



UNIVERSIDADE LUSÍADA
LISBOA

Programa da Unidade Curricular
REDES DE COMUNICAÇÃO

Ano Lectivo 2023/2024

1. Unidade Orgânica

Faculdade de Ciências da Economia e da Empresa

2. Curso

ENGENHARIA INFORMÁTICA

3. Ciclo

1º

4. Unidade Curricular

REDES DE COMUNICAÇÃO (L9015)

5. Área Científica

6. Ano Curricular

2º

7. Tipo de Unidade Curricular / Semestre

1º Semestre



UNIVERSIDADE LUSÍADA
LISBOA

8. Tipo de aula e carga horária (tempo de trabalho)

Aulas Teóricas:	
Aulas Práticas:	
Aulas Teórico-Práticas:	30,00
Orientação Tutorial:	20,00

9. Créditos ECTS

6,00

10. Coordenador da Área Científica

11. Regente

Prof. Doutor PEDRO RAMOS DOS SANTOS BRANDÃO

12. Assistentes

13. Língua de Ensino

Português

14. Objetivos Gerais

- O1 - Conhecer os conceitos fundamentais de Cybersecurity;
- O2 - Compreender o que são vulnerabilidades de um sistema;
- O3 - Entender como os ataques de segurança podem ser perpetrados;
- O4 - Compreender como podem ser defendidos os sistemas de ataques;
- O5 - Conhecer métodos de mitigar e recuperar de um ataque.

15. Objetivos Específicos

- O1 - Compreender os fundamentos da segurança nas redes informáticas;
- O2 - Compreender os princípios básicos das principais ameaças e vulnerabilidade da segurança nas redes informáticas;
- O3 - Compreender os princípios básicos das principais medidas de segurança a adotar para minimizar a probabilidade de sucesso das principais ameaças à segurança nas redes informáticas;
- O4 - Compreender os princípios básicos dos principais protocolos de segurança e serviço VPN de suporte à comunicação segura em

16. Competências a adquirir



UNIVERSIDADE LUSÍADA
LISBOA

Saber detetar anomalias de segurança.
Saber implementar um plano de segurança.
Saber mitigar um ciberataque.
Saber identificar comportamentos duvidosos numa rede.
Saber criptografar um ficheiro.
Saber atuar no campo do Ethical Hacking.

17. Metodologia de Ensino

Aulas teórico práticas.
O desenvolvimento será através de exposição, exercícios, discussão e participação do aluno.
As metodologias de avaliação formativa, traduzidas na análise de questões e na resolução de exercícios práticos, garantem que os objetivos definidos, em termos de compreensão teórica e de capacidades práticas, serão alcançados pelos alunos que participem nessas atividades.

18. Conteúdos Programáticos



UNIVERSIDADE LUSÍADA
LISBOA

1. Introdução e conceitos básicos de segurança
 - 1.1 Objectivos da Segurança Informática
 - 1.2 Visão Geral de Medidas de Segurança
 - 1.3 Visão Geral de Ameaças à Segurança
2. Ameaças e vulnerabilidades
 - 2.1 Tipos de malware
 - 2.2.1 Worms
 - 2.2.2 Virus
 - 2.2.3 Rootkits
 - 2.2.4 Troianos
 - 2.2.5 Ransomware
 - 2.2.6 Spyware
 - 2.2.7 APTs (Advanced Persistent Threats)
 - 2.2.8 Tools de análise de malware
 - 2.2 Vulnerabilidades comuns no software
 - 2.2.1 Falhas de segmentação
 - 2.2.2 Race conditions
 - 2.2.3 Validação de inputs
 - 2.3 Vulnerabilidades comuns nas redes de comunicação
 - 2.3.1 Password sniffing
 - 2.3.2 Session hijacking
 - 2.3.3 ARP Spoofing
 - 2.3.4 Denial of Service (DoS)
 - 2.4 Vulnerabilidades comuns na web
 - 2.4.1 Cross site scripting
 - 2.4.2 SQL injection
 - 2.4.3 Divulgação involuntária de dados
 - 2.4.4 Adware
 - 2.5 Metodologias de ataques a redes
 - 2.5.1 IP Spoofing
 - 2.5.2 Ataques DDoS (Distributed DoS)
 - 2.5.3 Ataques DNS
 - 2.5.4 E-mails de phishing
 - 2.5.5 Descoberta de passwords fracas
 - 2.5.6 Roubo de dados privados
 - 2.5.7 Remoção de provas de ataque
 - 2.5.8 Mapas de Ciberataques
3. Medidas de segurança informática
 - 3.1 Políticas de Segurança nas Organizações
 - 3.1.1 Especificação
 - 3.1.2 Implementação



