

Engenharia de Segurança

Profa. Dra. Kalinka Regina Lucas Jaquie Castelo Branco
kalinka@icmc.usp.br

1

Slides baseados nas transparências de diversos professores e autores de livros (prof. Márcio H. C. d'Ávila, Tannenbaum, Kurose, Adriano Cansian entre outros)

INTRODUÇÃO

- Computadores são mais úteis ligados em rede, compartilhando informação e recursos
 - Disponibilização ampla de informação
 - Interoperabilidade e intercâmbio de informação
 - Mobilidade de acesso e gerenciamento remoto
 - Sistemas de processamento distribuído
- A partir dos anos 80: evolução das interconexões de redes de computadores
- Aumento de extensão das redes e do acesso: mais necessidade de cuidado e controle

2

INTRODUÇÃO

- A todo momento surgem novos casos de redes invadidas ou comprometidas por ação de hackers, vírus e outros fatores de risco
- Estatísticas
 - Estudo do American Society for Industrial Security (ASIS) e Price Waterhouse-Cooper, EUA, 1999:
 - 97 empresas da lista Fortune 1000 responderam
 - Mais de US\$45 bilhões em perda/roubo de informação
 - Média: 2,45 incidentes e US\$0,5 milhão por incidente
 - Número de incidentes reportados por mês é crescente

3

INTRODUÇÃO

- Estatísticas
 - Levantamento anual de 2001 do FBI e Computer Security Institute (CSI) nos EUA:
 - Respostas de 538 atuantes no campo de segurança
 - 85% detectaram brechas de segurança nos últimos 20 meses e 70% declararam ter sofrido algum tipo de ataque nos últimos 12 meses
 - Perdas \$ mais sérias: roubos de informação proprietária
 - 70% citam conexão Internet como ponto freqüente de ataque (2000: 59%) e 31% citam os sistemas internos da empresa
 - 45% reportaram invasões de fontes externas (2000: 25%)
 - 55% reportaram invasões não-autorizadas por uma fonte interna à organização
 - 91% têm abuso do acesso à Internet por funcionários (2000: 79%)
 - 94% detectaram vírus de computador (2000: 85%)
 - 36% recorreram à Justiça pelas invasões (2000: 25%, 1996: 16%)

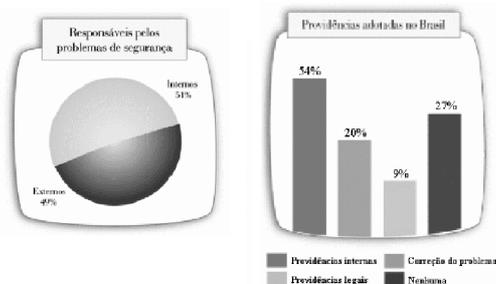
4

INTRODUÇÃO

- Estatísticas
 - Brasil: Pesquisa Nacional sobre Segurança da Informação, Junho/2000:
 - 93% reconhecem importância da proteção de dados para o sucesso do negócio, 39% consideram vital para corporações
 - Controle das redes corporativas ainda é fraco: 41% não sabem se foram invadidas, 85% não sabem medir o prejuízo
 - 38% c/ acesso à Internet via modem, sem grande segurança
 - Vírus: maior ameaça (75%) e 48% de contaminação nos últimos 6 meses, mesmo 93% adotando meios de prevenção
 - Causa interna: funcionários 39%, HD defeito 6%, prestadores de serviço 6%. Causa externa: hackers 28%, clientes 7%, fornecedores 6%, estudantes 6%, concorrentes 2%

5

INTRODUÇÃO



6

SEGURANÇA

- O que é segurança????
- O que é seguro???
- O que é segurança em rede de computadores??

7

ACME! Computer Security Research www.acmesecurity.org

Seguro !!?



© 2008 - Adriano Mauro Cansian 11

51.pdf (PROTEGIDO) - Adobe Acrobat Pro Extended

Documento Comentários Formulários Ferramentas Avançado Janela Ajuda

Colaborar Proteger Assinar Formulários Multimídia Comentário

6 / 26 150% Localizar

Seguro !!?

