Capítulo 3 – Panorama Atual na Área de Segurança

- ✔ 3.1 – Introdução
- ✔ 3.2 – Ameaças recentes
  - 3.2.1 – Vírus
  - 3.2.2 – Worms
  - 3.2.3 – Vulnerabilidades
- ✔ 3.3 – Estatísticas
  - 3.3.1 – CERT
  - 3.3.2 – CAIS
- ✔ 3.4 – Perfil dos atacantes
  - 3.4.1 – Hackers e Crackers
  - 3.4.2 – Script Kiddies
  - 3.4.3 - Motivação

3.1 – Introdução

- Instalar um SO numa máquina conectada diretamente à Internet pode levar a um comprometimento em poucos minutos
  - tempo insuficiente até para baixar as últimas atualizações do sistema instalado
- Panorama atual da rede:
  - lugar público
  - cheio de informações valiosas
  - cheio de vândalos, *hackers*, *crackers*, vírus, *worms* e outras ameaças

3.2 – Ameaças recentes

3.2.1 – Vírus

- ✔ Primeiro vírus conhecido: ping-pong
- ✔ Hoje, existem aproximadamente 100 mil vírus catalogados
- ✔ Os primeiros vírus eram transmitidos por disquetes e somente arquivos executáveis podiam ser infectados
- ✔ Hoje, a maior forma de contágio é o e-mail
- ✔ Hoje, vários tipos de arquivos podem ser contaminados:
  - e.g.: .com, .exe, .doc, .xls, .bat, .cpl, .htr, .js, .scr, etc.

- Apesar de existirem vírus para outros SO's (Linux, MacOS, PalmOS), essa quantidade é infinitamente menor, se comparado ao Windows
- Por que o Windows tem, proporcionalmente ao número de usuários, muito mais vírus que outros SO's ?
- Antivírus são programas capazes de detectar e remover os vírus de uma estação
  - podem ter recursos avançados como verificação de vírus em e-mail, e também verificação de vírus em arquivos em tempo real quando estão sendo acessados pelo SO
- Antivírus utiliza assinaturas de vírus para detectar arquivos infectados
  - Assinaturas de vírus: conjunto de informações que identificam unicamente um determinado vírus
  - As assinaturas devem ser frequentemente atualizadas

- Para tomar conhecimento de novos vírus e como eles funcionam basta visitar as páginas dos principais fabricantes de antivírus
  - Symantec: http://www.symantec.com/avcenter
  - McAfee: http://br.mcafee.com/virusInfo/default.asp
  - Trend Micro: http://www.trendmicro.com/vinfo/virusencyclo/
  - F-Secure: http://www.f-secure.com/v-descs/
- Computador com antivírus desatualizado há mais de uma semana é considerado altamente vulnerável
- Nem sempre a atualização das assinaturas é feita a tempo de conter a contaminação
- Em questão de horas um vírus pode ter se espalhado para outros continentes

3.2.2 – Worms

- Parecidos com vírus
- Principal diferença: um *worm* tenta infectar uma máquina enquanto o vírus tenta infectar um arquivo
- Ao infectar uma máquina, o passo seguinte do *worm* é procurar (ou sortear) endereços de rede para tentar infectar outras máquinas na rede
- Utiliza-se de vulnerabilidades conhecidas, e-mail, permissões de acesso, compartilhamentos, etc.
- Muitos *worms* utilizam múltiplas formas de replicação
  - O *Worm Code Red*, em 2001, em apenas 14 horas, infectou cerca de 360.000 computadores
- Prevenção de *worms* se faz através de atualizações frequentes do SO
- Na grande maioria dos casos, os *worms* exploram vulnerabilidades já conhecidas, com atualizações já disponíveis nos sites dos fabricantes

3.2.3 – Vulnerabilidades

- São falhas presentes em um programa, protocolo ou SO
  - Normalmente causadas por erros de especificação ou erros de programação
  - Solução “simples”: fabricante lança uma correção, chamada de *patch*
  - Quando existem muitas correções, o fabricante as agrupa num *service pack*
- O usuário deve fazer o download dessas correções
  - Muitas vezes o fabricante disponibiliza formas automáticas de aplicar correções
    - e.g.: Windows Update da Microsoft, SUSE Updater da Novell, apt do Debian

- Falhas de especificação são mais difíceis de se solucionar
  - especificação de protocolo ou produto deve ser revista
  - as alterações devem preservar a compatibilidade com sistemas que ainda não foram atualizados
  - problemas como o *syn flood* e ataques *smurf*, que são vulnerabilidades no próprio protocolo TCP/IP, até hoje não têm uma solução perfeita
- Listas de discussão fornecem informações sobre vulnerabilidades, além de sites de fabricantes
  - http://www.microsoft.com/security/bulletins/default.mspx
  - http://www.debian.org/security/
- Descobertas de vulnerabilidades, geralmente vêm acompanhadas de uma “prova por conceito”: programas capazes de explorara aquela vulnerabilidade
  - ***exploits***: programas criados para explorar determinada vulnerabilidade em um sistema. Tem como objetivo inicial provar que uma determinada vulnerabilidade é perigosa

