МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«30» _____ 2024 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«__» _____ 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни

«ТЕСТУВАННЯ НА ПРОНИКНЕННЯ»

ступінь вищої освіти - **бакалавр**
галузь знань - **12 - «Інформаційні технології»**
спеціальність – **125 - «Кібербезпека»**
освітньо-професійна програма – **«Кібербезпека»**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. роботи (год.)	ІРС (год.)	Тренінг (год)	СРС (год.)	Разом (год.)	Екзамен (сем)
ДНФ	4	7	40	52	6	14	68	180	7

Тернопіль – 2024

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 - «Інформаційні технології» за спеціальністю 125 - «Кібербезпека», затвердженої Вченою радою ЗУНУ протокол №9 від 26.05.2021 р.).

Робочу програму склали: д.т.н., професор, завідувач кафедри кібербезпеки Василь Яцків, викладач кафедри кібербезпеки Сергій Возняк

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2024 р.

Завідувач кафедри кібербезпеки Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності 125 «Кібербезпека та захист інформації», протокол №1 від 30.08.2024 р.

Голова групи
забезпечення спеціальності Василь ЯЦКІВ

Гарант ОП Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. **Опис дисципліни “Тестування на проникнення”**

Дисципліна - Тестування на проникнення ”	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 6	галузь знань – 12 Інформаційні технології	Статус дисципліни - обов’язкова Мова навчання - українська
Кількість залікових модулів – 5	спеціальність – 125 Кібербезпека	Рік підготовки: 4 Семестр: 7
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції: 46 год. Лабораторні заняття: 60 год.
Загальна кількість годин – 180 год.		Самостійна робота: 60 год. Тренінг 8 год. Індивідуальна робота: 6 год.
Тижневих годин – 12, з них аудиторних – 7		Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни «Тестування на проникнення»

2.1. Мета вивчення дисципліни.

Метою дисципліни «Тестування на проникнення» є - отримання знань та умінь, які необхідні для проведення тестування комп’ютерних систем на проникнення.

2.2. Завдання вивчення дисципліни

Основне завдання дисципліни дати студентам теоретичну та практичну підготовку з виконання тестів на проникнення.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни.

Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
Здатність до пошуку, оброблення та аналізу інформації.
Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
Здатність здійснювати тести на проникнення в комп’ютерні системи та мережі шляхом виявлення та експлуатації наявних вразливостей.

2.4. Передумови для вивчення дисципліни.

Перелік дисциплін, які мають бути вивчені раніше: програмування для наукових досліджень; дослідження і проектування систем захисту інформації; моніторинг мережевої безпеки.
Перелік раніше здобутих результатів навчання: використовувати технології програмування у професійних дослідженнях; науково обґрунтовувати та структурувати отримані наукові положення; Володіти сучасними технологіями програмування для організації наукових досліджень, обробки експериментальних даних та представлення результатів досліджень; Здійснювати систематичний збір і обробку інформації, яка може бути використана для підвищення захищеності мережі, процесу ухвалення рішення, оцінки програм або вироблення політики безпеки.

2.5. Результати навчання.

Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах.
Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно телекомунікаційних систем.
Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно телекомунікаційних системах.
Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно телекомунікаційних системах
Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно телекомунікаційних системах.
Використовувати інструментарій для моніторингу процесів в інформаційно телекомунікаційних системах.

2.6 Завдання лекційних занять

Проведення лекційних занять забезпечує отримання студентами теоретичної підготовки, знання основних видів тестування на проникнення, етапів огранізації pentesting у відповідності з програмою та робочим планом та формуванні у студентів цілісної системи теоретичних знань з курсу «Тестування на проникнення».

2.7 Завдання проведення практичних занять

Проведення практичних занять забезпечує формування у студентів практичних навичок, які необхідні для проведення тестування комп’ютерних систем на проникнення.

3. Програма навчальної дисципліни: «Тестування на проникнення»

Змістовий модуль 1. Види тестування на проникнення

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.

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.

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.

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.

Тема 5. Загальні вимоги до тестування на проникнення

Організаційні вимоги. Вимоги до персоналу. Технічні вимоги. Етичні питання.
Література: 1, 2, 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.

Змістовий модуль 2. Етапи тестування на проникнення

Тема 7. Виконання тестів на проникнення

Підготовка. Розвідка. Аналіз інформації / ризики. Активні спроби вторгнення. Остаточний аналіз.
Література: 1, 3, 9, 10.

