

ASSIGNMENT 6

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

1. whois

whois command searches a user name directory and displays information about the user ID or nickname specified in the Name parameter. The whois command tries to reach ARPANET host internic.net where it examines a user-name database to obtain information.

```
Lab1006@Lab1006-HP-280-G4-MT-Business-PC:~$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-H                      hide legal disclaimers
--verbose               explain what is being done
--help                  display this help and exit
--version               output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                      find the one level less specific match
-L                      find all levels less specific matches
-m                      find all one level more specific matches
-M                      find all levels of more specific matches
-c                      find the smallest match containing a mnt-irt attribute
-x                      exact match
-b                      return brief IP address ranges with abuse contact
-B                      turn off object filtering (show email addresses)
-G                      turn off grouping of associated objects
-d                      return DNS reverse delegation objects too
-l ATTR[,ATTR]...       do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...       only look for objects of TYPE
-K                      only primary keys are returned
-r                      turn off recursive look-ups for contact information
-R                      force to show local copy of the domain object even
                        if it contains referral
-a                      also search all the mirrored databases
-s SOURCE[,SOURCE]...   search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST    find updates from SOURCE from serial FIRST to LAST
-t TYPE                 request template for object of TYPE
-v TYPE                 request verbose template for object of TYPE
-q [version|sources|types] query specified server info

Lab1006@Lab1006-HP-280-G4-MT-Business-PC:~$
```

2. 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. Dig command replaces older tools such as nslookup and the host.

```
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: 18922
;; 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.                260     IN      A      142.251.42.36

;; Query time: 2 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Aug 12 15:05:27 IST 2024
;; MSG SIZE rcvd: 59

Lab1006@Lab1006-HP-280-G4-MT-Business-PC:~$
```

3.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.google.com
traceroute to www.google.com (142.251.42.36), 30 hops max, 60 byte packets
 1  gateway (192.168.0.1)  0.701 ms  0.459 ms  0.848 ms
 2  203.212.25.1 (203.212.25.1)  1.882 ms  1.682 ms  1.910 ms
 3  203.212.24.53 (203.212.24.53)  2.042 ms  1.936 ms  1.911 ms
 4  10.10.226.153 (10.10.226.153)  8.868 ms  8.913 ms  8.673 ms
 5  72.14.242.50 (72.14.242.50)  4.225 ms  5.696 ms  5.290 ms
 6  * * *
 7  142.250.60.134 (142.250.60.134)  2.689 ms  142.250.212.170 (142.250.212.170)  5.679 ms  108.170.235.50 (108.170.235.50)  3.614 ms
 8  142.251.69.45 (142.251.69.45)  3.561 ms  142.250.208.226 (142.250.208.226)  3.927 ms  142.251.69.45 (142.251.69.45)  2.750 ms
 9  bon12s20-in-f4.1e100.net (142.251.42.36)  3.750 ms  3.585 ms  3.560 ms
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

4.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 www.google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.251.42.36
Name:   www.google.com
Address: 2404:6800:4009:830::2004
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

5.nikto

Nikto is an Open Source software written in Perl language that is used to scan a web-server for the vulnerability that can be exploited and can compromise the server

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~/nikto/program$ perl nikto.pl -host https://www.webscantest.com/
Nikto v2.5.0
-----
* Target IP:      69.164.223.208
* Target Hostname: www.webscantest.com
* Target Port:    443
-----
* SSL Info:      Subject: /OU=Domain Control Validated/CN=webscantest.com
                  AltNames: webscantest.com, www.webscantest.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository/CN=Go Daddy Secure Certificate Authority - G2
* Start Time:    2024-08-12 15:19:31 (GMT+5)
-----
* Server: Apache/2.4.7 (Ubuntu)
* /: Cookie NB_SRVID created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
* /: Cookie NB_SRVID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
* /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
lab1006@lab1006-HP-280-G4-MT-Business-PC:~/nikto/program$
```

6.dmitry

Dmitry stands for DeepMagic Information Gathering Tool. Dmitry is a free and open-source tool that is available on GitHub. We used this tool for information gathering. Dmitry is a command-line tool. With the help of the Dmitry tool, we

can gather information about the target, which we can then use for social engineering attacks. It can be used to collect a variety of useful information.

```
Activities Terminal Mon 15:28
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~$ dnitry -o www.google.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"
Writing output to 'www.google.com.txt'
HostIP:142.251.42.36
HostName:www.google.com
Gathered Inet-whois information for 142.251.42.36
-----
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:
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: RTR
```