Fundamentos de Segurança para Redes e Computadores

Adriano Mauro Cansian
Professor Assistente Doutor

Maio – 2003

Contato:

Adriano Mauro Cansian
Professor Assistente Doutor

adriano@acmesecurity.org / adriano@unesp.br

UNESP - Universidade Estadual Paulista
Campus de São José do Rio Preto

Depto. de Ciência da Computação e Estatística
Laboratório ACME! de Pesquisa em Segurança de Computadores e Redes

Endereço:
R. Cristóvão Colombo, 2265 - Jd. Nazareth
15055-000 * São José do Rio Preto, SP.
Tel. (17) 221-2475 (laboratório) / 221-2201 (secretaria)
http://www.acmesecurity.org/~adriano

Chave PGP:

Adriano Mauro Cansian <adriano@unesp.br>
Key ID: **0x3893CD2B**
Key Type: DH/DSS
Key Fingerprint: **C499 85ED 355E 774E 1709 524A B834 B139 3893 CD2B**

Prefácio

Este material é uma coleção dos *slides* do mini-curso **"Fundamentos de Segurança para Redes e Computadores",** ministrado a convite da comissão organizadora do II Encontro de Evangelização e Informática, promovido pela CNBB – Confederação Nacional dos Bispos do Brasil (Regional Sul 1) realizado na Faculdade e Colégio Claretianos, na cidade de Rio Claro - SP, de 16 a 18 de maio de 2003.

A principal função destes *slides* e notas de aula é facilitar a realização das anotações dos tópicos mais importantes discutidos durante a apresentação. Sugestões e apontamentos de falhas podem ser enviadas diretamente ao autor, em adriano@acmesecurity.org. A versão revisada destas notas de aula, e outros eventuais materiais complementares, estão disponíveis em **http://www.acmesecurity.org/cnbb2003**

São José do Rio Preto, 06 de maio de 2003.
Adriano Mauro Cansian

ACME! STANDARD DISCLAIMER

Please, read carefully.

This ACME! product is meant for educational purposes only. Any resemblance to real persons, living or dead is purely coincidental. Void where prohibited. Some assembly required. List each check separately by bank number. Batteries not included. Contents may settle during shipment. Use only as directed. No other warranty expressed or implied. Do not use ACME! while operating a motor vehicle or heavy equipment. Postage will be paid by addressee. Subject to CAB approval. This is not an offer to sell securities. Apply only to affected area. ACME! may be too intense for some viewers. Do not stamp. Use other side for additional listings. For recreational use only. Do not disturb. All models over 18 years of age. If condition persists, consult your physician. No user-serviceable parts inside. Freshest if eaten before date on carton. Subject to change without notice. Times approximate. Simulated picture. No postage necessary if mailed in the United States. Breaking seal constitutes acceptance of agreement. For off-road use only. As seen on TV. One size fits all. Many suitcases look alike. Contains a substantial amount of non-tobacco ingredients. Colors may, in time, fade. We have sent the forms which seem right for you. Slippery when wet. For office use only. ACME! Research is not affiliated with the American Red Cross. Drop in any mailbox. Edited for television. Keep cool. process promptly. Post office will not deliver without postage. List was current at time of printing. Return to sender, no forwarding order on file, unable to forward. ACME! is not responsible for direct, indirect, incidental or consequential damages resulting from any defect, error or failure to perform. At participating locations only. Not the Beatles. Penalty for private use. See label for sequence. Substantial penalty for early withdrawal. Do not write below this line. Falling rock. Lost ticket pays maximum rate. Your canceled check is your receipt. Add toner. Place stamp here. Avoid contact with skin. Sanitized for your protection. Be sure each item is properly endorsed. Sign here without admitting guilt. Slightly higher west of the Mississippi. Employees and their families are not eligible. Beware of dog. Contestants have been briefed on some questions before the show. Limited time offer, call now to ensure prompt delivery. You must be present to win. No passes accepted for this engagement. No purchase ecessary. Processed at location stamped in code at top of carton. Shading within a garment may occur. Use only in a well-ventilated are. Keep ACME! away from fire or flames. Replace with same type. Approved for veterans. Booths for two or more. Check here if tax deductible. Some equipment shown is optional. Price does not include taxes. No Canadian coins. Not recommended for children. Prerecorded for this time zone. Reproduction strictly prohibited. No solicitors. No alcohol, dogs or horses. No anchovies unless otherwise specified. Restaurant package, not for resale. List at least two alternate dates. First pull up, then pull down. Call ACME! toll free before digging. Driver does not carry cash. Some of the trademarks mentioned in this product appear for identification purposes only. Record additional transactions on back of previous stub. Unix is a registered trademark of AT&T. Do not fold, spindle or mutilate. No transfers issued until the bus comes to a complete stop. Package sold by weight, not volume. Your mileage may vary. This article does not reflect the thoughts or opinions of either myself, my company, my friends, or my cat. Don't quote me on that. Don't quote me on anything. All rights reserved. You may distribute this article freely but you may not take a profit from it. Terms are subject to change without notice. Illustrations are slightly enlarged to show detail. Any resemblance to actual persons, living or dead, is unintentional and purely coincidental. Do not remove this disclaimer under penalty of law. Hand wash only, tumble dry on low heat. Do not bend, fold, mutilate, or spindle. No substitutions allowed. For a limited time only. This ACME! article is void where prohibited, taxed, or otherwise restricted. Caveat emptor. Article is provided "as is" without any warranties. Reader assumes full responsibility. An equal opportunity article. No shoes, no shirt, no articles. Quantities are limited while supplies last. If any defects are discovered, do not attempt to read them yourself, but return to an authorized service center. Read at your own risk. Parental advisory - explicit lyrics. Text may contain explicit materials some readers may find objectionable, parental guidance is advised. Keep away from sunlight. Keep away from pets and small children. Limit one-per-family please. No money down. No purchase necessary. You need not be present to win. Some assembly required. Batteries not included. Instructions are included. Action figures sold separately. No preservatives added. Slippery when wet. Safety goggles may be required during use. Sealed for your protection, do not read if safety seal is broken. Call before you dig. Not liable for damages arising from use or misuse. For external use only. If rash, irritation, redness, or swelling develops, discontinue reading. Read only with proper ventilation. Avoid extreme temperatures and store in a cool dry place. Keep away from open flames. Avoid contact with eyes and skin and avoid inhaling fumes. Do not puncture, incinerate, or store above 120 degrees Fahrenheit. Do not place near a flammable or magnetic source. Smoking this article could be hazardous to your health. The best safeguard, second only to abstinence, is the use of a condom. No salt, MSG, artificial color or flavoring added. If ingested, do not induce vomiting, and if symptoms persist,consult a physician. Warning: Pregnant women, the elderly, and children should avoid prolonged exposure to ACME! Caution: ACME! may suddenly accelerate to dangerous speeds. ACME! contains a liquid core, which if exposed due to rupture should not be touched, inhaled, or looked at. Do not use ACME! on concrete. Discontinute use of ACME! if any of the following occurs: Itching, Vertigo, Dizziness, Tingling in extremities, Loss of balance or coordination, Slurred speech, Temporary blindness, Profuse Sweating, or Heart palpitations. If ACME! begins to smoke, get away immediately. Seek shelter and cover head. ACME! may stick to certain types of skin. When not in use, ACME! should be returned to its special container and kept under refrigeration. Failure to do so relieves the makers of ACME! , ACME! Products Incorporated, and it's parent company, ACME! Chemical Unlimited, of any and all liability. Ingredients of ACME! include an unknown glowing substance which fell to Earth, presumably from outer space. ACME! has been shipped to troops in Saudi Arabia and is also being dropped by warplanes on Iraq. Do not taunt ACME! May cause any of the aforementioned effects and/or death. Articles are ribbed for your pleasure. Possible penalties for early withdrawal. Offer valid only at participating sites. Slightly higher west of the Rockies. Allow four to six weeks for delivery. Must be 18 to read. Disclaimer does not cover misuse, accident, lightning, flood, tornado, tsunami, volcanic eruption, earthquake, hurricanes and other Acts of God, neglect, damage from improper reading, incorrect line voltage, improper or unauthorized reading, broken antenna or marred cabinet, missing or altered serial numbers, electromagnetic radiation from nuclear blasts, sonic boom vibrations, customer adjustments that are not covered in this list, and incidents owing to an airplane crash, ship sinking or taking on water, motor vehicle crashing, dropping the item, falling rocks, leaky roof, broken glass, mud slides, forest fire, or projectile (which can include, put not be limited to, arrows, bullets, shot, BB's, shrapnel, lasers, napalm, torpedoes, or emissions of X-rays, Alpha, Beta and Gamma rays, knives, stones, etc.). ***Other restrictions may apply. This supersedes all previous notices. The ACME! Computer Security Research.***

"Nós trabalhamos no escuro. Fazemos o possível para combater o mal, que do contrário nos destruiria. Mas se o caráter de um homem é seu destino, a luta não é uma escolha, mas uma vocação."

