МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(Протокол №9/24 від 29 серпня 2024 р.)

Завідувач кафедри .

Петро ВЕНГЕРСЬКИЙ

Силабус з навчальної дисципліни
“Етичне тестування на злом і проникнення”,
що викладається в межах ОПП Технології штучного інтелекту в кібербезпеці
другого (магістерського) рівня вищої освіти для здобувачів з спеціальності 125 – Кібербезпека та захист інформації

Львів 2024 р.

Назва дисципліни	Етичне тестування на злом і проникнення
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Пелешко Дмитро Дмитрович, професор кафедри кібербезпеки Беляєв Ігор Сергійович, асистент кафедри кібербезпеки
Контактна інформація викладачів	dmytro.peleshko@lnu.edu.ua https://ami.lnu.edu.ua/employee/peleshko-d-d Igor.Beliaiev@lnu.edu.ua https://ami.lnu.edu.ua/en/employee/i-s-beliaiev Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Zoom чи Microsoft Teams. Для погодження часу онлайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua
Інформація про дисципліну	Дисципліна “Етичне тестування на злом і проникнення” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Технології штучного інтелекту в кібербезпеці, яка викладається у 3-му семестрі другого (магістерського) рівня освіти в обсязі 3 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей, розвитку системи знань про методики проведення етичного тестування на злом і проникнення, розвиток практичних навичок у аналізі різноманітних атак на веб-додатки, освоєння методів обходу фільтрації та інших захисних механізмів, а також рекомендації для підвищення рівня безпеки.
Мета та цілі дисципліни	Курс вибіркової дисципліни має на меті надати студентам теоретичні знання та практичні навички у сфері тестування на проникнення. Це досягається за допомогою використання спеціальних загальнодоступних платформ з завданнями, які допомагають засвоїти методики типових атак на веб-додатки.
Література для вивчення дисципліни	*Основна* 1. Dafydd Stuttard, Marcus Pinto.The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. 2. Peter Yaworski. Web Hacking 101. 3. Joel Scambray, Vincent Liu, and Caleb Sima. Hacking Exposed Web Applications, 3rd Edition

	4. Prakhar Prasad. Mastering Modern Web Penetration Testing 5. Peter Yaworski. Real-World Bug Hunting: A Field Guide to Web Hacking. 6. Joseph Muniz, Aamir Lakhani.Web Penetration Testing with Kali Linux. 7. Michal Zalewski. The Tangled Web: A Guide to Securing Modern Web Applications 8. Seth Fogie, Jeremiah Grossman, Robert Hansen, Anton Rager, and Petko D. Petkov. Cross-Site Scripting Attacks: XSS Exploits and Defense. *Рекомендовані онлайн курси* 9. Hack The Box: https://www.hackthebox.eu/ 10. PentesterLab: https://pentesterlab.com/ 11. Cybrary: https://www.cybrary.it/ 12. Udemy (Penetration Testing Courses): https://www.udemy.com/course/learn-ethical-hacking-from-scratch/ 13. TryHackMe: https://tryhackme.com/ 14. eLearnSecurity: https://www.elearnsecurity.com/ 15. Offensive Security Certified Professional (OSCP): https://www.offensive-security.com/pwk-oscp/
Обсяг курсу	Загальний обсяг: 90 годин. Аудиторних занять: 48 год., з них 16 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 42 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** - загальні концепції та принципи кібербезпеки, включаючи захист інформації, криптографію, ідентифікацію та аутентифікацію - технологічні рішення для підвищення рівня безпеки веб-додатків; - засоби захисту даних та вирішення пов'язаних з цим проблем; - характерні загрози, типи атак та їх поширення; - найбільш поширені види атак; - проблеми, пов'язані з фільтрацією даних, введених користувачами; - використання інструменту Burp Suite для аналізу мережевого трафіку. **вміти:** - використовувати інструмент Burp Suite для аналізу та перехоплення мережевого трафіку; - виявляти та аналізувати можливі загрози та атаки; - обходити фільтрацію даних, введених користувачами на веб-сервері; - експлуатувати типові вразливості, такі як XSS та SQL ін'єкції; - знаходити місконфігурації у HTTP заголовках запитів, що надходять до сервера; - застосовувати знання з кібербезпеки в реальних умовах; - складати рекомендації щодо захисту веб-додатків у професійній діяльності.
Ключові слова	Етичний хакінг, тестування на проникнення, кібербезпека, аутентифікація, авторизація, контроль доступу, кібератака, загроза, вразливість, конфіденційність, цілісність, безпека даних, криптографія, ін’єкції, Burp Suite, OWASP top 10.
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче

