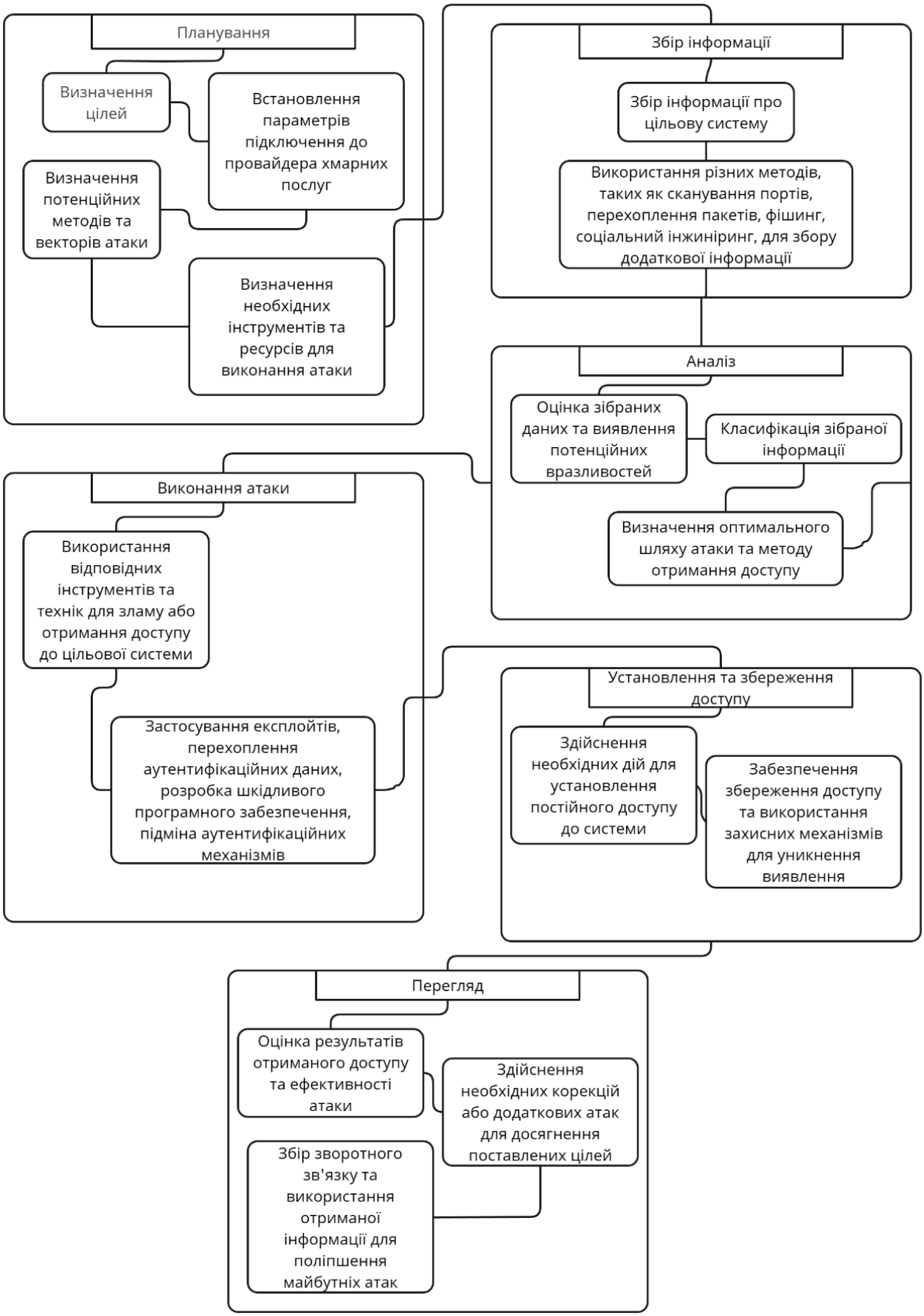
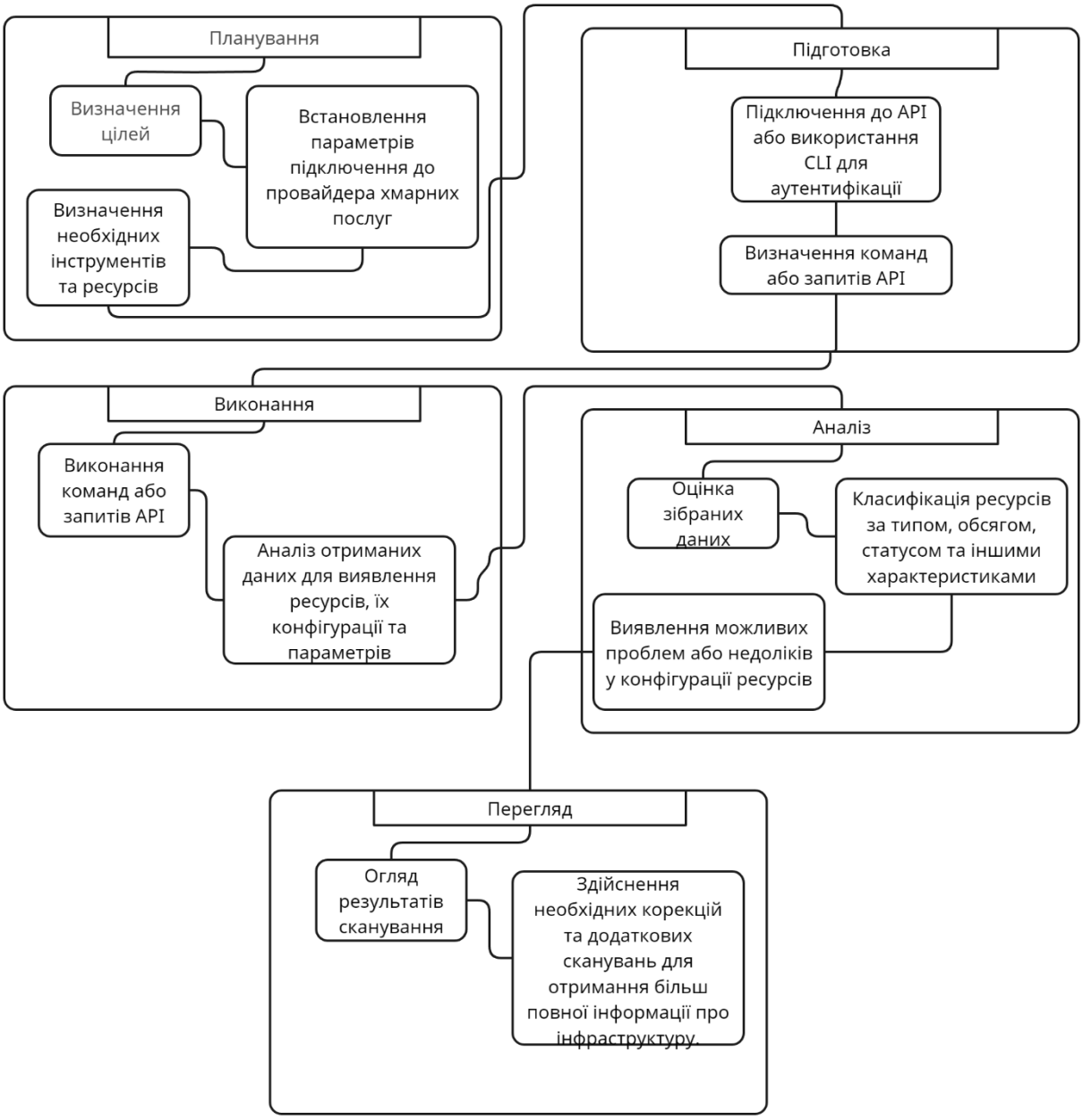


