КНУБА · Факультет автоматизації та інформаційних технологій
Кафедра кібербезпеки та комп'ютерної інженерії

Кваліфікаційна робота бакалавра

Сценарії мережевого «Penetration Testing» у віртуалізованому середовищі кіберполігону

Виконав: **Заремба Богдан Вадимович**

Київ · 2026

АКТУАЛЬНІСТЬ

Чому це потрібно

4,8 млн

Світовий дефіцит фахівців з кібербезпеки (ISC2)

90%

організацій головною проблемою називають розрив у практичних навичках

Опанувати пентест за підручником неможливо.
Потрібне ізольоване середовище з навмисно вразливими цілями, де студент безпечно відпрацьовує реальні атаки.

Практичні навички, а не теорія є вузьким місцем у підготовці фахівців.

МЕТА ТА ЗАВДАННЯ

Мета і завдання роботи

Розробити навчальні сценарії мережевого пентесту та програмний тренажер для їх виконання — придатний до інтеграції в навчальний процес кафедри.

П'ять задач — кожна розкрита далі окремим блоком доповіді:

1. Проаналізувати наявні рішення й обґрунтувати потребу
2. Спроєктувати віртуалізоване середовище із сегментами та знімками стану
3. Розробити 5 сценаріїв (55 кроків) трьох рівнів складності
4. Реалізувати тренажер: автоматична перевірка, звіти, розширюваність
5. Провести апробацію за п'ятьма напрямами

ЗАДАЧА 1 · АНАЛІЗ ПРЕДМЕТНОЇ ГАЛУЗІ

Наявні рішення не закривають потребу

Комерційні платформи

HackTheBox, TryHackMe

- Англомовні
- 14–18 $/міс за студента
- Потрібен інтернет
- Немає контролю викладача

Академічні полігони

KYPO

- 64+ ГБ ОЗП, 16 ядер
- Окремий адміністратор
- Складне розгортання

Безкоштовні мішені

Metasploitable, DVWA

- Лише мішені
- Без мережі та сценаріїв
- Без перевірки результату
- Без оцінювання

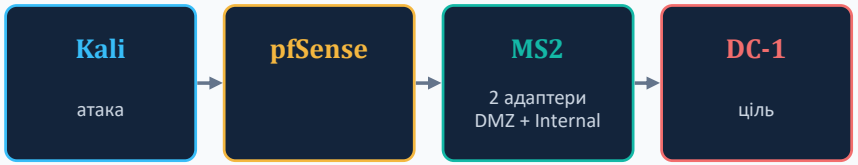
Розрив: немає безкоштовного україномовного засобу з готовими покроковими сценаріями, перевіркою відповідей і контролем викладача.

ЗАДАЧА 2 · СЕРЕДОВИЩЕ

Віртуалізоване середовище та знімки стану

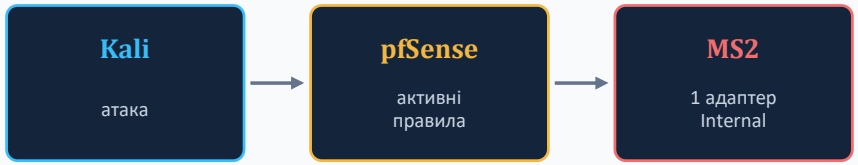
Сегментоване середовище (Kali · pfSense · Metasploitable 2 · DC-1). Кожна ВМ має знімок **`clean_state`** — той самий набір машин постає в різній топології залежно від сценарію.

Сценарій 3 · pivot



MS2 з двома адаптерами працює мостом DMZ → Internal — можливий pivot до ізольованого DC-1.

Сценарій 5 · обхід фаєрвола



MS2 лише за pfSense (один адаптер). Фаєрвол інлайн з правилами — обхід має реальний ефект.

Той самий хост грає дві ролі — завдяки знімкам стану, без ручного переналаштування мережі.