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, 7.

Тема 9. Написання звітів

Етапи написання звітів. Планування звіту. Зміст звіту про тестування на проникнення.
Література: 1, 8, 10.

Тема 10. Збір інформації.

Класифікація типів інформації. Класифікація методів збору. Перегляд фінансових послуг.
Література: 1, 6.

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

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.

4. Структура залікового кредиту з дисципліни

	Кількість годин					
	Лекції	Лабор. заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Види тестування на проникнення						
Тема 1. Безпека ІТ та тестування на проникнення	2	2	4	3	7	Поточне опитування
Тема 2. Види тестування на проникнення	2	2	4			
Тема 3. Класифікація та цілі проникнення	2	4	4			
Тема 4. Юридичні питання тестування на проникнення	2	4	5			
Тема 5. Загальні вимоги до тестування на проникнення	4	4	5			
Тема 6. Методика тестування на проникнення	4	4	5			
Змістовий модуль 2 Етапи тестування на проникнення						
Тема 7. Виконання тестів на проникнення	4	6	5	3	7	Поточне опитування
Тема 8. Тестування на проникнення інфраструктури	4	4	6			
Тема 9. Написання звітів	4	4	6			
Тема 10. Збір інформації	4	6	8			
Тема 11. Сканування портів	4	6	8			
Тема 12. Сканування вразливостей	4	6	8			
Разом	**40**	**52**	**68**	**6**	**14**	

5. Тематика лабораторних занять

Лабораторна робота №1

Тема: Роботи з Metasploit Framework

Мета: навчитися проводити тести на проникнення з використанням середовища Metasploit Framework

Питання для обговорення:

1. Основи Metasploit Framework;
2. msfcli; msfweb; msfconsole; exploits;
3. Корисні навантаження (Payloads);
4. Meterpreter.

Література: 2, 5.

Лабораторна робота №2

Тема: Збір інформації

Мета: вивчити засоби збору інформації Metasploit Framework

Питання для обговорення:

1. Рада Dradis
2. Конфігурація бази даних

3. Сканування портів.
4. Допоміжні плагіни.
5. Служби ідентифікації.

Література: 2, 5.

Лабораторна робота №3

Тема: Аналіз вразливості.

Мета: навчитися проводити аналіз вразливостей.

Питання для обговорення:

1. SMB перевірка входу.
2. Аутентифікація VNC.
3. Протокол X11. Веб-сканер WMAP.
4. Робота з NeXposeo. Робота з Nessus.
5. Використання бази даних MSF.

Література: 2, 5.

Лабораторна робота №4

Тема:. Експлуатація вразливості

Мета: вивчити принципи експлуатації вразливостей.

Питання для обговорення:

1. Дизайн експлуатації
2. Експлуатація цілі. Корисне навантаження
3. Буквено-цифрові оболонки.
4. Експлуатація портів.

Література: 2, 5.

Лабораторна робота №5

Тема: Експлуатація на стороні клієнта.

Мета: вивчити принципи експлуатації вразливості на стороні клієнта.

Питання для обговорення:

1. Бінарні корисні навантаження
2. Обхід антивірусу
3. Бінарні трояни для Linux
4. Інфекція Java-аплет
5. Атаки з боку клієнта
6. Методи зараження VBScript

Література: 2, 5.

Лабораторна робота №6

Тема:. Експлуатації після зламу.

Мета: вивчити принципи експлуатації вразливості з використанням Metasploit.

Питання для обговорення:

1. Експлуатація привілеїв за допомогою Metasploit
2. PSexec передача хешу
3. Управління журналом подій. Взаємодія з реєстром
4. Віддалена активація робочого столу
5. Пакети meterpreter

Література: 2, 5.

6. Самостійна робота

Самостійна робота з курсу «Тестування на проникнення» виконується самостійно студентом на основі одного сформованого завдання, що охоплює основні теми курсу. Метою виконання самостійної роботи є дослідження та оволодіння навиками тестування на проникнення.