Fox Mulder - *Grotesque*

II Encontro de Evangelização e Informática
CNBB - Sul 1

Rio Claro - 2003

Fundamentos de Segurança para Redes e Computadores

Adriano Mauro Cansian
ACME! Computer Security Research
unesp - Campus de São José do Rio Preto
www.acmesecurity.org

Conteúdo

Parte 1 - Conhecendo seu inimigo

- Introdução.
- Por que estamos vulneráveis?
- Quem é o *script kiddie*?
- Porque os ataques têm sucesso.
- A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia

- Algumas precauções úteis.
- Situações reais.
- Observando os bandidos: utilizando os *logs*.
- Congelamento de dados.
- Ferramentas e técnicas úteis.
- Legislação
- Conclusão

 3

Parte 1
Conhecendo seu Inimigo

Introdução

O que este curso **É**:

- Uma análise do problema de intrusão, focalizado no **comportamento** do atacante.
- Destaque para **conhecimento** e experiência.
- Totalmente baseado em software de livre distribuição (***freeware***).
- Ênfase em captura e análise de **informações**.

 6

O que este curso **NÃO** é:

- Propaganda de produtos comerciais.
- Um conjunto de receitas prontas sobre proteção e auditoria.
- Instruções de *hacking*.
- Um julgamento a ações de qualquer tipo.
- A verdade absoluta.

 7

Um panorama atual dos rumos da segurança em computadores e redes.

Onde estamos

Parte 1 - Conhecendo seu inimigo

- Introdução.
- ⇨ Por que estamos vulneráveis?
- Quem é o *script kiddie*?
- Porque os ataques têm sucesso.
- A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia

- Algumas precauções úteis.
- Situações reais.
- Observando os bandidos: utilizando os *logs*.
- Congelamento de dados.
- Ferramentas e técnicas úteis.
- Legislação
- Conclusão

 9

Rumos da segurança na Internet

Por que estamos vulneráveis ? (1)

- Os sistemas computacionais e os programas se tornaram muito mais complexos nos últimos 25 anos.
- O controle de qualidade de softwares é deficiente, em razão de pressões de mercado ou deficiências na habilidade dos programadores, dentre outras razões.

 11

(*Moore's Law* - 1965)

- *Descreve a predição de que o poder computacional dos processadores dobra a cada 18 meses.*
- Significa um crescimento tecnológico de 50 a 60% da capacidade, a cada ano.
  - Em 5 anos a tecnologia será 10 vezes melhor, **10 vezes mais rápida**,**10 vezes mais diferente,** e **10 vezes mais valiosa**.

 12

Por que estamos vulneráveis ? (2)

- **O ciclo de desenvolvimento e testes de produtos está diminuindo** .
- Empresas continuam produzindo *softwares* com vulnerabilidades, incluindo tipos de vulnerabilidades, onde a prevenção já é bem compreendida (como por exemplo problemas de *buffer overflow*).

(Buffer Overflow)

- Exemplo: um programa está preparado para uma entrada de dados máxima de 80 caracteres.
- O que acontece se você entregar a ele 5000 caracteres ? Como o código vai se comportar ?

Leitura recomendada: Artigo "*The Tao of Windows Buffer Overflow*". http://www.cultdeadcow.com/cDc_files/cDc-351/ 9/5/2003

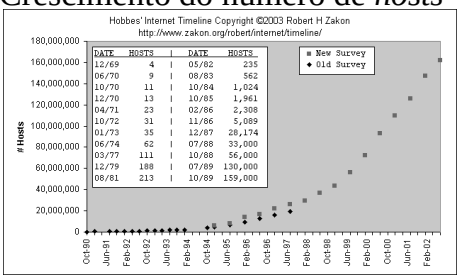
Por que estamos vulneráveis ? (3)

- A complexidade da Internet como rede está aumentando.
- A complexidade de protocolos e aplicações que rodam nos clientes e servidores ligados à Internet está aumentando.
- O número de empresas e usuários da Internet está aumentando.

Tantos sistemas, tão pouco tempo... (1)

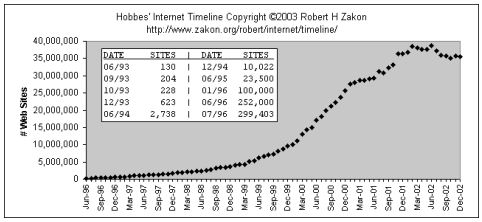
- 160 milhões de *hosts* estão conectados à Internet.
- Não existem 160 milhões de *sysadmins* !
- Alguém tem de dar conta do recado...
- ... e são os *sysadmins* !

Crescimento do número de *hosts*



http://www.zakon.org/robert/internet/timeline/ 9/5/2003

Crescimento do número de servidores www



http://www.zakon.org/robert/internet/timeline/ 9/5/2003

Tantos sistemas, tão pouco tempo... (2)

- *Sysadmins*:
  - Treinamento insuficiente e muita demanda conflitante.
  - Diretiva primeira: mantenha o sistema no ar !
  - Aplique os *patches*: quando tiver tempo !

Por que estamos vulneráveis ? (4)

- A infra-estrutura de informação tem muitos problemas de segurança fundamentais que não podem ser resolvidos depressa.
- O número das pessoas com conhecimento em segurança está aumentando, **mas a uma taxa significativamente menor que o aumento no número de usuários e *hosts*.**

Por que estamos vulneráveis ? (5)

- O número de ferramentas de segurança disponíveis está aumentando...
- ... mas não necessariamente tão rápido quanto a complexidade de softwares, sistemas e redes.

Por que estamos vulneráveis ? (6)

- O número de equipes de resposta a incidentes está aumentando...
- ... **mas a relação entre pessoal de resposta a incidentes e usuários de Internet, está diminuindo**.

Por que estamos vulneráveis ? (7)

- A sofisticação **dos ataques e ferramentas de intrusões** está aumentando.
- A **eficiência** dos intrusos está aumentando.
- O conhecimento está sendo passado aos intrusos menos hábeis.
- O número de intrusões está aumentando.

