# Segurança em Sistemas

## Aula 1 – Conceitos Básicos

Prof. Filipo Mór
www.filipomor.com

# Agenda

- Apresentação da Disciplina.
- Plano de Curso.
- Introdução a Segurança em TI.

# Apresentação do Professor

- B.Sc. SI – FDBPOA – 2012
- M.Sc. em CC – PUCRS/DALHOUSIE – 2015
- Atuação na área de TI desde 1995.
- Passagem por:

**Contato:**
ProfessorFilipo AT gmail DOT com
www.filipomor.com

# Apresentação da Turma

- Vocês!
  - Nome.
  - Experiência profissional.
  - Expectativa da disciplina.

# Plano da Disciplina

www.filipomor.com ➡ Teaching ➡ Segurança em Sistemas

***To be updated!***

- Cronograma de aulas.
- Datas das avaliações.
- Datas das APSs.

} **10/08/2017**

- Plano de Ensino já atualizado no Portal!

# Plano da Disciplina

- Avaliação:
  - 50%: Provas (P1 + P2)
  - 40%: Trabalhos (T1 + T2 + T3 + T4)
  - 10%: APSs
  - Nota Final =

**((P1*25)+(P2*25)+(T1*5)+(T2*5)+(T3*15)+(T4*15)+(APS*10)) / 100**

- Chamadas:
  - Primeira chamada as 09h30.
  - Segunda chamada as 11h45.
  - Dúvidas, justificativas, reclamações: diretamente com a coordenação do curso.


CAUTION
THIS IS SPARTA

# Introdução aos Conceitos de Segurança em TI

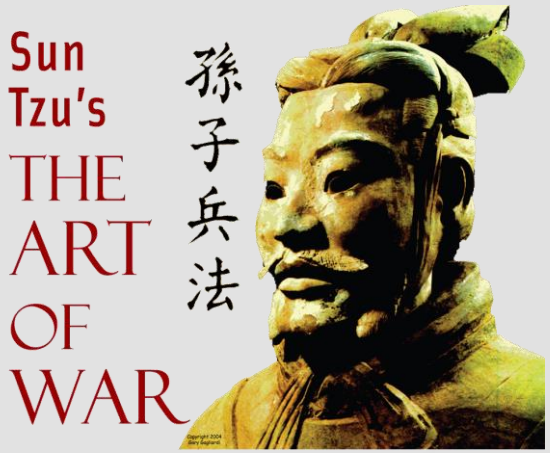
“Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas.

Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota.

Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas...”

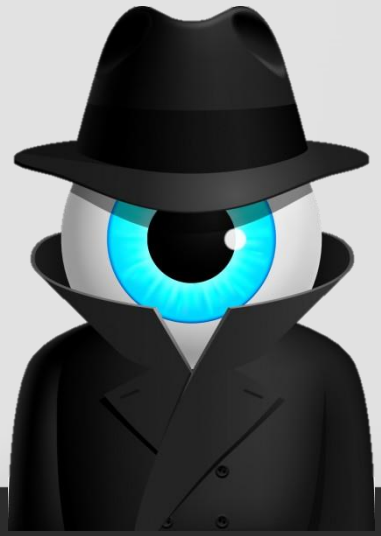
A arte da guerra

*Sun Tzu*



# Introdução aos Conceitos de Segurança em TI

Quando você conecta sua rede doméstica ou corporativa a internet, tudo o que está além da sua rede é literalmente o fim do mundo e o ínicio da *World Wide Web*, onde os hackers estão observando para tirar vantagem dos ingênuos...



# Introdução aos Conceitos de Segurança em TI

Pensamento hacker: primeiro de tudo procurar um alvo.

- Tenho internet, logo meu IP é público e podem me encontrar.
- Tenho tudo instalado e configurado (firewall, roteador, VPN, software antivirus, servidor proxy), mas e o fator humano ?
- Considere por um momento se as pessoas são treinadas em segurança?

# Introdução aos Conceitos de Segurança em TI

Considere por um momento se as pessoas são treinadas em segurança?

Elas saberiam o que fazer se alguém tentasse enganá-los em fornecer informações potencialmente sensíveis ?

Existem quantas cópias das chaves do prédio ?

O que o pessoal da limpeza faz quando não há ninguém lá ?

O seu lixo é descartado adequadamente, ou apenas jogado na lata ?

