1. Use the ping command to test the connectivity to a remote server (e.g., example.com).

```
┌──(kali㉿kali)-[~/nithesh]
└─$ ping example.com
PING example.com (93.184.215.14) 56(84) bytes of data.
64 bytes from 93.184.215.14: icmp_seq=1 ttl=128 time=253 ms
64 bytes from 93.184.215.14: icmp_seq=2 ttl=128 time=221 ms
64 bytes from 93.184.215.14: icmp_seq=3 ttl=128 time=224 ms
64 bytes from 93.184.215.14: icmp_seq=4 ttl=128 time=222 ms
64 bytes from 93.184.215.14: icmp_seq=5 ttl=128 time=223 ms
64 bytes from 93.184.215.14: icmp_seq=6 ttl=128 time=221 ms
64 bytes from 93.184.215.14: icmp_seq=7 ttl=128 time=222 ms
64 bytes from 93.184.215.14: icmp_seq=8 ttl=128 time=222 ms
64 bytes from 93.184.215.14: icmp_seq=9 ttl=128 time=248 ms
```

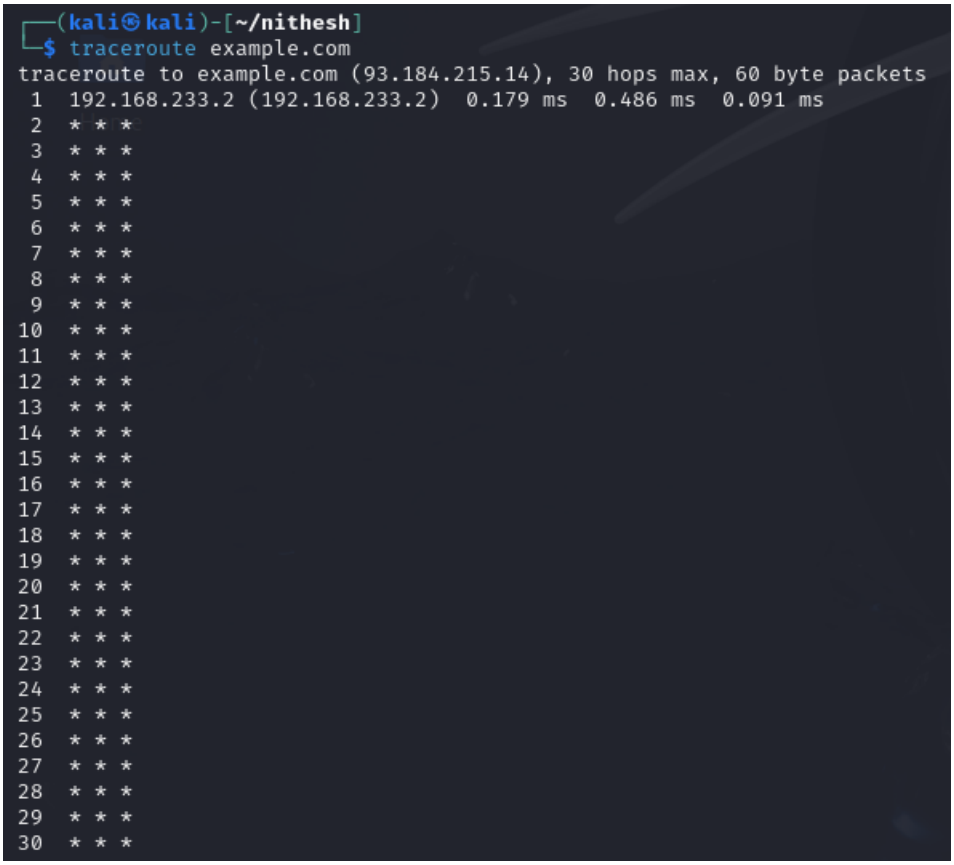
```
── example.com ping statistics ──
331 packets transmitted, 331 received, 0% packet loss, time 331360ms
rtt min/avg/max/mdev = 221.098/222.545/253.081/3.063 ms
```

