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

ЗАТВЕРДЖУЮ

Декана ФКІТ
Ігор ЯКИМЕНКО

«30» 08 2024 р.

ЗАТВЕРДЖУЮ

Проректор з науково-
педагогічної роботи
Віктор ОСТРОВЕРХОВ

«30» 08 2024 р.

ЗАТВЕРДЖУЮ
Директор ННІНОТ
Святослав ПИТЕЛЬ

30 08 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни «Тестування комп'ютерних систем на проникнення»
ступінь вищої освіти – магістр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (семін.) (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ. (год.)	Разом (год.)	Екз. (сем.)
Денна	1	1	30	14	4	6	96	150	1
Заочна	1	1,2	8	4	-	-	138	150	2

30-08-2024р.

Тернопіль – 2024

Робоча програма розроблена на основі освітньо-професійної програми підготовки магістра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпеки та захист інформації», затвердженої Вченою радою ЗУНУ (протокол №11 від 26.06.2024 р.).

Робочу програму склав завідувач кафедри кібербезпеки, д.т.н., професор Яцків Василь Васильович

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

Завідувач кафедри 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 освітньо-професійної
програми Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Тестування комп'ютерних систем на проникнення»

Дисципліна «Тестування комп'ютерних систем на проникнення»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS – 5	Галузь знань – 12 Інформаційні технології	**Статус дисципліни** - обов'язкова **Мова навчання** – українська
Кількість залікових модулів – 4	Спеціальність – 125 «Кібербезпека та захист інформації»	Рік підготовки: *Денна – 1* *Заочна – 1* Семестр: *Денна – 1* *Заочна – 1, 2*
Кількість змістових модулів – 2	Ступінь вищої освіти – магістр	Лекції (год.): *Денна – 30* *Заочна – 8* Практичні заняття (год.): *Денна – 14* *Заочна – 4*
Загальна кількість годин – 150		Самостійна робота (год.): *Денна – 96* *Заочна – 138* Тренінг (год.): *денна – 6* Індивідуальна робота (год.): *Денна – 4*
Тижневих годин – 10 з них аудиторних – 3		Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни «Тестування комп'ютерних систем на проникнення»

2.1. Мета вивчення дисципліни.

Метою дисципліни «Тестування комп'ютерних систем 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.

Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Здатність оцінювати та забезпечувати якість виконуваних робіт.

Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та

ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

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.

Розв’язувати складні науково-технічні та прикладні завдання та проблеми з інформаційної безпеки та/або кібербезпеки, що потребують оновлення та інтеграції фундаментальних знань, у тому числі в умовах неповної інформації та суперечливих вимог

Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міжпредметному рівні, зокрема з використанням інженерно-технічних і математичних наук, а також напрямів технологій створення та використання спеціалізованого програмного забезпечення.

Критично оцінювати захищеність систем, комплексів та засобів кіберзахисту, технологій створення та використання спеціалізованого програмного забезпечення, зокрема з використанням сучасних програмних та програмно-апаратних рішень та сучасних підходів.

Досліджувати та проводити системний аналіз забезпечення безперервності бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, проводити аналіз ризиків та визначати оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розуміти основні аспекти впровадження та супроводження проектів з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

Використовувати методи натурного, фізичного і комп’ютерного моделювання з метою детального вивчення і дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

3. Програма навчальної дисципліни: «Тестування комп’ютерних систем на проникнення»

Змістовий модуль 1. Види тестування на проникнення

Тема 1. Види тестування на проникнення

Що таке тестування на проникнення? Чому потрібне тестування на проникнення? Коли виконувати тестування на проникнення? Основні обмеження 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, 4.

Тема 2. Загальні вимоги до тестування на проникнення

Організаційні вимоги. Вимоги до персоналу. Технічні вимоги. Етичні питання.

Література: 1, 2, 6.

Тема 3. 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 4. Збір інформації.