You've taken precautions. Your data's protected. Absolutely. You sure?



© 2008 - Adriano Mauro Cansian 12

SEGURANÇA

- Importância da segurança de redes
 - Proteção de patrimônio (em especial: informação)
 - Credibilidade e vantagem competitiva
 - Cumprimento de responsabilidades
 - Continuidade de operação/atividade
- Segurança de redes
 - Segurança de computadores
 - Segurança da informação
- Segurança da informação = proteção + integridade + disponibilidade + autenticação

10

SEGURANÇA

- Prática: Prevenção, Detecção e Resposta



- Toda segurança é relativa, pode ser tomada em níveis e deve ser um balanceamento:
 - custo da segurança × valor do patrimônio
 - provável × possível
 - necessidades de segurança × do negócio

11

SEGURANÇA

- Análise de risco
 - Identificar e priorizar valores (patrimônio)
 - Identificar vulnerabilidades
 - Identificar ameaças e suas probabilidades
 - Identificar contramedidas (respostas)
 - Desenvolver análise de custo-benefício
 - Planejar políticas e procedimentos de segurança
 - Políticas e procedimentos de segurança
- Políticas: gerais, focam o que e porquê
 - Procedimentos: específicos e detalhados, focam quem, quando, como

12

SEGURANÇA

Modelos de segurança

- Obscuridade
 - proteção pelo sigilo e desconhecimento
- Defesa perimetral
 - proteção concentrada nos limites/bordas da rede
- Defesa extensiva
 - cuidar da segurança de cada sistema componente



13

SEGURANÇA

Elementos e requisitos de segurança

- **Identificação e Autenticação:** distinguir, determinar e validar a identidade do usuário/entidade (se é quem diz ser)
- **Controle de acesso:** limitar/controlar nível de autorizações de usuários/entidades a uma rede, sistema ou informação
- **Não-repúdio:** impedir que seja negada a autoria ou ocorrência de um envio ou recepção de informação
- **Confidencialidade:** proteção da informação contra descoberta ou interceptação não autorizada; privacidade
- **Integridade:** impedir informação/transmissão de ser alterada/danificada de forma não autorizada, imprevista ou acidental
- **Disponibilidade:** confiabilidade de redes, sistemas e equipamentos sobre evitar ou se recuperar de interrupções

14

Ministério da Justiça propõe lei para a proteção de dados pessoais

Governo pressiona em encaminhamento ao Congresso um projeto de Lei regulamentando os limites para o uso, compilação e repasse de informações pessoais.

Publicado em 10 de agosto de 2010 às 11:04

Como melhorar a segurança da rede corporativa

Os funcionários adotam técnicas para burlar os firewalls e acessar conteúdo indevido no ambiente de trabalho? Veja o que fazer.

Publicado em 12 de agosto de 2010 às 09:05

Akamai: cresce uso do Brasil como base de ataques de negação de serviço

País está ao lado da Turquia como fonte emergente de ataques; empresa chegou a afirmar que cultura local de segurança é praticamente nula.

Publicado em 11 de agosto de 2010 às 10:51

Característica do Android facilita vida de cibercriminosos

Sistema operacional permite a criação de pasta privadas que "desaparecem" quando o aplicativo que a controla é deletado.

Publicado em 11 de agosto de 2010 às 11:40

Links patrocinados são os novos alvos dos botnets

Segundo a Trend Micro, já existem redes controladas por crackers que "sequestram" o navegador e enviam o infomail para o anunciante, faturando em cada clique.

Publicado em 11 de agosto de 2010 às 10:55

Vírus Zeus provoca rombo de quase US\$ 1 milhão em banco na Inglaterra

A botnet atacou 3 mil contas e movimentou quase 1 milhão de dólares em transações não autorizadas, de acordo com empresa de segurança.

Publicado em 10 de agosto de 2010 às 11:40

http://www.us-cert.gov/reading_room/

Friday, August 13, 2010

US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Security Publications Alerts and Tips Related Resources About Us Search US-CERT: customize

Information for: Technical, Non-Technical, Government, Control Systems

Security Publications

The following documents are available from the US-CERT website.