2. Write a script to measure the round-trip time for each packet and analyze the results.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ ping -c 10 example.com
PING example.com (93.184.215.14) 56(84) bytes of data.
64 bytes from 93.184.215.14: icmp_seq=1 ttl=128 time=221 ms
64 bytes from 93.184.215.14: icmp_seq=2 ttl=128 time=221 ms
64 bytes from 93.184.215.14: icmp_seq=3 ttl=128 time=222 ms
64 bytes from 93.184.215.14: icmp_seq=4 ttl=128 time=222 ms
64 bytes from 93.184.215.14: icmp_seq=5 ttl=128 time=221 ms
64 bytes from 93.184.215.14: icmp_seq=6 ttl=128 time=221 ms
64 bytes from 93.184.215.14: icmp_seq=7 ttl=128 time=222 ms
64 bytes from 93.184.215.14: icmp_seq=8 ttl=128 time=222 ms
64 bytes from 93.184.215.14: icmp_seq=9 ttl=128 time=222 ms
64 bytes from 93.184.215.14: icmp_seq=10 ttl=128 time=222 ms

── example.com ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9047ms
rtt min/avg/max/mdev = 221.408/221.679/222.099/0.249 ms
```

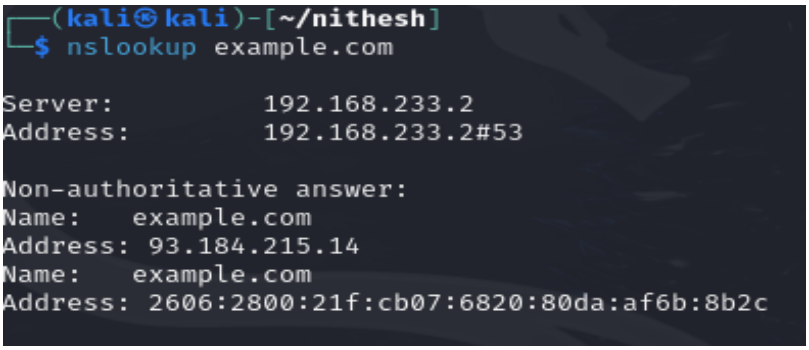
3. Use the traceroute to trace the route packets take to a destination



4. Analyze the output to identify any potential bottlenecks or points of failure in the route.

Analyzing the output of `traceroute` can help you identify any potential bottlenecks or points of failure in the route. Look for high latency or packet loss at specific hops.

5. Use the nslookup command to find the IP address of a given domain (e.g., example.com).



6. Use the netstat command to view active connections and listening ports on your machine.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ netstat -tuln example.com

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

```
┌──(kali㉿kali)-[~/nithesh]
└─$ netstat example.com
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.233.128:bootpc  192.168.233.254:bootps  ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     11314
unix  3      [ ]         STREAM     CONNECTED     8115
unix  3      [ ]         STREAM     CONNECTED     10475    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10023
unix  3      [ ]         STREAM     CONNECTED     10683
unix  3      [ ]         STREAM     CONNECTED     10447    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     7984
unix  3      [ ]         STREAM     CONNECTED     11333
unix  3      [ ]         STREAM     CONNECTED     9984     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     8032
unix  3      [ ]         STREAM     CONNECTED     10749
```

```
unix  3      [ ]         STREAM     CONNECTED     10085
unix  3      [ ]         STREAM     CONNECTED     8258     @b9e2a3d24b346483/bus/systemd/bus-api-system
unix  2      [ ]         STREAM                   11521    @printer-applet-lock-user-kali
unix  3      [ ]         STREAM     CONNECTED     9804     @2def52226d6cb5fd/bus/systemd/bus-system
unix  3      [ ]         STREAM     CONNECTED     10322    @ae93198f2f1738c9/bus/systemd/bus-api-user
unix  3      [ ]         STREAM     CONNECTED     7302     @23da3834f61df8cf/bus/systemd-logind/system
```

7. Use the ifconfig (Linux) or ip a command to display network interface configurations.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.233.128  netmask 255.255.255.0  broadcast 192.168.233.255
        inet6 fe80::7f60:4722:cf3:52e6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f8:1e:3a  txqueuelen 1000  (Ethernet)
        RX packets 351  bytes 24306 (23.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74  bytes 7564 (7.3 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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(kali㉿kali)-[~/nithesh]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:f8:1e:3a brd ff:ff:ff:ff:ff:ff
    inet 192.168.233.128/24 brd 192.168.233.255 scope global dynamic noprefixroute eth0
       valid_lft 1081sec preferred_lft 1081sec
    inet6 fe80::7f60:4722:cf3:52e6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

8. Write a script to report document the configuration of each interface, noting the IP address, subnet mask, and any other relevant information.

