



UNIVERSIDADE LUSÍADA
LISBOA

Course Unit Program
Communication Networks

Academic Year 2023/2024

1. Organic Unit

Faculty of Business and Economic Sciences

2. Course

Computer Engineering

3. Cycle

1st

4. Course Unit

Communication Networks (L9015)

5. Scientific Area

6. Curricular Year

2nd

7. Type of Curricular Unit / Semester

1st Semester



UNIVERSIDADE LUSÍADA
LISBOA

8. Class type and workload (work time)

Theoretical classes:

Practical classes:

Theoretical-Practical Classes 30,00

Tutorial Guidance: 20,00

9. ECTS Credits

6,00

10. Scientific Area Coordinator

11. Regent

Prof. Doutor PEDRO RAMOS DOS SANTOS BRANDÃO

12. Assistants

13. Teaching Language

Portuguese

14. General Objectives

- O1 - Know the fundamental concepts of Cybersecurity;
- O2 - Understand what system vulnerabilities are;
- O3 - Understand how security attacks can be perpetrated;
- O4 - Understand how attack systems can be defended;
- O5 - Know methods to mitigate and recover from an attack.

15. Specific Objectives

- O1 - Understand the fundamentals of security in computer networks;
- O2 - Understand the basic principles of the main threats and security vulnerabilities in computer networks;
- O3 - Understand the basic principles of the main security measures to be adopted to minimize the probability of success of the main threats to security in computer networks;
- O4 - Understand the basic principles of the main security protocols and VPN service to support secure communication in networks

16. Skills to be acquired



UNIVERSIDADE LUSÍADA
LISBOA

Know how to detect security anomalies.
Know how to implement a security plan.
Know how to mitigate a cyberattack.
Knowing how to identify dubious behavior in a network.
Know how to encrypt a file.
Knowing how to work in the field of Ethical Hacking.

17. Teaching Methodology

Practical theoretical classes.

The development will be through exposure, exercises, discussion and student participation.

The formative assessment methodologies, translated into the analysis of questions and the resolution of practical exercises, guarantee that the defined objectives, in terms of theoretical understanding and practical abilities, will be achieved by the students who participate in these activities.

18. Course Unit Program



UNIVERSIDADE LUSÍADA
LISBOA

1. Introduction and basic security concepts
 - 1.1 Objectives of Computer Security
 - 1.2 Overview of Security Measures
 - 1.3 Overview of Security Threats
2. Threats and vulnerabilities
 - 2.1 Types of malware
 - 2.2.1 Worms
 - 2.2.2 Viruses
 - 2.2.3 Rootkits
 - 2.2.4 Trojans
 - 2.2.5 Ransomware
 - 2.2.6 Spyware
 - 2.2.7 APTs (Advanced Persistent Threats)
 - 2.2.8 Malware Analysis Tools
 - 2.2 Common vulnerabilities in software
 - 2.2.1 Segmentation faults
 - 2.2.2 Race conditions
 - 2.2.3 Validation of inputs
 - 2.3 Common vulnerabilities in communication networks
 - 2.3.1 Password sniffing
 - 2.3.2 Session hijacking
 - 2.3.3 ARP Spoofing
 - 2.3.4 Denial of Service (DoS)
 - 2.4 Common vulnerabilities on the web
 - 2.4.1 Cross site scripting
 - 2.4.2 SQL injection
 - 2.4.3 Involuntary disclosure of data
 - 2.4.4 Adware
 - 2.5 Network attack methodologies
 - 2.5.1 IP Spoofing
 - 2.5.2 DDoS (Distributed DoS) attacks
 - 2.5.3 DNS Attacks
 - 2.5.4 Phishing emails
 - 2.5.5 Discovery of weak passwords
 - 2.5.6 Theft of private data
 - 2.5.7 Removal of evidence of attack
 - 2.5.8 Cyberattack Maps
3. Computer security measures
 - 3.1 Security Policies in Organizations
 - 3.1.1 Specification
 - 3.1.2 Implementation



