“Халықаралық ақпараттық технологиялар университеті” АҚ

АО “Международный университет информационных технологий”

Faculty of computer Technology and Cybersecurity

Department of Cybersecurity

«APPROVED»
Dean of faculty
Seilova N.A
«_ _ » _____ 2025

WORKING CURRICULUM OF THE DISCIPLINE (SYLLABUS)

Course: Ethical Hacking

Group of educational programsy B058-Information Security

Educational program: 6B06301 – Computer security, 6B06302 - Hardware security, 6B06303 – Network security

Year: 2 **Semester:** 4 **Number of academic credits**: 4

Lectures:	15	hours
Practical work:	15	hours
Laboratory work:	15	hours
IWST:	15	hours
IWS:	60	hours
TOTAL:	120	hours

Cycle of discipline: _____ Basic _____

Form of control: Test in Platonus

Almaty 2025

The working curriculum of the discipline (syllabus) Ethical Hacking has been developed based on basis of the educational program 6B06301 – Computer security, 6B06302 - Hardware security, 6B06303 – Network security

The academic program has been reviewed at the meeting of the "Cybersecurity" department.

The working curriculum of the discipline (syllabus) has been reviewed at the meeting of "Cybersecurity" department.

Minutes №. ___ dated «____» _____ 20___

Head of the Department _____ Yeskendirova D.M.

Author **_____** Babenko T.V. DSc., professor

The working curriculum of the discipline (syllabus) was approved at a meeting of the Faculty's Academic Quality Council.

Minutes № _____ dated "___"_____ 20__

Agreed:

Head of the Department of the Educational and Methodological activities	**_____**	**Ajibayeva A.**
Library	**_____**	**Seksenbayeva N**

1. General information	
Faculty	Computer Technology and Cybersecurity
Code and name of the educational program (EP)	B058- Information Security
Program level (bachelor's, master's, PhD)	6B06302 – Hardware security, 6B06301 - Computer security, 6B06303 – Network security
Year, semester	4 year, 8 semester
Name of the discipline	Ethical hacking
Cycle of the discipline	Basic
Number of academic credits	
Prerequisites	4
Postrequisites	Diploma project
Lecturer	Room #401b, 330-85-66 ext. 2039. E-mail: t.babenko@iitu.edu.kz Babenko T.B. DSc., professor
Teachers who conduct practical or laboratory classes	Name, title, position, office address, e-mail, office hours)

2. Goals, objectives and learning outcomes of the course

The primary goal of the course Ethical Hacking is a practice-oriented elective course that introduces students to offensive security methodologies used to identify, exploit, and remediate vulnerabilities in computer systems, networks, and web applications. The course provides a structured foundation that prepares students for future professional certification (EC-Council CEH, Offensive Security OSCP, CompTIA PenTest+) without requiring prior penetration testing experience

The course follows a methodology-first approach: students learn to understand how attacks work before using automated tools. All laboratory work is performed in isolated offline virtual environments (Kali Linux, Metasploitable 2, DVWA) on students' personal laptops, requiring no specialised hardware and no continuous internet connection.

The course is designed with awareness of challenging learning conditions, including unstable power and internet connectivity. All labs are modular, interruptible, and can be completed in short independent segments. The core toolkit is deliberately limited to reduce cognitive overload while maintaining professional relevance

Course Objectives

The course is structured to achieve the following objectives:

1. Knowledge

- Introduce the fundamental concepts of ethical hacking, including the penetration testing lifecycle, attack vectors, and the distinction between authorised and unauthorised security testing.
- Explain the legal and ethical frameworks governing penetration testing, including the Criminal Code of the Republic of Kazakhstan, the US CFAA, and the EU GDPR.
- Provide understanding of reconnaissance techniques, network scanning principles, service enumeration, and vulnerability identification methodologies.
- Familiarise students with common exploitation techniques, privilege escalation mechanisms, and web application vulnerabilities (OWASP Top 10).

2. *Skills*

- Develop the ability to configure and manage isolated virtual lab environments for safe penetration testing practice.

