



PENETRATION TESTING

Syllabus

Catalog Description

Higher education level	<i>First (Undergraduate)</i>
Knowledge field	<i>Information Technologies</i>
Profession	<i>121 Software Engineering</i>
Curriculum	<i>Software Engineering of Intelligent Cyberphysical Systems in Energy Industry</i>
Course status	<i>Elective</i>
Form of training	<i>Part-time</i>
Grade, term	<i>Fourth grade, fall semester</i>
Credits (hours)	<i>4 credits / 120 hours (part time: 6 hours of lectures, 4 hours of practice, 110 hours of individual assignments)</i>
Term control	<i>Exam, modular test</i>
Schedule	<i>http://schedule.kpi.ua/</i>
Teaching language	<i>Ukrainian/English</i>
Instructors	Lecturer: <i>DSc. (Econ), professor Andrii Sihaiov</i> Seminars: Laboratory work: <i>Andrii Sihaiov</i>
URL	<i>GitHub Classroom, eCampus</i>

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.

FC 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. Intertel 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., та ин. 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.*

- 2.1. *The Internet Protocol Suite.*
 - 2.1.1. *Internet Protocol Addresses.*
 - 2.1.2. *The Domain Name System.*
- 2.2. *Application Layer Protocols.*
 - 2.2.1. *HyperText Transfer Protocol.*
- 2.3. *Stateful Connections.*
- 2.4. *Encryption.*
- 2.5. *Summary.*
- 3. *How Browsers Work.*
 - 3.1. *Web Page Rendering.*
 - 3.1.1. *The Rendering Pipeline: An Overview.*
 - 3.1.2. *The Document Object Model.*
 - 3.1.3. *Styling Information.*
 - 3.2. *JavaScript.*
 - 3.3. *Before and After Rendering: Everything Else the Browser Does.*
 - 3.4. *Summary.*
- 4. *How Web Servers Work.*
 - 4.1. *Static and Dynamic Resources.*
 - 4.2. *Static Resources.*
 - 4.2.1. *URL Resolution.*
 - 4.2.2. *Content Delivery Networks.*
 - 4.2.3. *Content Management Systems.*
 - 4.3. *Dynamic Resources.*
 - 4.3.1. *Templates.*
 - 4.3.2. *Databases.*
 - 4.3.3. *Distributed Caches.*
 - 4.3.4. *Web Programming Languages.*
 - 4.4. *Summary.*
- 5. *How Programmers Work.*
 - 5.1. *Phase 1: Design and Analysis.*
 - 5.2. *Phase 2: Writing Code.*
 - 5.2.1. *Distributed vs. Centralized Version Control.*
 - 5.2.2. *Branching and Merging Code.*
 - 5.3. *Phase 3: Pre-Release Testing.*
 - 5.3.1. *Coverage and Continuous Integration.*
 - 5.3.2. *Test Environments.*
 - 5.4. *Phase 4: The Release Process.*

- 5.4.1. *Options for Standardized Deployment During Releases.*
 - 5.4.2. *The Build Process.*
 - 5.4.3. *Database Migration Scripts.*
- 5.5. *Phase 5: Post-Release Testing and Observation.*
 - 5.5.1. *Penetration Testing.*
 - 5.5.2. *Monitoring, Logging, and Error Reporting.*
- 5.6. *Dependency Management.*
- 5.7. *Summary.*
- 6. *Injection Attacks.*
 - 6.1. *SQL Injection.*
 - 6.1.1. *What Is SQL?*
 - 6.1.2. *Anatomy of a SQL Injection Attack.*
 - 6.1.3. *Mitigation 1: Use Parameterized Statement.*
 - 6.1.4. *Mitigation 2: Use Object-Relational Mapping.*
 - 6.1.5. *Bonus Mitigation: Use Defense in Depth.*
 - 6.2. *Command Injection.*
 - 6.2.1. *Anatomy of a Command Injection Attack.*
 - 6.2.2. *Mitigation: Escape Control Characters.*
 - 6.3. *Remote Code Execution.*
 - 6.3.1. *Anatomy of a Remote Code Execution Attack.*
 - 6.3.2. *Mitigation: Disable Code Execution During Deserialization.*
 - 6.4. *File Upload Vulnerabilities.*
 - 6.4.1. *Anatomy of a File Upload Attack.*
 - 6.4.2. *Mitigations.*
 - 6.5. *Summary.*
- 7. *Cross-Site Scripting Attacks.*
 - 7.1. *Stored Cross-Site Scripting Attacks.*
 - 7.1.1. *Mitigation 1: Escape HTML Characters.*
 - 7.1.2. *Mitigation 2: Implement a Content Security Policy.*
 - 7.2. *Reflected Cross-Site Scripting Attacks.*
 - 7.2.1. *Mitigation: Escape Dynamic Content from HTTP Requests.*
 - 7.3. *DOM-Based Cross-Site Scripting Attacks.*
 - 7.3.1. *Mitigation: Escaping Dynamic Content from URI Fragments.*
 - 7.4. *Summary.*
- 8. *Cross-Site Request Forgery Attacks.*
 - 8.1. *Anatomy of a CSRF Attack.*
 - 8.2. *Mitigation 1: Follow REST Principles.*