# Introdução aos Conceitos de Segurança em TI

No quesito segurança, vale ressaltar:

...Existe sempre alguém lá fora mais esperto, mais sábio e melhor equipado que você...

# Introdução aos Conceitos de Segurança em TI

Coletando informações inocentes:

- Também conhecida como Engenharia Social.
- Coletar informações inocentes de uma pessoa via engenharia social é muito mais fácil do que tentar passar pelo firewall.
- Fundamentalmente as pessoas querem confiar nas outras, sendo mais vulneráveis à engenharia social.
- Caso recente: acesso ao admin do Twitter...

# Introdução aos Conceitos de Segurança em TI

## Hacker steals Twitter admin password

Cliff Saran
Friday 01 May 2009 16:42

**Twitter's security was thrown into doubt as details emerged of how a French hacker obtained access to a Twitter staff account, allowing him to view user accounts on the micro-blogging site.**

The hacker, known as "Hacker Croll", claimed that he was able to access Twitter's internal administration system after stealing a password from a member of staff. By resetting the employee's Yahoo password after guessing the "secret question", Hacker Croll claimed he found information about the staffer's Twitter login credentials.


The lapse in security raises questions about how secure Twitter really is. Last month, security researchers at Secure Science developed a proof of concept worm that uses a cross-site scripting flaw on Twitter. And over Easter, a teenage hacker attacked the site four times with a worm.

"If a Twitter employee loses their password, it seems hackers can run riot on the site and cause all sorts of problems. By making staff adopt the kind of hardware authentication keys that many online banking customers now need to use to login online, Twitter would make an attack like this less likely to succeed," said Graham Cluley, senior technology consultant at Sophos.

# Introdução aos Conceitos de Segurança em TI

Alvos de oportunidade:

- Frases muitas vezes repetidas por administradores de empresas em geral:

... Nós somos um <*Negócio fora da TI*> e não há nada em nossa rede que um hacker deseje. Por que deveríamos nos preocupar?...

- Talvez a empresa em questão não seja um banco, mas sua empresa certamente contém: servidores, espaço em disco, largura de banda e informações pessoais de funcionários...

# Introdução aos Conceitos de Segurança em TI

Alvos de oportunidade:

- Considere o que um hacker pode fazer com tal informação:
  - **Servidores**: usado para atacar potencialmente outros computadores.
  - **Espaço em Disco**: usar o espaço em disco disponível, para armazenar qualquer tipo de informação.
  - **Largura de Banda**: uso de largura de banda extra como meio alternativo de conexão.
  - **Informações pessoais dos funcionários**: qualquer tipo de fraude pode ser executada.

# Introdução aos Conceitos de Segurança em TI

Alvos de oportunidade:

- O processo de ataque

1. Reconhecimento e FootPrinting.
2. Rastreamento.
3. Enumeração.
4. Obtenção de Acesso.
5. Escalonamento.
6. Criação de Portas secretas (backdoors) e encobrimento de rastros.

# Introdução aos Conceitos de Segurança em TI

Reconhecimento e Footprinting:

- Preparação inteligente do campo de batalha
- Metas de reconhecimento e pegadas

- Footprinting é a técnica utilizada pelos invasores para levantamento de informações ou perfil do alvo, o footprinting é um dos 03 instrumentos utilizados em um pré-ataque, os outros dois, são: varredura e enumeração.
  Através do footprinting o atacante poderá levantar desde alguns dados pessoais da vítima até perfil de redes.
- Footprint (Pegada)
- Fingerprint (Impressão digital)

# Introdução aos Conceitos de Segurança em TI

## Metas de reconhecimento e pegadas

| Tecnologia | O que é aprendido |
| --- | --- |
| Presença na internet | Idealmente, um alvo deve estar conectado à Internet; o atacante pode querer aprender o seguinte:<br>• Os nomes de domínio e DNS do servidores do alvo<br>• Quais endereços IPs específicos são acessíveis da Internet<br>• Dos IPs acessíveis, quais serviços (www, ftp, e-mail), são alvos viáveis?<br>• Dos serviços encontrados, quais tipos de computadores - tanto hardware como SO, estão sendo executados?<br>• Qual tipo de firewall, Sistema de Detecção de Intrusão está presente?<br>• Onde estão localizados fisicamente dispositivos/sistemas |

