Силабус курсу

ТЕСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА ПРОНИКНЕННЯ

Ступінь вищої освіти – магістр
Галузь знань – F Інформаційні технології
Спеціальність F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
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.

Структура курсу

Години лек/лаб	Тема	Результати навчання	Завдання
2/-	Вступ до тестування на проникнення.	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	Поточне опитування
2/-	Методологія тестування на проникнення OSSTMM	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	Поточне опитування
2/-	Методології тестування PTES та NIST	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки	Поточне опитування

		організації.	
2/2	Планування та підготовка до тестування на проникнення	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.	Поточне опитування
2/-	Види розвідки	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/-	Активна розвідка	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	Поточне опитування
4/4	Аналіз результатів сканування при тестуванні на проникнення	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	Поточне опитування
2/-	Експлуатація вразливостей	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	Поточне опитування
2/-	Атаки на паролі	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.	Поточне опитування
2/2	Тестування безпеки бездротових мереж	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.	Поточне опитування
2/2	Використання фреймворку MITRE ATT&CK у тестуванні на проникнення	З дійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	Поточне опитування

2/-	Соціальна інженерія в тестуванні на проникнення	Класифікувати та пояснювати основні види атак соціальної інженерії, які експлуатуються зловмисниками; розробляти та впроваджувати комплексні методи захисту від соціально-інженерних атак.	Поточне опитування
2/2	Тестування безпеки IoT-пристроїв	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	Поточне опитування
2/-	Юридичні питання тестування на проникнення	Аналізувати та пояснювати правові рамки та ключові нормативні акти України, які прямо чи опосередковано регулюють діяльність, пов'язану з кібербезпекою та тестуванням на проникнення.	Поточне опитування
2/2	Звітність та рекомендації	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	Поточне опитування

Рекомендовані джерела інформації

1. Опорний конспект лекцій з курсу «Тестування комп'ютерних систем на проникнення» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / Укл. В. Яцків. Тернопіль: ЗУНУ, 2025. – 132 с.
2. Тестування на проникнення: навч. посіб. Ч.1 / [Є.О. Живило]; за ред. Є.О. Живило. – П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. – 134 с.
3. Тестування на проникнення: навч. посіб. Ч.2 / [Є.О. Живило]; за ред. Є.О. Живило. – П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. – 239 с.
4. Яцків В.В., Яцків Н.Г., Возняк С.І., Кондратюк В.М. Методика виконання тестів на проникнення з використання MITRE ATT&CK. Інформатика та математичні методи в моделюванні. 2025. Том 15, № 2. – С. 288-297. DOI 10.15276/imms.v15.no2.288
5. OSSTMM 3 – The Open Source Security Testing Methodology Manual. https://www.isecom.org/OSSTMM.3.pdf
6. BSI - Study A Penetration Testing Model. Federal Office for Information Security, 111p. Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html
7. Vulnerability Scanning Tools. Режим доступу: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
8. PTES Technical Guidelines. http://www.pentest-standard.org/index.php/Exploitation
9. MITRE ATT&CK Documentation. https://attack.mitre.org
10. Isozaki, I., Shrestha, M., Console, R., & Kim, E. (2025, June). Towards automated penetration testing: Introducing llm benchmark, analysis, and improvements. In Adjunct Proceedings of the 33rd ACM Conference on User Modeling, Adaptation and Personalization, pp. 404-419.
11. 12 Types of social engineering attacks. Режим доступу: https://www.trendmicro.com/en_no/what-is/social-engineering/types-of-social-engineering-attacks.html
12. Що таке соціальна інженерія в кібербезпеці? Реальні приклади та методи запобігання. Режим доступу: https://hideez.com/uk-ua/blogs/news/social-engineering?srsltid=AfmBOooW2bDba7-SY8L7kkJavAw09QkjtAQs9jvt6QlAr1KGFSU3l_Dl

13. Hashcat. Режим доступу: https://hashcat.net/wiki/doku.php?id=hashcat
14. Hydra. Режим доступу: https://hackviser.com/tactics/tools/hydra
15. 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
16. Zigbee Security 101 (Architecture And Security Issues). Режим доступу: https://payatu.com/blog/zigbee-security-101-architecture-and-security-issues/
17. Barrera, D., Bellman, C., & Van Oorschot, P. (2023). Security best practices: a critical analysis using IoT as a case study. ACM Transactions on Privacy and Security, 26(2), 1-30.
18. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
19. Закон України «Про інформацію». Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
20. Закон України «Про захист персональних даних». Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Оцінювання

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 1-6.	Підсумкове тестування за темами №1-15.	Визначається як середнє арифметичне з оцінок за виконання трьох завдань тренінгу.	Оцінка виставляється за виконання наскрізного завдання.	1. Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів

Шкала оцінювання

За шкалою університуту	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75–84		C (добре)
65–74	задовільно	D (задовільно)
60–64		E (достатньо)
35–59	незадовільно	FX (незадовільно з можливістю повторного складання)
1–34		F (незадовільно з обов'язковим повторним курсом)