- Apply industry-standard tools (Nmap, Netcat, Metasploit, Burp Suite, Wireshark) to perform network scanning, manual service interaction, exploitation, and traffic analysis.
- Use manual techniques (banner grabbing, protocol analysis, CVE research) to understand how vulnerabilities and exploits work at a fundamental level before relying on automated frameworks.
- Employ systematic vulnerability assessment and basic exploitation techniques to identify and demonstrate security weaknesses in controlled environments.

3. *Competencies*

- Demonstrate critical thinking in analysing systems, identifying attack vectors, and evaluating risk within the penetration testing lifecycle.
- Integrate theoretical knowledge of offensive security with practical hands-on tasks aligned with industry certification requirements (CEH, OSCP, PenTest+).
- Communicate technical findings effectively through professional penetration testing reports with risk ratings, remediation recommendations, and executive summaries.
- Prepare for further specialisation in penetration testing, red teaming, digital forensics, or related cybersecurity career paths.

Learning Outcomes

Upon successful completion of the course, students will be able to:

1. Understand the legal and ethical framework governing penetration testing (CEH Domain 1; CompTIA PenTest+ Domain 1).
2. Conduct systematic reconnaissance using OSINT techniques and network scanning with Nmap (CEH Domains 2–4).
3. Manually interact with network services to understand protocols before using automated tools (pre-OSCP foundational skill).
4. Identify vulnerabilities using Nmap NSE scripts, Nikto, and manual CVE analysis (CEH Domains 5–6; CompTIA PenTest+ Domain 2).
5. Exploit common vulnerabilities using Metasploit Framework and basic manual techniques (OSCP core; CEH Domains 7–8).
6. Perform basic post-exploitation: privilege escalation via SUID binaries and sudo misconfigurations (pre-OSCP level).
7. Detect and exploit web application vulnerabilities (OWASP Top 10) using Burp Suite and manual techniques (CEH Domain 14).
8. Understand red team concepts: social engineering theory, adversary simulation, and MITRE ATT&CK mapping (CEH Domains 9–11).
9. Document findings in a professional penetration testing report following PTES standards

Competencies

By completing this course, students will develop the following competencies:

1. Professional competency: Ability to conduct basic authorised security assessments following industry methodology.
2. Critical thinking: Ability to analyse systems, identify common attack vectors, and evaluate risk.
3. ICT competency: Proficiency with virtualisation, Linux CLI, and a focused set of security tools (Nmap, Netcat, Metasploit, Burp Suite, Wireshark).
4. Communication competency: Ability to produce clear penetration testing reports for technical and executive audiences.

5. Ethical competency: Understanding of legal boundaries, responsible disclosure, and professional codes of conduct

3. Course description

The course follows a structured skill progression: students first understand services and protocols manually, then learn to identify vulnerabilities, and only then use exploitation frameworks. This methodology-first approach ensures genuine understanding rather than tool dependency

Module	Title	Topics
I	*Foundations (Weeks 1–3)*	Ethics, law, and methodology; lab environment setup; scanning and service discovery; threat modelling; MITRE ATT&CK overview; guided exploitation activity demonstrating the relationship between service discovery and vulnerability exploitation
II	*Reconnaissance and Manual Interaction (Weeks 4–6)*	Nmap scanning; service enumeration; manual banner grabbing with Netcat; understanding raw protocols; vulnerability identification with Nmap NSE and Nikto; manual CVE analysis
III	*Exploitation and Post-Exploitation (Weeks 8–10)*	Metasploit exploitation (after manual foundation); password attacks; basic privilege escalation (SUID binaries, sudo misconfigurations only); pivoting concepts
IV	*Web Security and Reporting (Weeks 11–14)*	OWASP Top 10; SQL injection; XSS; CSRF; Burp Suite; network traffic analysis with Wireshark; social engineering theory; MITRE ATT&CK adversary mapping; professional pentest reporting
V	*Midterm Assessments (Weeks 7, 15)*	Week 7: Midterm 1 — CTF + Platonus quiz (Modules I–II). Week 15: Midterm 2 — CTF + Platonus quiz (Modules III–IV).

