SYLLABUS

1. Data about the program of study

1.1 Institution	Technical University of Cluj-Napoca
1.2 Faculty	Automation and Computer Science
1.3 Department	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Master of Science
1.6 Program of study / Qualification	Cybersecurity Engineering / Master
1.7 Form of education	Full time
1.8 Subject code	13.00

2. Data about the subject

2.1 Subject Name				**Penetration testing**	
2.2 Course responsible/ Lecturer				Dr. eng. Andrei-Vlad Lutas - vlutas@bitdefener.com	
2.3 Teachers in charg of semiaries				Dr. eng. Andrei-Vlad Lutas - vlutas@bitdefener.com	
2.4 Year of study	II	2.5 Semester	3	2.6 Type of assessment (E - exam, C - colloquium, V - verification)	E
2.7 Subject category	Formative category: DA – advanced, DS – speciality, DC – complementary				DS
	Optionality: DI – imposed, DO – optional (alternative), DF – optional (free choice)				DI

3. Estimated total time

3.1 Number of hours per week	3	of which	Course	2	Seminary	-	Laboratory	-	Project	1
3.2 Număr de ore pe semestru	42	of which	Course	28	Seminary	-	Laboratory	-	Project	14
3.3 Individual study										
(a) Manual, lecture material and notes, bibliography										10
(b) Supplementary study in the library, online and in the field										20
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										73
(d) Tutoring										0
(e) Exams and tests										5
(f) Other activities										0

3.4 Total hours of individual study (sum (3.7(a)...3.7(f)))	108
3.5 Total hours per semester (3.4+3.8)	150
3.6 Number of credit points	6

4. Pre-requisites (where appropriate)

4.1 Curriculum	Software Security
4.2 Competence	Computer architecture, Operating systems, Programming in C and x86 assembler, Basic understanding of computer networks and protocols

5. Requirements (where appropriate)

5.1. For the course	Blackboard, Video Projector
5.2. For the project	Blackboard, Video Projector, Laptop with internet access

6. Specific competences

6.1 Profesional competences	**C1. Identify and understand the security issues specific to the different contexts of computing system usage. Appropriately apply the basic elements of security management and methods of evaluation and management of information security risks.** • **C1.1.** Knowledge of advanced theoretical and practical terminology, concepts, and principles specific to cybersecurity field. Knowledge of concepts about cybersecurity risk evaluation, and management. • **C1.3.** Capability to identify and model new types of cybersecurity risks affecting end users, computing systems, and software applications, and identify and evaluate possible solutions against such risks. • **C1.4.** Capability to identify and assess the limitations of existing cybersecurity solutions and their security risks, relative to well-known classifications. **C3. Analyze and evaluate the security characteristics of computing system. Identify the misconfigurations and software vulnerabilities.** • **C3.1.** Theoretical and practical knowledge of different cases of computing system misconfiguration and misusage that expose them to cybersecurity attacks, and of different types of software vulnerabilities and possible cybersecurity attacks. • **C3.2.** Be able to analyze and understand new kinds of software and communication protocols, in order to identify new possible cybersecurity threats, vulnerabilities, and risks. Be able to use commonly used databases of reported vulnerabilities and attacks in the process of assessing the cybersecurity of a new computing system. • **C3.3.** Capability to make cybersecurity assessments and identify possible attack surface of unknown computing systems, networks, or software applications. • **C3.4.** Capability to identify and assess theoretical and practical limitations of existing automatic vulnerability detection tools and propose possible combinations of such tools for improved results, where and if possible. • **C3.5.** Capability to propose new vulnerability identification, analysis, and classification, methods. Capability to propose solutions against exploitation techniques of such vulnerabilities.
6.2 Cross competences	N/A

7. Discipline objectives (as results from the *key competences gained*)

7.1 General objective	Understand how vulnerabilities and misconfigurations could lead to organization compromises and how an attacker may exploit architecture or software errors. Learn the pentesting process and how to write a pentesting report.
7.2 Specific objectives	**1.** Understand the pentesting process, its scope, how to obtain permission to perform it and how to present its findings. **2.** Understand the general pentesting steps, starting with information gathering, port scanning, service enumeration, exploitation, privilege elevation, lateral movement and finishing with the report. **3.** Learn how to use common pentesting tools (e.g. nmap for port scanning) **4.** Learn how to exploit main classes of vulnerabilities (Buffer/Heap overflow, SQL Injection, XSS, CSRF, LFI etc) **5.** Understand how to build shellcode and how to encode it correctly **6.** Understand the fundamental binary exploitation mitigation (DEP, ASLR, Stack Cookies, SafeSEH, CFG and CET) **7.** Understand privilege elevation techniques **8.** Understand tunneling and covert communication channels **9.** Learn about lateral movement (with applications in Active Directory and Azure Active Directory) **10.** Know how to elaborate a complete and clear pentesting report.

