Capítulo 4 – Acesso não autorizado

Hacking

Acesso autorizado: o usuário (empregado, estudante) tem conta válida no sistema, criada pelo administrador.

Usuário deve respeitar as regras de uso, técnicas e éticas

Desrespeito às regras: tentar executar funções do administrador, ler ou danificar arquivos, acessar outros computadores de forma não autorizada (invasão)

Capítulo 4 – Acesso não autorizado

Hacker

Significado: varrer, limpar uma área, cortar (segurança)

Pessoa que acessa sistemas computacionais sem autorização de empregador ou cliente ou de qualquer outra pessoa ou empresa

O acesso pode ser feito por rede de computadores

Objetivo da Varredura – encontrar senhas que permitam o acesso a sistemas ou computadores ligados à rede que possuem falhas de segurança e possibilitam acesso não autorizado

Capítulo 4 – Acesso não autorizado

Hacker

Acesso pelo hacker: intenção criminosa ou prazer de invadir sistema (teste de capacidade?)

MIT – Massachusetts – EUA – estudantes aprenderam a manipular circuitos telefônicos e rastrear as comunicações das redes MIT (1º hackers)

Hacker: má intenção ou profissional extremamente talentoso e dedicado que procura vencer desafios relativos aos computadores, desenvolve projetos altamente complexos, conhece detalhes internos dos computadores e softwares básicos

Capítulo 4 – Acesso não autorizado

Subconjunto Hacker:

1) Crackers: especializados em descobrir senhas de usuários com uso de linhas telefônica (craking - rachadura) usando programas que monitoram linhas e decodificam sinais (sniffers - farejadores) reconhecendo identificadores de contas e suas senhas
2) Pranksters (traquina ou travessos): adolescentes que estão aprendendo a usar computadores e tentam entrar em sistemas remotos sem a intenção de causar danos, podendo estar motivados pelo aprendizado ou desafio.

Capítulo 4 – Acesso não autorizado

Subconjunto Hacker:

3) Phreaks: descobriram que o apito que vinham na caixa de cereais matinais produziam a mesma frequencia utilizada pela rede telefônica americana para acesso de chamada gratuita (0800). Ligavam gratuitamente para todo país.

Alguns jovens desenvolveram aparelhos que reproduziram várias freqüências de controle de roteamento telefônico e conseguiram comunicar-se com o mundo todo. Foram identificados e condenados

Capítulo 4 – Acesso não autorizado

Tipos de invasão – 1) Vírus

Programa que faz cópia de si próprio e hospeda-se em outros programas legais.

Auto-duplicação: instalar-se no setor de carga (boot) do disco, em componentes do sistema operacional, em aplicativos e arquivos de dados (Ex. texto)

Causam: corrupção do arquivo e disco ou pequenas perturbações (diminuiu velocidade de processamento, mostra imagens indesejadas)

Capítulo 4 – Acesso não autorizado

Tipos de invasão – 1) Vírus

Anti-Vírus: programa que descobre o vírus, removem restauram o que foi afetado.

Espalhamento: disquetes (?), pen drive, software legal vendido pelo fabricante (Aldus vendeu milhares de cópias infectadas do software de publicação eletrônica – vírus Peace; arquivos anexados às mensagens eletrônicas; arquivos de dados ou programas de livre uso (internet), como imagem para proteção de tela e monitores de vídeo

Capítulo 4 – Acesso não autorizado

Tipos de invasão – 2) Cavalo de Tróia

Programa que facilita acesso a um sistema que já foi invadido e consegue identificar contas e senhas válidas, inclusive do administrador. O invasor pode usar várias contas e diminuir a chance de ser notado.

Ex: programa que imita a tela de login e aguarda que usuário legítimo faça acesso para armazenar conta e senha, envia msg erro no sistema e para a execução

Capítulo 4 – Acesso não autorizado

Tipos de invasão – 3) Bomba-relógio

Programa executado em determinado evento, como uma data: Ex: Dano no sistema de RH quando processar demissão do funcionário

Capítulo 4 – Acesso não autorizado

Tipos de invasão – 4) Vermes

Programa orientados a se espalhar em diferentes nós de uma rede buscando máquinas ociosas. Residem em memórias e não são permanentes. Não se instalam em disco como os vírus

1º Verme: 2 novembro de 1988 – Universidade de Cornell – EUA por Robert T Morris.

