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 № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри ____ П.С.Венгерський

Силабус з навчальної дисципліни "Інструменти проведення тестування на проникнення", що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	**Інструменти проведення тестування на 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	Беляєв Ігор Сергійович, асистент кафедри кібербезпеки (лекції та лабораторні заняття)
Контактна інформація викладачів	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/course/
Інформація про дисципліну	Дисципліна “ Інструменти проведення тестування на проникнення” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається у 6-му семестрі в обсязі 5-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Дисципліна "Інструменти проведення тестування на проникнення" спрямована на ознайомлення студентів з основними засобами та методиками, які використовуються для оцінки безпеки інформаційних систем. Курс включає в себе вивчення програмних і апаратних інструментів, призначених для виявлення вразливостей і потенційних проблем у системах безпеки, а також методів аналізу та реагування на виявлені загрози.
Мета та цілі дисципліни	Метою курсу є отримання практичних навичок з використання сканерів вразливостей, експлойтів, фішингових атак, систем моніторингу та аудиту безпеки, що допоможе їм ефективно захищати інформаційні ресурси в сучасних комп'ютерних системах.
Література для вивчення дисципліни	1. Cybersecurity Fundamentals/ ISACA/ www/isaca/org/cyber? Cybersecurity Fundamentals Study Guide/ 2003.- 156 p. 2. Sankar R. Burpsuite – A Beginner’s Guide For Web Application Security or Penetration Testing [Електронний ресурс] / Ravi Sankar. – 2018. – Режим доступу до ресурсу: https://kalilinuxtutorials.com/burpsuite/. 3. Державна служба спеціального зв'язку та захисту інформації України./ www.dsszzi.gov.ua 4. Learn Ethical Hacking from Scratch: Your Stepping Stone to Penetration Testing 5. Common Vulnerability Scoring System Calculator Version 3/ https://nvd.nist.gov/vuln- metrics/cvss/v3-calculator.

Обсяг курсу	Загальний обсяг: 150 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 86 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** • найрозповсюдженіші види атак та проблеми захисту даних • типові загрози, атаки та області їх розповсюдження; • популярні інструменти тестування на проникнення; • технології щодо поліпшення безпеки у веб-додатках; • експлуатацію баз даних через ін'єкції; • основні проблеми у фільтрації даних, які ввів користувач; **вміти:** • застосовувати знання з кібербезпеки в практичній діяльності; • розробляти моделі загроз інформації та моделі порушників інформаційної безпеки; • ідентифікувати можливі загрози чи атаки; • використовувати Web Proxy для перехвату трафіку • обходити фільтрацію введених даних на веб-сервері • експлотувати типові вразливості як XSS, SQL ін'єкція • обирати правильні рекомендації щодо захисту веб-додатку при здійсненні професійної діяльності; **Курс забезпечує набуття таких компетентностей: КІ, КЗ 1, КЗ 4, КЗ 5, КФ 1, КФ 3, КФ 4, КФ 6, КФ 7, КФ 8, КФ 9, КФ 10; та програмних результатів навчання: ПРН 3, ПРН 4, ПРН 5, ПРН 9, ПРН 10, ПРН 12, ПРН 14, ПРН 32,ПРН 34, ПРН 50, ПРН 54.**
Ключові слова	Кібербезпека, кібератака, загроза, вразливість, конфіденційність, цілісність, безпека даних, криптографія, OWASP top 10, Burp Suite, ін'єкції, тестування на проникнення, авторизація, аутентифікація, контроль доступу.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Подано в схемі курсу .
Підсумковий контроль, форма	Залік у кінці семестру.
Пререквізити	Для вивчення курсу студенти потребують базові знання з таких дисциплін: 1) Основи кібербезпеки; 2) Операційні системи та комп'ютерні мережі; 3) Основи криптографії.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Демонстрація інструментів тестування на проникнення Робота з інструментами для тестування на проникнення Індивідуальні завдання
Необхідне обладнання	Комп'ютер, чи ноутбук з можливістю віртуалізації; Програмне забезпечення віртуалізації: VirtualBox, або VMware; Операційні системи: Windows, Ubuntu, Kali Linux; Програмне забезпечення Burp Suite, або OWASP ZAP;
Критерії оцінювання (окремо для кожного виду	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • модульний контроль, тестування, усне опитування: 50% семестрової

