

# Segurança da Informação

## Uma Visão geral

Dênio Mariz, PhD  
[denio@ifpb.edu.br](mailto:denio@ifpb.edu.br)

Março, 2019

# Agenda

- Conceitos
- Ameaças & vulnerabilidades
- Ataques
- Terminologia

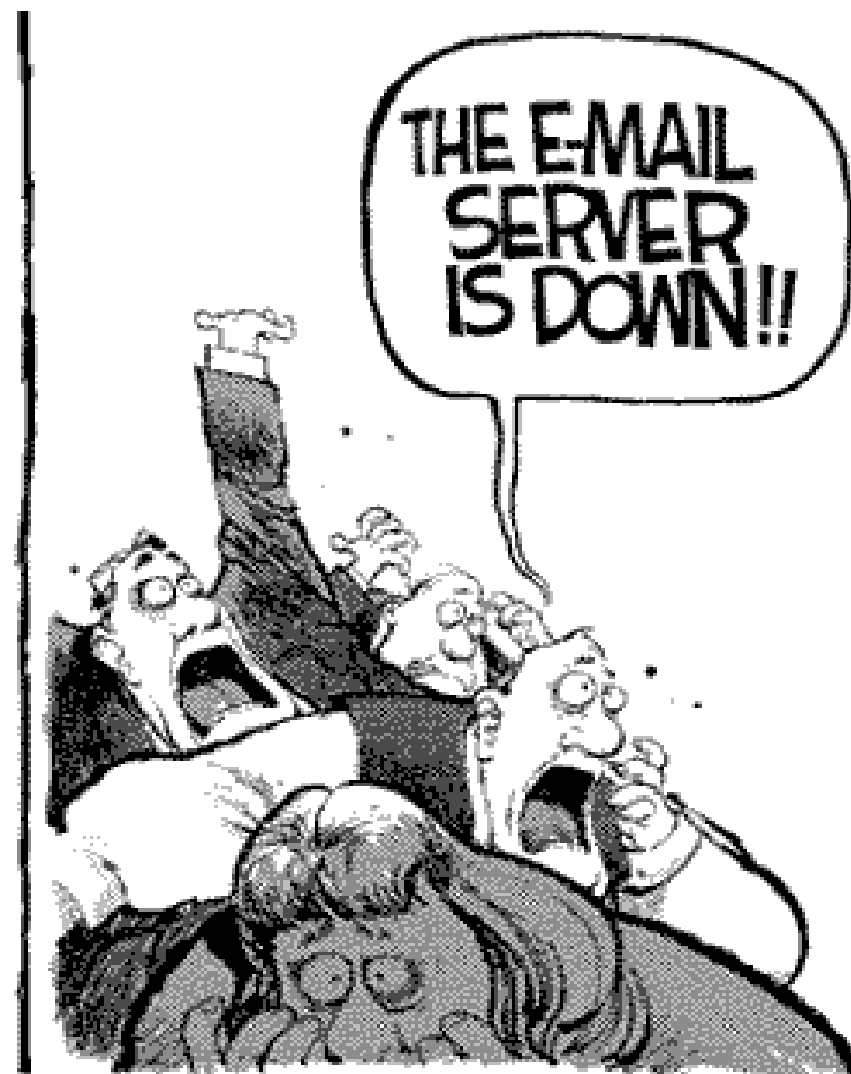


# Definições & Conceitos

# O Terror ontem e hoje



TERROR IN THE 20TH CENTURY...



TERROR IN THE 21ST CENTURY...

O esforço para proteger a informação  
depende do valor da informação

# Segurança da Informação: Objetivos e Requisitos

- Confidencialidade
  - Garantia de que apenas pessoas autorizadas tenham acesso a informação
- Integridade
  - Manutenção do estado da informação, comprovando que não foi modificada enquanto armazenada ou em trânsito
- Autenticação
  - Confirmação da identidade de uma pessoa ou dispositivo
  - Autenticação de mensagem: quando a parte receptora pode verificar a origem da mensagem
- Não repúdio (irrefutabilidade)
  - O autor de uma informação não pode contestar com êxito sua autoria ou validade.
- Disponibilidade
  - Garantia que a informação estará disponível quando necessária

