Terna Engineering College

Computer Engineering Department

Class: TE **Sem.: VI**

Course: System Security Lab

PART A

(PART A : TO BE REFFERED BY STUDENTS)

Experiment No.05

A.1 Aim: Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.

A.2 Prerequisite:

1. Basic Knowledge of IP addresses, DNS.

A.3 Outcome:

After successful completion of this experiment students will be able to

Apply basic network command to gather basic network information.

A.4 Theory:

Network Reconnaissance:

- Act of reconnoitoring ---explore with the goal of finding something(especially to gain information about enemy)
- In the world of hacking, reconnaisance begins with "Footprinting"
- i.e accumulating data about target's environment, and finding vulnerabilities.
- Attacker gathers information in two phases viz: passive attacks and active attacks

Passive attacks

- Gathering information about a target without his/her knowledge….Eavesdropping
- Yahoo or google search
- Surfing online community groups
- Gathering information from websites of organisations. e.g. contact details, email address etc.
- Blogs, newsgroups, press releases etc.
- Going through job posting in particular job profiles

Reconnaissance Tools

- WHOIS, dig, traceroute, nslookup

1. **WHOIS:**WHOISistheLinuxutilityforsearchinganobjectinaWHOISdatabase.TheWHOIS database of a domain is the publicly displayed information about a domains ownership, billing, technical, administrative, and nameserver information. Running a WHOIS on your domain will look the domain up at the registrar for the domain information. All domains have WHOIS information. WHOIS database can be queried to obtain the following informationvia WHOIS:

   - Administrative contact details, including names, email addresses, and telephone numbers
   - Mailing addresses for office locations relating to the targetorganization
   - Details of authoritative name servers for each given domain

Example: Querying Facebook.com

```
ssc@ssc-OptiPlex-380:~$ whois facebook.com
```

For more information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.

- Domain Name: facebook.com
- Registry Domain ID: 2320948_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.markmonitor.com Registrar URL: http://www.markmonitor.com
- Updated Date: 2014-10-28T12:38:28-0700
- reation Date: 1997-03-28T21:00:00-0800
- Registrar Registration Expiration Date: 2020-03-29T21:00:00-0700 Registrar: MarkMonitor, Inc.

- Registrar IANA ID: 292
- Registrar Abuse Contact Email: abusecomplaints@markmonitor.com Registrar Abuse Contact Phone: +1.2083895740
- 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)
- Registry Registrant ID:
- Registrant Name: Domain Administrator Registrant Organization: Facebook, Inc. Registrant Street: 1601 Willow Road, Registrant City: Menlo Park
- Registrant State/Province: CA Registrant Postal Code: 94025
- Registrant Country: US
- Registrant Phone: +1.6505434800
- Registrant PhoneExt:
- Registrant Fax: +1.6505434800
- Registrant Fax Ext:
- Registrant Email: domain@fb.com Registry Admin ID:
- Admin Name: Domain Administrator Admin Organization: Facebook, Inc. Admin Street: 1601 Willow Road, Admin City: Menlo Park
- Admin State/Province: CA Admin Postal Code: 94025 Admin Country: US
- Admin Phone: +1.6505434800 Admin Phone Ext:
- Admin Fax: +1.6505434800
- Admin Fax Ext:
- Admin Email: domain@fb.com Registry Tech ID:
- Tech Name: Domain Administrator

- Tech Organization: Facebook, Inc. Tech Street: 1601 Willow Road, Tech City: Menlo Park
- Tech State/Province: CA
- Tech Postal Code: 94025
- Tech Country: US
- Tech Phone: +1.6505434800
- Tech Phone Ext:
- Tech Fax: +1.6505434800
- Tech Fax Ext:
- Tech Email: domain@fb.com
- Name Server: b.ns.facebook.com
- Name Server: a.ns.facebook.com
- DNSSEC: unsigned
  URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

  >>> Last update of WHOIS database: 2015-07-16T21:08:30-0700 <<<

The Data in MarkMonitor.com's WHOIS database is provided by MarkMonitor.com for information purposes, and to assist persons in obtaining information about orrelated to a domain name registration record. MarkMonitor.com does not guarantee 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 of mass unsolicited, commercial advertising or solicitations via e-mail (spam);or
(2) Enable high volume, automated, electronic processes that apply to MarkMonitor.com (or its systems).

MarkMonitor.com reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this policy.

