Name: Harsh Mishra
Roll no: 64
Batch: T21

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 nikto: An open-source web server scanner designed to identify potential vulnerabilities in a web server, such as outdated software, default files, misconfigurations, and known security issues.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:**

Name: Harsh Mishra
Roll no: 64
Batch: T21

```
harsh@DESKTOP-8O5FLRG:~$ whois tsec.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

----------------------------------------------------------

Domain Name: TSEC.EDU

Registrant:
        Thadomal Sahani Engineering College
        P.G Kher Marg, Bandra(W)
        Mumbai, Maharashtra 400 050
        India

Administrative Contact:
        Dr. Gopakumaran Thampi
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
        +91.2226495808
        gtthampi@yahoo.com

Technical Contact:
        Chetan Agarwal
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
```

2. **dig:**

Name: Harsh Mishra
Roll no: 64
Batch: T21

```
harsh@DESKTOP-8O5FLRG:~$ dig tsec.edu

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> tsec.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1926
;; flags: qr rd ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;tsec.edu.                      IN      A

;; ANSWER SECTION:
tsec.edu.               0       IN      A       162.241.70.62
ns1.salesupp.in.        0       IN      A       162.241.70.62
ns2.salesupp.in.        0       IN      A       162.241.70.62

;; Query time: 420 msec
;; SERVER: 172.27.32.1#53(172.27.32.1) (UDP)
;; WHEN: Mon Oct 21 20:34:51 IST 2024
;; MSG SIZE  rcvd: 112
```

3. **traceroute:**

```
harsh@DESKTOP-8O5FLRG:~$ traceroute tsec.edu
traceroute to tsec.edu (162.241.70.62), 64 hops max
  1   172.27.32.1  0.256ms  0.151ms  0.113ms
  2   192.168.0.1  1.978ms  1.904ms  4.810ms
  3   103.31.144.7  2.847ms  6.793ms  2.622ms
  4   *  *  *
  5   103.31.144.21  4.537ms  9.380ms  11.770ms
  6   49.248.173.21  10.092ms  8.196ms  6.770ms
  7   *  *  *
```

4. **nslookup:**

```
harsh@DESKTOP-8O5FLRG:~$ nslookup tsec.edu
Server:         172.27.32.1
Address:        172.27.32.1#53

Non-authoritative answer:
Name:   tsec.edu
Address: 162.241.70.62
Name:   ns1.salesupp.in
Address: 162.241.70.62
Name:   ns2.salesupp.in
Address: 162.241.70.62
```

Name: Harsh Mishra
Roll no: 64
Batch: T21

5. **nikto:**

```
harsh@DESKTOP-8O5FLRG:~$ nikto -h tsec.edu
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          162.241.70.62
+ Target Hostname:    tsec.edu
+ Target Port:        80
+ Start Time:         2024-10-21 20:39:15 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://tsec.edu/
```

6. **dmitry:**

```
harsh@DESKTOP-8O5FLRG:~$ dmitry winse tsec.edu
Deepmagic Information Gathering Tool
"There be some deep magic going on"
^Charsh@DESKTOP-8O5FLRG:~$ dmitry winse tsec.edu
HostIP:162.241.70.62 found, but can be installed with:
HostName:tsec.edudmitry
harsh@DESKTOP-8O5FLRG:~$ sudo apt install dmitry
Gathered Inet-whois information for 162.241.70.62
---------------------------------
Reading state information... Done
inetnum:        162.222.91.0 - 162.244.23.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC.
remarks:        -----------------------------------------------------
remarks:is operation, 54.3 kB of additional disk space will be used.
remarks:        For registration information,universe amd64 dmitry amd64 1.3a-1.2
remarks:        you can consult the following sources:
remarks:16.7 kB in 1s (24.2 kB/s)
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        -----------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
```

Name: Harsh Mishra
Roll no: 64
Batch: T21

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