Security Incidents (CERT) :

Security (CERT) Incidents: 9/5/2003 - http://www.cert.org/stats/cert_stats.html

	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Inc	6	132	252	406	773	1334	2340	2412	2573	2134	3734	9859
Adv	1	7	12	23	21	19	15	18	27	28	13	17
Vul								171	345	311	262	417

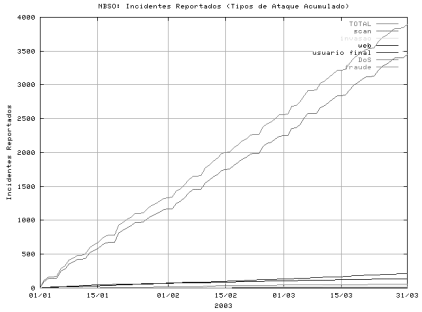
(Inc)idents, (Adv)isories, (Vul)nerabilities

	2000	2001	2002	2003(*)
Inc	21756	52658	82084	42586
Adv	22	37	37	12
Vul	774	2437	4129	959

(*) Total em 2003 somente até o 1o. Quadrimestre (Q1)

Total de incidentes (1988 até Q1/2003): 225.049

http://www.nbso.nic.br/stats/



Onde estamos

Parte 1 - Conhecendo seu inimigo

- Introdução.
- Por que estamos vulneráveis?
- ⇨ Quem é o *script kiddie*?
- Porque os ataques têm sucesso.
- A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia

- Algumas precauções úteis.
- Situações reais.
- Observando os bandidos: utilizando os *logs*.
- Congelamento de dados.
- Ferramentas e técnicas úteis.
- Legislação
- Conclusão

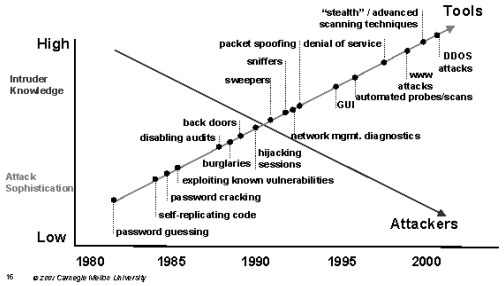
Quem é o *script kiddie*:

A metodologia dos atacantes.

Hacking = uma ciência em ascensão ?

- Definitivamente NÃO !
  - Qualquer bom *hacker* pode escrever uma ferramenta de ataque.
- **A verdadeira habilidade é o fato de se fazer uma ferramenta que qualquer um possa usar.**
  - Dezenas de sites onde ferramentas podem ser encontradas.
  - Os sites tentam se superar uns aos outros, tornando-se cada vez mais amigáveis e fáceis de serem usados.

Sofisticação X Conhecimento (1)



Sofisticação X Conhecimento (2)

Basta saber usar um *browser*...

...para encontrar sua ferramenta favorita:

- http://www.rootshell.com
- http://www.insecure.org
- http://www.securityfocus.com
- http://www.pimmel.com/thcarchive.php3 (11/5/2003)

- Felizmente a maioria das pessoas não sabe muito mais além do que usar um *browser*...

...mas em breve isso vai mudar.

 31

Quem é o *Script Kiddie* (1/4)

- Alguém em busca da morte fácil.
- Não está em busca de alvo específico.
- **Objetivo: ganhar acesso de *root,* da maneira mais fácil possível.**
- Foco: número pequeno de ferramentas e *exploits*, varrendo toda a Internet.

 32

Quem é o *Script Kiddie* (2/4)

- Alguns poucos...
  - São usuários avançados, que desenvolvem suas próprias ferramentas, e deixam *backdoors* sofisticados.
- A maioria...
  - Não têm a menor idéia do que estão fazendo.

 33

Quem é o *Script Kiddie* (3/4)

- Independentemente de suas habilidades, eles compartilham de uma estratégia comum:

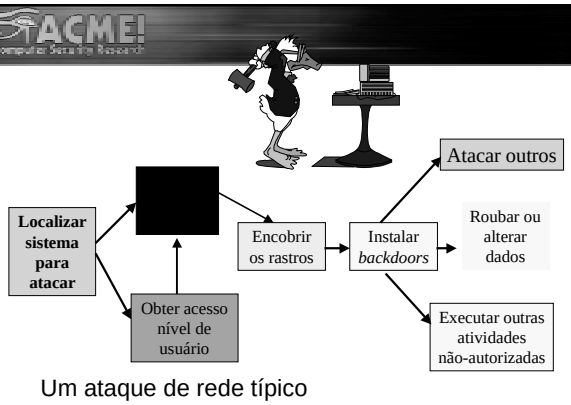
  Buscar aleatoriamente por uma vulnerabilidade específica e, então, explorar aquela vulnerabilidade.

 34

Quem é o *Script Kiddie* (4/4)

- Cedo ou tarde, os seus sistemas e redes serão verificados e "scanneados".
- Cedo ou tarde, eles encontrarão alguém **vulnerável** !

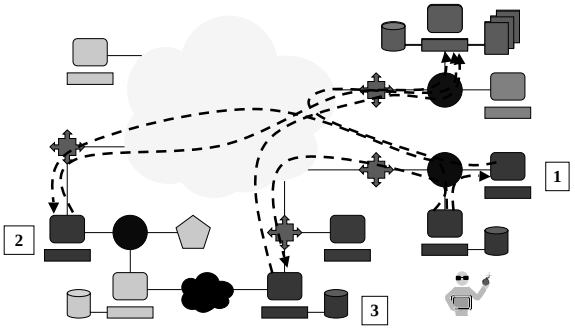
 35



Um ataque de rede típico

 36

Um ataque de ...



 37

Onde estamos

Parte 1 - Conhecendo seu inimigo

- Introdução.
- Por que estamos vulneráveis?
- Quem é o *script kiddie*?
- ⇨ Porque os ataques têm sucesso.
- A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia

- Algumas precauções úteis.
- Situações reais.
- Observando os bandidos: utilizando os *logs*.
- Congelamento de dados.
- Ferramentas e técnicas úteis.
- Legislação
- Conclusão

 38

Porque os ataques têm sucesso (1)

- As portas **não** foram fechadas porque estávamos ocupados demais fazendo as coisas “verdadeiramente importantes”.
- Se os atacantes são apanhados, eles não são punidos (seria embaraçoso demais admitir).
- Os **planos de resposta a incidentes** são inadequados.

 39

Porque os ataques têm sucesso (2)

- Os desenhistas do código de ataque analisam minuciosamente o alvo.
- Há tempo e esforço suficiente para desenhar o código de ataque.

 40

Porque os ataques têm sucesso (3)

- As ferramentas de busca de vulnerabilidades e ataques estão amplamente divulgadas.
- Qualquer pessoa pode obter e usar.
- Há um número crescente de pessoas fazendo uso delas.

 41

Porque os ataques têm sucesso (4)

- A **seleção aleatória de alvos** é que torna o *script kiddie* uma ameaça perigosa.
- Ao não buscar alvos específicos, todos os *sites* estão potencialmente ameaçados.

É impossível se esconder !

 42

Porque os ataques têm sucesso (5)

- Se a busca estivesse limitada a diversos *scans* individuais, não haveria problema
  - Com milhões de sistemas na Internet, seria pouco provável alguém encontrar um sistema específico.
- Entretanto... este não é o caso...

Porque os ataques têm sucesso (6)

- Uma vez que a Internet não tem fronteiras, estas ameaças estão se espalhando rapidamente em escala mundial.
- Não se trata de "**se**" , mas sim **"quando"** um sistema será atacado.

Resumo

- **Intrusos estão preparados e organizados.**
- **Ataques à Internet são fáceis, de baixo risco e difíceis de identificar.**
- **Ferramentas dos intrusos:**
  - **Estão crescendo em sofisticação**
  - **Fáceis de usar, especialmente por novatos.**
  - **Desenhadas para suporte a ataques em larga escala.**

Onde estamos

Parte 1 - Conhecendo seu inimigo

- Introdução.
- Por que estamos vulneráveis?
- Quem é o *script kiddie*?
- Porque os ataques têm sucesso.
- ⇨ A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia

- Algumas precauções úteis.
- Situações reais.
- Observando os bandidos: utilizando os *logs*.
- Congelamento de dados.
- Ferramentas e técnicas úteis.
- Legislação
- Conclusão

Vejamos um pouco sobre a metodologia dos atacantes

A morte fácil

- Estes são os sistemas que os *script kidies* estão procurando:
  - Sistemas **não supervisionados**. Sem *logs*.
  - Sistemas **sem política de uso**.
  - Sistemas desprotegidos.
  - Sistemas fáceis de explorar.

A motivação dos intrusos

- Dinheiro, lucro.
- **Vantagem competitiva**.
  - Econômica.
  - Política.
  - Pessoal.
- **Vandalismo**.
- Revanche, vingança pessoal.
- Curiosidade
- Acesso a recursos adicionais.
- Busca por atenção e projeção.

A metodologia

- A metodologia básica é muito simples:
  - "*Scannear*" a Internet buscando vulnerabilidades específicas.
  - Quando achar uma vulnerabilidade, explora-la.
- Base de dados de IPs que podem ser *scanneados*.
- Existe a vulnerabilidade naqueles IPs ?

