Cyber defense systems

Academic Year: (2023 / 2024) **Review date: 07-09-2023**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: PASTRANA PORTILLO, SERGIO

Type: Compulsory ECTS Credits : 6.0

Year : 1 Semester : 1

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.

Create, design, deploy and maintain a cyber defense global system in a given context.

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 systems to find attack evidences and to adopt the required measures to maintain the custody chain of the found evidences.

Apply the suited services, mechanisms and security protocols to a given case.

Design and evaluate security architectures of systems and networks.

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

Analyze the risks of introducing personal devices in a corporate professional environment (Bring your own device).
Know and apply the measures to control the risks.

LEARNING OUTCOMES
This course contributes to the following learning outcomes:

Design strategies to distribute sensors in a network and analyze observed events to determine which are relevant in a particular case.

Given a system under attack, identify the features of most of these attacks and point out the most probable sources.

Given an attack and its source, propose countermeasures to counteract it explaining its efficacy. Evaluate network zoning strategies and design traffic filtering policies.

To design and evaluate appropriate measures for the identification and authentication of users and management of identities and associated authorizations.

DESCRIPTION OF CONTENTS: PROGRAMME

Cyber Defense Systems:
1. Introduction to Cyber Defense

2. Local sensors: Audit and analysis of events
  2.1. Management of users and accesses
  2.2. Analysis of security logs

3. Firewall and network segmentation:
  3.1. Fundamentals of traffic filtering
  3.2. Types of firewalls
  3.3. Network segmentation

4. Detection and prevention of attacks
  4.1. Signature detection
  4.2. Anomaly detection
  4.3. Automated response to intrusion attacks

5. Security Information and Event Management (SIEM)
  5.1. Introduction and SIEMs architectures
  5.2. Aggregation and correlation rules
  5.3. Intrusion detection networks
  5.4. Strategies for network sensing

LEARNING ACTIVITIES AND METHODOLOGY

The course will consists of the following elements:

-- Master classes
-- Lab Sessions
-- Practical Exercises
-- Lab Assignments
-- Tutoring

ASSESSMENT SYSTEM

The assessment system is based on practical laboratories in groups, as well as a individual 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). A minimum mark of 3.5 out of 10 points is required.

The extraordinary assessment will be based on a single exam weighting 100% of the final mark. This exam will include questions regarding the labs.

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

BASIC BIBLIOGRAPHY

- P.W. Singer Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press , 2014

- Anton A. Chuvakin, Kevin J. Schmidt Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management, Syngress, 2012
- Brian Caswell, Jay Beale, Andrew Baker Snort Intrusion Detection and Prevention Toolkit, Syngress, 2007

- Chris Sanders, Jason Smith Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress, 2013
- David R. Miller , Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask Security Information and Event Management (SIEM) Implementation , Network Pro Library, 2010
- Dobromir Todorov Mechanics of User Identification and Authentication: Fundamentals of Identity Management , Auerbach Publications , 2007
- J. Michael Stewart Network Security, Firewalls And Vpns, Jones & Bartlett Learning, 2013

- Richard Bejtlich The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, 2013
- Timur Mehmet Firewall Hacking Secrets For Security Professionals, HackerStorm.com Publishing, 2013