3.1 Core Toolkit

To reduce cognitive overload, the course focuses on five core tools. Students must demonstrate proficiency with these before any additional tools are introduced:

Tool	Purpose
Nmap	Network scanning, host discovery, service detection, NSE vulnerability scripts
Netcat (nc)	Manual service interaction, banner grabbing, simple reverse/bind shells
Metasploit Framework	Exploitation of known vulnerabilities (introduced only after manual interaction skills are established)
Burp Suite Community	Web application proxy, request interception, manual web vulnerability testing
Wireshark	Network traffic capture and analysis, protocol inspection

Additional tools (John the Ripper/Hashcat for password cracking, Nikto for web server scanning) are used in specific labs but are not required for independent mastery.

Students are assessed on understanding methodology and reasoning, not on memorising tool commands. Tool usage is always evaluated in the context of the penetration testing lifecycle rather than as isolated technical skills

3.2 Offline Lab Environment

All laboratory work is designed to function fully offline after initial VM setup. The instructor provides a pre-prepared lab package containing:

- Kali Linux VM (pre-configured with all required tools)
- Metasploitable 2 VM (intentionally vulnerable target)
- DVWA (Damn Vulnerable Web Application, pre-installed on Metasploitable or separate VM)
- Pre-captured .pcap files for network analysis labs
- Offline copies of all lab instructions (PDF format)

No lab task requires internet access during execution. Online platforms (TryHackMe, HackTheBox) are optional bonus activities only.

4. TEACHING METHODS

The course employs a blended methodology that integrates theoretical instruction with practical application, ensuring that students develop both foundational knowledge and applied skills in Linux system administration.

1. **Interactive lectures:** Concept presentation with live demonstrations using the core toolkit; discussion of real-world case studies; emphasis on methodology before tools. Instructor demonstrations are recorded and provided offline to students for repeated viewing in case of missed sessions due to infrastructure issues.
2. **Modular laboratory work:** All labs are performed offline in isolated VMs. Each lab consists of clearly separated steps with explicit checkpoints ("if you completed this step, you are safe to stop and resume later"). Labs are designed to be completed in 30–40 minute segments to accommodate power interruptions. This structure allows students to recover from interruptions without loss of learning continuity.
3. **Problem-based learning:** Students solve CTF challenges within the offline lab environment, developing problem-solving skills in realistic but controlled contexts.

4. **Independent study (SRO):** Self-guided study of certification materials (CEH, PenTest+); offline lab report preparation; optional online platform challenges (TryHackMe, HackTheBox) for bonus credit.
5. **SROP consultations:** Weekly guided sessions for reviewing lab progress, discussing difficulties, providing individual feedback, and preparing for assessments.

5. COURSE POLICY

Attendance. Attendance is mandatory. If the number of missed classes exceeds 20% of the total contact hours, the student automatically receives a failing grade (F).
Deadlines. All assignments, lab reports, and projects must be submitted by the specified deadlines.
Late Submission Policy. Late submissions are accepted only with prior approval of the instructor for valid documented reasons. Without approval, a grade penalty of up to 10% per day may be applied.
Resubmission and Retake Policy. Retake of missed or failed assessments (quizzes, labs, exams) is allowed only in documented cases of illness, family emergency, or other valid reasons, and must be coordinated with the instructor. Retake conditions are determined individually.
Academic Behavior and Ethics. Students are expected to demonstrate professional conduct, respect towards peers and faculty, and to maintain discipline during all classes. Disruptive behavior will not be tolerated.
Respect for Diversity of Opinions. Discussions in class should be conducted respectfully, recognizing that multiple viewpoints may exist. Any form of harassment or disrespectful comments will result in disciplinary action.
Communication and Ethics of Interaction. Students are expected to use professional and polite language in oral and written communication. Official communication channels include Platonus, MS Teams, and institutional email.
Inclusion and Individual Needs. The course follows the university's inclusion policy. Students with documented individual learning needs, health conditions, or disabilities may request reasonable accommodations in advance.
Exemption from Physical Load (for Physical Education courses only) Not applicable to this course.

