

Backdoors

Por: Jonas Monteiro Carreira (Consultor em segurança da informação)
E-mail: J315@hotmail.com

Índice

1-Introdução

2-Definindo as Backdoors

3-Backdoors do bem

4-A “prevenção”

5-Conclusão

1-Introdução

Quando uma rede é invadida por uma determinada vulnerabilidade, a primeira coisa que o administrador faz é “tampar” o bug no qual fez com que seu sistema fosse invadido. Este tipo de prevenção a futuros ataques à sua rede é altamente recomendável, mas o que devemos fazer quando a nossa rede for invadida, vai além do que simplesmente “tampar” “furos”. É nesse esquema que entram as Backdoors.

Backdoors (porta dos fundos) são programas escritos para o cracker invadir o sistema, instalar o backdoor e, quando o administrador corrigir a falha, o cracker vai ter como acessar a máquina pela backdoor. Há casos raros, mas que acontecem, em que o administrador tem dificuldades até de descobrir uma backdoor dentro do seu sistema. Por isso estou escrevendo este simples artigo para termos meios de sabermos dificultar este tipo de ataque. Sendo que teremos que fazer tudo na “unha”, pois não existem ainda um “anti-ultrabackdoor” no mercado.

2-Definindo as Backdoors

Conhecidos no mundo da segurança como trojans. São programas que agem como vírus, mas muito sofisticados, pelo motivo não de destruir os sistemas, mas roubar informação da máquina invadida. No mundo do Windows, existem vários tipos de trojans que usam conexões implementando uma backdoor. Exemplos: Subseven, Back Orifice, Máster Paradise e etc... Desses exemplos citados, podemos destacar o subseven, por sua sofisticação de ataque, em que derruba a vítima por uma DOS (ataque de negação de serviço) e insere a backdoor por uma determinada porta para, posteriormente, o invasor conectar-se a máquina alvo.

Vemos que existem fatos em que uma backdoor pode ser inserida, simplesmente, por uma falta de informação do usuário, ou seja, um e-mail em anexo. Executar programas suspeitos faz com que, uma backdoor seja instalada na sua máquina, mas esses tipos de backdoor podem ser facilmente barrados por um bom antivírus na sua máquina. O problema seria ser invadido sem que você saiba. Isso pode ocorrer pelo fato de você estar usando um programa vulnerável, onde pode dar acesso ao cracker remotamente em sua máquina. Um caso como esse acontece muito no nosso dia-a-dia pela internet a fora. Exemplo: Seu browser pode estar vulnerável, seu programa de e-mail e até mesmo o seu programa de mensagens instantâneas. Caso como esses ocorreram em um programa de mensagem instantânea da AOL, onde uma função denominada “Goaway” possibilitava o cracker causar um desvio de memória no programa. Este desvio fazia com que a máquina da vítima abrisse portas causando, assim, a invasão por meio de uma backdoor. Por isso, devemos sempre ficar atentos em patches (programas feitos para corrigir vulnerabilidades) para evitar esse tipo de invasão.

Bem, podemos dizer que nossa rede está segura por firewalls bem configuradas e, com isso, estamos longe de ser atacados por backdoors. Mas o mundo da segurança não é tão feliz assim. Backdoors sofisticadas conseguiram barrar a segurança dos firewalls. Os famosos ataques de tráfegos reversos deram credibilidade a programas backdoors. Geralmente, os firewalls impedem que hosts de fora acessem sua rede interna, mas um host de dentro da rede pode acessar um host de fora

por uma porta. Uma backdoor bem programada pode conectar com o cracker por uma porta “segura” dentro da rede, fazendo o host executar uma Shell para o cracker. Um exemplo deste tipo de ataque foi o tão falado Code Red. Esse vírus instruía servidores IIS a executar conexões (TFTP) do servidor para um determinado host na internet. Com este esquema de ataque, o Code Red conseguia burlar a segurança de Firewalls através de um código falso. Firewalls permitem que servidores WEB iniciem conexões (TFTP).

Em sistemas operacionais Linux as backdoors podem ser ainda mais “camufladas”, com apenas uma simples Shell em `/etc/inetd.conf`, ou através de recursos de LKMs (Linux Kernel Modules). Estes módulos são “pedaços” do Kernel do Linux que podem ser programados durante uma execução do Kernel.

Existem módulos que possuem acesso ao filesystems e tabelas de syscall (chamadas do sistema), o que pode ser um sério risco para segurança do sistema. Uma redireção de uma syscall do Kernel do Linux pode esconder endereços IP, fazer listagens de arquivos e etc. Esse tipo de esquema tem sido muito usado em Backdoors.

3-Backdoors do bem

Quando falamos de backdoors, geralmente pensamos em invasões, roubos e etc. Mas podemos observar que existem também programas que agem como backdoors, mas para o bem. Não somente de portas discretas e conexões “camufladas” se sustenta um esquema de backdoor. O FBI usou esta técnica juntamente com o programa "magic lantern" como um espião que insere uma backdoor para monitoramento do suspeito. Temos o famoso VNC usado com conexões cliente e servidor fazendo assim uma conexão remota e controle das máquinas.

Esses foram alguns exemplos de vários backdoors que podem contribuir para ajudar o nosso dia-a-dia e até desvendar crimes.

4-A “prevenção”

Vimos que, a cada dia que passa, esses esquemas estão ficando mais sofisticados e, ao mesmo tempo, tornando sua detecção ainda mais difícil, mas ainda sim, podemos tentar se prevenir.

Outro tipo de prevenção para usuários Windows é não executar e-mails duvidosos, isso evitaria a instalação de uma backdoor e trojan.

Tenha cuidado em sistemas de administração remota. Eles podem estar mal configurados e servirem com uma backdoor para o invasor.

Tenha sempre uma firewall. Uma rede decente não tem longa vida sem uma firewall ou, até mesmo, usuários comuns. Uma firewall não evita totalmente uma backdoor, como visto anteriormente, mas pode evitar conexões por portas altas, evitando Script Kids.

Seja sempre cismado, busque patches de segurança para seu sistema operacional e softwares que você usa. Estude as mais recentes falhas de segurança e atualize sempre seu sistema.

Bem, podemos tentar encontrar backdoor em portas que não estão ativas, porém ainda não é um meio de detectar uma backdoor (se ela estiver bem programada), mas podemos tentar algo como: O comando netstat -na, em sistemas linux e windows, usado para listar as portas do seu sistema. Podemos usar um portscanner para facilitar ainda mais... portas que estejam em modo Listen podem estar provavelmente com uma backdoor instalada. Para isso, podemos configurar uma firewall para “fechar” tais portas.

5-Conclusão

Vimos neste básico estudo sobre backdoor que o mundo da invasão ainda está um passo a frente da segurança. Temos sempre que estar atentos para uma prevenção eficaz a este tipo de invasão, mas também não devemos ser sempre “neuróticos” com padrões de segurança na rede, ou seja, instalar Sistema criptográfico, IDS, firewall, antivírus, VPN, honeypots e etc. poderão deixar sua rede muito pesada e facilitar outro tipo de ataque de indisponibilização de serviço e de recursos. Temos que ser seguros, mas saber configurar bem uma ferramenta de segurança pode valer por muitas mal configuradas e mal administradas.

Abraços, e até a próxima.

Jonas Monteiro Carreira.