MarkMonitor is the Global Leader in Online Brand Protection. MarkMonitor Domain Management(TM)

MarkMonitor Brand Protection(TM) MarkMonitorAntiPiracy(TM) MarkMonitorAntiFraud(TM) Professional and Managed Services

```
Visit MarkMonitor at http://www.markmonitor.com Contact us at +1.8007459229
In Europe, at +44.02032062220 ssc@ssc-OptiPlex-380:~$
```

2. **Dig** - Dig is a networking tool that can query DNS servers for information. It can be veryhelpful fordiagnosingproblemswithdomainpointingandisagoodwaytoverifythatyourconfiguration is working. The most basic way to use dig is to specify the domain we wish toquery:

Example:

```
$ dig duckduckgo.com
```

3. **Traceroute** - traceroute prints the route that packets take to a network host. Traceroute utility uses the TTL field in the IP header to achieve its operation. For users who are new to TTL field, this field describes how much hops a particular packet will take while traveling on network. So, thiseffectivelyoutlinesthelifetimeofthepacketonnetwork.Thisfieldisusuallysetto 32or64. Each time the packet is held on an intermediate router, it decreases the TTL value by 1. When a router finds the TTL value of 1 in a received packet then that packet is not forwarded but instead discarded.Afterdiscardingthepacket,routersendsanICMPerrormessageof—Timeexceeded‖ back to the source from where packet generated. The ICMP packet that is sent back contains the IP address of the router. So now it can be easily understood that traceroute operates by sending packets with TTL value starting from 1 and then incrementing by one each time. Each time a routerreceivesthepacket,itcheckstheTTLfield,ifTTLfieldis1thenitdiscardsthepacketand sends the ICMP error packet containing its IP address and this is what traceroute requires. So traceroute incrementally fetches the IP of all the routers between the source and thedestination.

Example:

```
$traceroute example.com
```

PART B

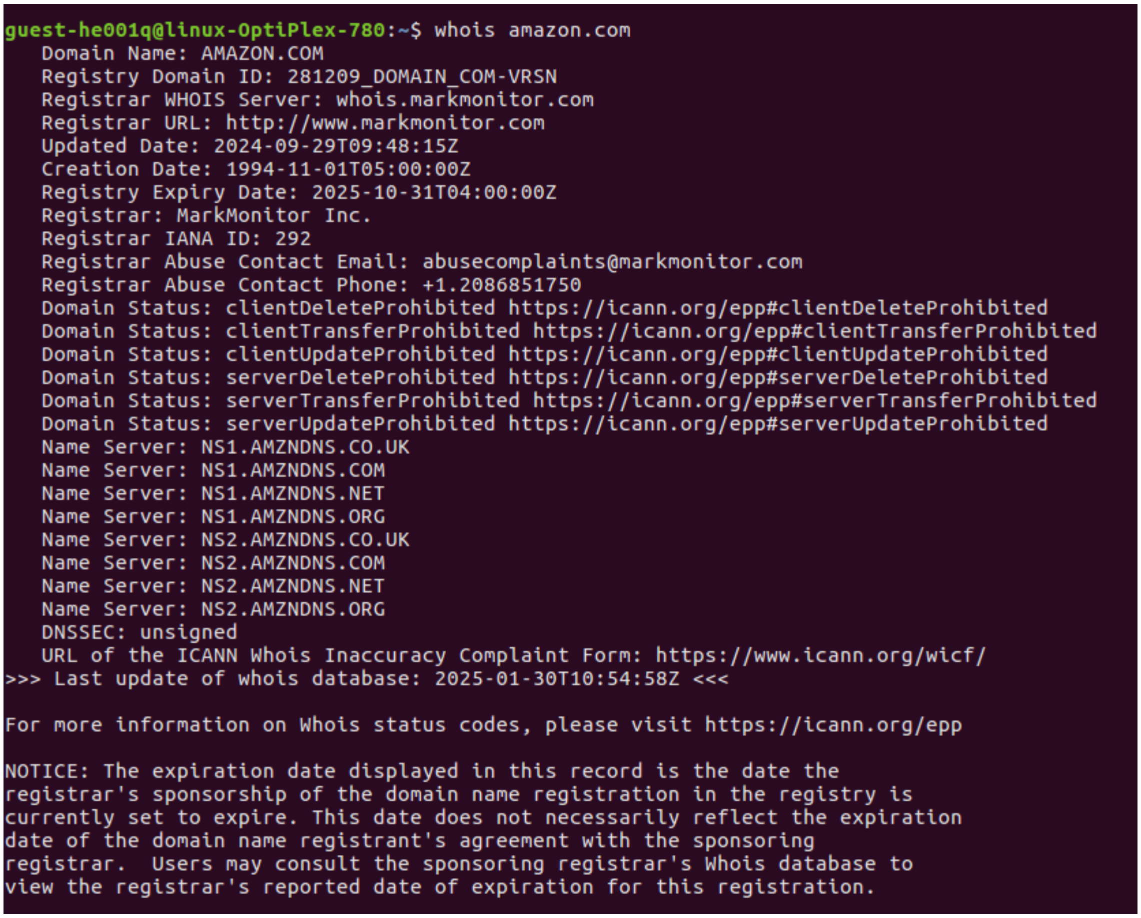
(PART B : TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)

Roll No.B30	**Name: Pranjal Bhatt**
Class :COMPS TE B2	**Batch :B2**
Date of Experiment:	**Date of Submission**
Grade :	