навчальної діяльності)	оцінки; максимальна кількість балів 50 • лабораторні роботи: 50% семестрової оцінки; максимальна кількість балів 50 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 практичні зайняття 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 при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного 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.
Питання до контролю	1. Які основні функції сканерів вразливостей і як вони допомагають у забезпеченні безпеки інформаційних систем? 2. Що таке фішингові атаки і які методи захисту від них можуть бути застосовані? 3. Які основні етапи експлуатації баз даних через ін'єкції і як їх можна запобігти? 4. Які інструменти використовуються для моніторингу та аналізу мережевого трафіку? 5. Які техніки можуть бути використані для поліпшення безпеки вебдодатків, і які переваги вони надають у забезпеченні захисту? 6. Що таке тестування на проникнення. 7. Види тестувань на проникнення. 8. OWASP TOP 10. 9. Назвати найрозповсюдженіші види атак. 10. Основні види XSS атак. 11. Як перевірити наявність ін'єкції. 12. Вразливісті в аутентифікації. 13. Типи вразливостей контролю доступу. 14. Чим можна перехопити трафік між користувачем та сервером. 15. DoS, DDos та SEO. Визначення типу атаки. 16. Види SQL ін'єкцій. 17. Захист від SQL ін'єкцій. 18. Як можна обійти фільтрацію на сервері. 19. Загрози для мобільних пристроїв. 20. Принципи безпечної роботи з мобільними пристроями.

	21. Надійна аутентифікація. Поширення особистої інформації. 22. Типи веб фаєрволів. 23. Визначення відповіді програми сканування. 24. Виявлення місконфігурацій у заголовках веб-запитів. 25. Виявлення шкідливого програмного забезпечення. 26. Найкращі практики безпеки. Безпека електронних фінансів 27. XXE. 28. Ланцюг вкрадення сеансових данних користувача. Методи захисту. 29. Що використовується для створення сеансу користувача. 30. Назвати етапи проведення тестування на проникнення. 31. Види обходу завантаження шкідливого файлу. 32. Оформлення звітів на тестування на проникнення.
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
1-2	РОЗДІЛ 1. ОСНОВИ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ: КОНЦЕПЦІЇ, МЕТОДИ ТА ЦІЛІ. Визначення тестування на проникнення та його роль у забезпеченні безпеки. Огляд основних фаз тестування на проникнення: розвідка, сканування, експлуатація та звіт. Порівняння тестування на проникнення з іншими методами тестування безпеки.	лекція, лаб, самостійна робота		4 4 10	2 тижні
3-4	РОЗДІЛ 2. ПІДХОДИ ДО ТЕСТУВАННЯ НА ПРОНИКНЕННЯ Існуючі види (мобільні додатки, веб додатки і т.д) Види тестувань (white box, black box, gray box) Фази тестування на проникнення (договір, розвідка, сканування, ескплотація, звіт) ..	лекція, лаб, самостійна робота		4 4 12	2 тижні
5-6	РОЗДІЛ 3. ВИДИ	лекція,		4	2 тижнів

	АТАК ТА ЇХ МЕТОДИКИ: ВІД СКАНУВАННЯ ДО ЕКСПЛУАТАЦІЇ. Розбір різних видів атак: зовнішні та внутрішні. Огляд інструментів для виявлення вразливостей та аналізу атак. Дослідження методів залучення до системи та отримання доступу до неї.	лаб самостійна робота		4 12	
7-8	РОЗДІЛ 4. Інструменти сканування вразливостей: Популярні програмні засоби сканування: відкриті та комерційні. Пошук та оцінка вразливостей за допомогою інструментів сканування. Створення звітів та рекомендацій для усунення виявлених проблем.	лекція, лаб самостійна робота		4 4 12	2 тижні
9-10	РОЗДІЛ 5. Аналіз загроз і вразливостей інформаційних систем. Типові загрози та їх вплив на інформаційну безпеку. Методи інвентаризації вразливостей: активний та пасивний аналіз. Використання стандартів та критеріїв для оцінки рівня загроз та вразливостей.	лекція, лаб самостійна робота		4 4 10	2 тижні
11-13	РОЗДІЛ 6. Експлуатація вразливостей Розбір основних методів експлуатації вразливостей. Практичні приклади використання різних типів атак для отримання доступу.	лекція, лаб, самостійна робота	[3, 7, 8, 9]	6 6 14	3 тижні

	Стратегії захисту від різних видів експлуатації вразливостей. .				
14-16	РОЗДІЛ 7. Системи моніторингу та реагування на інциденти безпеки. Визначення систем моніторингу та їх роль у процесі безпеки. Розгляд методів реагування на виявлені загрози та інциденти. Планування та впровадження систем моніторингу в організації	лекція, лаб, самостійна робота		6 6 16	3 тижні
				32/32/86	