

LAB ASSIGNMENT NO. 6

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

LAB OUTCOME ATTAINED:

LO 3: Explore the different network reconnaissance tools to gather information about networks.

THEORY:

1. whois

The "whois" command is used to retrieve registration and ownership details of domain names, IP addresses, or ASNs by querying WHOIS databases.

For example: ``whois example.com`` retrieves information about the domain "example.com".

Attackers use the "whois" command to gather domain ownership, contact details, and registration dates. This information aids in social engineering, spear phishing, and domain hijacking attacks, exploiting vulnerabilities based on the revealed organisational structure and registration history.

2. dig

The "dig" command is a network tool used to perform DNS queries, providing information about domain names, IP addresses, and DNS records. It assists in troubleshooting network issues and verifying DNS configurations.

Options:

- ``dig example.com MX`` - Retrieves Mail Exchange records for "example.com."
- ``dig -x 8.8.8.8`` - Performs reverse DNS lookup for IP address 8.8.8.8.
- ``dig +short example.com`` - Shows only IP addresses associated with "example.com."
- ``dig example.com NS +trace`` - Traces delegation path and queries authoritative nameservers for "example.com."
- ``dig example.com AAAA +dnssec`` - Requests IPv6 addresses with DNSSEC information.
- ``dig example.com SOA +noall +answer`` - Retrieves Start of Authority record, displaying only the answer section.

3. traceroute

The "traceroute" command is a network diagnostic tool that traces the route and measures the round-trip time of packets as they travel through routers between a source and a destination IP address. It helps identify network paths and potential bottlenecks.

The "traceroute" command works by sending packets with gradually increasing Time-to-Live (TTL) values. As each packet travels through routers, the TTL decreases. When the TTL becomes zero, the router discards the packet and sends an ICMP Time Exceeded message back to the source. By analysing the series of ICMP messages and their round-trip times, "traceroute" maps the network path from the source to the destination. The source IP and port remain constant, while the destination port and TTL change for each packet to build the path and calculate latency.

4. Nslookup

The "nslookup" command is a network utility used to query DNS servers for domain name resolution, IP address retrieval, and DNS record information. It assists in diagnosing DNS-related issues and providing essential network information.

5. Nikto:

Nikto is built on LibWhisker (by RFP) and can run on any platform which has a Perl environment. It supports SSL, proxies, host authentication, IDS evasion and more. It can be updated automatically from the command-line, and supports the optional submission of updated version data back to the maintainers.

Generally, vulnerabilities in websites can lead to various attacks such as Cross-Site Scripting (XSS), SQL Injection, Remote Code Execution, and Information Disclosure. The potential impact of an exploit depends on the nature of the vulnerability and the attacker's intentions, which could include data theft, website defacement, unauthorised access, and more. Always prioritise security patching and follow best practices to mitigate such risks.

6. Dmitry:

DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux command line application with the ability to gather as much information as possible about a host.

Basic functionality of DMitry allows for information to be gathered about a target host from a simple whois lookup on the target to uptime reports and TCP port scans.

The application is considered a tool to assist in information gathering when information is required quickly by removing the need to enter multiple commands and the timely process of searching through data from multiple sources.

1. WHOIS Lookup:

```
dmitry -w example.com
```

2. IP WHOIS Lookup:

```
dmitry -wi 8.8.8.8
```

3. Retrieve Netcraft Info:

```
dmitry -n example.com
```

4. Search for Subdomains:

```
dmitry -s example.com
```

5. Search for Email Addresses:

```
dmitry -e example.com
```

6. TCP Port Scan:

```
dmitry -p example.com
```

7. Save Output to example.txt:

```
dmitry -s -e -p example.com > example.txt
```

Email Harvesting Command:

dmitry -e example.com

Subdomain Harvesting Command:

dmitry -s example.com

OUTPUT:

```

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man whois
Domain Name: WIKIPEDIA.COM
Registry Domain ID: 51687032_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-12-09T09:17:04Z
Creation Date: 2001-01-13T00:12:14Z
Registry Expiry Date: 2024-01-10T05:28:20Z
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
Name Server: NS0.WIKIMEDIA.ORG
Name Server: NS1.WIKIMEDIA.ORG
Name Server: NS2.WIKIMEDIA.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-02T05:26:29Z <<<

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.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
warrant the accuracy or reliability of the data. VeriSign reserves the right
to remove or otherwise modify the information at any time without notice, and
is not responsible for any damages or losses, including those resulting from
reliance on the information.
  
