ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

СИЛАБУС

Базова інформація про дисципліну	
Назва дисципліни	**Тренінг-курс с кібербезпеки**
Рівень вищої освіти / фахової передвищої освіти	Фахова перед вища освіта
Семестр	ІІ семестр
Циклова комісія	програмування
Анотація курсу	Навчальна дисципліна відноситься до вибіркових дисциплін курса. Після проходження курсу студент придбаєте такі знання і навички: Отримає навички роботи з командним рядком (терміналом) в Windows і Linux, тобто зможете впевнено працювати з системою за допомогою команд. Детально вивчіть етапи хакинга. Навчіться проводити різні види сканування і виявляти уразливості у мережевих пристроїв. Навчіться зламувати Windows 7/8 / 8.1 / 10 різними методами. Отримає базові знання з соціальної інженерії, яка особливо актуальна останнім часом. Освоїте як створити і впровадити троянську програму в віддалену систему. Дізнаєтеся як легко і просто можна взаємодіяти з системою за допомогою командного рядка.
Сторінка курсу в MOODLE	http://78.137.2.119:1919/m72/course/view.php?id=703
Мова викладання	Українська
Лектор курсу	Черниш Світлана Володимирівна, викладач 1 категорії. Канали комунікації: СНД «Moodle»: повідомлення в чаті E-mail: lala68288@gmail.com
Місце дисципліни в освітній програмі	
Освітня програма	http://csbc.edu.ua/documents/otdel/moop_pr.pdf
Перелік загальних компетентностей (ЗК)	Знання та розуміння предметної області та розуміння професійної діяльності Здатність до пошуку, оброблення та аналізу інформації з різних джерел. Здатність до абстрактного мислення, аналізу та сінтезу. Здатність застосовувати знання у практичних ситуаціях.
Перелік спеціальних компетентностей (СК)	Здатність до алгоритмічного та логічного мислення. Здатність накопичувати, обробляти та систематизувати професіййні знання щодо створення і супроводу програмного забеспечення та визначення важливості навчання протягом

	усього життя. Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу програмногот забеспечення.
Перелік програмних результатів навчання	Вміти систематизувати та узагальнювати інформація про підходи, методи та засоби розробки супроводу програмного забеспечення, вдосконалювати відповідні знання, вміння і навички протягом усього життя. Вміти знаходити аналогії та застосовувати знання , вміння та навички з суміжних дісциплін для формування та виришення професійних завдань. Знати основні стандарти у галузі програмної інженерії та вміти дотримуватись рекомендацій, стандартів, специфікацій стосовно процессів життєвого циклу програмного забеспечення. Мати навички командної розробки, погодження, оформлення і випуску всіх видів програмної документації. Знати основні інструментальні засоби для розробки та супроводу програмного забеспечання та вміти застосовувати їх на практиці з урахуванням специфіки отриманого завдання та вимог користувача.
Опис дисципліни	
Структура навантаження на студента	Загальна кількість годин – 90 Кількість кредитів – 3 Кількість лекційних годин – 0 Кількість практичних занять – 36 Кількість годин для самостійної роботи студентів –54 Форма підсумкового контролю – залік
Методи навчання	Словесні (інформаційна, самостійна робота з джерелами інформації, науково-популярна розповідь); Наочні (презентаційні повідомлення); Практичні (лабораторні роботи); Інтерактивні методи (дистанційні консультації).
Зміст дисципліни	
Тема 1. Встановлення та налаштування лабораторного знаряддя. Введення в Metasploit.	Встановлення Kali Linux. Мережеві налаштування VirtualBox. Встановлення та налаштування OWASP. Принципи роботи Metasploit. Модулі. Основні команди. Встановлення та ініціалізація бази даних. Робота з базами даних. Репозиторії експлойтів.
Тема 2. Збір інформації про об’єкт	Попердній збір інформації про об’єкт, що атакується.Збір інформації про електронні поштові адреси користувачів. Google hacking – розширені пошукові можливості. Збір інформації за допомогою Shodan. Витяг інформації з метаданих файлів. Теоретичні основи сканування. Сканування портів інтегрованим NMAP. Сканування портів вбудованим сканером Metasploit. Установка сканера вразливостей OpenVas.