# Introdução aos Conceitos de Segurança em TI

## Metas de reconhecimento e pegadas

| Tecnologia | O que é aprendido |
| --- | --- |
| Características da Intranet | • Os engenheiros de rede compreendem que os hackers tentam e obtém acesso à Internet<br>• Como forma de proteção, muitas redes possuem infraestrutura duplicada interna e extrenamente ao firewall<br>• Como resultado, um hacker persistente repete os passos do reconhecimento que construiu para a Internet contra seus alvos na intranet |

# Introdução aos Conceitos de Segurança em TI

- Formas de conseguir informações sobre você (IP)
  - Observação do Sistema de Nomes de Domínio (DNS)
    - Comando: nslookup
  - Consulta ao Whois
    - Whois web interface (http://networksolutions.com)
    - www.who.is
    - Registro.br (http://registro.br)

# Introdução aos Conceitos de Segurança em TI

- Formas de conseguir informações sobre você (IP)
  - Reconhecimento Passivo: simples ‘escuta’ (nslookup)
  - Reconhecimento Ativo: determinar quais serviços estão rodando neste servidor
    - Ping Scan (Ex.: WhatRoute)

# Introdução aos Conceitos de Segurança em TI

Scanning

- Neste ponto o atacante possui informações gerais sobre sua rede:
  - Maquinas da rede
  - Seus Sistemas Operacionais
  - Administradores do Sistema
  - Localização física
  - Quem tem Sistemas de Prevenção contra Intrusos

# Introdução aos Conceitos de Segurança em TI

Enumeração

- Definir o ambiente de rede envolve:
  footprinting, rastreamento e enumeração.

- Footprinting - limita a abrangência do ataque
  - Alvos com maior vulnerabilidade

- Rastreamento - diz ao atacante quais portas estão abertas e quais serviços estão sendo executados

# Introdução aos Conceitos de Segurança em TI

Enumeração

- Enumeração - é a extração de informações de contas válidas e exportação de recursos.

- Três principais categorias dentro de uma rede

  - Recursos de rede e compartilhamentos
  - Usuários e Grupos
  - Aplicativos

# Introdução aos Conceitos de Segurança em TI

Enumeração

- Enumeração no MS Windows
  - net view
  - nbtstat -A (ip)
  - nbtstat -c
- Bloqueio da consulta
  - Portas TCP e UDP 135 até 139
  - Portas TCP e UDP 445

# Introdução aos Conceitos de Segurança em TI

Obtendo Acesso

- Quatro tipos principais de exploração:
  - Ataques a sistemas operacionais
  - Ataques a aplicativos
  - Ataques de desconfiguração (defacement)
  - Ataques de scripts
    - Buffer Overflow
    - Adivinhação de senhas por força bruta
    - Sniffing de senhas
    - Capturar o arquivo de senhas

# Introdução aos Conceitos de Segurança em TI

Cobrindo os rastros

- Depois de obter propriedade no sistema é preciso ocultar este fato do administrador...
  - Para Windows:
    - Limpar as entradas no registro de eventos (event log)
  - Para um sistema UNIX:
    - Limpar o arquivo de histórico
    - Limpar as entradas do UTMP, WTMP e Lastlog

# Introdução aos Conceitos de Segurança em TI

Mantendo o contato

- Criação de backdoors (portas de saída) para acesso futuro.

- Dentre eles estão:

  - Criação de contas
  - Tarefas em background
  - Infectar arquivos de inicialização
  - Permitir serviços de controle remoto/software
  - Substituir aplicativos e serviços legítimos por trojans

# Introdução aos Conceitos de Segurança em TI

Mantendo o contato

- As possíveis ferramentas incluem:
  - Netcat - ler e escrever dados em conexões de redes
  - VNC (Virtual Network Computing) - sistema de exibição/controle remoto
  - Registradores de Teclas (keystroke, loggers)
  - Programas personalizados
    - Windows - (chamada nos arquivos system.ini, win.ini, autoexec.bat, config.sys)
    - Linux - entradas no diretório /etc/rc.d

# Introdução aos Conceitos de Segurança em TI

De onde vêm os ataques ?