```

```

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ 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

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

Administrative Contact:
Dr. Gopakumaran Thampi
Thadomal Sahani Engineering College
Nari Gurshahani Marg, Bandra(W)
Mumbai, 400050
India
+91.2226495008
gtthampi@yahoo.com

Technical Contact:
Chetan Agarwal
Thadomal Sahani Engineering College
  
```

Roll no. : 53
Name: Shreya Kamath
Date: 7th August, 2023.

```
Activities Terminal Wed 11:06
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~

--back          ^-F -N 1'
                  Guess the number of hops in the backward path and
--V --version    print if it differs
--help          Print version info and exit
                  Read this help and exit

Arguments:
+ host           The host to traceroute to
+ packetlen      The full packet length (default is the length of an IP
                  header plus 40). Can be ignored or increased to a minimal
                  allowed value
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man traceroute
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute wikipedia.com
traceroute to wikipedia.com (103.102.166.226), 30 hops max, 60 byte packets
 1 _gateway (192.168.0.1)  0.559 ms  0.491 ms  0.639 ms
 2 203.212.25.1 (203.212.25.1)  1.754 ms  1.706 ms  1.792 ms
 3 203.212.24.53 (203.212.24.53)  2.060 ms  1.981 ms  1.933 ms
 4 * * *
 5 46-97-87-183.mysipl.com (183.87.97.46)  3.392 ms  42-97-87-183.mysipl.com (183.87.97.42)  3.712 ms  3.664 ms
 6 172.31.180.57 (172.31.180.57)  25.938 ms  27.698 ms  24.869 ms
 7 lx-ae-4-2.tcore1.cxr-chennai.as6453.net (180.87.36.9)  39.786 ms  24.777 ms  24.716 ms
 8 if-be-34-2.ecore2.esin4-singapore.as6453.net (180.87.36.41)  60.986 ms  61.035 ms  61.117 ms
 9 if-be-10-2.ecore2.svq-singapore.as6453.net (180.87.107.0)  60.576 ms  57.770 ms  57.640 ms
10 if-ae-46-2.thar1.svq-singapore.as6453.net (120.29.214.10)  61.923 ms  62.374 ms  60.524 ms
11 if-ae-1-2.thar1.40b-singapore.as6453.net (180.87.98.69)  58.864 ms  58.748 ms  57.118 ms
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$

Activities Terminal Wed 11:07
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~

allowed value
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man traceroute
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute wikipedia.com
traceroute to wikipedia.com (103.102.166.226), 30 hops max, 60 byte packets
 1 _gateway (192.168.0.1)  0.559 ms  0.491 ms  0.639 ms
 2 203.212.25.1 (203.212.25.1)  1.754 ms  1.706 ms  1.792 ms
 3 203.212.24.53 (203.212.24.53)  2.060 ms  1.981 ms  1.933 ms
 4 * * *
 5 46-97-87-183.mysipl.com (183.87.97.46)  3.392 ms  42-97-87-183.mysipl.com (183.87.97.42)  3.712 ms  3.664 ms
 6 172.31.180.57 (172.31.180.57)  25.938 ms  27.698 ms  24.869 ms
 7 lx-ae-4-2.tcore1.cxr-chennai.as6453.net (180.87.36.9)  39.786 ms  24.777 ms  24.716 ms
 8 if-be-34-2.ecore2.esin4-singapore.as6453.net (180.87.36.41)  60.986 ms  61.035 ms  61.117 ms
 9 if-be-10-2.ecore2.svq-singapore.as6453.net (180.87.107.0)  60.576 ms  57.770 ms  57.640 ms
10 if-ae-46-2.thar1.svq-singapore.as6453.net (120.29.214.10)  61.923 ms  62.374 ms  60.524 ms
11 if-ae-1-2.thar1.40b-singapore.as6453.net (180.87.98.69)  58.864 ms  58.748 ms  57.118 ms
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute instagram.com
traceroute to instagram.com (31.13.79.174), 30 hops max, 60 byte packets
 1 _gateway (192.168.0.1)  0.628 ms  0.610 ms  0.719 ms
 2 203.212.25.1 (203.212.25.1)  2.366 ms  2.354 ms  2.342 ms
 3 203.212.24.53 (203.212.24.53)  2.330 ms  2.319 ms  2.397 ms
 4 * * *
 5 5pak.choicerealtysservices.co.in (120.138.114.14)  3.056 ms  4.770 ms  3.027 ms
 6 poi04.psw03.bom1.tfbnw.net (157.240.52.207)  3.231 ms  2.067 ms  2.050 ms
 7 157.240.36.13 (157.240.36.13)  2.021 ms  157.240.39.71 (157.240.39.71)  1.985 ms  157.240.39.99 (157.240.39.99)  1.967 ms
 8 instagram-p42-shv-02-bom1.fbcnd.net (31.13.79.174)  1.954 ms  2.294 ms  1.916 ms
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

Roll no. : 53
Name: Shreya Kamath
Date: 7th August, 2023.