Securing your computer | Recovering from an attack | General internet security | Distributable materials | Monthly and quarterly reports

securing your computer

- Technical Information Paper: Cyber Threats to Mobile Devices
 - Introduces emerging threats likely to have a significant impact on mobile devices and their users
- Before You Connect a New Computer to the Internet
 - Tips for connecting a new (or newly upgraded) computer to the internet for the first time
 - For home users, students, small businesses, or any organizations with limited Information Technology (IT) support
- Governing for Enterprise Security
 - These web pages provide reports, presentations, and podcasts on how to manage security at the enterprise level
- Home Network Security
 - Information to help you use your home computer safely when you connect to the internet
- Recognizing and Avoiding Email Scams
 - Introduction to what email scams are, how they work, and how to avoid them
- Securing Your Web Browser
 - This paper will help you secure your web browser.
- Software License Agreements: Ignore at Your Own Risk

AMEAÇAS E ATAQUES

Vulnerabilidade

- Fraqueza inerente de um elemento do sistema
- Brecha: ponto fraco ou falha que pode ser explorado

Ameaça

- Qualquer coisa que possa afetar ou atingir o funcionamento, operação, disponibilidade, integridade da rede ou sistema

Ataque

- Técnica específica usada para explorar uma vulnerabilidade

Contra-medidas

- Técnicas ou métodos usados para se defender contra ataques, ou para fechar ou compensar vulnerabilidades

17

AMEAÇAS E ATAQUES

Vulnerabilidades

- Principais origens
 - Deficiência de projeto: brechas no hardware/software
 - Deficiência de implementação: instalação/configuração incorreta, por inexperience, falta de treinamento ou desleixo
 - Deficiência de gerenciamento: procedimentos inadequados, verificações e monitoramento insuficientes
- Exemplos
 - Instalação física: má proteção física de equipamentos e mídia
 - Hardware e Software: situações não previstas, limites, bugs no projeto, deixando brechas que podem ser exploradas
 - Mídia: roubo, perda, danificação, desgaste de discos, fitas etc.
 - Transmissão: interceptação de sinal, monitoramento, grampo
- Humana: desleixo, preguiça, estupidez, ganância, revolta etc.

18

AMEAÇAS E ATAQUES

o Ameaças

- Brasil: dados da 6ª Pesquisa Nacional sobre Segurança da Informação, 2000

| Principais ameaças às informações da empresa | |
|--|-----|
| 1- Vírus | 75% |
| 2- Divulgação de senhas | 57% |
| 3- Hackers | 44% |
| 4- Funcionários inatendidos | 42% |
| 5- Acessos indevidos | 40% |
| 6- Viamento de informações | 33% |
| 7- Erros e acidentes | 31% |
| 8- Falhas na segurança física | 30% |
| 9- Acessos remotos indevidos | 29% |
| 10- Superadores de acesso | 27% |
| 11- Uso de notebooks | 27% |
| 12- Pintaria | 23% |
| 13- Lixo informático | 25% |
| 14- Divulgação indevida | 22% |
| 15- Roubo / Furto | 18% |
| 16- Fraudes | 18% |

19

AMEAÇAS E ATAQUES

20

AMEAÇAS E ATAQUES

o Ataques

- Ataques sobre o fluxo de informação
 - Interrupção: ataca a disponibilidade
 - Interceptação: ataca a confidencialidade
 - Modificação: ataca a integridade
 - Fabricação: ataca a autenticidade
- Passivo
 - Interceptação, monitoramento, análise de tráfego (origem, destino, tamanho, frequência)
- Ativo
 - Adulteração, fraude, reprodução (imitação), bloqueio

