****

**Visão**

Com a crescente demanda sobre Tecnologias, percebemos que muitas pessoas apesar de buscarem informações, não possuem fontes que queiram realmente passar o conhecimento da maneira como ela deve ser, livre e com embasamento técnico que permita ser aplicado e utilizado quando necessário, além de serem testados em sua criação, tornando esta informação útil e confiável.

**Missão**

O Laboratório foi criado com a intenção de buscar e disseminar o conhecimento de uma maneira clara e objetiva, de forma gratuita, auxiliando na evolução dos membros e da sociedade na qual estas informações são compartilhadas, buscando o crescimento de todos os envolvidos nesta criação de valores.

**Licença**



Esta licença permite que outros remixem, adapte, e criem obras derivadas sobre a obra original, desde que com fins não comerciais e contanto que atribuam crédito ao autor e licenciem as novas criações sob os mesmos parâmetros. Outros podem fazer download ou redistribuir a obra da mesma forma que na licença anterior, mas eles também podem traduzir, fazer remixes e elaborar novas histórias com base na obra original. Toda nova obra feita a partir desta deverá ser licenciada com a mesma licença, de modo que qualquer obra derivada, por natureza, não poderá ser usada para fins comerciais.

This license lets other remix, tweak, and build upon your work non-commercially, as long as they credit you and license their new creations under the identical terms.

Para maiores informações sobre o método de licenciamento acesse os seguintes sites:

Brasil:

<http://creativecommons.org.br/as-licencas/>

<http://creativecommons.org/licenses/by-nc-sa/3.0/br/>

Internacional:

<http://creativecommons.org/licenses/by-nc-sa/3.0/>

<http://creativecommons.org/licenses/by-nc-sa/3.0/legalcode>

**1 – Testando o BIND no Linux**

Podemos testar nossas configurações de DNS utilizando algumas das ferramentas que vem no próprio **BIND** e outras que estão presentes no pacote **dnsutils**.

**2 – Testando com o Named-Checkconf**

Com esse utilitário podemos validar se nosso arquivo de configuração está correto. Casa haja algum erro, seremos informados em qual linha está a inconsistência e uma breve descrição.

dns-fusion:~# named-checkconf

dns-fusion:~# echo " {;;;;;;}" >> /etc/named/named.conf

dns-fusion:~# named-checkconf

/etc/named/named.conf:81: syntax error near '{'

dns-fusion:~#

Como podemos observar a primeira vez em que executamos o utilitário não tinha erro em nosso arquivo de configuração, após isso, inserimos uma linha sem sentido e executamos novamente o comando e eles nos informou que na **linha 81** do arquivo de configuração tem uma inconsistência.

**3 – Testando com o Named-Checkzone**

Semelhante ao utilitário anterior, porém, este analisa os arquivos de banco de dados de zonas. Para testarmos basta executar o utilitário seguido da zona a qual queremos consultar, e se arquivo de banco de dados.

dns-fusion:~# named-checkzone how2security.com.br \ /var/named/db/master/how2security.com.br

zone how2security.com.br/IN: 'how2security.com.br' found SPF/TXT record but no SPF/SPF record found, add matching type SPF record

zone how2security.com.br/IN: loaded serial 2014082000

OK

dns-fusion:~#

Observe que tivemos uma inconsistência no arquivo de zona do nosso domínio, e que o problema está no registro **SPF**. Por isso, vamos colocá-lo em conformidade com a **RFC 4408**.