6. ACADEMIC INTEGRITY

All students are bound by the IITU Code of Academic Integrity. The following policies apply:

1. Plagiarism policy: Copying lab reports or SRO assignments from other students or online sources is considered plagiarism. First offence: zero for the assignment; second offence: "F" for the course.
2. Collaboration policy: Students may discuss general approaches but must perform all exploitation and analysis independently and submit original reports, unless group work is explicitly designated.
3. AI usage policy: Use of AI tools (ChatGPT, Claude, Copilot, etc.) is permitted only for: (a) explaining concepts and error messages, (b) debugging student-written scripts, (c) improving the language quality of reports. AI must NOT be used to generate lab solutions, exploitation scripts, or report sections. All AI-assisted content must be disclosed. The instructor may conduct oral verification of any submitted work.

7. LITERATURE

Basic literature:

[1] Engebretson, P. (2013). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, 2nd ed. Syngress/Elsevier.

[2] Kennedy, D., O'Gorman, J., Kearns, D. and Aharoni, M. (2011). Metasploit: The Penetration Tester's Guide. No Starch Press.

[3] Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.

[4] Kim, P. (2015). The Hacker Playbook 2: Practical Guide to Penetration Testing. Secure Planet LLC.

[5] Svensson, R. (2016). From Hacking to Report Writing: An Introduction to Security and Penetration Testing. Apress.

[6] Sanders, C. (2017). Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, 3rd ed. No Starch Press

Supplementary literature:

[7] Graham, D. G. (2021). Ethical Hacking: A Hands-On Introduction to Breaking In. No Starch Press.

[8] Baloch, R. (2024). Web Hacking Arsenal: A Practical Guide to Modern Web Pentesting. CRC Press / Taylor & Francis.

[9] Sinha, S. (2021). Beginning Ethical Hacking with Python. Apress.

[10] Regalado, D., Harris, S., Harper, A., Eagle, C. et al. (2018). Gray Hat Hacking: The Ethical Hacker's Handbook, 5th ed. McGraw-Hill Education.

[11] Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking, 2nd ed. Wiley

Open Web Resources

[12] MITRE ATT&CK Framework (2025). https://attack.mitre.org/

[13] OWASP Testing Guide v4.2 (2023). https://owasp.org/www-project-web-security-testing-guide/

[14] PTES — Penetration Testing Execution Standard. http://www.pentest-standard.org/

Online Courses and Platforms (optional)

The following online courses may be used for optional bonus SRO credit. They are NOT mandatory due to internet connectivity requirements:

- TryHackMe — structured learning paths: https://tryhackme.com/ (optional bonus)
- HackTheBox Academy — hands-on training: https://academy.hackthebox.com/ (optional bonus)
- PortSwigger Web Security Academy (free): https://portswigger.net/web-security (optional bonus)
- Cisco Networking Academy — Ethical Hacker: https://www.netacad.com/courses/ethical-hacker

Software (Offline Lab Package)

- VirtualBox (free) — virtualisation platform
- Kali Linux (pre-configured VM image provided by instructor)
- Metasploitable 2 (pre-configured VM image provided by instructor)
- DVWA (pre-installed in lab environment)

– Pre-captured .pcap files (provided by instructor for Wireshark labs)

8. FORMS OF CONTROL AND ASSESSMENT

Period	Assessment Component	Max	Weight
Attestation 1	Laboratory reports (Labs 1–6)	100	30%
	Quizzes / current assessment	100	20%
	SRO 1–2	100	20%
	Midterm 1 (CTF + quiz)	100	30%
Attestation 2	Laboratory reports (Labs 7–13)	100	30%
	Quizzes / current assessment	100	20%
	SRO 3–4	100	20%
	Midterm 2 (CTF + quiz)	100	30%
Final Exam	Platonus test (30%) + Practical CTF (50%) + Written (20%)	100	

9. System for evaluating student performance in a discipline:

Each type of academic activity is graded on a **0–100 scale**. The final grade is calculated as:

Final Grade = 0.3 × (1st Attestation) + 0.3 × (2nd Attestation) + 0.4 × (Final Exam)