ЗАДАЧА 3 · СЦЕНАРІЇ

Стандарти й методології в основі сценаріїв

Кожен сценарій — структурований ланцюг атаки, побудований на визнаних галузевих стандартах:

PTES

Penetration Testing Execution Standard

Задає послідовність процесу пентесту — 7 фаз від розвідки до звітування.

MITRE ATT&CK

Adversarial Tactics, Techniques & Common Knowledge

Матриця технік реальних атак; кожен крок має код (напр. T1190).

Cyber Kill Chain

Модель Lockheed Martin

7 етапів логіки атакувальника — від розвідки до дій над ціллю.

Також застосовано у роботі:

NIST SP 800-115
методика тестування ІБ (4 фази)

ЗАДАЧА 3 · СЦЕНАРІЇ

П'ять сценаріїв — прогресія складності

№	Сценарій	Рівень	Кроки	Ключові техніки та інструменти
1	**Базовий пентест Metasploitable 2**	Початковий	10	Nmap · vsftpd (CVE-2011-2523) · John the Ripper
2	**Пентест додатку DVWA**	Середній	10	SQL Injection · Command Injection · Hydra
3	**Багатоетапна атака з pivot (DMZ → Internal)**	Просунутий	15	Drupalgeddon2 · proxychains · SUID · збір кред.
4	**Глибока мережева розвідка та enumeration**	Середній	10	SYN/FIN/Xmas · NSE · enum4linux · NFS
5	**Обхід stateful-фаєрвола**	Просунутий	10	fragmentation · decoy · idle-scan · ACK-scan

Прогресія: експлуатація одного сервісу → веб-рівень → багатоетапна атака крізь кілька сегментів мережі.

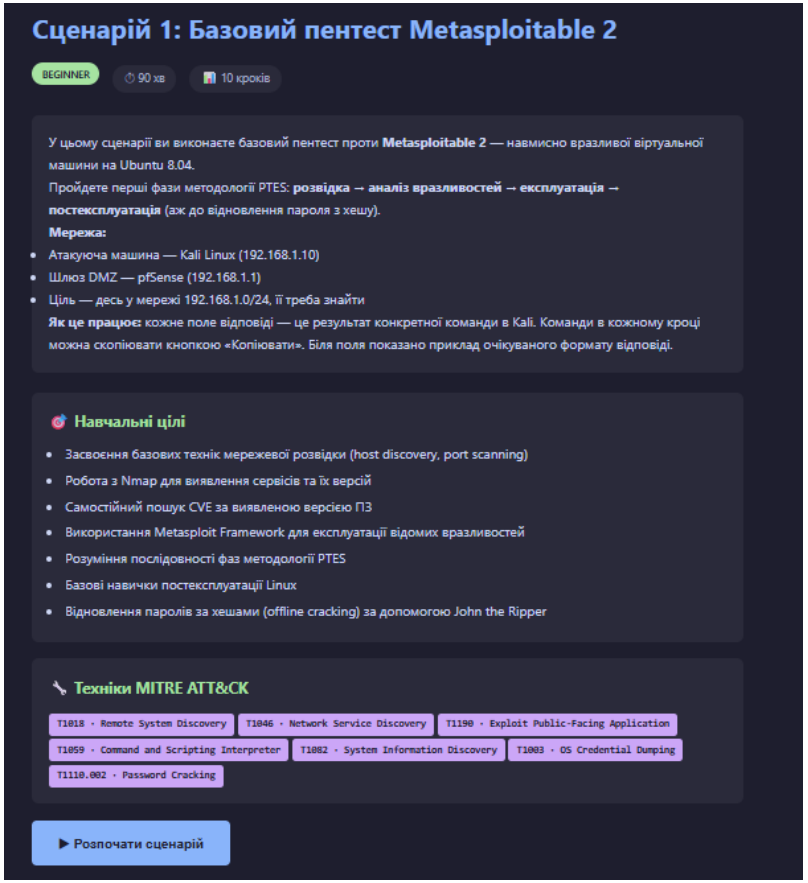
ЗАДАЧА 3 · СЦЕНАРІЙ 1 · ПОЧАТКОВИЙ

Базовий пентест Metasploitable 2

Повний цикл атаки на окремий хост — від розвідки до зламу облікових даних.

