Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра інженерії
програмного забезпечення
в енергетиці

ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ПРОНИКНЕННЯ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем в енергетиці*
Статус дисципліни	*Вибіркова*
Форма навчання	*Заочна*
Рік підготовки, семестр	*4-й курс, 1-й семестр*
Обсяг дисципліни	*4 кред. /120 год. (заочна форма: лекцій 6 год., лаб. 4 год., СРС 110 год.)*
Семестровий контроль/ контрольні заходи	*Залік, модульна контрольна робота*
Розклад занять	*http://schedule.kpi.ua/*
Мова викладання	*Українська/Англійська*
Інформація про керівника курсу / викладачів	Лектор: *д. е. н., професор Сігайов Андрій Олександрович* Практичні / Семінарські: Лабораторні: *Сігайов А. О.*
Розміщення курсу	GitHub Classroom, eCampus

Програма навчальної дисципліни

1 Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Чому майбутньому фахівцю варто вчити саме цю дисципліну?

З переважанням постійного підключення до Internet і досягнень в технологіях, які доступні на сьогодні, кіберзагрози швидко розвиваються для експлуатації різних аспектів цих технологій. Будь-який пристрій є вразливим для атаки, а з появою концепції "інтернету речей" (IoT) це стало реальністю.

За минулі роки інвестиції у сферу забезпечення безпеки перейшли з розряду "nice to have" в розряд "must have", і тепер організації по всьому світу розуміють, наскільки важливо постійно інвестувати в безпеку. Ці інвестиції забезпечать конкурентоспроможність компанії на ринку. Нездатність належним чином захистити свої ресурси може призвести до непоправних збитків, а в деяких випадках — до банкрутства. За нинішнього ландшафту кіберзагроз недостатньо інвестувати тільки в захист. Компанії повинні покращувати загальну стратегію безпеки, а це означає, що інвестиції в захист, виявлення і реагування повинні бути узгоджені.

Мета дисципліни. *Ознайомити студентів з сучасним станом інформаційної безпеки у кібер-енергетичних системах.*

Предмет дисципліни. *Огляд інформаційної безпеки, включаючи поточний ландшафт кіберзагроз, виклики простору кібербезпеки, як поліпшити свою стратегію безпеки, ролі Синьої та Червоної команд в установі.*

Очікувані результати навчання.

Фахові компетентності.

ФК 6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

Програмні результати навчання.

ПРН 30. Аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

ПРН 31. Реалізовувати застосунки корпоративних систем з інформаційної безпеки програм і даних, зокрема, в кібер-фізичних та енергетичних системах.

2 Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Дисципліна вивчається у сьомому семестрі. Пререквізитів у даного курсу на бакалаврському рівні немає. Постреквізитів у даного курсу на бакалаврському рівні немає.

3 Зміст навчальної дисципліни

1. *Як зламати вебсайт.*
2. *Як працює Інтернет.*
3. *Як працюють браузери.*
4. *Як працюють вебсервери.*
5. *Як працюють програмісти.*
6. *Ін'єкційні атаки.*
7. *Атаки міжсайтового скриптингу.*
8. *Атаки міжсайтової підробки запиту.*
9. *Компрометація аутентифікації.*
10. *Перехоплення сесій.*
11. *Дозволи.*
12. *Витоки інформації.*
13. *Шифрування.*
14. *Сторонній код.*
15. *Атаки XML.*
16. *Не будьте інструментом в чужих руках.*
17. *Атаки відмови у обслуговування.*
18. *Підсумкові роздуми.*

4 Навчальні матеріали та ресурси

Базова література:

McDonald, M. Web Security for Developers: San Francisco, CA: No Starch Press, 2020. 216 c. URL: http://gen.lib.rus.ec/book/index.php?md5=C07B7DD841D0F7180C06E08A8AF9D553

Додаткова література:

1. *Clark, B. RTFM: Red Team Field Manual: CreateSpace Independent Publishing Platform, 2014. 96 c. URL: http://libgen.rs/book/index.php?md5=4e34290b25a81c1132b46be57d181ad4*

