**COURSE SYLLABUS**

***Malware analysis***

**1. Program identification details**

|  |  |
| --- | --- |
| 1.1 Higher education institution | „Ovidius” University of Constanta |
| 1.2 Faculty | Faculty Mathematics and Computer Science |
| 1.3 Department | Mathematics and Computer Science |
| 1.4 Field of studies | Computer Science |
| 1.5 Cycle of studies (degree) | Master |
| 1.6 Degree program/qualification | Cyber Security and Machine Learning |
| 1.7 Academic year | 2022-2023 |

**2. Course identification details**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2.1 Course title | | | **MALWARE ANALYSIS** | | | | |
| 2.2 Course code | | | **FMI.CSML.I.1.10** | | | | |
| 2.3 Instructor | | | Assoc. Prof. IONESCU Viorel, Ph.D. | | | | |
| 2.4 Teaching assistant | | | Assoc. Prof. IONESCU Viorel, Ph.D. | | | | |
| 2.5 Year | 1 | 2.6 Semester | 1 | 2.7. Evaluation type | C | 2.8 Course type \*/\*\* | DAP/DO |

*\* DF – fundamental course, DD – field course, DS – specialty course, DC – complementary course, DAP – advanced study course, DSI – synthesis course, DCA – advanced knowledge course.*

*\*\* DI – mandatory course; DO – optional course.*

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3.1 Number of teaching hours/week | | 2 | of which:  3.2 course | 1 | 3.3 applications*\*\*\** | 1 |
| 3.4 Total of teaching hours within the program/semester | | 28 | of which:  3.5 lecture | 14 | 3.6 seminar | 14 |
| **3.7 Student workload for individual study** | | | | | | 72 |
| ***Distribution of workload*** | | | | | | [hours] |
| Individual study of texbooks, handbooks/reader, bibliography and notes | | | | | | 16 |
| Additional research (library, electronic resources, fieldwork) | | | | | | 10 |
| Homework (preparing seminar presentations, portfolios, critical essays, research papers, etc.) | | | | | | 28 |
| Individual consultations (optional) | | | | | | 14 |
| Evaluations / exams | | | | | | 4 |
| Other activities | | | | | | 0 |
| **3.8 Total hours per semester** | *28+72=100* | |  |  |  |  |
| **3.9 Number of credits** | 4 | |  |  |  |  |

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

**4. Prerequisites (if any)**

|  |  |
| --- | --- |
| 4.1 Curriculum-related | Undergraduade studies; |
| 4.2 Skills-related |  |

**5. Requirements (if any)**

|  |  |
| --- | --- |
| 5.1. For running the course |  |
| 5.2. For running the seminar / laboratory /project  *\*The type is to be chosen according to the discipline* |  |

**6. Acquired specific skills**

|  |  |
| --- | --- |
| Professional skills | Ability toquickly identify and respond to different types of cyber attacks |
| Cross-cutting skills | Execution of complex professional tasks, in conditions of autonomy and professional independence, involving the detection and solving of related problems in the development of a software application.  Efficient development of activities organized in an interdisciplinary group and development of empathic capacities for interpersonal communication, relationships and collaboration with various groups. |

**7. Course goal and objectives**

|  |  |
| --- | --- |
| 7.1 The general objective of the course | Mastering theoretical knowledge and practical skills needed to quickly identify and respond to different types of cyber attacks. |
| 7.2 Specific objectives | Use of system and network monitoring applications |

**8. Contents**

|  |  |  |
| --- | --- | --- |
| **8.1 Lecture** | **Teaching methods** | **Number of hours** |
| Introduction. Malware classification | Lecture with the synthesis and essentialization of information  Interactive learning teaching methods  Dialogue  Problematization  Conversation  Methods that contribute to the development of critical thinking  Programs  Independent and cooperative learning | 2 hours |
| Malware analysis techniques | 2 hours |
| Reverse engineering. Executable applications | 2 hours |
| Analysis of scripts, documents and web files | 2 hours |
| Computer memory analysis | 2 hours |
| Network traffic analysis | 2 hours |
| Automation and hunting | 2 hours |
| **Bibliography:**   1. M. Davis, S. Bodmer, A. LeMasters, *Hacking exposed. Malware & rootkits: secrets and solutions*, McGraw-Hill company, 2010 2. M. Christodorescu, S. Jha, D. Maughan, S. Song, C. Wang, *Malware Detection*, Springer, 2007 3. B. Dang, A. Gazet, E. Bachaalany, *Practical Reverse engineering. X86, x64, ARM, Windows Kernel, Reversing tools and obfuscation*, John Wiley & sons, 2014 | | |

|  |  |  |
| --- | --- | --- |
| **8.2 Applications\* (seminar / laboratory / project)**  *\*The type is to be chosen according to the discipline* | **Teaching methods** | **Number of hours** |
| Install malware and sandbox analysis lab | Dialogue  Problematization  Conversation  Methods that contribute to the development of critical thinking  Programs  Independent and cooperative learning | 2 hours |
| Applications used in the malware analysis process | 4 hours |
| Analysis of malicious documents | 4 hours |
| Malware networking | 4 hours |
| **Bibliography:**   1. M. Davis, S. Bodmer, A. LeMasters, Hacking exposed. Malware & rootkits: secrets and solutions, McGraw-Hill company, 2010 2. M. Christodorescu, S. Jha, D. Maughan, S. Song, C. Wang, Malware Detection, Springer, 2007 3. B. Dang, A. Gazet, E. Bachaalany, *Practical Reverse engineering. X86, x64, ARM, Windows Kernel, Reversing tools and obfuscation*, John Wiley & sons, 2014 | | |

**9. Correlation between the content of the course and the needs/expectations of the epistemic community, professional associations and/or significant employers relevant for the program**

|  |
| --- |
| Analyzing the behavior of malware applications, so that security engineers can detect, combat and remove them from the computer as quickly as possible. |

**10. Evaluation**

|  |  |  |  |
| --- | --- | --- | --- |
| Type of activity | 10.1 Evaluation criteria | 10.2 Evaluation methods | 10.3 Percentage of final grade |
| 10.4 Course | Active participation | Oral | 10% |
| 10.5 Applications\*  (Seminar/Laboratory / Project)  *\*The type is to be chosen according to the discipline* | Active participation | Oral | 10% |
|  | Project | Oral | 40% |
|  | Exam | Oral | 40% |
| 10.6 Minimum standard of achievement for the acquisition of the ECTS credits | | | |
| Analysis of PDF malicious documents | | | |

Date of completion Course Instructor, Teaching Assistant,

20.09.2022 Assoc. Prof. IONESCU Viorel, Ph.D. Assoc. Prof. IONESCU Viorel, Ph.D.

Date of approval in the Department Head of Department,

27.09.2022 Assoc. Prof. Puchianu Crenguta, Ph.D

Dean,

Assoc. Prof. Nicola Aurelian, Ph.D