Інструменти: Nmap · Metasploit Framework · John the Ripper

1. **Розвідка**
   Nmap: хости й порти
   T1046
2. **Пошук CVE**
   версія vsftpd
   T1190
3. **Експлуатація**
   бекдор vsftpd → shell
   T1190
4. **Облікові дані**
   хеш з /etc/shadow
   T1003
5. **Злам пароля**
   John (режим single)
   T1110.002



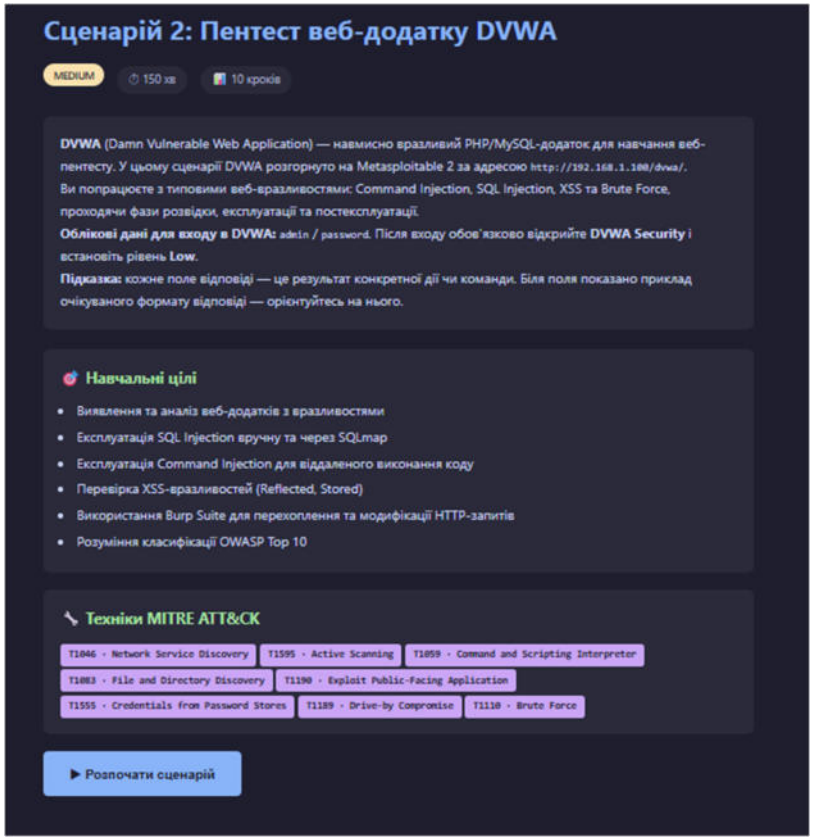
ЗАДАЧА 3 · СЦЕНАРІЙ 2 · СЕРЕДНІЙ

Пентест додатку DVWA

Веб-застосунок як мережевий сервіс на порту 80 — типові вразливості OWASP.

Інструменти: Браузер · SQLmap · Hydra

1. **Веб-сервер**
   Nmap, порт 80
   T1046
2. **Command Exec**
   RCE + файлова система
   T1059
3. **SQL Injection**
   Boolean + UNION SELECT
   T1190
4. **Витяг хешів**
   SQLi / SQLmap
   T1555
5. **XSS + Brute**
   Hydra на форму входу
   T1110



ЗАДАЧА 3 · СЦЕНАРІЙ 3 · ПРОСУНУТИЙ

Багатоетапна атака з pivot (DMZ → Internal)

Латеральний рух: компрометація DMZ → транзит → атака ізольованого DC-1.

