Course Contents and Rules

Técnicas de Perceção de Redes
Network Awareness

Mestrado em
Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro

deti.ua.pt

Professor

- Prof. Paulo Salvador
  - Email: salvador@ua.pt
  - Web: https://paulosalvador.net
  - Discord: https://discord.gg/bPPpKy5
    - Change your nickname to **your real name**
    - Aask for TPR role.
  - Office: IEETA

- Office hours
  - Flexible
    - Discord and e-mail to schedule.

TPR Objectives

- Integration of acquired knowledge on communication network and systems.
- Understand and develop architectures and methodologies for
  - Network and services monitoring,
  - Detection of attacks and functional anomalies, and
  - Deploy counter-measures and/or functional corrections.

Contents

- Characterization and identification of network usage profiles.
  - Acquisition, analysis and data mining of network information and statistics.
  - Characterization and classification of behaviors (activities/events).
  - Behavior anomaly detection methodologies.
- Prevention and detection of network intrusions.
  - Introduction to attack vectors.
  - Standard protection mechanisms/methodologies.
  - Detection of anomalies by known signatures.
  - Detection of behavior anomalies.
  - Counter-measures deployment.
- DDoS attacks mitigation.
  - Differentiation of licit and illicit accesses.
  - Blocking of illicit accesses at network and service levels.
  - Intelligent and automatic releasing of resources in firewalls and servers.

Evaluation

- Final Grade =
  - 40% * Theoretical Grade + 60% * Practice Grade
- Minimal grade: 7.0 in each component.
  - Theoretical Grade
    - Exam (40%) - Exam and/or Repeat Exam Seasons
      - Best grade is the one considered to calculate final grade.
  - Practice Grade
    - Project (60%) - in groups of 2 students (or 1 exceptionally).
      - First Presentation (20%) - November 9th
        - » Problem identification.
        - » Proposal of solution.
        - » Only presentation with slides, no report!
      - Final Presentation (40%) - last class.
        - » Presentation and demonstration of working solution.
      - During presentations/demo students must answer to specific questions. Grades may be different within a group.
    - Repeat Exam Season
      - The project can be improved (or fully redone).
      - Best grade is the one considered to calculate final grade.

Classes Planning (tentative)

	Class	Wednesday		Evaluation
1	21/Sep	Introduction.		
2	28/Sep	Cyber Situational Awareness.		
	05/Oct	Feriado		
3	12/Oct	Data Acquisition.	TP: Data Acquisition	
4	19/Oct	Data Processing.	TP: Data Processing	
6	26/Oct		TP: Data Processing	
7	02/Nov		Project problem support + TP: Data Processing	
8	09/Nov		Project problem presentation	A1
9	16/Nov	Network (Entities) Profiling.		
10	23/Nov		TP: Entity Profiling (Classification and Anomaly Detection)	
11	30/Nov		TP: Entity Profiling (Classification and Anomaly Detection)	
12	07/Dec		TP: Entity Profiling (Classification and Anomaly Detection)	
13	14/Dec		Project development	
	21/Dec		Project development	
	28/Dec	Férias Natal		
14	04/Jan		Project demo	A2

Bibliography

- Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security, Omar Santos, Cisco Press, 1 edition (22 Sept. 2015), ISBN-13: 978-1587144387.
- Network Security Through Data Analysis: Building Situational Awareness, Michael S. Collins, O'Reilly Media, 1 edition (23 Feb. 2014), ISBN-13: 978-1449357900.
- Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats, Bill Gardner, Valerie Thomas, Syngress; 1 edition (August 21, 2014), ISBN-13: 978-0124199675.
- Hacking: The Ultimate Beginners Guide, Max Green, CreateSpace Independent Publishing Platform (November 29, 2015), ISBN-13: 978-1519592668.
- Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies, Ira Winkler, Araceli Treu Gomes, Syngress; 1 edition (December 7, 2016), ISBN-13: 978-0128093160.
- Hacking Wireless Networks - The ultimate hands-on guide, Andreas Kolokithas, CreateSpace Independent Publishing Platform (March 5, 2015), ISBN-13: 978-1508476344.
- Hacking: Beginner's Guide to Expert Hacking, David Henry, (October 13, 2016).
- Outlier Analysis, Charu C. Aggarwal, Springer; 2nd ed. 2016 edition (January 2, 2017), ISBN-13: 978-3319475776.
- Designing Cisco Network Service Architectures (ARCH), John Tiso, Cisco Press, ISBN-13: 978-1587142888, 3rd Edition, 2011.
- Yusuf Bhaiji, Network Security Technologies and Solutions (CCIE Professional Development), Cisco Press, 1st edition, 2008.