N	Topic	Status
1	Module 1. Introduction to the penetration testing • What is hacking and ethical hacking? • Types of cyberattacks; • Penetration testing methodology: OSTMM, ISSAF, etc; • Penetration testing project management; • Hacking tools overview; • Know the applicable laws; • Dealing with third parties; • Social engineering issues; • Logging; • Reporting; • Scope. Links to other courses; Labs: • Lab 1.1 Basic configuration of ethical hacker workplace: Kali Linux • Lab 1.2 Basic configuration of machine for hacking: Metasploitable 2	Teacher's book – 100% Student's book – 100% PPT – 100% Virtual machine (ISO image) – 100%
2	**Module 2. Intelligence Gathering** • OpenSourceIntelligence methods; • Structured analytic techniques overview; • Types of collected information: o Business information (financial, clients, suppliers, partners); o Information about IT-infrastructure; o Employee; • Discovering sources of the information; • Google for penetration testers; • Other search instruments; • Tools overview; Labs: • Lab 2.1 Using of Google for OSINT; • Lab 2.2 Using Maltego; • Lab 2.3 Whois Reconnaissance, DNS Reconnaissance, SNMP reconnaissance, SMTPreconnaissance, Microsoft Netbios Information Gathering • Lab 2.4 Network discovery with NMAP scanner.	Teacher's book – 100% Student's book – 100% PPT – 100% Virtual machine (ISO image) – 100%

	• Lab 2.5 Using sniffers	
3	**Module 3. Vulnerability Analysis** • Types of vulnerabilities; • Manual search for vulnerabilities; • Automated search for vulnerabilities; • Vulnerability Analysistools. Labs: • Lab 3.1 Basic Netcat usage; • Lab 3.2 Manual search for vulnerability in Apache Web-server using Telnet\Netcat; • Lab 3.3 Using vulnerability scanners (Nessus, Nexpose, OpenVAS) for vulnerability discovery; • Lab 3.4 Using miscellaneous assessment tools.	Teacher's book – 100% Student's book – 100% PPT – 100% Virtual machine (ISO image) – 100%
4	Module 4. Vulnerability Analysis for Web-applications • OWASPprojects • Types of vulnerabilities in Web-applications. OWASP Top 10 vulnerabilities • OWASP testing guide overview; • Google Hacking. Google Hacking Database (GHDB) • Web security testing tools: - Web-scanners, - LocalProxies - Fuzzers - Specialized browsers and browser plugins Labs: • Lab 4.1 Google Hacking using Google Hacking Database (GHDB); • Lab 4.2 Vulnerabilities discovery with web-scanners Nikto, Arachni..; • Labs 4.3 – 4.12 on OWASP Top 10 vulnerabilities	Teacher's book – 0% Student's book – 0% PPT – 0% Virtual machine (ISO image) – 100%
5	Module 5. Exploitation • What is an exploit? (Dorofeev) • TheExploitDatabase • Google for penetration testers*:* *www.exploit-db.com*	Teacher's book – 50% Student's book –50% PPT – 0%

	• Localexploitation • Metasploit Framework overview; • Types of payloads; • Meterpreter usage; • Man-in-the-middle attacks; • Password attacks: online and offline; • Art of manual password guessing; • Pass the hash attack. Labs: • Lab 5.1 Exploitation of Metasploitable 2 with Metasploit (…);Dorofeev) • Lab 5.2 spoofing tools : basic Ettercap, arpspoof usage (Cain & Abel? - Dorofeev) • Lab 5.3 Perform A Man In The Middle Attack With Kali Linux &Ettercap (among others SSLStrip); • Lab 5.4 Online password attack with THC-Hydra; (Dorofeev) • Lab 5.5 Offline password attacks with John-the-Ripper (Dorofeev) • Lab 5.6 Modern 2014 attacks - heartbleed, shellshock, etc	Virtual machine (ISO image) – 100%
6	Module 6. Social engineering • Social engineering (Dorofeev) • The Social engineering Toolkit project overview; (Andrian) Labs: • Lab 6.1 SET usage;	Teacher's book – 0% Student's book – 0% PPT – 0% Virtual machine (ISO image) – 100%
7	Module 7. Exploitation using client-side attacks • Client side exploits • The browser exploitation framework project overview; Labs: • Lab 7.1 Client side exploits; • Lab 7.2BeEF usage;	Teacher's book – 0% Student's book – 0% PPT – 0% Virtual machine (ISO image) – 100%

8	Module 8. Maintaining Access - Maintaining Access utilities Labs: - 8.1 Remote rootkit installation and usage;	Teacher’s book – 0% Student’s book – 0% PPT – 0% Virtual machine (ISO image) – 100%