AfNOG 2003 Kampala, Uganda
Track 1 – Scalable Internet Services
Domain Name System – Exercise 3

Setting up a Caching-Only Name Server on a FreeBSD System

Enable named on your computer by following the steps below:

1. Using vi or your favorite text editor, edit the `/etc/rc.conf` file and add the lines in bold below. This will automatically start the named daemon during the boot process.

```
 # vi /etc/rc.conf

# -- Add the following lines to enable bind -- #
named_enable=”YES”
named_program=”/usr/sbin/named”
```

2. Save and exit the `/etc/rc.conf` file.

We will now configure the caching-only name server.

3. Create the `/etc/namedb/named.conf` file and make the following entries are in the file.

```
options {
      directory "/etc/namedb";
      recursion yes;
};

zone "." {
      type hint;
      file "named.root";
};

zone "0.0.127.IN-ADDR.ARPA" {
      type master;
      file "localhost.rev";
};
```

4. Save and exit the file.

In the following steps we will create the zone files for the localhost (127.0.0.1).

5. Change directory to `/etc/namedb`.

```
# cd /etc/namedb
```

6. Run the make-localhost script to create the `/etc/namedb/localhost.rev` zone file.

```
# sh /etc/namedb/make-localhost
```

Before starting the named daemon:

7. First check if named is running by issuing the following command.

```
# ps –aux | grep named
```

If the daemon is running you should get a response like the one below.

```
root     129  0.0  2.0  3880 2352  ??  Ss   Tue10PM   0:11.52 /usr/sbin/named
```

8. If the daemon is not running, start the BIND daemon with the following command.

```
# /usr/sbin/named
```

9. Check if named is running by issuing the following command.

```
# ps –aux | grep named
```

10. Check the log file for errors. The logs can be found in `/var/log/messages`

```
# grep named /var/log/messages
```

11. If any "named" errors are found in the log file fix them and start the named daemon again. Started without errors it looks like this

```
Jun 12 10:42:04 inst named[11614]: starting (/etc/namedb/named.conf).  named 8.3.4-REL
Thu Apr  3 08:26:42 GMT 2003     root@freebsd-
stable.sentex.ca:/usr/obj/usr/src/usr.sbin/named

Jun 12 10:42:04 inst named[11614]: limit files set to fdlimit (1024)

Jun 12 10:42:04 inst named[11631]: Ready to answer queries.
```

12. To restart the named daemon, type the following commands.

```
# ndc restart
```

13. Check the logs again to ensure there are no errors. Repeat this till named starts with no errors.

14. Check the version of BIND you are running by entering the following command.

```
# /usr/sbin/named -v
```

Question: What version of BIND are you running?

Ans:______________________________________

At this stage we now have a working caching-only name server.

15. We will now test the cache-only name server. To do this first edit the `/etc/resolv.conf` file to ensure that only your server does the resolving.

```
    # vi /etc/resolv.conf
```

The `/etc/resolv.conf` file should look like the text below after editing it. Save the changes.

```
nameserver     127.0.0.1
```

16. Test if your server is resolving using BINDs "dig" tool.

```
    # dig t1.ws.afnog.org
    # dig ws.afnog.org
    # dig afnog.org
```

17. Tick the domains for which you got authoritative answers.

afnog.org
ws.afnog.org
t1.ws.afnog.org

18. Repeat the commands in step 16 again and make a cross by the domains for which you did NOT get an authoritative answer.

Question: **Explain what happened with the second set of queries in step 18.**

Answer: ____

19. Flush the DNS cache on your caching-only name server by typing the following command.

```
    # ndc restart
```

20. Repeat step 16 again.

21. Compare the results with the two results you had in steps 16 & 18.

Question: List the domains tested in step 21 that returned an authoritative answer?

Answer: ____

22. To check what is in your nameservers cache, type the following command.

```
# ndc dumpdb
```

A file `/etc/namedb/named_dump.db` will be created with the contents of your nameservers cache.

23. To view the contents of the file.

```
# vi /etc/namedb/named_dump.db
```

Note: The caching-only server as configured above will allow any machine on the Internet to use it as a resolver, i.e. an open caching-only name server.

24. To restrict access to your caching-only name server, add the **`allow-query`** directive to the options section of the `/etc/namedb/named.conf` file.

```
options {
      directory "/etc/namedb";
      recursion yes;
      allow-query { 127.0.0.1; 81.199.110.#; };
};
```

Note: The **`allow-query`** directive accepts IP addresses written in CIDR format i.e. **`10.0.1.0/24`** or **`192.168.1.0/25.`**

25. Ask a colleague to try using your server to resolve a domain name. Your colleague should type the following command.

```
# dig @81.199.110.# <some domain> a
```

Where # is the number of your PC.

Question: Was he/she able to resolve using your caching-only server? And why?

Answer: ________________________

26. Restart the named daemon.

```
# ndc restart
```

27. Repeat step 25.

Question: Was he/she able to resolve using your caching-only server?

Answer: ________________________

Question: What is the status of that query?

Answer: ______________________

Congratulations you have just built a caching-only server, and you also know how to restrict access to it.

Optionally view the recursion process using tcpdump.

Open two command line windows. In the first window type the following command (as root).

```
# tcpdump –i fxp0 –n udp port 53
```

In the second window type the following command.

```
# dig @noc.ws.afnog.org < some domain > a
```

Go back to the first window and view the output.