Iremos alterar de:

@ IN TXT "v=spf1 a mx 192.168.5.0/24 - all"

Para :

how2security.com.br. IN TXT "v=spf1 +mx a ip4:192.168.5.0/24 -all"

@ IN SPF "v=spf1 +mx a ip4:192.168.5.0/24 -all"

O resultado agora é:

dns-fusion:~# named-checkzone how2security.com.br /var/named/namedb/master/how2security.com.br

zone how2security.com.br/IN: loaded serial 2014082000

OK

dns-fusion:~#

**4 – Testando com o NSLOOKUP**

A **ISC** não recomenda a utilização do **NSLOOKUP**, porém eles mantêm o pacote devido a legião de usuários que utilizam a ferramenta. Uma das poucas vantagens do **NSLOOKUP** é a utilização de uma biblioteca de resolução independente do **Resolver** e consultar um servidor por vez. Dentre as desvantagens está o fato de entregar respostas confusas e erros indefinidos.

root@fusion:~# nslookup

> www

Server: 192.168.5.129

Address: 192.168.5.129#53

www.how2security.com.br canonical name = fusion.how2security.com.br.

Name: fusion.how2security.com.br

Address: 192.168.5.128

> 192.168.5.128

Server: 192.168.5.129

Address: 192.168.5.129#53

128.5.168.192.in-addr.arpa name = fusion.how2security.com.br.

> set type=mx

> how2security.com.br

Server: 192.168.5.129

Address: 192.168.5.129#53

how2security.com.br mail exchanger = 1 fusion.how2security.com.br.

> set type=soa

> how2security.com.br

Server: 192.168.5.129

Address: 192.168.5.129#53

how2security.com.br

origin = fusion.how2security.com.br

mail addr = suporte.how2security.com.br

serial = 2014082000

refresh = 28800

retry = 7200

expire = 604800

minimum = 86400

> server 8.8.8.8

Default server: 8.8.8.8

Address: 8.8.8.8#53

> www

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

www.how2security.com.br canonical name = how2security.com.br.

how2security.com.br

origin = a.sec.dns.br

mail addr = hostmaster.registro.br

serial = 2014235000

refresh = 345600

retry = 900

expire = 604800

minimum = 900

Authoritative answers can be found from:

>

Aqui podemos observar algumas consultas diretas e recursivas, especificando o tipo de registro a ser consultado e até mesmo alterando o **Servidor DNS** para ver a resposta deles sobre o nosso domínio.

**5 – Testando com o HOST**

O utilitário HOST entrega respostas objetivas, sua vagagem é a simplicidade. Ele utiliza as configurações de **DNS** do **Resolver** para fazer as consultas. Iremos fazer as consultas anteriores, porém utilizando o **HOST**

root@fusion:~# host www

www.how2security.com.br is an alias for fusion.how2security.com.br.

fusion.how2security.com.br has address 192.168.5.128

root@fusion:~# host -v www.how2security.com.br.

Trying "www.how2security.com.br"

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52122

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:

;www.how2security.com.br. IN A

;; ANSWER SECTION:

www.how2security.com.br. 43200 IN CNAME fusion.how2security.com.br.

fusion.how2security.com.br. 43200 IN A 192.168.5.128

;; AUTHORITY SECTION:

how2security.com.br. 43200 IN NS fusion.how2security.com.br.

Received 92 bytes from 192.168.5.129#53 in 3 ms

Trying "fusion.how2security.com.br"

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50100

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:

;fusion.how2security.com.br. IN AAAA

;; AUTHORITY SECTION:

how2security.com.br. 43200 IN SOA fusion.how2security.com.br. suporte.how2security.com.br. 2014082000 28800 7200 604800 86400

Received 88 bytes from 192.168.5.129#53 in 1 ms

Trying "fusion.how2security.com.br"

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19367

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:

;fusion.how2security.com.br. IN MX

;; AUTHORITY SECTION:

how2security.com.br. 43200 IN SOA fusion.how2security.com.br. suporte.how2security.com.br. 2014082000 28800 7200 604800 86400

Received 88 bytes from 192.168.5.129#53 in 0 ms

root@fusion:~# host -v -t soa www.how2security.com.br.

Trying "www.how2security.com.br"

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40083

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:

;www.how2security.com.br. IN SOA

;; ANSWER SECTION:

www.how2security.com.br. 43200 IN CNAME fusion.how2security.com.br.