# Terminologia

# Terminologia

1/2

## → Ataque

- Uma tentativa de obter acesso não autorizado
  - aos serviços do sistema,
  - recursos ou
  - informações,
- Uma tentativa de comprometer a integridade do sistema

## → Vulnerabilidade

- Fraqueza em
  - um sistema de informação,
  - nos procedimentos de segurança,
  - nos controles internos ou
  - na aplicação
- ... que poderia ser explorada para violar uma política de segurança



# Terminologia

2/2

## → Ameaça

- Qualquer circunstância ou evento **com potencial** para ter um impacto adverso sobre
  - as operações da organização (incluindo missão, funções, imagem ou reputação) ou
  - sobre os ativos organizacionais, através de um sistema de informação

## → Incidente

- A violação ou ameaça de violação das políticas de segurança, das políticas de uso aceitável, ou das práticas de segurança padrão

## → Risco

- A probabilidade de que uma ameaça cause um dano real

## → Exploit code

- Um código preparado para explorar uma vulnerabilidade conhecida

# Atacantes e seus objetivos

## → Hacker

- Ataca sistemas pelo desafio técnico, por status ou pela "adrenalina" da invasão.
- Constrói suas próprias ferramentas
- Amplo conhecimento em protocolos, SO, linguagem C/Assembler, arquitetura de computadores

## → Cracker, defacer, vândalo

- Hacker com fins destrutivos
- “Black hats”

## → Espião (Corporate raider)

- Ataca sistemas dos concorrentes
- Roubam informação para ganho financeiro ou competitivo

## → Terroristas (cyberterrorist)

- Atacam para causar medo ou por motivação política

# Atacantes e seus objetivos

## → Script Kiddies

- Novato que segue "receitas de bolo" disponíveis na Internet (não sabem exatamente porque aquilo funciona)
- Buscam "fama" com os colegas da escola, ICQ, MSN, ...
- "If you're a good hacker everybody knows you.  
But if you're a great hacker, no one does."  
(“hacker não se diz hacker”)

## → White Hat, Black Hat

- Black hat = hacker
- White hat é um hacker (possivelmente aposentado) que trabalha como consultor de segurança.
- Odiado pelos "Black Hats" (hackers)

# Tipos de Ataques na Rede

- Sniffing, Snooping
  - Farejar a rede = capturar pacotes para análise
  - Monitoramento do tráfego da rede em busca de passwords
- Spoofing
  - Fazer uma mensagem parecer ter vindo de outro host (forjar origem)
- Message Replays (Replay attack)
  - Envio de mensagens em sequencia já ocorrida, visando repetir o resultado
- Message Alteration
  - Modificação da mensagem em trânsito
  - Man-in-the-middle (host anônimo intermediando a conexão)
- Message Delay and Denial
  - Redução da Qualidade de Serviço em uma rede (Denial-of-service)

