

DNS

Module 6 | Activity 1



Introduction

In this activity, you will learn how to configure and use your own DNS server. Up until now, you have been using the default ISELab server at 199.100.16.100 which is an IP-address that should seem familiar by now. Without DNS, you will have a hard time trying to access websites over the internet. During the cyber defense competition, your team may be required to configure a DNS server, or it might be provided to you. It all depends on the CDC scenario.

After the slideshow, are you still a little confused when it comes to the topic of DNS?

Do not worry! You will have a better understanding after this activity. For now, just look at DNS as a look up server for our contact book.

Think about the following example. It is hard to remember all your friends' phone numbers, but it is much easier to remember their names. DNS works in the same way as getting your friends phone number by looking up their name in your contact book.

Let's Get Started!

Note: In this activity spacing matters. Keep that in mind while editing files.

A. Installing bind9

- Before you begin you need to install bind9, use command **sudo apt install bind9**.

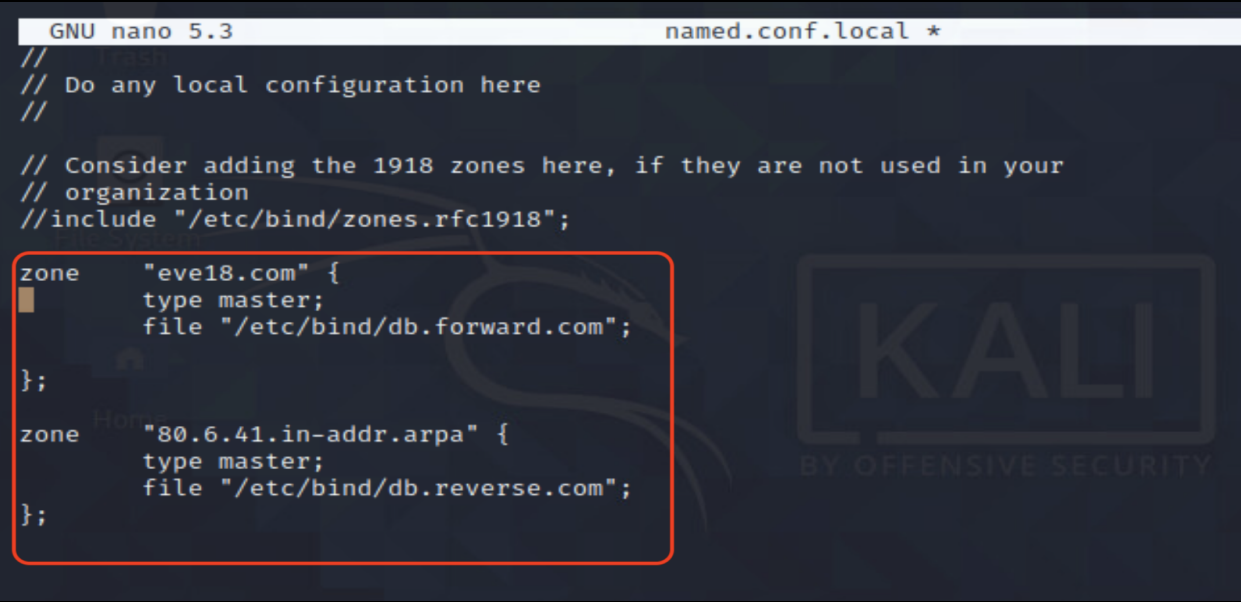
*If you receive a network connection error, run the three exports commands used in the network set-up activity.

- Navigate to the **/etc/bind/** directory. Use **cd /etc/bind**. This is where most of the files that we need to configure are located. Issue the **ls** command to see everything that is in here.

- You will also probably notice that most of the file names are prefixed by the word "named". This is because "named" is only one of the parts of the BIND package.

- Now, open the **named.conf.local** file with a text editor: **sudo nano named.conf.local**

- Include the following forward and reverse lookup-zones within your own file.



```
GNU nano 5.3                                named.conf.local *
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone     "eve18.com" {
type master;
file "/etc/bind/db.forward.com";
};

zone     "80.6.41.in-addr.arpa" {
type master;
file "/etc/bind/db.reverse.com";
};
```

- Once you have saved your changes, issue the **ls** command once again under the **/etc/bind** directory.

B. Creating New Files

You will need to create two new files called **db.forward.com** and **db.reverse.com**.

- Create these files by copying from the **db.local** and **db.127** files, respectively.

Issue commands:

```
cp db.local db.forward.com
```

and

```
cp db.127 db.reverse.com
```

- Your directory should now look like this, with the two new files included.

```
(wall-e@Mailey)-[/etc/bind]
$ ls
bind.keys  db.127  db.empty  db.local  named.conf  named.conf.local  rndc.key
db.0       db.255  db.forward.com  db.reverse.com  named.conf.default-zones  named.conf.options  zones.rfc1918
```

C. Editing db.local file

- We're going to edit the **db.local** file, open it with a text editor and make the following changes, denoted by the red "boxes".