- 8.3. *Mitigation 2: Implement Anti-CSRF Cookies.*
- 8.4. *Mitigation 3: Use the SameSite Cookie Attribute.*
- 8.5. *Bonus Mitigation: Require Reauthentication for Sensitive Actions.*
- 8.6. *Summary.*
- 9. *Compromising Authentication.*
 - 9.1. *Implementing Authentication.*
 - 9.1.1. *HTTP-Native Authentication.*
 - 9.1.2. *Non-Native Authentication.*
 - 9.1.3. *Brute-Force Attacks.*
 - 9.2. *Mitigation 1: Use Third-Party Authentication.*
 - 9.3. *Mitigation 2: Integrate with Single Sign-On.*
 - 9.4. *Mitigation 3: Secure Your Own Authentication System.*
 - 9.4.1. *Requiring Usernames, Email Address, or Both.*
 - 9.4.2. *Requiring Complex Passwords.*
 - 9.4.3. *Securely Storing Passwords.*
 - 9.4.4. *Requiring Multifactor Authentication.*
 - 9.4.5. *Implementing and Securing the Logout Function.*
 - 9.4.6. *Preventing User Enumeration.*
 - 9.5. *Summary.*
- 10. *Session Hijacking.*
 - 10.1. *How Sessions Work.*
 - 10.1.1. *Server-Side Sessions.*
 - 10.1.2. *Client-Side Sessions.*
 - 10.2. *How Attackers Hijack Sessions.*
 - 10.2.1. *Cookie Theft.*
 - 10.2.2. *Session Fixation.*
 - 10.2.3. *Taking Advantage of Weak Session IDs.*
 - 10.3. *Summary.*
- 11. *Permissions.*
 - 11.1. *Privilege Escalation.*
 - 11.2. *Access Control.*
 - 11.2.1. *Designing an Authorization Model.*
 - 11.2.2. *Implementing Access Control.*
 - 11.2.3. *Testing Access Control.*
 - 11.2.4. *Adding Audit Trails.*
 - 11.2.5. *Avoiding Common Oversights.*
 - 11.3. *Directory Traversal.*

- 11.3.1. *Filepaths and Relative Filepaths.*
- 11.3.2. *Anatomy of a Directory Traversal Attack.*
- 11.3.3. *Mitigation 1: Trust Your Web Server.*
- 11.3.4. *Mitigation 2: Use a Hosting Service.*
- 11.3.5. *Mitigation 3: Use Indirect File References.*
- 11.3.6. *Mitigation 4: Sanitize File References.*

11.4. *Summary.*

12. *Information Leaks.*

- 12.1. *Mitigation 1: Disable Telltale Server Headers.*
- 12.2. *Mitigation 2: Use Clean URLs.*
- 12.3. *Mitigation 3: Use Generic Cookie Parameters.*
- 12.4. *Mitigation 4: Disable Client-Side Error Reporting.*
- 12.5. *Mitigation 5: Minify or Obfuscate Your JavaScript Files.*
- 12.6. *Mitigation 6: Sanitize Your Client-Side Files.*
- 12.7. *Stay on Top of Security Advisories.*
- 12.8. *Summary.*

13. *Encryption.*

- 13.1. *Encryption in the Internet Protocol.*
 - 13.1.1. *Encryption Algorithms, Hashing, and Message Authentication Codes.*
 - 13.1.2. *The TLS Handshake.*
- 13.2. *Enabling HTTPS.*
 - 13.2.1. *Digital Certificates.*
 - 13.2.2. *Obtaining a Digital Certificate.*
 - 13.2.3. *Installing a Digital Certificate.*
- 13.3. *Attacking HTTP (and HTTPS).*
 - 13.3.1. *Wireless Routers.*
 - 13.3.2. *Wi-Fi Hotspots.*
 - 13.3.3. *Internet Service Providers.*
 - 13.3.4. *Government Agencies.*

13.4. *Summary.*

14. *Third-Party Code.*

- 14.1. *Securing Dependencies.*
 - 14.1.1. *Know What Code You Are Running.*
 - 14.1.2. *Be Able to Deploy New Versions Quickly.*
 - 14.1.3. *Stay Alert to Security Issues.*
 - 14.1.4. *Know When to Upgrade.*

14.2. *Securing Configuration.*

- 14.2.1. *Disable Default Credentials.*
- 14.2.2. *Disable Open Directory Listings.*
- 14.2.3. *Protect Your Configuration Information.*
- 14.2.4. *Harden Test Environments.*
- 14.2.5. *Secure Administrative Frontends.*

14.3. *Securing the Services That You Use.*

- 14.3.1. *Protect Your API Keys.*
- 14.3.2. *Secure Your Webhooks.*
- 14.3.3. *Secure Content Served by Third Parties.*

14.4. *Services as an Attack Vector.*

- 14.4.1. *Be Wary of Malvertising.*
- 14.4.2. *Avoid Malware Delivery.*
- 14.4.3. *Use a Reputable Ad Platform.*
- 14.4.4. *Use SafeFrame.*
- 14.4.5. *Tailor Your Ad Preferences.*
- 14.4.6. *Review and Report Suspicious Ads.*

14.5. *Summary.*

15. *XML Attacks.*

15.1. *The Uses of XML.*

15.2. *Validating XML.*

- 15.2.1. *Document Type Definitions.*

15.3. *XML Bombs.*

15.4. *XML External Entity Attacks.*

- 15.4.1. *How Hackers Exploit External Entities.*

15.5. *Securing Your XML Parser.*

- 15.5.1. *Python.*
- 15.5.2. *Ruby.*
- 15.5.3. *Node .js.*
- 15.5.4. *Java.*
- 15.5.5. *.NET.*

15.6. *Other Considerations.*

15.7. *Summary.*

16. *Don't Be an Accessory.*

16.1. *Email Fraud.*

- 16.1.1. *Implement a Sender Policy Framework.*
- 16.1.2. *Implement DomainKeys Identified Mail.*
- 16.1.3. *Securing Your Email: Practical Steps.*

- 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 assignment 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: not provided for part-time training.

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:

<i>Score</i>	<i>Grade</i>
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)