# Tipos de Ataques na Rede

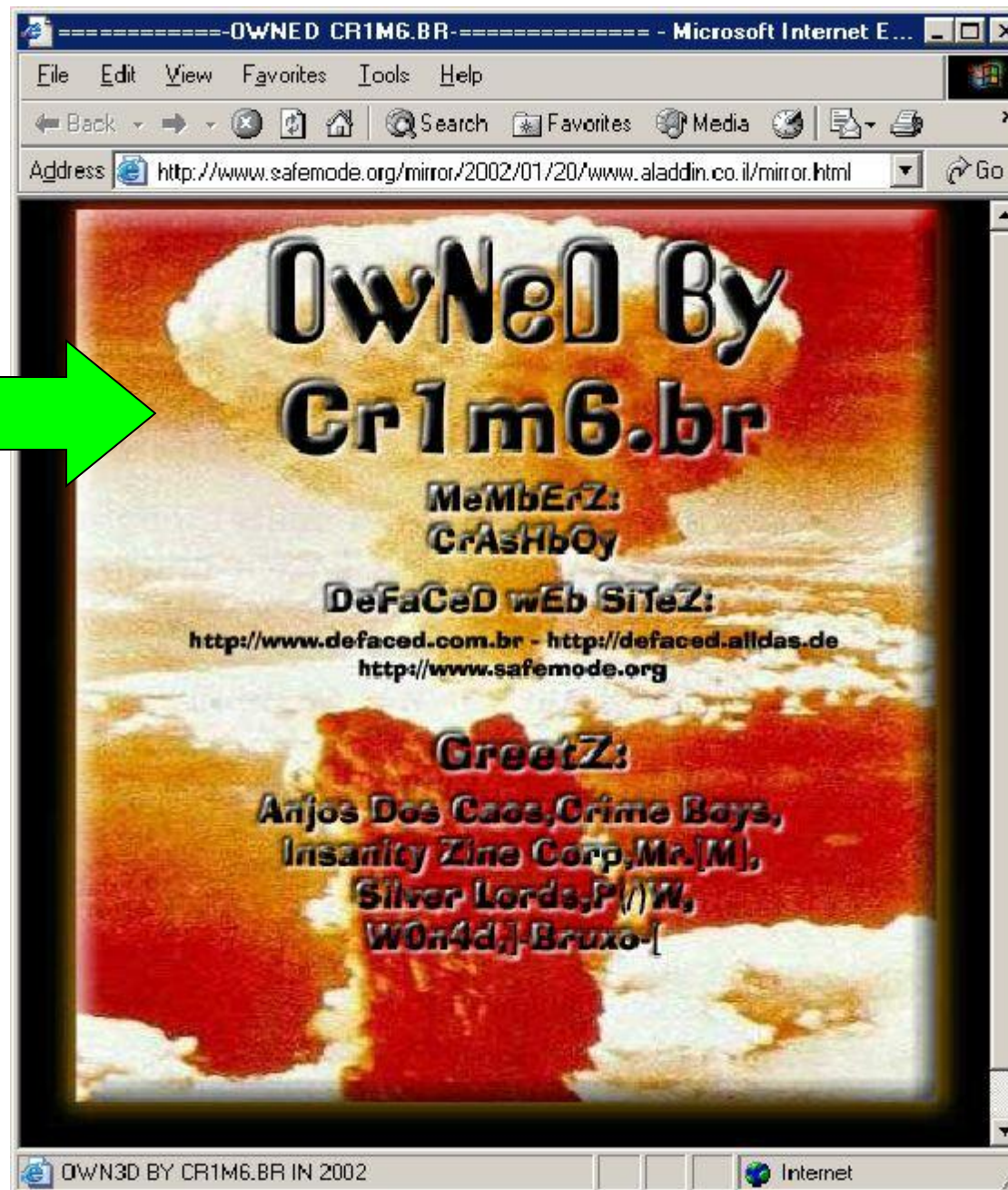
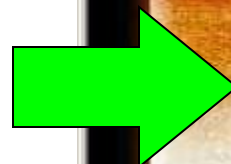
- Privilege scalation
  - Obter mais acesso do que permitido (ex: tornar-se root)
- Remote access, Remote control
  - Acesso remoto (sem login) explorando vulnerabilidades (ex: buffer overflow, falhas em web servers)
  - Controle remoto de um host (ex: backdoor, rootkits)
- Pilfering (chantagem)
  - Logic bombs programados, solicitação de resgate para desligar
  - Ramsonware: bloqueio de dados do usuário
- Defacement
  - Alteração de informação (ex: mudar páginas de sites web)

# Incidentes



# Defacement

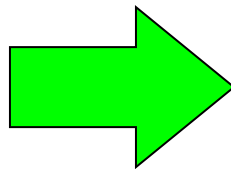
- Página de um famosa empresa de consultoria em segurança
- “Owned” ou “defaced”, “cracked”





# Defacement

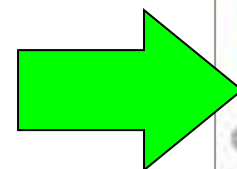
- Página do SBT pichada pelo hacker “Lady\_Lara” em 17/set/2007
- Protesto contra a corrupção





# Defacement

- O site da Câmara dos Deputados foi atacado em 28/jun/2007
- Todos os título das matérias trocados pela mensagem “hacked by hipermachine greetz: Skywalker”
- Auto-promoção



# Sniffing (captura de pacotes)

The screenshot displays the Wireshark interface with a packet capture of an FTP session. A red box highlights the first packet (No. 1) and its details, which show a successful login for the 'anonymous' user with the password 'denio@cin.ufpe.br'.