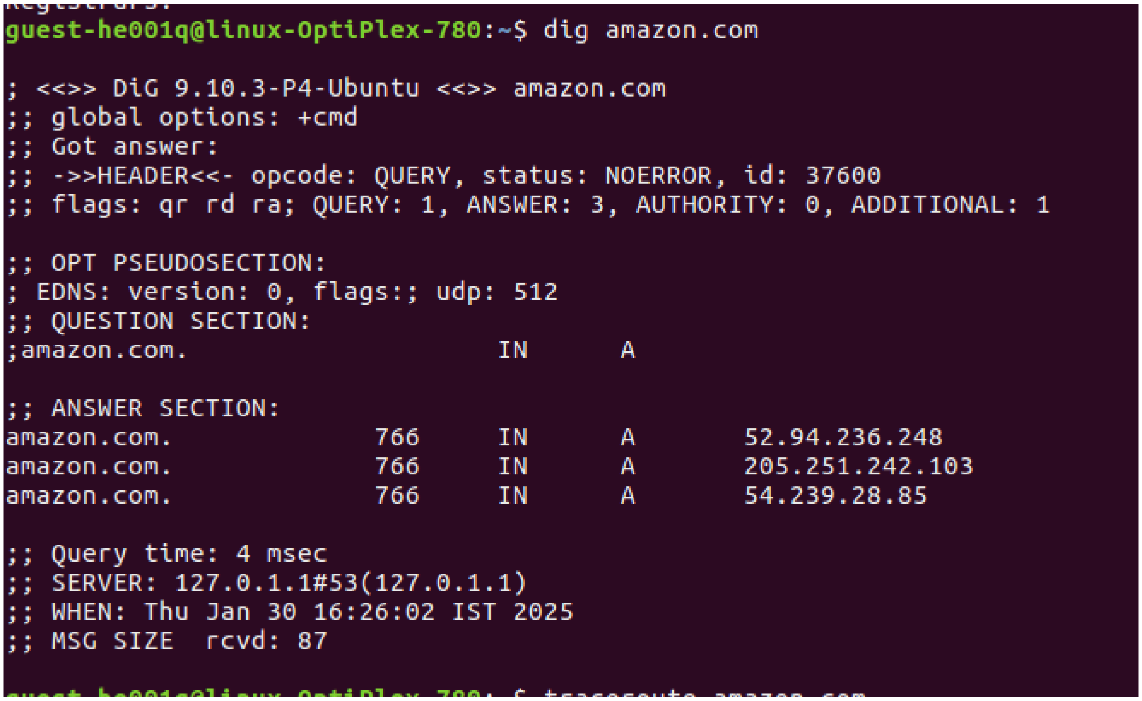
B.1 Output of Reconnaissance Tools

whois



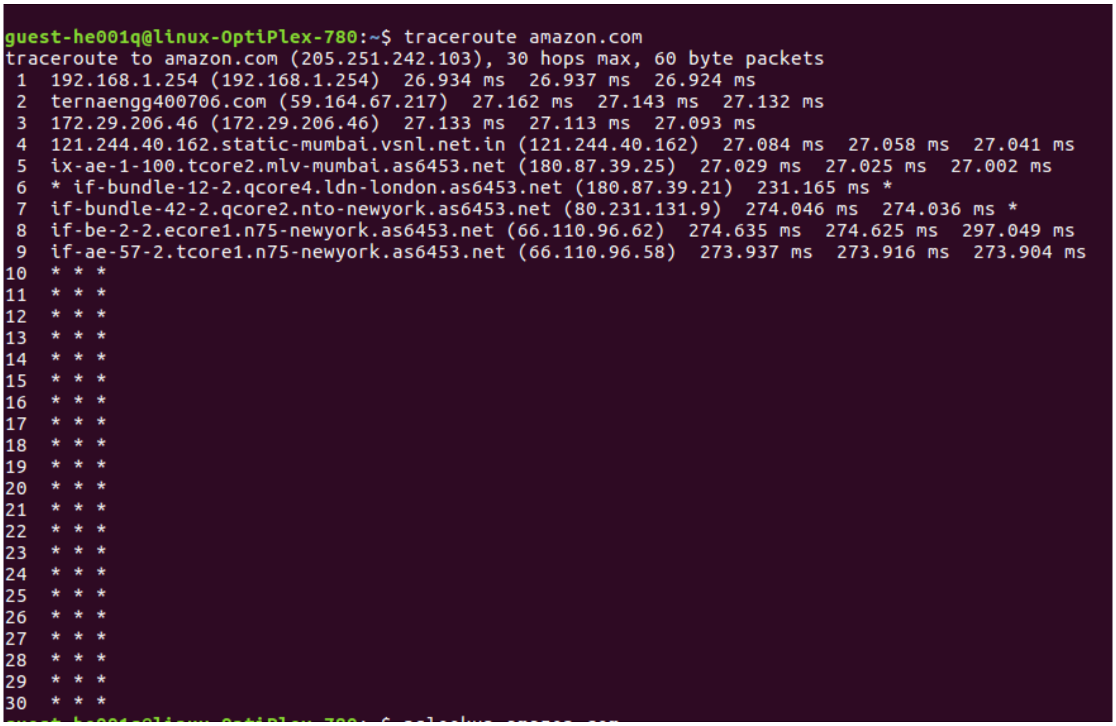
```
guest-he001q@linux-OptiPlex-780:~$ whois amazon.com
   Domain Name: AMAZON.COM
   Registry Domain ID: 281209_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-09-29T09:48:15Z
   Creation Date: 1994-11-01T05:00:00Z
   Registry Expiry Date: 2025-10-31T04:00:00Z
   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.AMZNDNS.CO.UK
   Name Server: NS1.AMZNDNS.COM
   Name Server: NS1.AMZNDNS.NET
   Name Server: NS1.AMZNDNS.ORG
   Name Server: NS2.AMZNDNS.CO.UK
   Name Server: NS2.AMZNDNS.COM
   Name Server: NS2.AMZNDNS.NET
   Name Server: NS2.AMZNDNS.ORG
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-01-30T10:54:58Z <<<

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.
```

