Programa e regras de funcionamento da disciplina

Técnicas de Perceção de Redes
Network Awareness

Mestrado Integrado em
Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro
deti.ua.pt

Docente

- Prof. Paulo Salvador (aulas teóricas e práticas)
  - Email: salvador@ua.pt
  - Web: http://www.av.it.pt/salvador
  - Gabinete: IT

- Atendimento
  - Flexível!

Objetivos de TPR

- Integração dos conhecimentos de rede de comunicações e sistemas.
- Compreender e desenvolver arquiteturas e metodologias para
  - Monitorização de rede e serviços,
  - Deteção de ataques ou anomalias de funcionamento
  - Despoletar medidas de proteção/correção.

Programa

- Caracterização e identificação de perfis de utilização de rede.
  - Aquisição, análise e exploração de dados de rede.
  - Caracterização e classificação de comportamentos (atividades/eventos).
  - Metodologias de deteção de anomalias comportamentais.
- Arquiteturas de rede e técnicas de inibição de ataques DDoS.
  - Sistemas de balanceamento de carga para firewalls e servidores.
  - Diferenciação entre acessos lícitos e ilícitos.
  - Bloqueio de acessos ilícitos ao nível da rede e dos serviços.
  - Libertação automática e inteligente de recursos em firewalls e servidores.
- Prevenção e deteção de intrusões em redes.
  - Introdução aos vetores de ataque.
  - Mecanismos/metodologias padrão de proteção.
  - Deteção de assinaturas de anomalias em comunicações.
  - Deteção de anomalias comportamentais.
  - Implementação de contra-medidas.

Avaliação

- Contínua com 4 momentos de avaliação:
  - A1 – Apresentação da ideia e plano de desenvolvimento e teste - 20%
  - A2 – Primeira demonstração - 20%
  - A3 – Pitch (Sales Pitch, Pitch Deck, ...) - 20%
  - A4 – Demonstração final - 40%

Plano (prov.)

	Semana	Segunda	Avaliação
1	19/Feb	Introduction. Network attack vectors.	
2	26/Feb	Network monitoring and data acquisition and processing.	
		TP: Data Acquisition	
3	05/Mar	TP: Data Acquisition	
4	12/Mar	Firewalls and Load Balancers. DoS and DDoS (Attacks and Defences).	
		TP: DDoS Detection and Counter-Actions	
5	19/Mar	Entity Statistical Profiling and Classification. Anomaly/Outlier Detection. Time Behaviour Profiling (Wavelets).	
		TP: Network Entities Profiling (Classification and Anomaly Detection)	
	26/Mar	Páscoa	
	02/Apr	Páscoa	
6	09/Apr	TP: Network Entities Profiling (Classification and Anomaly Detection)	
7	16/Apr	TP: Network Entities Profiling (Classification and Anomaly Detection)	A1
	23/Apr	Semana Académica	
8	30/Apr	Machine Learning: Clustering, SVM and NN.	
		TP: Machine Learning (Classification and Anomaly Detection)	
9	07/May	TP: Machine Learning (Classification and Anomaly Detection)	
10	14/May	Project	
11	21/May	Project	A2
12	28/May	Project	
13	04/Jun	Project	A3
			A4

A1	Idea and Planning Presentation.	20%
A2	First Demo	20%
A3	Pitch	20%
A4	Final Demo	40%

Bibliografia

- 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.