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	3.

2. Data about the subject

2.1	Subject name			***Reverse engineering and Malware analysis***	
2.2	Course responsible/lecturer			Assoc. Prof. Dr. Eng. Ciprian OPRIȘA- ciprian.oprisa@cs.utcluj.ro	
2.3	Teachers in charge of seminars			Assoc. Prof. Dr. Eng. Ciprian OPRIȘA- ciprian.oprisa@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: 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	4	of which	3.2 Course	1	3.3 Seminar	1	3.3 Laboratory	2	3.3 Project	
3.4 Total hours in the curriculum	56	of which	3.5 Course	14	3.6 Seminar	14	3.6 Laboratory	28	3.6 Project	

3.7 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	0
(e) Exams and tests	2
(f) Other activities	0
3.8 Total hours of individual study (summ (3.7(a)…3.7(f)))	69
3.9 Total hours per semester (3.4+3.8)	125
3.10 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, beamer, computers
5.2	For the applications	blackboard, beamer, computers

6. Specific competences

Professional competences	**C2. Investigate and analyze cyber-criminality actions and malware using advanced methods such as reverse engineering and behavior monitoring.** • **C2.1.** Advanced knowledge of classifications and characteristics of different cybersecurity attacks and malware. • **C2.2.** Be able to analyze and understand new kinds of malware, the new techniques they use to attack, gain persistence, escalate privileges etc., and be able to compare them with known attack techniques. • **C2.3.** Capability to identify malicious entities and activities, having no inside visibility on them (using black-box strategy) • **C2.4.** Capability to identify and assess theoretical and practical limitations of existing automatic malware analysis tools and propose improvements, where and if possible. • **C2.5.** Capability to derive new classes of attacks and exploitation techniques, supposed to be used by new malware, and propose the appropriate methods to identify and classify them correctly. **C4. Design and develop highly secure software, security solutions and tools.** • **C4.2**. Be able to identify new situations and scenarios when it is needed to develop a new cybersecurity solution or use an existing one. Be able to analyze proposed cybersecurity solutions and compare them with existing ones. • **C4.3.** Capability to develop complex secure software, complying with recommended good practices of built-in security and secure coding. Capability to develop software tools used for cybersecurity pentesting and assessment. • **C4.5.** Capability to develop software modules and tools that could provide a high degree of cybersecurity. Capability to propose new methods to assess the cybersecurity of computing systems and devices and ways to improve it.
Cross competences	N/A

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

7.1	General objective	Getting students familiar with malicious software and how informatic attacks are performed. Gaining skills for identifying and investigating an infected device
7.2	Specific objectives	1. Understand how malicious software is operating 2. Gain skills for identifying malicious software 3. Be able to identify an infected system

8. Contents

8.1. Lecture (syllabus)	Number of hours	Teaching methods	Notes
x86 System Architecture	1	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges	
x86 Assembly Language	1		
MS Windows Operating System Structure: user/kernel mode, Win32 APIs	1		
MZPE File Format (1)	1		
MZPE File Format (2)	1		
Disassembling Compiled Code	1		
Decompiling programs	1		
Running Samples in Virtual Environment with Monitoring Tools	1		
Debugging with Special Tools (eg: OllyDbg)	1		
Anti-Analysing and Anti-Emulation Techniques	1		
Code Packers and Protectors	1		

Polymorphic and Metamorphic Malware	1		
Analysing Exploits	1		
Mobile application analysis	1		

Bibliography

1. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (Sikorski, Michael – 2012 – No Strach Press)
2. The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (Eagle, Chris – 2011 – No Strach Press)
3. The Art Of Computer Virus Research And Defense (Szor, Peter - 2005 - Addison-Wesley)
4. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation (Dang, Bruce - 2014 - Wiley)
5. The Life of Binaries (Xeno Kovah – 2013 – http://opensecuritytraining.info/LifeOfBinaries.html)

8.2. Seminar /Laboratory / Project	Number of hours	Teaching methods	Notes
Reviewing the Basics of x86 Assembly Language	3	Brief reviews, blackboard illustrations and explanations, tutorials, roadmaps, short live demos, discussions, homework	
Security Tips While Programming in Assembly Language	3		
Programming Using Win32API	3		
Writing a Parser for MZPE Files	3		
Decompiling a Program Using IdaPro (1)	3		
Decompiling a Program Using IdaPro (2)	3		
Decompiling a Program Using IdaPro (3)	3		
Analysing Samples in Virtual Environments with monitoring tools (1)	3		
Analysing Samples in Virtual Environments with monitoring tools (2)	3		
Using Sandbox System to Analyse Files	3		
Analysing Infected Systems	3		
Cleaning an Infected System	3		
Exploits Analysing	3		
Mobile application analysis. Knowledge Evaluation	3		

Bibliography

1. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (Sikorski, Michael – 2012 – No Strach Press)
2. The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (Eagle, Chris – 2011 – No Strach Press)
3. The Art Of Computer Virus Research And Defense (Szor, Peter - 2005 - Addison-Wesley)
4. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation (Dang, Bruce - 2014 - Wiley)
5. The Life of Binaries (Xeno Kovah – 2013 – http://opensecuritytraining.info/LifeOfBinaries.html)

9. 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/

10. 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. In exceptional cases, which imposes remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	50%
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. Evaluate solutions of problems given in a final seminar exam. In exceptional cases, which imposes remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	10%
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. Evaluate lab assignments (homework). Evaluate solutions of problems given in a final lab exam. In exceptional cases, which imposes remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	40%
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:		Title Surname Name	Signature
	Lecturer	Assoc. Prof. Dr. Eng. Ciprian OPRIȘA	
	Teachers in charge of application	Assoc. Prof. Dr. Eng. Ciprian OPRIȘA	

Date of approval in the department 20.02.2024	Head of department Prof.dr.ing. Rodica Potolea
Date of approval in the Faculty Council 22.02.2024	Dean Prof.dr.ing. Mihaela Dinsoreanu