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

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.

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

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

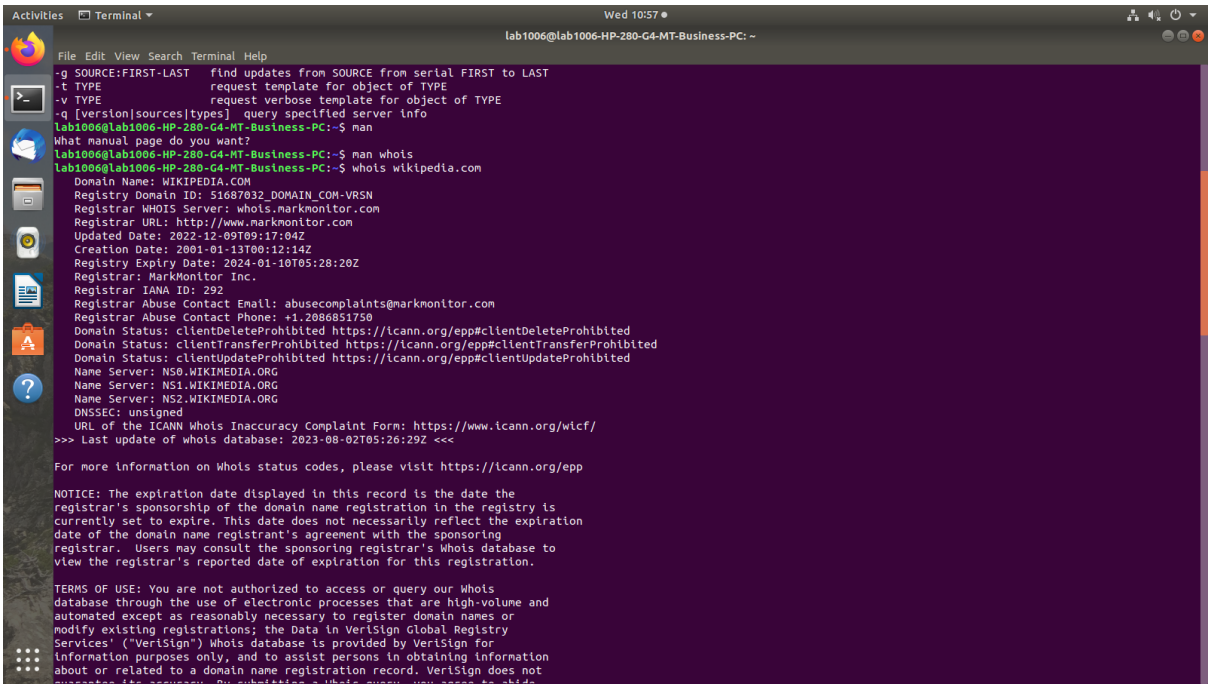
7. Save Output to example.txt:
   dmitry -s -e -p example.com > example.txt

