Aim:

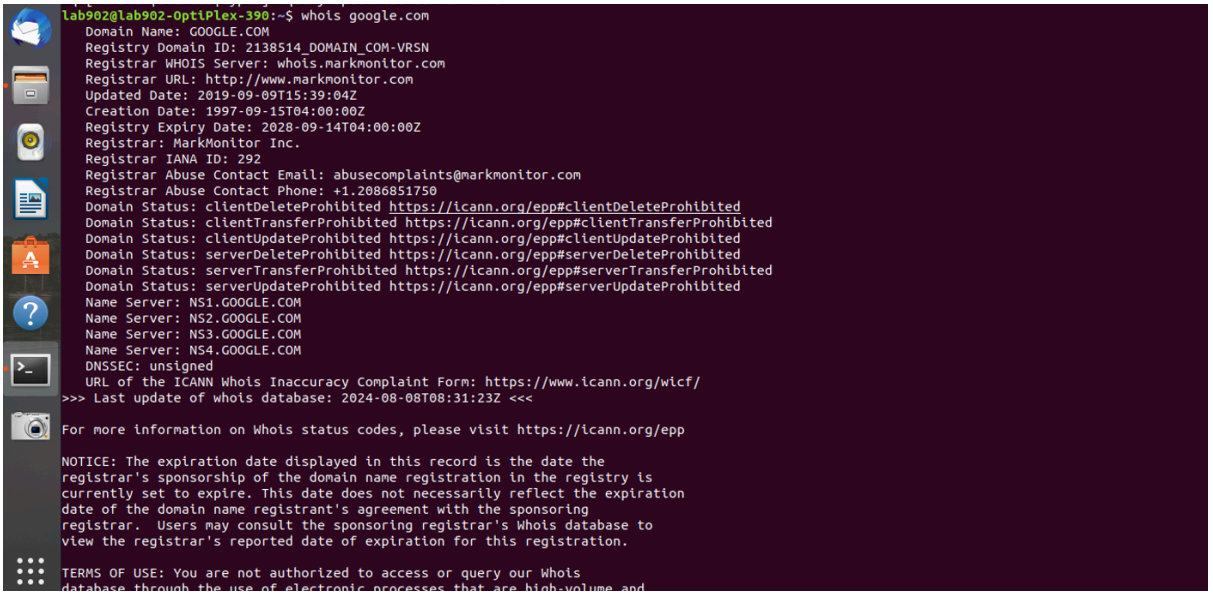
Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup, nikto, dmitry to gather information about networks and domain registrars.

LO Mapping: LO3

Theory:

Network reconnaissance tools are critical for gathering information about networks, domains, and registrars, which is an essential phase in cybersecurity operations, penetration testing, and network administration. These tools allow users to understand the layout, vulnerabilities, and configurations of networks, which can be used for both securing and attacking network infrastructures.

1. **WHOIS**: WHOIS is a query and response protocol used to look up details about domain names, including information about the domain's registrant, the registrar, and domain status. It is widely used to identify the ownership and administrative contacts for a domain.
   Popular Commands/Features:
   - **whois example.com**: Retrieves information about the domain "example.com".
   - **whois -h whois.arin.net 192.0.2.1**: Queries a specific WHOIS server for information related to an IP address.
   - **whois -r example.com**: Performs a WHOIS lookup without following referrals to other WHOIS servers.

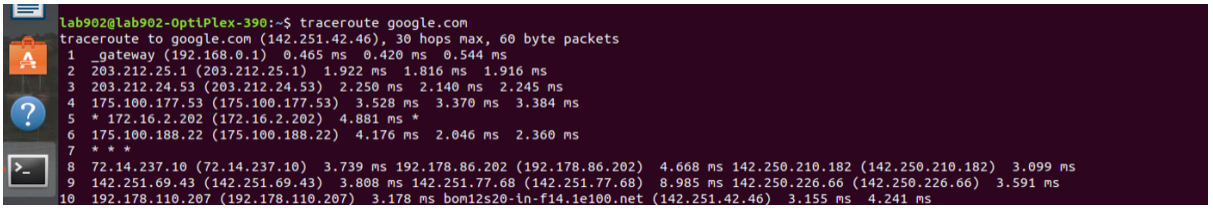


```
lab902@lab902-OptiPlex-390:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry 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: 2024-08-08T08:31:23Z <<<

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
```

