



## COURSE SYLLABUS

### Analiză Malware

#### 1. Program identification details

1.1 Higher education institution	<b>"OVIDIUS" UNIVERSITY OF CONSTANȚA</b>
1.2 Faculty	Facultatea de Matematică și Informatică
1.3 Department	Matematică și Informatică
1.4 Field of study	<b>Informatică</b>
1.5 Degree	Master
1.6 Programme of study	<b>Securitate Cibernetică și Învățare Automată</b>
1.7 Academic year	2025-2026

#### 2. Course identification details

2.1 Course title	Analiză Malware						
2.2 Course code	CSML.1.1.08						
2.3 Lecture instructor	<b>Lect. Dr. Ștefania Loredana NIȚĂ</b>						
2.4 Seminar instructor	<b>Lect. Dr. Ștefania Loredana NIȚĂ</b>						
2.5 Year	<b>1</b>	2.6 Semester	<b>1</b>	2.7 Evaluation	<b>C</b>	2.8 Course type	SC/OC

\* FC – fundamental course, SC – specialty course, CC – complementary course

\*\*MC – mandatory course; OC – optional course; EC – elective course

#### 3. Estimated workload (hours per semester)

3.1 Number of teaching hours/week	2	of which: 3.2 lecture	1	3.3 applications***	1
3.4 Number of teaching hours/semester	28	of which: 3.5 lecture	14	3.6 applications	14
3.7 Individual study workload					72
Workload distribution					[hours]
Reading (books, coursebooks, course reader, lecture notes, course bibliography)					16
Additional library / specialised platform research and fieldwork					10
Seminar / lab / project preparation, home assignments, research papers, portfolios and essays					28
Presentation or test preparation					14
Final examination preparation					4
Other activities: tutorials					0
3.8 Total hours/semester	28+72=100				
3.9 Number of credits	5				

\*\*\* S - seminar; L - lab; P - project

#### 4. Prerequisites (where applicable)

4.1 curriculum-related	Studii universitare de licență
4.2 skills-related	<ul style="list-style-type: none"><li>• Cunoștințe de bază de programare;</li><li>• Familiaritate cu mediile Windows și Linux;</li></ul>



	<ul style="list-style-type: none"><li>• Noțiuni introductive despre conceptele de securitate cibernetică (de exemplu, malware, exploit-uri, elementele de bază ale criptografiei).</li></ul>
--	--

### 5. Necessary requirements for optimum teaching and learning (where applicable)

5.1. for running the lecture	<ul style="list-style-type: none"><li>• Conexiune stabilă la internet</li><li>• Platformă de învățare online</li><li>• Acces la materiale didactice digitale (slide-uri, articole, studii de caz etc.)</li></ul>
5.2. for running the seminar/ lab / project*	<ul style="list-style-type: none"><li>• Stable Internet connection</li><li>• Online learning platform</li><li>• Access to digital teaching materials (case studies, etc.)</li></ul>

\*Type of application to be chosen according to the nature of the course

### 6. Course objectives

6.1 The general objective of the course	Stăpânirea cunoștințelor teoretice și a abilităților practice necesare pentru a analiza, clasifica și răspunde la diferite tipuri de programe malware și atacuri cibernetice aferente.
6.2 Specific objectives	<ul style="list-style-type: none"><li>• Capacitatea de a utiliza instrumente de monitorizare a sistemului și a rețelei pentru detectarea activităților rău intenționate.</li><li>• Aplicarea tehnicilor de analiză statică și dinamică pentru investigarea mostrelor de malware.</li><li>• Utilizarea ingineriei inverse, a analizei criminalistice a memoriei și a sandboxing-ului pentru a înțelege comportamentul malware-ului.</li><li>• Elaborarea de reguli automate de detecție și vânătoare (<i>hunting</i>) pentru identificarea tiparelor de malware.</li></ul>

### 7. Learning outcomes

Knowledge	<ul style="list-style-type: none"><li>• Înțelege conceptele fundamentale ale programelor malware, inclusiv clasificarea, vectorii de infecție, mecanismele de persistență și tehnicile de ofuscare.</li><li>• Explică amenințările cibernetice moderne asociate programelor malware, inclusiv fișiere executabile, scripturi, documente malițioase și malware bazat pe rețea.</li><li>• Identifică și diferențiază metodele de analiză statică și dinamică a programelor malware și explică rolul acestora în răspunsul la incidente.</li></ul>
Skills	<ul style="list-style-type: none"><li>• Analizează mostre de software malițios folosind tehnici statice și dinamice.</li><li>• Realizează investigații forensice pe memoria sistemelor și pe traficul de rețea pentru a detecta activități malițioase.</li><li>• Aplică instrumente specializate pentru investigarea comportamentului malware.</li><li>• Elaborează rapoarte și studii de caz pe baza rezultatelor analizei malware, sprijinind strategiile de apărare și luarea deciziilor în securitate.</li></ul>



