English version at the end of this document

Ano Letivo	2022-23
Unidade Curricular	CIBERSEGURANÇA NA ADMINISTRAÇÃO DE SISTEMAS
Cursos	CIBERSEGURANÇA
Unidade Orgânica	Faculdade de Ciências e Tecnologia
Código da Unidade Curricular	19381007
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 Adriano Pires

DOCENTE	TIPO DE AULA	TURMAS	TOTAL HORAS DE CONTACTO (*)
Adriano Pires	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

Não aplicável

Objetivos de aprendizagem (conhecimentos, aptidões e competências)

A Unidade Curricular de Cibersegurança na Administração de Sistemas pretende dotar o estudante com conhecimentos que lhe permita administrar e implementar as melhores práticas de segurança em sistemas operativos, como o Linux e o Windows Server. Visa também desenvolver a capacidade do estudante na utilização segura de serviços de diretório e políticas de grupo. Pretende ainda dotar o estudante de conhecimento das vulnerabilidades de roles como DNS, DHCP, e protocolos de comunicação e como ultrapassar esses constrangimentos nos referidos sistemas operativos. Pretende-se ainda dotar o estudante de conhecimentos para a implementação de estratégias de defesa nos mais modernos sistemas operativos e de sistemas informáticos.

Conteúdos programáticos

- O Sistema Operativo Linux, funcionalidades, serviços e configurações;
- O Sistema Operativo Windows Server, funcionalidades, serviços e configurações;
- Normas de configuração de Sistemas Operativos;
- Análise de vulnerabilidades especificas de cada sistema operativo;
- Técnicas de resolução das vulnerabilidades e limitação de constrangimentos dos Sistemas Operativos;
- Implementar estratégias de defesa nos Sistemas Operativos;
- Estratégias de defesa de Sistemas Informáticos e de Sistemas de Gestão de Bases de Dados.

Metodologias de ensino (avaliação incluída)

A presente unidade curricular combina diversos métodos de ensino:

- Exposição dos conteúdos programáticos, através das aulas teóricas
- Práticas laboratoriais com a utilização dos sistemas operativos Linux e Windows Server e técnicas de segurança a aplicar nos diversos serviços;
- 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

- Trent Jaeger (2008), Operating System Security, Morgan and Claypool Publishers, ISBN-10: 1598292129
- Michael Jang and Ric Messier (2015), Security strategies in Linux Platforms and Applications, Jones & Bartlett Learning, ISBN-10: 1284090655
- Ric Messier (2015), Operating System Forensics, Syngress, ISBN-10: 0128019492
- Donald A. Tevault (2020), Mastering Linux Security and Hardening: Protect your Linux Systems from Intruders, malware attacks and other Cyber threats, 2nd Edition, Packt Publishing, ISBN-10: 1838981772
- Jeremy Moskowitz (2015), Group Policy: Fundamentals, Security and the Managed Desktop, Sybex 3rd Edition, ISBN-10: 1119035589
- Yuri Diogenes and Tom Janetscheck (2021), Microsoft Azure Security Center (IT Best Practices), Microsoft Press, ISBN: 01373443426

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 Adriano Pires

Teaching staff	Type	Classes	Hours (*)
Adriano Pires	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 aplicable

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

The curricular unit (CU) of Cybersecurity in Systems Administration intends to provide the student with knowledge that allows him to apply the best security practices for operating systems, such as Linux or Windows Server. Also, as a goal of this CUis that students be able to develop the capacity to safely use of directory services and group policies.

Providing students with knowledge of the vulnerabilities of roles such as DNS, DHCP, and communication protocols and how to overcome these constraints on operating systems is also another goal of this CU. It is also intended to provide the student with knowledge for the implementation of defense strategies, in the most modern operating systems and computer systems.

Syllabus

- The Linux operating system, features, services, and configurations.
- The Windows Server operating system, features, services, and configurations.
- Operating Systems configuration standards.
- Analysis of specific vulnerabilities of each operating system.
- Techniques for solving vulnerabilities and limiting operating systems constraints.
- Implement defense strategies in operating systems.
- Strategies to secure computer systems and database management systems.

Teaching methodologies (including evaluation)

This curricular unit combines various teaching methods:

- Program content exhibition through theoretical lectures.
- Practice laboratorial lessons of identity management systems simulations, as autonomous work.
- Oral group presentations on developed work project.
- Individual or group attendance for out of classroom support.
- Activity support and curricular unit functioning clarification.

The 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

- Trent Jaeger (2008), Operating System Security, Morgan and Claypool Publishers, ISBN-10: 1598292129
- Michael Jang and Ric Messier (2015), Security strategies in Linux Platforms and Applications, Jones & Bartlett Learning, ISBN-10: 1284090655
- Ric Messier (2015), O777777perating System Forensics, Syngress, ISBN-10: 0128019492
- Donald A. Tevault (2020), Mastering Linux Security and Hardening: Protect your Linux Systems from Intruders, malware attacks and other Cyber threats, 2nd Edition, Packt Publishing, ISBN-10: 1838981772
- Jeremy Moskowitz (2015), Group Policy: Fundamentals, Security and the Managed Desktop, Sybex 3rd Edition, ISBN-10: 1119035589
- Yuri Diogenes and Tom Janetscheck (2021), Microsoft Azure Security Center (IT Best Practices), Microsoft Press, ISBN: 01373443426