Name: Pankaj Parihar

Roll No.: 74

Batch: T21

Assignment – 5

Aim: To study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup, nikto, dmitry to gather information about networks and domain registrars.

Theory :

1. WHOIS: A command-line utility used to query databases that store information about the registration of domain names. It provides details such as the domain owner, contact information, registration and expiration dates, and nameserver data. This tool is often used for identifying who controls a domain.

2. dig (Domain Information Groper): A powerful DNS querying tool used to retrieve DNS records like A, MX, NS, and CNAME records. It's frequently used for diagnosing DNS issues and understanding how a domain is configured.

3. traceroute: A network diagnostic tool that traces the path packets take from your computer to a specified destination. It identifies each router (hop) on the way and measures the time taken for the round trip to each hop, helping to troubleshoot network delays or routing issues.

4. nslookup: A DNS query tool used for looking up specific DNS records associated with a domain or IP address. It can query different DNS servers and is often used to verify domain resolutions or troubleshoot DNS issues.

5. nikto: An open-source web server scanner designed to identify potential vulnerabilities in a web server, such as outdated software, default files, misconfigurations, and known security issues. It's widely used in penetration testing to assess web security.

6. dmitry (Deepmagic Information Gathering Tool): An all-in-one information-gathering tool that collects subdomains, email addresses, whois data, and open ports from a target host. It's used in the reconnaissance phase of penetration testing to gain initial insights into a target domain.

Output:

1. **whois:**

```
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
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: 2024-08-02T02:17:33+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
```

2. **dig:**

```
ubuntu@ip-172-31-37-111:~$ dig geeksforgeeks.org

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> geeksforgeeks.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50540
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;geeksforgeeks.org.             IN      A

;; ANSWER SECTION:
geeksforgeeks.org.      30      IN      A       34.218.62.116

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Aug 08 06:43:41 UTC 2024
;; MSG SIZE  rcvd: 62

ubuntu@ip-172-31-37-111:~$
```

3. traceroute:

```
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-37-111:~$ traceroute google.com
traceroute to google.com (142.251.16.139), 30 hops max, 60 byte packets
 1  216.182.238.109 (216.182.238.109)  4.223 ms 216.182.238.147 (216.182.238.147)  1.800 ms 244.5.3.9 (244.5.3.9)  1.641 ms
 2  * * 100.65.53.144 (100.65.53.144)  6.516 ms
 3  100.66.11.186 (100.66.11.186)  15.542 ms 100.66.15.128 (100.66.15.128)  21.800 ms 100.66.40.72 (100.66.40.72)  0.727 ms
 4  100.66.50.28 (100.66.50.28)  17.251 ms 242.3.85.71 (242.3.85.71)  1.935 ms 241.0.4.66 (241.0.4.66)  0.397 ms
 5  241.0.4.78 (241.0.4.78)  0.379 ms 240.0.184.2 (240.0.184.2)  1.089 ms 100.66.6.29 (100.66.6.29)  1.993 ms
 6  240.0.184.2 (240.0.184.2)  1.194 ms 240.0.184.1 (240.0.184.1)  1.030 ms 99.82.180.135 (99.82.180.135)  2.081 ms
 7  * 100.65.97.4 (100.65.97.4)  1.965 ms 242.3.84.71 (242.3.84.71)  1.728 ms
 8  142.251.53.0 (142.251.53.0)  5.199 ms 100.100.34.104 (100.100.34.104)  2.400 ms 142.251.52.62 (142.251.52.62)  2.942 ms
 9  192.178.243.4 (192.178.243.4)  8.073 ms * 100.66.55.254 (100.66.55.254)  15.780 ms
10  142.251.49.189 (142.251.49.189)  2.431 ms 216.239.42.137 (216.239.42.137)  2.141 ms 241.0.4.70 (241.0.4.70)  0.360 ms
11  192.178.243.4 (192.178.243.4)  1.554 ms * *
12  72.14.236.229 (72.14.236.229)  6.448 ms * 142.250.209.110 (142.250.209.110)  4.060 ms
13  142.251.227.155 (142.251.227.155)  4.147 ms 108.170.235.157 (108.170.235.157)  6.260 ms 142.251.49.19 (142.251.49.19)  2.331 ms
14  142.250.210.4 (142.250.210.4)  1.879 ms * 99.82.180.135 (99.82.180.135)  2.383 ms
15  * 142.251.77.241 (142.251.77.241)  2.447 ms 142.251.227.157 (142.251.227.157)  2.305 ms
16  142.251.68.13 (142.251.68.13)  2.097 ms * 142.251.70.82 (142.251.70.82)  3.695 ms
17  * 192.178.110.210 (192.178.110.210)  1.640 ms *
18  * * *
19  * * 142.251.237.185 (142.251.237.185)  3.244 ms
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  bl-in-f139.1e100.net (142.251.16.139)  2.251 ms  2.446 ms  2.188 ms
ubuntu@ip-172-31-37-111:~$
```