Exemplo:

- Muitos sistemas Linux possuem uma vulnerabilidade nativa no *imapd*.
  - É feita uma busca por IPs válidos e ativos.
  - Desenvolver uma BD de sistemas rodando Linux: *Fyodor's nmap* (http://www.insecure.org/nmap/)
  - Usar ferramentas para verificar quais estão rodando *imapd* vulnerável.
  - Explorar os sistemas vulneráveis.

O terreno fértil: ausência de monitoração

- Muitas localidades não monitoram seus sistemas de forma alguma, e nunca percebem que estão sendo "scanneados".
- São raros os sistemas com uma **política clara e bem escrita** sobre geração de *logs*.
- **Quando** há *logs*, não são monitorados, nem automaticamente, nem por um humano.

Base de lançamento

- Os atacantes muitas vezes buscam silenciosamente por um sistema que possam explorar.
- Ao ganharem acesso a este sistema, o utilizam como base de lançamento para outros ataques, ocultando sua posição real.
- Colocam a culpa em outros *sysadmin*.

Arquivamento de resultados

- Resultados de *scans* são armazenados.
- Freqüentemente compartilhados com outros atacantes.
- **Resultados de *scans* anteriores** podem ser usados como referência.
- Mesmo que um sistema não tenha sido "*scanneado*" recentemente, **não** significa que está seguro contra um ataque.

Black-hats mais sofisticados...

- Implementam *trojans* e *backdoors* quando comprometem um sistema.
- *Backdoors* permitem fácil acesso.
- Os intrusos passam a usar o sistema sem serem notados
- Auditores (*logs*), indicadores de processos ou *filesystems* não são mais confiáveis.

 55

A questão temporal

- Horário não significa muita coisa.
- Os ataques acontecem a qualquer hora.
- Ferramentas de *scan* operam 24 horas
- Há abrangência mundial dos ataques.

 56

As ferramentas

- São de fácil utilização.
- Não exigem *expertise* .
- Buscam a Internet indiscriminadamente.

 57

Parte 2
Perícia

Onde estamos

Parte 1 - Conhecendo seu inimigo

- Introdução.
- Por que estamos vulneráveis?
- Quem é o *script kiddie*?
- Porque os ataques têm sucesso.
- A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia

⇨ Algumas precauções úteis.

- Situações reais.
- Observando os bandidos: utilizando os *logs*.
- Congelamento de dados.
- Ferramentas e técnicas úteis.
- Legislação
- Conclusão

 59

Algumas precauções úteis

Regras básicas para se proteger

Como se proteger (1/2)

- Estabeleça uma **política de segurança**.
- Estabeleça mecanismos de *logs*.
- Execute só serviços indispensáveis.
- Cautela com instalações *default*.
- Cautela com sistemas que fornecem informações (exemplo: transferência de zona de DNS dos seus *name servers*).

 61

Como se proteger (2/2)

- Os atacantes buscam por alvos fáceis.
- Verifique se seus sistemas não estão vulneráveis aos *exploits* mais comuns.
- Esteja informado sobre os *exploits* mais comuns:
  - http://www.cert.org
  - http://www.ciac.org
  - *Bugtraq* em http://www.securityfocus.com

 62

Exemplo de política

"O acesso a Internet usando computadores na organização X é permitida somente quando os usuários o fazem através do *firewall* Y da organização. Outras formas de acesso a Internet, tais como conexões *dial-up*, ou usando um provedor de acesso (*Internet Service Provider - ISP*), são proibidas se forem usados os computadores desta organização."

Referência: *Information Security Policies Made Easy*, Charles Cresson Wood, 1997, p. 318
http://www.rothstein.com/data/dr303a.htm 9/5/2003

http://www.rothstein.com/

 63

Onde estamos

Parte 1 - Conhecendo seu inimigo
- Introdução.
- Por que estamos vulneráveis?
- Quem é o *script kiddie*?
- Porque os ataques têm sucesso.
- A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia
- Algumas precauções úteis.
- ⇨ Situações reais.
- Observando os bandidos: utilizando os *logs*.
- Congelamento de dados.
- Ferramentas e técnicas úteis.
- Legislação
- Conclusão

 64

Casos reais de *sysadmins* em apuros...

(isso não é ficção)

Situação real:

- Vítima: "Eu estou com um problema de segurança. Eu fui invadido."
- *Security Officer:* "O.K. Vamos precisar dos seus *logs*."
- Vítima: "Huh? O que é isso ?"

 66

Fases frequentes e erros a evitar

"Eu não tenho meios para verificar a integridade do meu sistema."

 67

... e mais erros a evitar

"Eu não posso tirar a minha máquina do ar."

 68

... e mais erros a evitar

"Como eu monitoro a minha rede ?"

 69

... e mais erros a evitar

"O que é um *patch* ?"

"Como eu descubro quais *patches* estão disponíveis para o meu sistema operacional?"

 70

... e mais erros a evitar

"Eu vou deixar o meu sistema aberto e tentar apanhar o intruso."

 71

... e mais erros a evitar

"O administrador do sistema se demitiu, e agora eu tenho de lidar com esta situação. Na verdade o meu cargo atual é _____ ."

 72

... e mais erros a evitar

"Eu não tenho *backup* desta máquina."

 73

... e mais erros a evitar

"...mas eu não estou rodando *IMAP* nesta máquina!"

 74

... e mais erros a evitar

"Eu não sei onde esta máquina fica."

 75

... e mais erros a evitar

"Mas eu tenho um *firewall* !!"

"Esta máquina não se comunica com a Internet. Ela está bloqueada no *router*."

 76

... e mais erros a evitar

"Não, eu não sabia que esta máquina estava comprometida."

 77

... e mais erros a evitar

"Aqui o acesso físico é rigidamente controlado."

 78

... e mais erros a evitar

"O intruso está vindo da _____ ."

 79

Onde estamos

Parte 1 - Conhecendo seu inimigo
- Introdução.
- Por que estamos vulneráveis?
- Quem é o *script kiddie*?
- Porque os ataques têm sucesso.
- A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia
- Algumas precauções úteis.
- Situações reais.
- ⇨ Observando os bandidos: utilizando os *logs*.
- Congelamento de dados.
- Ferramentas e técnicas úteis.
- Legislação
- Conclusão

 80

Observando os bandidos

Como rastrear os movimentos dos atacantes e intrusos

O que veremos:

- Usando registros de auditoria (*logs*):
  - O que você consegue descobrir.
  - O que você **não** consegue descobrir.

 82

O que se **consegue** descobrir

O que é possível descobrir, usando medidas simples, e sem gastar dinheiro.

Informações básicas extraídas dos *logs*:

- Se seus sistemas foram **examinados**.
- O que seus visitantes **buscaram** saber.
- Que **ferramentas** ou técnicas foram usadas.
- Se os atacantes tiveram **sucesso** → talvez...

 84

Um problema significativo

- Numa quantidade alarmante de instalações, **sequer existe qualquer sistema auditor**, que registre as ocorrências e faça as contabilizações nos sistemas.
- Sistemas de *logs* são freqüentemente os primeiros alvos dos atacantes.

 85

Protegendo os seus *logs*

Algumas técnicas e conceitos básicos

Esta discussão...

- **Não** é baseada em um sistema particular.
- É baseada em "*Know-how*" e "***Peopleware***"
- Centrada em coleta de informações de inteligência, e contra-informação.
- Através da revisão dos registros de auditoria do seu sistema: **como descobrir o que o inimigo está fazendo**.

 87

Observe seus registros...

Você ficará surpreso ao descobrir a quantidade de informação útil que pode ser obtida, através da simples análise e revisão dos seus *logs*.

(quanto isso custa ??)

Mas, antes de mais nada...

- ...é preciso **PROTEGER** e garantir a integridade dos seus *logs.*
- Os seus *logs* são inúteis, se você não puder confiar neles.

Uma das primeiras coisas que a maioria dos intrusos fará, é tentar corromper os seus *logs*.