Інструменти: Metasploit · proxychains · Nmap

1. **Розвідка DMZ та Internal**

   Internal недоступний прямо

   `T1018`

2. **Initial Access**

   Samba на Metasploitable

   `T1190`

3. **Pivot**

   autoroute + SOCKS-проксі

   `T1090`

4. **Drupalgeddon2**

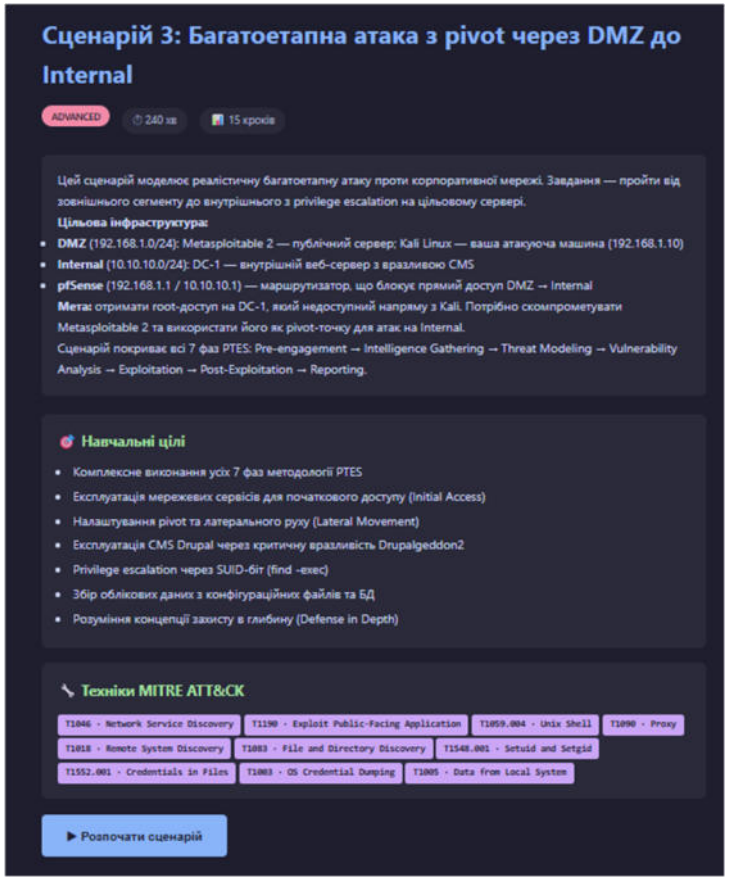
   DC-1 · CVE-2018-7600

   `T1190`

5. **Privesc + флаг**

   SUID find -exec

   `T1548.001`



ЗАДАЧА 3 · СЦЕНАРІЙ 4 · СЕРЕДНІЙ

Глибока мережева розвідка та enumeration

Глибока розвідка й enumeration — фундамент будь-якої подальшої атаки.

