

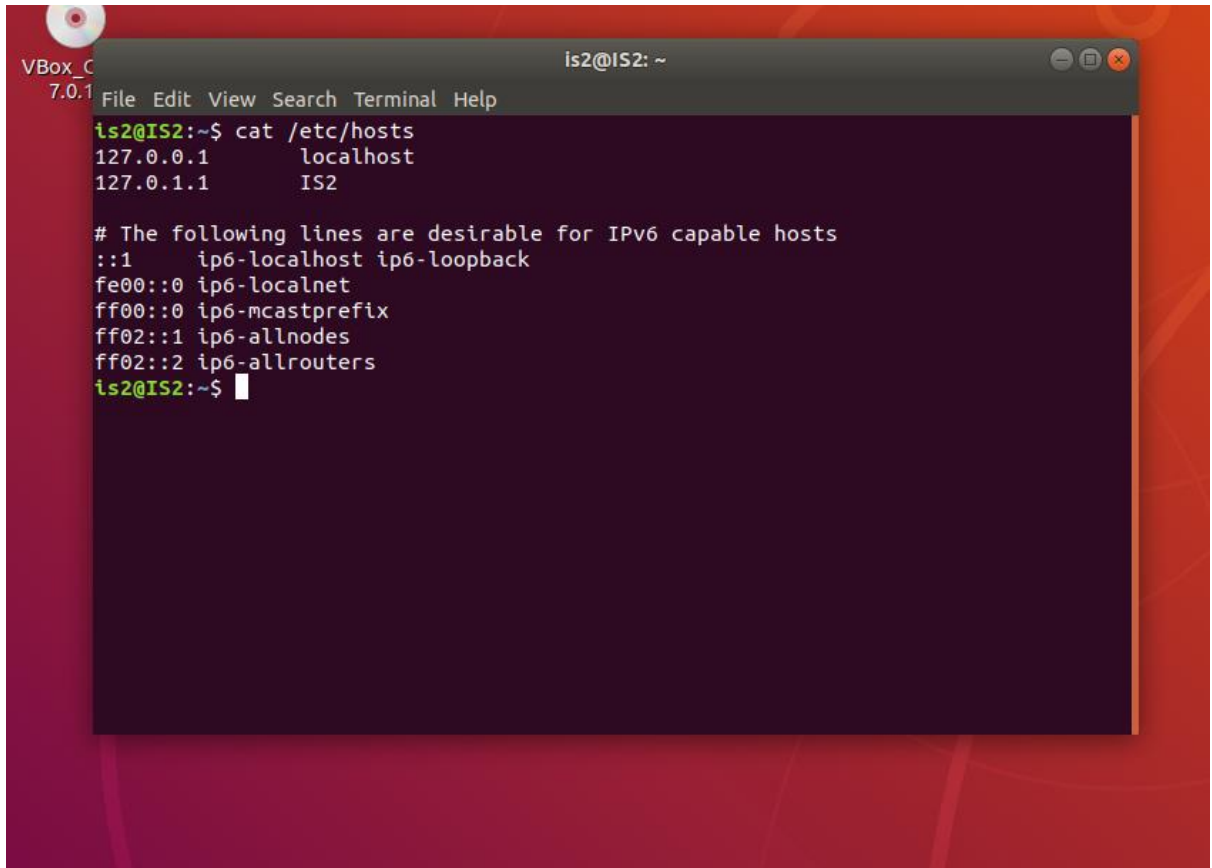
DNS Poisoning

- 1) Fetch and display entries of your Local DNS server.

DNS poisoning, often referred to as DNS spoofing or DNS cache poisoning, is a cyberattack that deceives your device or network into accessing a counterfeit website instead of the authentic one you intended to view. It especially focuses on the Domain Name System (DNS), which functions as a directory for the

The internet translates website names (such [invalid URL deleted]) into numerical IP addresses that computers can comprehend.

