OPS535 Lab 6

Purpose

In this lab you will learn to configure a DNS server to provide responses authenticated with DNSSec, first by querying other servers for their DNSSec records, then by adding DNSSec records to your own zones.

Pre-Requisites

Labs 1 through 4 should be complete so that your machines have functioning network connections between each other, and to the outside world. You also need a functioning DNS domain (configured in lab 3) in order for mail to be properly transported between your machines (and potentially other domains).
.

Investigation 1: Performing queries using DNSSec

Perform the following steps on your VM2

1. Ensure you have the bind-utils package installed.

2. Run the command dig senecacollege.ca
    - You should get output similar to the following:

```
>dig senecacollege.ca @1.1.1.1

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> senecacollege.ca @1.1.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12758
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;senecacollege.ca.            IN    A

;; ANSWER SECTION:
senecacollege.ca. 564   IN    A     205.207.147.230

;; Query time: 34 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Sun Nov 04 17:31:57 EST 2018
;; MSG SIZE  rcvd: 61
```

    - If you did not get the expected output, go back and ensure your machine has network connectivity (including an assigned default route).

3. Once you have a response, can you be sure it is accurate?
    - Re-run the previous dig command, but this time add +dnssec to request authentication of the results using DNSsec.

```
>dig senecacollege.ca @1.1.1.1 +dnssec

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> senecacollege.ca @1.1.1.1
+dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38472
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1452
;; QUESTION SECTION:
;senecacollege.ca.            IN    A

;; ANSWER SECTION:
senecacollege.ca. 285   IN    A     205.207.147.230

;; Query time: 42 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Sun Nov 04 17:36:36 EST 2018
;; MSG SIZE  rcvd: 61
```

    - Notice the addition of the do flag (DNSSec Ok, that is the server we queried is willing to perform authentication), but no other difference in the output. This information is **not** authenticated.

4. Now we will run a query that does get authenticated:
    - Run the following command (again you should get output similar to the following):

```
>dig isc.org @1.1.1.1 +dnssec

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> isc.org @1.1.1.1 +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51709
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1452
;; QUESTION SECTION:
;isc.org.                IN    A

;; ANSWER SECTION:
isc.org.          60    IN    A     149.20.64.69
isc.org.          60    IN    RRSIG A 5 2 60 20181128233334
20181029233334 19923 isc.org.
evUIhl3hmTGFchNe8GH7NDgMQS56fdgFgQy/BBqbE+zu0TXEVPLLsGxz
pAEnYJq+0gTTa/nJjIMmxxsXj7HNZ+gpL8koGNRJeZDt/Q4jmfcRh+A7
HJOn1LVpjwdzw459XF38mQmwBK7oh6ZTBg0UKzaw4J6zr5vql9KWoyJV KCo=

;; Query time: 31 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Sun Nov 04 17:42:44 EST 2018
```

```
;; MSG SIZE  rcvd: 219
```

- Notice that in addition to the do flag, the answer to this query also has an ad flag (authenticated data), along with extra information in the answer itself (the RRSIG record). This result **is** authenticated.
- If you want to see this result without the DNSSec information, simply rerun the query without the +dnssec request.

Investigation 2: Configuring DNSSec on a Recursive Server

Perform the following steps as root on your VM1

1. Now that you can spot the differences between authenticated and non-authenticated data, it is time to configure your local DNS server to perform authentication when your client machines request it.

2. Simply set the dnssec-validation parameter in your /etc/named.conf file to yes (it is already set this way if you didn't change it in an earlier lab).
   - Note that this relies on your server also having the initial key it will use to authenticate the root name servers it communicates with.
   - This can be found in /etc/named.iscdlv.key and /etc/named.root.key.
   - These too are included by default when you first install bind. If they are not there, add the following lines to your options statement and restart your service:

```
bindkeys-file "/etc/named.iscdlv.key";
include "/etc/named.root.key";
```

3. Make sure your dns server is configured to be provide recursive answers to other machines in your network, and that it will allow traffic to tcp port 53.
   - All of this should have already been done, so long as you followed the instructions in previous labs, and didn't deliberately break anything.

