Persistent Threats and Information Leakage

Academic Year: (2022 / 2023) **Review date: 19-01-2023**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: FUENTES GARCIA ROMERO DE TEJADA, JOSE MARIA

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

None.

OBJECTIVES

COMPETENCES

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.

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

Analyze and detect hiding 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.

LEARNING OUTCOMES

Regarding learning outcomes, this course contributes to the following ones:

Knowing the type of information and defense mechanisms deployed in a system, explain the impact of different threats and intrusions and, in particular, information leaks.

Explain the mechanisms that can be used to conceal an intrusion in a system.

DESCRIPTION OF CONTENTS: PROGRAMME

Persistent threats and information leakage:

1. Persistent threats
1.1. Persistent techniques in compromised systems
1.2. APTs. Definitions, description and analysis. Current trends.
1.3. Advanced Command and Control Techniques
1.4. Stealthiness and evasion mechanisms. Rootkits

2. Covert channels. Steganography and steganalysis
2.1. Science of steganography definition. History
2.2. Steganographic system classification. Security evaluation
2.3. Modern steganography
2.4. Modern steganalysis

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES
Theoretical lectures
Practical lectures
Mixed theoretical and practical lectures
Laboratory practices
Tutoring sessions
Teamwork
Individual work by the student

LEARNING METHODOLOGY
Lectures by means of audiovisual media and computes. The main concepts will be exposed and bibliography will be provided to complete the students learning.
Critical reading of recommended texts provided by the teacher:
Press articles, reports, manuals, academic papers, etc. A further discussion can be done in class or it can be considered a way to consolidate and expand the knowledge on the subject.
Practical case resolution, problems, etc. They can be assigned by the teacher in a team or individual manner
Report assignments that can be done either individually or in group

ASSESSMENT SYSTEM

The assessment may be continuous assessment or non-continuous assessment:

Ordinary sitting - continuous assessment only:
· End of term examination (30% of the final mark)
- A minimum grade of 4.0 is mandatory to pass the subject
· Periodical assignments (70% of the final mark)
A set of individual or in-groups assignments will be proposed. All of them have to be handed-in.

Extraordinary sitting
In the extraordinary sitting, the following rules apply:

a. If the student followed the continuous assessment method, the exam will have the same relative weight as in the ordinary sitting. The mark of the continuous evaluation is kept.
b. Otherwise, students will have an exam counting for 100% of the final mark. This exam may contain questions related to the proposed assignments. Assignments cannot be re-delivered in this sitting.

% end-of-term-examination:	30
% of continuous assessment (assigments, laboratory, practicals…):	70

BASIC BIBLIOGRAPHY

- Eric Cole Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization, Syngress, 2012
- Shabtai, Asaf, Elovici, Yuval, Rokach, Lior A Survey of Data Leakage Detection and Prevention Solutions, Springer, 2012
- Thales and Verint The cyberthreat handbook, Thales, 2019

ADDITIONAL BIBLIOGRAPHY

- ISACA Advanced Persistent Threats: How To Manage The Risk To Your Business , ISACA, 2015

BASIC ELECTRONIC RESOURCES

- George Silowash, Christopher King . Insider Threat Control: Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34008
- ThaiCert . Threat Group Cards: A Threat Actor Encyclopedia 2.0: https://apt.thaicert.or.th/cgi-bin/aptgroups.cgi

- Thales group and Verint . The Cyberthreat handbook: https://thalesgroup-myfeed.com/THECYBERTHREATHANDBOOK