Basically what's happening here is that we are creating the forward resolution for this new name server. So that we will be able to obtain the IP-address if we enter a domain name.

Whereas, a reverse resolution file would help the nameserver obtain the domain name given the IP-address.

Forward: Domain name → IP-Address

Reverse: IP-Address → Domain name

- Before you save and close the file you must remember that you will use your own virtual machine IP-Address instead of the one listed below which is "41.6.80.2".

- You may need to use the **chmod 777** command to change the file permission in order to edit and save the file.

- Replace the IP-Address within the **ns** and **server** rows with your own.

```

GNU nano 5.3 db.forward.com *
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA ns.eve18.com. root.localhost. (
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS ns.eve18.com.
ns IN A 41.6.80.2
server IN A 41.6.80.2
www 3600 IN CNAME ns.eve18.com.

```

D. Editing db.reverse.com file

- Now we will edit the **db.reverse.com** file in a similar manner. Open this file up with the text editor nano. Nothing too wild going on here. The number 2's in the right-most column should be replaced with your own fourth digit in your IP-Address.
- Save and exit.

```

GNU nano 5.3 db.reverse.com *
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA ns.eve18.com. root.localhost. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS ns.
2 IN PTR ns.eve18.com.

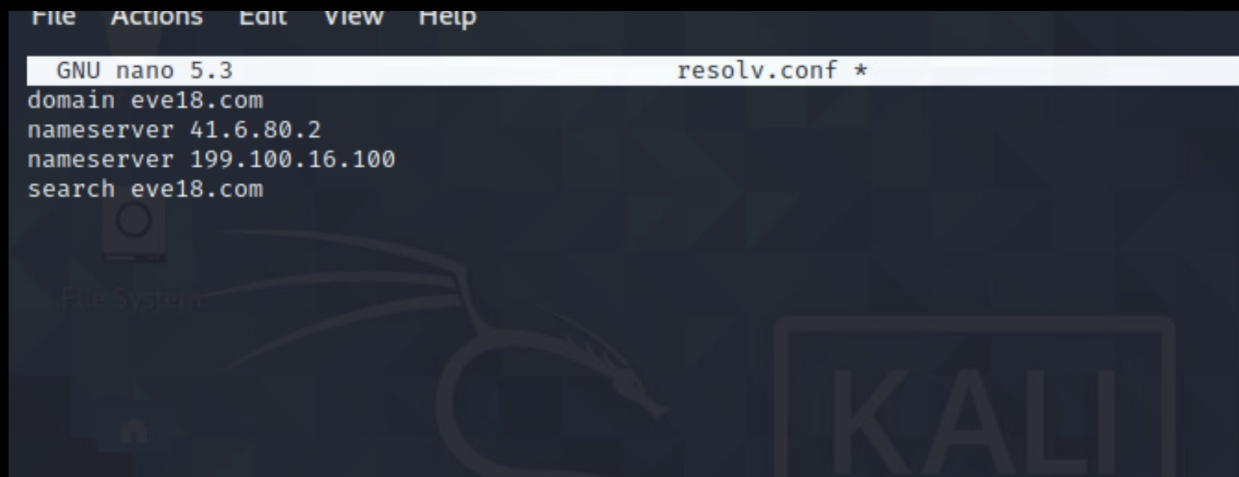
```

F. Configuring Nameserver

- Now we need to configure the nameserver that our machine points to: **sudo nano /etc/resolv.conf**

Add in the new lines and type in your own IP-Address, in place of "41.6.80.2"

The old name server needs to be left in there as an upstream server.



```
File Actions Edit View Help
GNU nano 5.3 resolv.conf *
domain eve18.com
nameserver 41.6.80.2
nameserver 199.100.16.100
search eve18.com
```

