

IMD0703 – Segurança de Redes

Apresentação da Disciplina e Avaliação Diagnóstica



Você errou de sala se espera...



Ementa

- Histórico e conceitos básicos de segurança
- Análise de riscos
- Técnicas de ataque e defesa: incluindo firewall, IDS e IPS
- Autenticação e Controle de Acesso
- Criptografia, PKI e suas aplicações
- Segurança física
- Segurança na comunicação, incluindo IPSec, VPN e SSL
- Segurança no sistema operacional
- Auditoria
- Leis, normas, boas práticas e padrões de segurança da informação
- Políticas, controles e medidas de Segurança da Informação

Objetivos, Competências e Habilidades

- Objetivos
 - Introduzir conceitos de segurança em redes de computadores
 - Apresentar mecanismos de ataque e defesa em redes de computadores
- Competências
 - Identificar ameaças/riscos de segurança em redes de computadores
 - Reconhecer, instalar e gerenciar mecanismos de segurança em redes de computadores
- Habilidades
 - Reconhecer as principais ameaças à segurança em redes de computadores
 - Instalar e configurar de ferramentas de segurança
 - Planejar e implementar auditoria de segurança
 - Reconhecer e utilizar protocolos de segurança

Conhecimentos Desejáveis

- Esta disciplina (IMD0703) não possui pré-requisitos formais.
 - E o que isso **NÃO significa?**
 - Que a disciplina é fácil
 - Que não é preciso saber nada específico para cursar esta disciplina
 - Que esta disciplina não exija esforço
 - Que são horas/créditos grátis
 - E o que isso **significa?**
 - Alguns conhecimentos são dados como conhecidos pelos alunos
 - Programação (Saber escrever e ler programas em diferentes linguagens)
 - Sistemas Operacionais (particularmente o Linux)
 - Redes de Computadores (particularmente a pilha TCP/IP)
 - Inglês (bons softwares, materiais e referências não estarão traduzidos)

Metodologia

- A construção das competências será facilitada por meio das seguintes estratégias:
 - Algumas aulas servirão para introduzir conceitos de segurança de redes (e tópicos relacionados)
 - Aulas expositivas (utilização de data show, quadro branco e slides interativos)
 - Discussão dos conceitos e problemas referentes aos assuntos abordados
 - Algumas aulas servirão para praticar a implementação dos conceitos vistos na disciplina
 - Resolução de exercícios
 - Implementação de programas
 - Práticas de laboratório (instalação, configuração e utilização de ferramentas de segurança)

Metodologia

- O conteúdo da disciplina é incremental
 - Os conceitos avançados somente podem ser compreendidos quando os conceitos básicos forem bem assimilados
- Os exercícios e laboratórios propostos devem ser resolvidos e implementados para melhor fixação dos conceitos apresentados
 - Inclusive fora do horário de aula!
- **Atenção:** o conteúdo da disciplina é abrangente e necessita um esforço importante e permanente dos alunos!

Conteúdo – Unidade 1

Histórico e conceitos básicos de segurança.

Introdução à Criptografia. Criptografia Simétrica. Cifra de Bloco. DES. AES.

Criptografia Assimétrica ou Infraestrutura de Chave Pública (PKI). RSA.

Funções Hash. Certificado Digital.

Avaliação Teórica I

Conteúdo – Unidade 2

Autenticação: Protocolos e Mecanismos.

Autorização: Controle de Acesso, Modelos de Controle de Acesso, Mecanismos de controle de Acesso.

Segurança na comunicação: SSL, IPSec e VPN.

Defendendo a rede: Firewall, IDS e IPS.

