МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(протокол № 3/22 від 3 жовтня 2022 р.)

Завідувач кафедри

 Венгерський П.С.

Силабус з навчальної дисципліни "Застосування Python в кібербезпеці", що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – Кібербезпека

Львів - 2022

Назва дисципліни	Застосування Python в кібербезпеці
Адреса викладання дисципліни	м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека
Викладачі дисципліни	Квасниця Галина Андріївна, канд. фіз.-мат. наук, доцент кафедри кібербезпеки
Контактна інформація викладачів	halyna.kvasnytsya@lnu.edu.ua; https://ami.lnu.edu.ua/employee/kvasnytsia; Головний корпус ЛНУ ім. І. Франка, каб. 360. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (а також за розкладом консультацій кафедри). Можливі он-лайн консультації через Microsoft Teams. Для погодження часу он-лайн конультації слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua/admission/specializations
Інформація про дисципліну	Дисципліна “Застосування Python в кібербезпеці” є вибірковою дисципліною з спеціальності 125 – кібербезпека для освітньої програми Кібербезпека, яка викладається в шостому семестрі в обсязі 4-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на поглиблене вивчення засобів мови програмування Python, що можуть бути використані як для проведення кібератак, так і з метою їх знешкодження та ефективної протидії.
Мета та цілі дисципліни	Метою курсу вибіркової дисципліни “Застосування Python в кібербезпеці” є набуття студентами теоретичних знань та практичних умінь для застосування Python у розробці власних та модифікації існуючих інструментів у галузі кібербезпеки.
Література для вивчення дисципліни	**1.** Duffy C. Python: Penetration Testing for Developers - Packt Publishing, 2016. -666 p. **2.** Seitz J., Arnold T. Black Hat Python: Python Programming for Hackers and Pentesters - No Starch Press, 2021, 216 p. 3. Lutz M/ Learning Python - O'Reilly Media, 2013. 1643 p. **4.** Rehim R. Effective Python Penetration Testing - Packt Publishing, 2016, 164 p. **5.** Buchanan C. Python Web Penetration Testing Cookbook - Packt Publishing Ltd, 2015. – 224 p. 6. O’Connor TJ. Violent Python. A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers. Elsevier, 2013. – 269 p. Он-лайн курси:

	1. https://www.coursera.org/learn/pythonforcybersecurity-introduction/ 2. https://ua.udemy.com/course/python-for-pentesters/ 3. https://ua.udemy.com/course/learn-python-and-ethical-hacking-from-scratch/	
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 48 год., з них 16 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 72 год.	
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** -бібліотеки Python, призначені для низькорівневого мережевого програмування, збору і аналізу інформації про мережевий трафік; - основи взаємодії з Web за допомогою Python; - механізми створення шкідливого програмного забезпечення та засоби для його виявлення і знешкодження. **вміти:** - розробляти сценарії Python у вигляді виконуваних файлів та модулів; - перехоплювати мережевий трафік, розробляти власні інструменти для його аналізу, - створювати і модифікувати сценарії для атак на веб-застосунки; - збирати відкриту і приховану інформацію з веб-сайтів для подальших атак; - виконувати та виявляти SQL- ін'єкції, експлуатувати файли –cookies; - виявляти вразливості та щкідливе програмне забезпечення, - здійснювати розробку інструментів кіберзахисту при здійсненні професійної діяльності. **Курс забезпечує набуття таких компетентностей: ЗК 1, ЗК 5, ФК 3, ФК 8, ФК 11, ФК 12; та програмних результатів навчання: ПРН 12, ПРН 20, ПРН 21, ПРН 22, ПРН 27, ПРН 42, ПРН 46, ПРН 50, ПРН 51,ПРН 52, ПРН 53.**	
Ключові слова	Кібербезпека, загроза, вразливість, цілісність, безпека даних, мережевий трафік, ескалація привілеїв, бекдор, веб-скрапінг.	
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.	
Теми		год
	1. Python для етичного хакінгу. Розробка скриптів. Модуль argparse для аналізу аргументів командного рядка. Використання модуля subprocess.	2
	2. Низькорівневе мережеве програмування на Python. Модуль socket.	2
	3. Засоби Scapy для аналізу мережевого трафіку.	2
	4. Розробка шкідливих програм – кейлогери, бекдори, ін'єкції коду, трояни. Використання модулів pynput, smtplib. Конвертація скриптів у виконувані файли.	2
	5. Реалізація взаємодії між клієнтом та сервером засобами Python.	2
	6. Виконання атак облікових даних за допомогою Python. Python для ескалації привілеїв	2
	7. Бібліотеки Python для взаємодії з Web (urrllib, urllib2, requests). Використання BeautifulSoup для HTML-парсингу.	2

8. Аналіз доступності веб-додатків та веб-сайтів.	2

Підсумковий контроль, форма	Залік у кінці 6 семестру
Пререквізити	Для вивчення курсу студенти потребують базових знань з : основ кібербезпеки, комп'ютерних мереж, програмування мовою Python.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Модульний контроль. Лабораторні заняття у вигляді виконання практичних завдань і презентації отриманих результатів, обговорення написаних програм, самостійна робота з опрацювання пропонованих модулів : 1. Розробка скриптів з використанням модуля argparse. 2. Знайомство з бібліотекою subprocess. Зміна Mac-адреси. 3. Бібліотека Scapy. Розробка простого сканера мережі. 4. ARP- та DNS-спуфінг. Сніфер пакетів. 5. Сканер вразливостей на Python. 6. Застосування ін'єкцій коду. 7. Розробка кейлогера. 8. Реалізація атаки грубої сили. 9. Шкідливе програмне забезпечення. Бекдори. 10. Конвертація скриптів у виконувані файли. Трояни 11. Робота з регістром Windows. Модуль winreg. Встановлення виконуваних файлів на цільовій машині. 12. Розробка сервера. Прослуховування потоку вхідних пакетів. Фільтрація даних. 13. Модуль requests. Надсилання та обробка запитів до сервера. 14. Веб-скрапінг та парсинг даних з HTML.
Необхідне обладнання	Лабораторія з обладнаними робочими станціями, з'єднаними в комп'ютерну мережу. Можливість підключення робочих станцій до мережі Інтернет Можливість встановлення віртуальних машин та резервної операційної системи Kali Linux.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • лабораторні роботи: 70% семестрової оцінки; максимальна кількість балів – 70. • контрольний тест: 20% семестрової оцінки; кількість балів – 20. • додаткові бали за активну участь у лекціях і лабораторних роботах 10% семестрової оцінки; максимальна кількість балів – 10. Підсумкова максимальна кількість балів – 100. **Академічна доброчесність**: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття курсу. Студенти

	повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх лабораторних робіт, передбачених курсом. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. П**олітика виставлення балів.** Враховуються бали набрані при самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до заліку	Залік – за результатами поточного контролю протягом семестру і усне опитування. Питання відповідають темам курсу.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.