

Segurança em Redes Informáticas

Este curso alerta para os problemas de segurança que podem advir da ligação de uma máquina ou rede local à Internet e explica de que forma os problemas podem ser minimizados ou evitados. Ajuda também os gestores das máquinas ou redes locais a saberem identificar os seus problemas de segurança e a perceberem bem o âmbito e alcance das políticas de protecção que podem implantar e dos mecanismos de segurança que existem para esse efeito.



Duração: 24 Horas

Objectivos Gerais

Alertar para o tipo de vulnerabilidades que tipicamente existem e são exploradas em ataques, como podem ser detectadas as vulnerabilidades ou a sua exploração, como pode ser minimizada a exploração de vulnerabilidades existentes e como se pode tomar medidas ativas e eficazes de protecção quando se interage com ou através de Internet, que é um meio inseguro por natureza.

Objectivos Específicos

No final deste curso, os participantes deverão ser capazes de identificar as principais ameaças de segurança assim como formas de minimização do seu impacto, identificar os principais componentes de uma solução de segurança, configurar um router, uma firewall, um sistema IDS, uma política de segurança nos servidores/clientes e proteger a transmissão de dados nos acessos remotos.

Destinatários/Pré-Requisitos

Este curso é destinado a todos os utilizadores ou Administradores de redes locais domésticas ou de redes de PME. Alunos de cadeiras de licenciatura ou de cursos de pós-graduação na área da Segurança de Redes.

Conteúdos Programáticos

Módulo 1 - Introdução

- Vulnerabilidades, ataques, riscos e defesas
- Políticas vs. mecanismos de segurança
- Segurança em sistemas distribuídos

Módulo 2 – Criptografia

Módulo 3 - Gestão de Chaves Públicas

Módulo 4 - Vulnerabilidades em Máquinas de Sistemas Distribuídos

- Detectores de vulnerabilidades
- Cenários absurdos
- Problemas de realização

Módulo 5 - Vulnerabilidades em Redes Locais e de Grande Escala

- Levantamento de informação arquitectural
- Tradução de nomes
- Confidencialidade
- Autenticidade
- Prestação de serviços

Módulo 6 - Firewalls

- Introdução
- Arquitectura de uma firewall
- Modelo de intervenção

- Serviços oferecidos

- Topologias elementares

Módulo 7 - Sistemas de Detecção de Intrusões

- Arquitectura dos IDS
- Classificação dos IDS
- Limitações dos IDS

Módulo 8 - Redes Privadas Virtuais (VPN)

- Definição
- Chaves de sessão
- Tipos de VPN

Módulo 9 - Segurança em Redes Sem Fios 802.11 (WLAN ou Wi-Fi)

- Arquitectura de uma rede 802.11
- Visão geral da segurança em redes estruturadas 802.11
- WEP (Wired Equivalent Privacy)
- Evolução
- TKIP (Temporal Key Integrity Protocol)
- AES-CCMP
- 802.1X
- EAP (Extensible Authentication Protocol)
- Ataques de negação de prestação de serviço