<b>Responsibility and autonomy</b>	<ul style="list-style-type: none"> <li>• Demonstrează responsabilitate în manipularea și analiza mostrelor de malware în medii controlate și etice.</li> <li>• Aplică independent tehnici de analiză malware pentru investigarea și atenuarea amenințărilor cibernetice.</li> <li>• Colaborează eficient în activități de investigație malware realizate în echipă, împărțind rezultatele și contribuind la măsuri defensive colective.</li> <li>• Integrează în mod etic rezultatele analizei malware în practicile mai largi de securitate cibernetică, respectând cerințele legale și organizaționale.</li> </ul>
------------------------------------	--

## 8. Contents

8.1 Lecture	Teaching methods	No. of hours
1. Introducere. Clasificarea programelor malware	• Prelegere cu sinteza și esențializarea informațiilor	2
2. Tehnici de analiză malware	• Metode interactive de predare-învățare	2
3. Inginerie inversă. Aplicații executabile	• Dialog	2
4. Analiza scripturilor, documentelor și fișierelor web	• Metode care contribuie la dezvoltarea gândirii critice	2
5. Analiza memoriei calculatorului	• Învățare independentă și cooperativă	2
6. Analiza traficului de rețea	• Utilizarea de programe	2
7. Automatizare și hunting		2
<b>Bibliography</b> [1]. Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. ACM Computing Surveys (CSUR), 52(5), 1-48. [2]. Monnappa, K. A. (2018). Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. Packt Publishing Ltd. [3]. Mohanta, A., & Saldanha, A. (2020). Malware analysis and detection engineering: a comprehensive approach to detect and analyze modern malware. New York, NY, USA: Apress. [4]. Gritzalis, D., Choo, K. K. R., & Patsakis, C. (Eds.). (2024). Malware: Handbook of Prevention and Detection (Vol. 91). Springer Nature.		
8.2 Applications (seminar/lab/project)* <i>* Type of application to be chosen according to the nature of the course</i>	Teaching methods	No. of hours
Configurarea mediului de lucru		2
Utilizarea aplicațiilor specifice în procesul de analiză malware	• Dialog	4
Analiza documentelor malițioase	• Metode care contribuie la dezvoltarea gândirii critice	4
Malware networking		4



### Bibliography

- [1]. Mohanta, A., & Saldanha, A. (2020). Malware analysis and detection engineering: a comprehensive approach to detect and analyze modern malware. New York, NY, USA: Apress.
- [2]. Bhatia, S., & Gabhane, C. (2024). Reverse Engineering with Terraform: An Introduction to Infrastructure Automation, Integration, and Scalability Using Terraform. Apress.
- [3]. Dang, B., Gazet, A., & Bachaalany, E. (2014). Practical reverse engineering: x86, x64, ARM, Windows kernel, reversing tools, and obfuscation. John Wiley & Sons.

### 9. Evaluation

Type of activity	9.1 Evaluation criteria	9.2 Evaluation methods	9.3 Percentage of final grade
9.4 Lecture	Participare activă	Oral	10%
	Test grilă	Online	40%
9.5 Applications* <i>*Type of application to be chosen according to the nature of the course</i>	Participare activă	Prezentarea unui studiu de caz	10%
	Proiect	Prezentare	40%

#### 9.6 Minimum standard of achievement / Pass requirements

Promovarea testului grilă cu un punctaj de minimum 50% și demonstrarea capacității de a realiza analiza completă a cel puțin unei mostre de malware (document, fișier executabil sau captură de trafic de rețea).

Date of completion,  
18.09.2025

Lecture instructor,  
Surname/First name /Signature  
Lect. Dr. Ștefania Loredana Niță

Application instructor,  
Surname/First name /Signature  
Lect. Dr. Ștefania Loredana Niță

Date of approval at Department level,  
24.09.2025

Head of Department,  
Assoc. Prof. Pelican Elena, PhD

Dean,  
Assoc. Prof. Nicola Aurelian, PhD