```
#!/bin/bash

for interface in $(ls /sys/class/net/); do
    echo "Interface: $interface"
    ip addr show "$interface" | grep -E 'inet|netmask'
    echo
done
```

```
┌──(kali㉿kali)-[~/nithesh]
└─$ vi script.sh

┌──(kali㉿kali)-[~/nithesh]
└─$ ./ script.sh

zsh: permission denied: ./
```

9. Perform a basic network scan using nmap on your local network to identify active devices and open ports.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ nmap -sP 192.168.1.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 04:44 EDT
Stats: 0:00:16 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 15.62% done; ETC: 04:45 (0:01:26 remaining)
Stats: 0:00:39 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 38.09% done; ETC: 04:45 (0:01:03 remaining)
Stats: 0:00:40 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 39.06% done; ETC: 04:45 (0:01:02 remaining)
Stats: 0:01:13 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 71.29% done; ETC: 04:45 (0:00:29 remaining)
Stats: 0:01:18 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 76.17% done; ETC: 04:45 (0:00:24 remaining)
Stats: 0:01:19 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 77.15% done; ETC: 04:45 (0:00:23 remaining)
Nmap done: 256 IP addresses (0 hosts up) scanned in 103.23 seconds
```

10. Create a report summarizing the devices found, their IP addresses, and the services running on the open ports.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ nmap -sn 192.168.1.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 05:42 EDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 103.62 seconds

┌──(kali㉿kali)-[~/nithesh]
└─$ nmap -sV 192.168.1.10

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 05:45 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.38 seconds
```

```
┌──(kali㉿kali)-[~/nithesh]
└─$ nmap -sV 192.168.1.0/24 -oN nmap_results.txt

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 05:46 EDT
Stats: 0:00:15 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 14.65% done; ETC: 05:48 (0:01:27 remaining)
Nmap done: 256 IP addresses (0 hosts up) scanned in 104.71 seconds
```

11. Capture network packets using tcpdump on a specific interface.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ sudo tcpdump -i eth0 -w example.com.pcap

[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 2621
44 bytes
```

12. Analyze the captured packets for specific protocols (like HTTP or DNS) and summarize your findings.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ sudo tcpdump -r example.com.pcap -A -s 0 | grep -i "HTTP"

reading from file example.com.pcap, link-type EN10MB (Ethernet), snapshot len
gth 262144
E.....................l..'.M-SEARCH * HTTP/1.1
E.....................8.l..6.M-SEARCH * HTTP/1.1
E.....................l..'.M-SEARCH * HTTP/1.1
E.....................l..'.M-SEARCH * HTTP/1.1
E.....................l..'.M-SEARCH * HTTP/1.1
tcpdump: pcap_loop: truncated dump file; tried to read 342 captured bytes, on
ly got 89
```

13. Use the whois command to gather registration information about a domain.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ whois example.com

connect: Network is unreachable
```

14. Use the hostname command to display and change the hostname of your machine.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ hostname

kali
```

15. Use the finger command to gather information about users on a system.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ finger kali
Login: kali                             Name:
Directory: /home/kali                   Shell: /usr/bin/zsh
On since Mon Oct  7 04:43 (EDT) on tty7 from :0
    1 hour 49 minutes idle
On since Mon Oct  7 06:08 (EDT) on pts/2   23 minutes 56 seconds idle
No mail.
No Plan.

┌──(kali㉿kali)-[~/nithesh]
└─$ finger nithesh
Login: nitzz                            Name: nithesh
Directory: /home/nitzz                  Shell: /bin/bash
Office: 201059037, 948-233-2372         Home Phone: 000-000-0000
Never logged in.
No mail.
No Plan.
```

16. Use the who command to see who is currently logged into the system and the last command to view the login history.

```
┌──(kali㉿kali)-[~/nithesh]
└─$ who nithesh

┌──(kali㉿kali)-[~/nithesh]
└─$ last nithesh

/var/lib/wtmpdb/wtmp.db begins Sun Aug 18 15:54:22 2024

┌──(kali㉿kali)-[~/nithesh]
└─$ last example.com

/var/lib/wtmpdb/wtmp.db begins Sun Aug 18 15:54:22 2024
```