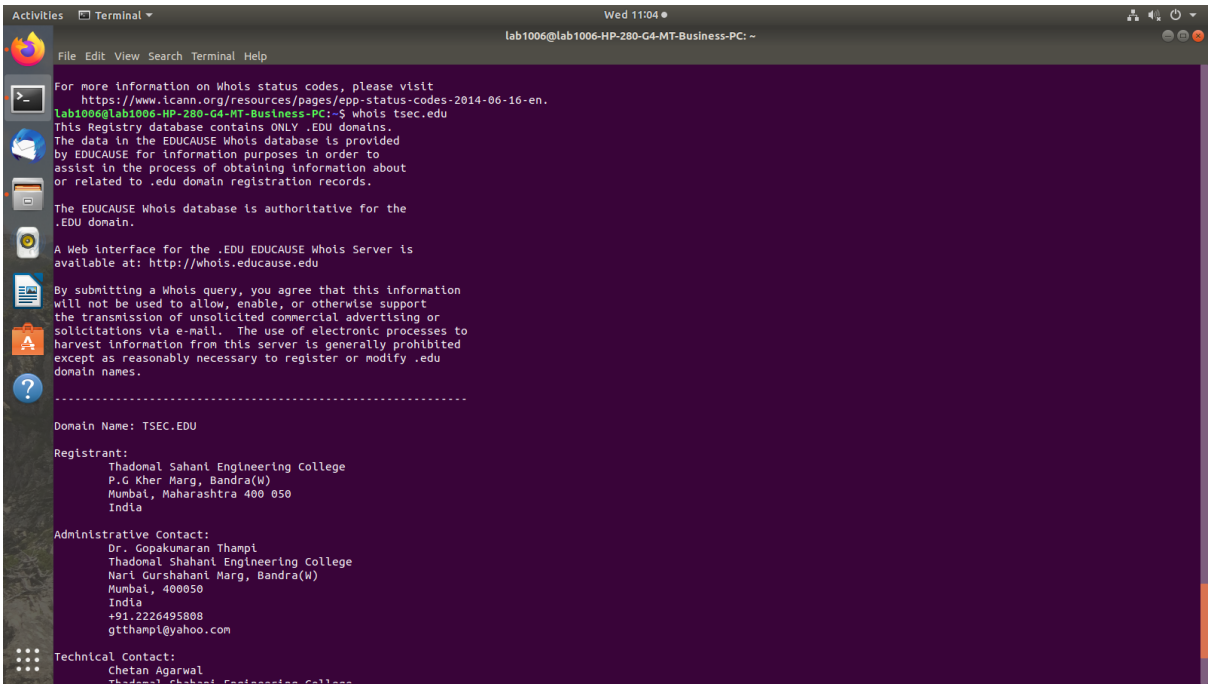
Roll no. : 53
Name: Shreya Kamath
Date: 7th August, 2023.

Email Harvesting Command:
dmitry -e example.com

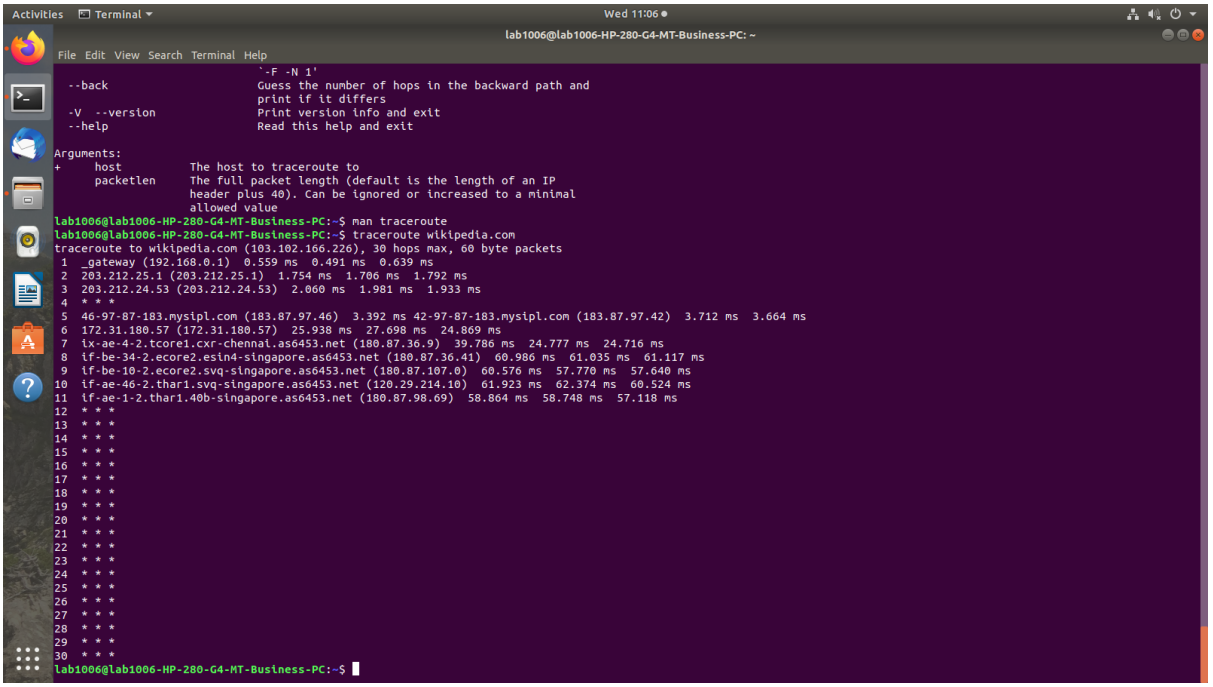
Subdomain Harvesting Command:
dmitry -s example.com