UNIVERSIDADE LUSÍADA
LISBOA

3.2 Firewalls

3.2.1 Introdução as Firewalls

3.2.2 Componentes das Firewalls

3.2.3 Topologias de Firewalls com DMZ

3.2.4 DMZ (zona desmilitarizada)

3.2.5 Funcionalidades das Firewalls

3.2.5.1 Filtros de pacotes (packet filter)

3.2.5.2 Filtros aplicacionais (application gateway)

3.2.5.3 Next Generation Firewalls (NGFW)

3.2.5.4 Network Address Translation (NAT)

3.2.5.5 Cenários de Firewalls em simulador Packet Tracer

3.3 Sistemas de Detecção de Intrusões (IDS)

3.3.1 Perfil de uma intrusão

3.3.2 Arquitetura dos IDS

3.3.3 Métricas de qualidade dos IDS

3.3.4 Honey pots

3.3.5 Classificação dos IDS

3.3.6 Caso de estudo- Tripwire

3.3.7 Caso de estudo PFSENSE

3.3.8 Cenários de IDSs em simulador Packet Tracer

3.4 Sistemas de Informações de Segurança e Gestão de Eventos (SIEM)

3.4.1 Arquitetura SIEM

3.4.2 SIEM vs IDS

3.5 Mecanismos de testes de defesa de redes

3.5.1 Testes de penetração nas redes

3.5.2 Aplicação Metasploit

3.5.3 Repositório de Vulnerabilidades

4. Protocolos de comunicação segura e Serviço VPN

4.1 Soluções de segurança nas comunicações na internet

4.2 SSL/TLS

4.2.1 Introdução ao SSL/TLS

4.2.2 Sub-Protocolos SSL/TLS

4.2.3 Protocolos de serviços com SSL/TLS

4.2.4 Análise de SSL/TLS em Wireshark

4.3 Protocolo IPSec

4.3.1 Funcionalidades do IPSec

4.3.2 Associações de segurança (SA)

4.3.3 Cabeçalho de autenticação (AH)

4.3.4 Cabeçalho de segurança de dados/conteúdo encapsulado (ESP)

4.3.5 Modos de operação: transporte e túnel

4.4 Redes Privadas Virtuais (VPN)

4.4.1 Introdução



UNIVERSIDADE LUSÍADA
LISBOA

- 4.4.2 Topologias de VPNs em redes corporativas
- 4.4.3 VPNs: IPsec/SSL-TLS
- 4.4.4 Cenários de VPNs em simulador Packet Tracer

5. Segurança em redes sem fios

- 5.1 Introdução às redes sem fios
- 5.2 Introdução às redes Wi-Fi
 - 5.2.1 Protocolo WEP (Wired Equivalent Privacy)
 - 5.2.2 Protocolo WPA (Wi-Fi Protected Access)
 - 5.2.3 Protocolo WPA2
 - 5.2.4 Protocolo WPA3
- 5.3 Introdução às redes celulares
 - 5.3.1 Introdução às Redes GSM (2G)
 - 5.3.2 Segurança em redes GSM (2G)
 - 5.3.3 Introdução às Redes UMTS (3G)
 - 5.3.4 Segurança em redes UMTS com USIM (3G)
 - 5.3.5 Introdução às Redes LTE (4G)
 - 5.3.6 Segurança em redes LTE (4G)
 - 5.3.7 Introdução às Redes 5G
 - 5.3.8 Segurança em redes 5G
 - 5.3.9 Principais vulnerabilidades das redes celulares

6. Caso de estudo: Padrão de segurança de dados da indústria, cartões de pagamento (PCI DSS),

- 6.1 Introdução ao PCI-DSS
- 6.2 Dados de cartões de pagamentos
- 6.3 Acesso ilícito a cartões de pagamentos
- 6.4 Requisitos de segurança PCI-DSS
- 6.5 Boas práticas de utilizadores de cartões de pagamentos

7. Casos práticos: laboratórios de cibersegurança.

19. Métodos de Avaliação

- Testes
- Trabalhos práticos

20. Recursos Didáticos

- PowerPoints
- Computadores
- Máquinas Virtuais

21. Objetivos de Sustentabilidade



UNIVERSIDADE LUSÍADA
LISBOA

22. Palavras Chave

Cibersegurança
Segurança Informática
Segurança de Redes

23. Bibliografia Principal

Autor(es):	Willian Stallings		
Título:	Computer Security		
Edição:	Global Edition	Ano:	2018
Local:	New York		
Editora:	Pearson		

Autor(es):	William Stallings		
Título:	Effective Cybersecurity		
Edição:	1	Ano:	2019
Local:	New York		
Editora:	Pearson		

Autor(es):	Wenliang Du		
Título:	Computer and Internet Security		
Edição:	Second	Ano:	2017
Local:	Syeacuse		
Editora:	Independently Published		

24. Bibliografia Complementar

Autor(es):	Pascal Ackerman		
Título:	Modern Cybersecurity Pratices		
Edição:	First	Ano:	2020
Local:	Mumbai		
Editora:	BPM Publications		

Autor(es):	Vijay Kumar Velu		
Título:	Mastering Kali Linux for Advanced Penetration Testing		
Edição:	Second	Ano:	2017
Local:	Birmimgham		
Editora:	Packt		



UNIVERSIDADE LUSÍADA
LISBOA

Ficha técnica MIP / MIP Datasheet	
Título / Title	Programa da unidade curricular 'REDES DE COMUNICAÇÃO': Ano Lectivo 2023/2024
Autor / Author	Prof. Doutor PEDRO RAMOS DOS SANTOS BRANDÃO
Classificação / Classification	-
Descritores / Descriptors	-
Colaborador(es) / Colaborator(s)	-
Data Hora / Date Time	24-07-2023 09:49:00
Formato de dados / Data Format	Texto / Text, PDF
Estatuto de utilização / Usage	Acesso público / Public Access
Relação / Relation	Versão 1,0
(c) Universidade Lusíada, 2024	