2. *White, A. J., Clark, B. Blue Team Field Manual: CreateSpace Independent Publishing Platform, 2017. 134 c. URL: http://libgen.rs/book/index.php?md5=51e0448ce4f9757f6939d74508bfee6d*
3. *Hack The Box :: Penetration Testing Labs: URL: https://www.hackthebox.com*
4. *The Enigma Group: URL: https://www.enigmagroup.org/*
5. *HackThisSite: URL: https://www.hackthissite.org/*
6. *Vulnerable By Design ~ VulnHub: URL: https://www.vulnhub.com/*
7. *Raienko, N. enaqx/awesome-pentest: 2021. URL: https://github.com/enaqx/awesome-pentest*
8. *vitalysim/Awesome-Hacking-Resources: 2021. URL: https://github.com/vitalysim/Awesome-Hacking-Resources*
9. *OlivierLaflamme/Cheatsheet-God: 2021. URL: https://github.com/OlivierLaflamme/Cheatsheet-God*
10. *Pwn Adventure 3: Pwnie Island: URL: http://www.pwnadventure.com/*
11. *PentesterLab: Learn Web Penetration Testing: The Right Way: URL: https://pentesterlab.com/*
12. *Seitz, J., Arnold, T. Black Hat Python: Python Programming for Hackers and Pentesters: San Francisco, CA: No Starch Press, 2021. 216 c. URL: http://libgen.rs/book/index.php?md5=FA5CF2BDA4AFD01B888D2FD8BD04888B*
13. *Davis, R. The Art of Network Penetration Testing: How to take over any company in the world: Shelter Island, NY: Manning Publications, 2020. 304 c. URL: http://libgen.rs/book/index.php?md5=1F7DE7879D5686BD9F91B22530EE485F*
14. *Pruteanu, A. Becoming the Hacker: The Playbook for Getting Inside the Mind of the Attacker: Birmingham, UK: Packt Publishing, 2019. 404 c. URL: http://libgen.rs/book/index.php?md5=6A6D404D4403C482D68AF38A92BB9AC4*
15. *Yaworski, P. Real-World Bug Hunting: A Field Guide to Web Hacking: San Francisco, CA: No Starch Press, 2019. 264 c. URL: http://libgen.rs/book/index.php?md5=9BDA3D95334A08FCB5F73B17E69DDE05*
16. *Grimes, R. A. Hacking the Hacker: Learn From the Experts Who Take Down Hackers: Indianapolis, IN: Wiley, 2017. 320 c. URL: http://libgen.rs/book/index.php?md5=2361f3ae95017aacaf02d0f94d1dded5*
17. *Parasram, S. V. N., Samm, A., Boodoo, D., ma ін. Kali Linux 2018: Assuring Security by Penetration Testing: Unleash the full potential of Kali Linux 2018, now with updated tools: Birmingham, UK: Packt Publishing, 2018. 528 c. URL: http://libgen.rs/book/index.php?md5=516C794F3B3563E35559261430DA642A*
18. *Davis, R. The Art of Network Penetration Testing: How to take over any company in the world: Shelter Island, NY: Manning Publications, 2020. 304 c. URL: http://libgen.rs/book/index.php?md5=1F7DE7879D5686BD9F91B22530EE485F*
19. *Sikorski, M., Honig, A. Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software: San Francisco, CA: No Starch Press, 2012. 800 c. URL: http://libgen.rs/book/index.php?md5=21F9FDBD90744C6AE0189B9CCDC26BF9*
20. *Eagle, C., Nance, K. The Ghidra Book: The Definitive Guide: San Francisco, CA: No Starch Press, 2020. 608 c. URL: http://libgen.rs/book/index.php?md5=69A5AC5AFB0F64EEBB918468238DF733*

Навчальний контент

5 Методика опанування навчальної дисципліни (освітнього компонента)