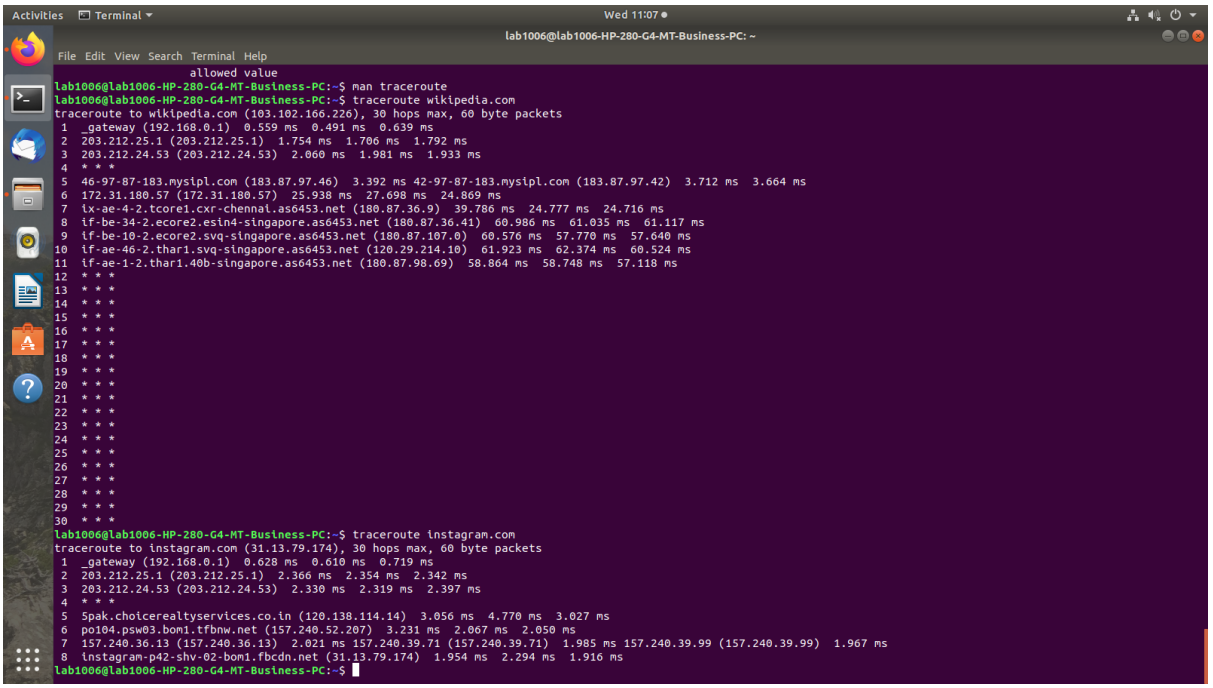
OUTPUT:



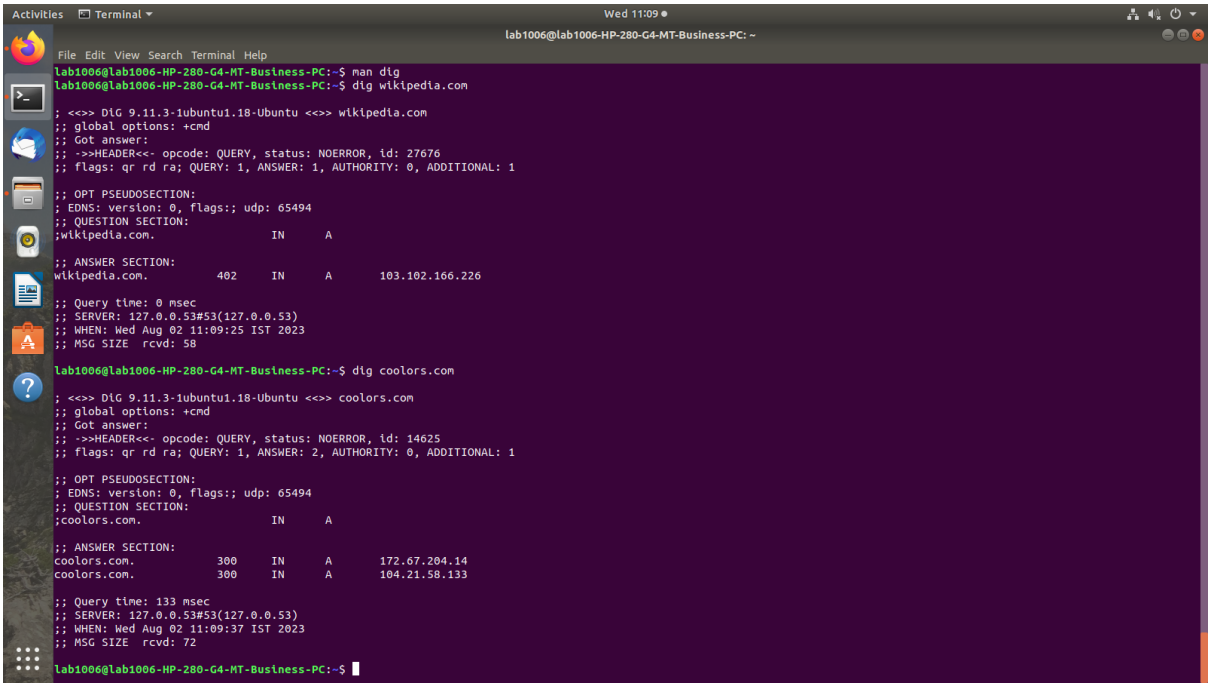


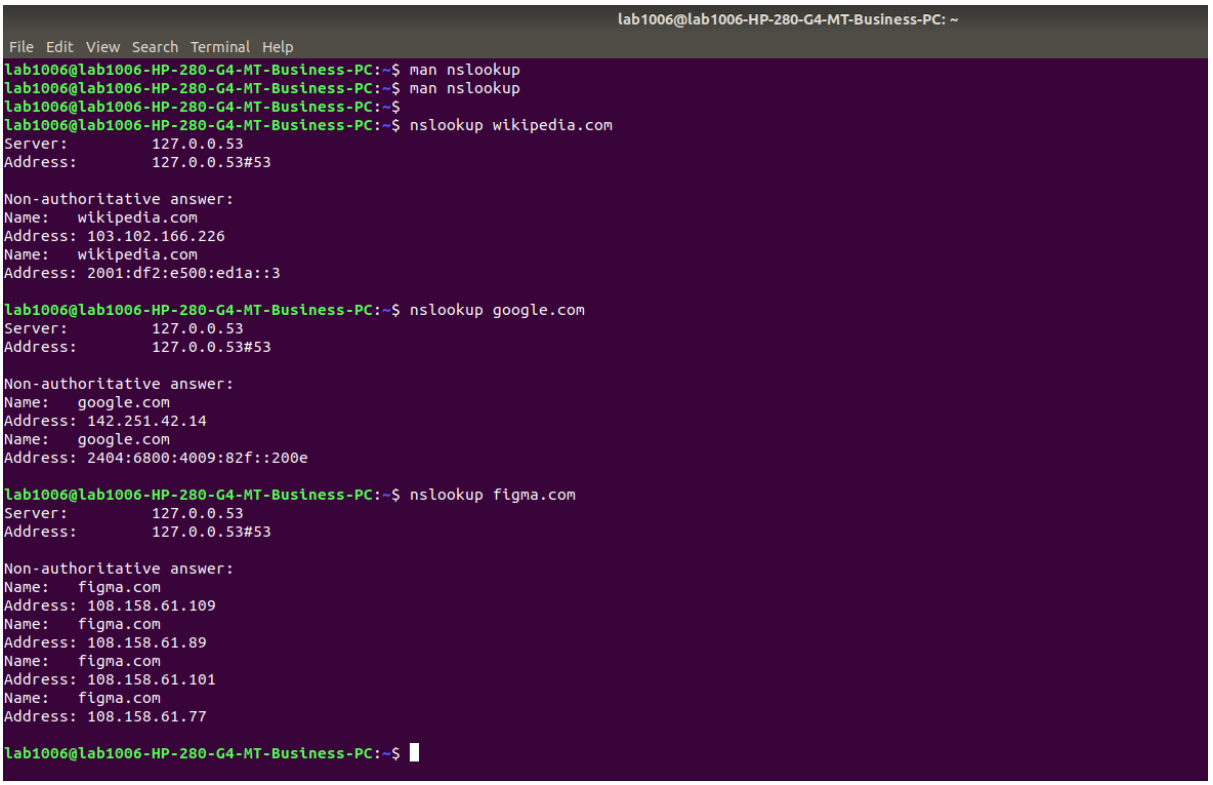
Roll no. : 53
Name: Shreya Kamath
Date: 7th August, 2023.