3.3 – Estatísticas

- Estatísticas sobre o número de vulnerabilidades e o número de incidentes reportados a cada ano
  - Importantes para acompanhamento da evolução das vulnerabilidades e incidentes de segurança

3.3.1 – CERT

- Estatísticas sobre:
  - incidentes
  - vulnerabilidades
  - alertas de segurança publicados
  - notas de segurança publicadas
  - mensagens de correiro eletrônico atendidas
  - chamadas telefônicas recebidas

Meet CERT
Employment Opportunities

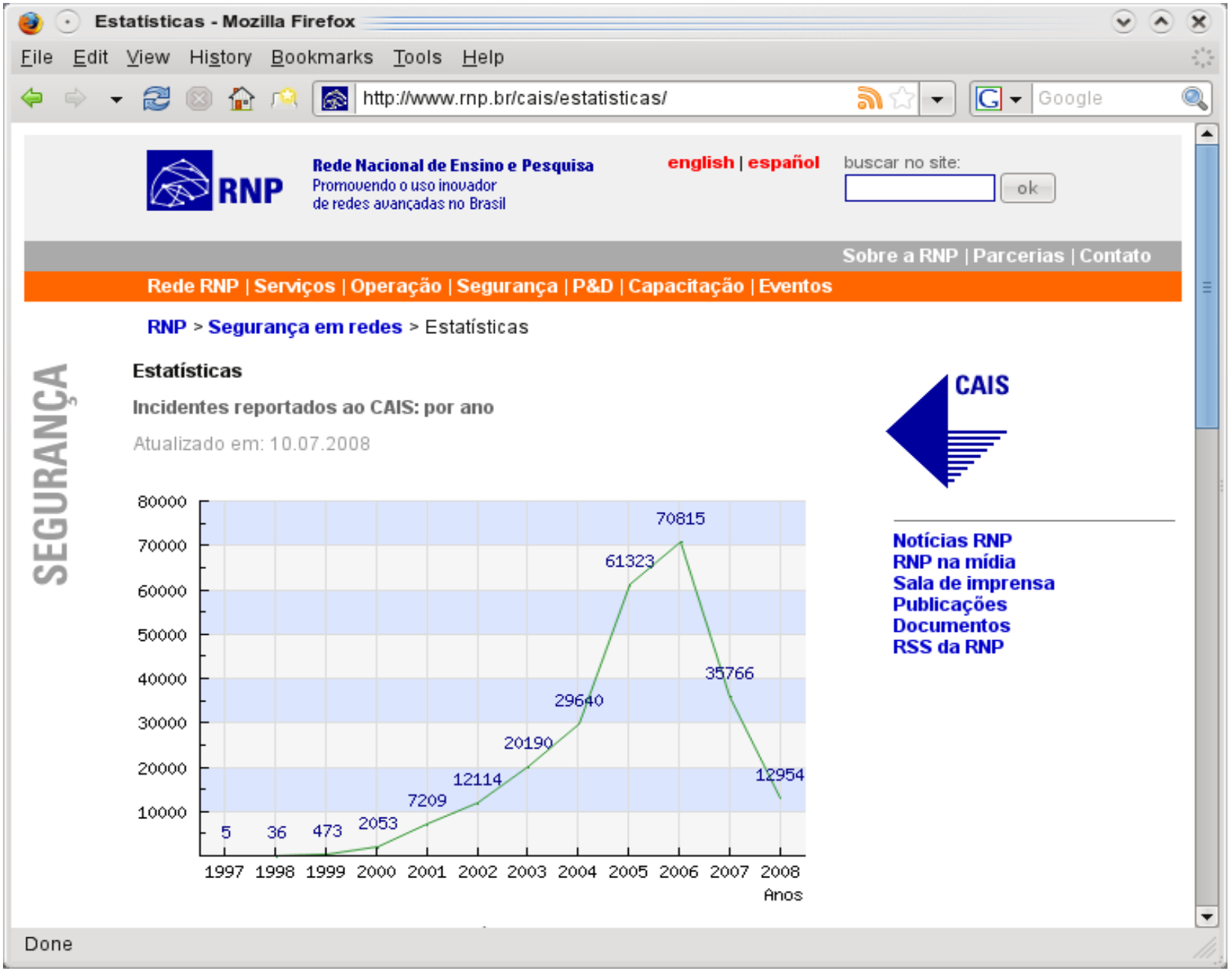
Vulnerability Remediation Statistics

Vulnerability remediation is one of the primary areas of work at the CERT® Coordination Center (CERT/CC). The CERT/CC strives to both reduce the number of vulnerabilities introduced into software and reduce the risk posed by existing vulnerabilities. Our standard remediation process includes collecting reports of vulnerabilities, performing technical analysis, coordinating with affected vendors, and establishing a reasonable timeframe for disclosing information about the vulnerability.

