Assignment 7

Aim:-
Study the use of network reconnaissance tools like WHOSI ,dig ,traceroute ,nslookup ,nikto ,dmitry to gather information about networks and domain registars

WHOIS

Whois is a command-line utility used in Linux systems to retrieve information about domain names, IP addresses, and network devices registered with the Internet Corporation for Assigned Names and Numbers (ICANN). The data received by Whois consists of the name and contact information of the domain or IP address owner, the registration and expiration date, the domain registrar, and the server information. Whois command can be very useful for network administrators, web developers, and security professionals for achieving various tasks like checking network connectivity or troubleshooting. In this article, we will go through the usage of the Whois command on Linux (Ubuntu system).

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ whois geeksforgeeks.org
Domain Name: geeksforgeeks.org
Registry Domain ID: f507261c73964021b7430545a8b370ee-LROR
Registrar WHOIS Server: http://whois.publicdomainregistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2022-04-21T06:36:07Z
Creation Date: 2009-03-19T06:08:55Z
Registry Expiry Date: 2030-03-19T06:08:55Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED
Registrant Name: REDACTED
Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org)
Registrant Street: REDACTED
Registrant City: REDACTED
Registrant State/Province: MA
Registrant Postal Code: REDACTED
Registrant Country: US
Registrant Phone: REDACTED
Registrant Phone Ext: REDACTED
Registrant Fax: REDACTED
Registrant Fax Ext: REDACTED
Registrant Email: REDACTED
Registry Admin ID: REDACTED
Admin Name: REDACTED
Admin Organization: REDACTED
Admin Street: REDACTED
Admin City: REDACTED
Admin State/Province: REDACTED
Admin Postal Code: REDACTED
Admin Country: REDACTED
Admin Phone: REDACTED
Admin Phone Ext: REDACTED
Admin Fax: REDACTED
Admin Fax Ext: REDACTED
Admin Email: REDACTED
Registry Tech ID: REDACTED
Tech Name: REDACTED
Tech Organization: REDACTED
Tech Street: REDACTED
Tech City: REDACTED
Tech State/Province: REDACTED
```

dig

dig command stands for ***Domain Information Groper***. It retrieves information about DNS name servers. Network administrators use it to verify and troubleshoot DNS problems and perform DNS lookups. The dignslookup and the host.

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

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18563
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
google.com.             262     IN      A       142.251.43.14

;; Query time: 2 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Jul 24 15:07:50 IST 2025
;; MSG SIZE  rcvd: 55
```

nslookup

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS-related problems.

```
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: 142.251.43.14
Name:   google.com
Address: 2404:6800:4009:809::200e
```

traceroute

The `**traceroute**` command is a network diagnostic tool used to trace the route taken by packets from a source to a destination over an IP network. It provides valuable insights into the network path, including the number of hops (routers) between the source and destination and the round-trip time (RTT) for each hop.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute www.goole.com
traceroute to www.goole.com (217.160.0.201), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  0.655 ms  0.614 ms  5.373 ms
 2  203.212.25.1 (203.212.25.1)  2.165 ms  2.275 ms  2.097 ms
 3  203.212.24.53 (203.212.24.53)  2.207 ms  2.297 ms  2.245 ms
 4  10.10.226.153 (10.10.226.153)  3.110 ms  3.620 ms  3.566 ms
 5  * * *
 6  203.200.11.141.ill-bgl.static.vsnl.net.in (203.200.11.141)  4.257 ms * *
 7  172.28.118.237 (172.28.118.237)  3.655 ms  3.585 ms *
 8  * * *
 9  if-ae-2-2.tcore2.mlv-mumbai.as6453.net (180.87.38.2)  192.463 ms if-ae-32-2.tcore2.mlv-mumbai.as6453.net (180.87.38.147)  189.349 ms  189.342 ms
10  * * *
11  * * *
12  195.219.213.137 (195.219.213.137)  129.937 ms  129.922 ms  129.983 ms
13  ldn-bb1-link.ip.twelve99.net (62.115.140.72)  132.854 ms ldn-bb2-link.ip.twelve99.net (62.115.140.70)  122.780 ms ldn-bb1-link.ip.twelve99.net (62.115.120.74)  122.
755 ms
14  prs-bb2-link.ip.twelve99.net (62.115.133.239)  128.429 ms  127.964 ms  127.780 ms
15  ffm-bb2-link.ip.twelve99.net (62.115.122.139)  141.139 ms  138.163 ms ffm-bb1-link.ip.twelve99.net (62.115.123.12)  129.086 ms
16  * * *
17  ionos-ic-350360.ip.twelve99-cust.net (62.115.181.11)  131.592 ms  129.463 ms  129.378 ms
18  lo-0.rc-b.bs.kae.de.net.ionos.com (212.227.117.207)  129.845 ms  130.239 ms  129.430 ms
19  lo-0.gw-distd-sh-1.bs.kae.de.net.ionos.com (212.227.112.252)  130.140 ms lo-0.gw-distd-sh-2.bs.kae.de.net.ionos.com (212.227.112.253)  138.687 ms  138.659 ms
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Nikto

Nikto is an open-source web server scanner which performs comprehensive tests against web servers for multiple items. You can use Nikto with any web servers like Apache, Nginx, IHS, OHS, Litespeed, and so on. Nikto can check for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Items and plugins scanned by Nikto are frequently updated and can be automatically updated

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h google.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          142.251.43.14
+ Target Hostname:    google.com
+ Target Port:        80
+ Start Time:         2025-07-24 15:32:33 (GMT5.5)
---------------------------------------------------------------------------
+ Server: gws
+ Uncommon header 'content-security-policy-report-only' found, with contents: object-src 'none';base-uri 'self';script-src 'nonce-3Ag21l5IuFZbmPsMF5lTPQ' 'strict-dynami
c' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Root page / redirects to: http://www.google.com/
+ Uncommon header 'referrer-policy' found, with contents: no-referrer
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'gws' to 'sffe' which may suggest a WAF, load balancer or proxy is in place
+ Uncommon header 'cross-origin-resource-policy' found, with contents: cross-origin
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Cookie AEC created without the httponly flag
+ Cookie NID created without the httponly flag
+ Uncommon header 'content-security-policy' found, with contents: object-src 'none';base-uri 'self';script-src 'nonce-Vvypc2knlVm2iE_1uvkrfQ' 'strict-dynamic' 'report-s
ample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
+ Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-W
oW64, Sec-CH-UA-Form-Factors, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version
+ Uncommon header 'permissions-policy' found, with contents: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=
*, ch-ua-form-factors=*, ch-ua-platform=*, ch-ua-platform-version=*
+ Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin
```

dmitry

Dmitry is a free and open-source tool available on GitHub. The tool is used for information gathering. You can download the tool and install in your Kali Linux. Dmitry stands for DeepMagic Information Gathering Tool. It's a command-line tool Using Dmitry tool You can collect information about the target, this information can be used for social engineering attacks. It can be used to gather a number of valuable pieces of information

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

HostIP:142.251.43.14
HostName:google.com

Gathered Inet-whois information for 142.251.43.14
---------------------------------

inetnum:        142.248.0.0 - 143.13.255.255
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:        2025-04-16T11:49:16Z
last-modified:  2025-04-16T11:49:16Z
source:         RIPE

role:           Internet Assigned Numbers Authority
```