Segurança de Redes

Objetivo: Fornecer conhecimento dos fundamentos sobre segurança em redes e suas aplicações de forma que, após o curso, o aluno esteja apto a manter a integridade das informações que trafegam através da rede e a limitar o acesso a determinados recursos do sistema.

Carga Horária: 40 Horas.

Pré-requisito: Possuir conhecimentos básicos de Informática.

Conteúdo Programático:

Capitulo 1 - Conceitos Básicos

Ameaças

Vulnerabilidades

Vírus e outros

Backup

Engenharia de Segurança

História da Segurança

Engenharia Social

Políticas de Segurança

Análise de Riscos

Vulnerabilidades / Inteligência e Contra Inteligência

Padrões e frameworks empregados para lidar com a segurança

Informação - Transmissão de Dados - Inteligência

Família ISO 27000

Norma ISO/IEC 17799 (Code of practice for information security management)

BS 7799 (British Standard)

Controles e Objetivos (Cobit) da Segurança da Informação

Riscos

Confidencialidade / Disponibilidade / Integridade

Capítulo 2 - Melhores Práticas em Segurança

O que fazer e por que fazer

Antivírus

Controle de Acesso (ACL)

Backups e Restauração

5S

Bloqueios e Segurança Física

Tokens e identificação

Senhas e ACL

Contas privilegiadas

Logs

Appliances, Firewalls e IDS

DNS

Capitulo 3 - TCP/IP

Histórico

Pacotes e Datagramas

Pilha TCP/IP

Tipos de ameaças

Spoofing

State Machine

Ipv6 / Ipv4

ICM

PTCP

IP

Capitulo 4 - Arquitetura de um ataque

Tipos de ataque

Arquiteturas de Ataques

Assinaturas dos 9 tipos de ataques mais comuns

Ferramentas de Ataque

Capitulo 5 - Criptografia

Confiabilidade

Criptografia

Transposição / Assimetria / Simetria

Chaves

Funções Hash

Aplicações

Certificados, Assinatura Digital

PKI

Padronizações de Criptografia

Produtos Microsoft / RSA de PKI

PGP

Capitulo 6 - IPSEC

Planejando e Implementando IPSEC com Windows 2003

Camadas de proteção

Plataformas que utilizam IPSEC e exemplos.

Capitulo 7 - Vírus e Outros Malwares

Tipos de Vírus

Assinaturas

Padronizações

Analises

Erros mais comuns

Ferramentas e tipos de injection

Capitulo 8 - IDS

IDS, Firewalls

Tipos de IDS

Tipos de Firewalls

Aplicações de Firewalls

Aplicações de IDS

Honeypots

Assinaturas

Padrões e softwares

Perímetro, DMZ, Roteadores

Filtros e Rotas

NAT

Ferramentas de Analise de Risco

Capitulo 9 - Autenticação e Serviços

RADIUS

TACACS

EAP

PAP

CHAP

MSCHAP

VPN (PPTP, L2F, L2TP, SSL)

VPDN

HTTPS / CERTIFICADOS E SSO

DNS + Segurança e Spoofing

Telnet

FTP

SSH

Capitulo 10 - A Lei

Direito aplicado a informática

Dercife e órgãos especializados

Propriedade Intelectual e quesitos legais

SOX

Capitulo 11 - Perícia Forense

Conceitos, Técnicas e Ferramentas para Investigação e Perícia Digital

Discos, Sistemas e Mídias

Duplicando dados, recuperando dados e arquivos

Forense no Windows e no Linux e processo de Boot

Investigando Trafego de rede e logs

Resposta de Incidentes