No.	Time	Source
1	0.00	192.168.0.2
2	0.00	192.168.0.2
3	0.00	192.168.0.2
4	0.00	192.168.0.2
5	0.01	192.168.0.2
6	0.01	192.168.0.2
7	0.01	192.168.0.2
8	0.03	192.168.0.2
9	0.03	192.168.0.2
10	0.17	192.168.0.2

Details of Frame 1 (62 on wire, 62 captured):

- Ethernet II
- Internet Protocol, Src Address: 192.168.0.2, Destination Address: 192.168.0.1
- Transmission Control Protocol, Source port: 1067, Destination port: 80

Raw data (hex):

```

0000  00 00 21 79 99 48 00
0010  00 30 0f ad 40 00 80
0020  00 01 04 2b 00 50 2a
0030  40 00 c8 a6 00 00 02
  
```

Filter: tcp.port == 80 and ip.addr == 192.168.0.1

Entire conversation (1186 bytes)

# Phishing

Browser tabs: (41) WhatsApp, Your Order No #4908 Has Arrived..., Autenticação, Backlog ICDv5 Fase 2 - Plan, Testes ICD - Permissões de C...

Address bar: mail.google.com/mail/u/0/#inbox/FMfcgXWJWXcXWwZmtcLhNsBIIQdPTtIW

Gmail interface:


- Compose
- Inbox (9,879)
- Snoozed
- Important
- Sent
- Drafts (196)
- Spam (116)
- Categories
- Social (5,624)
- Updates (17,325)
- Meet
  - Start a meeting
  - Join a meeting
- Chat
  - Denio
  - Giuliano Maia (13:30h)
  - Alexander de Almeida Pinto (You were in a video call)
  - Victor Andrade (Valeu Denio!)
  - Cheylla Interaminense (You: nao obrigado)
  - Alexander, Fidélis (You were in a video call)
  - Ciro Mendes (You were in a video call)
  - Cicero Silva (You: depois escolhemos os mais vol)
  - Lucas Aversari (You were in a video call)
  - christiano c

Selected email: Your Order No #4908 Has Arrived...deniomariz !

From: Amazon-Logistics <from.LrroBBJTWkCvZovPWljdjpiWiNsSirhMGInjZLWMuuT@akwardflop.com> to me

6:39 PM (22 minutes ago)

amazon 2019 Shopping Survey



**Congratulations! You have been selected to get an exclusive reward up to \$100**

To qualify for this special offer, simply complete our [30-second marketing survey](#) about your experiences with Amazon and choose your reward.

