Syllabus
Course Program

Ethical hacking

Specialty
125 – Cybersecurity and information protection

Institute
Educational and Scientific Institute of Computer Science and Information Technology

Educational program
Cybersecurity

Department
Cybersecurity (328)

Level of education
Bachelor's level

Course type
Profile training, Selective

Semester
4

Language of instruction
English

Lecturers and course developers

Oleksandr MILOV

oleksandr.milov@khpi.edu.ua
Doctor of technical sciences, professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

Author of more than 200 scientific and educational and methodological works. Academic supervisor for protected candidate theses, guarantor of the educational and professional program of the second (master's) level of higher education. Leading lecturer in the disciplines: "Mathematical foundations of cryptology and cryptanalysis", "Data structures", "Industrial and office espionage", "Digital forensics", for undergraduate and graduate students, Section "Methodology of scientific and pedagogical activity in the sciences of cyber protection" for postgraduate students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Ethical hacking" is an optional educational discipline. The study of the discipline provides personal and professional development of the student and is aimed at forming an effective researcher capable of using modern methods of cyberspace research and knowledge transfer. The course examines the methodology of penetration testing and its stages. Separate attention is paid to the creation of penetration reports, as one of the important stages in the evaluation of the security of the information system.

Course objectives and goals

Training of specialists in the field of information security, as well as specialists in ethical hacking, on the basis of mastering the principles and methods of collecting digital information for the study of vulnerabilities of Linux and Windows operating systems, conducting static analysis of vulnerabilities of information systems, using tools and methods of ethical hacking.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control - exam.

Competencies

GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-5. Ability to search, process and analyze information.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
PC-5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy.
PC-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
PC-12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security.

Learning outcomes

LO-1. Apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication;
LO-2. Organize own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness;
LO-3. Use the results of independent search, analysis and synthesis of information from various sources for the effective solution of specialized tasks of professional activity.
LO-4. Analyze, argue, make decisions when solving complex specialized tasks and practical problems in professional activity, which are characterized by complexity and incomplete determination of conditions, be responsible for the decisions made.
LO-5. Adapt under the conditions of frequent changes in the technologies of professional activity, to predict the final result.
LO-6. Critically understand the main theories, principles, methods and concepts in education and professional activity.
LO-7. Act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and/or cyber security.
LO-8. Prepare proposals for regulatory acts on ensuring information and/or cyber security.
LO-9. Implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents.
LO-10. Perform analysis and decomposition of information and telecommunication systems.
LO-11. Perform analysis of connections between information processes on remote computer systems.
LO-12. Develop threat and intruder models.
LO-13. Analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols.
LO-14. Solve the task of protecting programs and information processed in information and telecommunication systems by hardware and software tools and evaluate the effectiveness of the quality of the decisions made.
LO-15. Use modern hardware and software of information and communication technologies.
LO-16. Implement complex information security systems in the automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory and legal documents.
LO-17. Ensure the processes of security and functioning of information and telecommunication (automated) systems based on practices, skills and knowledge, regarding structural (structural-logical) schemes, network topology, modern architectures and models of security of electronic information resources with a reflection of relationships and information flows, processes for internal and remote components.
LO-18. Use software and software-hardware complexes for the security of information resources.

