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

ЗАТВЕРДЖУЮ

В.о. декана ФКІТ
Ігор ЯКИМЕНКО
_____
«____» _____ 2023 р.

ЗАТВЕРДЖУЮ

В.о. проректора з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ
_____
«____» _____ 2023 р.

ЗАТВЕРДЖУЮ:
Директор ННІНОТ
Святослав ПИТЕЛЬ
_____
_____2023 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	15	5	4	96	150	1
Заочна	1	1,2	8	4	-	-	138	150	2

Тернопіль – 2023

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 №10 від 23.06.2023 р.).

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

Робоча програма затверджена на засіданні кафедри кібербезпеки,
протокол № 1 від 28.08.2023 р.

Завідувач кафедри Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності 125 «Кібербезпека та захист інформації», протокол № 1 від 30.08.2023 р.

Голова групи
забезпечення спеціальності Василь ЯЦКІВ

Гарант ОП 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 – 15* *Заочна – 4*
Загальна кількість годин – 150		Самостійна робота (год.): *Денна – 100 (в т.ч. тренінг 4 год.)* *Заочна – 138* Індивідуальна робота (год.): *Денна – 5*
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	Практичні заняття	СРС	ІРС	Контрольні заходи
Змістовий модуль 1. ***Види тестування на проникнення***					
Тема 1. Види тестування на проникнення	2		2		Опитування під час заняття
Тема 2. Загальні вимоги до тестування на проникнення	2		2		Опитування під час заняття
Тема 3 Юридичні питання тестування на проникнення	2		4		Опитування під час заняття я
Тема 4. Збір інформації	2	1	8		Опитування під час заняття, оцінювання практ. занять
Тема 5. Сканування мережі	2	1	4		Опитування під час заняття, оцінювання практ. занять
Тема 6. Тунелювання та обхід брандмауера	2	1	4		Опитування під час заняття, оцінювання практ. занять
Тема 7. Перерахування	2	1	4		Опитування під час заняття, оцінювання практ. занять
Тема 8. Сканування та оцінка вразливості	2	2	4	2	Опитування під час заняття, оцінювання практ. занять
Змістовий модуль 2. ***Атаки на протоколи та програми***					
Тема 9. Атаки на паролі	2	2	4		Опитування під час заняття, оцінювання практ. занять
Тема 10. Сніффінг	2	1	10		Опитування під час заняття, оцінювання практ. занять
Тема 11. Робота з Metasploit	2	2	10	2	Опитування під час заняття, оцінювання практ. занять
Тема 12. Підвищення привілеїв	2	1	8		Опитування під час заняття, оцінювання практ. занять
Тема 13. Атаки на рівні програми	2	1	12		Опитування під час заняття, оцінювання практ. занять
Тема 14. Бездротові загрози	2	1	8		Опитування під час заняття, оцінювання практ. занять
Тема 15. Написання звітів	2	1	12	1	Опитування під час заняття, оцінювання практ. занять
Тренінг			4		Опитування під час заняття
Разом	**30**	**15**	**100**	**5**	

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	0,5	-	8
Тема 2. Загальні вимоги до тестування на проникнення	0,5	-	8
Тема 3 Юридичні питання тестування на проникнення	0,5	-	8
Тема 4. Збір інформації	0,5	-	8
Тема 5. Сканування мережі	0,5	1	8
Тема 6. Тунелювання та обхід брандмауера	0,5	-	10
Тема 7. Перерахування	0,5	1	10
Тема 8. Сканування та оцінка вразливості	1		10
Змістовий модуль 2. ***Атаки на протоколи та програми***			
Тема 9. Атаки на паролі	0,5	-	10
Тема 10. Сніффінг	0,5	1	10
Тема 11. Робота з Metasploit	0,5	1	10
Тема 12. Підвищення привілеїв	0,5	-	10
Тема 13. Атаки на рівні програми	0,5	-	10
Тема 14. Бездротові загрози	0,5	-	10
Тема 15. Написання звітів	0,5	-	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. Комплексне практичне індивідуальне завдання

Варіанти КПІЗ з дисципліни «Тестування комп'ютерних систем на проникнення»

Виконання тесту на проникнення.

1.1 Постановка задачі.
1.2 Збір інформації та пошук цілей.
1.3 Пошук вразливостей.
1.4 Експлуатація та проведення атак.
1.5 Розширення зони впливу і ескалація привілеїв.
1.6 Написання звіту.

7. Самостійна робота

№ п/п	Тематика
1	Топ-10 вразливостей OWASP
2	Топ-10 ризиків безпеки веб-додатків OWASP
3	Поверхня атаки
4	Атаки на стороні сервера
5	Уразливості виконання коду
6	База даних уразливостей
7	Експлуатація браузера
8	Експлуатація браузера
9	Тестування сайту на проникнення
10	Збір інформації про веб-сайт
11	Виявлення веб-сайтів на одному сервері
12	Використання інструменту Sqlmap
13	Захист від SQL ін'єкції
14	Інструмент тестування проникнення на веб-сайт OWASP ZAP
15	Сканування веб-сайтів за допомогою інструменту OWASP-ZAP
16	Тест на проникнення мобільного телефону
17	Вектори атак мобільного телефону
18	Життєвий цикл атаки на мобільний телефон