Інструменти: Nmap (NSE) · enum4linux · Nikto · dirb

1. **SYN / UDP**
   сканування портів
   `T1046`

2. **OS fingerprint**
   TCP/IP стек
   `T1082`

3. **NSE-скрипти**
   SMB-вразливості
   `T1595.002`

4. **enum4linux**
   SMB-облікові + NFS
   `T1087.001`

5. **Nikto / dirb**
   HTTP, приховані шляхи
   `T1595.001`

ЗАДАЧА 3 · СЦЕНАРІЙ 5 · ПРОСУНУТИЙ

Обхід stateful-фаєрвола

Інструменти: Nmap · proxychains · tshark

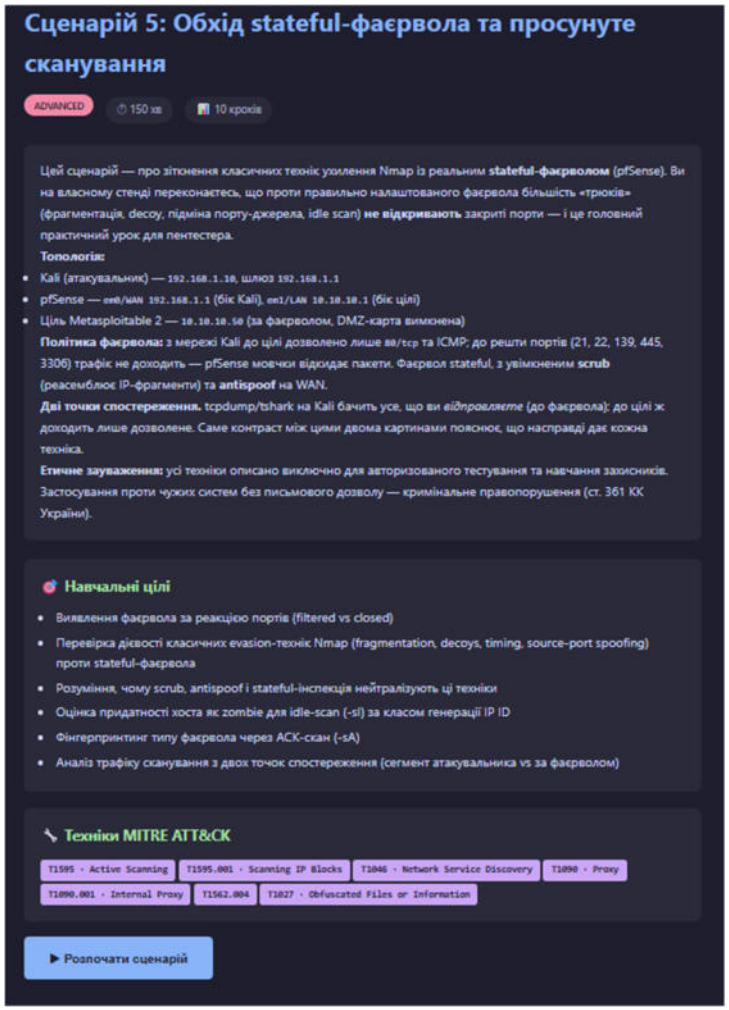
1. **Filtered/closed**
   розвідка крізь pfSense
   `T1046`