21

AMEAÇAS E ATAQUES

| Aplicações | |
|------------|-----|
| TCP | UDP |
| IP | |

o TCP/IP e Ataques

- Muitos ataques são baseados em características de TCP/IP
- TCP/IP: arquitetura de protocolos padrão da Internet, para interconexão de redes
 - IP (*Internet Protocol*): protocolo de camada de rede sem conexão, baseado no endereço internet *n.n.n.n* (32-bit)
 - TCP (*Transfer Control Protocol*): protocolo orientado a conexão (fim-a-fim lógica entre dois nodos), com controle de fluxo, detecção de erro e seqüenciamento de dados
 - UDP (*User Datagram Protocol*): protocolo na camada de transporte, com datagramas sem conexão, adequado para transmissão simplificada de porções de dados

22

AMEAÇAS E ATAQUES

o Exemplos de ameaças e ataques

o Vírus

- Programa ou fragmento de código parasita, que não funciona de forma autônoma; requer um hospedeiro (programa "autêntico") ao qual se anexa para funcionar
- Ativado pela execução de programa infectado
- Se propaga pela infecção de outros programas ou envio de programa infectado por e-mail (auto-propagação), ou ainda pela cópia de programa infectado

o Verme

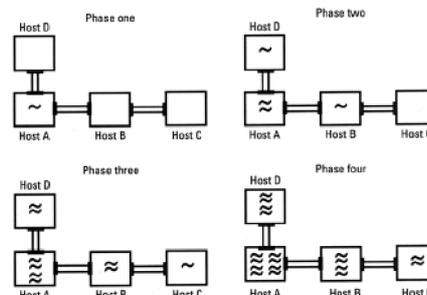
- Tipicamente é um programa independente (autônomo) feito para se propagar ou ativar nos sistemas infectados e procurar outros sistemas nas redes acessíveis
- Hoje existem intrusos mistos entre vírus e verme

23

AMEAÇAS E ATAQUES

o Exemplos

- Internet worm (Robert Morris, 1988)



24

AMEAÇAS E ATAQUES

Exemplos

- Cavalo de Tróia (Trojan Horse)
 - Programa ou fragmento de código maléfico que se esconde dentro de um programa, ou se disfarça de programa legítimo



25

AMEAÇAS E ATAQUES

Exemplos

- Back Door (Porta dos Fundos) ou Trap Door (Armadilha, Alçapão)
 - Forma não documentada de ganhar acesso a um sistema, criada no sistema por quem o projetou
 - Pode ser também um programa alterado ou incluído no sistema para permitir acesso privilegiado a alguém
- Bomba Lógica
 - Programa ou seção de um programa projetado com intuito malicioso, que é ativado por determinada condição lógica
 - Caso mais comum: funcionário programador mal intencionado

26

AMEAÇAS E ATAQUES

Exemplos

- Port Scanning (Varredura de Portas)
 - Técnica comum a hackers para reconhecimento
 - Programa que ouve a números de porta bem conhecidos para detectar informações e serviços em execução no sistema
- Exemplos de portas comuns padrão da Internet:
 - 20 FTP dados (transferência de arquivos)
 - 21 FTP controle
 - 23 Telnet (terminal)
 - 25 SMTP (envio de e-mail)
 - 80 HTTP (WWW)
 - 110 POP3 (recepção de e-mail)

27

AMEAÇAS E ATAQUES

Exemplos

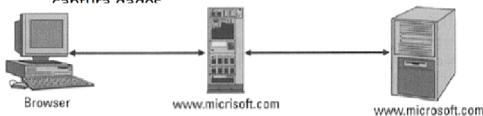
- Spoofs (Falsificação ou Disfarce de identidade)
 - IP Address Spoofing
 - Todo dispositivo em rede TCP/IP tem um endereço IP único, que é sua identificação (ex: 147.34.28.15)
 - IP Spoof: usar máquina configurada com IP aceito pelos sistemas de validação (roteador, firewall)
 - Sequence Number Spoofing
 - Conexões de rede TCP/IP usam n°s de sequência, incluídos em transmissões e trocados por transação
 - Se o algoritmo de geração de números é previsível, um hacker pode monitorar, gravar a troca de números de sequência e prever os próximos para se inserir na conexão

28

AMEAÇAS E ATAQUES

Exemplos

- DNS Spoof
 - MIM - Man In the Middle (Homem No Meio)
 - Técnica de se interpor no meio da comunicação
 - Ex.: registrar domínio parecido. Quando se comete erro de digitação, atacante se interpõe e pode repassar a comunicação c/ domínio correto, mas captura dados



