Computer Forensics

Academic Year: (2023 / 2024) **Review date: 28-04-2023**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: PERIS LOPEZ, PEDRO

Type: Electives ECTS Credits : 3.0

Year : 4 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

1. Programming.
2. Techniques of information hiding.
3. Information security management.
4. Forensic Science II.
5. Vulnerabilities, threats and computer security protocols.

OBJECTIVES

- Identify security objectives and vulnerabilities, threats and risks of a given information system in a defined operational environment.
- Evaluate the security services to be implemented in a given system and design and implement mechanisms and subsequent protocols.
- Evaluate and implement appropriate authentication mechanisms to access a specific system.
- Use the signature and certification systems in a particular environment.
- Design a security plan, developing the various parts of it, assessing their compliance over time and correcting deviations. Analyze and manage the risks of a particular installation.
- Develop a comprehensive recovery plan for an actual installation. Conduct a compliance audit of files and systems containing personal data.
- Use the tools that allow control of operating systems, mainly Windows and Linux.
- Manage the main techniques of collection, identification and analysis of events, guaranteeing the assurance testing and preserving the chain of custody of them. Assess and manage systems secure erase and data recovery.
- Implement databases over a transmission system. Assess and use different techniques to integrate data mining: extraction techniques and modeling analysis.

The course covers forensics tools, methods, and procedures used for investigation of computer crime, techniques of data recovery, protection and gathering of evidences, and expert witness skills.

Upon successful completion of this course, the student will be able to:

1. Know and use the methodology commonly used in computer forensics investigations.
2. Know and use methods for evidence gathering.
3. Use and evaluate various techniques for evidence analysis in file systems, memory and networks.
4. Install, configure and use forensics tools.
5. Get acquainted with hardware devices used in computer forensics investigations.
6. Retrieve, manipulate and organize evidences systematically.
7. Write forensics reports.
8. Know and use standards and legal regulations linked with computer forensics investigations.

DESCRIPTION OF CONTENTS: PROGRAMME

Module 1

a. Introduction.
b. Key technical concepts.

Module 2

a. Labs and Tools.
b. Evidence collection and archiving.
c. Forensic Report.

Module 3
a. Anti-forensics tools and techniques.
b. Steganography and covert channels.

Module 4.
a. Internet and email.
b. Logs (local and network).
c. Network forensics.
d. Cloud forensics.

LEARNING ACTIVITIES AND METHODOLOGY

Lectures, where the main theoretical concepts of the subject will be described and explained. The students will be able to follow these lectures using the appropriate course material as well as the corresponding intranet tools and bibliography. References will help the students to further elaborate on any topic of their interest.

Lab sessions in computer labs where the students will work with forensics tools. Real forensics cases will be introduced and the students will have to solve several exercises that will help them to strengthen their theoretical knowledge and get acquainted with forensics tools.

ASSESSMENT SYSTEM

The grading system includes continuous assessment of the student's work (tests assessing skils, theoretical, and practical concepts, and also laboratory tasks) and a final assessment through a written exam that will assess the concepts, skills, and abilities acquired throughout the module.

Grading will be done according to the following criteria:

1. Written exams containing both theory and problems: 70% of the final mark, consisting of:
   1.1. Continuous assessment exam: 15% of the final mark. This will take place approximately by mid-term.
   1.2. Final written exam: 55% of the final mark. To pass the module, the student must get a minimum grade of 4 in this exam.
2. Lab sessions: 30% of the final mark.

In the extraordinary exam, the student will choose between:
a) A final written exam accounting for 100% of the final grade. This exam consists of theory, problems, and practical material covered in the lab sessions; or
b) A final written exam accounting for 60% of the final grade. This exam consists of theory and problems. The remaining 45% comes from the grade obtained during the term in the continuous assessment exam (10%) and lab sessions (30%).

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

BASIC BIBLIOGRAPHY

- Brian Carrier File System Forensic Analysis., Addison-Wesley Professional.
- Cory Altheide and Harlan Carvey Digital Forensics with Open Source Tools, Syngress Media.
- John Sammons The Basics of Digital Forensics. , Syngress.
- Nelson et al. Guide To Computer Forensics and Investigations, Cengage Learning.

ADDITIONAL BIBLIOGRAPHY

- Eoghan Casey Handbook of Digital Forensics and Investigation, Academic Press Inc.
- Harlan Cavey Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry, Syngress Media.