<table>
<tr><td>Підсумковий контроль, форма</td><td>Залік у кінці семестру</td></tr>
<tr><td>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</td><td>Презентації, лекції
Модульний контроль
Індивідуальні завдання</td></tr>
<tr><td>Необхідне обладнання</td><td>Лабораторія з обладнаними робочими станціями, з’єднаними в комп’ютерну мережу або персональний ноутбук.</td></tr>
<tr><td>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</td><td>Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:
• усне опитування, індивідуальні завдання, самостійна робота: 60% семестрової оцінки; максимальна кількість балів 60
• модульний контроль: 40% семестрової оцінки; максимальна кількість балів 40
Підсумкова максимальна кількість балів 100.
Академічна доброчесність: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.
Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов’язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом.
Література. Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.
Політика виставлення балів. Враховуються бали набрані за виконання індивідуальних завдань, при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов’язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов’язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін.
Жодні форми порушення академічної доброчесності не толеруються.
<table>
<tr><th>Критерії оцінювання знань студентів</th><th>Бали рейтингу</th><th>Макс. к-сть балів</th></tr>
<tr><td colspan="3">1. Бали поточної успішності за виконання 5-ти індивідуальних завдань</td></tr>
<tr><td>Критерії оцінювання (5*10 бали)</td><td colspan="2">50 балів</td></tr>
</table>
</td></tr>
</table>

Студент в повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час захисту індивідуальних завдань, глибоко та всебічно розкриває зміст теоретичних питань. Реалізоване програмне забезпечення пройшло перевірку на плагіат та повністю виконує умову завдання.	**10-9**
Студент достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час захисту індивідуальних завдань, в основному розкриває зміст теоретичних питань. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації. Реалізоване програмне забезпечення містить окремі несуттєві неточності та незначні помилки.	**8-5**
Студент не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхнево (без аргументації та обґрунтування) викладає його під час захисту лабораторного завдання, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності, програмна реалізація індивідуального завдання частково виконана.	**4-1**
Студент не виконав індивідуальне завдання та не володіє матеріалом.	**0**
2. Самостійна робота студентів (СРС)	
Критерії оцінювання (5*2 бали)	**10 балів**
Самостійна робота (додаткове опрацювання матеріалу за темами дисципліни поза межами наданого лектором, з додаткових джерел) Самостійна робота студентів, оцінюється під час захисту відповідних лабораторних робіт. Студент додатково опрацював матеріал, підготував доповідь та аргументовано його викладає.	**2-1**
Студент не опрацював самостійно додаткових джерел і не володіє матеріалом	**0**
3. Модульний контроль	**40**
Критерії оцінювання (2*20 балів)	**40**
Протягом семестру проводиться **2 модульних контролі**. Кожен модуль містить **20 тестових питань.**	**15**
Критерії оцінювання вирішення тестів (20*1 бал):	***20***
Відповідь вірна	**1**
Відповідь невірна	**0**
Загальна кількість балів по завершенні вивчення дисципліни	**100**

Додаткові бали / або зарахування певних тем можна отримати за результатами **неформального та/або інформального навчання за** тематикою даної дисципліни. Визнання та зарахування результатів такого навчання відбувається у відповідності до наданих документів про неформальне та/або інформальне навчання.
Жодні форми порушення академічної доброчесності не толеруються.