```
Activities Terminal Wed 11:09
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man dig
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dig wikipedia.com

;<<<>> DIG 9.11.3-1ubuntu1.18-Ubuntu <<<>> wikipedia.com
;; global options: +cnd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 27676
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
wikipedia.com.                402     IN      A      103.102.166.226

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Aug 02 11:09:25 IST 2023
;; MSG SIZE rcvd: 58

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dig coolers.com

;<<<>> DIG 9.11.3-1ubuntu1.18-Ubuntu <<<>> coolers.com
;; global options: +cnd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 14625
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
coolers.com.                  300     IN      A      172.67.204.14
coolers.com.                  300     IN      A      104.21.58.133

;; Query time: 133 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Aug 02 11:09:37 IST 2023
;; MSG SIZE rcvd: 72

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man nslookup
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man nslookup
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nslookup wikipedia.com
Server:                127.0.0.53
Address:                127.0.0.53#53

Non-authoritative answer:
Name:    wikipedia.com
Address: 103.102.166.226
Name:    wikipedia.com
Address: 2001:df2:e500:ed1a::3

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

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

Non-authoritative answer:
Name:    figma.com
Address: 108.158.61.109
Name:    figma.com
Address: 108.158.61.89
Name:    figma.com
Address: 108.158.61.101
Name:    figma.com
Address: 108.158.61.77

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h wikipedia.com
- Nikto v2.1.5
-----
+ Target IP:      103.102.166.226
+ Target Hostname: wikipedia.com
+ Target Port:    80
+ Start Time:    2023-08-02 11:16:43 (GMT5.5)
-----
+ Server: nginx/1.18.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://wikipedia.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)

^lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h tsec.edu
- Nikto v2.1.5
-----
+ Target IP:      162.241.70.62
+ Target Hostname: tsec.edu
+ Target Port:    80
+ Start Time:    2023-08-02 11:19:35 (GMT5.5)
-----
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://tsec.edu/
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$

```