\$ cat /etc/hosts

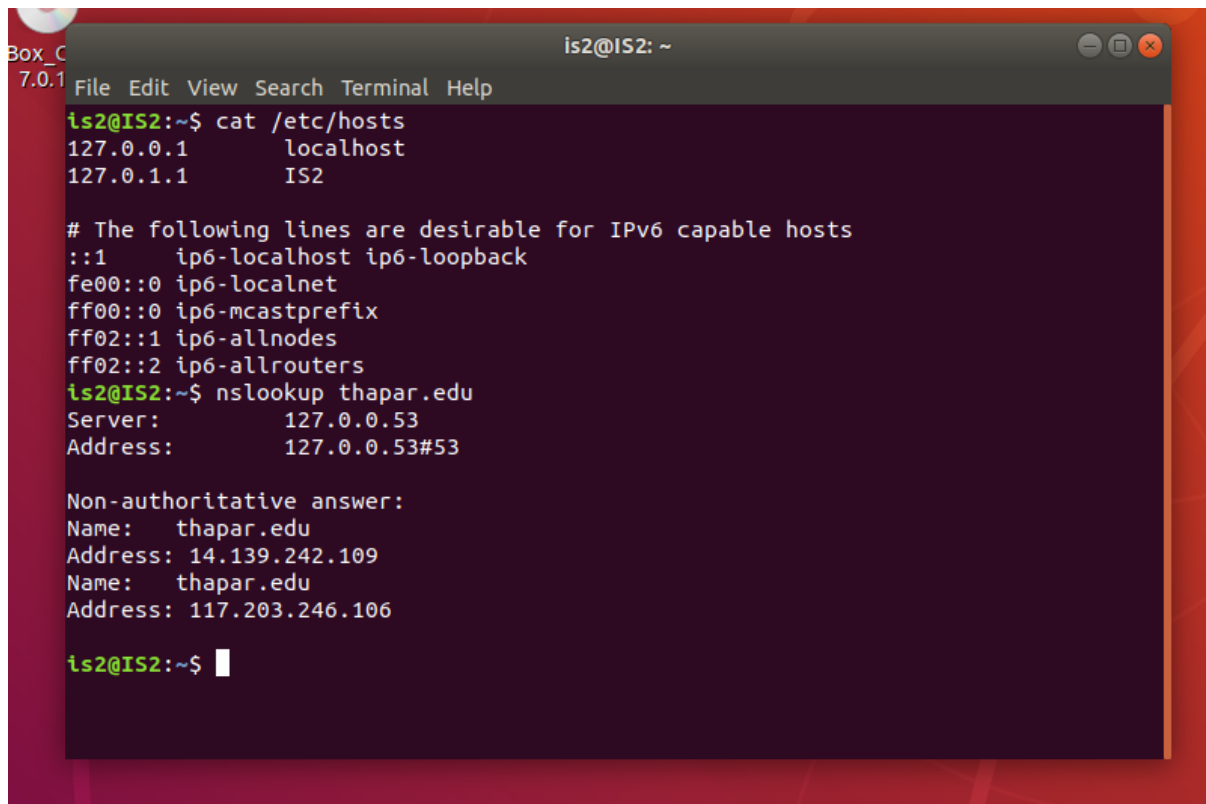
A screenshot of a terminal window titled 'is2@IS2: ~' with a menu bar containing 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'cat /etc/hosts' being executed. The output lists IP addresses and their corresponding hostnames: '127.0.0.1 localhost' and '127.0.1.1 IS2'. Below this, a comment line reads '# The following lines are desirable for IPv6 capable hosts', followed by several IPv6 address ranges and their associated names: '::1 ip6-localhost ip6-loopback', 'fe00::0 ip6-localnet', 'ff00::0 ip6-mcastprefix', 'ff02::1 ip6-allnodes', and 'ff02::2 ip6-allrouters'. The prompt 'is2@IS2:~\$' is visible at the bottom of the terminal output.

```
is2@IS2:~$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      IS2

# 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
is2@IS2:~$
```

On Linux, we may retrieve the DNS cache records on the Local DNS server using the command mentioned above.

- 2) Perform DNS poisoning by inserting a phished/wrong entry for a domain name/IP address.
Check and display the corresponding new redirection



A terminal window titled 'is2@IS2: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The user runs 'cat /etc/hosts' and the output shows the following entries:

```
127.0.0.1    localhost
127.0.1.1    IS2
```

Below these are IPv6-related entries. Then, the user runs 'nslookup thapar.edu'. The output shows the server used (127.0.0.53) and the address resolved (127.0.0.53#53). It then displays a non-authoritative answer for 'thapar.edu' with two IP addresses: 14.139.242.109 and 117.203.246.106.

```
is2@IS2:~$ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    IS2

# 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
is2@IS2:~$ nslookup thapar.edu
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   thapar.edu
Address: 14.139.242.109
Name:   thapar.edu
Address: 117.203.246.106

is2@IS2:~$
```

Here we can see that the IP of thapar.edu is 14.139.242.109

```
is2@IS2: ~  
File Edit View Search Terminal Help  
fe00::0 ip6-localnet  
ff00::0 ip6-mcastprefix  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters  
is2@IS2:~$ sudo nano /etc/hosts  
is2@IS2:~$ nslookup thapar.edu  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   thapar.edu  
Address: 104.21.65.14  
  
is2@IS2:~$ sudo cat /etc/hosts  
127.0.0.1      localhost  
127.0.1.1      IS2  
104.21.65.14   thapar.edu  
# 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  
is2@IS2:~$  
  
is2@IS2: ~  
File Edit View Search Terminal Help  
is2@IS2:~$ nslookup tiet360.in  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   tiet360.in  
Address: 104.21.65.14  
Name:   tiet360.in  
Address: 172.67.157.64  
Name:   tiet360.in  
Address: 2606:4700:3031::6815:410e  
Name:   tiet360.in  
Address: 2606:4700:3034::ac43:9d40  
  
is2@IS2:~$
```

We can see here we have poisoned the IP of Thapar.edu with tiet360.in and hence we can see when we ping to Thapar.edu it pings the IP of tiet360.in hence we have performed dns poisoning.

```
is2@IS2: ~  
File Edit View Search Terminal Help  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   tiet360.in  
Address: 104.21.65.14  
Name:   tiet360.in  
Address: 172.67.157.64  
Name:   tiet360.in  
Address: 2606:4700:3031::6815:410e  
Name:   tiet360.in  
Address: 2606:4700:3034::ac43:9d40  
  
is2@IS2:~$ ping thapar.edu  
PING thapar.edu (104.21.65.14) 56(84) bytes of data.  
64 bytes from thapar.edu (104.21.65.14): icmp_seq=1 ttl=56 time=136 ms  
64 bytes from thapar.edu (104.21.65.14): icmp_seq=2 ttl=56 time=139 ms  
64 bytes from thapar.edu (104.21.65.14): icmp_seq=3 ttl=56 time=138 ms  
64 bytes from thapar.edu (104.21.65.14): icmp_seq=4 ttl=56 time=148 ms  
^C  
--- thapar.edu ping statistics ---
```