8. Content

8.1. Lecture (syllabus)	Hours	Teaching methods	Notes
Introduction to pentesting methodology	2	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges.	
Information gathering and open source intellingence: google, dns, whois, SNMP, SMTP	2		
Port scanning techniques	2		
Enumeration: Banner grabing, NetBIOSns	2		
Memory corruptions: buffer/heap overflow, integer overflows, signed/unsigned	2		
Shellcode fundamentals: Assembly and operand encdings, avoiding special characters, obfuscation	2		
Web vulnerabilities (LFI, RFI, directory traversal, XSS, CSRF)	2		
SQL Injections: types, applications on various databases	2		
Exploitation fundamentals: Obtaining the initial shell	2		
Tunneling and covert communication channels	2		
Privilege elevation (lateral or vertical)	2		
Post exploitation and lateral movement	2		
Writing the pentesting report	2		
Evitarea ASLR, exploatarea folosind reutilizare de cod (ROP), exploituri de kernel	2		

Bibliography:

1. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)
2. Metasploit: The Penetration Tester's Guide (Kennedy, David – 2011 – No Stach Press)
3. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)
4. Hacking Exposed – Network Security Secrets Exposed (McClure, Stuart – 2012 – McGraw-Hill) (7th ed)
5. Pentesting tutorials from various websites (ex. http://www.offensive-security.com/metasploit-unleashed)

8.2 Applications - Seminars / Laboratory / Project	Hours	Teaching methods	Notes
Get familiar with the Hacknet virtual penetration lab. Learn about information gathering, pass the hash and forensics	1	Oral presentations, using PowerPoint, Teams and Moodle. Discussions about project work and submissions.	
Learn about OS int: Google, DNA, whois, SNMP, SMTP. Learn about port scanning and service enumeration	1		
Exploiting memory corruption in real applications	1		
Shellcode generation, encoding and obfuscation	1		
Web security (LFI, RFI, XSS, CSRF, directory traversal, SQL Injection)	1		
Privilege elevation	1		
Tunneling and post exploitation	1		

Bibliography

6. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)
7. Metasploit: The Penetration Tester's Guide (Kennedy, David – 2011 – No Stach Press)
8. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)
9. Hacking Exposed – Network Security Secrets Exposed (McClure, Stuart – 2012 – McGraw-Hill) (7th ed)
10. Pentesting tutorials from various websites (ex. http://www.offensive-security.com/metasploit-unleashed)

9. Bridging course contents with the expectations of the representatives of the community, professional associations, and employers in the field

Course was designed together with security profesionals from companies that have relevant activity in the field (e.g. Bitdefender) and is alligned with subjects evaluated for various pentesting certifications.
Related courses from other universities:

- *Offensive Security*, Dakota State University, USA
  http://catalog.dsu.edu/preview_course_nopop.php?catoid=8&coid=3804

- *CS6573 Penetration Testing and Vulnerability Analysis*, Masters in Cybersecurity, New York Polytechnic School of Engineering, New York, USA
  http://engineering.nyu.edu/academics/course/CS6573
- *Offensive Computer Security,* Florida State University, USA
  http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Ability to define concepts and methods specific to pentesting field. Capability to give correct and functional solutions to problems specific to pentesting field. Attendance frequency, interest, and interactivity during lecture classes.	Written exam, including online quiz tests (e.g. on Moodle platform) and presentation(s) of different subjects / paper in the course's field during semester time.	50%
Project	Capability and ability to give correct and functional solutions to problems specific to pentesting field. Attendance frequency, interest, and interactivity during project classes.	Testing vulnerabilities of machines in a virtual laboratory created for this subject. Writing reports about the vulnerabilities and how they may be exploited to gain access to machines.	50%

Minimum standard of performance:
Lecture
Minimum attendence requirement 50%
Minimum grade for exam: 5
Desired competences: understand basics of penetration testing, types of vulnerabilities, exploitation strategies and post exploitation activities.
Project
Minimum attendence requirement 100%
Minimum grade on all project submissions: 5
Minimum final project assesment exam grade: 5
Desired competences: Demonstrate ability to exploit vulnerabilities of real systems (virtual machines). Understand how to report such vulnerabilities.

Date of filling in: 26.02.2025	**Responsible**	**Title First name Last name**	**Signature**
	Course	Dr. eng. Andrei-Vlad LUȚAȘ	
	Applications	Dr. eng. Andrei-Vlad LUȚAȘ	

Date of approval in the department 17.09.2025	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council 19.09.2025	Dean, Prof.dr.eng. Vlad Mureșan