Malware analisys and engineering

Academic Year: (2020 / 2021) **Review date: 12-11-2020**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: ESTEVEZ TAPIADOR, JUAN MANUEL

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

- Software Systems Exploitation
- Secure Communications
- Data Protection
- Cyberdefense Systems
- Cyberattack Techniques
- Cybercrime, Cyberterrorism, and Cyberwar

OBJECTIVES

Master the knowledge required to propose original designs or developments, often in a research process within the area of cyber security.

Ability to apply acquired knowledge to solve problems under novel or almost novel situations or within broader (multidisciplinar) contexts related with cyber security.

Ability to state critical opinions and judgements having incomplete or limited information in the field of cyber security. These judgements must take into account include considerations about social and ethical responsibilities.

Discuss in a public audience about their acquired knowledge, and the conclusions from the work. Students will be able to give their foundational and most convincing reasons to a specialized and non specialized audience in a clear way, without ambiguities.

Students should have the learning skills required to continue studying in a autonomous or self-directed way.

Understand and apply methods and techniques to investigate vulnerabilities of a given site.

Create and refine concise and comprehensively documents, plans and projects in the scope of cyber security.

Know the relevant technique part of the legal regulation in cyber security and its implications in the design of systems and security tools.

Analyze and detect anomalies and attack signatures y systems and networks.

Analyze and detect ocultation techniques in attacks to systems and networks.

Knowledge of trends in the cyber attacks techniques and knowledge about learned experiences in real cases.

Know and apply the cryptographic and steganographic mechanisms required to protect data stored in a system or data transiting a network.

DESCRIPTION OF CONTENTS: PROGRAMME

1 Introduction
1.1 Basic Concepts and Evolution
1.2 Malware Analysis Techniques
1.3 The Lab

2 Basic Analysis Techniques
2.1 The Life of an Executable
2.2 Basic Static Analysis
2.3 Basic Dynamic Analysis

3 Advanced Analysis Techniques
3.1 x86 Disassembly
3.2 C Code Constucts in Assembly
3.3 IDA Pro
3.4 The Windows API
3.5 Debugging

4 Behaviors
4.1 Downloaders
4.2 Backdoors
4.3 Info Stealers
4.4 Persistence
4.5 Covert Launching
4.6 Data Encoding
4.7 Anti-disassembly
4.8 Anti-debugging
4.9 Anti-virtualization
4.10 Packers

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES:

- Lectures and practicals
- Lab sessions
- Tutorship
- Group work
- Individual work

METHODOLOGIES

- Lectures to introduce and discuss the main course concepts.

- Study and analysis of references provided by the lecturer, including academic papers, reports, selected book chapters, and press articles. This will be instrumental to consolidate and complement concepts introduced in the course, and also as material to be discussed during some lectures.

- Analysis of practical cases proposed by the lecturer, either individually or in group.

- Presentation and discussion of topics and practical cases related to the course.

- Preparation of individual essays and reports.

ASSESSMENT SYSTEM

The assessment system is based on practical laboratories in groups, and possibly the delivery of individual assignments, as well as a final exam. Specifically, the assessment of the subject is split into:

Continuous assessment (60% of the final mark)

Final Exam (40% of the final mark)

The extraordinary assessment will be as follows:
- A single exam weighting 30% of the final mark, in case that the continuous assessment has been passed (i.e., with a mark greater than or equal to 25%). Note that students may deliver the labs up to two weeks before the final exam.
- A single exam weighting 100% of the final mark, in case that the continuous assessment is failed. This exam will include questions regarding the labs.

% end-of-term-examination:	40
% of continuous assessment (assigments, laboratory, practicals…):	60

BASIC BIBLIOGRAPHY

- Michael Ligh, Steven Adair, Blake Harstein, Matthew Richard Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, Wiley, 2010
- Michael Sikorski, Andrew Honig Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012