Experiment 07

Study network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.

Roll No.	37
Name	Mikil Lalwani
Class	D15-B
Subject	Security Lab
LO Mapped	LO3: Explore the different network reconnaissance tools to gather information about networks

Aim:

Study the use of network reconnaissance tools like WHOIS, dig, traceroute, and nslookup to gather information about networks and domain registrars.

Methods:

1. traceroute

   traceroute command is commonly used to troubleshoot the network. It finds out the delay and pathway to your destination. It determines and reports where is network latency comes from. It is not installed by default on some Linux Distros, so you can install it using the following command.

   ```
   sudo apt install traceroute
   ```

   Syntax:

   ```
   traceroute <destination>
   ```

   Where <destination> is the host IP you want to troubleshoot, and its a mandatory parameter for this command.

2. nslookup

   nslookup (Name Server Lookup) command used to query DNS to get a domain name, IP address mapping, or DNS records.

   Syntax:

   ```
   nslookup <domainName>
   ```

   Where <domainName> is the DNS you want to analyze.

3. dig

   dig (Domain Information Groper) is another command used to investigate DNS. It is an updated version of nslookup. It performs a DNS Lookup query and displays the response returned from name servers. It is also used to verify DNS mappings, MX records, and other DNS records.

   Syntax:

   ```
   dig <domainName>
   ```

   Where <domainName> is the DNS you want to analyze.

4. whois

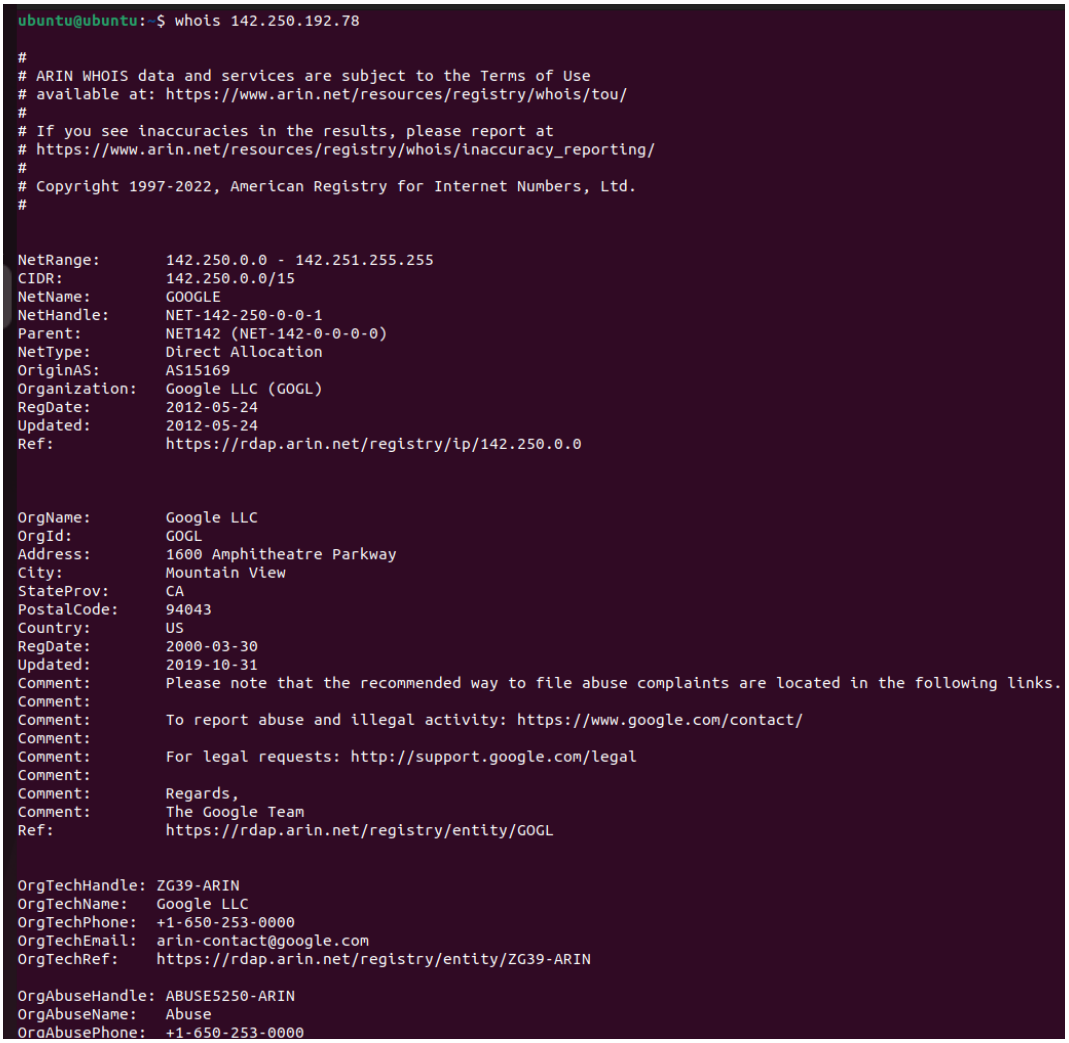
   whois command is used to get all the information about a website. You can get all registration and ownership details using it. You need to install the whois package before using it.

