



TECNOLOGIAS WEB – AULA 3

PROF. RAFAEL DIAS RIBEIRO
@RIBEIRORD



Objetivos:

- Apresentar os principais aspectos de segurança tanto no lado cliente quanto no servidor.
- Compreender as implicações de segurança individual e seus métodos de proteção.
- Compreender o uso da criptografia e da assinatura digital, suas vantagens e desvantagens.

Na concepção da Internet ,a ideia era baseada no aspecto de que se um nó fosse atacado, o outro deveria servir de caminho alternativo.

Caminhos alternativos podem ser utilizados por invasores, pois, se em nossa rede temos vários caminhos para ir e vir, nada mais lógico que aquele que se propõe a invadir nossa rede também tente percorrê-los.




⚠

SEGURANÇA

Falhas Técnicas:

- Protocolos
- Links
- Aplicações

Engenharia Social:

- Comportament
o



PERSONAGENS

HACKERS	CRACKERS	LAMMERS
		



ATAQUES (mais populares...)



Cavalo de Tróia

São programas de computador que parecem ser úteis, mas na verdade comprometem a sua segurança e causam muitos danos.

Ex:

Um cavalo de Tróia recente apresentava-se como um email com anexos de supostas atualizações de segurança do S.O., mas na verdade era um vírus que tentava desativar programas antivírus e firewalls.



Cavalo de Tróia

Outro tipo de cavalo de tróia (trojan), se destina a roubar senhas de bancos e aplicativos dos usuários da máquina alvo.

Eles conseguem até monitorar a sequência do mouse nos teclados de senhas. Estes são do tipo Keylogger.



E-MAIL – Caixa de Entrada (INBOX)

Mensagem : O serviço de Internet Banking está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem.

A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha.

Na verdade, este aplicativo está preparado para furtar sua senha de acesso a conta bancária e enviá-la para o atacante.

Quebra de Senha

Tem como objetivo quebrar as senhas de sistemas e usuários.

Técnicas:

**Dicionários
de
Palavras**



“Força Bruta”



Denial Of Service (DOS)



Este ataque se caracteriza pela utilização de computadores de usuários comuns para em um determinado momento **sobrecarregarem um servidor** com uma **quantidade excessiva de solicitações de serviços tirando-os do ar.**

Denial Of Service (DOS)



Geralmente , invasores implantam, nas máquinas dos usuários, **programas zumbis** que ficam aguardando a ordem de atacar coletivamente em uma determinada data.



Mail Bomb

O invasor sobrecarrega o servidor de mensagens de correio eletrônico com mensagens, fazendo com que este pare de responder pelo acúmulo de carga de serviço.

