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

Венгерський П.С.

Силабус з навчальної дисципліни

"Тестування на проникнення",

що викладається в межах ОПП Кібербезпека

першого (бакалаврського) рівня вищої освіти для здобувачів

зі спеціальності 125 – Кібербезпека та захист інформації

Львів - 2023

Назва дисципліни	Тестування на проникнення
Адреса викладання дисципліни	м. Львів, вул. Університетська 1
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	Костяк Марина Юріївна, к.т.н., доцент кафедри кібербезпеки Беляєв Ігор ,асистент каф.кібербезпеки
Контактна інформація викладачів	Maryna.Kostiak@lnu.edu.ua Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (а також за розкладом консультацій кафедри).
Сторінка курсу	https://ami.lnu.edu.ua/course/pentest
Інформація про дисципліну	Дисципліна "Тестування на проникнення" є нормативною дисципліною зі спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 3-му семестрі в обсязі 4 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про методи проведення тестування на проникнення, отримання практичних навичок у вивченні різних видів атак на веб-додатки, вивчення технік з обходу фільтрації та інших видів захисту та рекомендації щодо поліпшення рівня безпеки.
Мета та цілі дисципліни	Метою курсу нормативної дисципліни є формування у студентів теоретичної та практичної бази знань з тестування на проникнення шляхом отримання практичних навичок через спеціальні загально доступні платформи із завданнями, які дозволяють вивчити типові атаки на веб-додатки.
Література для вивчення дисципліни	*Основна* 1. Cybersecurity Fundamentals/ ISACA/ http://www.isaca.org.ua/ Cybersecurity Funamentals Study Guide/ 2021.- 156 p. 2. Mamilla, Sushmitha Reddy. A Study of Penetration Testing Processes and Tools. 2021. https://scholarworks.lib.csusb.edu/etd/1220 3. How to Protect Against SQL Injection Attacks [Електронний ресурс] // UC Berkeley. – 2019. – Режим доступу до ресурсу: https://security.berkeley.edu/education-awareness/how-protect-against-sql-injection-attacks 4. Choudhary A. SQL Injection Attacks: Know How to Prevent Them [Електронний ресурс] / Archana Choudhary // Security Zone. – 2019. –

	Режим доступу до ресурсу: https://dzone.com/articles/sql-injection-attacks-know-how-to-%20prevent-them 5. Cross Site Scripting (XSS) Attack Tutorial With Examples, Types & Prevention [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/ 6. Державна служба спеціального зв'язку та захисту інформації України./ www.dsszzi.gov.ua *Додаткова* 7. 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/ . 8. Ganore P. What Is A Web Server And How Does It Function? [Електронний ресурс] / Pravin Ganore. – 2017. – Режим доступу до ресурсу: https://www.milesweb.com/blog/hosting/web-server-function/. 9. How a Web server functions? [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.eukhost.com/blog/webhosting/how-a-web-server- functions/. 10. Common Vulnerability Scoring System Calculator Version 3/ https://nvd.nist.gov/vuln-%20metrics/cvss/v3-calculator 11. Brewer J. Web Server Vulnerabilities and a Defense in Depth Strategy Using the Squid Proxy [Електронний ресурс] / Jim Brewer // GSEC Practical version 1.4b. – 2004. – Режим доступу до ресурсу: https://www.giac.org/paper/gsec/3729/web-server-vulnerabilities-defense-in-depth-strategy-squid-proxy/105970 12. Melnick J. Top 10 Most Common Types of Cyber Attacks [Електронний ресурс] / Jeff Melnick. – 2018. – Режим доступу до ресурсу: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ 13. Top 8 Network Attacks by Type in 2017 [Електронний ресурс] // CALYPTIX. – 2017 14. How to Prevent SQL Injection Attacks [Електронний ресурс] // eSecurityPlanet. – 2018. – Режим доступу до ресурсу: https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks/ 15. Singh S. 5 Practical Scenarios for XSS Attacks [Електронний ресурс] / Satyam Singh // Pentest Tools. – 2018. – Режим доступу до ресурсу: https://www.advantio.com/penetration-testing 16. Cross-site Scripting (XSS) [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://owasp.org/www-community/attacks/xss/ .
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 48 год., з них 16 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 72 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **<u>знати:</u>** – типові загрози, атаки та області їх розповсюдження; – проблеми захисту даних;