 89

Nas mãos dos inimigos...

- Há uma variedade de *rootkits* que removem dos *logs* a presença do intruso.
- Existem *syslogd* com *trojans* que não registram a presença do intruso.
- O intruso pode deixar uma *time-bomb* que faça " **rm -rf /** "
- etc... use sua imaginação...

 90

Primeiros passos para assegurar seus *logs*:

- Independentemente de quão seguro é o seu sistema, você nunca poderá confiar nos *logs* de um sistema comprometido.
- Primeira recomendação: registrar os *logs* no sistema local, **e num servidor de *logs* remoto**.
- **IMPORTANTE: sincronia de relógios (*NTP - Network Time Protocol*)**

Outras vantagens dos *logs* remotos:

- Fácil **correlacionar** e **identificar padrões** nesses *logs*.
- **Rever** rapidamente o que está acontecendo em todas as máquinas, usando só uma fonte de informação.
- **Comparar** para determinar se os *logs* de origem foram modificados.

Primeiros passos:

- Possuir um sistema de *logs* dedicado, ou seja, que tenha como função exclusiva a coleta de registros de auditoria, sem outros processos ou serviços.
- Boa opção: máquina Linux, agindo exclusivamente como coletora de *logs* na rede local.

Uma opção ao *syslogd*:

- Trocar o syslogd pelo **syslog-ng** (*freeware - GPL*)
- Permite mais opções de configuração.
- Filtragem de mensagens com base em prioridade, tipo de serviço e conteúdo. Redirecionamento de mensagens para múltiplos destinos.
- Permite redirecionamento em TCP.
- Proteção de arquivos com algoritmo *hash* .
- Linux, BSD, AIX, HP-UX e Solaris.
- http://www.balabit.hu/en/products/syslog-ng/ 9/5/2003
- Mirror: ftp://ftp.fsn.hu/pub/balabit

TCP-Wrapper: em conjunto com o *syslog*

- Wietse Venema *TCP Wrapper*.
- Trabalha em conjunto com o *inetd* e o *syslogd*.
- Sistema simples para auditoria e regras de permissão e bloqueio a serviços.
- *Default* na maioria dos sistemas atuais.
- ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz 9/5/2003

Determinando padrões nos *logs*

- Maioria dos *Script kiddies* → varre a rede em busca de uma única vulnerabilidade.
- Exemplo: Se os *logs* indicam múltiplas conexões, do mesmo sistema remoto, na mesma porta, possivelmente trata-se de uma varredura de alguma vulnerabilidade.

Exemplo de um *scan* registrado num *log server*:

```
Servidor de logs - /var/adm/logs
Oct 09 22:13:48 wolverine  in.ftpd[7645]: connect from 200.145.202.223
Oct 09 22:13:51 shadowcat in.ftpd[7645]: connect from 200.145.202.223
Oct 09 22:13:54 casper in.ftpd[7645]: connect from 200.145.202.223
Oct 09 22:13:57 fantasma in.ftpd[7645]: connect from 200.145.202.223
Oct 09 22:13:58 nimitz in.ftpd[7645]: connect from 200.145.202.223
Oct 09 22:14:02 bart in.ftpd[7645]: connect from 200.145.202.223
```


Outro exemplo:

```
Servidor de logs -  /var/log/secure
Oct 09 22:13:56 bart in.telnetd[22545]: connect from 200.145.202.223
Oct 09 22:13:56 bart imapd[11635]: connect from 200.145.202.223
Oct 09 22:13:56 bart in.fingerd[22549]: connect from 200.145.202.223
Oct 09 22:13:56 bart ipop3d[11638]: connect from 200.145.202.223
Oct 09 22:13:56 bart in.telnetd[22540]: connect from 200.145.202.223
Oct 09 22:13:56 bart in.ftpd[22541]: connect from 200.145.202.223
Oct 09 22:16:03 bart ipop3d[22542]: connect from 200.145.202.223
Oct 09 22:16:03 bart imapd[22543]: connect from 200.145.202.223
Oct 09 22:16:04 bart in.fingerd[22546]: connect from 200.145.202.223
Oct 09 22:16:05 bart in.fingerd[22552]: connect from 200.145.202.223
```


Um ataque de *buffer overflow*

```
Oct 10 22:04:51 bart mountd[6688]: Unauthorized access by NFS client 200.145.202.223.
Oct 10 22:04:51 bart syslogd: Cannot glue message parts together
Oct 10 22:04:51 bart mountd[6688]: Blocked attempt of 200.145.202.223 to mount
~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P3Û3À°^[Í~@3Ò3À~KÚ°^FÍ~@þÂuô1À°^BÍ~@~EÀubëb^V¬<ýt^FþÀt^Këõ°0þÈ~HFÿëì^°^B~
I^FþÈ~IF^D°^F~IF^H°f1ÛþÃ~IñÍ~@~I^F°^Bf~IF^L°*f~IF^N~MF^L~IF^D1À~IF^P°^P~IF^H°
fþÃÍ~@°^A~IF^D°f³^DÍ~@ë^DëLëR1À~IF^D~IF^H°fþÃÍ~@~HÃ°?1ÉÍ~@°?þÁÍ~@°?þÁÍ~@¸.bin@~
I^F¸.sh!@~IF^D1À~HF^G~Iv^H~IF^L°^K~Ió~MN^H~MV^LÍ~@1À°^A1ÛÍ~@èEÿÿÿÿýÿPrivet
ADMcrew~P(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(Oct 10 22:04:51
bart ^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^
E^H(-^E^H-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E
^H(-^E^H-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^ H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E
^H(-^E^H(-^E
```


Um ataque a cgi-bin

```
Servidor de logs - /var/log/httpd/access_log

200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/phf HTTP/1.0" 302 192
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/Count.cgi HTTP/1.0" 404 170
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/test-cgi HTTP/1.0" 404 169
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/php.cgi HTTP/1.0" 404 168
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/handler HTTP/1.0" 404 168
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/webgais HTTP/1.0" 404 168
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/websendmail HTTP/1.0" 404 172
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/webdist.cgi HTTP/1.0" 404 172
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/faxsurvey HTTP/1.0" 404 170
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/htmlscript HTTP/1.0" 404 171
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/pfdisplay.cgi HTTP/1.0" 404 174
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/perl.exe HTTP/1.0" 404 169
200.145.202.223- - [10/Oct/2000:22:04:13 -0300] "GET /cgi-bin/wwwboard.pl HTTP/1.0" 404 172
200.145.202.223- - [10/Oct/2000:22:04:14 -0300] "GET /cgi-bin/ews/ews/architext_query.pl
HTTP/1.0" 404 187
200.145.202.223- - [10/Oct/2000:22:04:14 -0300] "GET /cgi-bin/jj HTTP/1.0" 404 163
```


Ataque *imap*, *pop3* e *sendmail*

```
Servidor de logs - /var/log/maillog

Oct 10 18:01:58 bart imapd[11667]: command stream end of file,
while reading line user=??? host=[200.145.2.223]

Oct 10 18:01:58 bart ipop3d[11668]: No such file or directory
while reading line user=??? host=[200.145.2.223]

Oct 10 18:02:05 bart sendmail[11675]: NOQUEUE:
[200.145.2.223]: expn root
```


Logs centralizados

- Determinam o que o atacante está procurando ⇨ Correlacionam eventos.
- Facilitam a ação de contra medidas
- Entretanto ⇨ lembre-se que se você não está registrando um serviço, não é possível saber se seu sistema foi rastreado por aquela vulnerabilidade.

É importante notar também que...

- *Scans* normalmente acontecem em fases
  - Exemplo: é disponibilizado um código para explorar POP3, e acontecem inundações de tentativas de ataque deste *exploit*.
  - Mais adiante é a vez do Wu-FTP... etc...
- Ferramentas buscam uma ou múltiplas vulnerabilidades.

