English version at the end of this document

| | |
|---|---|
| **Ano Letivo** | 2022-23 |
| **Unidade Curricular** | AVALIAÇÃO DE CIBERSEGURANÇA, TESTES DE PENETRAÇÃO E AUDITORIA |
| **Cursos** | CIBERSEGURANÇA |
| **Unidade Orgânica** | Faculdade de Ciências e Tecnologia |
| **Código da Unidade Curricular** | 19381005 |
| **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** Luís Manuel Pisco Rodrigues

| DOCENTE | TIPO DE AULA | TURMAS | TOTAL HORAS DE CONTACTO (*) |
|---|---|---|---|
| Luís Manuel Pisco Rodrigues | T; TP | T1; TP1 | 28T; 28TP |

* 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; 28TP | 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 Avaliação de Cibersegurança, Testes de Penetração e Auditoria pretende dotar o estudante com conhecimentos que lhe permita avaliar a segurança de sistemas e redes informáticas numa organização, através da simulação de ataques de fontes maliciosas. É ainda objetivo desenvolver o conhecimento do estudante de ?ethical hacking?, como proceder, detetando potenciais constrangimentos tais como, má configuração de sistemas, falhas de hardware e software, de redes e aplicar técnicas de contramedidas. Pretende ainda dotar o estudante de conhecimento das ferramentas e técnicas utilizadas para os testes de penetração e consequentes contra-medidas.

**Conteúdos programáticos**

- A segurança informática e da informação numa organização;
- Conceito de Ethical-Hacking e Testes de Penetração;
- Reconhecimento e recolha de informação;
- Scanning, Sniffing e Evasão;
- Analisar o contexto e determinar quais as tipologias de testes a executar;
- Ferramentas e técnicas a aplicar para detetar os constrangimentos;
- Avaliar a cibersegurança da organização;
- Relatório de auditoria e sugestões de contra-medidas.

**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 testes de penetração utilizando diversas ferramentas para o efeito;
- 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**

Gus Khawaja (2021), Kali Linux Penetration Testing Bible, Wiley, ISBN-10: 1119719089

Radhi Shatob (2020), Penetration Testing: Step by Step Guide, ISBN Canada, ISBN-10: 1999541243

Peter Kim (2018), The Hacker Playbook 3: Practical Guide to Penetration Testing, Independently Published, ISBN-10: 1980901759

Vijay Kumar Velu and Robert Beggs (2019), Mastering Kali Linux for Advanced Penetration Testing: Secure your network with Kali Linux 3rd Edition, Packt Publishing, ISBN-10: 178934056X

Ric Messier (2018), Learning Kali Linux: Security Testing, Penetration Testing, and Ethical Hacking, O?Reilly, ISBN-10: 9781492028697

| | |
|---|---|
| **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** Luís Manuel Pisco Rodrigues

| Teaching staff | Type | Classes | Hours (*) |
|---|---|---|---|
| Luís Manuel Pisco Rodrigues | T; TP | T1; TP1 | 28T; 28TP |

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

**Contact hours**

| T | TP | PL | TC | S | E | OT | O | Total |
|---|---|---|---|---|---|---|---|---|
| 28 | 28 | 0 | 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)**

The Curricular Unit of Cybersecurity Assessment, Penetration Testing and Auditing aims to provide students with knowledge that allows them to assess the security of computer systems and networks in an organization, through the simulation of attacks from malicious sources. It is also aimed to develop the student's knowledge of "ethical hacking", how to proceed, detecting potential constraints such as poor system configuration, hardware and software failures, networks and applying countermeasure techniques. It also intends to provide the student with knowledge of the tools and techniques used for penetration tests and consequent countermeasures.

**Syllabus**

- Computer and information security in an organization;
- Concept of Ethical-Hacking and Penetration Tests;
- Recognition and collection of information;
- Scanning, Sniffing and Evasion;
- Analyse the context and determine which types of tests to run;
- Tools and techniques to be applied to detect constraints;
- Assess the organization's cybersecurity;
- Audit report and countermeasure suggestions.

**Teaching methodologies (including evaluation)**

This course unit combines several teaching methods:

- Exposition of the syllabus, through the theoretical component
- Laboratory practice of computer networks with simulators and network equipment.
- Oral presentations of group work.
- Individual or group service to clarify doubts.
- Support for activities and clarification on the functioning of the curricular unit

Evaluation is continuous, with a final exam and includes:

- Individual test to assess knowledge (50%).
- Group work with oral presentation/discussion (50%).

Students who obtain a final grade equal to or greater than 9.5 in each evaluation element are exempt from the final exam.

**Main Bibliography**

Gus Khawaja (2021), Kali Linux Penetration Testing Bible, Wiley, ISBN-10: 1119719089

Radhi Shatob (2020), Penetration Testing: Step by Step Guide, ISBN Canada, ISBN-10: 1999541243

Peter Kim (2018), The Hacker Playbook 3: Practical Guide to Penetration Testing, Independently Published, ISBN-10: 1980901759

Vijay Kumar Velu and Robert Beggs (2019), Mastering Kali Linux for Advanced Penetration Testing: Secure your network with Kali Linux 3rd Edition, Packt Publishing, ISBN-10: 178934056X

Ric Messier (2018), Learning Kali Linux: Security Testing, Penetration Testing, and Ethical Hacking, O?Reilly, ISBN-10: 9781492028697