2. **dig**: `dig` (Domain Information Groper) is a command-line tool used for querying DNS name servers. It is commonly used to perform DNS lookups and troubleshoot DNS-related issues.
   Top 3 Popular Commands/Features:
   - **dig example.com**: Performs a DNS lookup for the domain "example.com".
   - **dig example.com MX**: Retrieves the Mail Exchange (MX) records for "example.com".
   - **dig +short example.com**: Provides a simplified output with just the answer section of the DNS query.

```
lab902@lab902-OptiPlex-390:~$ dig google.com

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43271
;; 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.             83      IN      A       142.251.42.46

;; Query time: 2 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Aug 08 14:02:31 IST 2024
;; MSG SIZE  rcvd: 55
```

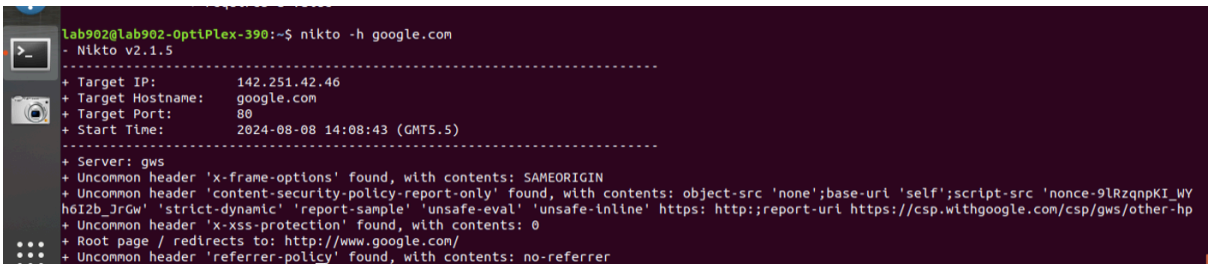
3. **traceroute**: `traceroute` is a network diagnostic tool that traces the path packets take from the source machine to the destination. It reveals the intermediate hops and their IP addresses, which can help in identifying routing issues.
   Top 3 Popular Commands/Features:
   - **traceroute example.com**: Traces the route to "example.com" to display the path and delay of each hop.
   - **traceroute -n example.com**: Displays IP addresses in numeric form without resolving them to hostnames.
   - **traceroute -T example.com**: Uses TCP SYN packets instead of the default UDP packets for tracing.