Класифікація типів інформації. Класифікація методів збору. Перегляд фінансових послуг. Розуміння понять Footprinting. Пошук через пошукові системи та передові методи злому Google. Відбиток через веб-сервіси та сайти соціальних мереж. Розуміння відбитків веб-сайтів, відбитків електронної пошти та конкурентної розвідки. Розуміння Whois, DNS і відбитків мережі. Відбиток за допомогою соціальної інженерії. Різні інструменти відбитків і контрзаходів.

Література: 1, 2, 3.

Тема 5. Сканування мережі

Концепція мережевого сканування. Різні інструменти сканування. Різні техніки сканування. Розуміння захоплення банерів. Створення мережевих схем за допомогою засобів виявлення мережі. Сканування мережі як частини тестування на проникнення.

Література: 1, 12

Тема 6. Тунелювання та обхід брандмауера

Тунелювання DNS. Тунелювання ICMP. Тунелювання HTTP/HTTPS. Розуміння тунелювання SSH. Методи ухилення від брандмауера та IDS.

Література: 1, 12

Тема 7. Перерахування

Розуміння понять перерахування. Різні методи перерахування NetBIOS. Методи нумерації SNMP. Методів нумерації LDAP. Методи перерахування NTP. Методи перерахування SMTP і DNS. Методи нумерації, такі як нумерація IPsec, VoIP, RPC і Linux/Unix. Контрзаходи перерахування.

Література: 1, 2, 6.

Тема 8. Сканування та оцінка вразливості

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, 6.

Змістовий модуль 2. Атаки на протоколи та програми

Тема 9. Атаки на паролі

Методи отримання доступу до системи. Техніки злому паролів. Особливості і недоліки автентифікації Windows.

Література: 1, 6, 11.

Тема 10. Сніффінг.

Аналіз пакетів. Різні техніками нюхання. Атаки спуфінгу як засобу для перехоплення. Методів отруєння DNS. Підходи до захисту від обнюхування. Володіння різними інструментами нюхання.

Література: 1, 2, 6.

Тема 11. Робота з Metasploit

Огляд архітектури Metasploit. Основні команд Metasploit. Огляд збору інформації за допомогою Metasploit. Огляд експлуатації на стороні сервера за допомогою Metasploit.

Література: 1, 4, 9.

Тема 12. Підвищення привілеїв

Концепція ескалації привілеїв. Ескалації привілеїв за допомогою динамічних бібліотек (dll або dylib). Вразливості Meltdown і Spectre і способів їх використання. Методи підвищення привілеїв. Знання цінних Інтернет-ресурсів. Огляд контрзаходів для підвищення привілеїв.

Література: 1, 2, 5.

Тема 13. Атаки на рівні програми

Атаки на MS Word. PDF атаки. Атаки CHM. Атаки PowerShell.

Література: 1, 2, 8, 12.

Тема 14. Бездротові загрози

Огляд бездротових концепцій. Алгоритми бездротового шифрування. Розуміння бездротових загроз. Методології бездротового злому.

Література: 1, 4, 9.

Тема 15. Написання звітів

Етапи написання звітів. Планування звіту. Зміст звіту про тестування на проникнення.

Література: 1, 8, 10.

4.1 Структура залікового кредиту
з дисципліни "Тестування комп'ютерних систем на проникнення"
(денна форма навчання)

	Кількість годин					
	Лекції	Прак-тичні заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. ***Види тестування на проникнення***						
Тема 1. Види тестування на проникнення	2		2	2	3	Поточне опитування
Тема 2. Загальні вимоги до тестування на проникнення	2		2			
Тема 3 Юридичні питання тестування на проникнення	2		4			
Тема 4. Збір інформації	2	2	8			
Тема 5. Сканування мережі	2	2	4			
Тема 6. Тунелювання та обхід брандмауера	2	1	4			
Тема 7. Перерахування	2	1	4			
Тема 8. Сканування та оцінка вразливості	2	1	4			
Змістовий модуль 2. ***Атаки на протоколи та програми***						
Тема 9. Атаки на паролі	2	1	4	2	3	Поточне опитування
Тема 10. Сніффінг	2	1	10			
Тема 11. Робота з Metasploit	2	1	10			
Тема 12. Підвищення привілеїв	2	1	8			
Тема 13. Атаки на рівні програми	2	1	12			
Тема 14. Бездротові загрози	2	1	8			
Тема 15. Написання звітів	2	1	12			
Разом	**30**	**14**	**96**	**4**	**6**	