	Сканування вразливостей за допомогою OpenVas. Сканування вразливостей скриптами NMAP. Сканування вразливостей за допомогою модулів Metasploit. Сканування Веб додатків.
Тема 3. Отримання доступу до системи через серверні атаки.	Теоретичні основи атаки переповнення буфера. Злом системи через уразливість переповнення буфера. Отримання віддаленого доступу через графічний інтерфейс. Bind vs. Reverse. DoS атака на віддалену систему.
Тема 4. Отримання доступу до системи через клієнтські атаки.	Теоретичні основи атаки DLL Hijacking. Злом системи через уразливість DLL Hijacking. Експлуатація FTP клієнта WinAxe. Впровадження виконуваного коду в HTA документ. Злом комп'ютера через USB носії та загальні мережеві папки. Впровадження макросу в документ MS Office – 1-й спосіб Впровадження макросу в документ MS Office – 2-й спосіб.
Тема 5. Способи створення троянської програми.	Генерування самостійного файлу з Msfvenom. Впровадження троянця в легітимну програму через Msfvenom. Впровадження троянця в легітимну програму через Trojanizer. Впровадження троянця в легітимну програму через Iexpress.
Тема 6. Атака на веб додаток через SQL Injection.	Основи SQLi – частина 1. Налаштування бази даних MySQL на Kali Linux. Основи роботи з SQL запитами.
Тема 7. Атака на веб додаток через SQL Injection (частина 2).	Основи SQLi. Частина 2 – техніки тестування. Перевірка на вразливість. Визначення кількості колонок в SQL запиті. Витяг інформації з БД. Виконання системних команд через SQLi. Сліпа ін'єкція (Blind SQLi). Злом БД за допомогою SQLMap. Отримання віддаленого доступу до системи за допомогою SQLMap.
Тема 8. Атака на веб додаток через Command Injection. Атака на веб додаток через Path Injection.	Теоретичні основи атаки Command Injection. Command Injection на практиці. Теоретичні основи атаки Path traversal. Path traversal на практиці.
Тема 9. Управління доступом. Взаємодія со зламаним комп'ютером. Підвищення привілей доступу. Встановлення бекдора.	Управління комп'ютером жертви через Meterpreter. Управління комп'ютером жертви через командний рядок CMD. Установка backdoor через Meterpreter. Установка backdoor через планувальник завдань. Установка backdoor через служби.
Тема 10. Управління доступом. Злом паролів. Видалення слідів своєї діяльності.	Де і як зберігається пароль на Linux. Теорія принципу злому паролів. Отримання хеша паролів. Злом паролів за допомогою John-the-Ripper. Як отримати пароль у відкритому вигляді на Windows – теорія. Як отримати пароль у відкритому вигляді за допомогою Mimikatz. Отримання паролів через фішинг. Як заховати файли в системах Windows. Замітання слідів – видалення логів.
Політика дисципліни	
Політика відвідування	Регулярне відвідування всіх видів занять, своєчасність виконання самостійної роботи.

	За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання зорганізується в он-лайн формі за погодженням із керівником курсу.
Політика щодо дедлайнів та перескладання	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.
Академічна доброчесність	У випадку недотримання політики академічної доброчесності (плагіат, амо плагіат, фабрикація, фальсифікація, списування, обман, хабарництво) передбачено повторне проходження оцінювання.

Система оцінювання

Поточний контроль здійснюється протягом семестру під час проведення практичних, семінарських та інших видів занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту отримати атестацію з предмету – 60 балів); підсумковий/ семестровий контроль, проводиться у формі заліку або іспиту, відповідно до графіку навчального процесу.

Підсумкова оцінка за умови заліку виставляється як загальна сума балів, набраних за результатами поточного контролю. Підсумкова оцінка за умови іспиту виставляється як загальна сума балів набраних за результатами поточного (70%) та підсумкового контролю.

Накопичування рейтингових балів з навчальної дисципліни

Види навчальної роботи	**Мах кількість балів**
Виконання практичних робіт по темах 1- 10 по 7 балів	70
Індивідуальна робота	30
Разом	100

Шкала оцінювання

ECTS	**Бали**	**Зміст**
A	90-100	Бездоганна підготовка в широкому контексті
B	80-89	Повні знання, міцні вміння
C	70-79	Хороші знання та вміння
D	65-69	Задовільні знання, стереотипні вміння
E	60-64	Виконання мінімальних вимог діяльності в стандартних умовах
FX	35-59	Слабкі знання, відсутність умінь
F	1-34	Необхідний повторний курс

Список рекомендованих джерел

1. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібербезпеки та кіберзахисту.-К.: Ліра-К, 2021. – 554 с.

2. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.

3. Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій – К.:ДУІКТ, 2010. – 508 с.

4. Богуш В.М., Довидьков О.А. Проектування захищених комп'ютерних Систем та мереж, навчальний посібник, - К.: ДУІКТ, 2008. – 508 с.

5. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки, підруучник, - К.:ПВП «Задруга», 2014. – 222 с.

6. Технології захисту інформації: навчальний посібник / С.Е.Остапов, С.П.Євсеєв, О.Г.Король. – Х.: Вид. ХНЕУ, 2013. – 476 с. (Укр.мов.)

7. Навчальний посібник / Ю.Я.Бобало, І.В.Горбатий, М.Д.Кіселичник, А.П.Бондарєв, С.С.Войтусік, та інші. Львів: Видавництво Львівської політехніки, 2019. – 580 с.

8. Cyber-Physical Security: Monograph / edit. Clark. - Springer International Publishing, 2017/ - ISBN 978-3-319-32822-5 (print); 978-3-319-32824-9 (online). 299 p.

9. Enterprise Security: Monograph / edit. Chang.- Springer International Publishing, 2017/ - ISBN 978-3-319-54379-6 (print); 978-3-319-54379-6 (online). 277 p.

10. Cyber Security. Simply. Make it Happen :Monograph / edit. Abolhassan. - Springer International Publishing, 2017/ - ISBN 978-3-319-46528-9 (print); 978-3-319-32824-9 (online). 227 p