Period	Assignment Type	Max Points (per activity)
1st Attestation (Weeks 1–7)	Laboratory works (set of labs during the period)	100
	Current control (set of lecture activities: quizzes, oral questioning, short assignments)	100
	Independent work (SRSP 1 – project/task)	100
	Independent work (SRSP 2 – project/task)	100
	Midterm Control 1 (written/practical test)	100
2nd Attestation (Weeks 8–14)	Laboratory works (set of labs during the period)	100
	Practical classes (set of activities: participation, quizzes, problem-solving)	100
	Current control (set of lecture activities: quizzes, oral questioning, short assignments)	100
	Independent work (SRSP 3 – project/task)	100
	Independent work (SRSP 4 – project/task)	100
	Midterm Control 2 (written/practical test) 2	100
Final Control	Online test in Platonus	100
Final Grade	Calculated as:	0.3 × Attestation 1 + 0.3 × Attestation 2 + 0.4 × Final Exam

Grading Scale

Letter	Score	GPA	Descriptor
A	95–100	4.0	Excellent — comprehensive, deep knowledge

A-	90–94	3.67	Excellent — comprehensive knowledge
B+	85–89	3.33	Good — systematic knowledge, independent development
B	80–84	3.0	Good — systematic knowledge
B-	75–79	2.67	Good — adequate knowledge
C+	70–74	2.33	Satisfactory — basic competency with gaps
C	65–69	2.0	Satisfactory — correctable errors
C-	60–64	1.67	Satisfactory — errors present
D+	55–59	1.33	Satisfactory — minimal competency
D-	50–54	1.0	Satisfactory — bare minimum
FX	25–49	0.5	Unsatisfactory — may retake exam
F	0–24	0	Unsatisfactory — must retake course

10. COURSE SCHEDULE

Wk	Topic	Refs	Lec	Pract	Lab	SROP	SRO
1	Introduction to Ethical Hacking. Legal framework (cyber law of RK, CFAA, GDPR). Penetration testing lifecycle (PTES). Lab setup: Kali Linux + Metasploitable 2 + DVWA in VirtualBox. First scan: discover target with Nmap.	[1][3][14]	1	—	2	1	4
2	Scanning and service discovery. Nmap basics: host discovery, SYN scan, service detection (-sV). Threat modelling basics. MITRE ATT&CK framework overview. Practical: scan Metasploitable 2, identify all open ports and services. Guaranteed visible result: full port/service map.	[1][3][12]	1	—	2	1	4
3	First guided exploitation. Review services found in Week 2. Identify vsftpd 2.3.4 vulnerability (CVE-2011-2523). Exploit with Metasploit (guided	[1][2][3]	1	—	2	1	4

	walkthrough). Interact with the shell. Students see the connection between service discovery and exploitation.						
4	Passive Reconnaissance Concepts and Advanced Scanning Techniques. OSINT theory: Google dorking, WHOIS, DNS concepts (instructor-provided real-world examples). Active scanning deep dive: Nmap port scanning (SYN, TCP, UDP), OS fingerprinting, NSE vulnerability scripts, Nikto.	[1][3][4]	1	—	2	1	4
5	Manual service interaction. Banner grabbing with Netcat. Understanding FTP, SSH, HTTP, SMB protocols by hand. Vulnerability identification with Nmap NSE and Nikto. Manual CVE lookup and analysis.	[1][3]	1	—	2	1	4
6	Enumeration: SMB, SNMP. Combining Nmap results with manual interaction. Preparing for exploitation: selecting targets and matching CVEs to available exploits.	[1][3][10]	1	—	2	1	4
7	Midterm 1: Practical CTF (reconnaissance + manual service interaction on offline VM) + Platonus quiz (Weeks 1–6).	[1]–[14]	—	—	—	1	4
8	Exploitation with Metasploit Framework. Architecture: modules, payloads, encoders, handlers. Exploiting known services on Metasploitable 2 (vsftpd, Samba, UnrealIRCd). Understanding why each exploit works.	[1][2][3]	1	—	2	1	4

