Assignment 04

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

Theory:

WHOIS:

1. Domain Information: WHOIS provides details about domain names, including registration and expiration dates, domain owner's contact information, and name servers.

2. Domain Ownership: It helps identify the owner or organization associated with a domain, aiding in investigations and establishing online presence.

3. Registrar Details: WHOIS reveals the domain registrar responsible for managing the domain, assisting in addressing technical issues or contacting the registrar.

4. DNS Information: WHOIS displays DNS-related details, such as name server information and IP addresses, crucial for network configuration.

5. Abuse Reporting: It offers a way to report abuse, like spam or trademark infringements, by contacting the domain owner or registrar.

dig (Domain Information Groper):

1. DNS Queries: dig queries DNS servers to retrieve various DNS-related information, including A, AAAA, MX, and CNAME records.

2. DNS Resolution: It assists in resolving domain names to IP addresses, crucial for network communication.

3. Name Server Lookup: dig identifies authoritative name servers for a domain, ensuring proper DNS routing.

4. TTL (Time to Live): dig displays TTL values for DNS records, indicating how long the record should be cached before being refreshed.

5. Reverse DNS Lookup: It performs reverse DNS lookups, mapping IP addresses to domain names, aiding in identifying services associated with an IP.

traceroute:

1. Network Path Analysis: traceroute traces the path that packets take from source to destination, identifying intermediate routers and their response times.

2. Hop Identification: It helps pinpoint network bottlenecks, delays, or connectivity issues by showing delays at each hop.

3. Route Divergence: traceroute can reveal if packets are taking unexpected routes, indicating potential network misconfigurations or malicious activity.

4. MTU Discovery: It assists in Maximum Transmission Unit (MTU) discovery, optimizing data transmission by avoiding fragmentation.

5. Geo-Location: traceroute can provide approximate geographical locations of routers, aiding in network monitoring and troubleshooting.

nslookup:

1. DNS Record Lookup: nslookup retrieves DNS records, including A, MX, PTR, and NS records, helping understand domain configurations.

2. Domain IP Resolution: It resolves domain names to IP addresses, aiding in troubleshooting and network analysis.

3. Name Server Information: nslookup provides details about authoritative name servers for a domain, ensuring proper DNS resolution.

4. Reverse DNS Lookup: Similar to dig, nslookup performs reverse DNS lookups to map IP addresses to domain names.

5. Query Type Customization: It allows querying specific DNS record types, tailoring the information retrieved for different purposes.

nikto:

1. Web Server Vulnerability Scanner: nikto scans web servers for known vulnerabilities, misconfigurations, and security issues.

2. Directory and File Enumeration: It identifies hidden directories, files, or CGI scripts on a web server, aiding in potential attack vectors.

3. HTTP Methods Analysis: nikto examines supported HTTP methods, revealing potential weaknesses or security gaps.

4. Outdated Software Detection: It flags outdated software versions on web servers that could be exploited by attackers.

5. nikto checks for SSL/TLS vulnerabilities and configuration weaknesses, enhancing the security of data transmission.

dmitry:

1. Information Gathering: dmitry gathers information about target domains, IP addresses, email addresses, and network services.

2. WHOIS Lookup: It performs WHOIS queries to retrieve domain registration and ownership details.

3. Subdomain Enumeration: dmitry identifies subdomains associated with a target domain, aiding in understanding the target's online presence.

4. Network Port Scanning: It scans open ports on a target system, revealing potential entry points for unauthorized access.

5. Banner Grabbing: dmitry captures banners and other information from network services, assisting in service identification and version detection.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ WHOIS
WHOIS: command not found
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man WHOIS
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: 2023-08-04T09:23:38Z <<<

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
```

```
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
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
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: 2019-09-09T15:39:04+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
```

```
Activities  Terminal                                   Fri 14:57
                                   lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
>>> Last update of WHOIS database: 2023-08-04T09:20:33+0000 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain’s Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN’s Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor’s WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name’s registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
--
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dig geeksforgeeks.org

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> geeksforgeeks.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18253
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
geeksforgeeks.org.      30      IN      A       34.218.62.116

;; Query time: 29 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Aug 04 14:58:30 IST 2023
;; MSG SIZE  rcvd: 62
```


