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 2021 р.

СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Засоби тестування на проникнення

(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

Спеціальність: 101 Екологія, 103 Науки про Землю, 113 Прикладна математика, 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки, 123 Комп'ютерна інженерія, 124 Системний аналіз, 125 Кібербезпека, 151 Автоматизація та комп'ютерно-інтегровані технології, 152 Метрологія та інформаційно-вимірювальна техніка, 163 Біомедична інженерія, 172 Телекомунікації та радіотехніка, 173 Авіоніка, 193 Геодезія та землеустрій

Освітня програма: усі освітні програми за відповідними спеціальностями

Рівень вищої освіти: ***другий (магістерський)***

Силабус введено в дію з 01.09.2021 року

Харків – 2021 р.

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

Силабус навчальної дисципліни розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки (№ 503)

Протокол № 1 від « 30 » серпня 2021 р.

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

Погоджено з представником здобувачів освіти:

_____ _____ _____
(підпис) (ініціали та прізвище)

1. Загальна інформація про викладача

Тецький Артем Григорович, к.т.н., старший викладач. З 2015 року проводить заняття з дисциплін, пов'язаних з адмініструванням і налагодженням мереж, а також Linux-систем.

Напрями наукових досліджень:

Кібербезпека Web-застосунків;

Реверс-інжинірінг.

2. Опис навчальної дисципліни

Семестр, в якому викладається дисципліна – 2 семестр.

Обсяг дисципліни:

5 кредитів ЄКТС (150 годин), у тому числі аудиторних – 48 годин, самостійної роботи здобувачів **–** 102 годин.

Форми здобуття освіти

Денна, дистанційна, дуальна.

Дисципліна – вибіркова.

Види навчальної діяльності – лекції, лабораторні роботи, самостійна робота здобувача.

Види контролю – поточний, модульний та підсумковий (семестровий) контроль (іспит).

Мова викладання – українська.

Необхідні обов'язкові попередні дисципліни (пререквізити) – теорія та технології розроблення безпечних розподілених систем.

Необхідні обов'язкові супутні дисципліни (кореквізити) – дипломне проєктування.

3. Мета та завдання навчальної дисципліни

Мета

Вивчення навчальної дисципліни «Засоби тестування на проникнення» полягає в ознайомленні та отриманні навичок роботи з інструментальними засобами тестування інформаційних систем на проникнення.

Завдання

Вивчення причин походження вразливостей, пошук вразливостей, експлуатація вразливостей та способи захисту для підвищення кібербезпеки об’єкта тестування на проникнення.

Після опанування дисципліни здобувач набуде наступні **компетентності**:

– здатність застосовувати знання у практичних ситуаціях;

– здатність до абстрактного мислення, аналізу та синтезу;

– 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..

Очікується, що після опанування дисципліни здобувачем будуть досягнуті наступні **результати навчання** і він буде здатний:

– інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах;

– застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки;

– ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

4. Зміст навчальної дисципліни

Модуль 1.

Змістовний модуль 1. Огляд сучасних проблем кібербезпеки веб-застосунків

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

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 4 години.*
- *Лабораторна робота: «Встановлення платформи для тестування».*
- *Обов’язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): комп’ютер зі встановленою віртуальною операційною системою Kali Linux.*

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.

- *Обсяг самостійної роботи здобувачів: 10 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Загальні принципи та етапи тестування на проникнення. Знайомство з Penetration Testing Execution Standard.

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

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 4 години.*
- *Лабораторна робота: «Перехоплення трафіку під час роботи в Інтернет».*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): комп'ютер зі встановленою віртуальною операційною системою Kali Linux.*

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.

- *Обсяг самостійної роботи здобувачів: 10 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Особливості роботи зі сніфферами. Способи доступу до cookies. Наслідки Man-in-the-Middle атак.

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

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 6 годин.*
- *Лабораторна робота: «Пошук і експлуатація SQL-ін'єкцій».*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): комп'ютер зі встановленою віртуальною операційною системою Kali Linux.*

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.

- *Обсяг самостійної роботи здобувачів: 14 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Порівняння інструментальних засобів для експлуатації ін'єкцій. Автоматизований пошук вразливостей за допомогою параметрів sqlmap. Завантаження файлів за допомогою ін'єкцій.

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

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 8 годин.*
- *Лабораторна робота: «Міжсайтовий скриптинг».*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): комп'ютер зі встановленою віртуальною операційною системою Kali Linux.*

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.

- *Обсяг самостійної роботи здобувачів: 14 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Особливості експлуатації Stored та Reflected XSS вразливостей різними інструментальними засобами.

Модульний контроль 1

- *Форма занять: виконання модульної роботи у вигляді тестування на комп'ютері в аудиторії (за рішенням лектора допускається проведення у дистанційній формі).*
- *Обсяг аудиторного навантаження: 1 година*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): комп'ютер зі встановленими тестовими завданнями.*
- *Обсяг самостійної роботи здобувачів – за необхідністю.*

Підготовка до модульного контролю.

Змістовний модуль 2. Аналіз проблем кібербезпеки мереж та системного програмного забезпечення

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

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 8 годин.*
- *Лабораторна робота: «Робота з фреймворком Metasploit».*

- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): комп'ютер зі встановленою віртуальною операційною системою Kali Linux.*

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.

