Cyber attack techniques

Academic Year: (2023 / 2024) **Review date: 21-04-2023**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: ALMENARES MENDOZA, FLORINA

Type: Compulsory ECTS Credits : 6.0

Year : 1 Semester : 1

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

This subject requires knowledge and skills gained in previous studies or in professional activities.
Students should work comfortable in Unix environments and have programming knowledge of some interpreted language such as Python, Ruby or shell scripting. They also need knowledge on communication networks, knowing the TCP/IP stack is basic to this subject. Knowledge of some Linux and Windows network administrative tools is also needed.

OBJECTIVES

This compulsory course strengthens the acquisition of the following basic and general competences:
- CB6: Master the knowledge required to propose original designs or developments, often in a research process within the area of cyber security.
- CB7: Ability to apply acquired knowledge to solve problems under novel or almost novel situations or within broader (multidisciplinar) contexts related with cyber security.
- CB8: 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
- CB9: 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.
- CB10: Students should have the learning skills required to continue studying in a autonomous or self-directed way.
- CG1: Create and refine concise and comprehensively documents, plans and projects in the scope of cyber security.
- CG3: Understand and apply methods and techniques to investigate vulnerabilities of a given site.
- CG4: Know the relevant technique part of the legal regulation in cyber security and its implications in the design of systems and security tools.

This compulsory course strengthens the acquisition of the following specific competences:
- CE1: Annalyze and detect anomalies and attack signatures y systems and networks.
- CE2: Analyze and detect ocultation techniques in attacks to systems and networks.
- CE3: Knowledge of trends in the cyber attacks techniques and about learned experiences in real cases.
- CE7: Know and apply the cryptographic and steganographic mechanisms required to protect data stored in a system or data transiting a network.

LEARNING OUTCOMES
This course contributes to the following learning outcomes:

Acquire remotely intelligence of technical origin about the components of a target system, using open sources as well as enumeration and reconnaissance techniques.

Detect, in a fixed time, a high percentage of the vulnerabilities of a given network system

Explain at least one way of compromising a system which have detected vulnerabilities.

Justify through reasoned reports the detected vulnerabilities and the detailed procedure to be followed to perform the intrusion.

Explain other attack techniques to a system that is not vulnerable to direct intrusion.

Given the dependencies among the different network services of a system, explain how different proposed attack would evolve and how the different parts and the total would be affected of each of those attacks.

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.

Propose different attacks that may be performed from inside a system in a controlled environment and explain the consequences.

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

DESCRIPTION OF CONTENTS: PROGRAMME

1. Introduction to cyber attacks techniques
1.1. Concepts and definitions
1.2. Types of cyber attacks
1.3. Phases of a intrusion

2. Acquiring information on the target and vulnerability analysis
2.1. Techniques of intelligence. Open sources
2.2. Network and port scanning
2.3. Identification and vulnerability analysis

3. Explotation
3.1. Exploiting software and authentication systems
3.2. Resource consumption/exhaustion and Denial of Service
3.3. Social Engineering, malware and evasion techniques

4. Persistence
4.1. Evidence hiding
4.2. Privilege scaling
4.3. Preparing alternative access channels
4.4. Presence hiding

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES
Theoretical lectures
Practical lectures
Laboratory practices
Tutoring sessions
Teamwork
Individual work by the student

TEACHING METHODOLOGIES
- Class lectures in which the main concepts of the subject are developed and the literature is provided to supplement student learning.
- Critical reading recommended by the subject teacher texts:
* Newspaper articles, reports, manuals, and / or scholarly articles, for subsequent class discussion to expand and consolidate the knowledge of the subject.
- Resolution of laboratory practices and problems posed by the teacher individually or in group.

ASSESSMENT SYSTEM

To opt in the continuous evaluation all the assignments and exams are required. Else, the assessment will be exclusively based in the final exam, with a maximum 80% of the mark in the ordinary and 100% of the mark in the extraordinary evaluation.

Continuous evaluation will be based in student involvement and participation, problems and study cases and laboratory assignments.
There will be between three to four assignments, that will be performed in groups and will count a 70% of the final assessment.
There will be two exams, that will count a 30% of the final assessment. A minimum media is required in the exams, else the students will be required a minimum grade in the final exam with the same assessment: 70% assignments and 30% exam.

% end-of-term-examination:	0
% of continuous assessment (assigments, laboratory, practicals…):	100

BASIC BIBLIOGRAPHY

- Broad, James, CISSP y Bindner, Andrew Hacking with Kali: practical penetration testing techniques, Syngress (Elsevier), 2014
- Peter Kim The Hacker Playbook: Practical Guide To Penetration Testing, CreateSpace Independent Publishing Platform, 2014

ADDITIONAL BIBLIOGRAPHY

- Johnny Long Google Hacking for Penetration Testers, Syngress, 2011
- Sparc Flow HOW TO HACK LIKE A GHOST: Breaching the Cloud, No Starch Press, Inc. www.nostarch.com, 2021

BASIC ELECTRONIC RESOURCES

- Kali Linux . Penetration Testing Distribution: https://www.kali.org/
- OWASP . Web Security: https://owasp.org