4.2 Структура залікового кредиту
з дисципліни «Тестування комп'ютерних систем на проникнення»
(заочна форма навчання)

	Кількість годин		
	Лекції	Практичні заняття	Самостійна робота
Змістовий модуль 1. ***Види тестування на проникнення***			
Тема 1. Види тестування на проникнення	2	2	8
Тема 2. Загальні вимоги до тестування на проникнення			8
Тема 3 Юридичні питання тестування на проникнення			8
Тема 4. Збір інформації			8
Тема 5. Сканування мережі	2		8
Тема 6. Тунелювання та обхід брандмауера			10
Тема 7. Перерахування			10
Тема 8. Сканування та оцінка вразливості			10
Змістовий модуль 2. ***Атаки на протоколи та програми***			
Тема 9. Атаки на паролі	2	2	10
Тема 10. Сніффінг			10
Тема 11. Робота з Metasploit			10
Тема 12. Підвищення привілеїв	2		10
Тема 13. Атаки на рівні програми			10
Тема 14. Бездротові загрози			10
Тема 15. Написання звітів			8
Разом	**8**	**4**	**138**

5. Тематика практичних (семінарських або лабораторних) занять
Лабораторна робота №1

Тема: Підготовка тестового оточення. Встановлення майданчика з уразливостями DAMN VULNERABLE WEB APPLICATION

Мета: встановити на локальній машині майданчик з уразливими, робота з якими буде проведена в наступних роботах

Завдання:

- закріплення навичок роботи в Linux-подібних системах;
- отримання навичок установки і настройки веб-сервера для установки на нього уразливого веб-додатки.
- провести порівняльний аналіз використовуваної майданчики DVWA з іншими майданчиками [1-3], які використовуються для отримання навичок в пошуку і експлуатації вразливостей;
- проаналізувати подібні системи, що використовують інші технології (ASP.NET, Java).

Література: 2, 5, 13.

Лабораторна робота №2

Тема: Аналіз трафіку комп'ютерних мереж і сценарії атаки типу MITM

Мета: отримання навичок роботи з аналізатором трафіку Wireshark і платформою Burpsuite, знайомство з атакою Man-in-the-Middle.

Завдання:

- знайомство зі структурою мережевих пакетів;
- отримання навичок роботи в сніффером на прикладі Wireshark і Burpsuite.

- провести аналіз сценаріїв MitM-атак на веб-додаток;
- розробити методи захисту веб-додатків від даного виду атак.

Література: 2, 5, 14.

Лабораторна робота №3

Тема: Пошук і експлуатація SQL-ін'єкцій

Мета: ознайомитися з атакою, пов’язаною з порушенням логіки запитів до бази даних, отримати навички роботи з інструментальним засобом для пошуку і експлуатації ін’єкцій.

Завдання:

- освоєння природи походження і принципів експлуатації уразливості в браузері;
- отримання навичок використання утиліти sqlmap для експлуатації SQL-ін’єкцій.
- провести порівняльний аналіз методів ін'єкцій при різної складності експлуатації вразливостей в DVWA;

1. - обґрунтувати, чому проекти, написані на PHP, частіше [4] схильні до проведення SQL-ін'єкцій.

Література: 2, 5, 12.

Лабораторна робота №4

Тема:. Робота з XSS-атаками

Мета: знайомство зі сценаріями здійснення атак і застосовуваними інструментами.

Завдання:

- освоєння природи походження і принципів експлуатації уразливості в браузері;
- отримання навичок використання утиліти xsser для пошуку вразливостей.
- визначити можливості XSS-атак;
- розробити заходи щодо захисту веб-додатки від XSS-атак

Література: 2, 5, 12.

Лабораторна робота №5

Тема: Робота з шеллом в METASPLOIT.

Мета: отримання навичок роботи в фреймворку на прикладі модуля управління шеллом.

