Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Голова НМК
_____ Д. М. Крицький
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Засоби тестування на проникнення (пентестингу, білого хакингу)
(назва навчальної дисципліни)

Галузь знань: 10 «Природничі науки», 11 «Математика та статистика», 12 «Інформаційні технології», 15 «Автоматизація та приладобудування», 16 «Хімічна та біоінженерія», 17 «Електроніка та телекомунікації», 19 «Архітектура та будівництво»
(шифр і найменування галузі знань)

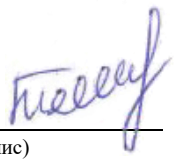
Спеціальність: _____
(код та найменування спеціальності)

Освітня програма: _____
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Харків 2023 рік

Розробник: Тецький А. Г., доцент, к.т.н. 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри
комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » 08 2023 р.

Завідувач кафедри д.т.н., професор  В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни
(денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="12">Галузь знань
10 «Природничі науки»,
11 «Математика та статистика»,
12 «Інформаційні технології»,
15 «Автоматизація та приладобудування»,
16 «Хімічна та біоінженерія»,
17 «Електроніка та телекомунікації»,
19 «Архітектура та будівництво»
(шифр та найменування)

Рівень вищої освіти:
другий (магістерський)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 2</td><td>2023/2024</td></tr>
<tr><td>Індивідуальне завдання: немає</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин: 64/150</td><td>2-й</td></tr>
<tr><td>Лекції*</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи здобувача – 5</td><td>32 години</td></tr>
<tr><td>Практичні, семінарські[1)]</td></tr>
<tr><td>немає</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>32 години</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>86 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: для денної форми навчання – 64/86.

*Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: отримати навички виявлення проблем безпеки компонент розподілених інформаційних систем, ознайомитися з методами атак таких компонент і способами протидії атакам. Оволодіти навичками роботи з набором інструментальних засобів для пошуку й усунення виявлених неполадок розподілених інформаційних систем.

Завдання:

встановлення і налаштування вразливого веб-застосунка, вразливості якого будуть розглядатися в навчальній дисципліні; освоєння способу компрометації даних при використанні незахищеного з'єднання; отримання навичок застосування інструментального засобу для експлуатації SQL-ін'єкції; отримання навичок застосування інструментального засобу для пошуку можливостей проведення XSS-атак; освоєння сценаріїв отримання вмісту бази даних з сервера, на який був завантажений шелл для виконання довільних команд; отримання навички сканування IP-мереж; виконання аналізу проблем безпеки застосунків на етапі проектування.

Компетентності, які набуваються:

– здатність виявляти наукову сутність проблем у професійній сфері, знаходити адекватні шляхи щодо їх розв`язання.

– навички використання інформаційних і комунікаційних технологій.

– здатність до самостійного освоєння нових методів дослідження, зміни науковою й науково-виробничого профілю своєї діяльності.

– здатність досліджувати проблеми з використанням системного аналізу, синтезу, комп`ютерного моделювання та методів оптимізації.

– здатність генерувати нові ідеї (креативність), виявляти, ставити та вирішувати проблеми, знаходити оптимальні шляхи щодо їх вирішення.

– здатність аналізувати верифікувати, оцінювати повноту інформації в ході професійної діяльності за необхідності доповнювати й синтезувати відсутню інформацію й працювати в умовах невизначеності.

– здатність вести професійну, у тому числі науково-дослідну діяльність у міжнародному середовищі.

– здатність оцінювати та забезпечувати якість виконуваних робіт.

Очікувані результати навчання. В результаті вивчення дисципліни здобувачі мають вміти застосовувати підходи та засоби для пошуку й експлуатації проблем кібербезпеки веб-застосунків.

Пререквізити – дисципліна є вибірковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки галузі знань 12 «Інформаційні технології».

Кореквізити – Відсутні.

3. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1 «Огляд сучасних проблем кібербезпеки веб-застосунків»

Тема 1. Підготовка тестового оточення. Встановлення Damn Vulnerable Web Application

Встановлення на локальній машині платформи з вразливостями. Закріплення навичок роботи в Linux-подібних системах. Отримання навичок встановлення і налаштування веб-сервера для подальшого встановлення на нього вразливого застосунка.