```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dig geeksforgeeks.org

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> geeksforgeeks.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18253
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
geeksforgeeks.org.      30      IN      A       34.218.62.116

;; Query time: 29 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Aug 04 14:58:30 IST 2023
;; MSG SIZE  rcvd: 62
```


```
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:~$ nikto -h 128.199.222.244
- Nikto v2.1.5
---------------------------------------------------------------------------
^Clab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nikto -h 128.199.222.244
- Nikto v2.1.5
---------------------------------------------------------------------------
+ No web server found on 128.199.222.244:80
---------------------------------------------------------------------------
+ 0 host(s) tested
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
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.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

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

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


Gathered Inic-whois information for google.com
---------------------------------
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
```

```
Gathered Inlc-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: 2023-08-04T09:48:19Z <<<

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
guarantee its accuracy. By submitting a Whois query, you agree to abide
```

```
Activities  Terminal                    Fri 15:20
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:maps.google.com
HostIP:142.250.183.14
HostName:www.google.com
HostIP:142.250.192.132
HostName:support.google.com
HostIP:142.250.192.46
HostName:myactivity.google.com
HostIP:74.125.130.101
HostName:accounts.google.com
HostIP:216.58.196.77
HostName:mail.google.com
HostIP:172.217.174.69
HostName:contacts.google.com
HostIP:142.250.192.110
HostName:analytics.google.com
HostIP:216.239.32.181
HostName:play.google.com
HostIP:142.250.183.142
HostName:keep.google.com
HostIP:216.239.34.176
HostName:trends.google.com
HostIP:142.250.183.4
HostName:scholar.google.com
HostIP:142.250.182.228
HostName:meet.google.com
HostIP:142.251.42.110
HostName:one.google.com
HostIP:142.250.183.46
HostName:policies.google.com
HostIP:142.250.183.142
HostName:cloud.google.com
HostIP:142.250.192.14
HostName:ads.google.com
HostIP:142.250.183.78
HostName:pay.google.com
HostIP:172.217.194.92
HostName:store.google.com
HostIP:142.250.192.46
HostName:takeout.google.com
HostIP:142.250.199.142
HostName:myaccount.google.com
HostIP:142.250.77.77
```

```
Activities  Terminal                    Fri 15:20
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
HostName:assistant.google.com
HostIP:142.250.183.78
HostName:news.google.com
HostIP:142.250.183.206
HostName:console.cloud.google.com
HostIP:142.250.183.46
HostName:developers.google.com
HostIP:142.250.182.206
HostName:docs.google.com
HostIP:142.250.192.78
HostName:drive.google.com
HostIP:142.250.192.14
HostName:classroom.google.com
HostIP:142.250.183.206
HostName:edu.google.com
HostIP:142.250.183.14
HostName:tagmanager.google.com
HostIP:142.250.183.46
HostName:picasa.google.com
HostIP:142.250.183.4
HostName:sites.google.com
HostIP:142.250.192.142
HostName:groups.google.com
HostIP:64.233.170.101
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...
jakearchibald@google.com
falken@google.com
admin@google.com
kbr@google.com
terryok@google.com
info@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:~$ nikto -h google.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          142.251.42.14
+ Target Hostname:    google.com
+ Target Port:        80
+ Start Time:         2023-08-04 15:22:53 (GMT5.5)
---------------------------------------------------------------------------
+ Server: gws
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'content-security-policy-report-only' found, with contents: object-src 'none';base-uri 'self';script-src 'nonce-k1vyNStBf6B2VqO20Z7a7Q' 'strict-dynami
c' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
+ 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 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'cross-origin-resource-policy' found, with contents: cross-origin
+ Cookie 1P_JAR created without the httponly flag
+ 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-XNmk6pldCgg_MSsb5o4U8A' 'strict-dynamic' 'report-s
ample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
+ Allowed HTTP Methods: GET, HEAD
```

Conclusion: Network reconnaissance tools such as WHOIS, dig, traceroute, nslookup, nikto, and dmitry provide vital insights into network structures, domain configurations, and security vulnerabilities. By utilizing these tools effectively, professionals can enhance cybersecurity efforts, troubleshoot network issues, and make informed decisions to safeguard digital assets and ensure smooth network operations. These tools remain essential in the ever-evolving landscape of technology, enabling proactive security measures and efficient network management.