

# Segurança em computadores e em redes de computadores

## Uma introdução



**Matheus Mota**  
matheus@lis.ic.unicamp.br  
@matheusmota

# Computador/rede segura

- Confiável
- Integro
- Disponível
- Não vulnerável

# Porque se preocupar com segurança?

- Dados confidenciais
  - Senhas, números de cartões de crédito ...
  - Dados pessoais e comerciais
  - Contas de acesso: Usuário e senha
- Danificação de sistemas (críticos ou não)
- etc.

# **Malware**

*Malicious Software*

# Principais Malware

- Vírus
- Worms
- Bots
- Cavalos de Troia
- Backdoors
- Spywares
  - Keyloggers/Screenloggers
- Rootkits
- SPAM

# Vírus

Programa que se propaga infectando outros programas e arquivos de um computador. **Precisa ser executado** no hospedeiro (host)



# Worm (Verme)

- Programa capaz de se propagar automaticamente através da rede explorando as vulnerabilidades dos hosts
- Diferente do vírus, este não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar



# Bot

- Programa capaz de se reproduzir através da rede.
- A diferença entre este e um Worm é o fato do invasor poder se comunicar com o bot remotamente e realizar ataques com inúmeros computadores infectados (botnets)

# Cavalo de Tróia

Programa que se propõe a executar funções específicas mas executa funções maliciosas sem o conhecimento do usuário. Normalmente são disseminados como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc).



# Backdoor

Programa, normalmente instalado após ataque, que permite a um invasor retornar a um computador comprometido sem ser notado.



# Spywares

Termo utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.



# Keylogger

Programas capazes de escutar, gravar e compartilhar iterações do usuário com o teclado (sequência de teclas pressionadas).



# Screenlogger

Programas capazes de escutar, salvar e compartilhar o estado total ou parcial da tela (printscreen)

- A partir dos cliques, por exemplo
- Utilizado para driblar teclados virtuais



# Rootkits

Programas que “maqueiam” a presença de invasores e garantem que estes possam ter acesso a privilégios após o ataque



# SPAM

- Termo usado para se referir a mensagens (não necessariamente email) não solicitadas, geralmente enviadas para um grande número de pessoas.
- São utilizados para propagar malware ou páginas falsas (phishing) que copiam dados de usuários



# Anti-Malware

# Principais Anti-Malware

- Anti-vírus
- Anti-spyware
- Filtro Anti-Spam

# Anti-virus

“Programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.” *antispam.br*



# Anti-spyware

Programa utilizado para combater spyware (keyloggers, screenloggers entre outros programas espiões).



# Anti-spam

Programa que utiliza mecanismos de detecção de mensagens indesejadas, além de permitir a separação dos *e-mails* conforme regras pré-definidas.



# Ataques a redes de computadores

# Principais tipos de ataques

- Ataques Força Bruta
- Scan (Varredura)
- Exploração de falhas em aplicações e Soss
- DOS
- DNS Poisoning
- Sniffing

# Ataques tipo 'força bruta'

- Coletam dados do usuário (nomes, datas, telefones etc.)
- Elaboram combinações entre estes dados
- Para cada combinação produzida, uma tentativa de acesso é feita.
  - Facilmente combatidos com limites de tentativas e captchas



**Security Check**

Enter **both** words below, separated by a **space**.  
Can't read this? Try another.  
Try an audio captcha

contribute of

Text in the box:

[◀ Back](#)

# Exploração de falhas em aplicações e SOs

- “Todo *software* está sujeito a falhas!
- Ataques que exploram exclusivamente as vulnerabilidades existentes ou falhas de configuração de *software*



# Ataques tipo Scan (varredura)

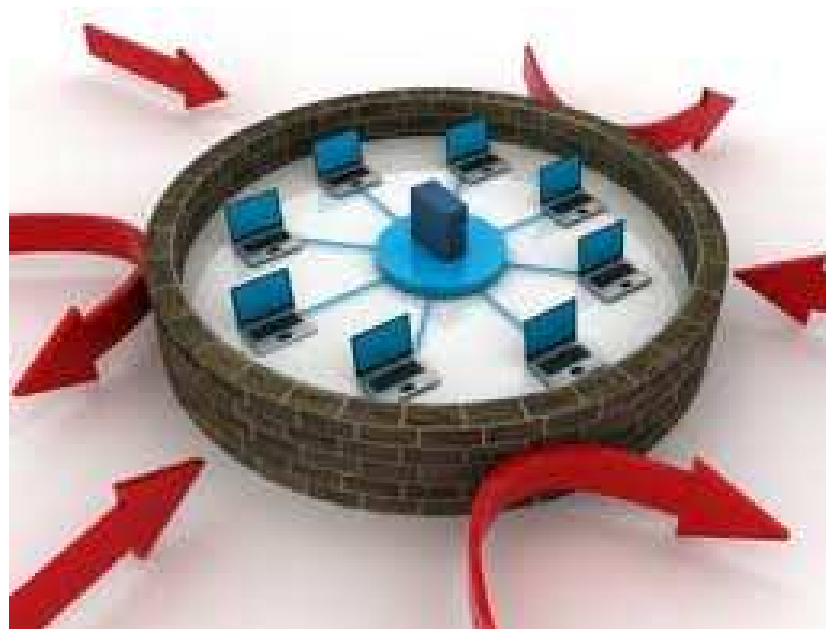
- Programas (scanners) que descubrem os hosts de uma rede
- Para cada host, fazem um conjunto de verificações para descobrir possíveis vulnerabilidades de SO ou aplicações