9	Password attacks: brute-forcing with Hydra (SSH, FTP); offline hash cracking with John the Ripper. Password policy best practices.	[1][3]	1	—	2	1	4
10	Privilege escalation fundamentals: SUID binaries and sudo misconfigurations only. Documenting escalation paths. No kernel exploits.	[1][3]	1	—	2	1	4
11	Web application security: OWASP Top 10 overview. SQL Injection — manual UNION and error-based injection on DVWA. Burp Suite: proxy setup, request interception, Repeater.	[1][8][13]	1	—	2	1	4
12	Web attacks continued: XSS (reflected, stored) and CSRF on DVWA. Understanding impact and remediation for each vulnerability type.	[1][8][13]	1	—	2	1	4
13	Network traffic analysis with Wireshark: HTTP, FTP, ARP traffic on pre-captured .pcap files. Wireless security theory (WPA2/WPA3 protocols). Social engineering theory: types, pretexts, real-world examples, defences.	[1][6][11]	1	—	2	1	4
14	Red team concepts (theory): adversary simulation, MITRE ATT&CK mapping exercise (paper-based), kill chain analysis. Penetration testing report writing (PTES). ESG in cybersecurity. Course review.	[1][5][12][14]	1	—	2	1	4
15	Midterm 2: Practical CTF (web exploitation + service exploitation on	[1]–[14]	—	—	—	1	4

	offline VM) + Platonus quiz (Weeks 8–14).						
	Total hours:		**13**	**0**	**26**	**15**	**60**

Note: *Weeks 7 and 15 are reserved for midterm assessments (no lectures or labs). Total: 13 Lec + 26 Lab + 15 SROP = 54 contact hours; 60 SRO hours; 6 hours midterm time. Grand total: 120 hours.*

11. LIST OF TOPICS/ASSIGNMENTS FOR LABORATORY CLASSES

Design principle: Every lab is fully offline, modular, and interruptible. Each lab contains 4–6 clearly separated steps with explicit checkpoints. Each step can be completed in 30–40 minutes independently. Labs 1–3 are designed for guaranteed visible success to build early confidence

No.	Lab Topic and Steps	Hours	Refs	Deliverable	Due
1	Lab Setup and First Discovery. Step 1: Install VirtualBox, import Kali and Metasploitable 2 VMs. Step 2: Configure host-only network. Step 3: Verify connectivity (ping). Step 4: First Nmap scan — discover target services. Checkpoint: screenshot of Nmap output showing open ports.	2	[1][2]	Setup checklist + Nmap screenshot	Week 1
2	Scanning and Service Discovery. Step 1: Run Nmap SYN scan against Metasploitable 2. Step 2: Run service version detection (-sV). Step 3: Identify all open ports, services, and versions. Step 4: Create a service map table (port / service / version). Checkpoint: complete service map with 10+ services identified.	2	[1][3]	Service map table + screenshot	Week 2
3	First Guided Exploitation. Step 1: Review service map from Lab 2 — identify vsftpd 2.3.4. Step 2: Research CVE-2011-2523 (instructor-provided CVE description). Step 3: Exploit with Metasploit (guided walkthrough). Step 4: Interact with the shell, run whoami and id. Checkpoint: screenshot of root shell. Students understand the link between discovery and exploitation.	2	[1][2]	Exploitation log + screenshot	Week 3
4	Passive Reconnaissance Concepts and Advanced Nmap Scanning. Step 1: Study instructor-provided real-world OSINT examples	2	[1][3][4]	OSINT summary + scan report	Week 4