- Consulta ao CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
  - Levantamento é considerado levando em conta as seguintes situações:
    - Worm
    - DOS
    - Invasão
    - Web
    - Scan
    - Fraude

# Introdução aos Conceitos de Segurança em TI

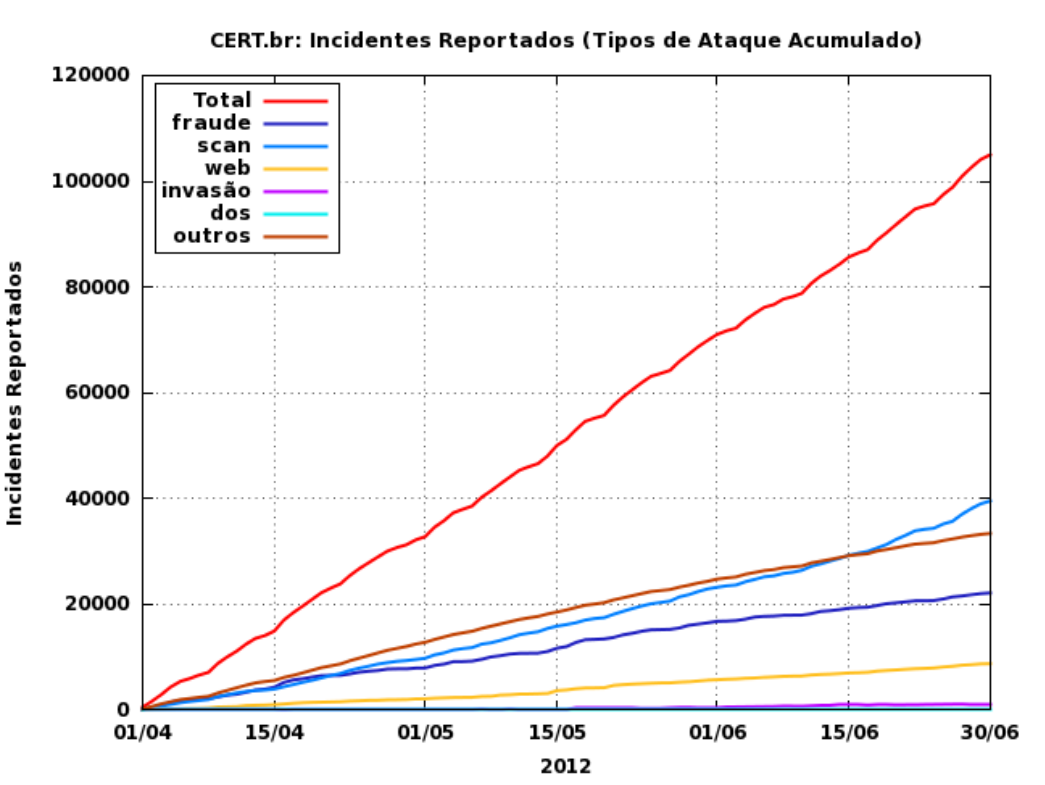
## Incidentes Reportados ao CERT.br - Abril a Junho de 2012

**Tabela:** Totais Mensais e Trimestral Classificados por Tipo de Ataque.

| Mês | Total | worm (%) | | dos (%) | | invasão (%) | | web (%) | | **scan** (%) | | **fraude** (%) | | outros (%) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| abr | **35342** | 3171 | 8 | 9 | 0 | 100 | 0 | 2111 | 5 | 9557 | 27 | 7923 | 22 | 12471 | 35 |
| mai | **40965** | 3242 | 7 | 11 | 0 | 413 | 1 | 3532 | 8 | 13339 | 32 | 8557 | 20 | 11871 | 28 |
| jun | **37806** | 2702 | 7 | 9 | 0 | 619 | 1 | 3124 | 8 | 16646 | 44 | 5653 | 14 | 9053 | 23 |
| Total | **114113** | 9115 | 7 | 29 | 0 | 1132 | 0 | 8767 | 7 | 39542 | 34 | 22133 | 19 | 33395 | 29 |

