

1. Find the domain name of Google DNS IP (8.8.8.8)

```
Applications ▾ Places ▾ Terminal ▾ Fri 13:46
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nslookup
> set query=NS
> 8.8.8.8
Server:      192.168.189.2
Address:     192.168.189.2#53

Non-authoritative answer:
8.8.8.8.in-addr.arpa      name = google-public-dns-a.google.com.

Authoritative answers can be found from:
>
```

I ran nslookup with the query set to the name server, and the domain name of the fully qualified domain name is google.com

2. Using your virtual machine, send 2 packets to: www.india.gov.in and 2 packets to 8.8.8.8. Is there any difference in the completion time, if so, why?

```
Applications ▾ Places ▾ Terminal ▾ Fri 12:36
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ping -c 2 www.india.gov.in
PING e16113.d.akamaiedge.net (23.223.243.109) 56(84) bytes of data:
64 bytes from a23-223-243-109.deploy.static.akamaitechnologies.com (23.223.243.109): icmp_seq=1 ttl=128 time=41.1 ms
64 bytes from a23-223-243-109.deploy.static.akamaitechnologies.com (23.223.243.109): icmp_seq=2 ttl=128 time=39.3 ms

--- e16113.d.akamaiedge.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 39.286/40.217/41.148/0.931 ms
root@kali:~#
```

```
Applications ▾ Places ▾ Terminal ▾ Fri 12:36
root@kali: ~

File Edit View Search Terminal Help

root@kali:~# ping -c 2 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=94.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=22.6 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 22.576/58.738/94.901/36.163 ms
root@kali:~#
```

The completion time is 3ms for both. The www.india.gov.in server is located in Massachusetts while the 8.8.8.8 server is located in California, and the difference in distance between those two states to the source IP is miniscule enough to where the ping is not affected.

3. How about using the ping command to 8.8.8.8 from your physical system versus using the VM? What are your findings?

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17134.471]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=37ms TTL=121
Reply from 8.8.8.8: bytes=32 time=30ms TTL=121
Reply from 8.8.8.8: bytes=32 time=28ms TTL=121
Reply from 8.8.8.8: bytes=32 time=26ms TTL=121