2. **Фрагментація**
   -f проти scrub
   `T1027`

3. **Decoy / spoof**
   підставні IP та порт
   `T1090`

4. **Idle scan**
   -sI через zombie
   `T1090`

5. **ACK-скан**
   мапа правил фаєрвола
   `T1595`

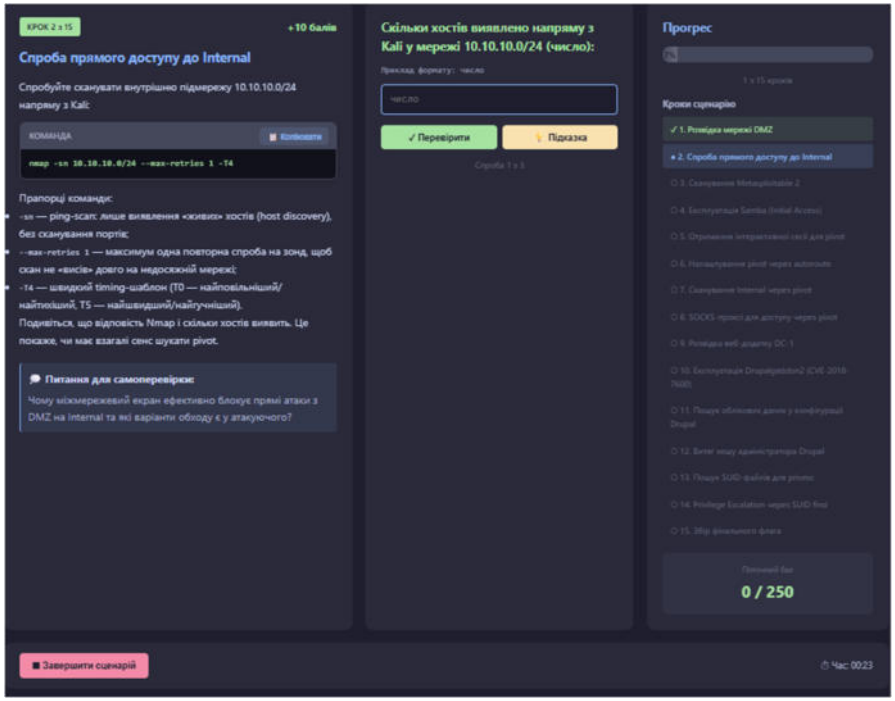


ЗАДАЧА 4 · ТРЕНАЖЕР

Як тренажер перевіряє відповіді

Команда — у Kali Linux › **Реальний вивід** — аналіз результату › **Прапор** — версія, CVE, хеш › **Валідатор** — 5 типів перевірки › **Бали** — залік кроку › **PDF-звіт** — оцінка у ЄКТС

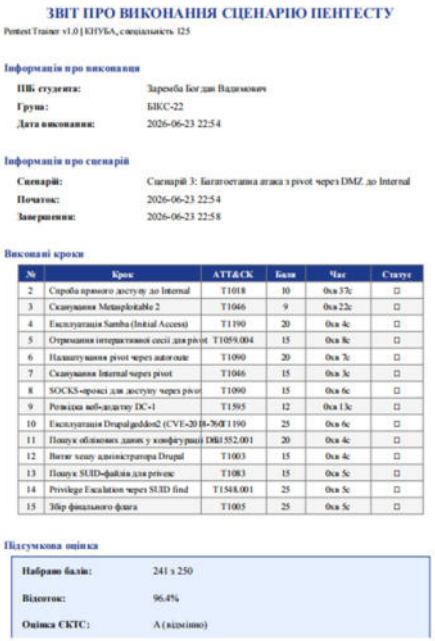
- Кожен крок прив'язаний до техніки MITRE ATT&CK
- Підказка трохи знижує бали за крок
- Контрольне теоретичне питання на розуміння



5 типів валідаторів: точний збіг · регулярний вираз · числовий діапазон · підрядок · вибір з варіантів

ЗАДАЧА 4 · ТРЕНАЖЕР

Автоматичний PDF-звіт про проходження



ЗВІТ ПРО ВИКОНАННЯ СЦЕНАРІЮ ПЕНТЕСТУ

Pentest Trainer v1.0 | КНУБА, спеціальність 125

Інформація про виконання

ПІБ студента:	Заремба Богдан Вадимович
Група:	БІКС-22
Дата виконання:	2026-06-23 22:54

Інформація про сценарій

Сценарій:	Сценарій 3: Багатоетапна атака з pivot через DMZ до Internal
Початок:	2026-06-23 22:54
Завершення:	2026-06-23 22:58

Виконані кроки

№	Крок	ATT&CK	Бали	Час	Статус
2	Спроба прямого доступу до Internal	T1018	10	0хв 37с	□
3	Сканування Metasploitable 2	T1046	9	0хв 22с	□
4	Експлуатація Samba (Initial Access)	T1190	20	0хв 4с	□
5	Отримання інтерактивної сесії для pivot	T1059.004	15	0хв 8с	□
6	Налаштування pivot через autoroute	T1090	20	0хв 7с	□
7	Сканування Internal через pivot	T1046	15	0хв 3с	□
8	SOCKS-проксі для доступу через pivot	T1090	15	0хв 6с	□
9	Розвідка веб-додатку DC-1	T1595	12	0хв 13с	□
10	Експлуатація Drupalgeddon2 (CVE-2018-7600)	T1190	25	0хв 6с	□
11	Пошук облікових даних у конфігурації	DBI 552.001	20	0хв 4с	□
12	Витяг хешу адміністратора Drupal	T1003	15	0хв 4с	□
13	Пошук SUID-файлів для privesc	T1083	15	0хв 5с	□
14	Privilege Escalation через SUID find	T1548.001	25	0хв 5с	□
15	Зчит фінального флага	T1005	25	0хв 5с	□

Підсумкова оцінка

Набрано балів:	241 з 250
Відсоток:	96.4%
Оцінка ECTS:	A (відмінно)

Звіт містить:

- **Бали за кожен крок** — і підсумкову суму
- **Підсумкова оцінка** — переведена у шкалу ЄКТС
- **Загальний час** — проходження сценарію
- **Використані підказки** — кількість і вплив на бали

Студент отримує об'єктивну автоматичну оцінку, викладач — готовий звіт без ручної перевірки.

