Unix for Telecommunications

Portfolio Task – P-Lab-03-Bind
Pass Level Task

I. INTRODUCTION

In this lab you will configure your RULE host to become a DNS (Domain Name Service) server. The program that will be used to provide the DNS service is BIND (Berkeley Internet Name Domain), occasionally also referred to as `named`. BIND will be configured and run on your RULE host, then used by your RULE host to query and observe some interesting DNS behaviour. Once you have completed your lab, you will have created a new top level domain (`.unix`) that sits alongside the existing top-level domains (eg. `.com`, `.org`). This new domain will be available to anybody that uses your RULE host as a DNS server.

II. PURPOSE

To gain and/or enhance the following practical skills:
- Deploying and configuring BIND to provide DNS service
- Configuring BIND as a forwarding DNS server
- Creating a new top level domain and configuring forward and reverse zone files
- Understand issues relating to service configuration
- Process and respond to error messages in log files
- Configure services to auto-start in Unix

III. PREPARATION

You can prepare for this lab by reading some of the BIND documentation. You should also review the basic concepts of:
- What is the purpose and function of DNS
- What is DNS used for
- How hierarchical system functions
- What protocol/port numbers that DNS uses

IV. METHODOLOGY

A. Preliminary investigation

1) Explore the functionality of the `nslookup`, `host` and `dig` commands.
2) Issue the commands

   ```
   nslookup www.swin.edu.au
   host www.swin.edu.au
   dig www.swin.edu.au
   ```

3) What is your output and what does it tell you?
4) What is the IP address of the Swinburne name server (DNS Server)?
5) Issue the command
   ```
   nslookup 136.186.229.16
   ```
6) What is returned? What does this tell you about the functionality of a DNS Server?
7) Issue the command
   ```
   nslookup labbind.unix
   ```
8) What is returned? Why? What does this mean?

B. Configuring the DNS Client

1) How does your RULE host know which DNS Server to use? (Hint: `man resolv.conf`)
2) What do each of the lines in this configuration file represent?
3) Changing the contents of this file is equivalent to doing what under Windows?
4) Configure your RULE host to use itself as a DNS server. (Hint: Use your rule hosts IP address as the DNS Server entry)
5) Do the previous `nslookup`'s you were asked to do work? Why/Why not?

C. Configuring the DNS Server

1) The BIND configuration information is stored in `/usr/local/etc/namedb/`. Examine the files in this directory.
2) Make a backup copy of the BIND configuration file (`named.conf`) Why do we do this?
3) Edit `named.conf` and make the following changes:
    - Comment out (add "//" to the beginning of the line) that reads

      ```
      listen-on { 127.0.0.1; };
      ```

    - Uncomment the section (remove the "/*" and "*/") that reads

      ```
      forwarders {
          127.0.0.1;
          };
      ```

    - Replace the `127.0.0.1` with the IP Address of one (or more) of Swinburne's DNS Servers (found earlier in the lab).
4) What is the purpose of the forwarders section of the `named.conf` file? (Hint: `man named.conf`)
5) At the very bottom of the file, under the section about zones, uncomment and remove/modify text so that it now reads

    ```
    zone "unix" {
        type master;
        file "unix";
    };

    zone "230.186.136.in-addr.arpa" {
        type master;
        file "230.186.136.in-addr.arpa";
    };
    ```

6) What is the purpose of the `zone` section, what does it represent in the DNS server?
7) Consider the *zones* section towards the end of the file. A number of zones are all configured to use the `empty.db` zone database file. What does this achieve?

D. Creating the DNS Database Files

1) Create the file `/usr/local/etc/namedb/working/unix` with the following contents (where **xx** is the number of your RULE host):

    ```
    $TTL 86400

    unix. IN SOA ns1.unix. admin.unix. (
                    2008070101 ; Serial
                    10800      ; Refresh
    ```

```
                         3600        ; Retry
                         604800      ; Expire
                         86400 )     ; Minimum TTL
    ; DNS Servers
    @           IN  NS      ns1.unix.

    ; MX Record
    @           IN  MX  1   ns1.unix.

    ; Machine Names
    localhost  IN  A      127.0.0.1
    ns1        IN  A      136.186.230.xx
    labbind    IN  A      136.186.230.xx
    labnmap    IN  A      136.186.230.21
```

2) Create the file `/usr/local/etc/namedb/working/230.186.136.in-addr.arpa` with the following contents (where **xx** is the number of your RULE host):

```
$TTL 3600

230.186.136.in-addr.arpa. IN SOA ns1.unix. admin.unix. (
                 2008070101 ; Serial
                 10800       ; Refresh
                 3600        ; Retry
                 604800      ; Expire
                 86400 )     ; Minimum TTL
    ; DNS Servers
    @           IN  NS      ns1.unix.

    ; Machines
    xx          IN  PTR     ns1.unix.
```
`21` ~~35~~   `IN  PTR     labnmap.unix.`

E. Starting BIND

1) Run `sockstat -4` and note the output.
2) Start BIND using the command `named`
3) Rerun `sockstat -4`. What does the output mean? What is the PID of your BIND server?
4) Test your DNS server by running (where **xx** is the number of your RULE host)

```
nslookup www.swin.edu.au
nslookup localhost.unix
nslookup ns1.unix
nslookup labbind.unix
nslookup labnmap.unix
nslookup 136.186.230.21
nslookup 136.186.230.xx
```

5) If some of these tests fail you will need to make changes to the configuration.
   Note: *You **MUST** stop and restart named for it to use your new configuration settings. It is essential that you kill the running DNS server and start a new server running.*

F. Automatically Starting BIND at System Boot

1) Once a service is properly configured and running, we often want to:
   - Start it automatically at boot-time, in case the system is rebooted for whatever reason
   - Enable starting/stopping/restarting the service via the use of the rc scripts – this simplifies the procedure and ensures that any dependent servers are also started if required

2) To configure both these tasks you need to edit the `/etc/rc.conf` file and add the lines:

   ```
   named_enable="YES"
   named_chrootdir=""
   ```

   The second line is required as named cannot be run chrooted from within a jailed host environment (your rule host is a BSD jailed host)

3) Stop the currently running BIND service by issuing the command:

   ```
   killall -9 named
   ```

4) You will now be able to start and stop BIND using the command:

   ```
   /usr/local/etc/rc.d/named <start|stop>
   ```

V. ASSESSMENT

The due date for completion of practical work is **11:00pm**, exactly **six** days after your scheduled class.

Note: *The nominated submission day/time holds regardless of whether that day is a non-teaching day or public holiday*

A. Self Assessment

You can self-assess your progress at any time via the marking script available at http://ruleprimary1.caia.swin.edu.au

B. Completion of task in Doubtfire

Download the PDF output of the marking script from http://ruleprimary1.caia.swin.edu.au and submit it to Doubtfire. Your tutor will confirm completion of the lab by examing the rule marking log files on the rule server.

If you complete the task during class beforehand, you may demonstrate completion in class to your tutor.

Note: *The downloaded PDF is not evidence of successful completion of the lab, it is a document to demonstrate completion within your portfolio. Your tutor will assess the evidence via either direct confirmation via the marking script or via the log files generated when you run the marking script*

C. Tutor Discussion

In order for the submission to be marked as complete, you must discuss your work with the tutor