Técnicas de invasão

Invasão é a entrada em um site, servidor, computador ou serviço por alguém não autorizado. Mas antes da invasão propriamente dita, o invasor poderá fazer um teste de invasão, que é uma tentativa de invasão em partes, onde o objetivo é avaliar a segurança de uma rede e identificar seus pontos vulneráveis.

Mas não existe invasão sem um invasor, que pode ser conhecido, na maioria das vezes, como Hacker ou Cracker. Ambos usam seus conhecimentos para se dedicarem a testar os limites de um sistema, ou para estudo e busca de conhecimento ou por curiosidade, ou para encontrar formas de quebrar sua segurança ou ainda, por simples prazer.

Mas também pode ser por mérito, para promoção pessoal, pois suas descobertas e ataques são divulgados na mídia e eles se tornam conhecidos no seu universo, a diferença é que o Cracker utiliza as suas descobertas para prejudicar financeiramente alguém, em benefício próprio, ou seja, são os que utilizam seus conhecimentos para o mau.

Existem muitas ferramentas para facilitar uma invasão e a cada dia aparecem novidades a respeito. Abaixo serão descritas algumas das mais conhecidas.

Spoofing

Nesta técnica, o invasor convence alguém de que ele é algo ou alguém que não é, sem ter permissão para isso, conseguindo autenticação para acessar o que não deveria ter acesso, falsificando seu endereço de origem. É uma técnica de ataque contra a autenticidade, onde um usuário externo se faz passar por um usuário ou computador interno.

Sniffers

Sniffer é um programa de computador que monitora passivamente o tráfego de rede, ele pode ser utilizado legitimamente, pelo administrador do sistema para verificar problemas de rede ou pode ser usado ilegitimamente por um intruso, para roubar nomes de usuários e senhas. Este tipo de programa explora o fato dos pacotes das aplicações TCP/IP não serem criptografados.

Entretanto, para utilizar o sniffer, é necessário que ele esteja instalado em um ponto da rede, onde passe tráfego de pacotes de interesse para o invasor ou administrador.

Ataque do tipo DoS - Denial of Service

É um ataque de recusa de serviço, estes ataques são capazes de tirar um site do ar, indisponibilizando seus serviços. É baseado na sobrecarga da capacidade ou em uma falha não prevista.

Um dos motivos para existirem esse tipo de falha nos sistemas é um erro básico de programadores, na hora de testar um sistema, muitas vezes, eles não testam o que acontece se um sistema for forçado a dar erro, se receber muitos pacotes em pouco tempo ou se receber pacotes com erro, normalmente é testado o que o sistema deveria fazer e alguns erros básicos. O invasor parte deste princípio e fica fazendo diversos tipos de testes de falhas, até acontecer um erro e o sistema parar.

Este tipo de ataque não causa perda ou roubo de informações, mas é um ataque preocupante, pois os serviços do sistema atacado ficarão indisponíveis por um tempo indeterminado, dependendo da equipe existente na empresa para disponibilizá-lo novamente e dependendo do

negócio da empresa, este tempo de indisponibilidade pode trazer muitos prejuízos.

De acordo com um estudo da Universidade da Califórnia, Crackers tentam realizar em torno de 15 mil ataques do tipo DoS por semana. Os alvos mais comuns são grandes empresas.

Ataque do tipo DDoS – Distributed Denial of Service

São ataques semelhantes ao DoS, tendo como origem diversos e até milhares de pontos disparando ataques DoS para um ou mais sites determinados. Para isto, o invasor coloca agentes para dispararem o ataque em uma ou mais vítimas. As vítimas são máquinas escolhidas pelo invasor por possuírem alguma vulnerabilidade. Estes agentes, ao serem executados, se transformam em um ataque DoS de grande escala. Uma ferramenta chamada DDoS Attack, desenvolvida pelo programador brasileiro que se intitula OceanSurfer, é capaz de causar negação de serviços em computadores na Internet através de uma inundação de conexões em determinada porta.