	(screenshots of Google dorking, WHOIS, Shodan results). Step 2: SYN scan vs TCP connect scan on Metasploitable (compare). Step 3: UDP scan. Step 4: OS fingerprinting (-O). Step 5: NSE vuln scripts. Step 6: Nikto scan of web server. Checkpoint: OSINT summary + complete scan report.				
5	Manual Service Interaction. Step 1: Banner grab FTP (port 21) with Netcat. Step 2: Banner grab SSH (port 22) with Netcat. Step 3: Manual HTTP request with Netcat (GET / HTTP/1.0). Step 4: Connect to SMB and identify shares. Step 5: Identify service versions, look up CVEs manually. Checkpoint: table of services, versions, and CVEs.	2	[1][3]	Service interaction report	Week 5
6	Enumeration and Vulnerability Mapping. Step 1: SMB enumeration with Nmap scripts. Step 2: SNMP enumeration (snmpwalk). Step 3: Compile vulnerability map: match discovered services to known CVEs. Step 4: Select 3 most promising attack vectors and justify choices.	2	[1][3][10]	Vulnerability map + justification	Week 6
7	Metasploit Exploitation (Multiple Targets). Step 1: Exploit Samba (CVE-2007-2447). Step 2: Exploit UnrealIRCd backdoor. Step 3: Exploit distcc daemon. Step 4: For each: explain the vulnerability, why the exploit works, and how to fix it. Step 5: Generate payload with msfvenom (awareness).	2	[1][2][3]	Exploitation report (3 exploits)	Week 8
8	Password Attacks. Step 1: Brute-force SSH with Hydra (small wordlist, 5 min max). Step 2: Crack MD5 hashes with John the Ripper (pre-provided hash file). Step 3: Crack SHA256 hash with Hashcat (short wordlist). Step 4: Discuss password policy recommendations.	2	[1][3]	Cracking report + recommendations	Week 9
9	Privilege Escalation Fundamentals. Step 1: Find SUID binaries (find / -perm -4000). Step 2: Exploit a SUID binary to escalate privileges. Step 3: Check sudo -l for misconfigurations. Step 4: Exploit	2	[1][3]	Escalation path report	Week 10

	sudo misconfiguration. Step 5: Document escalation path. No kernel exploits.				
10	SQL Injection on DVWA. Step 1: Set DVWA to "Low" security. Step 2: Manual UNION-based SQLi. Step 3: Extract database name, tables, user credentials. Step 4: Set DVWA to "Medium" — try same attack, observe difference. Step 5: Discuss remediation (parameterised queries).	2	[1][8][13]	SQLi exploitation report	Week 11
11	XSS and CSRF on DVWA. Step 1: Reflected XSS — inject alert popup. Step 2: Stored XSS — persistent payload. Step 3: CSRF — forge a password change request. Step 4: Test with Burp Suite Repeater. Step 5: Discuss impact and remediation for each.	2	[1][8][13]	Web attack report	Week 12
12	Network Traffic Analysis (Offline). Step 1: Open pre-captured HTTP .pcap — extract credentials. Step 2: Open pre-captured FTP .pcap — extract file transfer. Step 3: Analyse ARP traffic — identify spoofing indicators. Step 4: Wireless theory: analyse WPA2 handshake pcap (structure only). All pcaps provided by instructor.	2	[1][3]	Traffic analysis report	Week 13
13	Professional Penetration Testing Report. Step 1: Choose one target machine exploited during the course. Step 2: Write executive summary. Step 3: Describe methodology (PTES phases). Step 4: Document 3 findings with CVSS ratings. Step 5: Write remediation recommendations. Step 6: Compile into professional report format.	2	[1][5][14]	Full pentest report	Week 14
	Total:	**26**			

12. LIST OF TOPICS/ASSIGNMENTS FOR STUDENT'S INDEPENDENT WORK

Design principle: All SRO tasks can be completed offline. Online platform tasks (TryHackMe, HackTheBox) are optional bonus activities only. Workload is realistic for students with limited and unstable internet access.

No.	SRO Topic	Hours	Refs	Deliverable	Due

1	Cyber Law Overview. Read Chapter 1 of [1] (CEH Study Guide). Write a summary (1000 words) comparing cybercrime legislation in Kazakhstan and one international framework (GDPR or CFAA). Include ESG governance perspective.	15	[1][10]	Written summary (1000 words)	Week 5
2	CEH Study: Modules 1–6. Self-study of CEH v13 Study Guide chapters on reconnaissance, scanning, and enumeration. Prepare a one-page cheat sheet of key Nmap commands and their purposes. Optional bonus: complete 1 TryHackMe room (if internet available).	15	[1][3][4]	Cheat sheet + study notes	Week 8
3	OWASP Top 10 Study. Read the OWASP Top 10 document (offline PDF provided). For each of the top 5 vulnerabilities, write: (a) what it is, (b) how it works, (c) how to prevent it. Total: ~1500 words. Optional bonus: complete 1 PortSwigger lab (if internet available).	15	[8][13]	OWASP summary report	Week 12
4	CTF Write-ups (Offline). Complete 2 instructor-provided offline CTF challenges (packaged as VM snapshots). Write a detailed write-up for each: methodology, tools used, findings, lessons learned. ~500 words per write-up.	15	[1][3]	2 CTF write-ups	Week 14
	Total:	**60**			

