Enjaulando Bind DNS

By admin on 5 de março de 2014 in Dicas, Linux, Segurança

Jauling , ou Jail Bind, é uma forma de colocar nosso servidor DNS dentro de um único diretório de forma que ele não tenha acesso ao restante dos diretórios de Linux.

A grande vantagem em mantê-lo enjaulado é que caso nosso Servidor de nomes seja invadido, ou invasor só terá acesso ao nosso sistema Operacional, e somente terá acesso ao diretório onde o Bind foi enjaulado.

Para conseguirmos enjaular, devemos ter todos os arquivos utilizados pelo Bind dentro de um único diretório, arquivos do /var, /dev e /etc/. Então consiste basicamente em trazer tudo que é necessário para o Bind em um diretório que será utilizado para o Jail.

Vamos então aos passos para criar os diretórios e arquivos para o Bind. Usaremos neste Post o /var/lib/named como diretório para enjaular. Tendo em vista que o bind já está instalado. Usaremos como referencia o Debian, mas poderia ser feito em qualquer outra distribuição.

Primeiro passo criar os diretórios necessários:

/etc/init.d/bind9 stop

mkdir -p /var/lib/named/etc
mkdir -p /var/lib/named/dev
mkdir -p /var/lib/named/var/cache/bind
mkdir -p /var/lib/named/var/run/bind/run

Dois dispositivos do /dev são utilizados pelo bind, no caso o /dev/null e o /dev/random, para isso deveremos criar esses dois dispositivos no novo diretório, veja abaixo:

mknod /var/lib/named/dev/null c 1 3
mknod /var/lib/named/dev/random c 1 8
chmod 666 /var/lib/named/dev/null
chmod 666 /var/lib/named/dev/random

Devemos mover os dados do /etc/bind para o diretório que será utilizado por padrão em /var/lib/named:

mv /etc/bind /var/lib/named

Como já estamos acostumados ao diretório padrão, e muitos itens, como script de inicialização, fazem referencia para o diretório anterior então podemos criar um link simbólico, de forma que evitaremos maiores problemas:

ln –s /var/lib/named/etc/bind /etc/bind

Vamos dar as permissões adequadas para os diretórios e arquivos que foram criados:

chown -R bind:bind /var/lib/named/var/*
chown -R bind:bind /var/lib/named/etc/bind

Desta forma já concluímos as configurações em relação às criações de diretórios do Bind9, então devemos agora informar ao Bind que deverá rodar em Jail, no caso chroot. Para isso devemos ir ao arquivo de configuração, já o script de inicialização, ou o utilizado pela distribuição. Em nosso caso do Debian, devemos alterar o arquivo /etc/default/bind9, altere a linha conforme abaixo :

OPTS=”-u bind -t /var/lib/named”

As configurações acima informam ao bind rodar com o usuário chamado bind e a opção –t informa ao bind rodar em chroot no diretório /var/lib/named.

Basta agora iniciar o serviço e verificar se realmente está sendo executado em Jail.

O primeiro item a ser visto será verificar o log:

tail –f /var/log/daemon

E por fim verificar se o processo existe e está rodando conforme solicitado:

ps aux | grep named | grep –v grep

O resultado deverá aparecer mais ou menos assim:

bind 4555 … ./usr/sbin/named -u bind **-t /var/lib/named**

Realmente um processo muito simples, que pode ser feito em alguns minutos, mas que garante a integridade de seu servidor caso esteja seja invadido.

Espero que aproveitem e tenham gostado deste Post, num próximo falaremos de DNSSec.

Abraços

.’.André Stato