Avaliação (Teórica e Prática) II

Conteúdo – Unidade 3

Segurança Web

Segurança em email: S/MIME e PGP

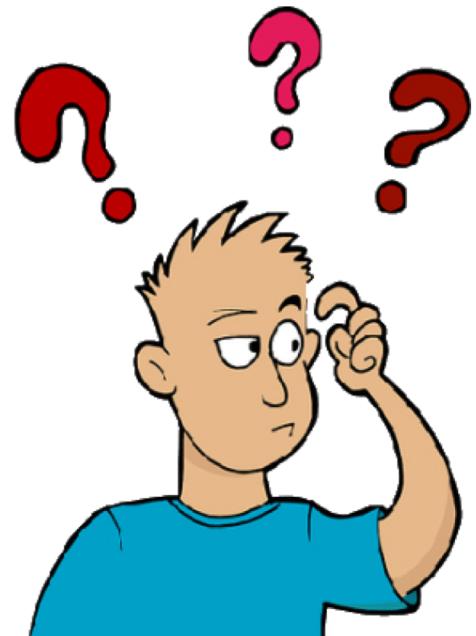
Segurança de redes sem fio: WEP, WPA, WPA2

Segurança de software: programação segura, tratamento de dados e engenharia reversa.

Ferramentas para Teste de Intrusão.

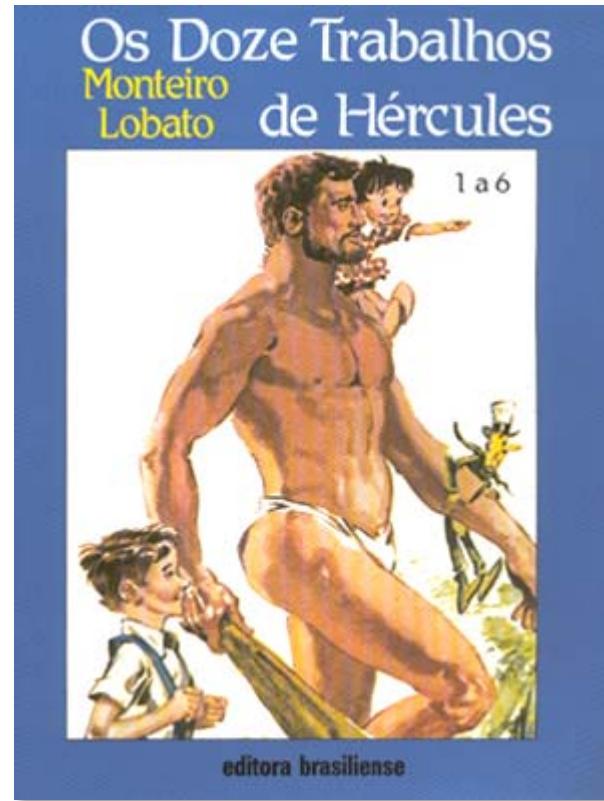
Avaliação (Teórica e Prática) III

Alguma Questão?



Avaliação Diagnóstica

Hora de mostrar o que já sabem...