13. ASSESSMENT CRITERIA

The point-rating letter system for assessing the educational achievements of students with their interpretation in the traditional grading scale:

Letter system assessment	The digital equivalent of points	Percentage content	Traditional system assessment	General description of grading criteria
A	4,0	95-100	Excellent	The student has knowledge of the subject in the full scope of the curriculum, understands the discipline deeply enough; shows a high level of knowledge that exceeds the volume provided by the syllabus, gives an exhaustive answer
A-	3,67	90-94		The student has knowledge of the subject in the full scope of the curriculum, understands the discipline deeply enough; gives an exhaustive answer
B+	3,33	85-89	Good	The student shows a complete, well-founded knowledge of the subject, but the answers did not
B	3,0	80-84		
B-	2,67	75-79		

C+	2,33	70-74		always highlight the main idea, rational methods of calculation were not always used; the answers were mostly brief and sometimes unclear.
C	2,0	65-69	Satisfactory	The student demonstrates sufficient knowledge of the subject, but without proper depth and justification, the answers are unclear and without proper logical sequence.
C-	1,67	60-64		
D+	1,33	55-59		
D	1,0	50-54		
FX	0,5	25-49	Unsatisfactory	The student demonstrates insufficient knowledge of the subject, positive answers were not given to individual questions.
F	0	0-24		The student demonstrates a very low level of knowledge of the subject.

13.3 Final Exam Components

- **Type:** Written online test (Testing)
- **Platform:** Platonus
- **Format:** Multiple-choice questions, short-answer, problem-solving tasks, and command analysis
- **Duration:** 50 minutes
- **Evaluation:** Each task is scored individually; the final exam grade is the weighted average of all tasks

14. Sample Exam (Example Platonus Test)

1. What is the primary legal document governing computer crimes in the Republic of Kazakhstan?
2. Name the phases of a penetration test according to PTES.
3. What is the difference between passive and active reconnaissance?
4. What information does the Nmap -sV flag provide?
5. What is a CVE identifier and why is it important?
6. How do you perform a banner grab using Netcat? Write the command.
7. What is the difference between a bind shell and a reverse shell?
8. What is a SUID binary and how can it be used for privilege escalation?
9. Explain the difference between stored and reflected XSS.
10. Describe what a UNION-based SQL injection does.
11. What does Wireshark show in an ARP spoofing attack?
12. What are the key sections of a professional penetration testing report?
13. What is the CVSS scoring system used for?
14. What is the MITRE ATT&CK framework and how does it classify attacks?
- 15. What is responsible disclosure?

15. ESG Integration

In accordance with IITU Policy P-57 (Appendix 1), this course integrates ESG principles:

- **Environmental (E):** Week 12 discusses environmental impact of cyberattacks (energy costs of cryptomining malware, infrastructure strain from botnets). SRO assignments include consideration of ecological implications.
- **Social (S):** Social engineering (Week 12) is analysed both as an attack technique and in terms of social harm — privacy violations and psychological manipulation. The course emphasises responsible use of knowledge throughout.
- **Governance (G):** Week 1 covers legal frameworks. Week 14 teaches professional reporting standards. SRO 1 analyses governance across jurisdictions. The Responsible Use Agreement reinforces ethical governance.

  SDG Alignment: SDG 9 (Industry, Innovation and Infrastructure); SDG 16 (Peace, Justice and Strong Institutions); SDG 4 (Quality Education

  I have read and agree with the requirements of the discipline «_____».\

16. Student Acknowledgement

Students are introduced to the syllabus during the first session. By signing below, the student confirms that they have read and understood the course structure, assessment criteria, course policy, academic honesty requirements, and the Responsible Use Agreement.

№	Full name of the student	Signature	Date
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			