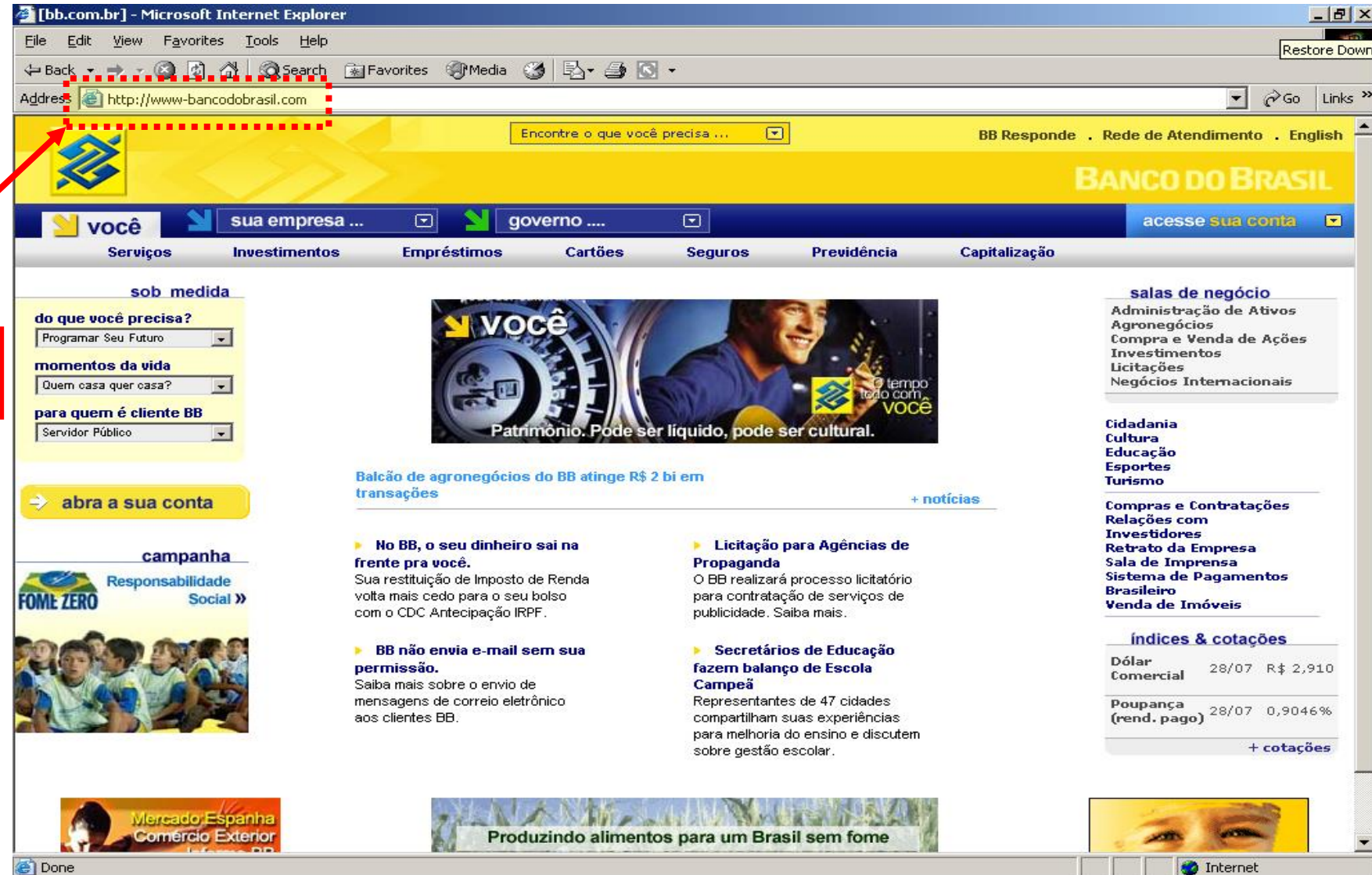
**Take the Survey**

Link in chat: [adjbw.malimosac.com/t?encv=2&v=WGfH52pHm2VnBGRm5VMUNaUU5XRVNqNnR5MndLVUxGNExPQUU0K1hNeGFDNk9DL3ZYEHYSzFEMXIZb2pML290VVewcWFpY1RoUGhQOHZpWXMxUFNsQWk3bGZDWVpPMGUzZlp4Q2ltVXVzSE...](https://adjbw.malimosac.com/t?encv=2&v=WGfH52pHm2VnBGRm5VMUNaUU5XRVNqNnR5MndLVUxGNExPQUU0K1hNeGFDNk9DL3ZYEHYSzFEMXIZb2pML290VVewcWFpY1RoUGhQOHZpWXMxUFNsQWk3bGZDWVpPMGUzZlp4Q2ltVXVzSE...)



# Phishing

URL falsa



# Ameaças à Segurança da Informação

# Ameaças

→ Existem ameaças à segurança da informação sob vários aspectos

- Software
- Rede
- Humano
- Riscos naturais

# Ameaças

## → Software (Aplicações, SO)

- Negação de serviço (Denial of Service - DoS)
- Negação de serviço distribuído (DDoS)
- Backdoors, trojans, worms, vírus
- Código móvel malicioso (ActiveX, JavaScript, Flash, ...)
- Gerenciamento de chaves
- Falta de Atualização de sistemas (Patching)
- Buffer overflow

# Ameaças

## → Rede

- Protocolos (concepção, configuração, implementação)
- Riscos em várias camadas
- Informações não criptografadas (senhas planas)
- “Man-in-the-middle”
- Firewalls mal configurados



# Ameaças

## → Humano (pessoas, processos)

- Senhas fracas
- Engenharia social
- Negligência e/ou Despreparo de usuários ou de equipe técnica de TI para segurança
- Excesso de privilégios
- Segurança física: vandalismo, roubo, furto
- Falta de políticas

# Ameaças

## → Fatores naturais

- Incêndio
- Inundação
- Furacões
- Desabamentos
- Explosões
- Raios
- Terremotos

# Segurança em Camadas