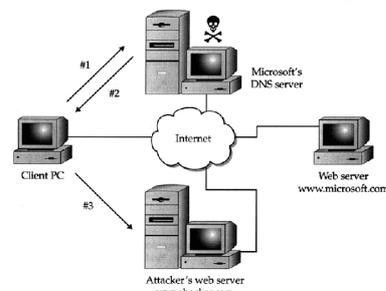
- Redirecionamento: inserir links para destinos falsos

29

AMEAÇAS E ATAQUES

Exemplos

- Envenenamento de DNS (DNS Poisoning)



30

Brasil | Entrada (1178) | Shopping Center Ig... | RapidShare Webhos... | Só Desenh...

COMEÇA A DISPUTA

Usuário
Quero acessar **www.banco.com.br**
O endereço **www.banco.com.br** está em **6.7.8.9**

Servidor de cache DNS

Servidor de autorização DNS banco

Servidor do criminoso

Criminoso vem
Se a resposta do cri...
real do servidor de a...
cache vai aceitar a r...
vai passar as inform...
define que o site do...
malicioso).

Enviar por e-ma

AMEAÇAS E ATAQUES

Exemplos

- Spoofs (Falsificação ou Disfarce de identidade)
 - Replay (Reprodução)
 - Interceptar e capturar uma transmissão legítima entre dois sistemas e retransmitir esta mais tarde
 - Pode-se evitar com *timestamp* (controle de tempo)
- Estouro de Pilha (Stack Overflow)
 - Consiste em preencher um buffer alocado na pilha com informação que excede o tamanho previsto, de forma que o endereço de retorno da função seja modificado
 - A modificação normalmente faz com que uma *shell root* seja acionada no retorno da função original

32

AMEAÇAS E ATAQUES

Exemplos

- Quebra de Senha (Password Cracking)
 - Tentar várias possibilidades de senha para ver se uma coincide com a de algum usuário/recurso
 - Geralmente usa-se o mesmo algoritmo que codifica (protege) as senhas de um sistema para codificar cada tentativa e comparar o resultado com a lista de senhas do sistema
 - Comum o uso de "dicionário" de palavras/expressões comuns
 - Existem muitos programas quebra-senha disponíveis, para a maioria dos sistemas operacionais e de rede
- Engenharia Social
 - Métodos não-técnicos para obter acesso a um sistema, em geral um processo de convencer alguém a revelar informação
 - Exemplo típico: ligar para alguém pertencente ou com acesso a uma corporação, fingindo ser do suporte técnico desta e inventar uma história p/ solicitar a senha de acesso da vítima

33

AMEAÇAS E ATAQUES

Exemplos

- Sniffing (Monitoramento, "Grampo")
 - Monitoramento de pacotes transitando na rede (passivo)
 - Muitas vezes são usadas ferramentas de fabricantes ou comerciais, criadas com propósitos legítimos (gerenciamento e manutenção de rede)
 - Conteúdo = informação: endereços IP, senhas etc. (Ex.: telnet e rlogin não criptografam as senhas digitadas pelo usuário)
 - Estatísticas = análise de tráfego: Ex.: servidores mais usados
- Web Site Defacement
 - Ataque muito comum na Internet, para inserir mensagem de protesto, aviso, ridicularização etc. na home-page de um site
 - Normalmente hackers exploram alguma configuração frágil ou vulnerabilidade conhecida de um servidor web, do sistema operacional ou dos protocolos e componentes envolvidos

34

AMEAÇAS E ATAQUES

DoS - Denial of Service (Interrupção de Serviço)