	– найрозповсюдженіші види атак; – експлуатація баз даних через ін'єкції; – поняття ідентифікації, методів аутентифікації, авторизації; – основні проблеми у фільтрації даних, які ввів користувач; – технології щодо поліпшення безпеки у веб-додатках; – інструмент Burp Suite для перехвату трафіку **вміти:** – ідентифікувати можливі загрози чи атаки; – використовувати утиліту Burp Suite для перехвату трафіку – обробляти відправлені дані на сервер через утиліту Burp Suite – обходити фільтрацію введених даних на веб-сервері – навчитися експлотувати типові вразливості як XSS, SQL ін'єкція – відрізняти та розуміти який метод шифрування найкраще підійде для використання в певних умовах; – знаходити місконфігурації у заголовках реквестів до сервера – застосовувати знання з кібербезпеки в практичній діяльності; – написання рекомендацій щодо захисту веб-додатку при здійсненні професійної діяльності; – розробляти моделі загроз інформації та моделі порушників інформаційної безпеки; **Курс забезпечує набуття таких компетентностей:** ІК, КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КФ-1, КФ-2, КФ-3, КФ-5, КФ-6, КФ-8, КФ-10, КФ-12; **та програмних результатів навчання:** ПРН-1, ПРН-2, ПРН-3, ПРН-4, ПРН-6, ПРН-7, ПРН-10, ПРН-14 ПРН-15, ПРН-21, ПРН-23, ПРН-26, ПРН-28, ПРН-29, ПРН-46, ПРН-48.
Ключові слова	Кібербезпека, кібератака, загроза, вразливість, конфіденційність, цілісність, KaliLinux, OWASP top 10, Burp Suite, ін'єкції, тестування на проникнення, авторизація, аутентифікація, контроль доступу.
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.

Підсумковий контроль, форма	Екзамен у кінці 3 семестру
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції
Необхідне обладнання	Комп'ютер, чи ноутбук з можливістю віртуалізації; Програмне забезпечення віртуалізації: VirtualBox, або VMware; Операційні системи: Windows, Ubuntu, Kali Linux; Програмне забезпечення NMap, 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 оцінки; максимальна кількість балів 50

навчальної діяльності)	• екзамен: 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 незарахуванння 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 екзамену	1. Що таке тестування на проникнення? 2. Види тестувань на проникнення. 3. Основні середовища застосування. 4. Віртуальна машина Virtual Box. 5. Операційна система Kali Linux. 6. Основні тести на проникнення. 7. OWASP TOP 10. 8. Назвати найрозповсюдженіші види атак. 9. Основні види XSS атак. 10. Як перевірити наявність ін'єкції? 11. Вразливості в аутентифікації. 12. Типи вразливостей контролю доступу. 13. Чим можна перехопити трафік між користувачем та сервером? 14. DoS, DDos та SEO. Визначення типу атаки. 15. Види SQL-ін'єкцій. 16. Захист від SQL-ін'єкцій. 17. Як можна обійти фільтрацію на сервері? 18. Загрози для мобільних пристроїв. 19. Принципи безпечної роботи з мобільними пристроями. 20. Надійна аутентифікація. Поширення особистої інформації. 21. Типи веб-фаєрволів. 22. Визначення відповіді програми сканування. 23. Виявлення місконфігурацій у заголовках веб-запитів. 24. Виявлення шкідливого програмного забезпечення. 25. Найкращі практики безпеки. Безпека електронних фінансів

	26. XXE. 27. Ланцюг викрадання сеансових даних користувача. Методи захисту. 28. Що використовується для створення сеансу користувача. 29. Назвати етапи проведення тестування на проникнення. 30. Види обходу завантаження шкідливого файлу. 31. Оформлення звітів на тестування на проникнення.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано після завершенню курсу.

