DNSSEC Training Course

Exercise Booklet

December 2016

RIPE NCC

RIPE NETWORK COORDINATION CENTRE

IMPORTANT

Labs environment

The labs are run on RIPE NCC's infrastructure, and consist of one server per participant. Every participant has access to a server with BIND running in a UNIX environment, with all the necessary software (shell, text editors, etc.).

For every exercise, please fill in your number from the participants list in the ovals (◯) to obtain the exact information for your environment.

For example, if your number on the list is 29, then:

www.domain◯.workshop would be www.domain29.workshop.

If your number is 7, then:

www.domain◯.workshop would be www.domain7.workshop.

To connect to the lab environment, use an SSH client (like Putty on windows or terminal on OSX), with the following details:

Host: lab.dnssec-course.net
Username: user◯
Port: 220◯ (if your number is below 10, add a zero in front of it)
Password: user◯_secret

An example for the OS X terminal is as follows:

ssh -p 220◯ user◯@lab.dnssec-course.net

Whenever you see the reversed triangle (▽) symbol in the following exercises, replace it with your number on the list.

The **password** for the lab is **user▽_secret**

Exercise A: Creating a zone file

Task: Create a zone file on paper

In this exercise, you are going to create a zone file according to the requirements.

You have a domain, which is domain___.workshop.

Fill in the blanks you find in the scheme on page 5 according to the requirements listed below:

A) Host www.domain___.workshop has IPv4 address 10.___.0.80

B) Host www-test.domain___.workshop has IPv4 address 10.___.2.80

C) Mail servers for domain___.workshop are
mx1.domain___.workshop,
mx2.domain___.workshop. and
secondary.mail.workshop. These are in order of preference.
The two internal servers have respectively
10.___.0.25 and
10.___.2.25 as IPv4 addresses, and
2001:ff___:abcd::25 and
2001:ff___:cafe::25 as IPv6 addresses.

There is a development team managing their own infrastructure, and having a delegation for the domain dev.domain___.workshop.

D) They have two nameservers:
ns1.dev.domain___.workshop and
dev-dns.domain___.workshop.
ns1.dev.domain___.workshop has IPv4 address 192.168.___.53 and IPv6 address 2001:ff___:de55::53.
dev-dns.domain___.workshop has IPv4 address 10.___.9.53 and IPv6 address 2001:ff___:9999::53.

E) The email address of the administrators of the zone file is
admins@domain___.workshop

F) www.domain___.workshop has IPv6 address 2001:ff___:abcd::80

G) www-test.domain___.workshop has IPv6 address 2001:ff___:cafe::80

H) The TTL for www-test.domain.workshop should be 3600

I) support.domain.workshop uses the same server as www.domain.workshop

J) The general TTL for the zone is 300.

K) The serial should be YYYYMMDDXX, where YYYY is the Year, MM is the month, DD is the day of the month, and XX is the number daily update. This should start from 00.

L) The name servers for the zone are
ns1.domain.workshop and
ns1.secondary-dns.workshop.
ns1.domain.workshop has IPv4 address 172.16.30. and IPv6 address 2001:ff:abcd::53

You can find the SOA Record on the next page

Host	Class	Type	DATA
www.domain[redacted].workshop.	IN		10.[redacted].0.80
www-test.domain[redacted].workshop.	IN	A	
domain[redacted].workshop.	IN	MX 10	
domain[redacted].workshop.			mx2.domain[redacted].workshop.
	IN		secondary.mail.workshop.
mx1.domain[redacted].workshop.		A	
		A	10.[redacted].2.25
	IN	AAAA	
		AAAA	2001:ff[redacted]:cafe::25
dev.domain[redacted].workshop.	IN	NS	
dev.domain[redacted].workshop.		NS	
	IN		192.168.[redacted].53
ns1.dev.domain[redacted].workshop.		AAAA	
dev-dns.domain[redacted].workshop.		A	
dev-dns.domain[redacted].workshop.	IN		2001:ff[redacted]:9999::53
		AAAA	
www-test.domain[redacted].workshop.	3600 IN		2001:ff[redacted]:cafe::80
support.domain[redacted].workshop.	IN	CNAME	
@	IN	NS	
@	IN	NS	
ns1.domain[redacted].workshop.	IN	A	
ns1.domain[redacted].workshop.			

$TTL _____

domain.workshop.	IN SOA	
		300
		300
		300
		300

Remember to either use the short name for the host, or to use the dot (.) at the end of the hostname.

Note: Instead of typing the whole domain, you can replace it with the @ sign.

Exercise B: New changes to the zone file

Task: Add/change records to the zone from the previous exercise

1) Connect to the lab environment following the instructions on page 2

nano domain/domain.conf or vim domain/domain.conf

2) Use a text editor to edit the domain file domain/domain.conf

3) Make the following modifications to the zone file:

A) Add a host called www-pre.domain.workshop with IP address 10..0.88 and IPv6 address 2001:ff:abcd::88

B) Set the serial number as the one you used in the previous exercise;

C) Add two mail exchangers for the subdomain dev.domain.workshop., which will be mx1.mail.workshop and mx2.mail.workshop.

Don't forget to add the dots at the end of host and domain names!

4) Once finished, you should save the file (ctrl+x on nano - escape, :wq on vim), and then reload named in order for the changes to take effect with the following command:

sudo /usr/local/etc/rc.d/named reload

5) Once you are ready, you can proceed to check if your domain works by moving on to exercise C.