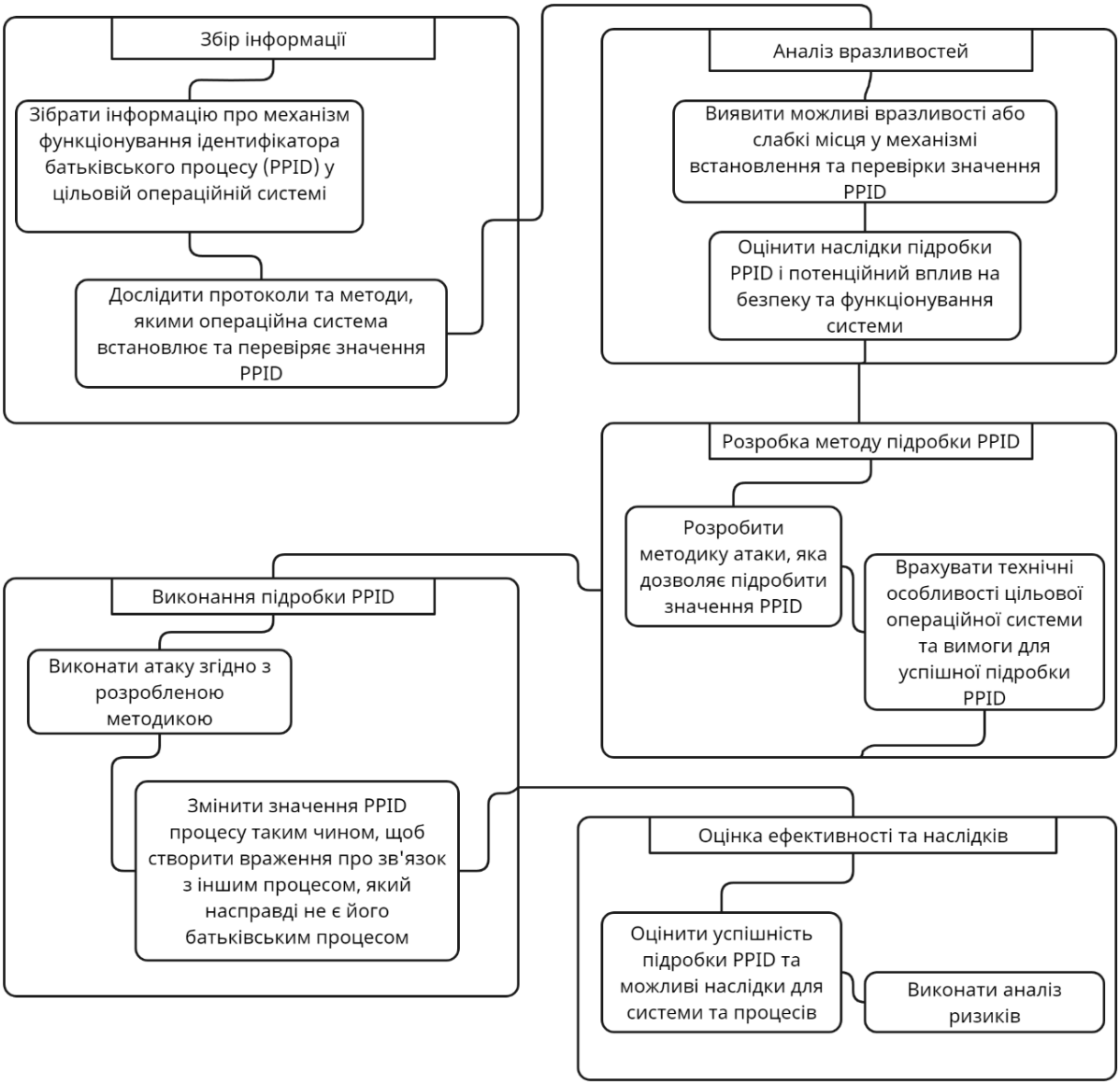
СХЕМА МОДЕЛІ ЦИКЛУ ОТРИМАННЯ ДОСТУПУ



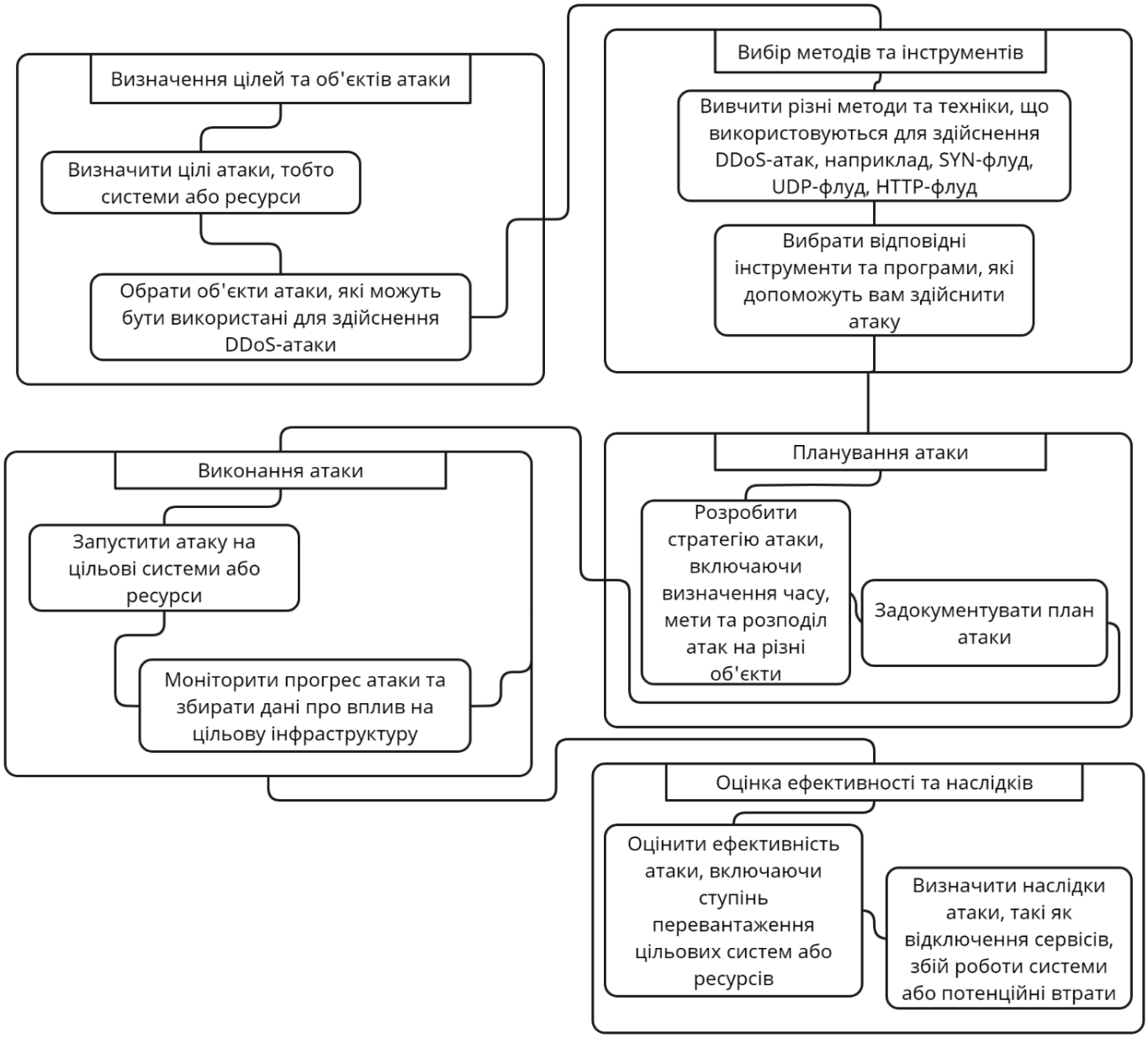
ПРОЦЕС ВИЯВЛЕННЯ ІНФРАСТРУКТУРИ IAAS



МОДЕЛЬ ЦИКЛУ ПІДРОБКИ ІДЕНТИФІКАТОРА БАТЬКІВСЬКОГО ПРОЦЕСУ (PPID)



МОДЕЛЬ ЦИКЛУ ЗДІЙСНЕННЯ АТАКИ НА ВІДМОВУ В ОБСЛУГОВУВАННІ



МОДЕЛЬ ЦИКЛУ ПІДВИЩЕННЯ ПРИВІЛЕЇВ