Cataloged vulnerabilities

Year	Total vulnerabilities cataloged	From direct reports
Q1-Q2, 2008	4,110	196
2007	7,236	357
2006	8,064	345
2005	5,990	213
2004	3,780	170
2003	3,784	191
2002	4,129	343
2001	2,437	153
2000	1,090	-
1999	417	-
1998	262	-
1997	311	-
1996	345	-
1995	171	-
Totals	**42,126**	

3.3.2 – CAIS


Estatísticas - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.rnp.br/cais/estatisticas/
Google
RNP
Rede Nacional de Ensino e Pesquisa
Promovendo o uso inovador
de redes avançadas no Brasil
english | español
buscar no site:
ok
Sobre a RNP | Parcerias | Contato
Rede RNP | Serviços | Operação | Segurança | P&D | Capacitação | Eventos
RNP > Segurança em redes > Estatísticas
SEGURANÇA
Estatísticas
Incidentes reportados ao CAIS: por ano
Atualizado em: 10.07.2008
80000
70000
60000
50000
40000
30000
20000
10000
5
36
473
2053
7209
12114
20190
29640
61323
70815
35766
12954
1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008
Anos
CAIS
Notícias RNP
RNP na mídia
Sala de imprensa
Publicações
Documentos
RSS da RNP
Done

3.4 – Perfil dos atacantes

- ✔ Quem são as pessoas que produzem os ataques?
- ✔ O que elas pensam?
- ✔ Quais são as suas motivações?
- ✔ Por que fazem esse tipo de coisa?

3.4.1 – Hackers

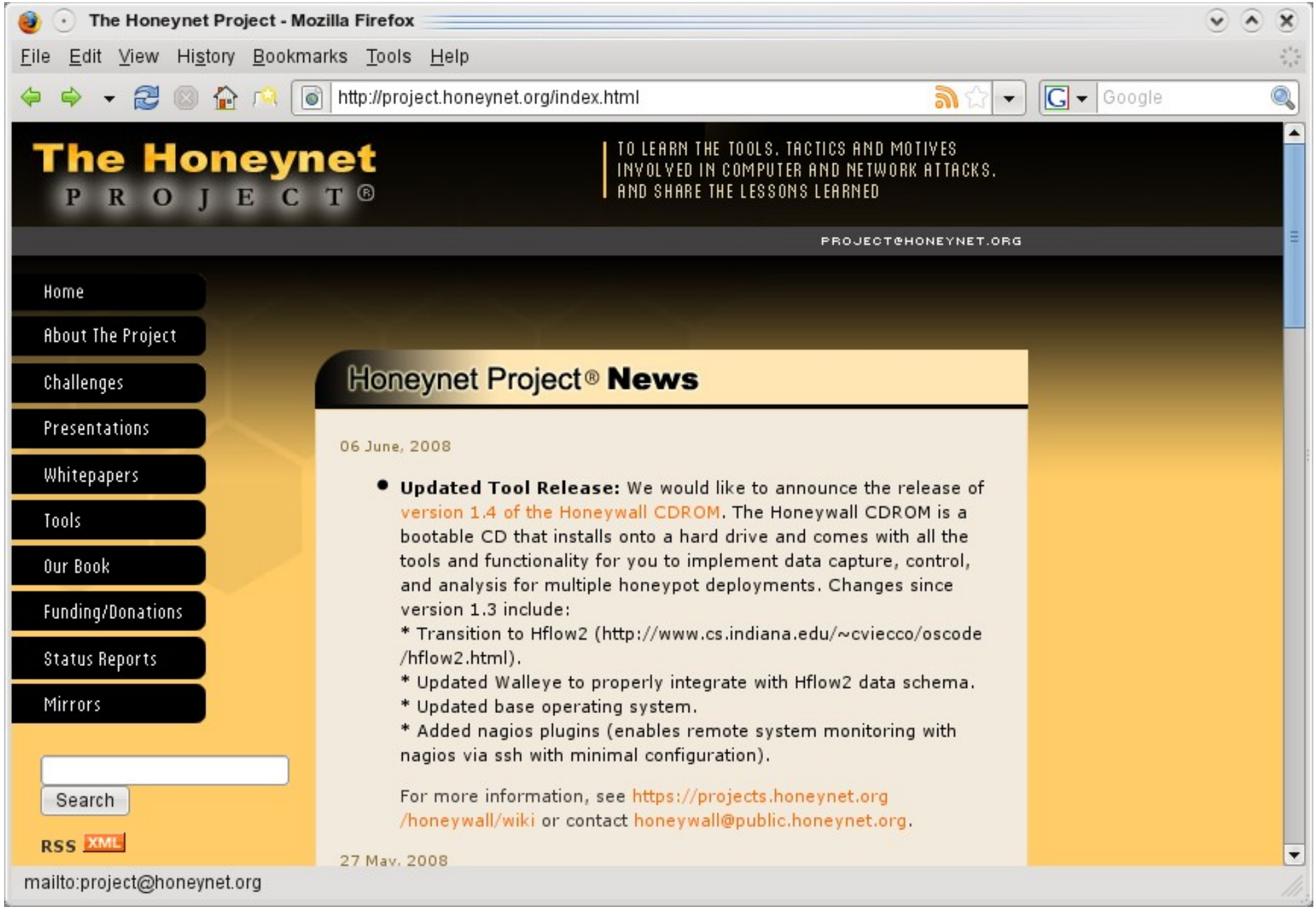
- O termo *hacker* foi por muito tempo associado a pessoas mal-intencionadas
- *Hacker* é uma pessoa que detém muitos conhecimentos sobre a área de computação
  - sistemas operacionais
  - software
  - programação
  - segurança
  - redes
  - Intenet
- Tem interesse em descobrir coisas novas (inclusive vulnerabilidades)
- Não possui motivação destrutiva