   ```
   sudo apt install whois
   ```

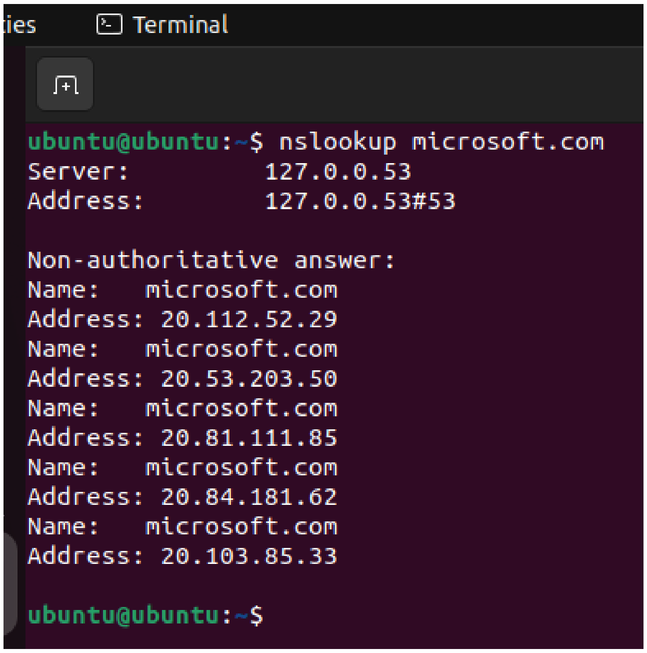
   Syntax:

   ```
   whois <website>
   ```

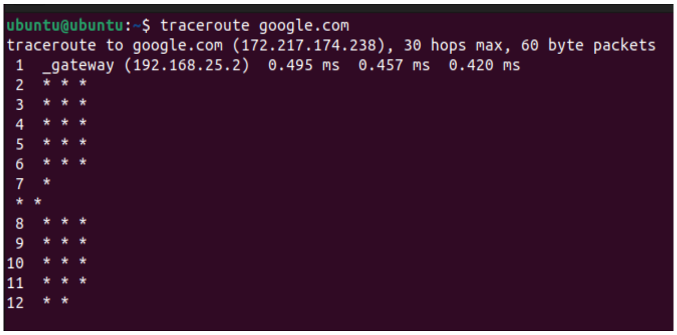
Results:



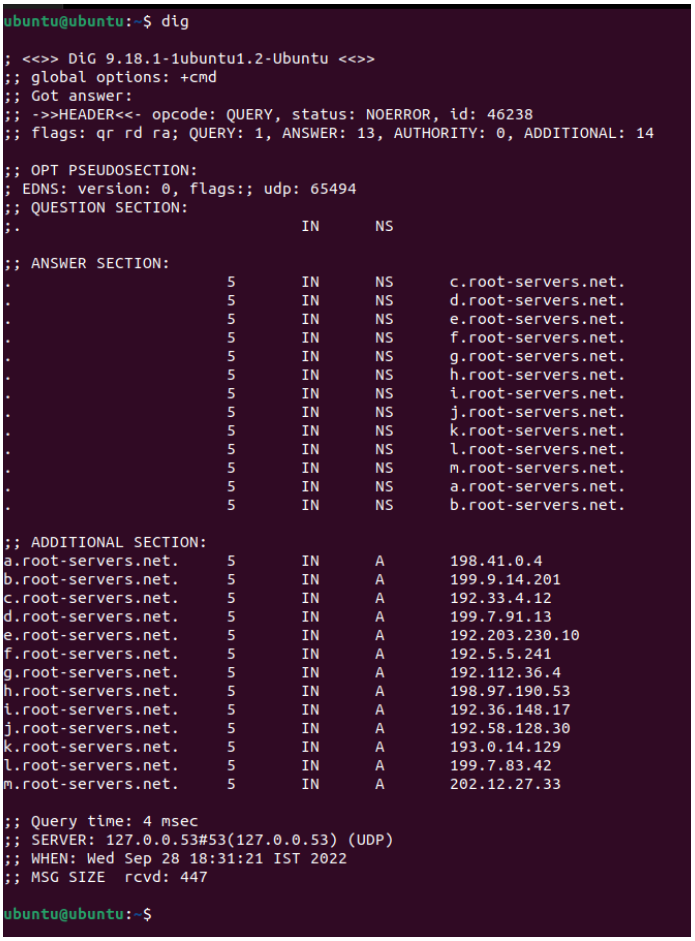
```
ubuntu@ubuntu:~$ whois 142.250.192.78

#
# 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 1997-2022, American Registry for Internet Numbers, Ltd.
#


NetRange:       142.250.0.0 - 142.251.255.255
CIDR:           142.250.0.0/15
NetName:        GOOGLE
NetHandle:      NET-142-250-0-0-1
Parent:         NET142 (NET-142-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS15169
Organization:   Google LLC (GOGL)
RegDate:        2012-05-24
Updated:        2012-05-24
Ref:            https://rdap.arin.net/registry/ip/142.250.0.0



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 the 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


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

OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-253-0000
```



```
ubuntu@ubuntu:~$ nslookup microsoft.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   microsoft.com
Address: 20.112.52.29
Name:   microsoft.com
Address: 20.53.203.50
Name:   microsoft.com
Address: 20.81.111.85
Name:   microsoft.com
Address: 20.84.181.62
Name:   microsoft.com
Address: 20.103.85.33

ubuntu@ubuntu:~$
```



```
ubuntu@ubuntu:~$ traceroute google.com
traceroute to google.com (172.217.174.238), 30 hops max, 60 byte packets
 1  _gateway (192.168.25.2)  0.495 ms  0.457 ms  0.420 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  *
 * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * *
```



```
ubuntu@ubuntu:~$ dig

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46238
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 14

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       5       IN      NS      c.root-servers.net.
.                       5       IN      NS      d.root-servers.net.
.                       5       IN      NS      e.root-servers.net.
.                       5       IN      NS      f.root-servers.net.
.                       5       IN      NS      g.root-servers.net.
.                       5       IN      NS      h.root-servers.net.
.                       5       IN      NS      i.root-servers.net.
.                       5       IN      NS      j.root-servers.net.
.                       5       IN      NS      k.root-servers.net.
.                       5       IN      NS      l.root-servers.net.
.                       5       IN      NS      m.root-servers.net.
.                       5       IN      NS      a.root-servers.net.
.                       5       IN      NS      b.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     5       IN      A       198.41.0.4
b.root-servers.net.     5       IN      A       199.9.14.201
c.root-servers.net.     5       IN      A       192.33.4.12
d.root-servers.net.     5       IN      A       199.7.91.13
e.root-servers.net.     5       IN      A       192.203.230.10
f.root-servers.net.     5       IN      A       192.5.5.241
g.root-servers.net.     5       IN      A       192.112.36.4
h.root-servers.net.     5       IN      A       198.97.190.53
i.root-servers.net.     5       IN      A       192.36.148.17
j.root-servers.net.     5       IN      A       192.58.128.30
k.root-servers.net.     5       IN      A       193.0.14.129
l.root-servers.net.     5       IN      A       199.7.83.42
m.root-servers.net.     5       IN      A       202.12.27.33

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Sep 28 18:31:21 IST 2022
;; MSG SIZE  rcvd: 447

ubuntu@ubuntu:~$
```

Conclusion:

Thus we have successfully used network reconnaissance tools to gather information about networks and domain registrars.