



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

ППП

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 навички перехоплення та аналізу пакетів	Поточне опитування
2/2	Робота з Metasploit	використовувати Metasploit для проникнення в ціль	Поточне опитування
2/1	Підвищення привілеїв	демонструвати навички 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. Norman, Alan T. *Computer Hacking Beginners Guide: How to Hack Wireless Network, Basic Security and Penetration Testing, Kali Linux, Your First Hack*. Independently published, 2018.
6. Chu, Ge, and Alexei Lisitsa. "Penetration Testing for Internet of Things and Its Automation.", 2018 *IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 2018.
7. Vulnerability Scanning Tools. https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
8. PTES Technical Guidelines. <http://www.pentest-standard.org/index.php/Exploitation>
9. 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.
10. ASAAD, Renas R. Penetration testing: Wireless network attacks method on Kali Linux OS. *Academic Journal of Nawroz University*, 2021, 10.1, pp.7-12
11. Yaacoub, Jean-Paul A., et al. A Survey on Ethical Hacking: Issues and Challenges. arXiv preprint arXiv:2103.15072, 2021.
12. Alanda, Alde, et al. Web Application Penetration Testing Using SQL Injection Attack. *JOIV: International Journal on Informatics Visualization*, 2021, 5.3, pp. 320-326
13. 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

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4
20%	20%	20%	40%
1. Усне опитування на заняттях – мах 8*3=24 балів. 2. Письмова робота – мах 52 балів. 3. Практичне завдання – мах 3*8=24 балів	1. Усне опитування на заняттях – мах 7*2=14 балів. 2. Письмова робота – мах 54 балів. 3. Практичне завдання – мах 4*8=32 балів	1. Підготовка КПЗ – мах 30 балів. 2. Захист КПЗ – мах 40 балів. 3. Оцінка за тренінг – мах 30 балів	1. Розв'язання 20 тестів по 3 бали = мах 60 балів. 2. Практичне завдання = мах 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