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 37ms, Average = 30ms

C:\WINDOWS\system32>
```

```
Applications ▾ Places ▾ Terminal ▾ Fri 15:15
root@kali: ~

File Edit View Search Terminal Help

root@kali:~# ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=30.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=30.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=31.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=25.2 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 10ms
rtt min/avg/max/mdev = 25.188/29.463/31.866/2.551 ms
root@kali:~#
```

Initially, on the virtual machine the ping would be continuous, so I limited the packet count to 4 so it matched the physical system. There is minor difference between runtime minimum, maximum, and averages but nothing drastic. If enough test were ran then the findings would eventually become similar.

4. What is the IP address assigned to your Virtual Machine (VM)? How that IP address was assigned to your VM?

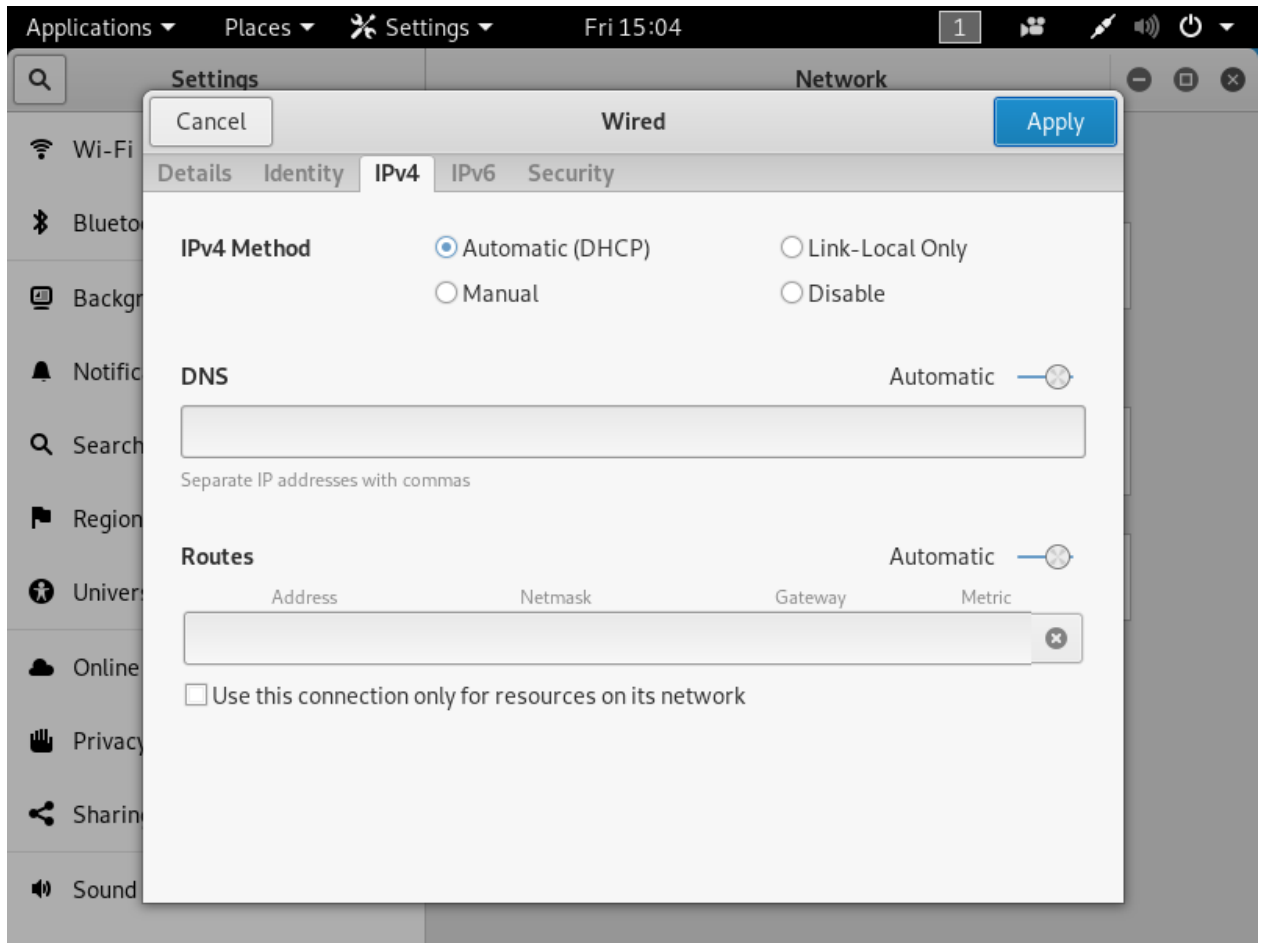
```
Applications ▾ Places ▾ Terminal ▾ Fri 12:39
root@kali: ~

File Edit View Search Terminal Help

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.189.130 netmask 255.255.255.0 broadcast 192.168.189.255
    inet6 fe80::20c:29ff:fe19:5aae prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:19:5a:ae txqueuelen 1000 (Ethernet)
    RX packets 223 bytes 17029 (16.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 74 bytes 6068 (5.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

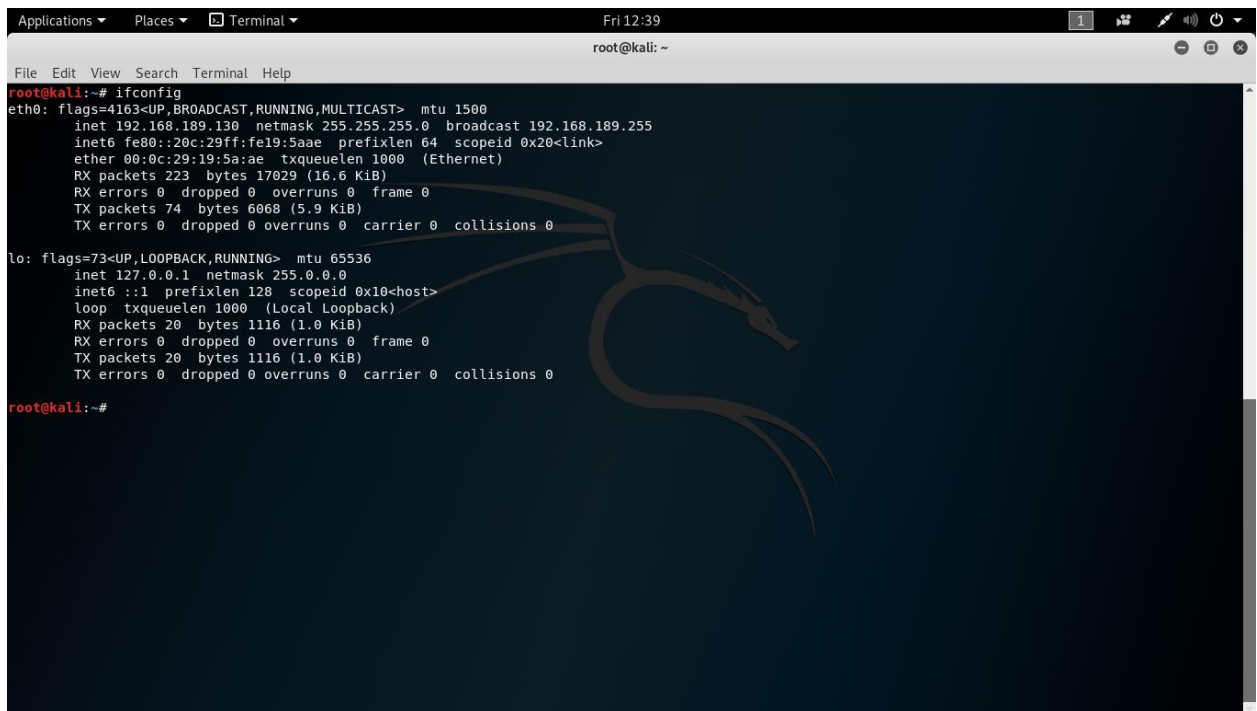
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```