Питання до модульних контролів	1. Що таке тестування на проникнення? 2. Види тестувань на проникнення. 3. Основні середовища застосування пентесту. 4. Що таке OWASP TOP 10? 5. Назвати найрозповсюдженіші види атак. 6. Основні види XSS атак.

	7. Як перевірити наявність SQL ін’єкції? 8. Які вразливості існують в аутентифікації та авторизації? 9. Які загрози пов'язані з бездротовими мережами? 10. Які інструменти використовуються для виявлення вразливостей у веб-додатках? 11. Які методи шифрування даних застосовуються для захисту інформації? 12. Які основні принципи етичного хакінгу? 13. Які загрози існують для IoT пристроїв? 14. Як здійснюється тестування на проникнення мобільних додатків? 15. Які заходи безпеки необхідно враховувати при розробці веб-додатків? 16. Як використовується соціальна інженерія в пентесті? 17. Які правові аспекти пов'язані з проведенням тестування на проникнення? 18. Які методи використовуються для захисту від CSRF атак? 19. Які вимоги до документування результатів пентесту? 20. Які стратегії використовуються для мінімізації наслідків вразливостей? 21. Як використовується фаззінг для виявлення вразливостей у програмному забезпеченні? 22. Які методи захисту від витоку інформації? 23. Як виконується аналіз вразливостей в реальному часі? 24. Які існують методики відновлення після кібератак? 25. Які основні елементи включаються до звіту з пентесту?
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання
1	**Тема 1. Введення в етичний хакінг** (Цей модуль знайомить учасників з основами етичного хакінгу, включаючи правові аспекти та етичні норми, необхідні для авторизованого тестування систем на вразливості. Види тестувань (white box, black box, gray box))	лекція, самостійна робота	[1-10]	1 3	1 тиждень
		лаб.	[1-10]	2	
2	**Тема 2. Тестування на проникнення.** (У цьому розділі розглядаються методи та інструменти тестування на проникнення, які використовуються для ідентифікації та виправлення вразливостей в IT-інфраструктурі та додатках.)	лекція, самостійна робота	[1-10]	2 4	1 тиждень
		лаб.	[1-10]	4	
3	**Тема 3. Веб-безпека та вразливості.** (Вивчення структури веб-додатків, клієнт-серверної архітектури, HTTP/HTTPS протоколів та технологій, які часто використовуються у веб-додатках.)	лекція, самостійна робота	[1-10]	2 5	1 тиждень
		лаб.	[1-10]	2	
4	**Тема 4. Використання інструментів для тестування на проникнення. Перехоплення та аналіз трафіку** (Використання інструментів для перехоплення та аналізу трафіку мережі, таких як Wireshark та Burp Suite.)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
		лаб.	[1-10]	4	

5	**Тема 5. Найпоширеніші вразливості OWASP TOP 10.** (Вивчення і аналіз десяти найпоширеніших вразливостей веб-додатків за класифікацією OWASP.)	лекція, самостійна робота	[1-10]	2 6	1 тиждень
		лаб.	[1-10]	4	
6	**Тема 6. Аутентифікація, авторизація та управління сесіями.** (Аналіз типових помилок у реалізації механізмів аутентифікації та авторизації, а також управління сесіями. Атаки на них)	лекція, самостійна робота	[1-6]	2 5	1 тиждень
		лаб.	[1-6]	4	
7	**Тема 7. Cross-Site Scripting (XSS), Ін'єкції SQL та інші типи ін'єкцій** (Теоретичні основи та практичні вправи по виявленню та усуненню XSS та CSRF вразливостей, Практичні заняття з виявлення та експлуатації SQL ін'єкцій, а також інших типів ін'єкцій, таких як Command Injection.)	лекція, самостійна робота	[1-10]	3 7	1 тиждень
		лаб.	[1-10]	8	
8	**Тема 9. Підготовка звітів та рекомендацій з усунення вразливостей** (Навички підготовки детальних звітів про виявлені вразливості та розробка рекомендацій щодо їх усунення для замовників або команди розробників.)	лекція, самостійна робота	[1-10]	2 5	1 тиждень
		лаб.	[1-10]	4	