Ferramentas mais usadas para *scan*

- SSCAN de JsBach
  - http://packetstorm.decepticons.org/UNIX/scanners/sscan.tar.gz
- NMAP de Fyodor
  - http://www.insecure.org/nmap/
- NESSUS
  - http://www.nessus.org
- Mais: http://packetstorm.decepticons.org/UNIX/scanners/

9/5/2003

O que NÃO se consegue descobrir

Nem sempre os registros de *syslogd* resultam em informações úteis

Ferramentas de *scan* com *IP spoof*

- Diversas ferramentas possuem a opção de fazer a varredura com *IP spoof* .

→ falsificação do endereço de origem.

Exemplo: *% nmap -D www.algum.lugar.br*

- Opção de "*Decoy*" apresenta *scans* vindos de 15 fontes diferentes, mas somente uma é a real: difícil determinar a verdadeira.

"*Half-scan*"

- É mais freqüente.
- Opção de *half-scan* usa só um pacote SYN do *handshake* de 3 vias.
- Se o sistema remoto responde : a conexão é descartada com um pacote RST.
- Difícil determinar a origem.

Exemplo: *% nmap -sS www.algum.lugar.br*

Exemplo de *log*

```
Servidor de logs - /var/adm/log
Oct 10 22:12:08 bart in.rshd[12717]: warning: can't get client address:
Connection reset by peer
Oct 10 22:12:08 bart in.rshd[12717]: connect from unknown
Oct 10 22:12:09 bart in.timed[11718]: warning: can't get client address:
Connection reset by peer
Oct 10 22:12:09 bart in.timed[12718]: connect from unknown
Oct 10 22:12:09 bart imapd[12719]: warning: can't get client address:
Connection reset by peer
Oct 10 22:12:09 bart imapd[12719]: connect from unknown
Oct 10 22:12:09 bart ipop3d[12720]: warning: can't get client address:
Connection reset by peer
Oct 10 22:12:09 bart ipop3d[12720]: connect from unknown
Oct 10 22:12:09 bart in.rlogind[12722]: warning: can't get client address:
Connection reset by peer
Oct 10 22:12:09 bart in.rlogind[12722]: connect from unknown
```


Scans com opção "*stealth*" total

- Diversos sistemas de *scan* conseguem ocultar suas atividades dos sistemas auditores normais.
- Por exemplo:
- *nmap* combinando várias opções

% *nmap -sF -sX -sN www.vitima.com.br*

 109

Exemplo de *log* de um *Scan stealth*

Servidor de logs - /var/adm/log

assustador, não ? :-)

 110

Ferramenta para análise, filtragem e correlação de *logs*:

- *Swatch - "Simple WATCHdog"*
- Permite filtragem, monitoração e análise de *logs* em tempo real, à medida em que eles são gerados. Permite emitir alertas e correlacionar eventos.
- Excelente, em conjunto com TCP Wrapper
  - ftp://ftp.stanford.edu/general/security-tools/swatch/
  - http://ftp.uwm.edu.pl/pub/security/unix/logutils/swatch/

9/5/2003

 111

O atacante teve sucesso ?

Como saber se um atacante ganhou acesso a seu sistema

O intruso teve sucesso ?

- Situações podem ser identificadas em /var/logs/messages ou /var/adm/messages
- Identificação depende muito da experiência do analista.
- Recuperação de um incidente:

http://www.cert.org/nav/recovering.html 9/5/2003

 113

Conclusão sobre *logs*:

- *Logs* podem dizer muito sobre o inimigo.
- Importante: **Política de *logging***.
- Os *logs* precisam estar protegidos.
- Uma vez que existem os *logs*, é possível identificar padrões e correlações.
- É possível saber o que o intruso procura, ou (talvez) se ele teve ou não sucesso.

 114

Onde estamos

Parte 1 - Conhecendo seu inimigo

- Introdução.
- Por que estamos vulneráveis?
- Quem é o *script kiddie*?
- Porque os ataques têm sucesso.
- A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia

- Algumas precauções úteis.
- Situações reais.
- Observando os bandidos: utilizando os *logs*.
- ⇨ Congelamento de dados.
- Ferramentas e técnicas úteis.
- Legislação
- Conclusão

 115

Forensics
Congelamento de dados

Uma (breve) introdução às técnicas de perícia forense em computadores e redes

"Forensic Computing"

"Trata-se da captura e análise de evidências, **tanto quanto possível livres de estarem distorcidas ou tendenciosas**, de tal forma a reconstruir determinados dados ou o que aconteceu num sistema no passado."

- Dan Farmer

 117

Os grandes desafios (1/2)

- Sistemas são grandes e **complexos**, e mudam rapidamente.
- Fatos podem estar **ocultos** em qualquer lugar.
- Não há software disponível para tratar o problema.
- Exige-se **conhecimento** e **experiência**.

 118

Os grandes desafios (2/2)

- É fácil coletar dados, mas a análise é difícil.
- Além disso, a análise exige muito tempo disponível.
- Como armazenar as grandes quantidades de dados resultantes de registros de *logs*, auditoria e perícia.

 119

Requisitos de um perito

Altamente ético !

- **Conhecimento** e habilidades.
- **Entendimento** acerca das **implicações técnicas** de suas ações.
- Esperto, desconfiado, alerta, etc...

 120

Ao se deparar com um caso:

- **Isolar** e assegurar o perímetro.
- **Registrar** a "cena do crime".
- Conduzir uma busca sistemática por **evidências**.
- **Coletar** e armazenar as **evidências** que achar.

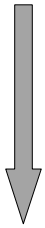
Coisas a se lembrar:

- Velocidade é essencial, **mas sem desespero**.
- Qualquer coisa que você faça num sistema, **causará alguma perturbação em seu estado**.
- Você nunca pode confiar plenamente no sistema.
- Suas **políticas** devem ser levadas em consideração, e respeitadas.
- Resigne-se aos **erros** que você cometer.
- Prepare-se para se **surpreender**.

Busca por evidências

- Preservação do *status* do sistema.
- Pode acontecer de **nunca** se saber o passado.
- Até mesmo o presente pode ser traiçoeiro.
- Sempre faça a coleta de dados de acordo com a **ordem de volatilidade**.

Ordem de volatilidade



- Registros, memória periférica, *cache*, etc...
- Memória *kernel* e física.
- Estado da rede.
- Processos em execução.
- Discos.
- *Floppies*, fitas, outros meios magnéticos.
- CD-ROM, impressões, etc..

Grandes problemas

- Não conhecer o que aconteceu.
- Não conhecer **contra quem**, ou o que, você está lutando.
- Não saber **em que confiar**.
- Problemas mais complexos exigem mais preparação.

Se você não conhece o sistema...

- Conheça e entenda as suas **limitações e do sistema**.
- Cuidado: **é fácil danificar as evidências**.
  - Mesmo uma análise simples é arriscada.

• Peça ajuda !

Plano de batalha

- **PENSE**. **Teclar rápido não adianta**.
- Use a sua política de segurança.
  - Execute o *checklist* de sua política.
  - Defina suas metas.
  - Deve-se contactar alguém ?
- Anote ou registre (*log*) suas ações.
- Trabalhe o menos possível com os dados originais.

 127

Reconstrução

- A maioria dos dados tem um componente **dependente do tempo**.
  - Construa uma linha do tempo de referência.
  - Examine uma determinada janela de tempo.
- Tente determinar o que aconteceu.

 128

Quem contactar ?

- A equipe de segurança de sua organização ?
- Seu superior ?
- A sua gerência superior ?
- NBSO ? (http://www.nbso.nic.br)
- Polícia ?
- CVV ? :-)

 129

Congelamento de dados

Capturando a situação do sistema para a análise

Diretiva primeira

“ Esforçar-se, ao máximo, para capturar uma representação fiel do sistema, tão livre de distorções ou influências quanto possível. ”

 131

Uma jornada no tempo

Reconstruindo eventos com base nas informações obtidas

Jornada no tempo

- Reconstrução de eventos passados.
- Palavra chave: **Correlacionar**.
  - Associar e comparar informações de diferentes fontes
- Importante: **sincronismo de relógios**
  - **Protocolo NTP**
  - http://www.eecis.udel.edu/~ntp/ 9/5/2003

Metas

- Observar a **atividade** de interesse.
- Determinar e reconstruir o que aconteceu.
- Entender e determinar o dano ocorrido.
- Ter acesso aos arquivos usados.

