COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

Syllabus
2020 - 2021

GENERAL INFORMATION

Data of the subject	
Subject name	Forensic Monitoring, Detection and Analysis
Subject code	DTC-MCS-524
Mainprogram	
Involved programs	Máster en Ciberseguridad [Primer Curso]
Level	Master
Quarter	Semestral
Credits	3,0 ECTS
Type	Obligatoria
Department	Department of Telematics and Computer Sciencies
Course overview	To familiarize the student with the foundations on which detection tools such as logs and events of Windows and Linux and the analysis of traffic and its dump are based. Establish the bases on the tools for the operation of the monitoring systems, events and information systems (SIEM), the specific approach for intrusion detection (IDS), and understand the correlation mechanisms, generation or import of rules. The specific part of industrial systems will also be covered, both for the inclusion of monitoring with specific tools in industrial networks and for the discovery of specific tools for open sources. The forensic part will include both the forensic understanding related to the judicial field (regulations, preservation of evidence, chain of custody) and the familiarization with the forensic analyst's own tools for computer equipment (memory dump, disk dump, evidence analysis) and extension to mobile devices.

Teacher Information	
Teacher	
Name	Agustín Valencia Gil-Ortega
Department	Department of Telematics and Computer Sciencies
EMail	avalencia@icai.comillas.edu
Teacher	
Name	Antonio Carmona Rosanes
Department	Escuela Técnica Superior de Ingeniería (ICAI)
EMail	acarmona@icai.comillas.edu

DESCRIPTION OF THE SUBJECT

Contextualization of the subject

Prerequisites

Basic knowledge about Virtual Machines

Course contents

Contents
Monitoring and Detection
Monitoring
-Fundamentals of monitoring -Event generation: Linux -Event generation: Windows -Event generation: Adding sources -Monitoring traffic
Detection
-Detection with IDS -Detection with YARA and SIGMA -Repositories
Correlation
-Open sources -External sources -SIEM correlation
Industrial point of view
Forensic Analysis
Fundamentals and first response
Documentation: Minutes, chain of custody, worksheet
First response, acquisition and analysis tools.
Analysis of digital evidence
Advanced techniques. Storage. Low-level analysis

EVALUATION AND CRITERIA

Grading
Evaluation Criteria: Monitoring (66.6% of the final grade)

- 60% Lab
- 40% Final Exam

Forensic Analysis (33.3% of the final grade)

- 50% Lab, Documenting (Mintures, Evicendes, Worksheets) and Expert Report
- 50% Quiz before each class, and Final Exam.

BIBLIOGRAPHY AND RESOURCES

Basic References

MONITORIZACIÓN:

Libros: Security Information and Event Management (SIEM) Implementation. McGrawHill. 2011. David R.Miller
OSSIM: https://cybersecurity.att.com/products/ossim
IBM Qradar: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_oview.html
Snort: https://www.snort.org/
Yara: https://virustotal.github.io/yara/
Sigma: https://github.com/Neo23x0/sigma
Sysinternals: https://docs.microsoft.com/en-us/sysinternals/
Ossec: https://www.ossec.net/
Wireshark: https://www.wireshark.org/
Censys: https://censys.io/
Shodan: https://www.shodan.io/
MISP: https://www.misp-project.org/

FORENSE:

SANS: https://digital-forensics.sans.org/
Forensic focus: https://www.forensicfocus.com/
Interpol: https://www.interpol.int/How-we-work/Innovation
Europol: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
ENFSI: http://enfsi.eu/about-enfsi/structure/working-groups/information-technology/
XDA developers: https://www.xda-developers.com/
NFI: https://www.forensischinstituut.nl/
Informes de evaluación de herramientas forenses: https://www.dhs.gov/
Estándares y metodologías USA: https://www.nist.gov/
Estándares ISO: https://www.iso.org/
Android: https://developer.android.com/
Autopsy: https://www.sleuthkit.org/
Ftk Imager: https://accessdata.com/product-download/ftk-imager-version-4-2-0
Nirsoft:
USBdeview: https://nirsoft.net/utils/usb_devices_view.html

Launcher: https://launcher.nirsoft.net/
Volatility: https://www.volatilityfoundation.org/
Testdisk y photorec: https://www.cgsecurity.org/wiki/TestDisk_ES