ЗАДАЧА 4 · ТРЕНАЖЕР

Модульність і розширюваність

Формат JSON

Новий додається без зміни коду

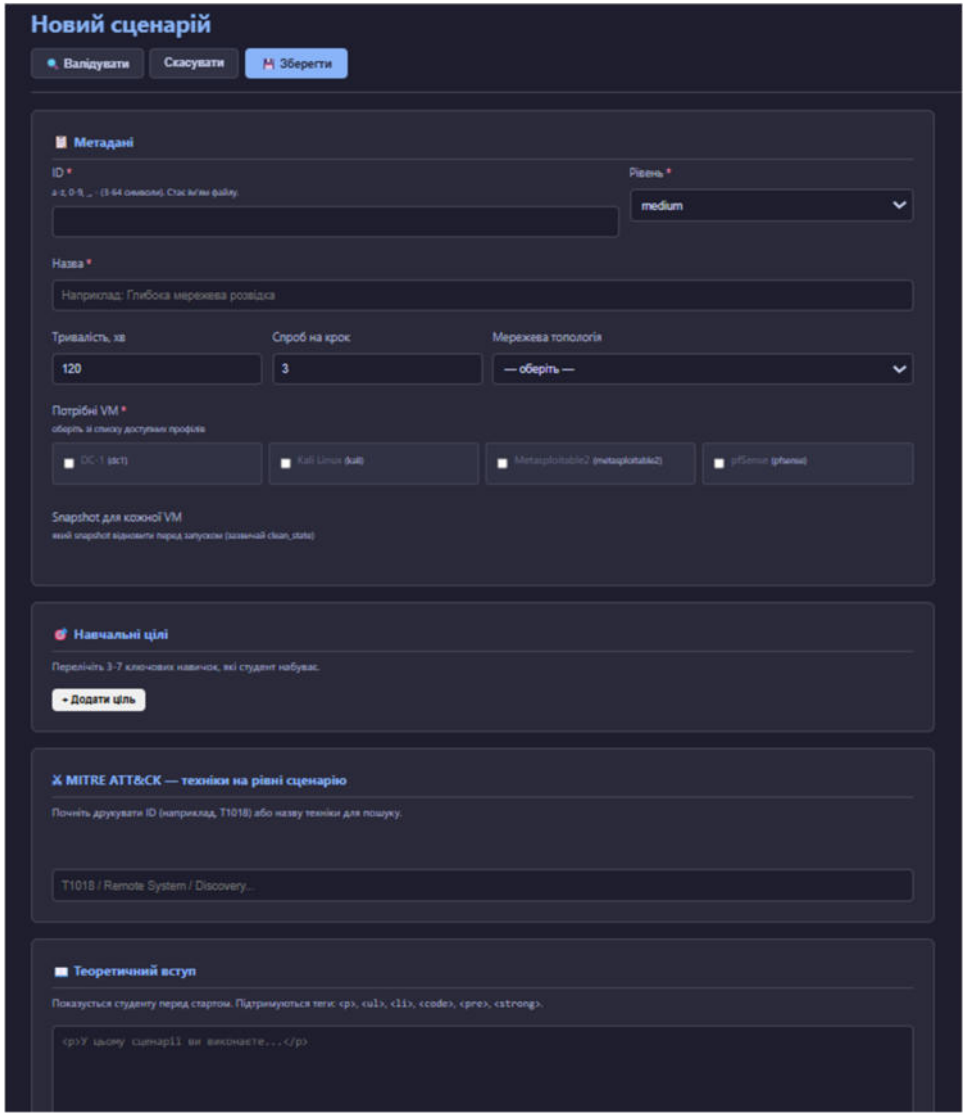
CLI-інструменти

Створення та валідація сценаріїв із командного рядка

Веб-редактор

Візуальне створення з заповненням технік ATT&CK

Новий сценарій — 8 хвилин
проти 52 хв ручним JSON



ПРАКТИЧНИЙ ВНЕСОК

Що дає робота на практиці

Безкоштовне, україномовне, автономне рішення з готовими сценаріями — придатне до впровадження в навчальний процес без комерційних ліцензій і без доступу до інтернету.

Рішення побудоване за модульним принципом — розширюється без зміни коду:

1

Модульні сценарії

Опис у форматі JSON — новий сценарій додають без зміни коду

`scenario_loader.py`

2

Додавання ВМ з вебінтерфейсу

Нові віртуальні машини реєструють і запускають через панель

`vm_manager.py`

3

Знімки стану й топологія

Відкат до еталона перед стартом; знімок задає топологію сценарію

`clean_state`

4

Гнучка перевірка

П'ять типів валідаторів, стійких до змінного стану цілі

`5 валідаторів`

Викладач розширює середовище — нові сценарії та машини — без програмування

ЗАДАЧА 5 · ОЦІНЮВАННЯ

Апробація за п'ятьма напрямами

1	**Вимірювання середовища**	старт ВМ 43–87 с · RAM ~1,2 ГБ · диск ~30 ГБ → працює на ПК з 8 ГБ
2	**Самотестування сценаріїв**	усі 55 кроків прийняв валідатор · 160 хв проти 290 планових (–44,8%)
3	**Розширюваність**	новий сценарій 8 хв через веб-редактор проти 52 хв ручним JSON
4	**Порівняння з аналогами**	україномовність · безкоштовність · автономність