4. Run the following command from one of your other VMs (making sure to use the ip address of your own DNS server):

```
>dig +tcp +dnssec @192.168.83.1 www.isc.org
```

   - You should get output similar to the following.

```
; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> +tcp +dnssec
@192.168.83.1 www.isc.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13512
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL:
13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
```

```
;; QUESTION SECTION:
;www.isc.org.                IN    A

;; ANSWER SECTION:
www.isc.org.           60    IN    A     149.20.64.69
www.isc.org.           60    IN    RRSIG A 5 3 60 20181128233334
20181029233334 19923 isc.org.
EzPGoD0DDKUONuWUhXsNqW0xt1q3l8Nwg8Ec3SW9QZafwyQDYj9/dZ/F
d4ch3UIQ1oKfHYUtAsev7aVjwbisM5HgHSjGtBMWZngzY/mBTmy+uVog
yBKuXHawR13il4fY6Z68qTZpaq8gH9jKqpPJYomruSxYFZVAI8Ct+tBB 0SE=

;; AUTHORITY SECTION:
isc.org.          6575  IN    NS    ord.sns-pb.isc.org.
isc.org.          6575  IN    NS    sfba.sns-pb.isc.org.
isc.org.          6575  IN    NS    ams.sns-pb.isc.org.
isc.org.          6575  IN    NS    ns.isc.afilias-nst.info.
isc.org.          6575  IN    RRSIG NS 5 2 7200 20181128233334
20181029233334 19923 isc.org.
IzXvpUxVCC15yG74ChGSlUgNOAPtvb6688zZm97SYSB6772gzS09VhmR
WfpdOx5IJFwhhIl87bB49yiEHP4SimMrAfoAmGIpe5G4hI8uirhGlWNM
Rh6SVIMSXdPMCKF8pSqe387ERK9ZcEPfVVTxeA+/C0Ajyg+KhrwbS4A6 3wU=

;; ADDITIONAL SECTION:
ams.sns-pb.isc.org.     85775 IN    A     199.6.1.30
ams.sns-pb.isc.org.     85775 IN    AAAA  2001:500:60::30
ord.sns-pb.isc.org.     85775 IN    A     199.6.0.30
ord.sns-pb.isc.org.     85775 IN    AAAA  2001:500:71::30
sfba.sns-pb.isc.org.    85775 IN    A     149.20.64.3
sfba.sns-pb.isc.org.    85775 IN    AAAA  2001:4f8:0:2::19
ams.sns-pb.isc.org.     7200  IN    RRSIG A 5 4 7200 20181128233334
20181029233334 19923 isc.org.
fN6lhMQKcNsl889c8e0n7b0xBLWHnp9oLUn8ji4T7sNykobHObfihcvL
LpX2DGqVKUW/9kIe5hvikVNfiDxjZx89V6jMnhyavSsJdchyv3zuEedx
pFa8Kq9y28Na+/7v+3eCVp/L0SRx1na88bxiFpLpIk1aIV5pAthgtQSH 9hY=
ams.sns-pb.isc.org.     7200  IN    RRSIG AAAA 5 4 7200 20181128233334
20181029233334 19923 isc.org.
mvlEcSyHnq/O1B8+awGkUPp3+G+QOHf5Vdeq+vhReo+um8Jg8aks3uYy
CMZjC/NAtFPNUzjTyDtirn79/lDan3GgwpICHvWq2DHCslp7hbZC7qRs
cFQjstONnLcprPS5q8T1TRFs97SuqTS7OK4B3f0Lf0ilC+ohOYQR/1bW Fg8=
ord.sns-pb.isc.org.     7200  IN    RRSIG A 5 4 7200 20181128233334
20181029233334 19923 isc.org. ZPsHODiOXBRsXN3K1Al/Nq+
+dkx0HMaUpSdEMLXwlcASrC8FWjKETiRS
NhgXq1u+JiBkXTEWVsR81CSk2uFEAxMlWOfoIKKVnc9Hp7ZNjdHlgIWe
bLWGweMoCwGa6o6yuRqMjCrceDqTKQSq1RTvQRL3As9J1V4vMY5i+KQy IhY=
ord.sns-pb.isc.org.     7200  IN    RRSIG AAAA 5 4 7200 20181128233334
20181029233334 19923 isc.org.
usTQJB2VfLzzfA3TPWTUXiSKM3w7bfK6zGQf1t+LXdJBDLLrjvhmwWTp
5DjLDIxIvd77mudcFQsXq7oVvmiJHmnA6zaJhF6cFAIKI7dJm5rGhGFs
ZkX7OD4x5LxDH1knah7AYTPdme+QDxcLzIsmY5iozQeMh3UKd+gfpork RqI=
sfba.sns-pb.isc.org.    7200  IN    RRSIG A 5 4 7200 20181128233334
20181029233334 19923 isc.org.
ryZ18IlvB7q/qPwIFHgLU7LSjnTBx3JpzpV2BQtb/2jdDM7zBQ/bnQ28
/H+MSWoAAKmPEiND2XWqtvdCPwOv4kcQexcTnLoIfieq6HgraO8//AIL
wMmwUBgZc51tZ1e+k9krCvNlLKZXe92KgGYWwGNxp3Gp1TkdlywRtMUM Y9w=
sfba.sns-pb.isc.org.    7106  IN    RRSIG AAAA 5 4 7200 20181128233334
20181029233334 19923 isc.org.
betjxdRZREj3fMHm7TsE7kn8vrZHRdpzrkJ3mxIe4jdhyUbQytxcIfnJ
aTOz5JT5ESF5n7k/pq+UK05ApZFc5b5slX0g5S/ahYm7ynLzz/Uw8/sW
UrPFePNdAxS00mX91rRYG7tVLHq79VOvIt18C69ac+oVGVfIBN/OJzan /gE=
```

```
;; Query time: 85 msec
;; SERVER: 192.168.83.1#53(192.168.83.1)
;; WHEN: Sun Nov 04 18:18:23 EST 2018
;; MSG SIZE  rcvd: 1623
```

