English version at the end of this document

Ano Letivo	2022-23
Unidade Curricular	ANÁLISE FORENSE DE SISTEMAS COMPUTACIONAIS
Cursos	CIBERSEGURANÇA
Unidade Orgânica	Faculdade de Ciências e Tecnologia
Código da Unidade Curricular	19381006
Área Científica	
Sigla	
Código CNAEF (3 dígitos)	481
Contributo para os Objetivos de Desenvolvimento Sustentável - ODS (Indicar até 3 objetivos)	4, 9, 11
Línguas de Aprendizagem	Inglês

Modalidade de ensino

B-Learning

Docente Responsável JÚLIO CARLOS BOTEQUILHA FERNANDES

DOCENTE	TIPO DE AULA	TURMAS	TOTAL HORAS DE CONTACTO (*)
JÚLIO CARLOS BOTEQUILHA FERNANDES	PL; T	T1; PL1	28T; 28PL

* Para turmas lecionadas conjuntamente, apenas é contabilizada a carga horária de uma delas.

ANO	PERÍODO DE FUNCIONAMENTO*	HORAS DE CONTACTO	HORAS TOTAIS DE TRABALHO	ECTS
1º	S2	28T; 28PL	150	6

* A-Anual;S-Semestral;Q-Quadrimestral;T-Trimestral

Precedências

Sem precedências

Conhecimentos Prévios recomendados

N/A

Objetivos de aprendizagem (conhecimentos, aptidões e competências)

A Unidade Curricular de Análise Forense de Sistemas Computacionais pretende dotar o estudante com conhecimentos que lhe permita conhecer o processo de investigação digital e das técnicas de cibercrime. É ainda objetivo desenvolver a capacidade do estudante de recolher a informação de suportes digitais, analisa-la e elaborar relatórios forenses de sistemas que foram comprometidos. Pretende ainda dotar o estudante de conhecimento das ferramentas e técnicas utilizadas deteção, recolha de informação e de reverse engineering para a análise do cibercrime e deteção dos cibercriminosos e das técnicas utilizadas.

Conteúdos programáticos

- Conceito de Análise Forense e técnicas de cibercrime;
- O Processo de investigação digital;
- Metodologias de recolha e análise de informação de sistemas comprometidos;
- Reverse Engineering para deteção dos eventos efetuados e comunicações estabelecidas;
- Ferramentas e técnicas de análise forense;
- Elaborar um relatório de auditoria forense;

Metodologias de ensino (avaliação incluída)

A presente unidade curricular combina diversos métodos de ensino:

- Exposição dos conteúdos programáticos, através das aulas teóricas
- Práticas laboratoriais de auditorias forenses em sistemas utilizando diversas ferramentas para o efeito e de análise e relatório forenses dos sistemas comprometidos;
- Apresentações orais dos trabalhos de grupo
- Atendimento individual ou em grupo para esclarecimento de dúvidas
- Apoio às atividades e esclarecimento sobre funcionamento da unidade curricular.

A avaliação é contínua, com exame final e inclui:

- Teste individual para a avaliação de conhecimentos (50%)
- Trabalho de grupo com apresentação oral/discussão (50%)

Os estudantes que obtiverem uma classificação final igual ou superior a 9,5 valores em cada elemento de avaliação estão dispensados do exame final.

Bibliografia principal

William Oettinger (2020), Learn Computer Forensics: A beginner's guide to searching,analyzing, and securing digital evidence, Packt Publishing, ISBN-10: 1838648178

Ric Messier (2017), Network Forensics, Wiley, ISBN-10: 9781119328285

Nadean H. Tanner (2019), Cybersecurity Blue Team Toolkit, Wiley, ISBN-10: 1119552931

Saed Alrabaee and Mourad Debbabi (2020), Binary Code Fingerprinting for Cybersecurity: Application to Malicious Code Fingerprinting, Springer, ISBN-10: 3030342379

Gerard Johansen (2020), Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition, Packt Publishing, ISBN-10: 183864900X

Alex Matrosov (2019), Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats, No Starch Press, ISBN-10: 1593277164

Academic Year	2022-23
Course unit	
Courses	
Faculty / School	FACULTY OF SCIENCES AND TECHNOLOGY
Main Scientific Area	
Acronym	
CNAEF code (3 digits)	481
Contribution to Sustainable Development Goals - SGD (Designate up to 3 objectives)	4, 9, 11
Language of instruction	English
Teaching/Learning modality	B-Learning

Coordinating teacher JÚLIO CARLOS BOTEQUILHA FERNANDES

Teaching staff	Type	Classes	Hours (*)
JÚLIO CARLOS BOTEQUILHA FERNANDES	PL; T	T1; PL1	28T; 28PL

* For classes taught jointly, it is only accounted the workload of one.

Contact hours

T	TP	PL	TC	S	E	OT	O	Total
28	0	28	0	0	0	0	0	150

T - Theoretical; TP - Theoretical and practical ; PL - Practical and laboratorial; TC - Field Work; S - Seminar; E - Training; OT - Tutorial; O - Other

Pre-requisites

no pre-requisites

Prior knowledge and skills

N/A

The students intended learning outcomes (knowledge, skills and competences)

The Curricular Unit of Computer Systems Forensic Analysis intends to provide the student with knowledge that allows him to come to know the process of digital investigation and cybercrime techniques. It also aims to develop the student's ability to collect information from digital media, analyze it and prepare forensic reports of systems that have been compromised. It also intends to provide the student with knowledge of the tools and techniques used to detect, collect information and reverse engineering for the analysis of cybercrime and the detecting of cybercriminals and the techniques used.

Syllabus

- Forensic Analysis Concept and Cybercrime techniques;
- The Digital Investigation Process;
- Methodologies for collecting and analyzing information from compromised systems;
- Reverse Engineering for detection of happened events and established communications;
- Techniques and Tools for Forensic Analysis;
- Preparing a forensic audit report;

Teaching methodologies (including evaluation)

This curricular unit combines various teaching methods:

- Program content exhibition through theoretical lectures
- Practice laboratorial lessons, with an autonomous hands on project in forensic audits that explores various tools for this subject and that create forensic analysis reports for compromised systems;
- Oral group presentations on developed work project
- Individual or group attendance for out of classroom support;
- Activity support and curricular unit functioning clarification.

Evaluation is continuous with a final exam, and includes:

- Individual knowledge evaluation test (50%)
- Hands on Group Project development with oral presentation (50%)

Students that achieve a final grade of 9.5 or higher in each of the evaluation components, are excused from the final exam.

Main Bibliography

William Oettinger (2020), Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence, Packt Publishing, ISBN-10: 1838648178

Ric Messier (2017), Network Forensics, Wiley, ISBN-10: 9781119328285

Nadean H. Tanner (2019), Cybersecurity Blue Team Toolkit, Wiley, ISBN-10: 1119552931