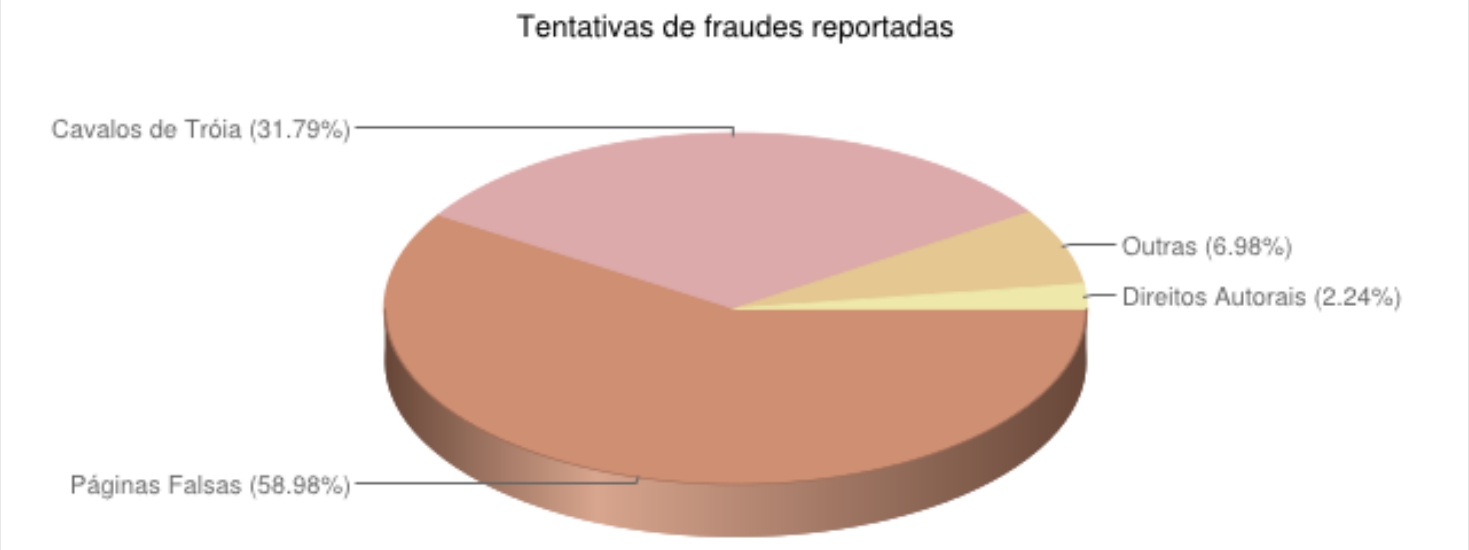
# Introdução aos Conceitos de Segurança em TI