- Again, note the do and ad flags, along with the RRSIG record (and similar data for the nameservers in the isc.org domain).

Investigation 3: Configuring DNSSec on an Authoritative Server

Perform the following steps as root on your VM1

1. Now that you know your nameserver is capable of performing authentication of other domains (so long as they are configured to provide authentication), it is time to set up authentication in your domain.

2. First make sure that the SELinux boolean named_write_master_zones is still set to allow the service to make changes in the zone files (this should have already been done in a previous lab).

```
> getsebool named_write_master_zones
named_write_master_zones --> on
```

   - And that named has write permission to the /var/named directory

```
> ls -ldZ /var/named
drwxrwx---. root named system_u:object_r:named_zone_t:s0 /var/named
```

   - If either of those are not configured, go back and fix them.

3. Install the haveged service to generate random values for your system.

   - It can be found in the epel-release repo. Install that if you have not already done so.
   - You would not have to use this service on a 'real' server, but our VMs will not have enough activity to provide normally random data within a reasonable time-frame.
   - Start, but do not enable haveged service, as we will not need it on a regular basis. Anytime you need to re-generate the random keys from the next step, simply start the service.

4. Next, we will use the dnssec-keygen command to generate two sets of paired keys.
   - Create a directory at /etc/named/<yourdomain>-keys
     - Making sure you replace <yourdomain> with the name of your domain.
     - Make sure it has that only root and the named service user can access it.
     - cd into it, then run the dnssec-keygen commands below.

   - First, to generate the Zone Signing Key (ZSK) that is used to sign individual records (make sure to use your own zone name):

```
dnssec-keygen -a RSASHA256 -b 1024 <yourzone>
```

- And to generate the Key Signing Key (KSK) that is used to create an RRSIG for your DNSKEY (the public half of the ZSK):

```
dnssec-keygen -a RSASHA256 -b 2048 -f KSK <yourzone>
```

- Note that the algorithm and number of bytes used here are current standards, but may change over time.
- Change the permissions on those files so that only root and the named service can read them.

5. There are three parameters for bind that need to be set in order to sign your zones. The first two could be set in the options statement, but the third is only acceptable in a zone statement. Our machines only have two zone statements (the forward and reverse lookups of your domain), so it won't make a significant difference where we place them. If your server hosted multiple domains, the placement of these parameters would be something to consider:
   - Add the following lines to your two zones (again replacing <yourdomain> with the name of your domain):

```
key-directory "/etc/named/<yourdomain>-keys";
inline-signing yes;
auto-dnssec maintain;
```

   - Double check that the value you put in the key-directory parameter matches the directory you created your key files in.

6. Make sure the dnssec-enable parameter in /etc/named.conf is set to yes so that your server will provide the extra DNSSec records if a client requests them.
   - This is the default value, so unless you took it out, it should already be there.
   - Note that this parameter is different from the dnssec-validation parameter which only controls whether or not your server will request those records from other servers when a client asks for them.

7. Restart the named service. If you have dynamic DNS set up from the earlier labs, you can use named-journalprint to view the journal files for your zones in order to see the new records.

8. In order to confirm that your server will provide the extra records when requested, use the dig command to obtain a zone transfer (including the DNSSec records) from your server:
   - Making sure to replace <yourzone> with the name of your zone, and <ip-of-server> with the ip address of your server.

```
dig AXFR <yourzone> @<ip-of-server>
```

9. Normally, there would be a few more steps here to create an encrypted copy of your ZSK to provide to your parent zone as a DS record, but we will not be configuring that in this lab.
   - Note that this means responses your server provides will not be 'authenticated data', and will not have the ad flag.
   - You will be performing this final step in the next assignment.

Completing the Lab

Your DNS server is now capable of performing recursive queries using DNSSec when client machines request it. It has also been configured to provide the extra DNSSec records when clients request them. Note that it is not yet truly providing DNSSec answers, as it is not being authenticated through the domain above yours.

Follow the instructions on blackboard to submit the lab.