- *Обсяг самостійної роботи здобувачів: 16 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Можливості Metasploit під час пошуку проблем безпеки у застарілому програмному забезпеченні. Створення плагінів для Metasploit.

Тема 6. Основи сканування IP-мереж.

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 8 годин.*
- *Лабораторна робота: «Робота з мережевим сканером».*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): комп'ютер зі встановленою віртуальною операційною системою Kali Linux.*

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.

- *Обсяг самостійної роботи здобувачів: 16 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Загрози та проблеми безпеки даних моніторингу хмарних обчислень.

Тема 7. Забезпечення безпеки багатокомпонентного веб-застосунка.

- *Форма занять: лекція, лабораторна робота, самостійна робота.*
- *Обсяг аудиторного навантаження: 8 годин.*
- *Лабораторна робота: «Методи та засоби захисту модульних веб-застосунків».*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): комп'ютер зі встановленою віртуальною операційною системою Kali Linux.*

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.

- *Обсяг самостійної роботи здобувачів: 30 годин.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Вимоги до безпеки застосунків, що використовують дані платіжних карт (PCI DSS). Можливості IDS/IPS при забезпеченні безпеки.

Модульний контроль 2

- *Форма занять: виконання модульної роботи у вигляді тестування на комп'ютері в аудиторії (за рішенням лектора допускається проведення у дистанційній формі).*
- *Обсяг аудиторного навантаження: 1 година*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): комп'ютер зі встановленими тестовими завданнями.*
- *Обсяг самостійної роботи здобувачів – за необхідністю.*

Підготовка до модульного контролю.

5. Індивідуальні завдання

Не передбачено навчальним планом

6. Методи навчання

Словесні, наочні, практичні.

7. Методи контролю

Поточний контроль (теоретичне опитування й розв'язання практичних завдань), модульний контроль (тестування за розділами курсу) та підсумковий (семестровий) контроль (іспит).

8. Критерії оцінювання та розподіл балів, які отримують здобувачі

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**

Контроль знань при проведенні занять оцінюється за такими шкалами:

1) активність на лекції під час відповідей на питання:

– повна відповідь на питання – 0,5 бала;

– неповна відповідь – 0,25 бала;

– відсутність на лекції – 0 балів;

2) виконання і захист лабораторних робіт:

– виконані всі завдання лабораторної роботи, оформлені відповідно до вимог, надано вичерпні правильні відповіді на всі запитання – 6 балів;

– виконані всі завдання лабораторної роботи, мають місце незначні відхилення від оформлення відповідно до вимог, надано правильні відповіді на всі запитання – 5 балів;

– виконано 88-99% завдань лабораторної роботи, мають місце незначні відхилення від оформлення відповідно до вимог, надано правильні відповіді не на всі запитання – 4 бали;

– виконано 76-87% завдань лабораторної роботи, мають місце незначні відхилення від оформлення відповідно до вимог, надано правильні відповіді не на всі запитання – 3 бали;

– виконано 63-75% завдань лабораторної роботи, мають місце незначні відхилення від оформлення відповідно до вимог, надано правильні відповіді не на всі запитання – 2 бали;

– виконано 50-62% завдань лабораторної роботи, мають місце значні відхилення від оформлення відповідно до вимог, надано правильні відповіді не на всі запитання – 1 бал;

– студент не допущений до захисту роботи (виконано менше 50% її завдань) або робота не захищена – 0 балів.

На модульний контроль (всього 25 балів) виносяться всі пройдені за контрольований період теми, які включаються у варіанти тестових завдань, що містять по 20 питань. Максимальна кількість балів за кожне тестове питання – 1,25.

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до заліку. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

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

Прийнята шкала оцінювання

Сума балів за всі види навчальної діяльності	Оцінка для екзамену, *курсового проекту* (роботи), практики
90-100	відмінно
75-89	добре
60-74	задовільно
01-59	незадовільно з можливістю повторного складання

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.

9. Політика навчального курсу

Відпрацювання пропущених занять відбувається відповідно до розкладу консультацій, за попереднім погодженням з викладачем. Питання, що стосуються академічної доброчесності, розглядає викладач або за процедурою, визначеною у Положенні про академічну доброчесність.

10. Методичне забезпечення та інформаційні ресурси

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки. Інформаційні ресурси:

1. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https://moodle.csn.khai.edu
2. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution [Ел. ресурс]. URL: https://www.kali.org/
3. National Vulnerability Database [Ел. ресурс]. URL: https://nvd.nist.gov/
4. OWASP Foundation | Open Source Foundation for Application Security [Ел. ресурс]. URL: https://owasp.org/

11. Рекомендована література

Базова

1. Ric Messier. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems / Apress, 2016. – 115 p.
2. Ron Lepofsky. The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web / Apress, 2014. – 232 p.
3. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni. Metasploit. – 2011. – 328 p.
4. А. Г. Тецкий, О. А. Ильяшенко, Д. Д. Узун. Методы и средства тестирования на проникновение веб-приложений и сетей. Практикум / под ред. В.С. Харченко – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ». 2017. – 77 с.

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.