1. *Злам вебсайтів.*
    - 1.1. *Програмні експойти.*
    - 1.2. *Як зламати вебсайт.*
2. *Як працює Інтернет.*
    - 2.1. *Інтернет-протокол.*
        - 2.1.1. *Адреси мережі Інтернет.*
        - 2.1.2. *Система доменних імен.*
    - 2.2. *Протоколи рівня застосунку.*
        - 2.2.1. *Гіпертекстовий протокол.*
    - 2.3. *З'єднання з підтримкою стану.*
    - 2.4. *Шифрування.*
    - 2.5. *Підсумки.*
3. *Як працюють браузери.*
    - 3.1. *Рендерінг вебсторінки.*
        - 3.1.1. *Конвеєр рендерінгу.*
        - 3.1.2. *Документна об'єктна модель.*
        - 3.1.3. *Стилі відображення інформації.*
    - 3.2. *JavaScript.*
    - 3.3. *До та після рендерінгу: що ще робить браузер.*
    - 3.4. *Підсумки.*
4. *Як працюють вебсервери.*
    - 4.1. *Статичні та динамічні ресурси.*
    - 4.2. *Статичні ресурси.*
        - 4.2.1. *Резолюція URL.*
        - 4.2.2. *Мережі доставлення контенту.*
        - 4.2.3. *Системи управління контентом.*
    - 4.3. *Динамічні ресурси.*
        - 4.3.1. *Шаблони.*
        - 4.3.2. *Бази даних.*
        - 4.3.3. *Розподілені кеші.*
        - 4.3.4. *Мови програмування вебу.*
    - 4.4. *Підсумки.*
5. *Як працюють програмісти.*
    - 5.1. *Фаза 1: дизайн і аналіз.*
    - 5.2. *Фаза 2: написання коду.*

15.5.4. Java.

15.5.5. .NET.

15.6. Інші міркування.

15.7. Підсумки.

16. Не будьте інструментом в чужих руках.

16.1. Шахрайство з Email.

16.1.1. Використовуйте Sender Policy Framework.

16.1.2. Використовуйте DomainKeys Identified Mail.

16.1.3. Убезпечення вашої Email: практичні кроки.

16.2. Приховування зловмисних посилань у листах.

16.2.1. Open Redirect.

16.2.2. Запобігання Open Redirect.

16.2.3. Інші міркування.

16.3. Clickjacking.

16.3.1. Запобігання Clickjacking.

16.4. Підробка запитів на стороні сервера.

16.4.1. Захист від Server-Side Request Forgery.

16.5. Ботнети.

16.6. Захист від інфікування зловмисним програмним забезпеченням.

16.7. Підсумки.

17. Атаки відмови в обслуговуванні (DoS).

17.1. Типи Denial-of-Service Attacks.

17.1.1. Атаки на Internet Control Message Protocol (ICMP).

17.1.2. Атаки на Transmission Control Protocol (TCP).

17.1.3. Атаки на Application Layer (HTTP).

17.1.4. Відображені та підсилені атаки.

17.1.5. Атаки Distributed Denial-of-Service (DDoS).

17.1.6. Ненавмисні атаки DoS.

17.2. Нейтралізація наслідків атаки відмови у обслуговуванні.

17.2.1. Файерволи та системи запобігання вторгненню.

17.2.2. Сервіси захисту від DDoS.

17.2.3. Масштабування.

18. Прикінцеві роздуми.

6 Самостійна робота студента/аспіранта

Студент витрачатиме 4 години на тиждень на самостійну роботу з матеріалом курсу.

Політика та контроль

7 Політика навчальної дисципліни (освітнього компонента)

Студенти отримують бали за правильне та вчасне виконання лабораторних робіт. Загальний рейтинг (кількість балів) складається з: 1) лабораторних робіт (у формі практичних завдань з програмування) та МКР 60%, 2) заліку 40%.
Наразі в курсі наявні три лабораторні роботи, кожне оцінюється до 20 балів. Студент повинен здати правильно виконану лабораторну роботу протягом двох тижнів з дня видачі завдання для отримання повної кількості балів, в іншому випадку застосовуються штрафні бали не більше 40% від загальної кількості за лабораторну роботу.

8 Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: МКР, лабораторні роботи
Календарний контроль: заочною формою навчання не передбачений.
Семестровий контроль: залік
Умови допуску до семестрового контролю: зарахування усіх лабораторних робіт, семестровий рейтинг не менше 40 балів.
Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менш як 60	Незадовільно
Не виконані умови допуску	Не допущено

9 Додаткова інформація з дисципліни (освітнього компонента)

- *перелік питань, які виносяться на семестровий контроль (див. додаток до силабусу).*

Робочу програму навчальної дисципліни (силабус):

Складено Професор кафедри інженерії програмного забезпечення в енергетиці, д.е.н., професор А. О. Сігайов

Ухвалено кафедрою інженерії програмного забезпечення в енергетиці (протокол № 28 від 15 травня 2023 р.)

Погоджено Методичною комісією Навчально-наукового інституту атомної і теплової енергетики КПІ ім. Ігоря Сікорського (протокол № 9 від 26 травня 2023 р.)