Орієнтовна тематика рефератів:

1. Архітектура безпеки OSI
2. Напади на безпеку, послуги та механізми
3. Елементарні команди Linux
4. ОС Kali Linux. Установка Kali Linux
5. Встановлення Metasploitable
6. Налаштування мережі для тестування на проникнення
7. Створення та запуск веб-сервер
8. Збір інформації
9. Тестування на проникнення бездротових мереж
10. Стрес-тести мережі
11. Аналіз вразливостей в веб-додатках
12. Аналіз вразливостей в операційних системах і серверному програмному забезпеченні
13. Сканування вразливостей з OpenVAS 8.0
14. Інструкція по Armitage: автоматичний пошук і перевірка експлойтів в Kali Linux
15. Аудит безпеки Linux
16. Сканування мереж. Перехоплення даних в мережах
17. Атаки на паролі.

7. Організація та проведення тренінгу з дисципліни «Тестування на проникнення»

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання вибраного завдання тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Тематика тренінгу: Налаштування інфраструктури, виявлення сервісів і аналіз вразливостей на досліджуваній машині.

Завдання для тренінгу:

№ п/п	**Вид роботи**	**Порядок проведення тренінгу**
1	Налаштувати інфраструктуру для виконання завдання.	Для виконання завдання необхідні: 1. Засіб віртуалізації - VirtualBox; 2. Образ віртуальної машини для дослідження - Metasploitable2; 3. Образ віртуальної машини атакуючого – Kali Linux.
2	Визначити доступні сервіси на досліджуваній машині.	Для визначення запущених на досліджуваній машині мережевих сервісів з машини «атакуючого» необхідно провести сканування за допомогою утиліти nmap.
3	Визначити наявні вразливості в запущених сервісах	Провести сканування використовуючи сканер вразливості

8. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни “ Тестування на проникнення ” використовуються наступні методи оцінювання навчальної роботи студента:

– поточне опитування;
– підсумковий модульний контроль за кожним змістовним модулем;
– оцінювання виконання лабораторних робіт;
– оцінювання тренінгів;
– оцінювання результатів самостійної роботи;
– підсумковий письмовий екзамен.

9. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни “Тестування на проникнення” визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Семестр 7 – іспит

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-3.	Підсумкова письмова робота за темами №1-6.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №4-6.	Підсумкова письмова робота за темами №7-12.	Визначається як середнє арифметичне з оцінок за виконання двох вибраних завдань тренінгу.	Визначається як середнє арифметичне за завдання самостійної роботи.	1. Теорети-чні питан-ня: 2 пита-ння по 30 балів - max 60 балів. 2. Практич-не завдання - max 40 балів

Шкала оцінювання:

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов’язковим повторним курсом)

10. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	**Найменування**	**Номер теми**
1.	Мультимедійний проектор	1 - 12
2.	Комп’ютерна лабораторія. Доступ до Інтернету.	1 - 12
3.	Програмне забезпечення: Oracle VM VirtualBox, OpenSSH, OpenVAS, Nessus, Aircrack-NG, Nmap, Metasploit, Wireshark, VM VirtualBox, образи віртуальних машин з заданими вразливостями.	

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Mamilla, Sushmitha Reddy. A Study of Penetration Testing Processes and Tools. 2021. https://scholarworks.lib.csusb.edu/etd/1220
2. BSI - Study A Penetration Testing Model. Federal Office for Information Security, 111p. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ Publications/Studies/Penetration/penetration_pdf.html.
3. Vulnerability Scanning Tools. https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
4. PTES Technical Guidelines. http://www.pentest-standard.org/index.php/Exploitation
5. Johari, Rahul, et al. Penetration Testing in IoT Network. In: 2020 5th International *Conference on Computing, Communication and Security (ICCCS)*. IEEE, 2020, pp. 1-7.
6. ASAAD, Renas R. Penetration testing: Wireless network attacks method on Kali Linux OS. *Academic Journal of Nawroz University*, 2021, 10.1, pp.7-12
7. Yaacoub, Jean-Paul A., et al. A Survey on Ethical Hacking: Issues and Challenges. arXiv preprint arXiv:2103.15072, 2021.
8. Alanda, Alde, et al. Web Application Penetration Testing Using SQL Injection Attack. *JOIV: International Journal on Informatics Visualization*, 2021, 5.3, pp. 320-326
9. Akhilesh, R.; Bills, O.; Chilamkurti, N.; Chowdhury, M.J.M. Automated Penetration Testing Framework for Smart-Home-Based IoT Devices. Future Internet 2022, 14, 276. https://doi.org/10.3390/fi14100276
10. High Level Organization of the Standard. http://www.pentest-standard.org/index.php/Exploitation