- Ação que interrompe um serviço ou impede totalmente seu uso por usuários/entidades legítimos
- Objetivo principal é "tirar do ar" (indisponibilizar) um serviço, apenas para causar o transtorno/prejuízo da interrupção ou para eliminar uma proteção que assim permita atingir outras formas de acesso não autorizado
- Tipos de ataques DoS
 - Consumo de banda de rede: atacante tem banda maior que a da rede alvo ou vários atacantes simultâneos para sobrecarga
 - Consumo de recursos de sistema: criar situações de abuso ou sobrecarga que ultrapassem o limite do recurso (buffer, HD...)
 - Atingir falhas que levam à interrupção
 - Adulteração de rotas/DNS: ao invés de desativar um serviço, impede o acesso ao serviço legítimo (usa *DNS Poisoning*)

35

AMEAÇAS E ATAQUES

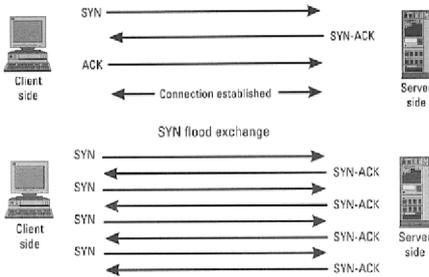
Exemplos

- Interrupção de Serviço (DoS - Denial of Service)
 - SYN Flooding (Inundação de SYN)
 - Ataca o *handshake* de 3-vias do estabelecimento de conexão TCP: cliente envia bit SYN (*synchronize sequence number*), servidor reconhece e responde com SYN-ACK, cliente reconhece a resposta enviando ACK e inicia a transferência de dados
 - Ataque: enviar SYNs e não responder aos SYN-ACK, deixando em aberto os estabelecimentos de conexão até ocupar todos os *buffers* de conexão no servidor
 - Outros clientes não conseguem estabelecer conexões legítimas e o ataque pode derrubar o sistema operacional se a situação consumir toda a memória livre do servidor

36

AMEAÇAS E ATAQUES

• SYN Flooding (cont.)



AMEAÇAS E ATAQUES

◦ Exemplos

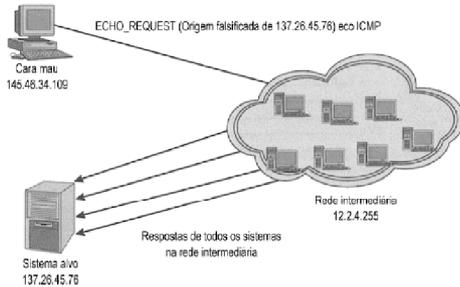
• Interrupção de Serviço (DoS - Denial of Service)

- Ping da Morte (Ping of Death)
- De aplicação simples, baseado em vulnerabilidade
- Ping: comando TCP/IP que envia um pacote IP p/ um endereço, para testar se existe e está "vivo"
- Vulnerabilidade: sistemas que não tratam adequadamente pacotes ICMP (pacote de controle a nível de IP) maiores do que o normal
- Ataque: enviar sequência de ping com campo ICMP de tamanho máximo (maior que o comum)
- Smurf
- Atacante envia um ECHO_REQUEST ICMP geral fazendo spoof do endereço origem com o endereço IP da máquina alvo = solicita uma resposta (eco) ICMP a todas as máquinas de uma rede, fingindo ser a máq. alvo
- Todas as máquinas da rede respondem para a máquina alvo real, sobrecarregando a rede e o sistema alvo

38

AMEAÇAS E ATAQUES

• Smurf (cont.)



AMEAÇAS E ATAQUES

◦ Exemplos

• SPAM / Junk Mail

- Prática do envio de e-mail não solicitado, em larga escala
- Normalmente são mensagens de propaganda ou solicitação de marketing de empresa tentando vender ou divulgar algo (que não queremos / não precisamos)
- Grandes quantidades de SPAM podem ser usados para causar sobrecarga de servidores de e-mail (DoS)
- Falsos e-mails de descadastramento de SPAM (remove@...) podem ser usados para confirmar e-mails válidos/em uso

• Mensagem-Bomba (Mail Bomb)

- Enviar e-mail enorme p/ sobrecarregar servidor e/ou o usuário

• War Dialing

- Método força-bruta para encontrar um telefone ligado a um modem (acesso discado a um sistema ou rede)
- Normalmente automatizado, tentando uma faixa de um prefixo de telefone associado a uma grande empresa

40