dig



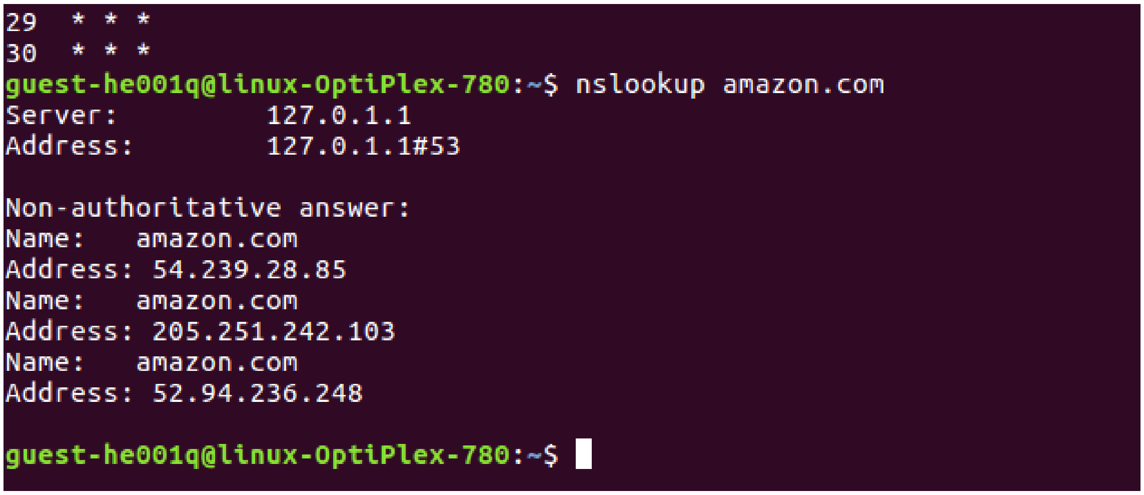
```
guest-he001q@linux-OptiPlex-780:~$ dig amazon.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> amazon.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37600
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;amazon.com.                    IN      A

;; ANSWER SECTION:
amazon.com.             766     IN      A       52.94.236.248
amazon.com.             766     IN      A       205.251.242.103
amazon.com.             766     IN      A       54.239.28.85

;; Query time: 4 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Thu Jan 30 16:26:02 IST 2025
;; MSG SIZE  rcvd: 87
```

traceroute



```
guest-he001q@linux-OptiPlex-780:~$ traceroute amazon.com
traceroute to amazon.com (205.251.242.103), 30 hops max, 60 byte packets
 1  192.168.1.254 (192.168.1.254)  26.934 ms  26.937 ms  26.924 ms
 2  ternaengg400706.com (59.164.67.217)  27.162 ms  27.143 ms  27.132 ms
 3  172.29.206.46 (172.29.206.46)  27.133 ms  27.113 ms  27.093 ms
 4  121.244.40.162.static-mumbai.vsnl.net.in (121.244.40.162)  27.084 ms  27.058 ms  27.041 ms
 5  ix-ae-1-100.tcore2.mlv-mumbai.as6453.net (180.87.39.25)  27.029 ms  27.025 ms  27.002 ms
 6  * if-bundle-12-2.qcore4.ldn-london.as6453.net (180.87.39.21)  231.165 ms *
 7  if-bundle-42-2.qcore2.nto-newyork.as6453.net (80.231.131.9)  274.046 ms  274.036 ms *
 8  if-be-2-2.ecore1.n75-newyork.as6453.net (66.110.96.62)  274.635 ms  274.625 ms  297.049 ms
 9  if-ae-57-2.tcore1.n75-newyork.as6453.net (66.110.96.58)  273.937 ms  273.916 ms  273.904 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

nslookup



