Assignment 4

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

LO Mapped: LO3

Theory:

- WHOIS

The whois command displays information about a website's record. You may get all the information about a website regarding its registration and owner's information.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ 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: 2023-08-08T05:48:12Z <<<
```

- dig

dig command stands for **Domain Information Groper**. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dig www.google.com

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27441
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         75      IN      A       142.250.192.132

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Aug 08 11:29:33 IST 2023
;; MSG SIZE  rcvd: 59
```

- Traceroute

traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute google.com
traceroute to google.com (142.251.42.14), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  0.713 ms  0.711 ms  0.694 ms
 2  203.212.25.1 (203.212.25.1)  2.584 ms  2.592 ms  2.813 ms
 3  203.212.24.53 (203.212.24.53)  2.560 ms  2.552 ms  3.053 ms
 4  * * 10.10.226.153 (10.10.226.153)  4.219 ms
 5  72.14.196.213 (72.14.196.213)  8.154 ms  8.143 ms  4.715 ms
 6  108.170.248.177 (108.170.248.177)  4.904 ms  5.474 ms  5.204 ms
 7  209.85.250.139 (209.85.250.139)  4.781 ms  2.042 ms  2.030 ms
 8  bom12s19-in-f14.1e100.net (142.251.42.14)  2.126 ms  2.289 ms  2.755 ms
```

- nslookup

The nslookup command **queries internet domain name servers in two modes**. Interactive mode allows you to query name servers for information about various hosts and domains, or to print a list of the hosts in a domain.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.42.14
Name:   google.com
Address: 2404:6800:4009:82f::200e
```

- nikto

Nikto is an open source web server and web application scanner. Nikto can perform comprehensive tests against web servers for multiple security threats, including over 6700 potentially dangerous files/programs. Nikto can also perform checks for outdated web servers software, and version-specific problems.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          157.240.192.35
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2023-08-08 11:54:26 (GMT5.5)
---------------------------------------------------------------------------
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'proxy-status' found, with contents: http_request_error; e_clientaddr="AcLHSJ5kd9scY9Ol-zV7mMz9J6eFGG4gXftcTKNsDdkDmXSUcRbJ2nGiv_7tHwQnA4jVNpHWWbGPy10
0sdw3"; e_fb_vipaddr="AcJwsHMwiQCLSif1b7SUxciHeBFfdSYSW1L2ZH7vu_pVS5UIWbAxlLRu2MgV_5W_UZuOiHpaNRo"; e_fb_builduser="AcI_kbko1ZVnsYpCBYc17BqMhEI_iSAJnbhpR21CLdqX_6-4q-3j
LCG90z_pY9h5SDE"; e_fb_binaryversion="AcJ_73IhdWgJ_X0eWF9RCd5OVod35-dSK1tG2RZIM4ZISC4BdSRO0YUkiOd90SlGlaqnI02f24A8Q_JabP5x1R9bxog0y1Yzouc"; e_proxy="AcIFqBFJpc1Eb5F2iXd
TkwMxfB3Y6HYd5ZZYnGhjfTAS9bGIT_b0fZc2aeZ2HNr5MwsudQwNHh-rK5E"
+ 6544 items checked: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2023-08-08 11:57:25 (GMT5.5) (179 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- dmitry

dmitry can find possible subdomains, email addresses, uptime information, perform tcp port scan, whois lookups, and more.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dmitry google.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:142.251.42.14
HostName:google.com

Gathered Inet-whois information for 142.251.42.14
---------------------------------

inetnum:        142.248.0.0 - 143.46.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        -----------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
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
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2023-07-24T14:32:43Z
last-modified:  2023-07-24T14:32:43Z
source:         RIPE
```

Conclusion: In this experiment we used different network reconnaissance tools to gather information about the network.