Nenhum método funciona sozinho

- **Combinar** táticas para obter as respostas.
- **Associar**.
- Operar dentro de um **tempo** específico.

Nunca se terá tudo, mas pode se ter o SUFICIENTE.

Métodos

- Reconstrução e história dos usuários.
- Reconstrução e história dos processos.
- Reconstrução da situação de rede.
- Arquivos de *log*.
- *Network Sniffing* (se possível)

Offline vs. *Online*

- Devo manter o sistema *up* ou não ?
- Manter *up* permite obter **mais evidências** ?
- Tenho maiores ou menores restrições de **tempo** ?
- Podem ocorrer erros na replicação ou interpretação dos dados ?
- Novamente: POLÍTICA de Segurança.

Como, e o que capturar (1/2)

- Mantenha controle de tudo que você digitar ou fizer.
- Considere restrições de espaço.
- **Capture primeiro, analise depois**.
- Anote: hardware, software e configuração do sistema.

Como, e o que capturar (2/2)

- Se possível, automatize os procedimentos e mantenha consistência do tempo.
- Siga a ordem de **volatilidade**.
- Faça cópias, inclusive das ferramentas, date, assine e armazene em segurança.

 139

Outras informações

Alguns exemplos de dados que são fáceis de serem obtidos, de forma simples

who - retrato dos usuários ativos

- *Username*
- Terminal ou window
- Início da sessão. Origem, se acesso remoto.

```
bilbo:/ide2/home/adriano/tct-1.03/docs$ who
adriano  pts/0    Oct 14 17:03 (shephard.unesp.br)
```

Arquivos associados: /var/utmp, /var/log/utmp, /var/adm/utmp

 141

last - atividade de *login* passada

- *Username*, terminal ou window.
- Início/fim/duração da sessão. Origem (truncado), se acesso remoto.

```
bilbo:/ide2/$ last | more
adriano  pts/0      shephard.unesp.b Sat Oct 14 17:03   still logged in
adriano  pts/0      shephard.unesp.b Sat Oct 14 14:56 - 15:08  (00:12)
aleck    pts/8      shephard.unesp.b Wed Oct 11 14:42 - 14:42  (00:00)
aleck    pts/7      :0.0          Wed Oct 11 11:08 - 19:33  (08:25)
aleck    pts/5      :0.0          Wed Oct 11 11:08 - 19:33  (08:25)
aleck    pts/6      :0.0          Wed Oct 11 11:08 - 19:33  (08:25)
```

Arquivos associados: /var/wtmp, /var/run/wtmp, /var/adm/wtmp

 142

lastlog - hora do último *login*

- *Um por usuário, indexado por UID.*
- Terminal, tempo de login e origem se remoto (freqüentemente truncado)

```
bilbo:/ide2/$ last | more

aleck      pts/8   shephard.unesp.b Wed Oct 11 14:42:55 -0200 2000
adriano    pts/0   shephard.unesp.b Sat Oct 14 17:03:36 -0200 2000
```

Arquivos associados: */var/lastlog, /var/log/lastlog, /var/adm/lastlog*

 143

Correlações de hora e *login*

- Quais usuários acessaram o sistema numa determinada hora ?
- Qual foi o padrão de uso de uma conta em particular?

```
bilbo:/ide2/home/adriano/docs$ last adriano | more
adriano  pts/0      shephard.unesp.b Sat Oct 14 17:03   still logged in
adriano  pts/0      shephard.unesp.b Sat Oct 14 14:56 - 15:08  (00:12)
adriano  pts/0      shephard.unesp.b Sat Oct 14 14:53 - 14:54  (00:00)
adriano  pts/0      shephard.unesp.b Fri Oct 13 21:27 - 21:40  (00:13)
adriano  pts/0      shephard.unesp.b Fri Oct 13 09:10 - 11:05  (01:54)
adriano  pts/0      shephard.unesp.b Thu Oct 12 11:28 - 12:01  (00:32)
```

 144

ps - retrato dos processos

- *Username*, terminal, hora de início.
- Quantidade de uso de memória e CPU.
- Linha de comando (facilmente forjado)
- Estado do processo (*running, sleeping, suspended, dead*, etc...)
- Ferramentas de interesse: *top*, *lsof* (*GPL*)
- Arquivos: */vmunix*, */dev/kmem*, */proc*

Correlações de processos e hora (1/2)

- Quais os comandos executados por um usuário específico ?
- Quais os comandos dentro de uma sessão específica ?
- Quais as sucessivas instâncias de um **processo** ?

Correlações de processos e hora (2/2)

- Quais as seqüências de comandos específicos de um usuário ?
- Relacionar todos os processos rodando durante uma determinada janela de tempo.
- Quais os processos residentes que iniciaram após o tempo de *reboot* ?

TCP Wrapper - conexões de rede

- Data, horário e destino da conexão.
- Nome do processo de rede e ID.
- *Host* cliente.
- Opcional: usuário cliente - *identd*.
- Baseia-se na informação de conexão fornecida pelo cliente.

TCP Wrapper - exemplo

```
Oct 16 03:20:45 wolverine in.comsat[7517]: connect from loopback
Oct 16 14:08:32 wolverine in.ftpd[9387]: connect from cindy.ensino.ibilce.unesp.br
Oct 16 15:32:21 wolverine in.ftpd[9843]: connect from batman
Oct 16 15:37:27 wolverine in.ftpd[9870]: connect from batman
Oct 16 16:34:59 wolverine in.telnetd[10152]: connect from jenny.dcce.ibilce.unesp.br
Oct 16 19:40:24 wolverine in.ftpd[10811]: connect from homer
Oct 16 19:41:08 wolverine in.telnetd[10816]: connect from homer
Oct 18 08:35:14 wolverine su: 'su root' succeeded for cristian on /dev/console
Oct 18 08:35:24 wolverine in.comsat[168]: connect from loopback
Oct 18 09:52:43 wolverine in.telnetd[237]: connect from master
Oct 18 10:57:45 wolverine in.ftpd[273]: refused connect from p8483ca.ickw.ap.so-
net.ne.jp
```


Correlações de rede

- Quais as conexões de um *site* específico?
- Quais as conexões para um serviço específico? (por exemplo, *telnetd* ou *ftpd*)
- Quais as seqüências sucessivas específicas de conexão de um *site* ? (por ex. *finger* seguido de *telnet*)
- Observar todas as conexões ocorridas num intervalo de tempo.

Outros sistemas de *tracing* baseados em *host*

- ***ltrace***: registra toda chamada de bibliotecas
- http://packages.debian.org/unstable/utils/ltrace.html
  9/5/2003
- ***ttywatcher***: monitoração em tempo real e outras funções (*keylogger*).
  - ftp://coast.cs.purdue.edu/pub/tools/unix/sysutils/ttywatcher/
    9/5/2003

Epílogo...

As ferramentas disponíveis podem tornar esperto até o intruso não-sofisticado.

Esperto o suficiente para explorar a vulnerabilidade, remover seus registros de *login* e, quase de forma invisível, instalar *trojans*.

Entretanto...

- **As ferramentas não impedem o intruso de cometer erros primários**, tais como, por exemplo, deixar um rastro nos horários de acesso a arquivos, dentre outros detalhes.
- O analista de segurança deve se aproveitar dos erros, e **enxergar entre a fumaça**.

Onde estamos

Parte 1 - Conhecendo seu inimigo

- Introdução.
- Por que estamos vulneráveis?
- Quem é o *script kiddie*?
- Porque os ataques têm sucesso.
- A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia

- Algumas precauções úteis.
- Situações reais.
- Observando os bandidos: utilizando os *logs*.
- Congelamento de dados.
- Ferramentas e técnicas úteis.
- ⇨ Legislação
- Conclusão

Legislação

Leis aplicáveis a crimes eletrônicos e Internet

A materialidade no ciberspaço

- Provas de Probabilidade
- Número Suficiente
- Fatos Jurídicos
  - Naturais
  - Humanos
  - Técnicos

Para obter um bom resultado

- Depende da perícia (*forensics*)
- Coleta de evidências é fundamental
- Lei é interpretação
- Para se formar um caso judicial é preciso coletar e preservar as provas.
- Evidências eletrônicas são efêmeras e mutáveis.