Завдання:

- отримання навичок використання модулів фреймворка Metasploit;
- отримання навичок управління атакований сервером.
- визначити можливі наслідки експлуатації шеллів;
- розробити заходи щодо захисту веб-додатки від завантаження шелл.

Література: 2, 5, 13.

Лабораторна робота №6

Тема:. Сканування IP-мереж

Мета: ознайомитися з призначенням і функціоналом утиліти nmap в ОС Kali Linux, ознайомитися з основними відкритими базами даних вразливостей.

Завдання:

- отримання навичок використання утиліти nmap;
- отримання навичок пошуку інформації у відкритих базах вразливостей.
- запропонувати методи і засоби виявлення сканування;
- розробити заходи щодо захисту мережі від сканування.

Література: 2, 5, 14.

Лабораторна робота №7

Тема: Забезпечення безпеки багатокомпонентних WEB-додатків.

Мета: проаналізувати можливі проблеми безпеки Web-додатки на етапі проектування.

Завдання:

- виявити можливі проблеми безпеки Web-додатки, грунтуючись на його функціональності;
- скласти список вимог, які повинні бути перевірені перед здачею проекту замовнику.
- запропонувати методи і засоби захисту від поширених атак;
- проаналізувати, які методи використовує Web Application Firewall (WAF) [26] для виявлення потенційно небезпечного трафіку.

6. Самостійна робота

Для самостійної роботи кожному студенту пропонується виконання наскрізного проєкту **«Виконання тесту на проникнення»**, який складається із шести завдань**:**

1. Вибір цілі (віртуальна машина із заданими вразливостями).
2. Збір інформації та пошук цілей.
3. Пошук вразливостей.
4. Експлуатація та проведення атак.
5. Розширення зони впливу і ескалація привілеїв.
6. Написання звіту.

7. Організація та проведення тренінгу з дисципліни «Тестування комп'ютерних систем на проникнення»

№ 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; 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	Отримати віддалений доступ, шляхом експлуатації вразливостей чотирьох різних сервісів.	Вибрати чотири різних сервісів, які мають вразливості. Запустити Metasploit. Отримати доступ до вибраних сервісів використовуючи знайдені вразливості

8. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; лабораторні роботи, індивідуальні заняття; самостійна робота студентів, робота в Інтернет.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «**Тестування комп'ютерних систем на проникнення**» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

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

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «**Тестування комп'ютерних систем на проникнення**» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Для екзамену

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20 %	20 %	5 %	15 %	40 %
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-7.	Підсумкова письмова робота за темами №1-15.	Визначається як середнє арифметичне з оцінок за виконання трьох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання наскрізного завдання.	1. 15тестів по 4 бали - 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)

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

№	**Найменування**	**Номер теми**
1.	Мультимедійний проектор	1 - 15
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 - 15
3.	Програмне забезпечення: Oracle VM VirtualBox,	

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Опорний конспект лекцій з курсу «Тестування комп'ютерних систем на проникнення» для студентів спеціальності 125 «Кібербезпека» – Тернопіль: ТНЕУ, 2019. – 119 с.
2. Mamilla, Sushmitha Reddy. A Study of Penetration Testing Processes and Tools. 2021. https://scholarworks.lib.csusb.edu/etd/1220
3. 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
4. Najera-Gutierrez, Gilberto, and Juned Ahmed Ansari. *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd, 2018.
5. Vulnerability Scanning Tools. https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
6. PTES Technical Guidelines. http://www.pentest-standard.org/index.php/Exploitation

7. 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.

8. ASAAD, Renas R. Penetration testing: Wireless network attacks method on Kali Linux OS. *Academic Journal of Nawroz University*, 2021, 10.1, pp.7-12

9. Yaacoub, Jean-Paul A., et al. A Survey on Ethical Hacking: Issues and Challenges. arXiv preprint arXiv:2103.15072, 2021.

10. Alanda, Alde, et al. Web Application Penetration Testing Using SQL Injection Attack. *JOIV: International Journal on Informatics Visualization*, 2021, 5.3, pp. 320-326

11. 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