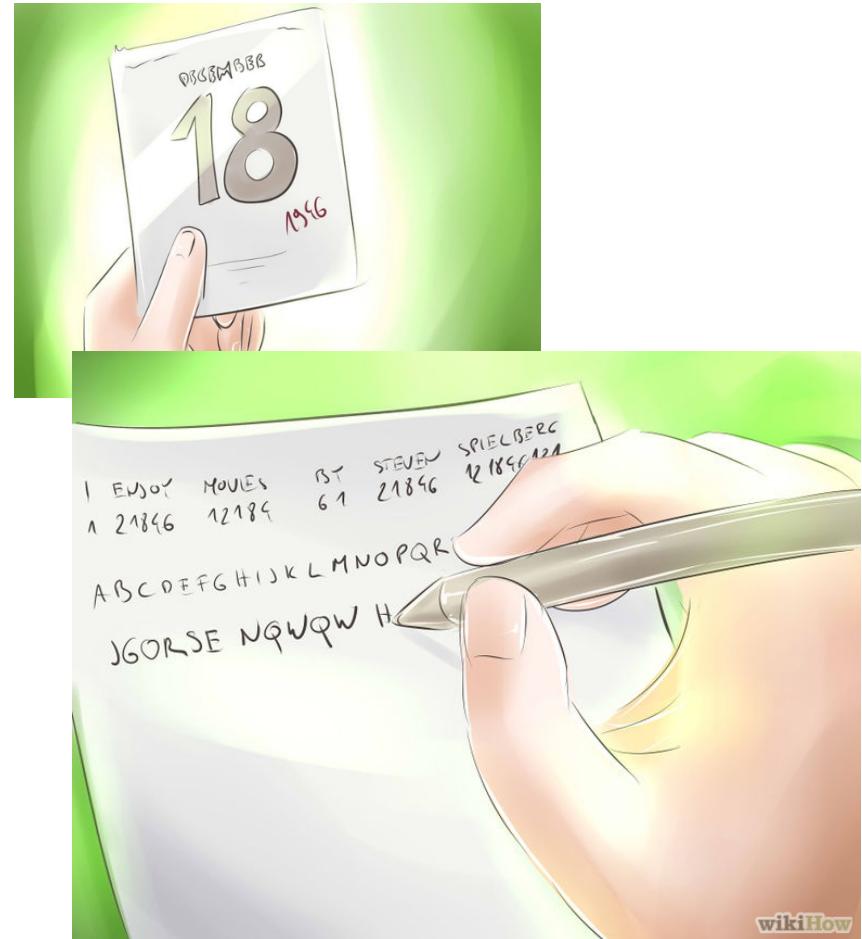


Programação (1)

- Escreva dois programas (na linguagem que você domina) que permitam **cifrar** e **decifrar** um arquivo de texto indicado pela linha de comando, seguindo a **Cifra de Troca de Data**
 - Exemplo: **#./cifrar data mensagem.txt mensagem.sec**
 - **cifrar** : nome do programa de cifragem
 - **mensagem.txt** : arquivo de entrada com a mensagem em claro
 - **mensagem.sec** : arquivo de saída com a mensagem cifrada
 - **data** : a data a ser usada para cifrar os dados
- O programa de decifragem deve ler um arquivo de texto cifrado (.sec), indicado na linha de comando e imprimir em tela o texto decifrado.
 - Exemplo: **#./decifrar data mensagem.sec**
 - **decifrar** : nome do programa de decifragem
 - **mensagem.sec** : arquivo de entrada com a mensagem cifrada
 - **data** : a data a ser usada para decifrar os dados
- Faça alguns testes entre seus colegas, enviando a eles mensagens cifradas+data escolhida

Programação (2)

- Como funciona a **Cifra de Troca de Data** (fonte: <http://pt.wikihow.com/Criar-Cifras-e-C%C3%B3digos-Secretos>)
 - Passo 1: **Escolha uma data**. Escolha uma data. Um exemplo pode ser o aniversário de Steven Spielberg: 18 de Dezembro de 1946. Escreva esta data usando números e barras (18/12/46) e depois remova as barras, deixando você com um número de seis dígitos que você usará para cifrar sua mensagem: 121846.
 - Passo 2: **Atribua os números a letras**. Presumindo que a mensagem seja "Eu gosto dos filmes de Steven Spielberg". Abaixo da mensagem, você escreverá o número de seis dígitos repetidamente até chegar ao fim: 18 12461 812 461218 12 461812 461812461.



Programação (3)

- (Cont)
 - Passo 3: **Criptografe sua mensagem**. Escreva o alfabeto da esquerda para a direita. Troque cada letra do texto pelo número de espaços indicado abaixo dela. A letra E troca um espaço, o que a transforma em F; U troca 8 espaços, o que a torna C. Note que esta última letra faz com que você volte ao início do alfabeto, caindo no C. Sua mensagem final deve ser: FC HQWZP LPU JOMOFA EG WZFDPP WVJMMMDIXH.
 - Passo 4: **Traduza a mensagem**. Quando alguém quiser ler sua mensagem, tudo o que a pessoa precisa saber é a data usada para codificá-la. Basta reverter o processo e a pessoa lerá a mensagem: escreva o código numérico, depois volte a quantidade de letras do alfabeto.