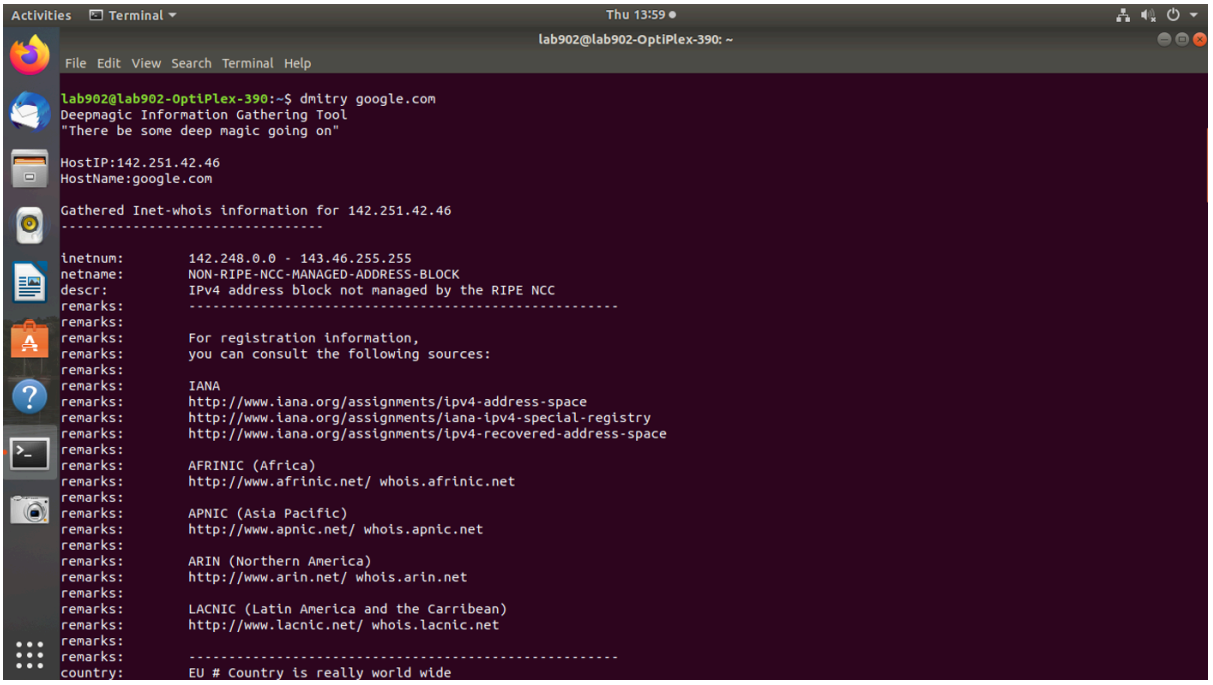
```
lab902@lab902-OptiPlex-390:~$ traceroute google.com
traceroute to google.com (142.251.42.46), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  0.465 ms  0.420 ms  0.544 ms
 2  203.212.25.1 (203.212.25.1)  1.922 ms  1.816 ms  1.916 ms
 3  203.212.24.53 (203.212.24.53)  2.250 ms  2.140 ms  2.245 ms
 4  175.100.177.53 (175.100.177.53)  3.528 ms  3.370 ms  3.384 ms
 5  * 172.16.2.202 (172.16.2.202)  4.881 ms *
 6  175.100.188.22 (175.100.188.22)  4.176 ms  2.046 ms  2.360 ms
 7  * * *
 8  72.14.237.10 (72.14.237.10)  3.739 ms 192.178.86.202 (192.178.86.202)  4.668 ms 142.250.210.182 (142.250.210.182)  3.099 ms
 9  142.251.69.43 (142.251.69.43)  3.808 ms 142.251.77.68 (142.251.77.68)  8.985 ms 142.250.226.66 (142.250.226.66)  3.591 ms
10  192.178.110.207 (192.178.110.207)  3.178 ms bom12s20-in-f14.1e100.net (142.251.42.46)  3.155 ms  4.241 ms
```

4. **nslookup**: `nslookup` is a command-line utility that allows users to query Internet domain name servers. It is commonly used to obtain domain name or IP address mapping and diagnose DNS-related problems.
   Top 3 Popular Commands/Features:
   - **nslookup example.com**: Looks up the IP address associated with the domain "example.com".
   - **nslookup -type=MX example.com**: Retrieves the Mail Exchange (MX) records for "example.com".
   - **nslookup -type=NS example.com**: Retrieves the Name Server (NS) records for "example.com".

5. **nikto**: `nikto` is an open-source web server scanner that performs comprehensive tests against web servers for multiple items, including over 6,700 potentially dangerous files/programs, checks for outdated versions of servers, and version-specific problems.
   Top 3 Popular Commands/Features:
   - **nikto -h http://example.com**: Scans the web server at "example.com" for known vulnerabilities.
   - **nikto -Plugins**: Lists available plugins that can be used with `nikto`.
   - **nikto -Display V**: Provides verbose output, showing more detailed information during the scan



6. **dmitry**: `dmitry` (Deepmagic Information Gathering Tool) is a command-line tool used for gathering as much information as possible about a host, including subdomains, email addresses, uptime reports, and open ports.
   Top 3 Popular Commands/Features:
   - **dmitry -winse example.com**: Performs a comprehensive scan including whois lookups, IP address information, subdomains, and email addresses for "example.com".
   - **dmitry -i example.com**: Displays interesting open ports found on the target host.
   - **dmitry -o output.txt example.com**: Saves the output of the scan to a file named "output.txt".



Conclusion:

In conclusion, network reconnaissance tools such as WHOIS, `dig`, `traceroute`, `nslookup`, `nikto`, and `dmitry` are essential for gathering detailed information about networks and domain registrars. These tools allow network administrators and cybersecurity professionals to understand the network's structure, discover potential vulnerabilities, and ensure proper network configuration. By mastering these tools, one can effectively map out and secure network environments, making them a critical component of any network analysis and security toolkit.