Imaginou que a duplicação poderia ser controlada, mas um erro ocasionou a duplicação descontrolada e, em pouco tempo a rede entrou em colapso

Capítulo 4 – Acesso não autorizado

Tipos de invasão – 5) Farejadores

Programa que monitoram o tráfego da rede, capturam dados e buscam sequencias de identificadores de contas e senhas, tornando possível o acesso via FTP (acesso a arquivos em outros computadores) ou telnet (teste de comunicação de rede internet: web ou servidores), a qualquer equipamento ligado

Capítulo 4 – Acesso não autorizado

Motivação dos Hackers, segundo Branscomb (1995):

1) Proeza: jovens fascinados por computação procuram emoções no exercício de suas habilidades – mais comum
2) Proteção: descobrir falhas no sistema para melhorar a segurança. Hackers contratados para a segurança
3) Punição: vírus escondidos em programas com objetivo de punir compradores de softwares piratas

Capítulo 4 – Acesso não autorizado

Motivação dos Hackers, segundo Branscomb (1995):

4) Espreita: apenas querem entrar no computador para descobrir as informações existentes (vouyerismo - espionagem) sem intenções de causar danos

5) Filosofia/ideologia: hackers acreditam que a informação é um bem público e que o acesso não deve ser proibido e sim compartilhado

6) Potencial sabotador: invasão de terroristas e sabotadores para espionagem, chantagem,etc.

Capítulo 4 – Acesso não autorizado

Argumentos dos Hackers (Spafford, 1995)

1) Ética dos hackers: toda informação deve ser livre (filosofia/ideologia)... Não deveria haver propriedade intelectual e nem necessidade de segurança

Contra-argumento de Spafford: perda de privacidade e controle de alterações de informações, além do custo alto de coleta e desenvolvimento da informação

Capítulo 4 – Acesso não autorizado

Argumentos dos Hackers (Spafford, 1995)

2) Segurança: acessos não autorizados revelam problemas de segurança que não seriam encontrados de outra forma

3) Uso dos sistemas ociosos: recursos de equipamento são usados com acesso não autorizado, sem capacidade plena

Contra-argumento: muitas máquinas são dimensionadas para atender momentos de picos. Durante o período de uso médio podem ter desempenho satisfatório

Capítulo 4 – Acesso não autorizado

Tipos de pessoas que cometem invasões ou atos criminosos

1) Empregados
2) Desenvolvedores de software
3) Traquinas – pranksters
4) Profissionais classificados em 3 tipos: a)os que tem propósitos criminosos; b) os que estão tentando melhorar suas habilidades; c) os que testam as vulnerabilidades do software e aumentam o conhecimento de suas falhas

Capítulo 4 – Acesso não autorizado

Tipos de pessoas que cometem invasões ou atos criminosos

6) Cyberpunks: pessoas com habilidades para a computação com comportamento anti-social, cujo objetivo é criar problemas em sistemas computacionais por prazer e satisfação pessoal
7) Sabotadores e terroristas

Capítulo 4 – Acesso não autorizado

Administradores de sistemas devem ser preocupar cada vez mais coma segurança

Fabricantes de software procuram corrigir falhas sempre que as descobrem

Governo EUA - 1988:

Grupo Computer Emergence Response Team – CERT localizado no Software Engeneering Institute – Universidade Carnegie Mellon

Casos vem aumentando desde a sua criação

Capítulo 4 – Acesso não autorizado

Brasil:

Rede Nacional de Pesquisas – RNP – suporte as atividades de segurança

Centro de atendimento a incidentes de segurança – CAIS auxilia e identifica invasões e reparo dos danos causados

www.rnp.br/cais

cais@cais.rnp.br

Capítulo 4 – Acesso não autorizado

Web Police: reúne policiais do mundo numa rede para troca de informações e experiência no combate aos crimes pela internet

Brasil

911@Web-Police.org (endereço usado para casos de emergências graves)

www.web-police.org

Representante brasileiro: Brazilcop@WebPolice.org

Capítulo 4 – Acesso não autorizado

Programa de segurança

Satan – Security Administration Tool for Analyzing NetWorks – Ferramenta de administração de segurança para analise de redes

** com as pessoas erradas, pode ajudar invasores

Foram desenvolvidos programas para analisar a presença de Satan (Courtney, Gabriel)

www.ja.net/CERT/JANET-CERT/SOFTWARE/html