UNIVERSIDADE LUSÍADA
LISBOA

3.2 Firewalls

3.2.1 Introduction to Firewalls

3.2.2 Firewall Components

3.2.3 Topologies of Firewalls with DMZ

3.2.4 DMZ (demilitarized zone)

3.2.5 Functionalities of Firewalls

3.2.5.1 Packet filters (packet filter)

3.2.5.2 Application filters (application gateway)

3.2.5.3 Next Generation Firewalls (NGFW)

3.2.5.4 Network Address Translation (NAT)

3.2.5.5 Firewall Scenarios in Packet Tracer simulator

3.3 Intrusion Detection Systems (IDS)

3.3.1 Profile of an intrusion

3.3.2 IDS Architecture

3.3.3 IDS quality metrics

3.3.4 Honey pots

3.3.5 Classification of IDS

3.3.6 Case study - Tripwire

3.3.7 PFSENSE case study

3.3.8 IDS scenarios in Packet Tracer simulator

3.4 Security Information and Event Management Systems (SIEM)

3.4.1 SIEM architecture

3.4.2 SIEM vs IDS

3.5 Network defense testing mechanisms

3.5.1 Network penetration tests

3.5.2 Metasploit Application

3.5.3 Vulnerability Repository

4. Secure Communication Protocols and VPN Service

4.1 Internet communications security solutions

4.2 SSL/TLS

4.2.1 Introduction to SSL/TLS

4.2.2 SSL/TLS Sub-Protocols

4.2.3 Service protocols with SSL/TLS

4.2.4 SSL/TLS analysis in Wireshark

4.3 IPsec Protocol

4.3.1 IPsec Features

4.3.2 Security Associations (SA)

4.3.3 Authentication Header (AH)

4.3.4 Encapsulated Data/Content Security Header (ESP)

4.3.5 Modes of operation: transport and tunnel

4.4 Virtual Private Networks (VPN)

4.4.1 Introduction



UNIVERSIDADE LUSÍADA
LISBOA

- 4.4.2 VPN topologies in corporate networks
- 4.4.3 VPNs: IPsec/SSL-TLS
- 4.4.4 Scenarios of VPNs in Packet Tracer simulator

5. Security in wireless networks

- 5.1 Introduction to wireless networks
- 5.2 Introduction to Wi-Fi networks
 - 5.2.1 WEP Protocol (Wired Equivalent Privacy)
 - 5.2.2 WPA Protocol (Wi-Fi Protected Access)
 - 5.2.3 WPA2 protocol
 - 5.2.4 WPA3 protocol
- 5.3 Introduction to cellular networks
 - 5.3.1 Introduction to GSM Networks (2G)
 - 5.3.2 Security in GSM (2G) networks
 - 5.3.3 Introduction to UMTS Networks (3G)
 - 5.3.4 Security in UMTS networks with USIM (3G)
 - 5.3.5 Introduction to LTE (4G) Networks
 - 5.3.6 Security in LTE (4G) networks
 - 5.3.7 Introduction to 5G Networks
 - 5.3.8 Security in 5G networks
 - 5.3.9 Main vulnerabilities of cellular networks

6. Case Study: Industry Data Security Standard, Payment Cards (PCI DSS),

- 6.1 Introduction to PCI-DSS
- 6.2 Payment card data
- 6.3 Illicit access to payment cards
- 6.4 PCI-DSS Security Requirements
- 6.5 Good practices for payment card users

7. Practical cases: cybersecurity laboratories.

19. Assessment Methods

- Tests
- practical works

20. Didactic Resources

- powerpoints
- computers
- Virtual Machines

21. Sustainability Objectives



UNIVERSIDADE LUSÍADA
LISBOA

22. Keywords

cybersecurity
IT Security
Network Security

23. Main Bibliography

Author(s): Willian Stallings
Title: Computer Security
Edition: Global Edition Year: 2018
Local: New York
Publisher: Pearson

Author(s): William Stallings
Title: Effective Cybersecurity
Edition: 1 Year: 2019
Local: New York
Publisher: Pearson

Author(s): Wenliang Du
Title: Computer and Internet Security
Edition: Second Year: 2017
Local: Syeacuse
Publisher: Independently Published

24. Complementary Bibliography

Author(s): Pascal Ackerman
Title: Modern Cybersecurity Pratices
Edition: First Year: 2020
Local: Mumbai
Publisher: BPM Publications

Author(s): Vijay Kumar Velu
Title: Mastering Kali Linux for Advanced Penetration Testing
Edition: Second Year: 2017
Local: Birmimgham
Publisher: Packt



UNIVERSIDADE LUSÍADA
LISBOA

Ficha técnica MIP / MIP Datasheet	
Título / Title	Course Unit Program 'REDES DE COMUNICAÇÃO': Academic Year 2023/2024
Autor / Author	Prof. Doutor PEDRO RAMOS DOS SANTOS BRANDÃO
Classificação / Classification	-
Descritores / Descriptors	-
Colaborador(es) / Colaborator(s)	-
Data Hora / Date Time	
Formato de dados / Data Format	Texto / Text, PDF
Estatuto de utilização / Usage	Acesso público / Public Access
Relação / Relation	Version 1,0
(c) Universidade Lusíada, 2024	