

Exercícios do Tópico 207 – DNS (Domain Name Server)

207.1 – Configuração básica de um servidor DNS

1. Configure o servidor DNS para que ele escute conexões em todas as suas interfaces de rede ativas.

Resposta:

- Verificar as interfaces com o ifconfig
- No arquivo /etc/named.conf, na seção options, configurar o parâmetro listen-on:
 - listen-on port 53 { localhost; IP1; IP2; };
- Executar o comando rndc reload

2. Configure seu servidor DNS para funcionar como “Caching-Only”.

Resposta:

- Em um sistema baseado em RedHat:

```
zone "." IN {
    type hint;
    file "named.ca";
};
```
- Em um sistema baseado em Debian:

```
zone "." {
    type hint;
    file "/etc/bind/db.root";
};
```
- Ao final do processo reinicie o serviço: # rndc reload

3. Crie 2 arquivos de logs diferentes no sistema, um chamado “seguranca” e que registre as informações referentes aprovação e bloqueio de requisições, e um chamado “consultas” que contenha as pesquisas realizadas no servidor. Use a severidade debug no arquivo “seguranca” e info no “consultas”.

Resposta:

```
logging {
    channel seguranca {
        file "data/seguranca.log";
        severity debug;
    };
};
```

```
channel consultas {  
    file "data/consultas.log";  
    severity info;  
};  
category security {  
    seguranca;  
};  
category queries {  
    consultas;  
};  
};
```

207.2 – Criar e Manter Zonas de DNS

1. Crie um registro do tipo master chamado exerciciolpi.com.br. Esse registro deve conter no mínimo as seguintes configurações:

- TTL de 12 horas
- Servidor NS chamado ns1.exerciciolpi.com.br e terá IP 200.201.202.203
- O e-mail do administrador do domínio será contato@exerciciolpi.com.br
- Criar um glue record
- O servidor de e-mails será o mx.exerciciolpi.com.br e terá IP 200.201.202.210
- O endereço www.exerciciolpi.com.br terá o IP 200.201.202.220
- O endereço sistema.exerciciolpi.com.br terá o mesmo IP do endereço www

Resposta:

- Configurar no /etc/named.conf:

```
zone "exerciciolpi.com.br" IN {  
    type master;  
    file "exerciciolpi.zone";  
};
```

- Criar o arquivo de zona /var/named/exerciciolpi.zone:

```
$TTL 12h  
@      IN      SOA    ns1.exerciciolpi.com.br. contato.exerciciolpi.com.br. (  
        2018032801  ; serial  
        28800      ; refresh  
        7200       ; retry  
        2419200    ; expire  
        150        ; negative caching  
)  
                NS      ns1  
                MX      5      mx  
ns1             A       200.201.202.203  
mx              A       200.201.202.210  
www             A       200.201.202.220  
sistema         CNAME    www
```

- Reiniciar o servidor DNS:
 - # rndc reconfig/reload

2. Configurar um servidor como slave do dominio exerciciolpi.com.br.

Resposta:

- Configurar no /etc/named.conf:

```

zone "exerciciolpi.com.br" {
    type slave;
    file "exerciciolpi.zone";
    masters { IP; };
};

```

- Reiniciar o servidor DNS:
 - # rndc reload

3. Configure uma zona de DNS Reverso que resolva os seguintes IPs e Nomes:

- 172.32.16.1 = roteador.exerciciolpi.com.br
- 172.32.16.10 = interno.exerciciolpi.com.br
- 172.32.16.20 = intranet.exerciciolpi.com.br
- 172.32.16.30 = proxy.exerciciolpi.com.br

Resposta:

- Configurar no /etc/named.conf:

```

zone "16.32.172.in-addr.arpa" IN {
    type master;
    file "16.32.172.in-addr.arpa.zone";
};

```

- Criar o arquivo de zona /var/named/16.32.172.in-addr.arpa.zone:

```

$TTL 3h
@      IN      SOA    ns1.exerciciolpi.com.br. contato.exerciciolpi.com.br. (
        2018032801  ; serial
        28800      ; refresh
        7200       ; retry
        2419200    ; expire
        150        ; negative caching
)
               NS      ns1.exerciciolpi.com.br.
1         PTR    roteador.exerciciolpi.com.br.
10        PTR    interno.exerciciolpi.com.br.
20        PTR    intranet.exerciciolpi.com.br.
30        PTR    proxy.exerciciolpi.com.br.

```

- Reiniciar o servidor DNS:
 - # rndc reconfig/reload

207.3 – Segurança no Servidor DNS

1. Configure o servidor de DNS para que as seguintes regras sejam cumpridas:

- a) Apenas IPs das Redes Internas 192.168.1.0/24 192.168.22.0/24 e 192.168.100.0/24 possam realizar consultas de DNS (recursivas e internas)
- b) Apenas os IPs 192.168.1.50 e 192.168.1.100 possam realizar operações de transferência de zona
- c) Toda a rede 172.32.0.0/16 seja ignorada pelo servidor DNS

Resposta:

```
acl "rede-interna" {  
    192.168.1.0/24;  
    192.168.22.0/24;  
    192.168.100.0/24;  
};  
options {  
    allow-query ( rede-interna; );  
    allow-transfer { 192.168.1.50; 192.168.1.100; };  
    blackhole { 172.32.0.0/16; };  
}
```

2. Configure a zona exerciciolpi.com.br para que funcione com o recurso de DNSSEC.

Resposta:

- Gere as chaves:
 - # dnssec-keygen -a DSA -b 1024 -r /dev/urandom -n ZONE exerciciolpi.com.br
- Insira o registro do arquivo .key dentro do arquivo da zona
- Assine as informações do arquivo de zona utilizado a chave privadas
 - # dnssec-signzone -P -r /dev/urandom -o exerciciolpi.com.br exerciciolpi.zone
Kxxxx.private
- Edite o arquivo /etc/named.conf alterando o arquivo do domínio exerciciolpi.com.br para exerciciolpi.zone.signed
- Reinicie o servidor DNS
 - # rndc reload