Name: Kunal Demla Roll No: 102003088 Subgroup: 3COE4

DNS Poisoning

In this experiment, we will perform DNS poisoning.

First of all, we need to setup a web server to host a cloned website. We will be making a clone of www.punjabiuniversity.ac.in.

Steps to setup web server:-

We will be using Linux system to host the website.

Step 1: Install Apache2

In this step, we will install Apache2 web server. For this, execute the below command in Terminal:

```
tin@ubuntu:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprut
il1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
libaprutil1-dbd-sqlite3 libaprutil1-ldap
  liblua5.2-0
0 upgraded, 9 newly installed, 0 to remove and 343 not upgraded.
Need to get 1,818 kB of archives.
After this operation, 7,935 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Firewall configuration

Now, we will need to open certain ports on our system in order to access Apache from outside. We will use the highly restrictive profile ‘Apache’ to enable network ctivity on port 80.

(My System already had them enabled and configuered)

(Using command **sudo ufw allow ‘Apache’**)

Now check the status which will show Apache allowed in firewall.

(Using command **sudo ufw status**)

Configuring Apache web server; Verifying Apache service

Before moving towards configuration, first, verify if the Apache service is operational. For this, execute the below command in Terminal:

From the above output, you can see the Apache2 service is active and running.

Another approach to verify if Apache is running fine by requesting a web page from the Apache web server. To do so, find your IP address using the following command:

Then open the web browser and access apache welcome page as follows:

http://192.168.216.128
Replace the 192.168.244.128 by the IP address of your machine.

By navigating to the above link in the browser, you see the Apache welcome page which is the indication that the Apache server is working properly.

Setting Up Virtual Hosts in Apache

If you have multiple domains that need to be server from the single Apache web server, then you will require to set up virtual hosts. In the following, we will show you how to set up a virtual host in Apache.

Step 1: Create a directory for your domain

In this step, we will create a directory for our domain name. This directory will be used for storing the data on our website.

Run the following command in Terminal by replacing the info.net with your own domain name:

Change the directory ownership to current user:

Assign necessary permissions as follows: .

Step 2: Create a virtual host file

Apache server comes with virtual host file by default. This file is used to serve the contents of the web server. However, we will generate the new virtual host file with the following command:

Now enter the below lines by replacing the **info.net** by your own domain name.

```
<VirtualHost *:80>
ServerAdmin admin@info.net
ServerName info.net
ServerAlias info.net
DocumentRoot /var/www/info.net/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Step 3: Activate virtual host configuration file

In this step, we will be creating the virtual host configuration file. For this, execute the following command in Terminal:

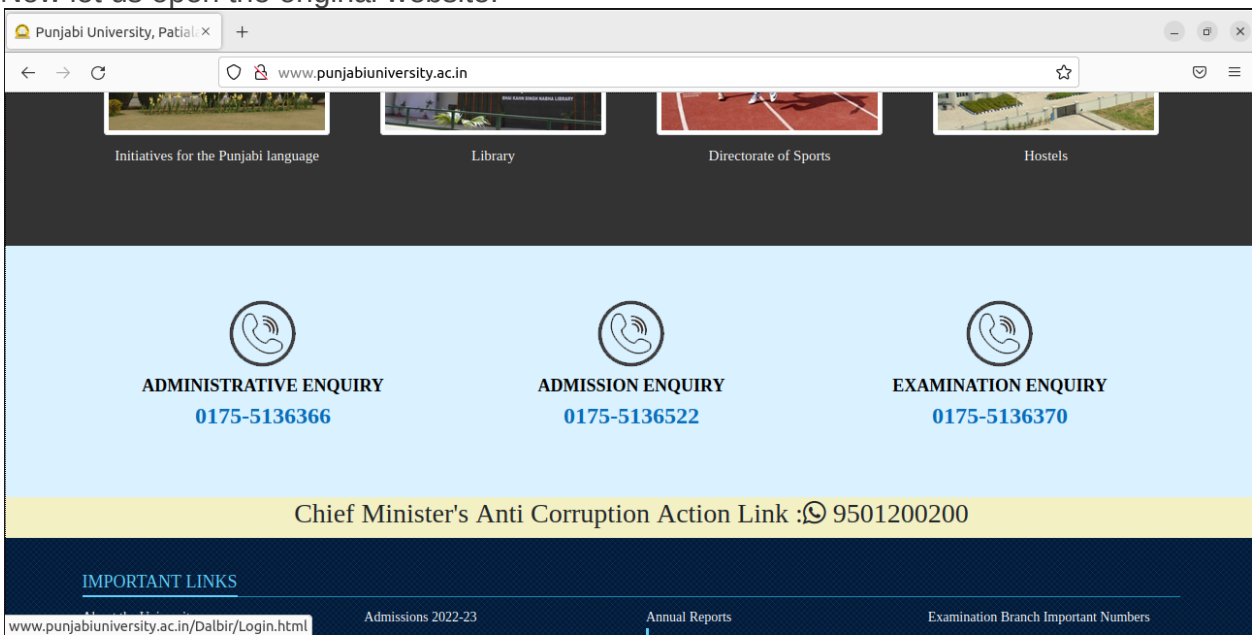
Now disable the “000-default.conf” default virtual configuration file as follows:

Now restart Apache to activate the new configuration as follows:

Step 4: Test for errors

Once all the configurations are completed, you can test for any configuration errors:

Now let us open the original website.



Now we will do dns poisoning on victim's machine, i.e., we will manipulate host file on victim's machine.

```
127.0.0.1       localhost
127.0.1.1       anshika

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.244.128 www.punjabiuniversity.ac.in
```

Here we have mapped www.punjabiuniversity.ac.in to an ip address where cloned website is hosted.

Name: Kunal Demla Roll No: 102003088 Subgroup: 3COE4