LO-19. Apply theories and methods of protection to ensure information security in information and telecommunication systems.
LO-20. Ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems.
LO-21. Solve tasks of provision and support (including: review, testing, accountability) of the access control system according to the stated security policy in information and telecommunication (automated) systems.
LO-22. Solve the management procedures of identification, authentication, authorization of processes and users in information and telecommunication systems according to the established policy of information and/or cyber security.
LO-23. Implement measures to prevent unauthorized access to information resources and processes in information and telecommunication (automated) systems.
LO-24. Solve the problems of managing access to information resources and processes in information and telecommunication (automated) systems based on access management models (mandatory, discretionary, role-based).
LO-25. Ensure the introduction of accountability of the access management system to electronic information resources and processes in information and telecommunication (automated) systems using event registration logs, their analysis and stated protection procedures.
LO-26. Implement measures and ensure the implementation of processes of prevention of unauthorized access and protection of information, information and telecommunication (automated) systems based on the reference model of interaction of open systems.
LO-27. Solve problems of data flow protection in information and telecommunication (automated) systems.
LO-28. Analyze and evaluate the effectiveness and level of security of resources of various classes in information and telecommunication (automated) systems during tests in accordance with the established policy of information and/or cyber security.
LO-29. Evaluate the possibility of realization of potential threats of information processed in information and telecommunication systems and the effectiveness of the use of complexes of protection means under the conditions of realization of threats of various classes.
LO-30. Assess the possibility of unauthorized access to elements of information and telecommunication systems.
LO-31. Apply protection theories and methods to ensure the security of elements of information and telecommunication systems.
LO-32. Solve the tasks of managing the processes of restoring the regular functioning of information and telecommunication systems using backup procedures in accordance with the stated security policy.
LO-33. Solve the problems of ensuring the continuity of business processes of the organization on the basis of risk management theory.
LO-34. Participate in the development and implementation of an information security and/or cyber security strategy in accordance with the goals and objectives of the organization.
LO-35. Solve the tasks of providing and supporting complex information security systems, as well as countering unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the stated policy of information and/or cyber security.
LO-36. Detect dangerous signals of technical means.
LO-37. Measure the parameters of dangerous and interfering signals during the instrumental control of information security processes and determine the effectiveness of information security against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information security system.
LO-38. Interpret the results of special measurements using technical means, monitoring the characteristics of information and telecommunication systems in accordance with the requirements of regulatory documents of the technical information security system.
LO-39. Carry out attestation (based on accounting and survey) of regime territories (zones), premises, etc. under the conditions of compliance with the secrecy regime, recording the results in the relevant documents.
LO–40. Interpret the results of special measurements using technical means, control of ITS characteristics in accordance with the requirements of regulatory documents of the technical information security system.

LO-41. Ensure the continuity of the event and incident logging process based on automated procedures.
LO-42. Implement processes of detection, identification, analysis and response to information and/or cyber security incidents.
LO-43. Apply national and international regulatory acts in the field of information security and/or cyber security to investigate incidents.
LO-44. Solve the problems of ensuring the continuity of the organization's business processes on the basis of risk management theory and the stated information security management system, in accordance with national and international requirements and standards.
LO-45. Apply early classes of information security and/or cyber security policies based on risk-based access control to information assets.
LO-46. Analyze and minimize the risks of information processing in information and telecommunication systems.
LO-47. Solve the problems of protection of information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information.
LO-48. Implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems.
LO-49. Ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems.
LO-50. Ensure the functioning of software and software-hardware complexes for detecting intrusions of various levels and classes (statistical, signature, statistical-signature).
LO-51. Maintain operational efficiency and ensure configuration of intrusion detection systems in information and telecommunication systems.
LO-52. Use tools for monitoring processes in information and telecommunication systems.
LO-53. Solve problems of software code analysis for the presence of possible threats.
LO-54. Be aware of the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine.

Student workload

The total volume of the course is 90 hours (3 ECTS credits): lectures - 16 hours, laboratory classes - 16 hours, self-study - 58 hours.

Course prerequisites

Mathematical foundations of cryptology, Information security of the state, Basics of programming, Basics of cryptographic protection.

Features of the course, teaching and learning methods, and technologies

In the course of teaching the discipline, the teacher uses explanatory-illustrative (informational-receptive) and reproductive teaching methods. Presentations, conversations, and master classes are used as teaching methods aimed at activating and stimulating the educational and cognitive activities of applicants.

