Ficha de Unidade Curricular A3ES
Segurança em Redes de Computadores
Mestrado em Engenharia Informática e de Computadores
2024-25

1. Caracterização da Unidade Curricular

1.1 Designação
[2520] Segurança em Redes de Computadores / Computer Networks Security

1.2 Sigla da área científica em que se insere
IC

1.3 Duração
Unidade Curricular Semestral

1.4 Horas de trabalho
162h 00m

1.5 Horas de contacto
Total: 67h 30m das quais TP: 67h 30m

1.6 ECTS
6

1.7 Observações
Unidade Curricular Opcional

2. Docente responsável [726] Vitor Jesus Sousa de Almeida

3. Docentes e respetivas cargas letivas na unidade curricular Não existem docentes definidos para esta unidade curricular

4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes)

Os estudantes ao terminarem com sucesso esta unidade curricular serão capazes de:

1. Perceber claramente os conceitos de confidencialidade, integridade e autenticação e os protocolos usados para os garantir.
2. Identificar, quer do ponto de vista dos atacantes, quer dos defensores, os pontos críticos em termos de segurança.
3. Definir soluções possíveis para o incremento da segurança através da análise das vulnerabilidades, ameaças e tipos de ataques a sistemas de comunicação.
4. Usar e configurar os equipamentos de rede com os diferentes protocolos usados para incrementar a segurança.
5. Efetuar a escolha consciente da política de segurança mais adequada a cada situação.

4. Intended learning outcomes (knowledge, skills and competences to be developed by the students)

Students to successfully finish this course you will:

1. Clearly perceive the concepts of confidentiality, integrity and authentication and protocols used to ensure them.

2. Identify, either from the standpoint of the attackers or defenders, the critical points in terms of security.

3. Define possible solutions to increase the security by analyzing the vulnerabilities, threats and attacks of communication systems.

4. Use and configure network equipment with different protocols used to increase safety.

5. Make the conscious choice of the security policy most appropriate for each situation.

5. Conteúdos programáticos

Factos sobre segurança.

Ameaças, vulnerabilidades e ataques.

Noções de confidencialidade, integridade e autenticação.

Criptografia (algoritmos de *hash* , MAC e HMAC, números aleatórios, distribuição de chaves, Conceitos de teoria dos números/matemática modular, cifras simétricas (substituição e transposição, algoritmos de César ao AES) e assimétricas (RSA), certificados digitais x.509 e autoridades de certificação, assinaturas digitais (DSA e Schnorr)).

Segurança em:

· Camadas OSI de baixo nível (MACSec - 802.1ae, controlo de acessos - 802.1x, RADIUS, VPN: PPP, EAP, GRE, PPTP, L2TP).

· Redes sem fios (WLAN: WEP ao WPA3).

· Comunicações ao nível das camadas OSI de rede e transporte e *web* (IPsec, IKEv2, SSH, SSL/TLS, HTTPS).

· Serviços de *email* (SMTP, POP, IMAP, MIME, Sender Policy Framework (SPF), Domain keys).

· Blockchain *,* IOTA *, smart contracts e Dapps.*

· IoT.

· Redes: *routers* , *firewalls* , IDS e armadilhas, gestão.

Políticas de segurança.

5. Syllabus

Facts about safety .
Threats , vulnerabilities and attacks .
Cryptography (hash algorithms, key distribution, symmetric (substitution and transposition, algorithms from Cesar to AES) and asymmetric ciphers (introduction to number theory/modular mathematics, elliptical curves, RSA) , digital certificates x.509 and certification authorities , digital signatures (DSA , Schnorr)).
Security in low level OSI layers (MACSec - 802.1ae, *access control - 802.1x , RADIUS , support for VPN ? PPP, EAP, GRE, PPTP , L2TP).*
Security in wireless networks (WLAN ? from WEP to WPA 3).

Communications security at the network layer of the OSI model (IPsec, IKEv2).
Security in Web (SSH, SSL/TLS , HTTPS).

Security services in email (security in SMTP, POP, IMAP, MIME; Sender Policy Framework (SPF), Domain keys).

Security concepts applied in *Blockchain, IOTA, smart contracts and Dapps .*

Security concepts applied in IoT.

Security practices : routers , firewalls, IDS and traps .

Security in network management.
Security policies.

6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular

A segurança em redes é cada vez mais uma área do conhecimento incontornável para aqueles que se pretendem dedicar às redes de computadores. Nesta unidade curricular os estudantes ficam a conhecer os principais conceitos referentes à segurança aplicada às redes, assim como os protocolos usados ao nível das diversas camadas do modelo de referência OSI, desde os de suporte ao controlo de acessos, passando pelas VPN, pela segurança nas redes sem fios e em diversas aplicações mais comuns como *browsers* e *email* . Aprendem a usar os equipamentos de rede (*switches* e *routers*) como auxiliares dos *firewalls* para minimizarem eventuais ataques já descritos anteriormente. Aprendem o que é política de segurança e a sua importância para a segurança das empresas, isto respeitando a legislação em vigor.