The IP address assigned to my virtual machines is 192.168.189.130, and it was assigned by the dynamic host configuration protocol.

5. Explain on detail the network information from your VM. Example, IP address, broadcast, mask, MAC address, localhost IP.



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.189.130 netmask 255.255.255.0 broadcast 192.168.189.255
    inet6 fe80::20c:29ff:fe19:5a:ae prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:19:5a:ae txqueuelen 1000 (Ethernet)
    RX packets 223 bytes 17029 (16.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 74 bytes 6068 (5.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

IP address – 192.168.189.130

Value assigned to a device connected to a computer network. This one was assigned through DHCP.

Broadcast – 192.168.189.255

Network address at which all devices connected to a multiple-access communications network are enabled to receive datagrams. By performing a bitwise OR operation between the bit complement of the netmask and IP address.

Netmask – 255:255:255:0

Used to tell which network devices are local. So IP addresses would follow the format 192.168.189.xxx because the IP address is 192.168.189 and the subnet is 255:255:255:0.

MAC address – 00:0c:29:19:5a:ae

Hardware identification number usually assigned by the manufacturer, in this case VMware, Inc.

Localhost IP – 127.0.0.1

Considered a loopback address because the information sent to it is routed back to the local machine.

6. Find the IP of www.facebook.com?

```
Applications ▾ Places ▾ Terminal ▾ Fri 13:36
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nslookup www.facebook.com
Server:      192.168.189.2
Address:     192.168.189.2#53

Non-authoritative answer:
www.facebook.com      canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.2.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f127:83:face:b00c:0:25de
root@kali:~#
```

I ran nslookup, and the IP address is 157.240.2.35

7. Are you able to execute tracert or traceroute to 8.8.8.8 from campus and off-campus? Why or why not?

```
Applications ▾ Places ▾ Terminal ▾ Fri 14:08
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# traceroute 8.8.8.8 -I
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 _gateway (192.168.189.2)  0.201 ms  0.124 ms  0.075 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 google-public-dns-a.google.com (8.8.8.8)  52.381 ms  52.372 ms  27.528 ms
root@kali:~#
```

Initially the request timed-out so because traceroute in linux uses UDP so the firewall blocked the traffic. However, the firewall does not block ICMP so I added the -I command and there

eventually was a response. In conclusion, execution of tracert or traceroute depends on the firewall configurations.

8. Inquire about famous attacks to some of the 13 root DNS servers, write a summary of the attacks methods that were used? Include a link to the website(s) you found.

On November 30, 2015 many of the root servers received approximately five million queries per second. The queries were valid DNS messages for a single domain name and were enough to flood network connections and cause timeouts.