Program of the course

Topics of the lectures

Topic 1. Introduction.
Goals and objectives of the study discipline "Penetration Testing and Ethical Hacking". The place of the discipline in the training process of a cyber security specialist. The structure and content of the thematic plan for studying the discipline; educational and methodical literature. Peculiarities of studying the discipline; forms of control of students' knowledge, abilities and skills. Directions of students' research work.
Topic 2. Vulnerability assessment methodologies.
Basic conditions. Hacking and ethical hacking. What real hackers do. Penetration testing methodology: OSTMM, ISSAF, etc. Penetration testing project management. Hacking Tools Review. Applicable laws. Work with third parties. A question of social engineering. Logging in. Compilation of reports..

Topic 3. Overview of ethical hacking tools.
The Ethical Hacker's Workplace: Kali Linux. Targets: Metasploitable 2, etc. Port scanners. Vulnerability scanners. Operating framework.
Topic 4. Structured approaches to information gathering.
Open source intelligence methods. Overview of methods of structured analysis. Types of information collected: Business information (financial, customers, suppliers, partners). Information about IT infrastructure. Identification of sources of information.
Topic 5. Collection of technical information.
Detection of IP addresses. Tracing Using Maltego. DNS zone transfer. DNS Brutforce.
Topic 6. Analysis of vulnerabilities.
Types of vulnerabilities. Manual search for vulnerabilities. Automatic search for vulnerabilities. Vulnerability analysis tools.
Topic 7. Basic operation of the Metasplot framework.
What is an exploit?Use Google databases for penetration testers: www.exploit-db.com. Local and remote operation. Overview of the Metasploit Platform. Payload types. Man-in-the-middle attacks.
Topic 8. Password attacks.
Password attacks: online and offline. Password hashes. The art of manual password selection. Pass a hash attack.
Topic 9. Operation of web applications.
A typical structure of a Web program. Common web vulnerabilities. OWASP projects. Overview of the OWASP Testing Guide. scrap Google. Hacking the Google Database (GHDB). Web Security Testing Tools. e-scanners. Local proxies. Phasers. Specialized browsers and browser plugins.
Topic 10. Social engineering.
Social engineering. Overview of the "Social Engineering Toolkit" project.
Topic 11. Exploitation using client attacks.
Client-side exploits. Overview of the browser operation infrastructure project.
Topic 12. Access support.
Access technology support. Using an interpreter.
Topic 13. Penetration testing of wireless networks.
Topic 14. Network stress tests.
Network Stress Test (Website DoS) with SlowHTTPTest in Kali Linux: slowloris, slow body and slow read attacks in one tool. Network Stress Test: Website DoS in Kali Linux with GoldenEye. Network stress test with Low Orbit Ion Cannon (LOIC). Network stress test: DoS using hping3 and IP Spoofing in Kali Linux.
Topic 15. Hacking and protection of accounts in social networks.
Targets and executors of hacking accounts. Collection of information. Hacking methods. Email Hacking. Social engineering. Password recovery. Phishing or fake page. Keyboard spy. DNS replacement.
Topic 16. Compiling a report and presenting the results of intrusion testing.
Importance of Penetration Testing Reporting. General Intrusion Report Template. Types of reports and methods of their preparation. A specialist in ethical hacking as a witness. Comparing the roles of experts and technical specialists.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Basic configuration of Kali Linux and Metasploitable 2.
Topic 2: Using Google for OSINT in penetration testing projects. Technical intelligence of IT infrastructure. Using Maltego for Intelligence.
Topic 3. Vulnerability analysis Port scanning. Manual vulnerability assessment. Using vulnerability scanners to assess vulnerabilities. Configuration overview. Special scanning tools.
Topic 4. Exploitation Attack using ARP spoofing. Using the Metasploit command line to exploit vulnerabilities. Using Armitage to exploit vulnerabilities. Attacks on database passwords. Attacks on passwords for various services.
Topic 5. Operation of web applications Scanning of web applications. Choosing a web application password. Executing OS commands through a web server.

Topic 6. Operation of web applications. SQL injection and offline password cracking. Exploitation of XSS vulnerability.
Topic 7. Exploitation Using Client Attacks Client Exploitation with BeEF.
Topic 8. Access support Installation and use of rootkits.