# DOS – Negação de serviço

Atividade maliciosa onde o atacante é capaz de tirar de operação um serviço ou computador

- e.g., flood de requisições automáticas feitas por diversos bots coordenados pode derrubar um servidor



# Envenenamento de DNS - Introdução

## O que é DNS?

- Domain Name Server
  - Dispositivos na internet são localizados por números únicos (IPs)
  - Números são difíceis de se memorizar, porque não associá-los a nomes?
- 
- Servidor DNS
    - Entidade que mantém uma tabela de associação entre nomes e os números que identificam computadores (serviços) na internet
    - Funciona como um espécie de agenda de telefone

Nome	Telefone
Flavia Silva	19 555 4471
Juca Lopes	73 323 8993

Nome	Identificador
google.com	74.125.229.115
unicamp.br	143.106.10.101

# Ataque por envenenamento de DNS

É uma fraude na associação entre os nomes e os identificadores dos computadores/serviços na internet

- e.g., um host que está em uma rede que “sofre” de envenenamento de DNS pode ser redirecionado para uma página fraudulenta quando solicitar o identificador de [www.bancodobrasil.com.br](http://www.bancodobrasil.com.br) para um servidor DNS



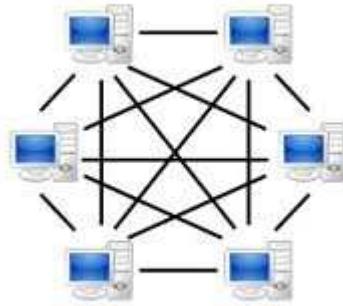
# Ataque por envenenamento de DNS

Exemplo prático

# Ataques tipo Sniffing

Atividade maliciosa onde o atacante se conecta a uma LAN, por exemplo, e passa a “escutar” os dados que trafegam nos canais de comunicação

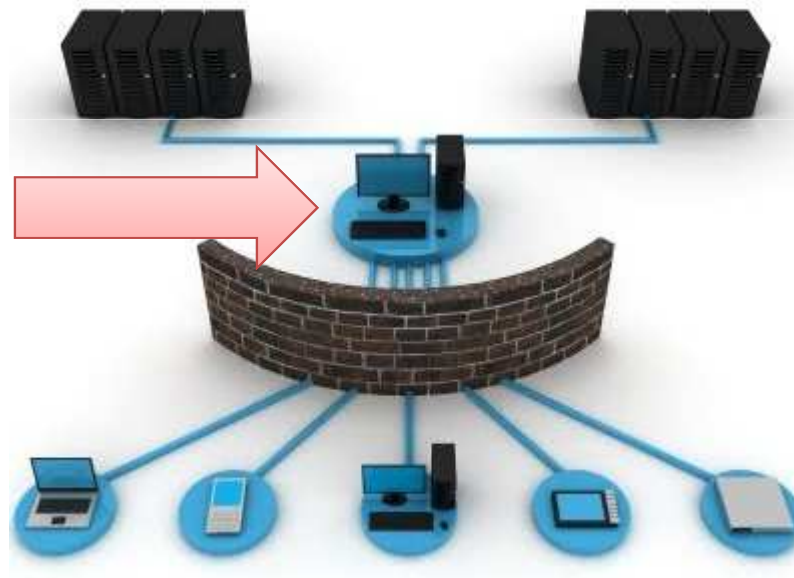
- Dados não protegidos podem ser capturados



# Protegendo-se de ataques

# Firewall

Dispositivo (computador) especializado em dividir e controlar o acesso entre redes e hosts



# Firewall pessoal

- Software especializado em proteger a conexão de rede do comp.
- É executado diretamente no computador do usuário

# Criptografia

- Estratégia para escrever mensagens em forma cifrada ou em código
- Permite que apenas transmissor e receptor compreendam a mensagem
- Exemplo:

a	b	c	d	e	f	g	h	i	j
T	U	I	O	P	R	V	B	M	N
Mensagem Criptografada					Mensagem Original				
TTMNBVOR					aaijhgdf				

# Dicas: Protegendo-se

- Atualize seus sistemas!
  - Incluindo os sistemas de proteção
- Tenha uma boa política de uso
- Não utilize sistemas críticos em computadores/redes desconhecidas
- Procure observar sinais do sistema
  - e.g., sistema mais lento do que o normal
  - Mensagens vindas dos anti-virus e firewalls
- Não utilize conta de administrador no dia-a-dia
- Faça backup dos dados importantes

# Dicas: Elaboração de senhas

- O que não utilizar
  - Nomes, Datas, Números de documentos, Números de telefone, Placas de carro, Palavras de dicionário
- Recomendações
  - Mais de 7 caracteres
  - Deve conter letras maiúsculas e minúsculas
  - Deve conter números
  - Deve conter caracteres especiais (!@#\$%^&\*(){}[])
  - e.g., utilize resumo de frases fáceis de memorizar
    - Frase: “Eu sou da turma 9 de telecom”. Senha: “#E\$dt9dT”

## Créditos e Referências

- **Apresentação** *“Introdução sobre segurança em redes de computadores apresentando conceitos gerais sobre segurança”*
  - Disponível em <http://www.csirt.pop-mg.rnp.br/docs/documentos.html>
- **Site do projeto antispam.br**
  - <http://www.antispam.br>
- **Cartilha de Segurança do Cert.br**
  - <http://cartilha.cert.br>
- **Cartilha de Segurança para Administradores de Rede do Cert.br**
  - <http://www.cert.br/docs/segadmredes/segadmredes.html>