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	***Reverse Engineering and Malware Analysis***			Subject code	**3**
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	I	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	4	of which:	Course	1	Seminars	1	Laboratory	2	Project	-
3.2 Number of hours per semester	56	of which:	Course	14	Seminars	14	Laboratory	28	Project	-
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										16
(b) Supplementary study in the library, online and in the field										16
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										35
(d) Tutoring										-
(e) Exams and tests										2
(f) Other activities:										-

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	69
3.5 Total hours per semester (3.2+3.4)	125
3.6 Number of credit points	5

4. Pre-requisites (where appropriate)

4.1 Curriculum	Computer programming, Computer Architecture, Operating Systems
4.2 Competence	Assembly Language x86, Programming in C, Operating System Architecture

5. Requirements (where appropriate)

5.1. For the course	blackboard, video project/smart board, computers
5.2. For the applications	blackboard, video project/smart board, computers

6. Specific competence

6.1 Professional competences	• develop information security strategy • lead disaster recovery exercises • perform ICT security testing • execute ICT audits • manage system security • implement ICT recovery system • manage IT security compliances • identify ICT security risks • define security policies • perform risk analysis • provide ICT consulting advice • perform data analysis • 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; software anomalies; operating systems; computer forensics; cyber security; attack vectors; ICT network security risks; security threats; cyber attack counter-measures; ICT encryption; ICT infrastructure; ICT security standards; security engineering; risk management; cloud monitoring and reporting; cloud security and compliance; information confidentiality; ICT security legislation; incidents and accidents recording
Skills	perform ICT security testing; identify ICT security risks; perform risk analysis; implement ICT risk management; manage system security; establish an ICT security prevention plan; execute ICT audits; provide ICT consulting advice; manage IT security compliances; ensure compliance with legal requirements
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	Getting students familiar with malicious software and how informatic attacks are performed. Gaining skills for identifying and investigating an infected device
8.2 Specific objectives	1. Understand how malicious software is operating 2. Gain skills for identifying malicious software 3. Be able to identify an infected system

9. Contents

9.1 Lectures	Hours	Teaching methods	Notes
Security solutions and malware	1		
Static Reverse Engineering 1: Static Analysis Fundamentals on Windows	1		
Static Reverse Engineering 1: From Binary to Decompiled code	1		

Static Reverse Engineering 2: Packers and Obfuscated Code	1	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges.	
Static Reverse Engineering 3: Advanced Concepts in Binary Reverse Engineering	1		
Static Reverse Engineering 4: Fileless Malware	1		
Malware on the network: Delivery and Command and Control	1		
Dynamic Analysis 1: Fundamentals	1		
Dynamic Analysis 2: Common Malware Tactics	1		
Dynamic Analysis 3: Advanced Concepts	1		
Evasion Tactics 1: Preventing Detection on the Endpoint	1		
Evasion Tactics 2: Preventing Detection over the Network	1		
Threat intelligence & Malware attribution	1		
Current Threat Landscape & Malware in the future	1		

Bibliography

1. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware (Abhijit Mohanta and Anoop Saldanha – 2020 – APRESS)
2. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware (Monnappa K A – 2018 – PACKT)
3. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (Sikorski, Michael – 2012 – No Strach Press)
4. The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (Eagle, Chris – 2011 – No Strach Press)
5. The Art Of Computer Virus Research And Defense (Szor, Peter - 2005 - Addison-Wesley)
6. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation (Dang, Bruce - 2014 - Wiley)

- The Life of Binaries (Xeno Kovah – 2013 – http://opensecuritytraining.info/LifeOfBinaries.html)

9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
Environment setup	3	Brief reviews, blackboard illustrations and explanations, tutorials, roadmaps, short live demos, discussions, homework.	
Exploring the PE format	3		
First Steps in Reverse Engineering	3		
Decompiling a Program Using IdaPro (1)	3		
Decompiling a Program Using IdaPro (2)	3		
Analyzing Files malware	3		
Analyzing Network Traffic	3		
Analyzing Samples in Virtual Environments with monitoring tools (1)	3		
Analysing Samples in Virtual Environments with monitoring tools (2)	3		
Analysing Samples in Virtual Environments with monitoring tools (3)	3		
Analysing Across a Malware Kill Chain	3		
Dynamic Analysis of Network Traffic	3		
Practical Threat Intelligence with MISP	3		
Lab Exam	3		

Bibliography

1. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware (Abhijit Mohanta and Anoop Saldanha – 2020 – APRESS)
2. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware (Monnappa K A – 2018 – PACKT)
3. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (Sikorski, Michael – 2012 – No Strach Press)
4. The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (Eagle, Chris – 2011 – No Strach Press)
5. The Art Of Computer Virus Research And Defense (Szor, Peter - 2005 - Addison-Wesley)
6. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation (Dang, Bruce - 2014 - Wiley)

- The Life of Binaries (Xeno Kovah – 2013 – http://opensecuritytraining.info/LifeOfBinaries.html)

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

It is performed by periodic talks with important cybersecurity industry representatives.
We also keep updated with good ideas and proposals of other academic institutions in our country and abroad that run cybersecurity related study programs or/and research projects, like for instance:

- *CS 675 Reverse Software Engineering*, Masters in Computer Science, Drexel University, Philadelphia, USA. https://www.cs.drexel.edu/~spiros/teaching/CS675/
- *CISC6800 Malware Analytics and Software Security*, Fordham University, Masters Degree in Cybersecurity, New York, USA http://www.fordham.edu/academics/colleges__graduate_s/undergraduate_colleg/school_of_profession/pcs_home/degrees_and_programs/ms_cybersecurity_94711.asp
- *Malware*, Masters in Cybersecurity, Tallinn University of Technology, Estonia. http://www.ttu.ee/studying/masters/masters_programmes/cyber-security/cyber-security-4/

11. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Ability to define concepts and methods specific to malware analysis and reverse engineering field. Capability to give correct and functional solutions to problems specific to malware analysis and reverse engineering 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)* In exceptional cases, which imposes remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	40%
Seminar	Capability and ability to analyze problems specific to malware analysis and reverse engineering field. Attendance frequency, interest, and interactivity during seminar classes.	Evaluate seminar activity. Evaluate seminar assignments (homework) and / or presentations. *(continuous assessment)* Evaluate solutions of problems given in a final seminar exam. *(summative assessment)* In exceptional cases, which imposes remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	20%
Laboratory	Capability and ability to give correct and functional solutions to problems specific to malware analysis and reverse engineering field. Attendance frequency, interest, and interactivity during lab classes.	Evaluate lab activity. *(continuous assessment)* Evaluate lab assignments (homework). *(continuous assessment)* Evaluate solutions of problems given in a final lab exam. *(summative assessment)* In exceptional cases, which imposes remote classes, the	40%

		exam could be given online remotely, using Moodle and Teams platforms.	
Project	N/A	N/A	

Minimum standard of performance

***Lecture*.** Attending minimum 50% of lecture classes, to be allowed to take the final examination. Students must be able understand and explain the functionality of a simple malware. Minimum final grade must be 5 for the exam to be considered passed.

***Lab*.** Attending all lab **classes** (one lab could be recovered during the semester, and one more during re-examination sessions). Students must be able to identify a malware sample using static and dynamic analysis methods and tools and explain its functionality. Minimum lab grade must be 5 for being allowed at final exam.

Date of filling in: 29.04.2026	**Responsible**	**Title First name Last name**	**Signature**
	Course	Eng. PhD. Radu-Marian PORTASE	
	Applications	Eng. PhD. Radu-Marian PORTASE	

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