Quebra de Senhas

Para acessar algo é necessário uma senha de acesso, muitos invasores tentam quebrar estas senhas através de técnicas de quebras de senhas, como tentar as senhas padrões de sistemas ou as senhas simples como nomes pessoais, nome da empresa, datas, entre outros. Mas para facilitar a descoberta da senha, existem diversos programas, como dicionários de senhas e programas que tentam todas as combinações possíveis de caracteres para descobrir a senha.

Vírus

O vírus de computador é outro exemplo de programa de computador, utilizado maliciosamente ou não, que se reproduz embutindo-se em outros programas. Quando estes programas são executados, o vírus é ativado e pode se espalhar ainda mais, geralmente danificando sistemas e arquivos do computador onde ele se encontra. Um exemplo deste tipo de programa é o Worm, criado por Robert Morris.

Os vírus não surgem do nada, ou seja, seu computador não tem a capacidade de criar um vírus, quem cria os vírus são programadores de computador mal intencionados.

Para que o vírus faça alguma coisa, não basta você tê-lo em seu computador. Para que ele seja ativado, passando a infectar o micro, é preciso executar o programa que o contém. E isto você só faz se quiser, mesmo que não seja de propósito. Ou seja, o vírus só é ativado se você der a ordem para que o programa seja aberto, por ignorar o que ele traz de mal pra você. Se eles não forem “abertos”, “executados”, o vírus simplesmente fica alojado inativo, aguardando ser executado para infectar o computador.

Após infectar o computador, eles passam a atacar outros arquivos. Se um destes arquivos infectados for transferido para outro computador, este também vai passar a ter um vírus alojado, esperando o momento para infectá-lo, ou seja, quando for também executado. Daí o nome de vírus, devido à sua capacidade de auto-replicação, parecida com a de um ser vivo.

Por que os vírus são escritos ? Esta pergunta foi feita na convenção de Hackers e fabricantes de vírus na Argentina. As respostas seguem abaixo:
· Porque é divertido;
· Para estudar as possibilidades relativas ao estudo de vida artificial (de acordo com a frase de Stephen Hawkind: “Os vírus de computador são as primeiras formas de vida feitas pelo homem”). Esta proposta é seguida por vários cientistas.
· Para descobrir se são capazes de fazer isso, tentando seus conhecimentos de computação, ou para mostrarem aos colegas que são capazes de fazer;

· Para conseguir fama;
· Fins militares. Falou-se sobre isso na primeira Guerra do Golfo, em 1991, e os vírus para uso militar são uma possibilidade.

Trojans

A denominação " Cavalo de Tróia" (Trojan Horse) foi atribuída aos programas que permitem a invasão de um computador alheio com espantosa facilidade. Nesse caso, o termo é análogo ao famoso artefato militar fabricado pelos gregos espartanos. Um
"amigo" virtual presenteia o outro com um " presente de grego" , que seria um aplicativo qualquer. Quando o leigo o executa, o programa atua de forma diferente do que era esperado.

Ao contrário do que é erroneamente informado na mídia, que classifica o Cavalo de Tróia como um vírus, ele não se reproduz e não tem nenhuma comparação com vírus de computador, sendo que seu objetivo é totalmente diverso. Deve-se levar em consideração, também, que a maioria dos antivírus fazem a sua detecção e os classificam como tal. A expressão " Trojan" deve ser usada, exclusivamente, como definição para programas que capturam dados sem o conhecimento do usuário.

O Cavalo de Tróia é um programa que se aloca como um arquivo no computador da vítima. Ele tem o intuito de roubar informações como passwords, logins e quaisquer dados, sigilosos ou não, mantidos no micro da vítima. Quando a máquina contaminada por um Trojan conectar-se à Internet, poderá ter todas as informações contidas no HD visualizadas e capturadas por um intruso qualquer. Estas visitas são feitas imperceptivelmente. Só quem já esteve dentro de um computador alheio sabe as possibilidades oferecidas.