

Experiment No. 6

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

Theory:-

1. WHOIS : WHOIS is the Linux utility for searching an object in a WHOIS database. The WHOIS database of a domain is the publicly displayed information about a domains ownership, billing, technical, administrative, and nameserver information. Running a WHOIS on your domain will look the domain up at the registrar for the domain information. All domains have WHOIS information. WHOIS database can be queried to obtain the following information via WHOIS:

- Administrative contact details, including names, email addresses, and telephone numbers
- Mailing addresses for office locations relating to the target organization
- Details of authoritative name servers for each given domain

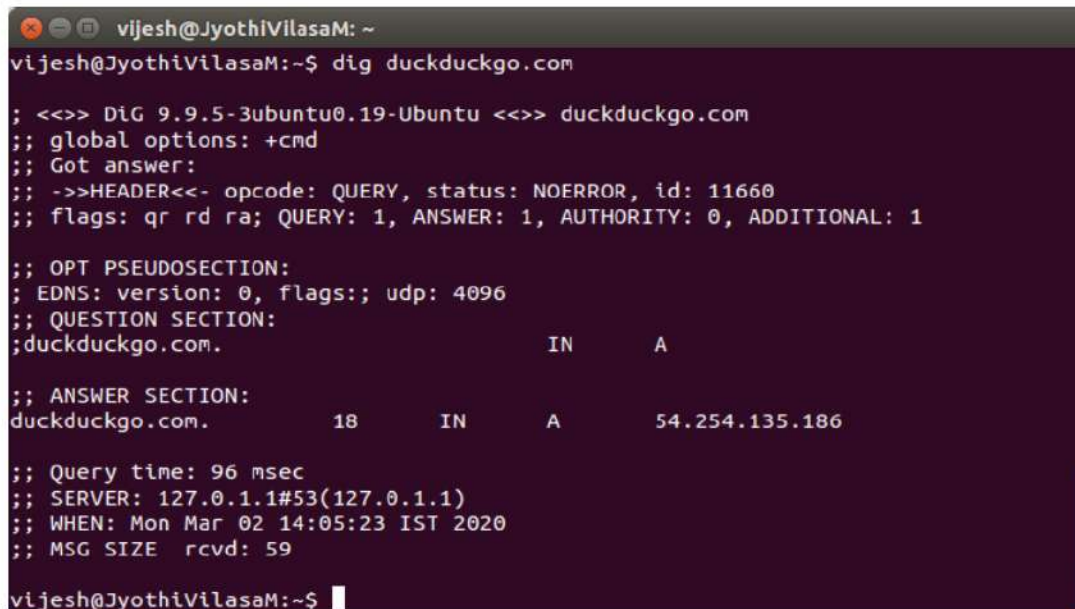
Example: Querying Facebook.com (in Figure 6.1)

```
viresh@jyothivilasam:~$ whois facebook.com
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2020-01-15T16:52:39Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2028-03-30T04:00:00Z
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#clientDeleteProhi
bited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP
rohibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhi
bited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhi
bited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferP
rohibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhi
bited
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-03-02T08:29:04Z <<<

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
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

2. Dig - Dig is a networking tool that can query DNS servers for information. It can be very helpful for diagnosing problems with domain pointing and is a good way to verify that your configuration is working. (in Figure 6.2)

A terminal window with a dark background and light-colored text. The prompt is 'vijesh@JyothiVilasaM: ~'. The command entered is 'dig duckduckgo.com'. The output shows DNS query details for duckduckgo.com, including header information, question section, and answer section with IP address 54.254.135.186.

```
vijesh@JyothiVilasaM: ~  
vijesh@JyothiVilasaM:~$ dig duckduckgo.com  
  
; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> duckduckgo.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11660  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;duckduckgo.com.                IN      A  
  
;; ANSWER SECTION:  
duckduckgo.com.                18      IN      A      54.254.135.186  
  
;; Query time: 96 msec  
;; SERVER: 127.0.1.1#53(127.0.1.1)  
;; WHEN: Mon Mar 02 14:05:23 IST 2020  
;; MSG SIZE  rcvd: 59  
  
vijesh@JyothiVilasaM:~$
```

Figure 6.2

3. Traceroute - traceroute prints the route that packets take to a network host. Traceroute utility uses the TTL field in the IP header to achieve its operation. For users who are new to TTL field, this field describes how much hops a particular packet will take while traveling on network. So, this effectively outlines the lifetime of the packet on network. This field is usually set to 32 or 64. Each time the packet is held on an intermediate router, it decreases the TTL value by 1. When a router finds the TTL value of 1 in a received packet then that packet is not forwarded but instead discarded. After discarding the packet, router sends an ICMP error message of —Time exceeded back to the source from where packet generated. The ICMP packet that is sent back contains the IP address of the router. So now it can be easily understood that traceroute operates by sending packets with TTL value starting from 1 and then incrementing by one each time. Each time a router receives the packet, it checks the TTL field, if TTL field is 1 then it discards the packet and sends the ICMP error packet containing its IP address and this is what traceroute requires. So traceroute incrementally fetches the IP of all the routers between the source and the destination. (in Figure 6.3)


```

vijesh@JyothiVilasaM: ~
vijesh@JyothiVilasaM:~$ traceroute google.co.in
traceroute to google.co.in (172.217.166.35), 30 hops max, 60 byte packets
 1 192.168.12.1 (192.168.12.1) 448.037 ms 448.028 ms 448.017 ms
 2 aipl-137-92-179-202.ankhnet.net (202.179.94.137) 448.011 ms 448.014 ms 44
7.994 ms
 3 * * *
 4 * * 10.241.1.6 (10.241.1.6) 449.092 ms
 5 10.240.254.130 (10.240.254.130) 447.931 ms 447.927 ms 447.900 ms
 6 * 10.240.254.1 (10.240.254.1) 31.824 ms 233.637 ms
 7 * * *
 8 150-232-14-103.intechonline.net (103.14.232.150) 211.929 ms 211.939 ms 21
1.915 ms
 9 * * *
10 bom07s18-in-f3.1e100.net (172.217.166.35) 62.026 ms 74.125.253.106 (74.125.
253.106) 35.558 ms bom07s18-in-f3.1e100.net (172.217.166.35) 61.878 ms
vijesh@JyothiVilasaM:~$

```

Figure 6.3

4. Nslookup - The nslookup command is used to query internet name servers interactively for information. nslookup, which stands for "name server lookup", is a useful tool for finding out information about a named domain. By default, nslookup will translate a domain name to an IP address (or vice versa). For instance, to find out what the IP address of microsoft.com is, you could run the command: (in Figure 6.4)

```

vijesh@JyothiVilasaM: ~
vijesh@JyothiVilasaM:~$ nslookup microsoft.com
Server:          127.0.1.1
Address:         127.0.1.1#53

Non-authoritative answer:
Name:   microsoft.com
Address: 40.76.4.15
Name:   microsoft.com
Address: 40.112.72.205
Name:   microsoft.com
Address: 40.113.200.201
Name:   microsoft.com
Address: 104.215.148.63
Name:   microsoft.com
Address: 13.77.161.179

vijesh@JyothiVilasaM:~$

```

Figure 6.4

Conclusion:

Various reconnaissance tools are studied and used to gather primary network information.