```

lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
-----
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://tsec.edu/
^lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man dmitry
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 Caribbean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
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

```

Roll no. : 53
Name: Shreya Kamath
Date: 7th August, 2023.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.107 (SHETLAND)

Gathered Inic-whois information for 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: 2023-08-02T05:52:13Z <<<

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.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
update domain name contact information. The Data is provided by Global Registry
```

```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
Gathered Subdomain Information for google.com
-----
Searching Google.com:80...
HostName:naps.google.com
HostIP:142.250.183.14
HostName:www.google.com
HostIP:142.250.192.132
HostName:scholar.google.com
HostIP:142.250.182.228
HostName:analytics.google.com
HostIP:216.239.34.181
HostName:contacts.google.com
HostIP:142.250.192.110
HostName:keep.google.com
HostIP:216.239.32.176
HostName:support.google.com
HostIP:142.250.192.46
HostName:myactivity.google.com
HostIP:74.125.130.102
HostName:accounts.google.com
HostIP:216.58.196.77
HostName:images.google.com
HostIP:142.250.183.142
HostName:play.google.com
HostIP:142.250.183.142
HostName:one.google.com
HostIP:142.250.183.46
HostName:trends.google.com
HostIP:142.250.183.4
HostName:passwords.google.com
HostIP:142.250.183.46
HostName:meet.google.com
HostIP:142.251.42.110
HostName:cloud.google.com
HostIP:142.250.192.14
HostName:store.google.com
HostIP:142.250.192.46
HostName:ads.google.com
HostIP:142.250.183.78
HostName:apps.google.com
HostIP:142.250.183.46
HostName:pay.google.com
HostIP:172.217.194.92
HostName:takeout.google.com
HostIP:142.250.199.142
HostName:developer.google.com
```

```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~  
File Edit View Search Terminal Help  
HostName:earth.google.com  
HostIP:142.250.183.46  
HostName:firebase.google.com  
HostIP:142.250.183.14  
HostName:search.google.com  
HostIP:142.250.183.46  
HostName:developers.google.com  
HostIP:142.250.182.206  
HostName:console.cloud.google.com  
HostIP:142.250.183.46  
HostName:docs.google.com  
HostIP:142.250.192.78  
HostName:drive.google.com  
HostIP:142.250.192.14  
HostName:groups.google.com  
HostIP:216.239.32.177  
HostName:picasa.google.com  
HostIP:142.250.183.4  
HostName:tagmanager.google.com  
HostIP:142.250.183.46  
HostName:messages.google.com  
HostIP:142.250.182.238  
HostName:classroom.google.com  
HostIP:142.250.183.206  
Searching Altavista.com:80...  
Found 38 possible subdomain(s) for host google.com, Searched 0 pages containing 0 results  
  
Gathered E-Mail information for google.com  
-----  
Searching Google.com:80...  
admin@google.com  
kbr@google.com  
security@google.com  
terryok@google.com  
info@google.com  
postmaster@aspmx.l.google.com  
Searching Altavista.com:80...  
Found 6 E-Mail(s) for host google.com, Searched 0 pages containing 0 results  
  
Gathered TCP Port information for 142.251.42.14  
-----  


| Port | State |
|------|-------|
|------|-------|

  
  
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~  
File Edit View Search Terminal Help  
HostName:developers.google.com  
HostIP:142.250.182.206  
HostName:console.cloud.google.com  
HostIP:142.250.183.46  
HostName:docs.google.com  
HostIP:142.250.192.78  
HostName:drive.google.com  
HostIP:142.250.192.14  
HostName:groups.google.com  
HostIP:216.239.32.177  
HostName:picasa.google.com  
HostIP:142.250.183.4  
HostName:tagmanager.google.com  
HostIP:142.250.183.46  
HostName:messages.google.com  
HostIP:142.250.182.238  
HostName:classroom.google.com  
HostIP:142.250.183.206  
Searching Altavista.com:80...  
Found 38 possible subdomain(s) for host google.com, Searched 0 pages containing 0 results  
  
Gathered E-Mail information for google.com  
-----  
Searching Google.com:80...  
admin@google.com  
kbr@google.com  
security@google.com  
terryok@google.com  
info@google.com  
postmaster@aspmx.l.google.com  
Searching Altavista.com:80...  
Found 6 E-Mail(s) for host google.com, Searched 0 pages containing 0 results  
  
Gathered TCP Port information for 142.251.42.14  
-----  


| Port   | State |
|--------|-------|
| 80/tcp | open  |

  
Portscan Finished: Scanned 150 ports, 0 ports were in state closed  
  
All scans completed, exiting  
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

CONCLUSION:

Hence, I have successfully executed a comprehensive study of network reconnaissance tools, including WHOIS, dig, traceroute, nslookup, Nikto, and Dmitry. These tools revealed invaluable data about network configurations, domain ownership, and potential vulnerabilities. This practical exposure enhances my understanding of network analysis, security assessment, and the critical role these tools play in ensuring robust network security.