**Incidentes Reportados ao CERT.br - Abril a Junho de 2012**



# Introdução aos Conceitos de Segurança em TI

## Incidentes Reportados ao CERT.br - Abril a Junho de 2012

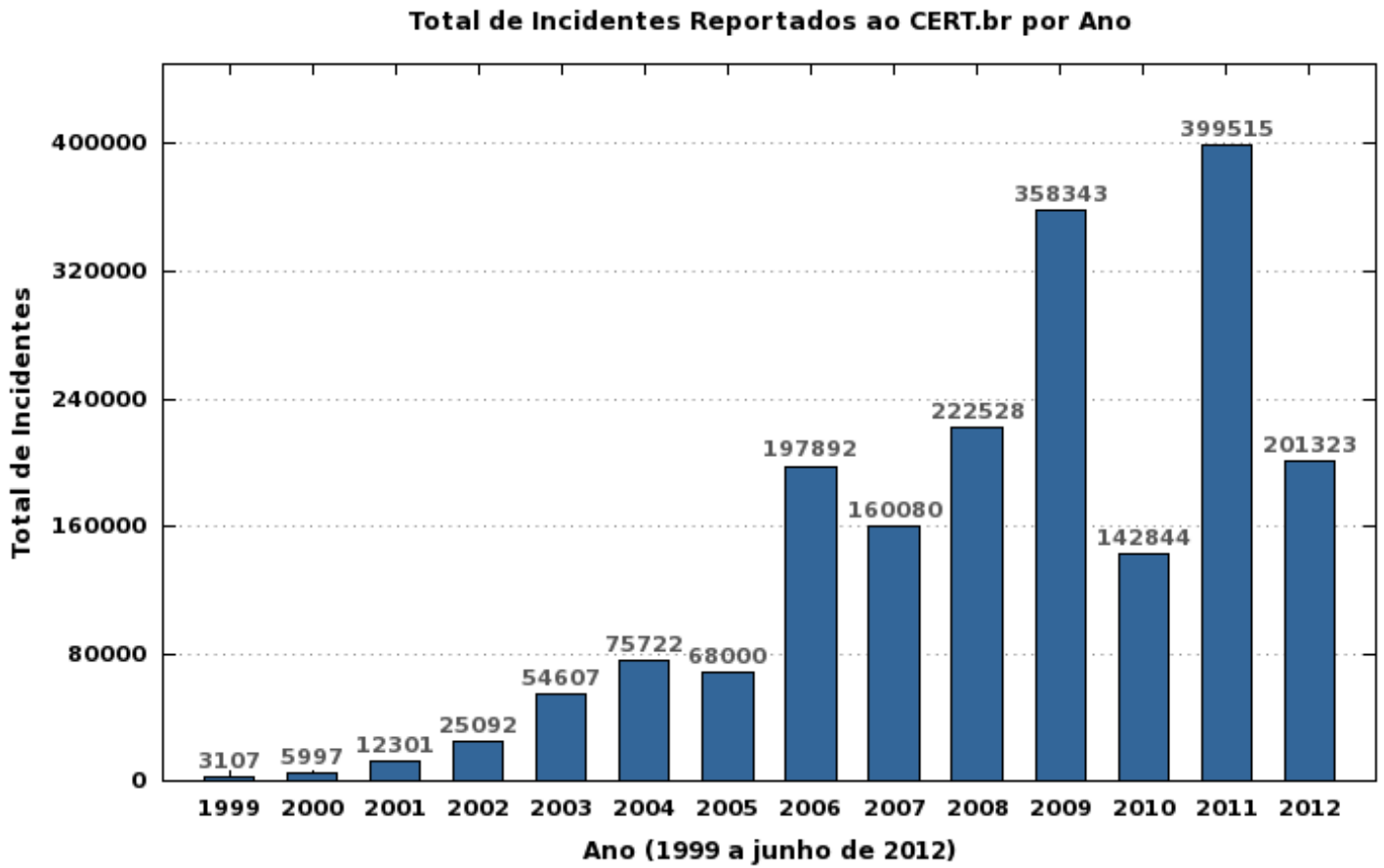



**Legenda:**

**Cavalos de Tróia**: Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.
**Páginas Falsas**: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.
**Direitos Autorais**: Notificações de eventuais violações de direitos autorais.
**Outras**: Outras tentativas de fraude.

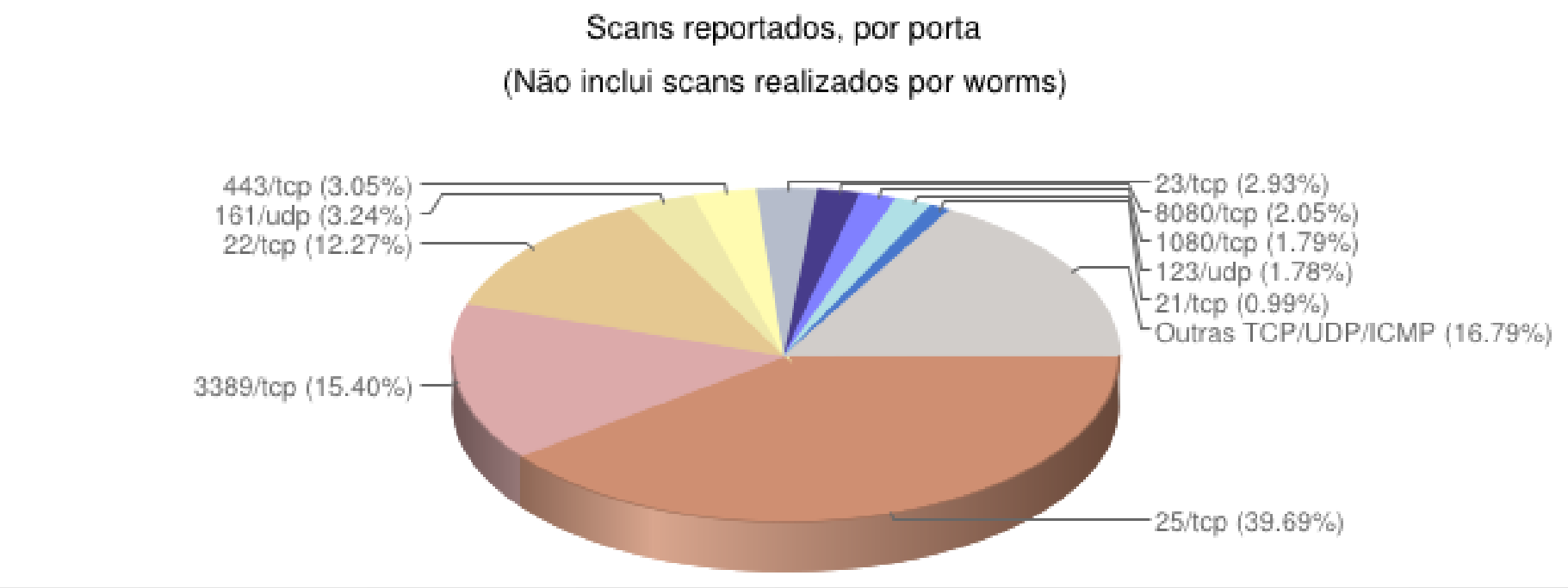
# Introdução aos Conceitos de Segurança em TI