Тема 2. Аналіз трафіку комп'ютерних мереж і сценарії атаки типу Man-in-the-Middle

Отримання навичок роботи з аналізатором трафіку Wireshark і платформою Burpsuite, знайомство з атакою Man-in-the-Middle. Знайомство зі структурою мережевих пакетів. Отримання навичок роботи в сніффером на прикладі Wireshark і Burpsuite. Аналіз сценаріїв MitM-атак веб-застосунку. Розробка методів захисту веб-застосунку від даного виду атак.

Тема 3. SQL-ін'єкції. Принципи, пошук і експлуатація SQL-ін'єкцій. Методи ін'єкцій та їх наслідки

Атаки з порушенням логіки запитів до бази даних. Робота з інструментальним засобом для пошуку і експлуатації ін'єкцій. Освоєння природи походження і принципів експлуатації вразливості в браузері. Отримання навичок використання утиліти sqlmap для експлуатації SQL-ін'єкцій. Порівняльний аналіз методів ін'єкцій при різної складності експлуатації вразливостей в DVWA.

Тема 4. Робота з XSS-атаками. Особливості атак та їх наслідки

Сценарії здійснення атак та інструменти атак. Освоєння природи походження і принципів експлуатації вразливості в браузері. Отримання навичок використання утиліти xsser для пошуку вразливостей. Можливості XSS-атак. Розроблення заходів щодо захисту веб-застосунка від XSS-атак.

Модульний контроль

ЗМІСТОВИЙ МОДУЛЬ 2 «Аналіз проблем кібербезпеки мереж та системного програмного забезпечення»

Тема 5. Робота з шеллом в Metasploit. Виконання довільних команд в атакованій системі

Отримання навичок роботи в фреймворку на прикладі модуля управління шеллом. Отримання навичок використання модулів фреймворка Metasploit. Отримання навичок управління атакованим сервером. Можливі наслідки експлуатації шелл. Розроблення заходів щодо захисту веб-застосунка від

завантаження шелл.

Тема 6. Основи сканування IP-мереж

Знайомство з призначенням і функціоналом утиліти nmap в ОС Kali Linux, знайомство з основними відкритими базами даних вразливостей. Отримання навичок використання утиліти nmap. Отримання навичок пошуку інформації у відкритих базах вразливостей. Методи і засоби виявлення сканування. Розроблення заходів щодо захисту мережі від сканування.

Тема 7. Забезпечення безпеки багатокомпонентного веб-застосунка

Аналіз можливих проблем безпеки веб-застосунка на етапі проєктування. Список вимог, які повинні бути перевірені перед здачею проєкту замовнику. Методи і засоби захисту від поширених атак. Аналіз методів Web Application Firewall для виявлення потенційно небезпечного трафіку.

Модульний контроль

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. Огляд сучасних проблем кібербезпеки веб-застосунків.					
Тема 1. Підготовка тестового оточення. Встановлення Damn Vulnerable Web Application.	16	4		4	8
Тема 2. Аналіз трафіку комп'ютерних мереж і сценарії атаки типу Man-in-the-Middle.	16	4		4	8
Тема 3. SQL-ін'єкції. Принципи, пошук і експлуатація SQL-ін'єкцій. Методи ін'єкцій та їх наслідки.	20	4		4	12
Тема 4. Робота з XSS-атаками. Особливості атак та їх наслідки.	20	4		4	12
Модульний контроль	1			1	
Разом за змістовим модулем 1	**73**	**16**		**17**	**40**
Змістовий модуль 2. Аналіз проблем кібербезпеки мереж та системного програмного забезпечення.					
Тема 5. Робота з шеллом в Metasploit. Виконання довільних команд в атакованій системі.	22	4		4	14
Тема 6. Основи сканування IP-мереж.	24	6		4	14
Тема 7. Забезпечення безпеки багатокомпонентного веб-застосунка.	30	6		6	18
Модульний контроль	1			1	
Разом за змістовим модулем 2	77	16		15	46
Усього годин	**150**	**32**		**32**	**86**

5. Теми семінарських занять

№ п/п	Назва теми	Кількість годин
1	*Не передбачено.*	
	Разом	

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин
1	*Не передбачено.*	
	Разом	

7. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Підготовка тестового оточення. Встановлення Damn Vulnerable Web Application.	4
2	Аналіз трафіку комп'ютерних мереж і сценарії атаки типу Man-in-the-Middle.	4
3	SQL-ін'єкції. Принципи, пошук і експлуатація SQL-ін'єкцій. Методи ін'єкцій та їх наслідки.	4
4	Робота з XSS-атаками. Особливості атак та їх наслідки.	4
5	Робота з шеллом в Metasploit. Виконання довільних команд в атакованій системі.	4
6	Основи сканування IP-мереж.	4
7	Забезпечення безпеки багатокомпонентного веб-застосунка.	6
	Разом	**30**

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Знайомство з Penetration Testing Execution Standard.	8
2	Особливості роботи зі сніфферами.	8
3	Автоматизований пошук вразливостей за допомогою параметрів sqlmap.	12
4	Особливості експлуатації Stored та Reflected XSS вразливостей різними інструментальними засобами.	12
5	Можливості Metasploit під час пошуку проблем безпеки у застарілому програмному забезпеченні.	14

6	Методи і засоби виявлення сканування.	14
7	Аналіз методів Web Application Firewall для виявлення потенційно небезпечного трафіку.	18
	Разом	**86**

9. Індивідуальні завдання

Індивідуальні завдання не передбачені.

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота здобувачів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

12.1. Розподіл балів, які отримують здобувачі (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…0,5	8	0…4
Виконання і захист лабораторних робіт	0...6	4	0…24
Модульний контроль	0…25	1	0…25
Змістовний модуль 2			
Робота на лекціях	0…0,5	8	0…4
Виконання і захист лабораторних робіт	0...6	3	0…18
Модульний контроль	0…25	1	0…25
Усього за семестр			**0…100**

Білет для іспиту складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань складає 50 балів.

Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 балів.

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60 - 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи та домашні завдання. Знати основні загрози безпеки веб-застосунків. Знати назви стандартів / спільнот, що описують вимоги до кібербезпеки веб-застосунків та надають рекомендації з підвищення

кібербезпеки досліджуваних систем. Знати назви основних інструментальних засобів, що використовуються під час тестування на проникнення.

Добре (75 - 89). Твердо знати мінімум знань, виконати усі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах. Вміти пояснювати природу походження вразливостей веб-застосунків. Вміти складати план тестування веб-застосунка відповідно до його функціональності. Вміти обирати інструментальні засоби тестування на проникнення. Знаходити вразливості за допомогою інструментальних засобів тестування на проникнення.

Відмінно (90 - 100). Повно знати основний та додатковий матеріал. Знати усі теми. Орієнтуватися у підручниках та посібниках. Вміти аналізувати сирцевий код та прогнозувати можливі вразливості (статичний аналіз коду). Розуміти відмінності у межах окремих вразливостей (зокрема, SQL-ін’єкцій та XSS-атак). Вміти проводити всі етапи тестування на проникнення відповідно до Penetration Testing Execution Standard. Знати рекомендації зі створення безпечних веб-застосунків відповідно до OWASP. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

1. Тецький А. Г. Теоретичне введення до лабораторних робіт.
2. Тецький А. Г. Методичні вказівки щодо виконання лабораторних робот.

Електронний ресурс https://mentor.khai.edu/course/view.php?id=8275, на якому розміщено навчально-методичний комплекс дисципліни, який включає в себе:

- робоча програма дисципліни;
- конспект лекцій, в тому числі в електронному вигляді, які за змістом повністю відповідають робочій програмі дисципліни;
- методичні вказівки та рекомендації для виконання лабораторних робіт, а також рекомендації для самостійної підготовки;
- модульний контроль.

14. Рекомендована література

Базова

1. OWASP Foundation | Open Source Foundation for Application Security [Ел. ресурс]. URL: https://owasp.org/
2. Ric Messier. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems / Apress, 2016. – 115 p.
3. Ron Lepofsky. The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web / Apress, 2014. – 232 p.
4. Peter Kim. The Hacker Playbook 3: Practical Guide To Penetration Testing. – 2018. – 289 p.

Допоміжна

1. William Shotts. The Linux Command Line, 2nd Edition: A Complete Introduction / No Starch Press, 2019. – 504 p.
2. Raphaël Hertzog, Jim O'Gorman, Mati Aharoni. Kali Linux Revealed - Mastering the Penetration Testing Distribution / Offsec Press, 2017. – 344 p.

15. Інформаційні ресурси

1. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution [Ел. ресурс]. URL: https://www.kali.org/
2. National Vulnerability Database [Ел. ресурс]. URL: https://nvd.nist.gov/