# CS 473: Network Security – Section 2 Setup

---

**Guidelines:**

*Please download the zipped image file for your VM from* the link given below.
*https://drive.google.com/drive/folders/1V0giZb0HEQtTPD6cAM8Emp9bKFpTTMDh*

***please use Virtual Box 6.1.32.***
In your task, you will be exploring various DNS attacks for which you will have to set up your local DNS server.

---

## Step 1: Setting up the VMs

For this part, you would have needed three distinct machines (DNS Server, Victim and Attacker). However, you will be running all three of these on one physical machine using 3 virtual machines. The source VM image (*SEEDUbuntu-16.04-32bit.vmdk* from the zip folder) will remain the same for all three and has been provided to you. Name them as follows:

1. User Machine
2. DNS Server
3. Attacker Machine

*Suggestion: simply make one Vm and then use the clone option to make the other two.*

***Steps:***

1. Create a new VM in VirtualBox
2. Provide a name & select the following:

   Type: linux

   Version: Ubuntu (32-bit)

3. Set the memory size (preferably 2gb but will also work for around 1.2gb)
4. Select the Pre-built VM file provided to you
5. Go to settings -> general -> advanced and make the following changes:

   Shared Clipboard: Bidirectional

   Drag'n'Drop: Bidirectional

6. Go to settings -> system -> processor and assign 2 CPUs
7. Go to settings -> display -> screen and do the following:

   Graphics Controller: VBoxVGA

   Scale Factor: Min (100%)
8. Go to settings -> network -> set Adapter 1 to "NAT Network"
9. Go to settings -> network -> Adapter 1 → Advanced → set Promiscuous Mode to "Allow All"
10. Start the VM

While setting up your virtual box, in the ***VM Network Settings***, use "NAT Network" as the network adaptor and make sure promiscus mode is set to "Allow all". Please note that to make things simple, we have put all the VMs on the same network.

In case your VM doesn't connect to the internet due to the NAT network, you can watch this video to resolve this issue: https://www.youtube.com/watch?v=y0PMFg-oAEs

***Please remember the IP addresses of all of your machines and note them down. Use ifconfig to find the IP address.***

*We don't need to configure the virtual machine in the case of the attacker as the default setup is enough.*

---

## Step 2: Configuring the User Machine

Do the following on your ***User Machine***.

We need to change the resolver configuration file (/etc/resolv.conf) of the user machine so that the server 10.0.2.7 is added as the first nameserver entry in the file. This will result in our server being the primary DNS server for the user machine.

***Steps:***

1. Run on the terminal:

   ```
   cd /etc/resolvconf
   sudo nano resolv.conf.d/head
   ```

2. Add the following line to the file & save it:

   ```
   nameserver [IP address of the DNS server machine]
   ```

   So if your IP address is 10.0.2.7

   ```
   nameserver 10.0.2.7
   ```

3. Run on the terminal:

   ```
   sudo resolvconf -u
   ```

---

## Step 3: Setup the DNS Server

Do the following on your ***DNS Server Machine***.

The BIND 9 server program has already been installed in the VM image. However, you still have to configure the BIND 9 server.

***Steps:***

1. Run on the terminal: `cd /etc/bind`

```
sudo nano named.conf.options
```

2. Add the following line, if it is not already written, to the file inside options {...} & save it:

```
dump-file “/var/cache/bind/dump.db”;
```

3. Run on the terminal:

```
sudo rndc dumpdb -cache
sudo rndc flush
```

Now, we need to *manually* turn off DNSSEC because it protects against spoofing attacks on DNS servers.

***Steps:***

1. Run on the terminal:

```
sudo nano named.conf.options
```

2. Scroll down and comment out the following line,, if it is not already commented out, & save the file:

```
dnssec-validation auto
```

Now, let's run the DNS Server. You can do so by running this command: `sudo service bind9 restart`

Try pinging google by writing: `ping www.google.com`

---

## Step 4: Host a Zone in the Local DNS Server

Do the following on your ***DNS Server Machine***.
Let's start with creating a zone.

***Steps:***

1. Run on the terminal:

```
cd /etc/bind
sudo nano named.conf
```

2. Append the following lines to the end of file & save it:

```
zone "example.com" {
      type master;
      file "/etc/bind/example.com.db";
};

zone "0.0.10.in-addr.arpa" {
      type master;
      file "/etc/bind/10.0.0.db";
};
```

Now, let's set up the forward & reverse lookup zone file. ***Steps:***

1. Run on the terminal:

   ```
   sudo nano example.com.db
   ```

2. Add the following lines to the file & save it.

   ```
   $TTL 3D ; default expiration time of all resources records without
   ; their own TTL
   @ IN SOA ns.example.com. admin.example.com. (
   1 ; Serial
   8H ; Refresh
   2H ; Retry
   4W ; Expire
   1D ) ; Minimum
   @ IN NS ns.example.com ; Address of nameserver
   @ IN MX 10 mail.example.com. ; Primary Mail Exchanger
   www IN A 10.0.0.7 ; Address of www.example.com
   mail IN A 10.0.0.10 ; Address of mail.example.com
   ns IN A 10.0.0.1 ; Address of ns.example.com
   *.example.com. IN A 10.0.0.100 ; Address for other URL in
   ; the example.com domain
   ```

3. Run on the terminal:

   ```
   sudo nano 10.0.0.db
   ```

4. Add the following lines to the file & save it.

   ```
   $TTL 3D
   @ IN SOA ns.example.com. admin.example.com. (
   1
   8H
   2H
   4W
   1D )
   @ IN NS ns.example.com.
   7 IN PTR www.example.com.
   10 IN PTR mail.example.com.
   1 IN PTR ns.example.com.
   ```

Finally, let's restart the BIND server and test. Go to the user machine and simply run `dig www.example.com`

If you have done everything correclty then you should get the server as the IP of the DNS server.

If you don't get the server as the IP of the DNS server then you must be doing something wrong. One possible mistake must have been the users DNS server IP not being set to the IP of the local DNS server you have made.

To resolve this issue, you can simply go to the settings and do the following:
1. Edit connection
2. Go to IPv4 settings
3. Choose the method "Automatic DHCP addresses only"
4. Add the IP address against the DNS servers