Силабус курсу
ТЕСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА ПРОНИКНЕННЯ

Ступінь вищої освіти – магістр
Рік навчання: 1
Семестр: 1
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Василь Яцків
Контактна інформація	vy@wunu.edu.ua

Опис дисципліни

Даний курс знайомить із принципами та прийомами пов'язаними із застосуванням етичних методів зламу та проникнення в комп'ютерні системи. Ви ознайомитеся з сучасними методами та інструментами зламу, які зазвичай використовуються для компрометації комп'ютерних систем. Етичний злам, також відомий як тестування на проникнення - це процес зламу системи з дозволу та юридичної згоди організації чи фізичної особи, яка є власником та керує системою, з метою виявлення вразливих місць та посилення безпеки організації. Ви будете проводити практичне тестування на проникнення у віртуальному лабораторному середовищі, що забезпечує практику концепцій, представлених у курсі, використовуючи актуальні версії інструментів для зламу, які використовуються в цій галузі. Важливо ще раз зазначити, що курс «Тестування комп'ютерних систем на проникнення» - це етичний хакерський курс, який означає, що ви навчитесь техніці зламу в контрольованому середовищі для досягнення кращої безпеки комп'ютерних систем.

Метою курсу «Тестування комп'ютерних систем на проникнення» є - отримання знань та навиків, які необхідні для проведення тестування комп'ютерних систем на проникнення.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/0	Види тестування на проникнення	пояснювати різницю між різними видами тестування на проникнення	Поточне опитування
2/0	Загальні вимоги до тестування на проникнення	описувати загальні вимоги до тестування на проникнення	Поточне опитування
2/1	Юридичні питання тестування на проникнення	застосовувати юридичні питання тестування на проникнення	Поточне опитування
2/1	Збір інформації	збирати інформацію про ціль тестування	Поточне опитування
2/1	Сканування мережі	застосовувати методи сканування мереж	Поточне опитування
2/1	Тунелювання та обхід брандмауера	використовувати тунелювання та обхід брандмауера	Поточне опитування
2/1	Перерахування	застосовувати методи перерахування	Поточне опитування
2/1	Сканування та оцінка вразливості	застосовувати методи для виявлення вразливостей	Поточне опитування, тестування

2/2	Атаки на паролі	демонструвати атаки на паролі	Поточне опитування
2/1	Сніффінг	демонструвати навики перехоплення та аналізу пакетів	Поточне опитування
2/2	Робота з Metasploit	використовувати Metasploit для проникнення в ціль	Поточне опитування
2/1	Підвищення привілеїв	демонструвати навики роботи з підвищення привілеїв на цілі	Поточне опитування
2/1	Атаки на рівні програми	здійснювати атаки на рівні програми	Поточне опитування
2/1	Бездротові загрози	виявляти вразливості в бездротових мережах	Поточне опитування
2/1	Написання звітів	робити звіт про виконану роботу з тестування на проникнення	Поточне опитування, тестування

Рекомендовані джерела інформації

1. Опорний конспект лекцій з курсу «Тестування комп'ютерних систем на проникнення» для студентів спеціальності 125 «Кібербезпека» – Тернопіль: ТНЕУ, 2019. – 119 с.
2. Mamilla, Sushmitha Reddy. A Study of Penetration Testing Processes and Tools. 2021. https://scholarworks.lib.csusb.edu/etd/1220
3. BSI - Study A Penetration Testing Model. Federal Office for Information Security, 111p. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ Publications/Studies/Penetration/penetration_pdf.html
4. Najera-Gutierrez, Gilberto, and Juned Ahmed Ansari. *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd, 2018.
5. Vulnerability Scanning Tools. https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
6. PTES Technical Guidelines. http://www.pentest-standard.org/index.php/Exploitation
7. Johari, Rahul, et al. Penetration Testing in IoT Network. In: 2020 5th International *Conference on Computing, Communication and Security (ICCCS)*. IEEE, 2020, pp. 1-7.
8. ASAAD, Renas R. Penetration testing: Wireless network attacks method on Kali Linux OS. *Academic Journal of Nawroz University*, 2021, 10.1, pp.7-12
9. Yaacoub, Jean-Paul A., et al. A Survey on Ethical Hacking: Issues and Challenges. arXiv preprint arXiv:2103.15072, 2021.
10. Alanda, Alde, et al. Web Application Penetration Testing Using SQL Injection Attack. *JOIV: International Journal on Informatics Visualization*, 2021, 5.3, pp. 320-326
11. Akhilesh, R.; Bills, O.; Chilamkurti, N.; Chowdhury, M.J.M. Automated Penetration Testing Framework for Smart-Home-Based IoT Devices. Future Internet 2022, 14, 276. https://doi.org/10.3390/fi14100276

Політика оцінювання

Політика щодо дедлайнів та перескладання: Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Використання друкованих і електронних джерел інформації під час контрольних заходів заборонено.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Оцінювання

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20 %	20 %	5 %	15 %	40 %
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-7.	Підсумкова письмова робота за темами №1-15.	Визначається як середнє арифметичне з оцінок за виконання трьох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання наскрізного завдання.	1. 15тестів по 4 бали - max 60 балів. 2.Практич-не завдання - max 40 балів

Шкала оцінювання:

ECTS	**Бали**	**Зміст**
A	90–100	відмінно
B	85–89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов’язковим повторним курсом