5	**Покриття стандартів**	36 технік ATT&CK · 7 фаз PTES · 7/8 підфаз NIST 800-115

ЗАДАЧА 5 · ПОКРИТТЯ

Покриття MITRE ATT&CK

Сценарії покривають 9 із 12 ключових тактик — загалом 36 технік:

Reconnaissance T1595	**Initial Access** T1190	**Execution** T1059	**Privilege Esc.** T1548.001	**Defense Evasion** T1027 · T1036
Credential Access T1003 · T1110 · T1555	**Discovery** T1046 · T1018 · T1082	**Command & Control** T1090 · T1572	**Collection** T1005	

Детальне покриття PTES і NIST SP 800-115 — на наступному слайді.

ЗАДАЧА 5 · ПОКРИТТЯ

Покриття PTES та NIST SP 800-115

PTES 7 / 7 фаз

- ✓ Pre-engagement
- ✓ Intelligence Gathering
- ✓ Threat Modeling
- ✓ Vulnerability Analysis
- ✓ Exploitation
- ✓ Post-Exploitation
- ✓ Reporting

NIST SP 800-115 7 / 8 підфаз

- ✓ Planning
- ✓ Discovery: Network Discovery
- ✓ Discovery: Vulnerability ID
- ✓ Attack: Gaining Access
- ✓ Attack: Escalating Privileges
- ✓ Attack: System Browsing
- — Attack: Install Add. Tools
- ✓ Reporting

ВИСНОВКИ

Мету досягнуто — усі 5 задач виконано

- Проаналізовано наявні рішення й обґрунтовано потребу
- Побудовано віртуалізоване середовище зі знімками стану
- Розроблено 5 сценаріїв (55 кроків, 3 рівні складності)
- Реалізовано тренажер: автоматична перевірка, звіти, розширюваність
- Проведено апробацію за 5 напрямами з підтвердженням покриття стандартів

Безкоштовний україномовний інструмент, готовий до впровадження в навчальний процес кафедри.

Дякую за увагу!

Готовий відповісти на запитання

Заремба Богдан Вадимович · КНУБА · 2026