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



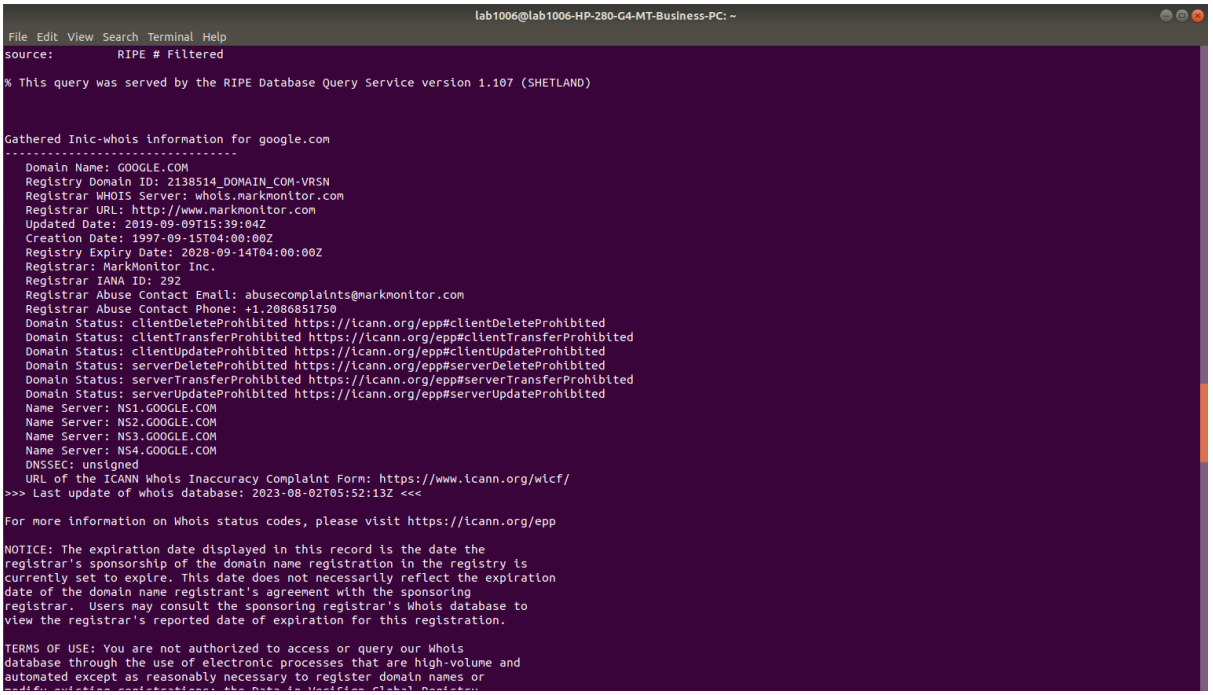


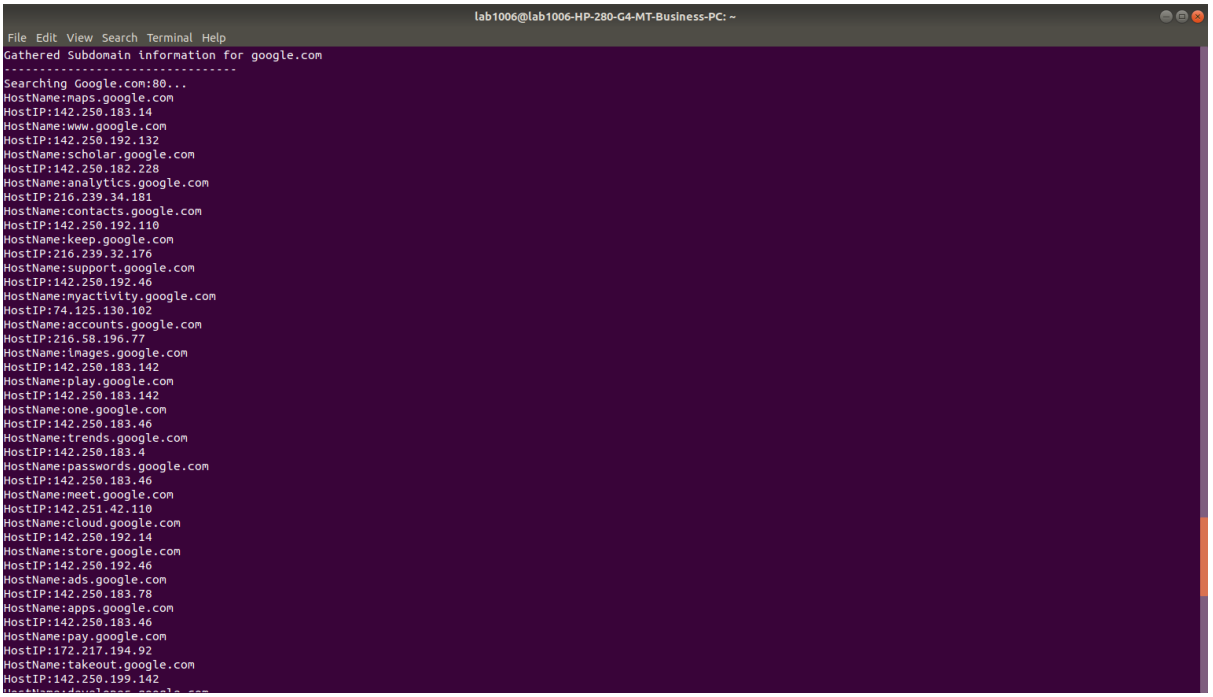
Roll no. : 53
Name: Shreya Kamath
Date: 7th August, 2023.

```
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)