3.4.2 – Crackers

- *Cracker* é um *hacker* com propósitos maldosos de invadir e violar a integridade dos sistemas

3.4.3 – Script kiddies

- Pessoas que possuem pouco conhecimento em informática e têm aspirações a *hacker/cracker*
- Utilizam os *exploits* criados por terceiros (*hackers*) para invadir sistemas vulneráveis
- Têm pouca idade
- Não estão interessados em algo específico, simplesmente querem invadir um site qualquer
- São responsáveis por boa parte dos ataques na Internet, e provavelmente serão os responsáveis caso o seu site seja atacado
- http://project.honeynet.org/papers/


The Honeynet Project - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://project.honeynet.org/index.html
Google
The Honeynet PROJECT®
TO LEARN THE TOOLS, TACTICS AND MOTIVES INVOLVED IN COMPUTER AND NETWORK ATTACKS, AND SHARE THE LESSONS LEARNED
PROJECT@HONEYNET.ORG
Home
About The Project
Challenges
Presentations
Whitepapers
Tools
Our Book
Funding/Donations
Status Reports
Mirrors
Search
RSS XML
Honeynet Project® News
06 June, 2008
Updated Tool Release: We would like to announce the release of version 1.4 of the Honeywall CDROM. The Honeywall CDROM is a bootable CD that installs onto a hard drive and comes with all the tools and functionality for you to implement data capture, control, and analysis for multiple honeypot deployments. Changes since version 1.3 include:
* Transition to Hflow2 (http://www.cs.indiana.edu/~cviecco/oscode/hflow2.html).
* Updated Walleye to properly integrate with Hflow2 data schema.
* Updated base operating system.
* Added nagios plugins (enables remote system monitoring with nagios via ssh with minimal configuration).
For more information, see https://projects.honeynet.org/honeywall/wiki or contact honeywall@public.honeynet.org.
27 May, 2008
mailto:project@honeynet.org

3.4.4 – Motivação

- O que leva uma pessoa a invadir um sistema?
  - impunidade, delinquência, tentativa de chamar a atenção, notoriedade, para mostrar que pode, para mostrar aos amigos, e muitas outras
    - http://project.honeynet.org/book/Chp16.pdf
- Geralmente, um invasor não quer invadir a sua rede especificamente, mas uma rede qualquer que seja fácil de invadir
- Seguindo o princípio do ponto mais fraco, torne a sua rede forte o suficiente para o atacante tentar atacar outra rede e não a nossa
- Em alguns casos, o atacante pode ter muitos conhecimento em informática e interesses específicos

- ✔ Kevin Mitnick e Tsutomu Shimomura
  - *Hacker* (ou *cracker*?) mais famoso do mundo
  - Sua história virou livros e filme
  - Hoje Mitnick trabalha numa empresa de segurança
  - Livros:
    - “Mitnick, A Arte de Enganar”, escrito pelo próprio Mitnick
    - “O Pirata Eletrônico e o Samurai”
    - “Takedown”, escrito por Shimomura
  - Filme:
    - “Takedown, A Caçada Virtual”
  - Links:
    - http://www.takedown.com/
    - http://www.freedomdowntime.com
    - http://pt.wikipedia.org/wiki/Kevin_Mitnick

3.5 – Atividades

1. Atualizar o Windows nos computadores da sua bancada, através da atualização manual. Você habilitaria a atualização automática? Por quê? Que perigos um site de atualizações automáticas pode trazer?