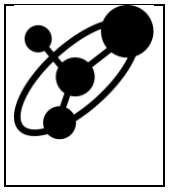
Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»



Software Engineering in
Energy Industry Department

PENETRATION TESTING

Syllabus

Catalog Description

Higher education level	***First (Undergraduate)***
Knowledge field	*Information Technologies*
Profession	*121 Software Engineering*
Curriculum	*Software Engineering of Intelligent Cyberphysical Systems in Energy Industry*
Course status	*Elective*
Form of training	*Full-time*
Grade, term	*Fourth grade, fall semester*
Credits (hours)	*4 credits / 120 hours (full time: 36 hours of lectures, 18 hours of practice, 66 hr of individual assignments*
Term control	*Exam, modular test*
Schedule	*http://schedule.kpi.ua/*
Teaching language	*Ukrainian/English*
Instructors	Lecturer: *DSc. (Econ), professor Andrii Sihaiov* Seminars: Laboratory work: *Andrii Sihaiov*
URL	GitHub Classroom, eCampus

Course Program

1 Course description, aim, subject, and expected outcomes

Why future specialist should study this course?

With the prevalence of always-on connectivity and advancements in technology that is available today, threats are evolving rapidly to exploit different aspects of these technologies. Any device is vulnerable to attack, and with Internet of Things (IoT) this became a reality.

Over the years, the investments in security moved from nice to have to must have, and now organizations around the globe are realizing how important it is to continually invest in security. This investment will ensure that a company remains competitive in the market. Failure to properly secure their assets could lead to irreparable damage, and in some circumstances could lead to bankruptcy. Due to the current threat landscape, investing in protection alone isn't enough. Organizations must enhance their overall security posture. This means that the investments in protection, detection, and response must be aligned.

Course Aim. *To familiarize students with modern state of information security in cyber-energetic systems.*

Course Subject. *An overview of information security, including current threat landscape, the challenges in the cybersecurity space, how to enhance your security posture, and understanding the roles of the Blue Team and Red Team in organization.*

Expected Outcomes.

Professional Competencies.

PC 6. Ability to analyze, choose and apply methods and tools to ensure information security (including cybersecurity).

Program Learning Outcomes.

PLO 30. Analyze, select, and competently apply means of ensuring information security (including cybersecurity) and data integrity in accordance with the applied tasks being solved and the software systems being created.

PLO 31. Implement applications of corporate systems for information security of programs and data, in particular, in cyber-physical and energy systems.

2 Course prerequisites (Where the course fits into our curriculum)

The course is taken in spring semester of first year. Intertet of Things and Sensor Networks Application Development is the prerequisite. There is no required course that has this course as a prerequisite.

3 Course contents

1. *Let's Hack a Website.*
2. *How the Internet Works.*
3. *How Browsers Work.*
4. *How Web Servers Work.*
5. *How Programmers Work.*
6. *Injection Attacks.*
7. *Cross-Site Scripting Attacks.*
8. *Cross-Site Request Forgery Attacks.*
9. *Compromising Authentication.*
10. *Session Hijacking.*
11. *Permissions.*
12. *Information Leaks.*
13. *Encryption.*
14. *Third-Party Code.*
15. *XML Attacks.*
16. *Don't Be an Accessory.*
17. *Denial-of-Service Attacks.*
18. *Summing Up.*

4 Course textbooks and materials

Required reading:

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

Optional reading:

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*

Educational Content

5 Pedagogical advice

1. *Let's Hack a Website.*
   - 1.1. *Software Exploits and the Dark Web.*
   - 1.2. *How to Hack a Website.*
2. *How the Internet Works.*

16.2. Disguising Malicious Links in Email.

16.2.1. Open Redirects.

16.2.2. Preventing Open Redirects.

16.2.3. Other Considerations.

16.3. Clickjacking.

16.3.1. Preventing Clickjacking.

16.4. Server-Side Request Forgery.

16.4.1. Protecting Against Server-Side Forgery.

16.5. Botnets.

16.5.1. Protecting Against Malware Infection.

16.6. Summary.

17. Denial-of-Service Attacks.

17.1. Denial-of-Service Attack Types.

17.1.1. Internet Control Message Protocol Attacks.

17.1.2. Transmission Control Protocol Attacks.

17.1.3. Application Layer Attacks.

17.1.4. Reflected and Amplified Attacks.

17.1.5. Distributed Denial-of-Service Attacks.

17.1.6. Unintentional Denial-of-Service Attacks.

17.2. Denial-of-Service Attack Mitigation.

17.2.1. Firewalls and Intrusion Prevention Systems.

17.2.2. Distributed Denial-of-Service Protection Services.

17.2.3. Building for Scale.

17.3. Summary.

18. Summing Up.

6 Individual Assignments

Students are expected to spend 4 hours a week outside of class on course material.

Політика та контроль

7 Course study rules

Students receive points relative to the correct and timely completion of coursework. The total grade consists of: 1) laboratories (programming assignments) and modular test 60%, 2) final exam 40%.
Presently there are three programming assignments, each worth up to 20% of the total grade. Student have to submit correctly fulfilled assigdnment during fortnight period from the date of give out to obtain full score for it, otherwise penalty points are applied but not more than 40% of the total score for laboratory work.

8 Assessment policy

How students are assessed: modular test, programming assignments

Calendar control: conducted twice a term to monitor the current state of compliance with the requirements of the syllabus.
Term assessment: final exam
Term assessment admission condition: all programming assignment submission, start score not less than 40 points.
Exam scores map to the course grade according to the table:

Score	*Grade*
100-95	Excellent
94-85	Very Good
84-75	Good
74-65	Satisfactory
64-60	Sufficient
Less than 60	Unsatisfactory
Conditions for exam admission not met	Not allowed

9 Additional topics

- *Exam questions (see appendix).*

Syllabus:

Developed by Software Engineering in Energy Industry Department Professor, Sc. D. Andrii Sihaiov

Approved by Software Engineering in Energy Industry Department (minutes #28 on May 15, 2023)

Endorsed by Methodical Commission of Heat Power Faculty (minutes #9 on May 26, 2023)