National Military University "Vasil Levski"
Doc.: Erasmus/2021/09
Date: 14-09-2021
Origin: BG VELIKO02

Country	Institution	Module	ECTS
BULGARIA	Vasil Levski National Military University	**Network Penetration Testing – Part I**	**5.0**

Service	Minimum Qualification for Lecturers
ICT	• English: Common European Framework of Reference for Languages (CEFR) Level B2 or NATO STANAG 6001 Level 2. • Computer Architectures. • Computer Networks. • Network Security Fundamentals.
Languages **English, Bulgarian**	

Prerequisites for international participants:	Goal of the Module:
• English: Common European Framework of Reference for Languages (CEFR) Level B1 or NATO STANAG Level 2. • 3rd year of national (military) higher education. • Knowledge of computer systems and computer networks.	• Presentation of computer system and computer network vulnerabilities. • Description of common cybersecurity attacks. • Development of skills for network penetration testing. • Knowledge of possible network attack vectors. • Risk mitigation actions.

Learning outcomes		
	Knowledge	• Computer systems vulnerabilities. • Computer networks vulnerabilities. • Software applications vulnerabilities. • Instruments and methodologies for network attacks.
	Skills	• Usage of different instruments for penetration testing. • Network vulnerabilities estimation. • Performing basic penetration testing. • Applying basic network security.
	Competences	• Description of software instruments functionality. • Capacity to combine different instruments for penetration testing. • Describing networks topology and their visible security. • Performing initial penetration tests.

Verification of learning outcomes

- **Observation**: Throughout the course students are to accomplish different practical tasks individually or in teams. This course has two chapters. During the tasks students are to be evaluated for competences.
- **Test**: At the end of each chapter, the students have to accomplish specific practical tasks, which include usage of software instruments and techniques learned throughout the course.

Module Details		
Study topics	**class hours**	**Details**
Chapter I "Networks and systems security fundamentals"		
Basics of ICTs and security	15	• Computer systems and security. – 4 hours • Computer networks and network security. – 8 hours • Attack vectors. – 3 hours
Practical aspects of cybersecurity	15	• Information gathering. – 4 hours • Live IP addresses estimation. - 4 hours • Operation system and opened ports estimation. – 4 hours • Software vulnerabilities estimation. – 3 hours
Chapter II "Initial penetration testing"		
Introduction to Ethical hacking	15	• Attacking instruments exploration and learning. – 3 hours • Systems exploitation. – 6 hours • Remote sessions. - 6 hours
Practical Ethical hacking	15	• Scanning with NeXpose. - 2 • Scanning with Nessus (OpenVas). - 2 • Special vulnerability scanning. - 2 • Basic exploitation with Metasploit. - 2 • Dumping usernames and passwords. - 4 • Compromising with Meterpreter. - 3
Additional hours to increase the learning outcomes		
Self-Study	30	• Enhancing knowledge by studying specific computer and network standards. • Reflection of the topics issued.
Total	60	**Lections: 30 Practice: 30**

This study course description is created and revised at "Communication network and systems" Department and accepted at Faculty council.

Developed by:

major, assist. prof. PhD Linko Nikolov

REFERENCES:

1. Joseph Migga Kizza, "Guide to computer network security", Springer, 2017.
2. Andrew Mckinsey, "Computer Hacking, Basic Security, Cyber Crime, Network Security"
3. William Stallings, "Cryptography and network security - principles and practice", Pearson, 2017
4. Aicklen H. G., „Remote Control of Diverse Network Elements Using SNMP"
5. Александър Цокев „Етично хакерство", БАРЗИКТ, София 2017