4.10 Recomendações para evitar o abuso de Servidores DNS

4.10.1 Protegendo a recursividade

Dois tipos bastante utilizados de servidores DNS (Domain Name System) são o autoritativo e o recursivo, que embora possam ser executados em uma mesma máquina, possuem características distintas:

- O autoritativo é responsável por manter os mapas referentes a uma zona local e responder a requisições vindas de máquinas de todo o mundo, que precisarem resolver nomes de domínio da zona sobre a qual este servidor tem autoridade;
- O recursivo é responsável por receber as consultas DNS dos clientes locais e consultar os servidores externos, de modo a obter respostas às consultas efetuadas.

Um problema bastante comum de configuração é permitir que qualquer máquina na Internet faça consultas ao servidor DNS recursivo de uma determinada rede. Servidores com esse problema são comumente chamados de servidores DNS recursivos abertos, pois apenas o servidor autoritativo é que deve responder a consultas vindas de máquinas externas. (CERT.BR, 2016)

Diante do exposto, uma alternativa para evitar a utilização da recursividade de um servidor DNS por parte de redes não autorizadas é a criação de ACL junto as seguintes opções:

- **allow-query**: controla as consultas às zonas de autoridade do Servidor DNS.
- **allow-recursion**: especifica quais hosts estão autorizados a fazer consultas recursivas através do Servidor DNS.
- **allow-query-cache**: controla o acesso ao cache local do Servidor DNS.

Para isso, adicionaremos as seguintes configurações no arquivo **named.conf.options** do servidor **DNS primário**. (As mesmas configurações podem ser aplicadas no servidor DNS Secundário.)

> ***root@ns:/# vim /etc/bind/named.conf.options***

No cabeçalho do arquivo creie uma ACL denominada "liberados", nela deverá constar o endereço das redes que serão autorizadas a fazer consultas recursivas e ter acesso ao cache do servidor DNS. As opções localhost e localnets indicam respectivamente os endereços 127.0.0.1/8 e as redes que estão ao alcance do servidor DNS, neste caso a 172.16.1.0/24.

```
acl "liberados"  {
        200.132.50.0/24;
        localhost;
        localnets;
 };
```

No corpo do arquivo, dentro da seção "options" deverá ser inseridas as linhas que efetuarão o controle de acesso.

```
allow-query { any; };
allow-recursion { liberados; };
allow-query-cache { liberados; };
```

Observe que nas linhas inseridas as consultas autoritativas ao domínio (allow-query) estão liberadas para qualquer rede (any), enquanto as consultas recursivas (allow-recursion) e acesso ao cache (allow-query-cache) estão vinculdas a ACL "liberados", permitindo então acesso somente as redes listadas.

Após os ajustes, reinicie o serviço bind9 e posteriormente verifique seu *status*.

```
root@ns:/# systemctl restart bind9
root@ns:/# systemctl status bind9
```

4.10.2 Escondendo a versão do Bind

Outro pequeno ajuste de segurança que pode ser efetivado no Bind9 é configurar a omissão da versão que está rodando no seu servidor, a fim de evitar que vulnerabilidades que possam ser divulgadas referente a versão possam ser exploradas por usuários indevidos.

Para consultar a versão do servidor Bind9 de um domínio que utilize-o, pode ser executado o comando dig como segue:

```
root@ns:/# dig @ns.empresax.com.br version.bind chaos txt
```

Agora, a fim de efetivar a proteção, edite o arquivo named.conf.options e na seção options insira a seguinte linha:

```
version "DNS Server Empresa";
```

Após os ajustes, reinicie o serviço bind9 e posteriormente verifique seu *status*.

```
root@ns:/# systemctl restart bind9
root@ns:/# systemctl status bind9
```

Verifique novamente o retorno do comando dig.

4.10.3 Melhorando o desempenho do Bind

Restringir que as respostas do servidor DNS não envie seções adicionais melhora o rendimento deste. Para isso, pode ser adicionado no arquivo named.conf.options, na seção options, a seguinte linha:

```
minimal-responses yes;
```

O padrão do Bind9 para esta opção é "no". Após a inserção da linha, reinicie o serviço Bind9.