6. Evidence of the syllabus coherence with the curricular unit´s intended learning outcomes

Network security is increasingly an area of knowledge essential for those who intend to devote themselves to computer networks . In this course students get to know the main concepts related to security applied to networks , as well as the protocols used across the various layers of the OSI reference model , since the support for access control , through the VPN, to the security at wireless networks and in many applications such as browsers and email . They learn to use the network equipment (switches and routers) as auxiliaries of firewalls to minimize any attack, previously described . Learn what is the security policy and its importance to the safety of enterprises , that respecting the law.

7. Metodologias de ensino (avaliação incluída)

As aulas teóricas destinadas a expor e discutir os conteúdos programáticos, incentivando a interatividade e colocação de questões. As aulas práticas destinadas à prática do explanado nas teóricas.

Avaliação distribuída com exame final:

Nota: NM="Nota mínima".

- 2 testes teóricos (NM 8) durante o semestre (CT1, média aritmética simples (NM 9,5)) ou exame teórico (CT2) (NM 9,5); CT (NM 9,5)=max(CT1;CT2);
- Até 4 fichas teóricas de realização extra-aula, pesos iguais; CR=média aritmética simples das fichas teóricas/20;
- 3 trabalhos com relatórios (CP1)(NM 8) realizados em grupo, aulas práticas e extra-aula. Pesos CP1: 20, 30 e 50%. Discussão final oral dos relatórios dos trabalhos (CP2) (NM 8). CP (NM 9,5)=40%xCP1+60%xCP2.

Classificação final=min(20; 0,5xCT+0,5xCP+CR).

CP e CT são pedagogicamente fundamentais.

Discussão final oral: Necessária a entrega dos relatórios dos trabalhos práticos (CP1).

7. Teaching methodologies (including assessment)

Theoretical classes aim to present and discuss the syllabus, encouraging interactivity and asking questions. Practical classes aimed at practicing what was explained in the theoretical ones.

Distributed assessment with final exam:

Note: NM="Minimum grade".

- 2 theoretical tests (NM 8) during the semester (CT1, simple arithmetic average (NM 9.5)) or theoretical exam (CT2) (NM 9.5); CT (NM 9.5)=max(CT1;CT2);
- Up to 4 extra-class theoretical sheets, equal weights; CR=simple arithmetic mean of theoretical sheets/20;
- 3 works with reports (CP1)(NM 8) carried out in groups, practical classes and extra-class. CP1 weights: 20, 30 and 50%. Final oral discussion of work reports (CP2) (NM 8). CP (NM 9.5)=40%xCP1+60%xCP2.

Final classification=min(20; 0.5xCT+0.5xCP+CR).

CT and CP are pedagogically fundamental.

Final oral discussion: Submission of practical work reports (CP1) is required.

8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular

Os objetivos da unidade curricular são obtidos através de aulas teóricas e respetivos elementos de apoio (slides) e bibliografia, da realização de exercícios práticos e de casos de estudo selecionados pelo docente. A maioria dos trabalhos é realizada recorrendo a laboratórios virtuais (máquinas virtuais, contentores, ?). O objetivo do ponto de vista prático é alcançado através de trabalhos práticos, em que os alunos estudam o funcionamento de mecanismos de segurança com realce para as redes. A realização dos trabalhos práticos é acompanhada pelo docente para assegurar o correto desenvolvimento dos conhecimentos e das competências dos estudantes.

8. Evidence of the teaching methodologies coherence with the curricular unit´s intended learning outcomes

The objectives of the curricular unit are achieved through theoretical classes and respective supporting elements (slides) and bibliography, through practical exercises and case studies selected by the teacher. Most work is carried out using virtual laboratories (virtual machines, containers, ?). The objective from a practical point of view is achieved through practical work, in which students study the functioning of security mechanisms with an emphasis on networks. The completion of the practical works is monitored by the teacher to ensure the correct development of the students' knowledge and skills.

9. Bibliografia de consulta/existência obrigatória

- Folhas/ *Slides* da disciplina

- ?Cryptography and Network Security - Principles and Practice, 8th edition?, William Stallings, Prentice-Hall, 2020

- ?Internet Security: A Hands-on Approach, Second Edition?, Wenliang DU, CreateSpace, 2019

Outra bibliografia/other bibliography

- ?Segurança em Redes Informáticas, 6ª edição?, André Zúquete, FCA, 2021

10. Data de aprovação em CTC «INFORMAÇÃO NÃO DISPONIVEL»

11. Data de aprovação em CP «INFORMAÇÃO NÃO DISPONIVEL»