Self-study

A student's independent work is one of the forms of organization of learning, the main form of mastering educational material in free time from classroom training. During independent work, students study lecture material, do individual homework, prepare for tests, tests and exams. Students are also recommended additional materials (videos, articles) for self-study and analysis.

Non-formal education

Within the framework of non-formal education, according to the relevant Regulation (http://surl.li/pxssv), the educational component or its individual topics may be taken into account in the case of independent completion of professional courses/trainings, civic education, online education, vocational training, etc.
In particular, certain topics of this component can be taken into account in case of successful completion of the following CISCO courses:
Ethical Hacker
https://www.netacad.com/catalogs/learn?category=course.

Course materials and recommended reading

Basic literature:

1. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand, 2017, 363 p. 2. Baloch Rafay. Ethical hacking and penetration testing guide. Auerbach Publications, 2017, 523 p.
https://www.tsoungui.fr/ebooks/Ethickal-haking-postexploitation.pdf
2. Yevseyev S.P. Cybersecurity: Laboratory workshop on the basics of cryptographic protection. - Lviv "New World-2000", 2020. - 241 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
3. Bobalo Yu.Ya., Horbaty I.V. (ed.) Information security. Study guide. — Lviv: Publishing House of Lviv Polytechnic, 2019. — 580 p. — ISBN 978-966-941-339-0.
https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf
4. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, O. Milov, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
6. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, O. Milov, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Additional literature:

7. Information protection technologies./ S.E. Ostapov, S.P. Yevseev, O.G. King. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.
http://kist.ntu.edu.ua/textPhD/tzi.pdf
8. Security of Linux operating system: laboratory workshop / S. Yevseiev, S. Pogasiy, A. Goloskokova, O. Shmatko, M. Melnik / S.P. Yevseev, S.S. Pogasiy, A.O. Shmatko, M.O. Melnyk - Lviv: "New World - 2000" Publishing House, 2021. - 256 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Yevseev S.P. Cyber security: basics of coding and cryptography/ S.P. Yevseev, O.V. Milov, S.E. Ostapov, O.V. Severinov. - Kharkiv: Ed. "New World-2000", 2023. - 657 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

10. Ethernet technology: laboratory workshop / M. O. Bilova, S. P. Yevseev, O. S. Zhuchenko, I. S. Ivanchenko, O. V. Shmatko.– Lviv: "Novyi Svit-2000", 2020. - 196 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
11. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010.
https://needuxnworkplace.wordpress.com/wp-content/uploads/2014/01/hacking-exposed-computer-forensics-secrets-solutions.pdf
12. Wilhelm, Thomas. Professional penetration testing: Creating and learning in a hacking lab. Newnes, 2013, 525 p.
http://ppdi.stmik-banjarbaru.ac.id/data.bc/13.%20Hacking/2013%20Professional%20Penetration%20Testing%20Creating%20and%20Learning%20in%20a%20Hacking%20Lab.pdf.

Assessment and grading

Criteria for assessment of student performance, and the final score structure

Points are awarded according to the following ratio:
- laboratory work: 40% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 10% of the semester grade;
- exam: 40% of the semester grade.

Grading scale

Total points	National	ECTS
90–100	Excellent	A
82–89	Good	B
75–81	Good	C
64–74	Satisfactory	D
60–63	Satisfactory	E
35–59	Unsatisfactory (requires additional learning)	FX
1–34	Unsatisfactory (requires repetition of the course)	F

Norms of academic integrity and course policy

The student must adhere to the Code of Ethics of Academic Relations and Integrity of NTU "KhPI": to demonstrate discipline, good manners, kindness, honesty, and responsibility. Conflict situations should be openly discussed in academic groups with a lecturer, and if it is impossible to resolve the conflict, they should be brought to the attention of the Institute's management.
Regulatory and legal documents related to the implementation of the principles of academic integrity at NTU "KhPI" are available on the website: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Approval

Approved by

28.08.2024 — Head of the department
Serhii YEVSEIEV

28.08.2024 — Guarantor of the educational program
Serhii YEVSEIEV