Схема курсу
Лекційні заняття

Теми	Назва теми та короткий зміст	год.
Модуль 1	**Змістовий модуль 1. Види тестування на проникнення**	
Тема 1	**Тема 1. Безпека ІТ та тестування на проникнення** Що таке тестування на проникнення? Чому потрібне тестування на проникнення? Коли виконувати тестування на проникнення? Основні обмеження тестування на проникнення. ***Література: 1, 2, 4, 22.***	1
Тема 2	**Тема 2. Види тестування на проникнення** Тестування на проникнення – "чорний ящик". Тестування на проникнення – "білий ящик". Тестування на проникнення – "сірий ящик". Області тестування на проникнення. ***Література: 1, 2, 3, 22.***	1
Тема 3	**Тема 3. Класифікація та цілі проникнення** Стартові точки та канали доступу для тестів на проникнення. Цілі проникнення. Межі тестування на проникнення. Класифікація. ***Література: 1, 2, 5, 22.***	1
Тема 4	**Тема 4. Юридичні питання тестування на проникнення** Юридичні причини тестування на проникнення. Правові рамки тестування на проникнення. Важливі умови договору між тестером на проникнення та клієнтом. Обов'язки тестера. Обмеження відповідальності. ***Література: 1, 3, 10, 22.***	1
Тема 5	**Тема 5. Загальні вимоги до тестування на проникнення** Організаційні вимоги. Вимоги до персоналу. Технічні вимоги. Етичні питання. ***Література: 1, 2, 6, 22.***	1
Тема 6	**Тема 6. Методика тестування на проникнення** Вимоги до методики випробування на проникнення. П'ять фаз тесту на проникнення. Модулі для процедур тестування. Принцип виключення. ***Література: 1, 4, 9, 22.***	2
Модуль 2	**Змістовий модуль 2. Етапи тестування на проникнення**	
Тема 7	**Тема 7. Виконання тестів на проникнення** Підготовка тесту. Розвідка. Аналіз інформації та ризиків. Активні спроби вторгнення. Остаточний аналіз. ***Література: 1, 3, 11, 10, 22.***	1

Тема 8	**Тема 8. Тестування на проникнення інфраструктури** Види тестування на проникнення інфраструктури. Тестування зовнішньої інфраструктури. Тестування на проникнення внутрішньої інфраструктури. Кваліфікація тестерів на проникнення. Роль тестера на проникнення. ***Література: 1, 2, 13, 22.***	2
Тема 9	**Тема 9. Написання звітів** Етапи написання звітів. Планування звіту. Зміст звіту про тестування на проникнення. ***Література: 5, 8, 14, 22.***	1
Тема 10	**Тема 10. Збір інформації** Класифікація типів інформації. Класифікація методів збору. Перегляд фінансових послуг. ***Література: 4, 6, 13, 22.***	1
Тема 11	**Тема 11 Сканування портів** Утиліти сканування. Використання AngryIP. Виконання сканування портів. Повне сканування портів. Стелс-сканування або напіввідкрите сканування. Xmas дерево сканування. FIN Сканування. Сканування NuLL. ACK сканування. ***Література: 1, 14, 15, 22.***	2
Тема 12	**Тема 12 Сканування вразливостей** Вступ до сканування вразливостей. Сканери уразливості. Визнання обмежень сканування вразливостей. Визначення процесу сканування вразливостей. Оцінка нової системи. Типи сканувань, які можна виконувати. Аутентифіковане сканування. ***Література: 1, 2, 8, 12, 22.***	2

Лабораторні роботи

№	Назва лабораторної роботи	Год.
1.	Налаштування середовища для тестування.	2
2.	Встановлення віртуальної машини Virtual Box.	2
3.	Інсталяція операційної системи Kali Linux.	2
4.	Тестування на проникнення утилітою John The Ripper.	2
5.	Тестування на проникнення утилітою Aircrack-ng	2
6.	Тестування на проникнення утилітою THC Hydra	2
7.	Тестування на проникнення утилітою Burp Suite	2
8.	Тестування на проникнення утилітою WireShark	2
9.	Тестування на проникнення утилітою OWASP Zed	2

10.	Тестування на проникнення утилітою Maltego	2
11.	Тестування на проникнення утилітою Metasploi	2
12.	Тестування на проникнення утилітою Nmap	2
13.	Тестування на проникнення утилітою Nikto Website Vulnerability Scanner	2
14.	Тестування на проникнення утилітою Social-Engineer Toolkit	2
15.	Тестування на проникнення утилітою Hashcat	2
16.	Підготовка і написання звіту та висновків про тестування.	2