TIPOS DE ATAQUES

Cavalo de Tróia

O cavalo-de-tróia, ou trojan-horse, é um programa disfarçado que executa alguma tarefa maligna. Um exemplo: o usuário roda um jogo que conseguiu na Internet. O jogo secretamente instala o cavalo de tróia, que abre uma porta TCP do micro para invasão. Alguns trojans populares são NetBus, Back Orifice e SubSeven. Há também cavalos-de-tróias dedicados a roubar senhas e outros dados sigilosos.

Quebra de Senha

O quebrador, ou cracker, de senha é um programa usado pelo hacker para descobrir uma senha do sistema. O método mais comum consiste em testar sucessivamente as palavras de um dicionário até encontrar a senha correta.

Denial Of Service (DOS)

Ataque que consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços. Há muitas variantes, como os ataques distribuídos de negação de serviço (DDoS), que paralisaram sites como CNN, Yahoo! e ZD Net em fevereiro deste ano. Nessa variante, o agressor invade muitos computadores e instala neles um software zumbi, como o Tribal Flood Network ou o Trinoo. Quando recebem a ordem para iniciar o ataque, os zumbis bombardeiam o servidor-alvo, tirando-o do ar.

Mail Bomb

É a técnica de inundar um computador com mensagens eletrônicas. Em geral, o agressor usa um script para gerar um fluxo contínuo de mensagens e abarrotar a caixa postal de alguém. A sobrecarga tende a provocar negação de serviço no servidor de e-mail.

Phreaking

É o uso indevido de linhas telefônicas, fixas ou celulares. No passado, os phreakers empregavam gravadores de fita e outros dispositivos para produzir sinais de controle e enganar o sistema de telefonia. Conforme as companhias telefônicas foram reforçando a segurança, as técnicas tornaram-se mais complexas. Hoje, o phreaking é uma atividade elaborada, que poucos hackers dominam.

Scanners de Portas

Os scanners de portas são programas que buscam portas TCP abertas por onde pode ser feita uma invasão. Para que a varredura não seja percebida pela vítima, alguns scanners testam as portas de um computador durante muitos dias, em horários aleatórios.

Smurf

O Smurf é outro tipo de ataque de negação de serviço. O agressor envia uma rápida seqüência de solicitações de Ping (um teste para verificar se um servidor da Internet está acessível) para um endereço de broadcast. Usando spoofing, o cracker faz com que o servidor de broadcast encaminhe as respostas não para o seu endereço, mas para o da vítima. Assim, o computador-alvo é inundado pelo Ping.

Sniffing

O sniffer é um programa ou dispositivo que analisa o tráfego da rede. Sniffers são úteis para gerenciamento de redes. Mas nas mãos de hackers, permitem roubar senhas e outras informações sigilosas.

Spoofing

É a técnica de se fazer passar por outro computador da rede para conseguir acesso a um sistema. Há muitas variantes, como o spoofing de IP. Para executá-lo, o invasor usa um programa que altera o cabeçalho dos pacotes IP de modo que pareçam estar vindo de outra máquina.

Scamming

Técnica que visa roubar senhas e números de contas de clientes bancários enviando um e-mail falso oferecendo um serviço na página do banco. O Banrisul não envia e-mails oferecendo nada, portanto qualquer e-mail desta espécie é falso.

Teclado virtual falso

Software malicioso que abre uma tela de teclado virtual clonado exatamente sobre o teclado virtual legítimo do banco, para que o usuário informe os seus dados nele.

Popups maliciosos

Popups que tentam enganar o usuário para que este digite seus dados sensíveis, algumas vezes imitam perfeitamente os teclados virtuais.

Key Loggers

Software que captura os dados digitados no teclado do computador, como senhas e números de cartões de crédito.

Mouse Loggers

Software que captura os movimentos do mouse e cliques de botões, com o objetivo de contornar os teclados virtuais dos bancos. Os mais recentes capturam, inclusive, uma pequena imagem da área onde o clique do mouse ocorreu, para driblar teclados virtuais que embaralham suas teclas.

DNS Poisoning

Um atacante compromete um servidor DNS para, quando este receber a solicitação de resolução de uma URL de interesse (por exemplo www.banrisul.com), devolver o endereço IP de um site clonado ou malicioso, desviando o usuário sem que este perceba.

BHOs

Browser Helper Objects são DLLs que funcionam como plug-ins do Internet Explorer, podendo ver (e alterar) todos os dados que trafegam entre o computador e um servidor web. Nem todos são, necessariamente, maliciosos, mas são muito usados para construir em cavalos-de-tróia e spyware.

Clonagem de URLs

URLs podem ser clonadas por semelhança (wwwbanrisul.com.br, www.bamrisul.com.br, www.banrrisul.com.br, www.bamisul.com.br, www.banrissul.com.br) ou por falhas de segurança de browsers (por exemplo falhas de interpretação de nomes de site em unicode).

Scanning de memória/DLL Injection

Técnicas usadas por um programa para acessar a memória ocupada por outro programa, podendo assim ler dados sensíveis como a senha informada pelo usuário, chaves criptográficas, etc.