English version at the end of this document

Ano Letivo	2022-23
Unidade Curricular	IDENTIFICAÇÃO, ANÁLISE E EXPLORAÇÃO DE VULNERABILIDADES
Cursos	CIBERSEGURANÇA
Unidade Orgânica	Faculdade de Ciências e Tecnologia
Código da Unidade Curricular	19381000
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 Joel David Valente Guerreiro

DOCENTE	TIPO DE AULA	TURMAS	TOTAL HORAS DE CONTACTO (*)
Joel David Valente Guerreiro	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	S1	28T; 28PL	150	6

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

Precedências

Sem precedências

Conhecimentos Prévios recomendados

Não Aplicável.

Objetivos de aprendizagem (conhecimentos, aptidões e competências)

A Unidade Curricular de Deteção, Análise e Exploração de Vulnerabilidades pretende dotar o estudante de conhecimentos que lhe permita identificar, analisar a exploração de vulnerabilidades, utilizando ferramentas de deteção de vulnerabilidades, obtendo conhecimento e implementando técnicas para determinar e limitar as vulnerabilidades. Pretende também o desenvolvimento de competências de planeamento, conceção e análise das vulnerabilidades, aplicar técnicas e protocolos de resposta para a defesa e implementando modelos que detetem e impeçam ataques informáticos. É objetivo também a aquisição de conhecimentos para uma análise das vulnerabilidades existentes numa organização.

Conteúdos programáticos

- Conceito de vulnerabilidades e de segurança ativa;
- Vulnerabilidades físicas, software, desenvolvimento e serviços;
- Metodologias e ferramentas de deteção de vulnerabilidades;
- Análise e exploração de vulnerabilidades;
- Ferramentas e técnicas de avaliação e limitação de vulnerabilidades;
- Implementação de modelos de defesa e deteção de ataques.

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 deteção, análise e limitação de vulnerabilidades, assim como trabalho autónomo;
- 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

- Morey J. Haber and Brad Hibbert (2018), *Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations* , Apress ISBN-10: 1484236262
- Christopher J. Hodson (2019), *Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls* , Kogan Page, ISBN-10: 0749484128
- Andrew Magnusson (2020), *Practical Vulnerability Management: A strategic Approach to Managing Cyber Risk* , No Starch Press, ISBN-10: 1593279884
- Cyber Security Resource (2021), *Vulnerability Management Program Guide: Managing the Threat and Vulnerability Landscape* , independently published, ISBN-13: 979-8713500658
- Yuri Diogenes and Erdal Ozkaya (2018), *Cybersecurity ? Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics* , Packt Publishing, ISBN-10: 9781788475297
- Heather Adkins et al (2020), *Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems 1 st* , O?Reilly, ISBN-10: 1492083127

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 Joel David Valente Guerreiro

Teaching staff	Type	Classes	Hours (*)
Joel David Valente Guerreiro	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

Not Applicable

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

Vulnerability detection analysis and exploration Curricular Unit aims to provide to the student knowledge that allows the Vulnerabilities identification, analysis and exploration, using detection tools and implementing techniques to obtain knowledge and limit the vulnerabilities that can be explored.

It is also a goal the skills development in planning, designing and analysing vulnerabilities, apply and implement techniques, response protocols and models to detect and prevent computer attacks. It is also an objective for the student acquire knowledge in an organization vulnerabilities analysis.

Syllabus

- Active security and vulnerability concepts;
- Physical, software, development and services vulnerabilities;
- Tools and methodologies to detect vulnerabilities;
- Vulnerabilities analysis and exploration;
- Evaluation techniques and tools to limit vulnerabilities;
- Detect and defence model?s implementation.

Teaching methodologies (including evaluation)

This curricular unit combines several teaching methods:

- Theoretical classes syllabus exposition
- Vulnerability detection, analysis and limitation Laboratorial practical classes as autonomous work
- Oral presentations of group works
- Individual or group doubt clarification
- Activity support and curricular unit functioning clarification

The evaluation is continuous, with a final exam and includes:

- Individual knowledge evaluation test (50%)
- Group Work with oral discussion presentation (50%)

The students that acquire 9.5 values in 20 final classification in each evaluation element are exempt from final exam.

Main Bibliography

- Morey J. Haber and Brad Hibbert (2018), *Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations* , Apress ISBN-10: 1484236262
- Christopher J. Hodson (2019), *Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls* , Kogan Page, ISBN-10: 0749484128
- Andrew Magnusson (2020), *Practical Vulnerability Management: A strategic Approach to Managing Cyber Risk* , No Starch Press, ISBN-10: 1593279884
- Cyber Security Resource (2021), *Vulnerability Management Program Guide: Managing the Threat and Vulnerability Landscape* , independently published, ISBN-13: 979-8713500658
- Yuri Diogenes and Erdal Ozkaya (2018), *Cybersecurity ? Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics* , Packt Publishing, ISBN-10: 9781788475297
- Heather Adkins et al (2020), *Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems 1 st* , O?Reilly, ISBN-10: 1492083127