## Incidentes Reportados ao CERT.br - Abril a Junho de 2012



# Introdução aos Conceitos de Segurança em TI

**Incidentes Reportados ao CERT.br - Abril a Junho de 2012**

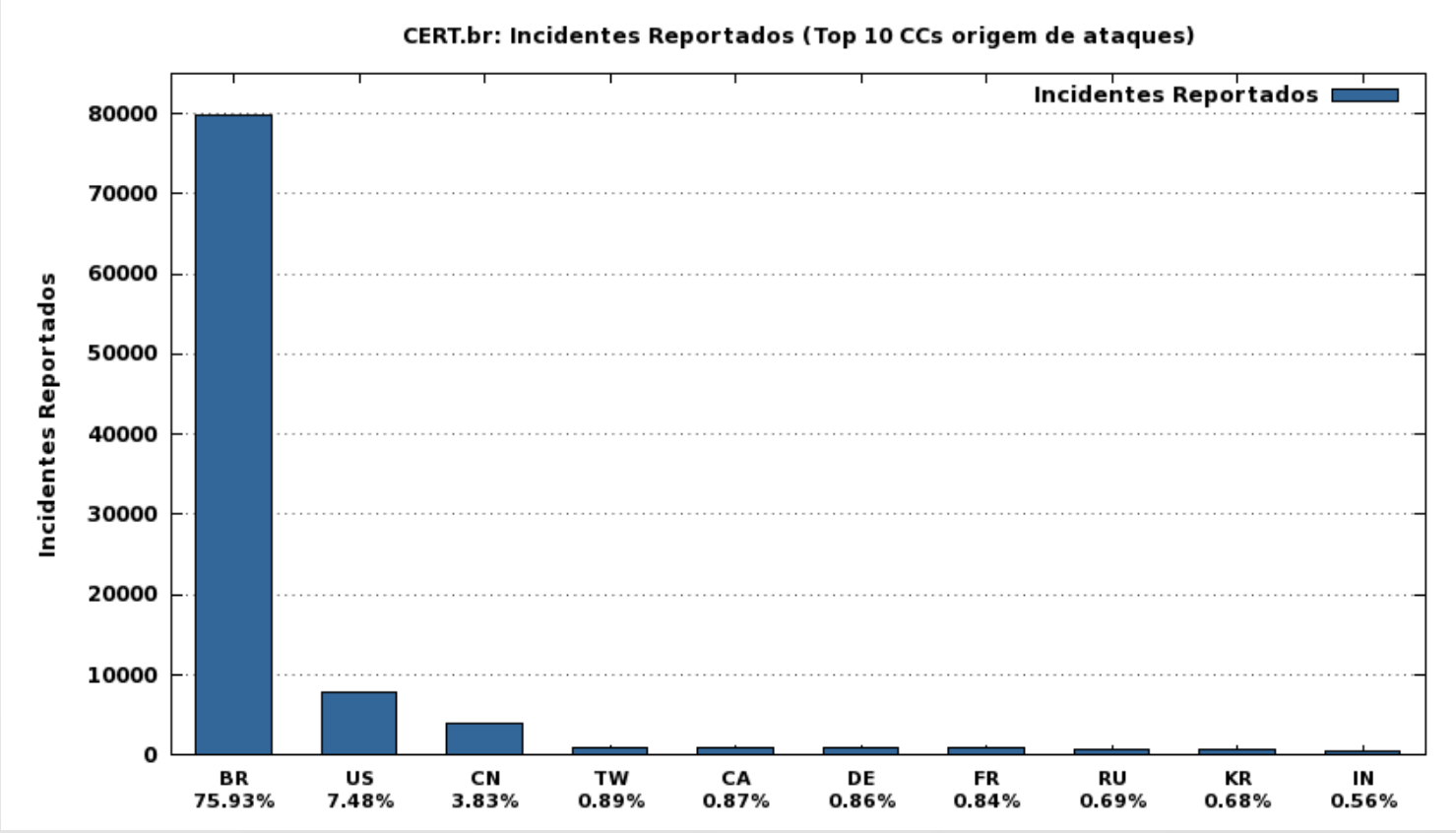


# Introdução aos Conceitos de Segurança em TI

**Incidentes Reportados ao CERT.br - Abril a Junho de 2012**

# Introdução aos Conceitos de Segurança em TI

## Incidentes Reportados ao CERT.br - Abril a Junho de 2012



# Introdução aos Conceitos de Segurança em TI

- Organizações de segurança de Redes
  - Antigamente, fabricantes e vendedores eram responsáveis por rastrear todas as vulnerabilidades de seus produtos...
  - O problema é que diferentes empresas poderiam reportar a mesma vulnerabilidade, causando certa confusão
  - Criação de organizações específicas destinadas a segurança de redes...

# Introdução aos Conceitos de Segurança em TI

- Organizações de segurança de Redes
  - Algumas delas (principais)
    - CVE (www.cve.mitre.org)
    - CERT (www.cert.org)
    - SANS (www.sans.org)
    - CIS (www.cisecurity.com)
    - SCORE (www.sans.org/score/)
    - ISC (www.isc.sans.org)
    - ICAT Metabase (www.icat.nist.gov/icat.cfm)
    - Security Focus (www.security-focus.com)
    - CAIS (www.rnp.br/cais)

# Introdução aos Conceitos de Segurança em TI

- Organizações de segurança de Redes
  - Algumas delas (principais)
    - CVE (www.cve.mitre.org)
      - Lista de nomes padronizados para vulnerabilidades e outras informações de exposição de segurança
      - Variedade de artigos, grupos de e-mail, fóruns, discussão, alertas e melhores práticas de segurança

# Introdução aos Conceitos de Segurança em TI

- Organizações de segurança de Redes
  - Algumas delas (principais)
    - SANS (www.sans.org)
      - Define-se como um confiável líder em pesquisa de segurança da informação, certificação e educação
