“Atividade pártica de Segurança de Dados”

Anderson de França Queiroz

Tiago de França Queiroz

7 de maio de 2012

“If you don’t stand for something,
you’ll fall for anything”
(Filme Sucker Punch)

Sumário

1 Descrição de um ataque

Um atacante deseja tronar indisponível o acesso por SSH do servidor de um conhecido. O modo que ele escolhe para fazer é utilizar um programa que ele desenvolveu para gerar requisições de conexção com o servidor initerruptamente partindo de vários computadores diferentes, ou seja, um ataque de DDoS – *Distributed Denial-of-Service*.

A disponibilidade de serviço é muito importante para várias empresas, principalmente quando o produto que a empresa ofereçe é o serviço. Ter um serviço pode causar perdas como: uma compra não ser realizada(sites de e-commerce); clientes trocarem de empresa para uma cujos serviços não fiquem indisponíveis; perda de confiabilidade; entre outras coisas.

Um ataque simples que visa indisponibilizar serviço é o ataque de negação de serviço, DoS (*Denial-of-Service*), em resumo esse tipo de ataque realiza um número muito grande de requisições ao serviço em curto espaço de tempo, assim o servidor não consegue reponder a todos, o que gera indisponibilidade do sistema. Existe a variante distribuida do DoS, o DDoS (*Distributed Denial-of-Service*), que utiliza simultaneamente vários computadores para realizar ataques de DoS a um mesmo alvo.

No cenário descrito o atacante desenvolve um programa que chama o cliente padrão de SSH do sistema operacional e tenta logar no host alvo. O programa apenas solicita a conexão e utiliza uam senha qualquer, uma vez que o objetivo é apenas indisponibilizar o sistema e não invadi-lo. De posse do programa ele vai a um laboratório de informica de sua universidade e instala o programa em todos os computadores de modo que quando se faça o login o programa inicialize em background. Como é preciso apenas a senha de usuário para realizar essa operação e todos os alunos utulizam o mesmo usuário, sempre que alguém logar no computador o ataque de DoS iniciará.

2 *Roteiro de ataque de DDoS*

O ataque de DDoS (*Distributed Denial-of-Service*) que será estudado nesta aula objetiva indisponibilizar o serviço de SSH comumente utulizado para acesso remoto a computadores. bla bla bla...

2.1 Criando um programa de DoS

A negação de serviço consiste em muitas requisições em um curto intervalo de tempo, de modo que o servidor não consiga atender a todas. Então nesse experimento criaremos um programa em linguagem C que utiliza *mult-thread* para realizar inúmereas requisições `SSH` a um servidor.

1. Abra o editor ASCI de sua preferência, sugere-se a utulização do `VIM`. Em um terminal execute `vim`;
2. Digite o código REFERENCIAR O CODIGO;
3. Salve com o nome `DoS.c`. Utilize ESC :w Dos.c;
4. Saia o editor. Utilize ESC :q;
5. Compile. No terminal execute `cc DoS.c -o DoS`;