NIKOLA VAPTSAROV
NAVAL ACADEMY

Erasmus+ BIP – Winter 2026

Name of the BIP: Introduction to penetration testing and ethical hacking	
Organizer: Nikola Vaptsarov Naval Academy	**ECTS credits for participating students:** 3
Online period: TBC	**Onsite period:** 9 -13 March 2026
Academic coordinator: Assistant Prof. Dimitar Nikolov	**Administrative coordinator:** erasmus@nvna.eu
Academic requirements: 3th and 4th year or master students with basic knowledge in Information Technologies	**Language requirement for students:** English B2
Nominations and number of students accepted: Up to 15. For nominating, please send your students information to erasmus@nvna.eu before January 15th 2026	
Content of the onsite program: The course will cover the fundamental concepts of penetration testing and ethical hacking of Linux, Windows machines and Web Applications, Initial compromise, privilege escalation, pivoting, persistence and command and control (C2).	

The program includes 1 day for outdoor training activities in the summer camp of Nikola Vaptsarov Naval Academy.

Module details		
Online period –TBC		
Main Topic	Recommended WH	Details
Ethical hacking and penetration testing fundamental concepts	2	• Terminology • History • Ethical Hacking vs Penetration testing
Building an ethical hacking lab	8	• Introduction to VirtualBox • Introduction to Vagrant • Networking • Saving machine state • Creating and managing Snapshots • Vulnerable machines and apps
Linux attacks	5	• Network Scanning • Port scanning • Attacking services and ports • Linux Bind, Reverse Shells, Rootkits, Backdoors and C2 Implants • Linux persistence
Windows attacks	5	• Network Scanning • Port scanning • Attacking services and ports • Windows Bind, Reverse Shells, Rootkits, Backdoors and C2 Implants • Windows persistence
Attacks against Web Apps	6	• Broken Access Control • Cryptographic Failures • Injections • Insecure Design • Security Misconfiguration • Vulnerable and Outdated Components • Identification and Authentication Failures
Privilege escalation, pivoting and C2	8	• Linux privilege escalation • Windows privilege escalation • Linux pivoting and port redirection • Windows pivoting and port redirection • Command and Control systems and implants • Actions on Objectives and Effects
Reporting	6	• 3 types of report • Describing a finding and severity scoring • Suggesting mitigations

On-site period – 09 – 13 March 2026		
Practice Tasks	30	• Linux attacks • Windows attacks • Web Application attacks • Privilege escalation, pivoting and C2 • Actions on Objectives and Effects
Total WH	**70**	