^Clab1006@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/
^Clab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

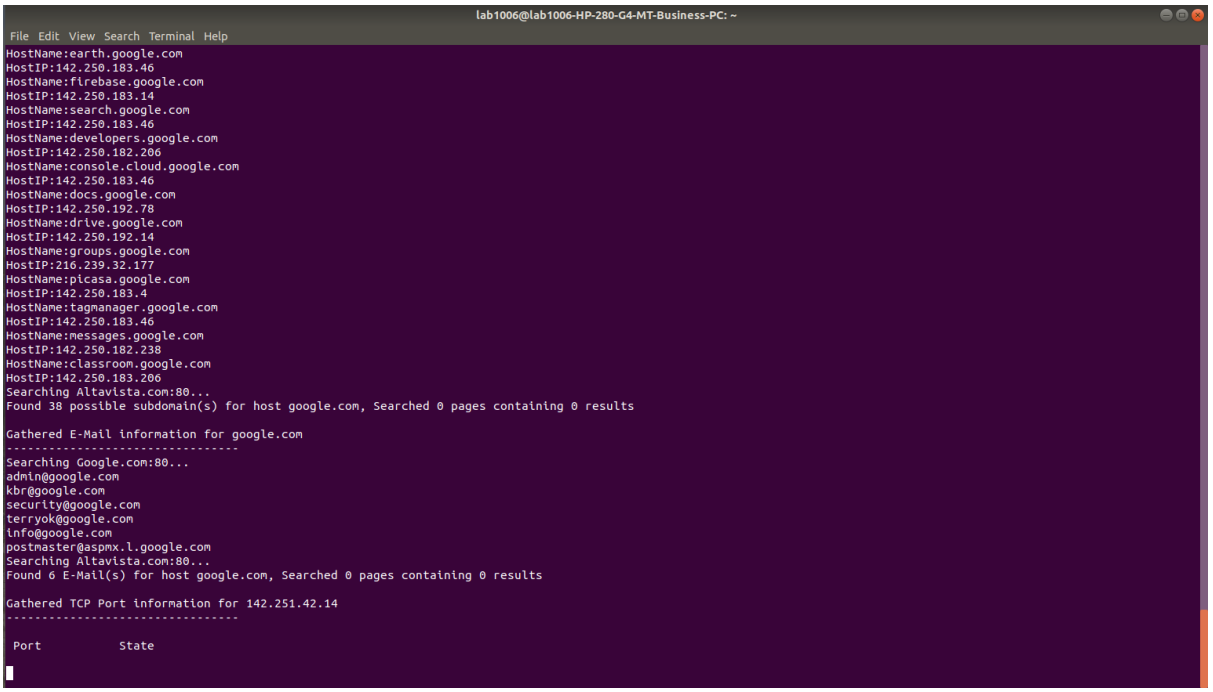
```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://tsec.edu/
^Clab1006@lab1006-HP-280-G4-MT-Business-PC:~$ 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 