```
29   * * *
30   * * *
guest-he001q@linux-OptiPlex-780:~$ nslookup amazon.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   amazon.com
Address: 54.239.28.85
Name:   amazon.com
Address: 205.251.242.103
Name:   amazon.com
Address: 52.94.236.248

guest-he001q@linux-OptiPlex-780:~$ 
```

B.2 Commands / tools used with syntax:

Here are the commands with their syntax:

1. whois:

```
whois amazon.com
```

2. dig:

```
dig amazon.com
```

- For specific record types:

```
dig amazon.com A
dig amazon.com MX
```

3. traceroute:

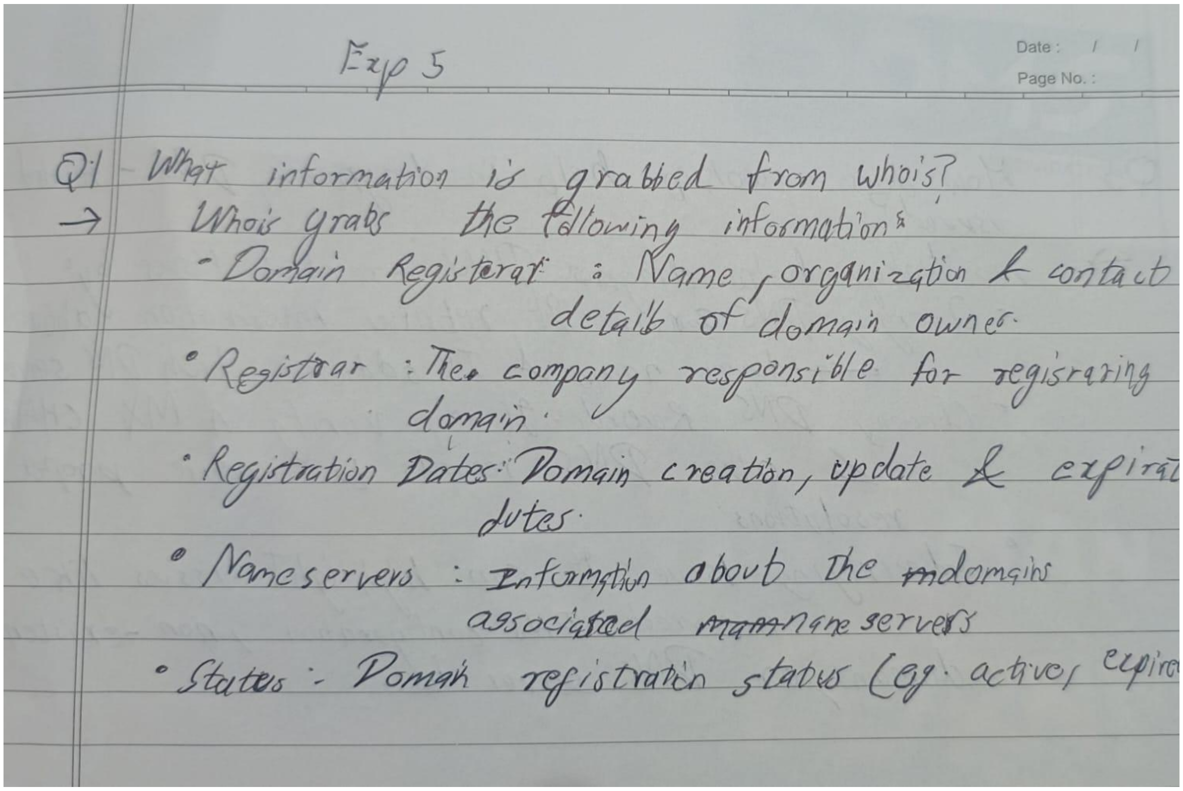
```
traceroute amazon.com
```

4. nslookup:

```
nslookup amazon.com
```

B.3 Question of Curiosity: *(At least 3 questions should be handwritten)*

1. What information is grabbed from Whois?



Exp 5

Date : / /

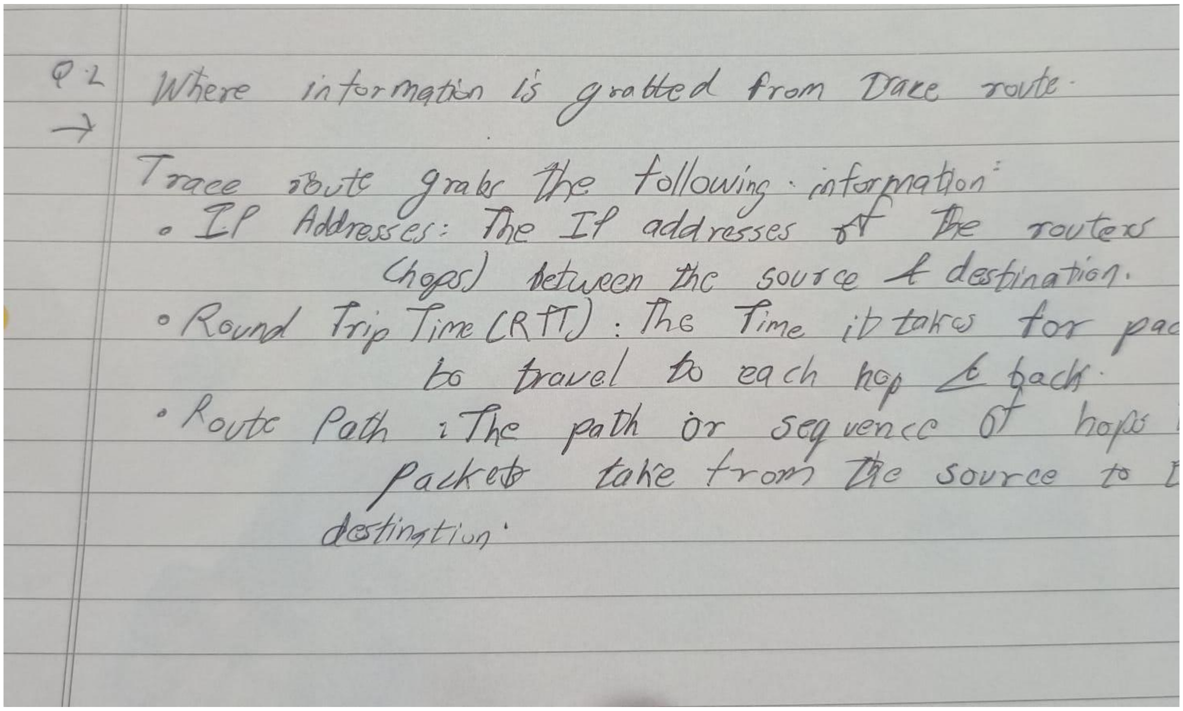
Page No. :

Q1 What information is grabbed from whois?

→ Whois grabs the following information:

- Domain Registerat : Name, organization & contact details of domain owner.
- Registrar : The company responsible for regisraring domain.
- Registration Dates: Domain creation, update & expirat dutes.
- Nameservers : Information about the ~~m~~domains associated ~~mam~~name servers
- Status :- Domain refistration status (eg. active, expire

2. What information is grabbed from traceroute?



Q.2 Where information is grabbed from Trace route.

→

Trace route grabs the following information:

- IP Addresses: The IP addresses of the routers (hops) between the source & destination.
- Round Trip Time (RTT) : The Time it takes for pac to travel to each hop & back.
- Route Path : The path or sequence of hops packets take from the source to destination.

3. What information is grabbed from dig?

The `dig` command retrieves various pieces of information about a domain from its DNS

(Domain Name System) records. The key details it can provide include:

1. **A Record (Address Record)**: Maps a domain to an IPv4 address.
2. **AAAA Record (IPv6 Address Record)**: Maps a domain to an IPv6 address.
3. **MX Record (Mail Exchange Record)**: Lists mail servers for the domain.
4. **CNAME Record (Canonical Name Record)**: Points a domain to another domain.
5. **NS Record (Name Server Record)**: Shows the authoritative name servers for the domain.
6. **TXT Record (Text Record)**: Provides arbitrary text data, often used for verification (e.g., SPF records for email).
7. **SOA Record (Start of Authority Record)**: Provides information about the DNS zone, including the primary DNS server and contact email.
8. **PTR Record (Pointer Record)**: Used for reverse DNS lookup, mapping an IP address to a domain.
9. **SRV Record (Service Record)**: Specifies services available for the domain, such as for SIP or XMPP.
10. **TTL (Time to Live)**: Specifies how long a record is cached by DNS resolvers.

For example, running:

```
dig amazon.com
```

will return the **A Record**, IP addresses, and possibly other relevant information depending on the query type.

4. After using traceroute how attacker can use the information, based on the same what kind of attacks can be applied?

After using **traceroute**, an attacker can gather information about the network path between their device and the target, which can be used in several malicious ways. Here's how an attacker might exploit this data and the types of attacks they could potentially carry out:

Information Gained from Traceroute:

1. **Network Path**: The full path of routers and devices between the attacker and the target domain or IP address.
2. **IP Addresses**: The IP addresses of intermediate routers or network segments.
3. **Geographical Location**: The approximate geographical location of intermediate routers based on IP address geolocation.
4. **Network Topology**: The structure of the network, including the devices and their order in

the data flow.

Possible Attacks:

1.

Denial of Service (DoS) / Distributed Denial of Service (DDoS):

2.

1. **Targeting Network Routers**: If an attacker knows the IP addresses of routers, they could target specific routers or network segments in a DDoS attack, overwhelming them with traffic.
2. **Overloading Network Links**: Attackers can focus traffic on particular segments in the network path, creating congestion or taking down intermediate routers.

3.

Man-in-the-Middle (MITM) Attack:

4.

1. **Packet Interception**: If an attacker identifies the specific routers or devices in the network path, they may attempt to gain access to these points, allowing them to intercept, alter, or inject malicious traffic between the source and destination.

5.

IP Spoofing:

6.

1. **Using Traceroute Data for IP Spoofing**: Knowing the routers and their IP addresses, an attacker can craft packets with spoofed source IP addresses that appear to come from within the same network segment, making it more difficult to detect the origin of the attack.

7.

Route Hijacking:

8.

1. **Manipulating Routing Information**: With knowledge of the network path, an attacker might attempt **BGP (Border Gateway Protocol)** hijacking by advertising false routes to redirect traffic through malicious or compromised devices, allowing them to monitor, alter, or drop data.

9.

Network Reconnaissance:

10.

1. **Mapping Network Infrastructure**: Traceroute allows attackers to map out the network infrastructure of an organization or ISP, which can be used for further exploitation or to identify weaknesses in the network.

11.

Targeting Weak Points:

12.

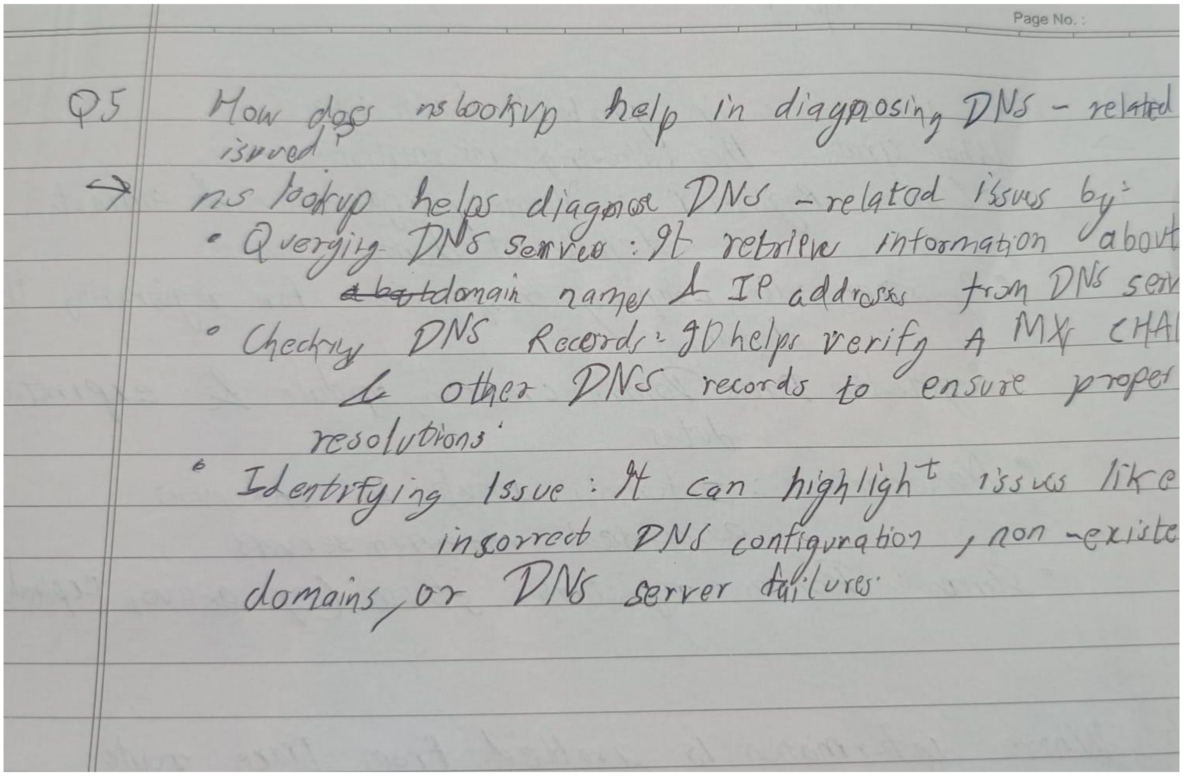
1. **Identifying Vulnerable Routers**: Attackers can focus on specific routers or network devices that appear to have weak security configurations, based on the data gathered from traceroute, and attempt to exploit vulnerabilities.

Countermeasures:

- **Routing Security**: Use secure routing protocols like **BGP monitoring** and **Route Validation** to prevent route hijacking.
- **Encryption**: Encrypt sensitive data in transit to mitigate MITM risks.
- **Traffic Anomaly Detection**: Implement systems to detect unusual traffic patterns that could indicate DDoS attacks or spoofing.
- **Firewall and Network Segmentation**: Secure routers and networks by implementing firewalls and segmentation to limit access from unknown or unauthorized sources.

In summary, traceroute provides an attacker with crucial information about the network infrastructure that could be exploited for several types of attacks, including DDoS, MITM, and route hijacking. Security measures should be taken to mitigate these risks.

5. How does nslookup help in diagnosing DNS-related issues?



Page No. :

Q5 How does nslookup help in diagnosing DNS - related issues?

→ ns lookup helps diagnose DNS - related issues by:

- Querying DNS Server : It retrieve information about ~~about~~ domain names & IP addresses from DNS serv
- Checking DNS Records : It helps verify A MX, CNA & other DNS records to ensure proper resolutions.
- Identifying Issue : It can highlight issues like incorrect DNS configuration, non -existe domains, or DNS server failures.

6. What are the ethical considerations when using network reconnaissance tools like WHOIS and traceroute?

When using network reconnaissance tools like **WHOIS** and **traceroute**, there are several **ethical considerations** that must be taken into account:

1. Permission and Consent:

- **Ethical Use**: Before performing any kind of network reconnaissance, it’s important to have **explicit permission** from the network owner. Unauthorized use of tools like **WHOIS** or **traceroute** on networks you don’t own or have consent to test can be considered a violation of privacy and may be seen as an intrusion or hacking.
