ipt Instituto Politécnico de Tomar

Escola Superior de Tecnologia de Tomar **Ano letivo:** 2022/2023

Engenharia Informática
Licenciatura, 1º Ciclo
Plano: Despacho n.º 8644/2020 - 08/09/2020

Ficha da Unidade Curricular: Segurança Informática
ECTS: 5; Horas - Totais: 135.0, Contacto e Tipologia, TP:28.0; PL:28.0;
Ano | Semestre: 3 | S1
Tipo: Obrigatória; Interação: Presencial; Código: 911944
Área Científica: Arquitectura de Computadores e Redes

Docente Responsável
Luís Miguel Lopes de Oliveira
Professor Adjunto

Docente(s)
Luís Miguel Lopes de Oliveira
Professor Adjunto
Luis Agnelo de Almeida
Professor Adjunto

Objetivos de Aprendizagem

Aplicar as boas práticas à gestão da segurança da informação.
Concretizar políticas de segurança recorrendo aos mecanismos mais adequados.
Desenvolver e aplicar estratégias de gestão do risco.

Objetivos de Aprendizagem (detalhado)

1. Conhecer e saber aplicar as boas práticas da gestão e manutenção de redes informáticas.
2. Identificar as principais ameaças à integridade, disponibilidade e confidencialidade de um serviço.
3. Identificar as principais técnicas criptográficas e os seus contributos na garantia da confidencialidade e integridade.
4. Relacionar os principais ataques à segurança com os mecanismos de protecção mais adequados para os mitigar.
5. Identificar as principais limitações dos mecanismos de segurança.

6. Implementar soluções de segurança adequadas ao risco dos recursos a proteger.

Conteúdos Programáticos

1. Computer Security concepts and principles.
2. Cryptographic building blocks.
3. User Authentication
4. Authentication Protocols and Key Management.
5. Operating Systems Security and Access Control.
6. Software security.
7. Malware.
8. PKI.
9. Web and browser security
10. Firewalls, VPNs and IDSs.
11. Wireless LAN security.

Conteúdos Programáticos (detalhado)

1. Conceitos básicos e princípios da segurança
. Principais objectivos da segurança informática
. Políticas e ataques de segurança
. Avaliação e gestão dos risco
. Conhecer o adversário
. As ameaças, classificação das ameaças de acordo com as categorias STRIDE

2. Mecanismos criptográficos
. Cifra e decifra
. Mecanismo critptográficos de chave simétrica
. Mecanismos critpográficos de chave assimétrica
. Funções de Hash e MAC.

3. Autenticação de utilizadores
. Passwords
. Ataques contra as passwords
. Recuperação de passwords
. Geradores de passwords e Tokens
. Autenticação sem passwords (FIDO)
. Mecanismos de autenticação por múltiplos factores

4. Protocolos de autenticação e de gestão de chaves
. Autenticação e estabelecimento de chaves
. Protocolos de autenticação
. Acordo de chaves (DH)
. Password-authenticated key exchange: EKE e SPEKE

5. Mecanismos de segurança para os sistemas operativos e controlo de acessos
. Proteção da memória, accountability (responsabilização) e supervisão

. The reference monitor, access matrix, and security kernel
. Permissões e controlo de acesso
. Role-based (RBAC)

6. Segurança do software.
. Race conditions
. Stack-based buffer overflows
. Heap-based buffer overflows e heap spraying
. Exploração de Buffer overflow e medidas de mitigação

7. Malware.
. Vírus e worms e mecanismos de deteção e eliminação
. Trojan horses, backdoors, keyloggers, rootkit
. Rootkit
. Ransomware, botnets e outros tipos de malware

8. PKI.
. Certificados, autoridades de certificação
. Cadeia de certificação
. Arquitetura de uma CA/PKI architectures e modelos de confiança
. TLS web site certificates

9. Security para a Web
. Revisões acerca de HTML, do HTTP e de scripts
. O TLS
. HTTP cookies e DOM objects
. Autenticação baseada em cookies, e respetivos ataques
. Cross-site scripting (XSS) e SQL-injection

10. Firewalls, VPNs and IDSs.
. Proxies e Firewalls
. SSH
. VPNs e túneis seguros
. Sistemas de deteção de intrusões
. Analisadores de protocolos, ferramentas de reconhecimento

11. Segurança aplicada às rede sem fios
. Mecanismos de segurança da família protocolar 802.11
. Vulnerabilidades das redes 802.11
. A arquitectura 802.1x
. O WPAv3

Metodologias de avaliação

A avaliação é composta por duas componentes:
. Componente teórica com o peso de 60% na nota final e com a nota mínima de 7.5 valores.

. Componente prática com o peso de 40% na nota final e com a nota mínima de 10 valores.
A avaliação da componente teórica é composta pela classificação de uma prova escrita realizada individualmente e sem consulta.
A avaliação da componente prática corresponde à média da classificação dos trabalhos práticos realizados durante as aula práticas laboratoriais. Os trabalhos laboratotiais podem ser realizados individualmente ou em grupos de dois alunos.
Estas regras aplicam-se a todas as épocas de avaliação.

Software utilizado em aula

Não aplicável

Estágio

Não aplicável

Bibliografia recomendada

- William, S. (2000). *Network Security Essentials* . 1, Prentice-Hall. .
- Zúquete, A. (2006). *Segurança em Redes Informáticas* . 1, FCA - Editora de Informática. Lisboa
- Van Oorschot, P. (2021). *Computer Security and the Internet* (Vol.). (pp. -). Springer. Canada

Coerência dos conteúdos programáticos com os objetivos

Objetivo 1: 1,2
Objetivo 2: 2
Objetivo 3: 2,3,45
Objetivo 4: 2,3,4,5
Objetivo 5: 2,3,4,5,6
Objetivo 6: 3,4,5,6

Metodologias de ensino

Aulas teórico-práticas onde são estudados os fundamentos teóricos desta UC. Aulas laboratoriais onde se simulam problemas e se testam e avaliam soluções.

Coerência das metodologias de ensino com os objetivos

Não aplicável

Língua de ensino

Português

Pré-requisitos

Não aplicável

Programas Opcionais recomendados

Não aplicável

Observações

Não aplicável
Objetivos de Desenvolvimento Sustentável:

4 - Garantir o acesso à educação inclusiva, de qualidade e equitativa, e promover oportunidades de aprendizagem ao longo da vida para todos;
9 - Construir infraestruturas resilientes, promover a industrialização inclusiva e sustentável e fomentar a inovação;
16 - Promover sociedades pacíficas e inclusivas para o desenvolvimento sustentável, proporcionar o acesso á justiça para todos e construir instituições eficazes, responsáveis e inclusivas a todos os níveis;

Docente responsável

Luís Miguel Lopes de oliveira

Digitally signed by Luís Miguel Lopes de oliveira
Date: 2022.09.22 09:19:24 +01'00'

Homologado pelo C.T.C.
Acta n.º 30 data 19/10/2022