Caso virtual

- Arquivos de textos
- Arquivos de áudio e vídeo
- Imagens
- Registro de Transações (*logs*)
- Outros dados que sirvam como base para retratar a verdade.

Local do crime

Conceito:

"Porção do espaço compreendida num raio que, tendo por origem o ponto no qual é constatado o fato, se estenda de modo a abranger todos os lugares em que, aparente, necessária ou presumivelmente, hajam sido praticados, pelo(s) criminoso (s), os atos materiais, preliminares ou posteriores, à consumação do delito, e com este diretamente relacionados."

Legislação aplicável a crimes eletrônicos

Crimes contra a honra

- INJÚRIA
  - Código Penal Art. 140
- CALÚNIA
  - Código Penal Art. 138
- DIFAMAÇÃO
  - Código Penal Art. 139

Ataques e invasões

- Introdução de escutas Telemáticas (*Sniffers*)
- Lei de interceptação de comunicações telemáticas
  - Lei 9.296/96
- Produção de danos mensuráveis
  - Código Penal Art. 163

Ganho ilícito

- Estelionato: obter vantagem ilícita, induzir a erro, uso de ardil
  - Código Penal Art. 171
- Atribuir-se falsa identidade para obter vantagem indevida.
  - Código Penal - Art. 307

 163

Violação de sigilo

- Violação de sigilo de operação ou de serviço prestado por instituição financeira.
  - Lei 7.492/86, art.18

 164

Crimes contra telecomunicações

- Crimes contra a Segurança Nacional, ordem política e social
  - Lei 7.170 de 14.12.83

 165

Violação de propriedade

- Obra literária, artística ou científica e Direitos do Autor
  - Lei 9.610/98
- Software como Produção Intelectual
  - Lei 9.609/98

 166

Pedofilia na Internet

- Lei sobre Pornografia envolvendo crianças
  - Lei 8069 / 1990

 167

Lei de Crimes Ambientais (9.605/98)

- Cuida do ordenamento urbano, patrimônio histórico, artístico e cultural.
  - Art. 62: Destruir, inutilizar ou deteriorar: Arquivo, registro, museu, biblioteca, pinacoteca, instalação científica ou similar protegido por lei, **ato administrativo** ou decisão judicial.
    - Pena- reclusão, de um a três anos, e multa ....”

 168

Crimes contra o Estado

- Inviolabilidade dos segredos do Estado
- Divulgar Segredo de Sistema de Informações da Administração Pública
- Inserção de dados falsos em sistema de informações - Previdência Social
  - Lei No. 9.983/00

 169

Projeto de Lei Crimes de Informática

Projeto de Lei (PL) - 84 / 99

Ementa: Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

Autor: Luiz Piauhylino - PSDB / PE
Data de Apresentação: 24/2/1999
Situação: em tramitação.

Use o link abaixo para pesquisar a situação deste Projeto:
http://www.camara.gov.br/Internet/integras/default.asp

 170

Sites para consulta de legislação

http://www.planalto.gov.br/legisla.htm

Leis e decretos:
http://www.presidencia.gov.br
Projetos de Lei:
http://www.camara.gov.br

 171

Sites sobre direito na Internet

- http://www.direitodainformatica.com.br/
- http://www.internetlegal.com.br/

 172

Onde estamos

Parte 1 - Conhecendo seu inimigo

- Introdução.
- Por que estamos vulneráveis?
- Quem é o *script kiddie*?
- Porque os ataques têm sucesso.
- A ameaça e a metodologia dos atacantes.

Parte 2 - Perícia

- Algumas precauções úteis.
- Situações reais.
- Observando os bandidos: utilizando os *logs*.
- Congelamento de dados.
- Ferramentas e técnicas úteis.
- Legislação
- ⇨ Conclusão

 173

Conclusões

Antes de um incidente (1/3)

- Tenha uma boa **política de segurança**.
- Aprenda sobre seus sistemas.
- Ative os processos auditores e de *log*.
- Crie uma base com suas configurações.
- Auditore regularmente seus sistemas.
- **A imprevisibilidade deve ser sua aliada !**

 175

Antes de um incidente (2/3)

- Mantenha seus sistemas atualizados (*patches*).
- Mantenha uma educação continuada aos seus usuários. **Envolva os usuários**.
- Mantenha uma educação continuada e treinamento de seu pessoal.
- **Treine** seus procedimentos de emergência.

 176

Antes de um incidente (3/3)

- Saiba como os intrusos agem.
- Saiba, pelo menos, como capturar dados de perícia (mesmo que você não saiba analisar).
- Saiba quem chamar numa emergência.
  - Conheça seus vizinhos.
  - Não aceite doces de estranhos. :-)

 177

Política de Segurança

- **É a coisa mais importante !**
- Deve ser bem documentada, concisa e consistente.
- Deve ser mantida atualizada.
- Deve ser treinada.

 178

Cuidado com abusos

- Respeite a privacidade das pessoas.
- Seja ético.

Conhecimento com responsabilidade.

 179

"Nós trabalhamos no escuro. Fazemos o possível para combater o mal, que do contrário nos destruiria. Mas se o caráter de um homem é seu destino, a luta não é uma escolha, mas uma vocação."

Fox Mulder - Grotesque

Apêndice: URLs gerais sobre segurança

- www.acmesecurity.org 9/5/2003
- www.cert.org
- www.ciac.org
- www.sans.org
- www.first.org
- www.net-security.org
- www.securityfocus.com
- www.opensec.net
- www.nbso.nic.br

Apêndice: Fóruns de discussão

- Português:

http://forum.acmesecurity.org

http://www.linuxsecurity.com.br/forum

- Inglês:

http://www.whitehats.com/cgi/forum/messages.cgi

9/5/2003

Apêndice: ferramentas de segurança de domínio público

- ftp://ciac.llnl.gov/pub/ciac/sectools/unix
- ftp://coast.cs.purdue.edu/pub/tools
- http://cert.org/others_sources/tool_sources.html
- ftp://ftp.porcupine.org/pub/security/index.html
- ftp://ftp.funet.fi/pub/unix/security
- ftp://ftp.unicamp.br/pub/security/tools

Leituras obrigatórias

- "***Secrets and Lies***" - Bruce Schneier - Wiley Computer Publishing , ISBN 0-471-25311-1
- "***Network Intrusion Detection***", 2nd Ed. - Stephen Northcutt & Judy Navak - New Riders Publishing, ISBN 0735710082
- ***"Practical Unix and Internet Security",*** 2nd Ed. - Simson Garfinkel & Gene Spafford, O'Reilly & Associates, ISBN 1565921488

Apêndice: material complementar

- Cópia dos *slides* da versão atualizada desta apresentação, conjunto de *links* úteis, e demais materiais complementares deste curso podem ser obtidos em:

http://www.acmesecurity.org/cnbb2003
(disponível a partir de 19/maio/2003)

Para falar com o autor:

Adriano Mauro Cansian
adriano@acmesecurity.org / adriano@unesp.br

Laboratório ACME! de Pesquisa em Segurança de Redes
UNESP - Universidade Estadual Paulista
Campus de São José do Rio Preto
Depto. de Ciência da Computação e Estatística
R. Cristóvão Colombo, 2265 - Jd. Nazareth
15055-000 São José do Rio Preto, SP.
Tel. (17) 221-2475 (laboratório) / 221-2201 (secretaria)
http://www.acmesecurity.org

Chave PGP

Adriano Mauro Cansian <adriano@unesp.br>

Key ID: **0x3893CD2B**

Key Type: DH/DSS

Key Fingerprint:

C499 85ED 355E 774E 1709 524A B834 B139 3893 CD2B

http://www.pgpi.com

 187

 188