- **Penetration Testing**: For legitimate purposes like penetration testing, **written consent** should always be obtained from the organization, outlining the scope and limitations of the testing.

2. Privacy Concerns:

- **Personal Data**: Some tools like **WHOIS** can reveal private information about domain owners (e.g., contact details), which might be used maliciously if gathered without consent. **Ethically**, such data should only be accessed for lawful and legitimate purposes.
- **Data Protection**: It’s important to respect individuals' privacy and not collect or use

information for **unethical purposes** (e.g., spamming or social engineering).

3. Avoiding Harm:

- **Network Disruption**: Tools like **traceroute** can provide information that could potentially be used for **Denial of Service (DoS)** attacks. Ethical users must be cautious not to disrupt or harm the networks they analyze.
- **Intrusion and Exploitation**: Gathering network data should not be used to identify vulnerabilities with the intent to exploit them for personal or financial gain, such as launching attacks or gaining unauthorized access.

4. Legal Compliance:

- **Laws and Regulations**: Many countries have strict laws regarding **cybersecurity** and **data protection**. Using reconnaissance tools on a network without consent can be a violation of laws such as the **Computer Fraud and Abuse Act (CFAA)** in the United States or **GDPR** in the European Union. Ethical use involves understanding and complying with relevant laws.
- **Cybersecurity Ethics**: Ethical hackers or cybersecurity professionals follow a **code of conduct** that aligns with legal and moral guidelines. Unauthorized use of these tools can have legal consequences.

5. Disclosure of Findings:

- **Responsible Disclosure**: If a vulnerability is discovered through the use of tools like **WHOIS** or **traceroute**, it should be reported **responsibly** to the organization or network owner. **Disclosing vulnerabilities publicly** without giving the owner a chance to fix them can be harmful.
- **Non-disclosure Agreements (NDAs)**: When conducting network reconnaissance on behalf of a client, make sure to comply with **NDAs** and only share findings with the authorized parties.

6. Intent:

- **Legitimate Purpose**: The ethical use of network reconnaissance tools should be for **defensive** purposes (e.g., securing one's own network, research, or education). Using them for **malicious intent** (e.g., cyberattacks, espionage, or data theft) is **unethical** and **illegal**.
- **Research and Education**: When used for **educational purposes** or **security research**, ensure that the research is conducted in a responsible manner and does not cause harm or violate privacy.

7. Impact on Network Resources:

- **Network Load**: Tools like **traceroute** can create unnecessary network traffic, especially if used indiscriminately or frequently. While not as impactful as a DDoS attack, excessive use of these tools can still affect network performance. Ethical users should be mindful of the load they impose on other people's networks.

Summary:

- **Ethical Use**: Always use tools like **WHOIS** and **traceroute** with explicit permission.
- **Privacy**: Avoid collecting personal data without consent.
- **Responsibility**: Ensure your actions do not harm the network or its users.
- **Legality**: Abide by all relevant laws and regulations regarding network testing.
- **Intent**: Use these tools for **defensive, educational, or research purposes** only, with a responsible approach.

B.4 Conclusion:

In this experiment, the use of network reconnaissance tools like **WHOIS**, **dig**, **traceroute**, and **nslookup** was explored to gather valuable information about networks and domain registrars. These tools provide insights into domain ownership, IP address resolution, network paths, and DNS configurations.

Through the study, it became clear that while these tools are powerful for legitimate network management, troubleshooting, and security testing, they also raise ethical and legal concerns. Unauthorized use could lead to privacy violations and network disruption. Therefore, responsible use, proper consent, and adherence to ethical guidelines are essential when employing these tools.

Overall, the experiment reinforced the importance of understanding the functionality of network reconnaissance tools and their potential risks, while highlighting the need for ethical considerations in network security practices.