      - Compartilhamento de conhecimentos entre mais de 156000 profissionais de segurança em TI

# Introdução aos Conceitos de Segurança em TI

- Organizações de segurança de Redes
  - Algumas delas (principais)
    - SANS (www.sans.org)
      - Define-se como um confiável líder em pesquisa de segurança da informação, certificação e educação
      - Compartilhamento de conhecimentos entre mais de 156000 profissionais de segurança em TI

# Introdução aos Conceitos de Segurança em TI

- Organizações de segurança de Redes
  - Algumas delas (principais)
    - SCORE (www.sans.org/score/)
      - Tem o objetivo de promover, desenvolver e publicar verificações (checklists) de segurança

# Introdução aos Conceitos de Segurança em TI

- Organizações de segurança de Redes
  - Algumas delas (principais)
    - ISC (www.isc.sans.org)
      - Define-se como um centro que pega mais de 3.000.000 de entradas de registro de detecção de invasão a cada dia.

# Introdução aos Conceitos de Segurança em TI

- Organizações de segurança de Redes
  - Algumas delas (principais)
    - Security Focus (www.security-focus.com)
      - Possui cerca de 2.5 milhões de usuários anualmente e é a maior comunidade de profissionais de segurança disponível.

# Introdução aos Conceitos de Segurança em TI

- Organizações de segurança de Redes
  - Algumas delas (principais)
    - CAIS (www.rnp.br/cais)

# Introdução aos Conceitos de Segurança em TI

"A arte da guerra nos ensina a contar não com a probabilidade de o inimigo não chegar, mas com nossa própria prontidão para recebê-lo; não com a chance de não ser atacado, mas com o fato de tornar nossa posição inatacável.”

A arte da guerra
*Sun Tzu.*

# Dúvidas e Comentários?

***Agradecimentos:***
Prof. Marcelo Conterato
Prof. Samuel Souza
Prof. Roberto Franciscatto

# Segurança em Sistemas

**Faculdade SENAC de Porto Alegre**
Prof. Filipo Mór
www.filipomor.com

2017/II