Redes e Segurança Informática

2º semestre | 1º ano | 2024.2025

Carlos Guerra | Mário Pinto

Cofinanciado por: NORTE 2020 Programa Regional do Norte | PORTUGAL 2030 | Cofinanciado pela União Europeia

Objetivos

- Identificar os principais requisitos de segurança da informação. Descrever o funcionamento das ferramentas baseadas em criptografia. Aplicar os mecanismos e ferramentas apropriados para proteção da informação.
- Reconhecer a infraestrutura de chave pública (PKI) como um conjunto de equipamento, software e políticas com o objetivo de gerir certificados digitais. Implementar/gerir uma (PKI).
- Selecionar e aplicar mecanismos de autenticação.
- Utilizar protocolos de comunicação seguros.
- Observar as boas práticas no desenvolvimento de software.
- Caracterizar, instalar, administrar e discutir os objetivos de utilização dos sistemas de deteção de intrusão.
- Minimizar riscos de segurança no desenvolvimento de software.

Resultados de Aprendizagem

- Aplicar os principais conceitos de criptografia, discutir a sua utilização em aplicações e protocolos em função de objetivos de segurança e utilizar ferramentas para a cifra e assinatura de conteúdos.
- Caracterizar os principais componentes de uma PKI, discutir a sua utilização em função de objetivos de segurança, implementar e gerir uma entidade certificadora local.
- Aplicar os conceitos de autenticação e a sua utilização em aplicações e protocolos de comunicação seguros.
- Utilizar os protocolos de comunicação segura, discutir a sua aplicação em função de objetivos de segurança e de configuração de aplicações para a utilização destes.
- Interpretar os principais tipos de vulnerabilidades em redes e aplicações e utilizar técnicas e ferramentas para sua deteção, demonstração e mitigação.
- Caracterizar os sistemas de deteção de intrusões, discutir objetivos da sua utilização e efetuar a sua instalação e administração.

Conteúdos

- Riscos de segurança em aplicações web
- Criptografia
- Segurança
- Infraestruturas PKI
- Autenticação
- Redes de Computadores
- Protocolos de Comunicação Seguros
- Software Seguro
- Deteção de Vulnerabilidades

Aulas

- Duas Componentes
  - **Teórico-Prática** (TP) 1 hora 14:00 às 15:00
  - **Prática** (P) 3 horas 15:00 às 18:00
- Faltas
  - TP **sem** registo de faltas
  - P **com** registo de faltas

Avaliação

- **Avaliação Discreta** [Pré-definida]
  - **Teste 01** **25%** **31** de **março**
  - **Teste 02** **25%** Data do **Exame Normal**
  - **Trabalhos Práticos** **50%** Entrega e Discussão ao longo das aulas

- Avaliação Final:
  - **Teste** **50%** Data do **Exame Normal**
  - **Trabalhos Práticos** **50%** Entrega 7 dias antes da data do **Exame Normal**
    Discussão na data do **Exame Normal**

Referências Bibliográficas

- elearning
- Bibliografia

  - ZÚQUETE, André. **"Segurança em redes informáticas"**, 6ª Edição, FCA, 2021
  - STALLINGS, William. **"Network Security Essentials: Applications and Standards"**, 6th Edition, Pearson, 2017
  - CORREIA, Miguel; SOUSA, Paulo. **"Segurança no Software"**, 2ª Edição, FCA, 2017
  - STALLINGS, William. **"Cryptography and Network Security: Principles and Practice"**, 7th Edition, Pearson, 2016
  - STALLINGS, William; BROWN, Lawrie. **"Computer Security: Principles and Practice"**, 4th Edition, Pearson, 2018
  - BARRET, Daniel J; SILVERMAN, Richard E.; BYRNES, Robert G. **"SSH, The Secure Shell: The Definitive Guide"**, 2nd Edition, O'Reilly Media, Inc. , 2005
  - CRIST, Eric F; KEIJSER, Jan Just. **"Mastering OpenVPN"**, Packt Publishing, 2015