F01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2024/2025**		**University Specialization**	**Cybersecurity**	
Course No.	**0133407**		**Course name**	**Malware Analysis**	
Credit Hours	**3**		**Prerequisite Co-requisite**	**Secure Communication Protocols (0125347)**	
Course type	☐ MANDATORY UNIVERSITY Requirement	☐ University elective Requirement	☐ FACULTY MANDATORY Requirement	☐ Support course family requirements	☐ ✓ **Mandatory requirement** ☐ Elective requirements
Teaching style	☐ **Full online learning**		☐ Blended learning		☐ ✓Traditional learning
Teaching model	☐ Synchronous:1asynchronous		☐✓2 face to face: synchronous		☐ 3 Traditional

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

Students will learn different techniques for analyzing malicious software and understanding its behavior. This will be achieved using several malware analysis methods such as reverse engineering, binary analysis, and obfuscation detection, as well as by analyzing real-life malware samples.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	Practical Malware Analysis . The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig February 2012, 800 pp. ISBN-13: 9781593272906
Supportive learning resources	1. Malware Data Science , Attack Detection and Attribution by Joshua Saxe with Hillary Sanders September 2018, 272 pp.

(Books, databases, periodicals, software, applications, others)	ISBN-13: 978-1-59327-859-52			
Supporting websites				
The physical environment for teaching	☐ **Class room**	☐ labs	☐ **Virtual educational platform**	☐ Others
Necessary equipment and software				
Supporting people with special needs				
For technical support	**E-learning and Open Educational Center. Computer Center**			

Security Department

Course learning outcomes (S= Skills, C= Competences K= Knowledge,)

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	knowledge of methodology, technology and application of malware analysis and reverse engineering	**MK1**
K2	knowledge of anonymous analysis.	**MK2**
K3	knowledge of advanced static malware analysis	**MK4**
K4	knowledge of advanced dynamic malware analysis	**MK1**
K5	knowledge of malware classification and functionality	**MK5**
K6	knowledge of building and using a malware lab	**MK6**
	Skills	
S1	Applying malware analysis methodology and technology.	**MS1**
S2	Applying advanced static malware analysis	**MS2**
S3	Applying advanced dynamic malware analysis	**MS3**
S4	identify basic and some advanced malware functionality	**MS4**
	Competences	
C1	Working independently as a malware analyst and is familiar with terminology	**MC1**
C2	Discussing professional problems, analysis and conclusions in the field of malware analysis, both with professionals and with general audience	**MC2**

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0
Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	learning style*	Reference **
1	Malware analysis primer: Definition - Needs - Goals -		
2	Types of malicious software analysis		
3	Basic Static Techniques-1		
4	Malware Analysis in Virtual Machines-1		
5	Basic dynamic techniques		
6	A Crash Course in x86 Disassembly		
7	Advanced static analysis: IDA Pro-2		
8	Midterm Exam (30%)		
9	Analyzing Malicious Windows Programs		

Security Department

10	Advanced dynamic analysis: Debugging-2		
11	Advanced dynamic analysis: OllyDbg-2		
12	Kernel Debugging with WinDbg-1		
13	Malware Behavior-2		

14	ANTI-REVERSE-ENGINEERING: Anti-Disassembly		
15	Projects Discussion		
16	Final Exam		

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**

**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

Week	Task / activity	Reference	Expected results
1	Basic Static Analysis-1	Ligh, M. H., Adair, S., Hartstein, B., & Richard, M. (2010). The Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley Publishing.	
2	Basic Static Analysis-2	Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press	
3	Basic Dynamic analysis	Russinovich, M. E., Solomon, D. A., & Ionescu, A., & Yosifovich, P. (2021). Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (7th Edition). Microsoft Press.)	
4	Assembly lab using Jasmin	Hyde, R. (2010). The Art of Assembly Language (2nd Edition). No Starch Press.	

5	Advanced Dynamic Analysis	Russinovich, M. E., Solomon, D. A., & Ionescu, A., & Yosifovich, P. (2021). Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (7th Edition). Microsoft Press.)	
6	Advanced static Analysis	Russinovich, M. E., Solomon, D. A., & Ionescu, A., & Yosifovich, P. (2021). Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (7th Edition). Microsoft Press.)	
7	Debugging	Russinovich, M. E., Solomon, D. A., & Ionescu, A., & Yosifovich, P. (2021). Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (7th Edition). Microsoft Press.)	
8	Dis-Assembly	Russinovich, M. E., Solomon, D. A., & Ionescu, A., & Yosifovich, P. (2021). Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (7th Edition). Microsoft Press.)	