;; AUTHORITY SECTION:

how2security.com.br. 43200 IN SOA fusion.how2security.com.br. suporte.how2security.com.br. 2014082000 28800 7200 604800 86400

Received 106 bytes from 192.168.5.129#53 in 1 ms

root@fusion:~# host -l -v -t any www.how2security.com.br.

Trying "www.how2security.com.br"

; Transfer failed.

Trying "www.how2security.com.br"

Host www.how2security.com.br not found: 9(NOTAUTH)

Received 41 bytes from 192.168.5.129#53 in 0 ms

; Transfer failed.

root@fusion:~#

Observe que a última consulta solicitamos uma consulta **AXFR**, que iria transferir a base de dados através da consulta. Caso seu **Servidor DNS** respondo essa consulta você corre um risco de segurança.

**6 – Testando com o DIG**

O utilitário **DIG** é o acrônimo para **Domain Information Groper**, que significa **Busca por Informações de Domínio no Escuro**. E inglês a palavra **DIG** significa “**Escavar**”. O **DIG** é a ferramenta mais poderosa de consulta do **BIND**.

O **DIG** não utiliza as configurações de **DNS** do **Resolver**, por isso, é necessário utilizar o **FQDN** em todas as consultas.

Vamos começar

.

**7 – BIND DNS em Linux – Referencias**

**Referencias Bibliográficas**

**[1]** Freitas, Andrey Rodrigues de – Perícia forense aplicada à informática: em ambientes Microsoft, 1º Ed, Rio de Janeiro, 2006, Brasport.

**[2]** Forouzan, Behrouz A. – Protocolo TCP/IP, 3º Ed, São Paulo, 2008, McGraw-Hill.

**[3]** Freitas, Andrey Rodrigues de – Perícia forense aplicada à informática: em ambientes Microsoft, 1º Ed, Rio de Janeiro, 2006, Brasport.

**[4]** Registro BR. Disponível em: [< http://registro.br/dominio/categoria.html](file:///C:\Users\Aline\Documents\How2Sec%20-%20Feito\02%20-%20Sistemas%20Operacionais\001%20-%20Linux\BIND\%3c%20http:\registro.br\dominio\categoria.html) >. Acessado em: 15/04/2014.

**[5]** Gregoriano. Disponível em: <<http://www.gregoriano.org.br/portinha/005.htm>>. Acessado em: 15/04/2014.

**[6]** Wikipedia. Disponível em: <<http://pt.wikipedia.org/wiki/Anexo:Lista_de_TLDs>>. Acessado em: 16/04/2014.

**[7]** Hugo Azevedo. Disponível em: <<http://www.hugoazevedo.eti.br/html/nscd.html>>. Acessado em: 05/08/2014.

**[8]** Alex. Disponível em: <<http://alex.laner.net.br/?p=10> >. Acessado em: 12/08/2014.

**[9]** RNP. Disponível em: <<http://www.pop-ba.rnp.br/Site/ConfDNSSecundario> >. Acessado em: 05/08/2014.

**[10]** ISC (Internet System Conbsortium). Disponível em: <<http://lamejournal.com/2013/06/10/bind-enabling-tsig-for-zone-transfers/>>. Acessado em: 09/09/2014.

**[11]** ISC (Internet System Conbsortium). Disponível em: <<http://www.isc.org/downloads/bind/doc/bind-9-10/> >. Acessado em: 11/09/2014.

**[12]** Registro.BR. Disponível em: <[ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf](ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf%20) >. Acessado em: 16/09/2014.

**[13]** Registro.BR. Disponível em: <[https://registro.br/tecnologia/root-anchor.html](https://registro.br/tecnologia/root-anchor.html%20) >. Acessado em: 16/09/2014.

**[14]** Registro.BR. Disponível em: <[ftp://ftp.registro.br/pub/doc/dns-fw.pdf](ftp://ftp.registro.br/pub/doc/dns-fw.pdf%20) >. Acessado em: 16/09/2014.

**[15]** Registro.BR. Disponível em: <[https://registro.br/tecnologia/root-anchor.html](https://registro.br/tecnologia/root-anchor.html%20) >. Acessado em: 17/09/2014.