https://www.theregister.co.uk/2015/12/08/internet_root_servers_ddos/

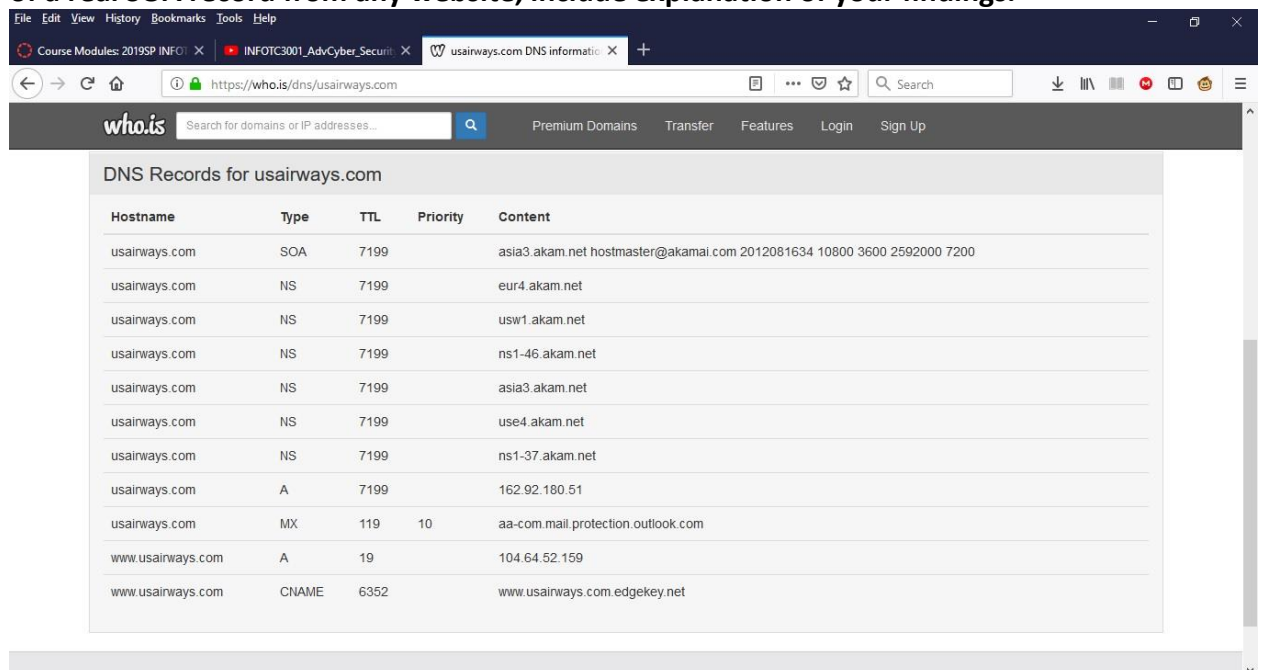
On February 6, 2007 a DDos attack targeted five of the thirteen root DNS servers causing two to stop responding to up to 90% of queries. However, the RIPE NCC managed K-root server kept the internet working.

<https://www.ripe.net/publications/news/industry-developments/global-root-server-system-stands-firm-against-ddos-attack>

9. We covered a few footprinting techniques, how do you think the information gathered can be used maliciously? Include an example as part of your answer.

The information gathered during the reconnaissance phase of footprinting identifies flaws and weaknesses of their targets. In the tutorial videos the website archive.org was utilized. The archival of prior web pages can be exploited by attackers to locate changes between web pages and find vulnerabilities between changes.

10. Using the 'registrar queries' or 'DNS queries' shown in INFOTC3001_Adv_Cyber_Security_SP19_03_Footprinting_I.pdf provide complete information of a real SOA record from any website, include explanation of your findings.



The screenshot shows a web browser window with the URL <https://who.is/dns/usairways.com>. The page displays the DNS records for the domain usairways.com. The records are listed in a table with columns: Hostname, Type, TTL, Priority, and Content.

Hostname	Type	TTL	Priority	Content
usairways.com	SOA	7199		asia3.akam.net hostmaster@akamai.com 2012081634 10800 3600 2592000 7200
usairways.com	NS	7199		eur4.akam.net
usairways.com	NS	7199		usw1.akam.net
usairways.com	NS	7199		ns1-46.akam.net
usairways.com	NS	7199		asia3.akam.net
usairways.com	NS	7199		use4.akam.net
usairways.com	NS	7199		ns1-37.akam.net
usairways.com	A	7199		162.92.180.51
usairways.com	MX	119	10	aa-com.mail.protection.outlook.com
www.usairways.com	A	19		104.64.52.159
www.usairways.com	CNAME	6352		www.usairways.com.edgekey.net

The asia3 server is the master server because it is denoted by the SOA record.
hostmaster@akamai.com is in charge of the domain.

It was first configured on 08/16/2012 and was configured 34 times.

The following values are representative, in seconds, for the slave servers (before the zone should be refreshed, before a failed refresh should be retired, upper limit before a zone is considered no longer authoritative).

11. In a separate file, write a disclaimer indicating that you fully understand the following text, sign it, write your full name and include the date clearly.

“All the material, such as slides, videos, additional documents, laboratories, etc., shared as part of this course is for Educational Purpose Only, you (as a student registered in the Advanced Cyber Security course) can not use the acquired knowledge to perform malicious attacks. Neither the TA, myself, or anyone related with the University of Missouri are responsible for the malicious usage of the acquired knowledge in this course.”