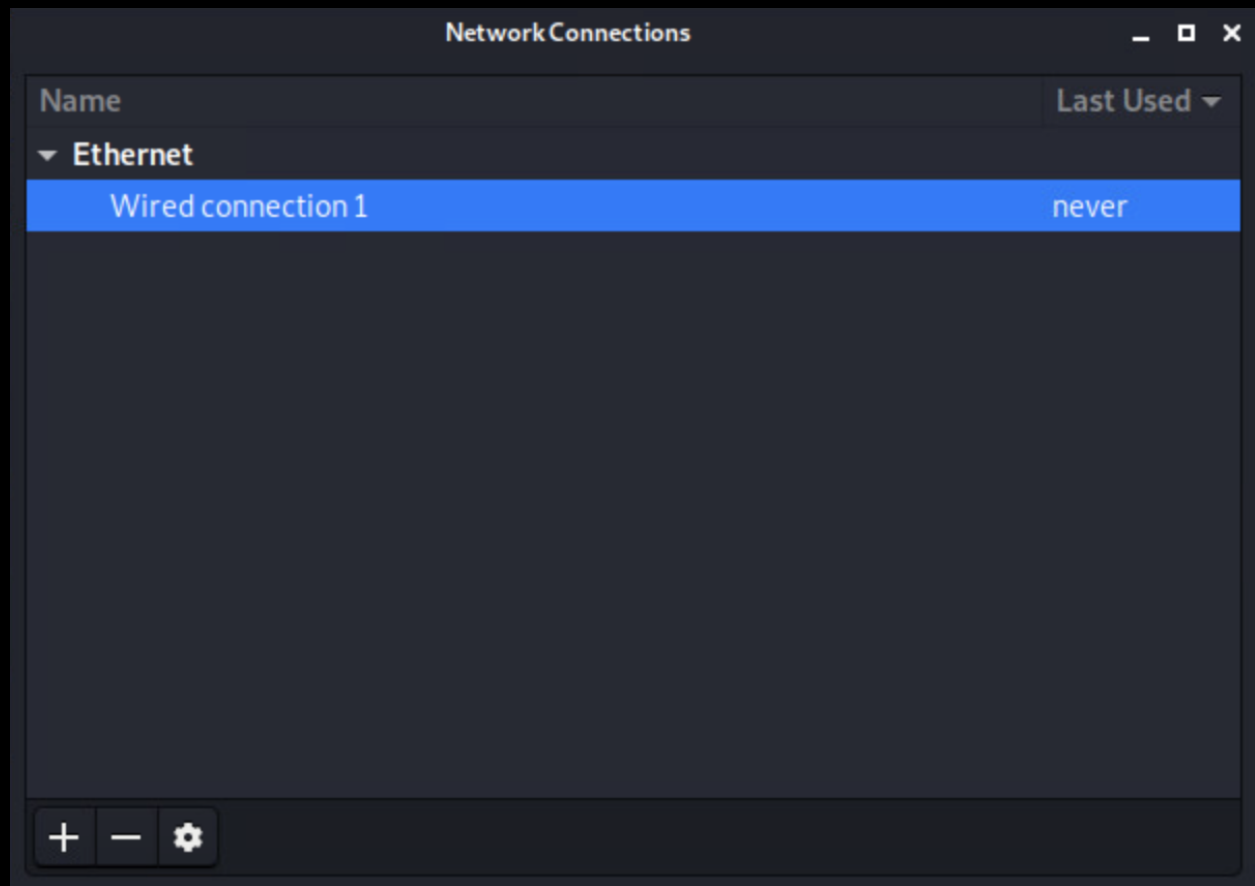
G. Making Changes to Connection Settings

- Finally one of the last steps is going to be making some changes to the wired connection settings of your Kali machine.
-Right click on the small rectangle shaped icon in the top right corner of your desktop and you should be able to click on the Edit Connections option.

- This is what it should look like from the desktop.



Select the Wired connection 1 option and click the small gear at the bottom.



- Under IPv4 settings and the Additional DNS servers field write in the address of the DNS server you just configured, before you click save and exit.

Editing Wired connection 1

Connection name: Wired connection 1

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: Automatic (DHCP)

Additional static addresses

Address	Netmask	Gateway

Add Delete

Additional DNS servers: 41.6.80.2

Additional search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

H. Starting Your DNS

- To start your new DNS server and ensure that it is running correctly run the following commands: "**service named start**" and "**service named status**". You should receive the following output.

```
(wall-e@Hailey)-[~]
$ service named status
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2021-06-21 15:54:44 CDT; 2h 4min ago
     Docs: man:named(8)
    Main PID: 1212 (named)
      Tasks: 5 (limit: 2309)
     Memory: 25.9M
    CGroup: /system.slice/named.service
            └─1212 /usr/sbin/named -f -u bind
```

- Now that we can confirm the DNS service is running, Try running some forward and reverse DNS-queries. A forward query would look something like: **nslookup iastate.edu** A reverse query would be: **dig -x [IP-Address] +noall +answer**

These queries should resolve and output something similar to what is seen below.

```
(wall-e@Hailey)-[/etc/bind]
$ dig +noall +answer -x 129.186.90.84
84.90.186.129.in-addr.arpa. 13923 IN PTR redirect.its.iastate.edu.

(wall-e@Hailey)-[/etc/bind]
$ nslookup iastate.edu
Server:          199.100.16.100
Address:         199.100.16.100#53

Non-authoritative answer:
Name:   iastate.edu
Address: 129.186.90.84
Name:   iastate.edu
Address: 2610:130:108:480::81ba:5a54
```

- If you receive any sort of error at this point go back and check the spacing and content of the files that you edited in this activity. It might just be a simple typo :)