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
```

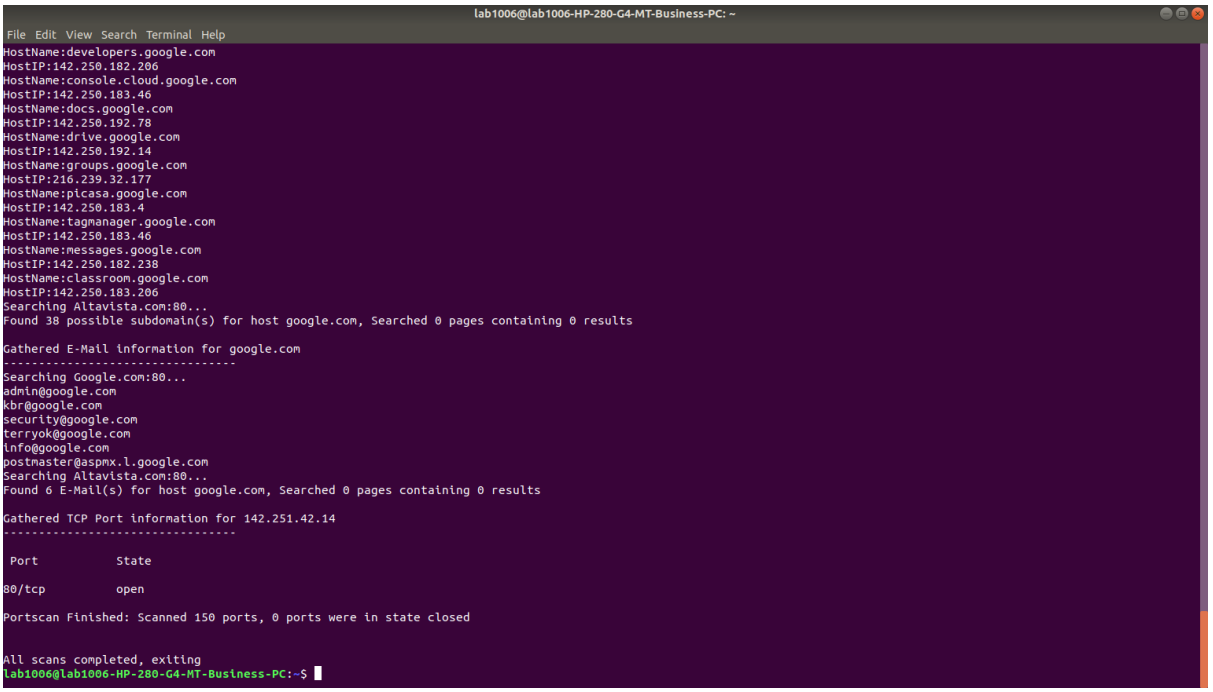
Roll no. : 53
Name: Shreya Kamath
Date: 7th August, 2023.





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





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.