SYLLABUS

1. Data about the program of study

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

2. Data about the subject

2.1 Subject name	***Penetration Testing***			Subject code	**13**
2.2 Course responsible / lecturer	Eng. PhD. Portase Radu-Marian - radu.portase@cs.utcluj.ro				
2.3 Teachers in charge of seminars / Laboratory / project	Eng. PhD. Portase Radu-Marian - radu.portase@cs.utcluj.ro				
2.4 Year of study	II	2.5 Semester	1	2.6 Type of assessment (E - exam, C - colloquium, V – verification)	E
2.7 Subject category	Formative category: DF – fundamental, DS – speciality, DC – complementary				DS
	Optionality: DOB – mandatory, DOP – optional (alternative), DFA – optional (free choice)				DOB

3. Estimated total time

3.1 Number of hours per week	3	of which:	Course	2	Seminars	-	Laboratory	-	Project	1
3.2 Number of hours per semester	42	of which:	Course	28	Seminars	-	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										-
(e) Exams and tests										5
(f) Other activities:										-

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	108
3.5 Total hours per semester (3.2+3.4)	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 applications	Blackboard, Video Projector, Laptop with internet access

6. Specific competence

6.1 Professional competences	• implement ICT risk management • develop information security strategy • perform ICT security testing • execute ICT audits • manage system security • manage IT security compliances • identify ICT security risks • perform risk analysis • educate on data confidentiality • provide ICT consulting advice • perform data analysis • ensure compliance with legal requirements • ensure information privacy • monitor developments in field of expertise • keep up with the latest information systems solutions
6.2 Cross competences	• develop an analytical approach • taking a proactive approach • developing strategies to solve problems • being open minded

7. Expected Learning Outcomes

Knowledge	ethical hacking principles; web application security threats; attack vectors; software anomalies; operating systems; ICT network security risks; cyber attack counter-measures; ICT encryption; ICT security standards; security engineering; risk management; cloud security and compliance; ICT infrastructure; information security strategy; incidents and accidents recording
Skills	perform ICT security testing; identify ICT security risks; perform risk analysis; implement ICT risk management; establish an ICT security prevention plan; manage system security; define security policies; execute ICT audits; provide ICT consulting advice; educate on data confidentiality
Responsibilities and autonomy	develop an analytical approach; developing strategies to solve problems; taking a proactive approach; being open minded; coordinate engineering teams

8. Discipline objective (as results from the *key competences gained*)

8.1 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.
8.2 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.

9. Contents

9.1 Lectures	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)
   - Pentesting tutorials from various websites (ex. http://www.offensive-security.com/metasploit-unleashed)

9.2 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

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

10. 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/

11. 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. *(summative assessment)*	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. *(continuous assessment)*	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: 29.04.2026	**Responsible**	**Title First name Last name**	**Signature**
	Course	Eng. PhD. Portase Radu-Marian	
	Applications	Eng. PhD. Portase Radu-Marian	

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