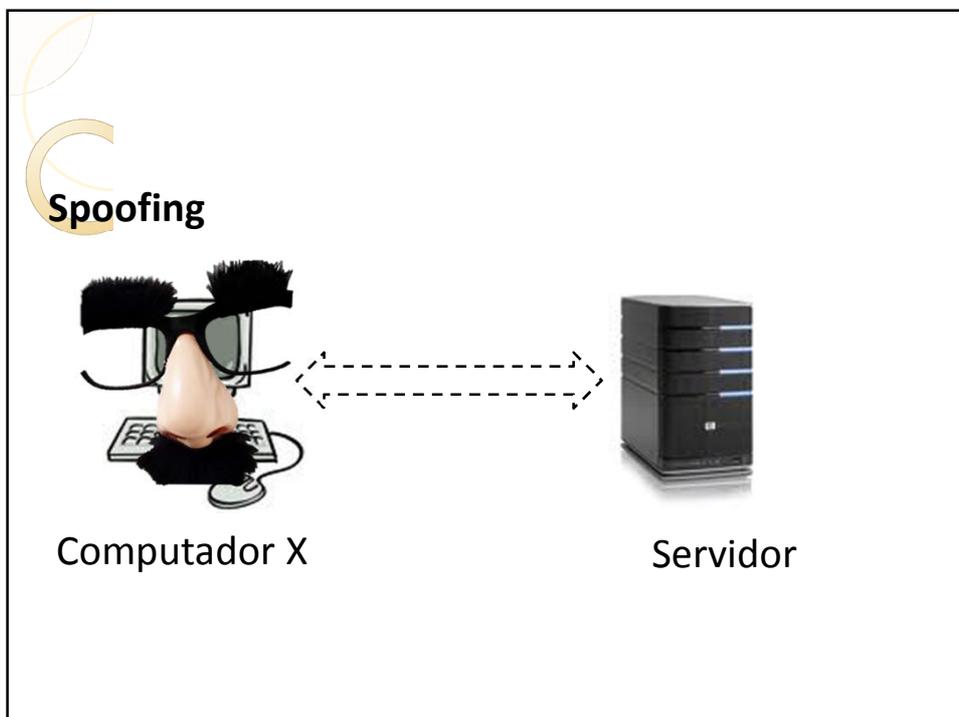
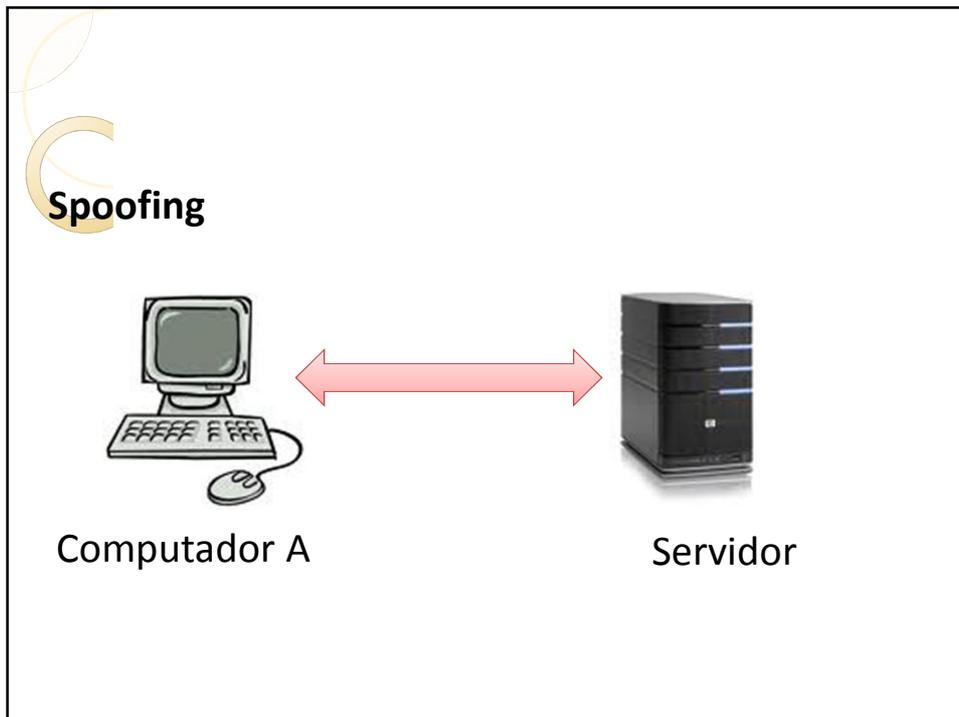


Phreaking



Hackers de Telefonia
(Phone+Freak ou Phreak)

Hoje com a propagação da Telefonia Celular os Phreakers vieram a tona, seja clonando celulares ou realizando escuta telefônica via frequência .



Scamming

O intuito deste ataque é roubar senhas de bancos enviando ao usuário uma página simulando o site do banco do mesmo.

Ex:

<http://www.nomedobanco.com.br>

<http://www.nomedbanco.com.br>

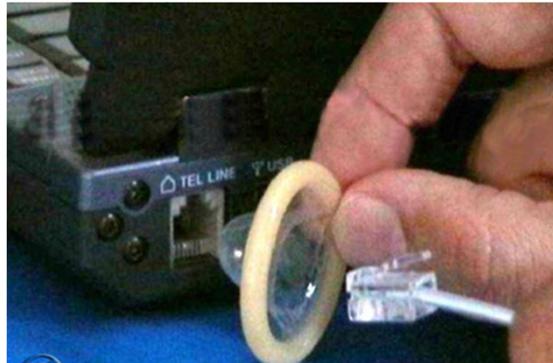
Scamming

Este é um dos ataques que mais bem realizados, pois muitos usuários não reparam no endereço da URL, nem mesmo no cadeado do site.





DICAS DE SEGURANÇA



SENHA “QUASE” FORTE

- Use uma senha longa
- Quanto menos tipos de caracteres houver na senha, mais longa ela deverá ser
- Use todo o teclado, e não apenas os caracteres mais comuns
- Use palavras e frases que você possa lembrar com facilidade, mas que outras pessoas tenham dificuldade de adivinhar



SENHA “QUASE” FORTE

Mais dicas:

<http://www.microsoft.com/brasil/athome/security/privacy/password.mspx>

<http://www.google.com/support/accounts/bin/answer.py?hl=br&answer=32040>



CRIPTOGRAFIA

Para proteger uma informação (privacidade e confidencialidade) é necessário um algoritmo de criptografia capaz de transformar a mensagem original em uma mensagem cifrada, isto é, não compreensível por uma terceira entidade.

O método ou algoritmo para cifrar e decifrar é chamado de cifra

