

DNS Poisoning

Steps for DNS poisoning:

1. Cloning a website using wget command

```
sky@saurav:/var/www/cyber.com/public_html$ wget https://www.thapar.edu/
--2022-08-31 13:46:43-- https://www.thapar.edu/
Resolving www.thapar.edu (www.thapar.edu)... 14.139.242.109, 117.203.246.106
Connecting to www.thapar.edu (www.thapar.edu)|14.139.242.109|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html           [ <=> ] 56.74K --.-KB/s in 0.06s

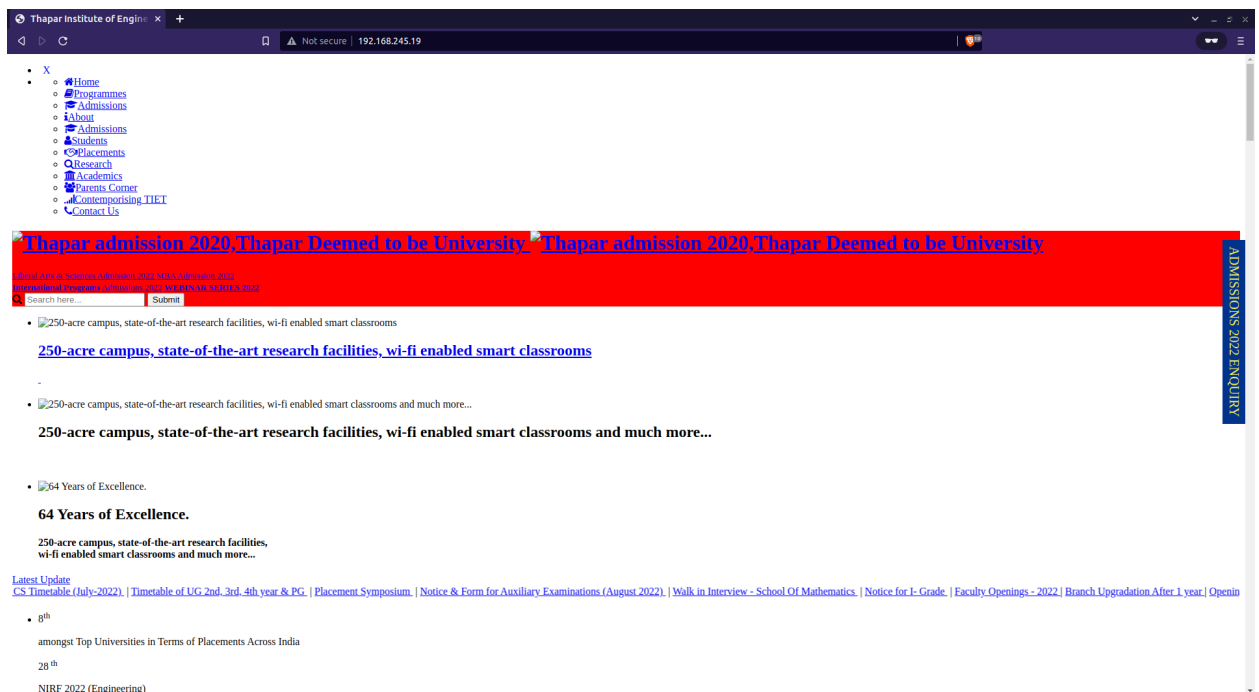
2022-08-31 13:46:43 (994 KB/s) - 'index.html' saved [58101]

sky@saurav:/var/www/cyber.com/public_html$
```

The cloned website is as follow:

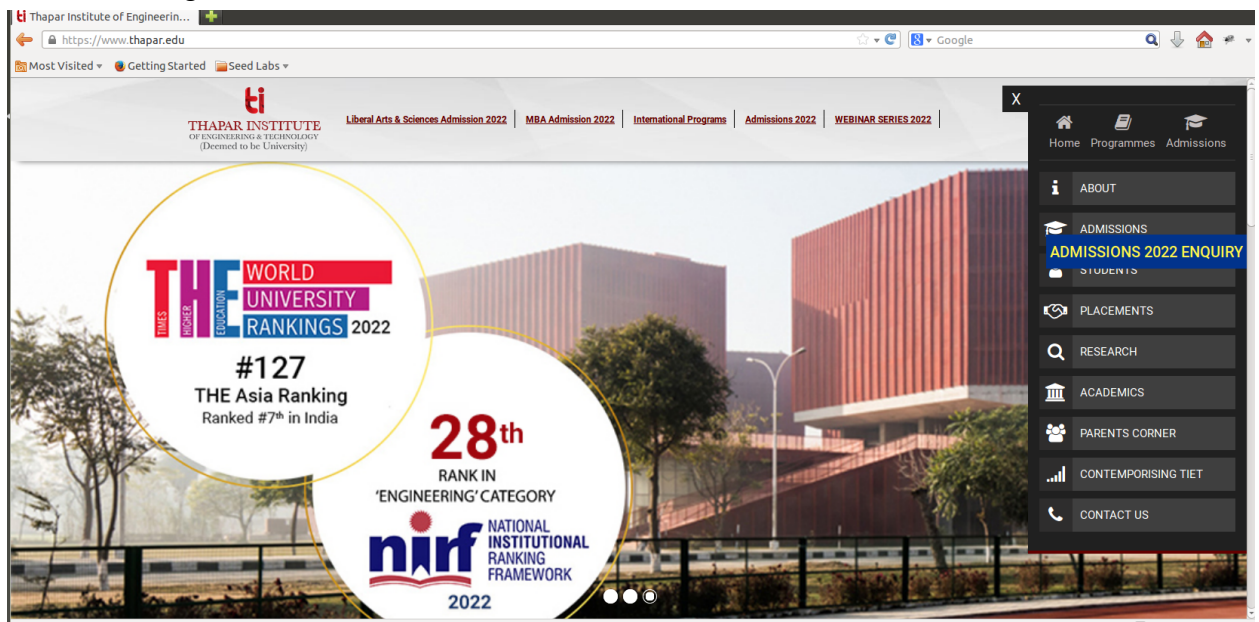


2. The website is hosted using apache at 192.168.245.19



3. The /etc/file of the machine is edited, and a new entry is added for thapar.edu which points to the IP 192.168.245.19

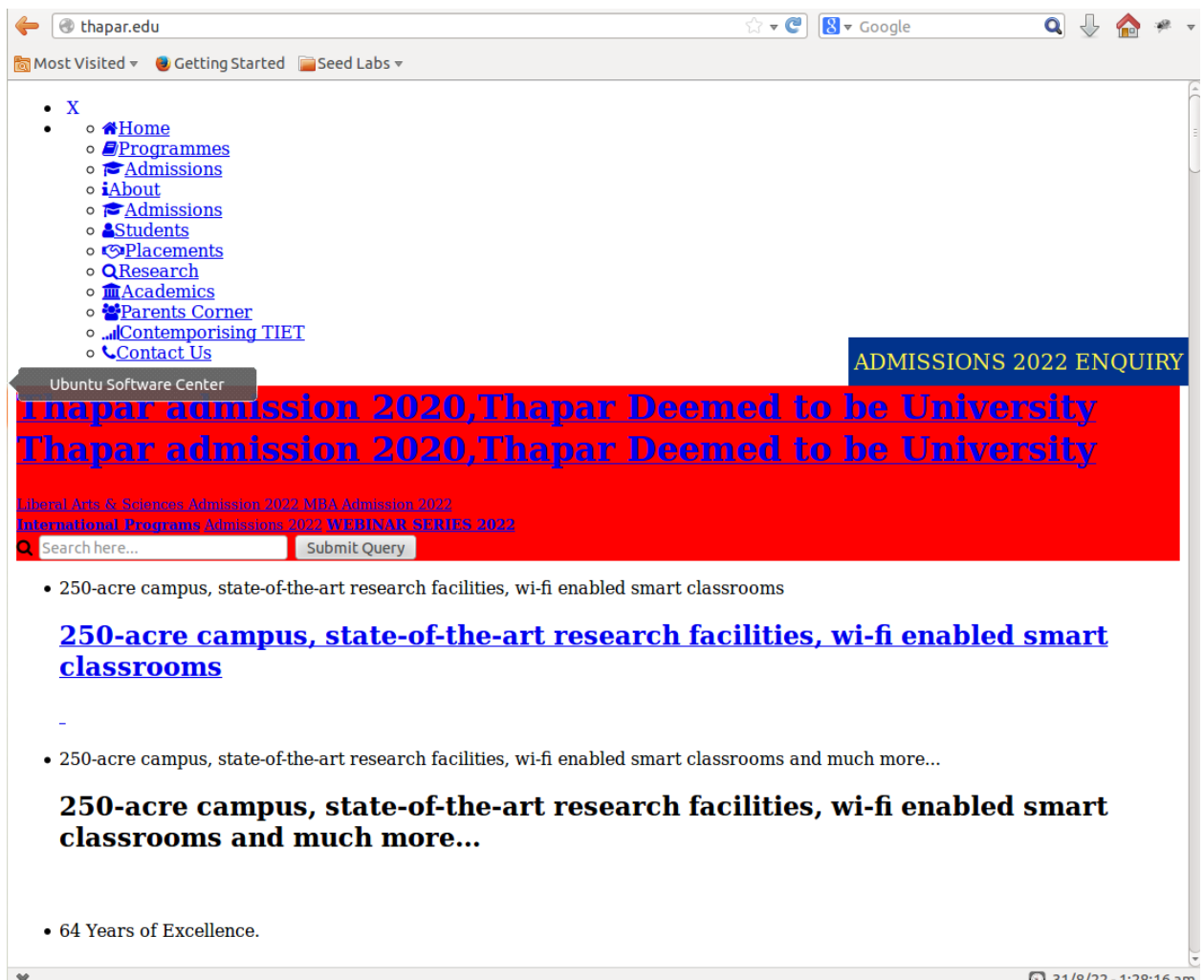
Before editing:



Changing the content of /etc/hosts:

```
GNU nano 2.2.6 File: /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntu
192.168.245.19 thapar.edu
```

4. Now when “thapar.edu” is entered in the search bar instead of the original website the cloned website is showed



DNS poisoning is successful on the machine.