# Силабус курсу
# ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

**Ступінь вищої освіти –** бакалавр
**Рік навчання: 4**
**Семестр**: 7
**Кількість кредитів: 5**
**Мова викладання:** українська

## Керівник курсу


**ПІП** Сергій ВОЗНЯК
**Контактна інформація** sv@wunu.edu.ua


## Опис дисципліни

Метою дисципліни «Тестування на проникнення» є - отримання знань та умінь, які необхідні для проведення тестування комп'ютерних систем на проникнення. Основне завдання дисципліни дати студентам теоретичну та практичну підготовку з виконання тестів на проникнення.

## Структура курсу

| Години лек/пр | Тема | Результати навчання | Завдання |
|---|---|---|---|
| 2/2 | Безпека ІТ та тестування на проникнення | Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах | Поточне опитування |
| 2/2 | Види тестування на проникнення | Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту | Поточне опитування |
| 2/2 | Класифікація та цілі проникнення | Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки | Поточне опитування |
| 2/2 | Юридичні питання тестування на проникнення | Розуміння юридичних причинитестування на | Поточне опитування |

| | | | |
|---|---|---|---|
| | | проникнення, їх правових рамок та важливих умови договору між тестером на проникнення та клієнтом. Усвідомлення обов'язків тестера та обмеження відповідальності. | |
| 3/2 | Загальні вимоги до тестування на проникнення | Розуміння організаційних вимог, вимог до персоналу та технічних вимог тестування на проникнення. Визначення етичних питанн. | Поточне опитування |
| 4/2 | Методика тестування на проникнення | Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів | Поточне опитування |
| 4/8 | Виконання тестів на проникнення | Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно телекомунікаційних систем | Поточне опитування |
| 4/10 | Тестування на проникнення інфраструктури | Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно телекомунікаційних системах | Поточне опитування |
| 4/4 | Написання звітів | Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно телекомунікаційних системах | Поточне опитування |
| 4/6 | Збір інформації | Використовувати інструментарій для моніторингу процесів в інформаційно телекомунікаційних системах | Поточне опитування |
| 4/6 | Сканування портів | Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно телекомунікаційних системах | Поточне опитування |
| 4/6 | Сканування вразливостей | Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно телекомунікаційних системах | Поточне опитування |

**Рекомендовані джерела інформації**

1. Mamilla, Sushmitha Reddy. A Study of Penetration Testing Processes and Tools. 2021. https://scholarworks.lib.csusb.edu/etd/1220

2. 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

3. 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.

4. 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.

5. 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.

6. Vulnerability Scanning Tools. https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

7. PTES Technical Guidelines. http://www.pentest-standard.org/index.php/Exploitation

8. 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.

9. ASAAD, Renas R. Penetration testing: Wireless network attacks method on Kali Linux OS. *Academic Journal of Nawroz University*, 2021, 10.1, pp.7-12

10. Yaacoub, Jean-Paul A., et al. A Survey on Ethical Hacking: Issues and Challenges. arXiv preprint arXiv:2103.15072, 2021.

11. Alanda, Alde, et al. Web Application Penetration Testing Using SQL Injection Attack. *JOIV: International Journal on Informatics Visualization*, 2021, 5.3, pp. 320-326

12. 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

13. High Level Organization of the Standard. http://www.pentest-standard.org/index.php/Exploitation

## 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 – max 6*4=24 балів.<br>2. Письмова робота – max 52 балів.<br>3. Практичне завдання – max 3*8=24 балів | 1. Усне опитування на заняттях – max 6*4=24 балів.<br>2. Письмова робота – max 52 балів.<br>3. Практичне завдання – max 3*8=24 балів | 1. Підготовка КПІЗ – max 30 балів.<br>2. Захист КПІЗ – max 40 балів.<br>3. Оцінка за тренінг – max 30 балів | 1. Розв'язання 20 тестів по 3 бали = max 60 балів.<br>2. Практичне 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 |