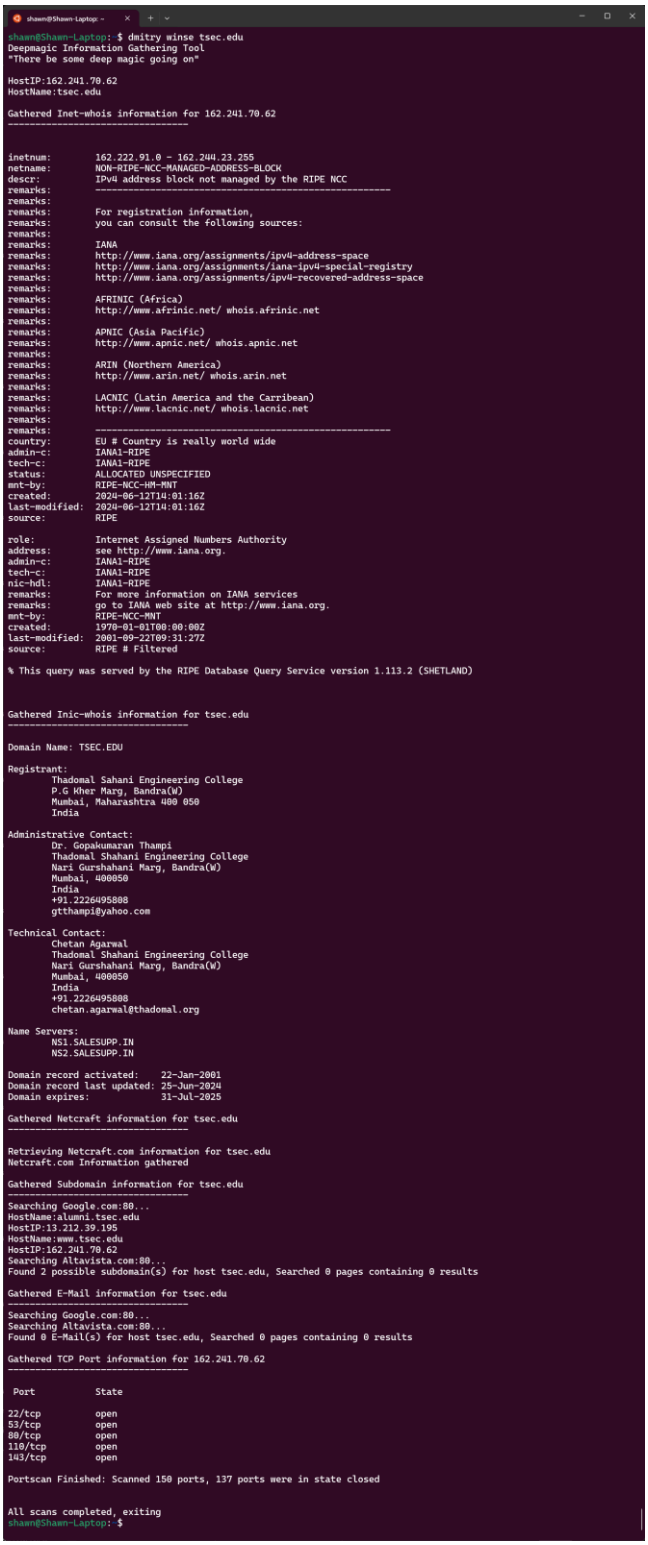
4. **nslookup:**

```
ubuntu@ip-172-31-37-111:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.16.102
Name:   google.com
Address: 142.251.16.113
Name:   google.com
Address: 142.251.16.138
Name:   google.com
Address: 142.251.16.139
Name:   google.com
Address: 142.251.16.100
Name:   google.com
Address: 142.251.16.101
Name:   google.com
Address: 2607:f8b0:4004:c1b::8a
Name:   google.com
Address: 2607:f8b0:4004:c1b::64
Name:   google.com
Address: 2607:f8b0:4004:c1b::65
Name:   google.com
Address: 2607:f8b0:4004:c1b::66

ubuntu@ip-172-31-37-111:~$
```

5. **nikto:**

```
ubuntu@ubuntu:~/nikto/program$ perl nikto.pl -h tsec.edu
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          162.241.70.62
+ Target Hostname:    tsec.edu
+ Target Port:        80
+ Start Time:         2024-10-21 13:51:16 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache
+ Root page / redirects to: https://tsec.edu/
```

6. **dmitry:**



Conclusion: Explored the different network reconnaissance tools to gather information about networks (LO3 is achieved).