You can check if there have been problems loading the zone file by issuing:

tail /var/log/messages

and checking the log messages from bind.

Exercise C: Using DIG to find information on DNS

Task: Use dig to find information in the DNS and answer the questions

For this exercise, you have to still be logged in the lab environment.

1) Find out the root servers in the lab (type dig without any query)

_____

2) Find out the name servers for the dns.workshop domain

_____

3) Can you find out the IPv4 addresses for www.dns.workshop ?

_____

4) Check if the secondary DNS server for your domain has updated its records (add @10.0.2.53 to the query for a SOA record), and check if the serial number matches the one you set in the previous exercise:

_____

5) If the data propagated, you can check if you can resolve the MX records for domain✷.workshop directly from your secondary server

_____

6) Check the SOA for the sync.workshop domain. (Use the +nssearch flag) Do you see anything strange?

_____

7) Check that a TCP query works and find the IPv6 address for www.mail.workshop (using the +tcp flag)

_____

8) Check the MX records for mail.workshop:

_____

Exercise D: Configure DNSSEC for the domain

Task: Generate the required keys, and configure your domain for DNSSEC and automatic key rollover

1) Connect to the lab environment following the instructions on page 2

2) Enter the directory where we will store the keys:

```
cd domain
```

3) Generate the Key Signing Key (KSK)

```
dnssec-keygen -a RSASHA256 -f KSK -b 4096 -n zone domain▽.workshop
```

4) Generate the Zone Signing Key (ZSK)

```
dnssec-keygen -a RSASHA256 -b 4096 -n zone domain▽.workshop
```

5) Change the ownership of the files so that Bind can read them, and use the keys to sign the zone:

```
sudo chown bind:bind K*
```

6) Configure bind to enable DNSSEC

```
cd ../
nano named.conf or vim named.conf
```

In the “options” section, we need to enable dnssec, adding these two lines:

```
dnssec-enable yes;
dnssec-validation auto;
```

With this change, we also enabled the server to be a DNSSEC-enabled resolver. This way we can perform DNSSEC queries through it to test if it is working.

7) In the section related to the zone “domain✷.workshop”, modify it to look like this:

```
zone "domain▽.workshop" {
        type master;
        file “/usr/local/etc/namedb/domain/domain.conf”;
        key-directory “/usr/local/etc/namedb/domain/”;
        allow-transfer { 10.0.2.53; };
        inline-signing yes;
        auto-dnssec maintain;
};
```

8) Restart/Reload Bind for the changes to take effect

```
sudo /usr/local/etc/rc.d/named reload
```

After this, you should try to check if the zone is signed by running this command:

```
$  dig RRSIG www.domain▽.workshop @172.16.30.▽
```

If the answer shows RRSIG records, then it means the zone is being signed by Bind.

9) Generate the DS records and input them in the domain interface by connecting with a browser to http://lab.dnssec-course.net
Log in using the same user name and password you used for the lab.

You first have to identify which one is the Key Signing Key for your domain:

```
$ cd domain
$ grep "key-signing" K*
KdomainX.workshop.+010+08763.key:; This is a key-signing key, keyid 8763, for
domainX.workshop.
```

Then you can proceed to extract the DS records.
Copy the file name of the key, without the “.key” extension.

Copy and paste this part from the output:

Kdomain▽.workshop.+010+08763
(The numbers will be different for you, this is just an example)

Now paste it and use it to launch **dnssec-dsfromkey**:

```
$ dnssec-dsfromkey Kdomain▽.workshop.+010+08763

domainXX.workshop. IN DS 8763 10 1 DB8079B2D667C4A4F9D39C91C72548C1EC183965
domainXX.workshop. IN DS 8763 10 2
567797EDE2E1C305ABB8AAF490E76744A84763CB0B67FC08B753D4CB6ACBEB54
```

Just copy the text you got as an answer and paste it into the web interface:

- Make sure you copy the key tag correctly. It's the first number after "DS" (It's the same for both entries);
- Choose the correct algorithm. (8);
- Choose the correct digest type (1 for the SHA1 hash, 2 for the SHA256 hash).

These are just the records to put in the web interface, as you would do with any domain registrar that supports DNSSEC.

Remember: Even if your zones are signed, DNSSEC will not be enabled until you supply the DS records to your registrar! This is what you are doing right now.

To test if your zone is now correctly signed, you can try running the following commands:

```
$ dig +dnssec A www.domain▽.workshop
```

The answer should contain the AD flag. If it doesn't try waiting for the TTL to expire, and then retry.

You can also try using Drill, as in this example:

```
$ drill -S www.domain▽.workshop
```

Which gives you a full output of the validation of the record.

Exercise E: Check and troubleshoot DNSSEC

Task: Use dig, drill and delv to verify DNSSEC and troubleshoot broken implementations

For this exercise, you have to still be logged in the lab environment. For dig, remember to always use the +dnssec flag in every query.

1) Check the RRSIG records for nic.workshop

_____

2) Launch “drill -S mx1.secondary-dns.workshop”. What do you see ?

_____

3) What is the key ID for the keys of secondary-dns.workshop ?

_____

4) And what is the algorithm used for them ?

_____

5) What type of RRSIG can you see if you run a query for the A record for www.broken-dnssec.workshop? If you can’t see it, try with the +cdflag

_____

6) Why do we have to use that flag ? What is the problem ?

_____

7) Can you try running the same query with drill, using the -S flag ?

_____

8) And what about with delv, with the +vtrace flag ?

_____