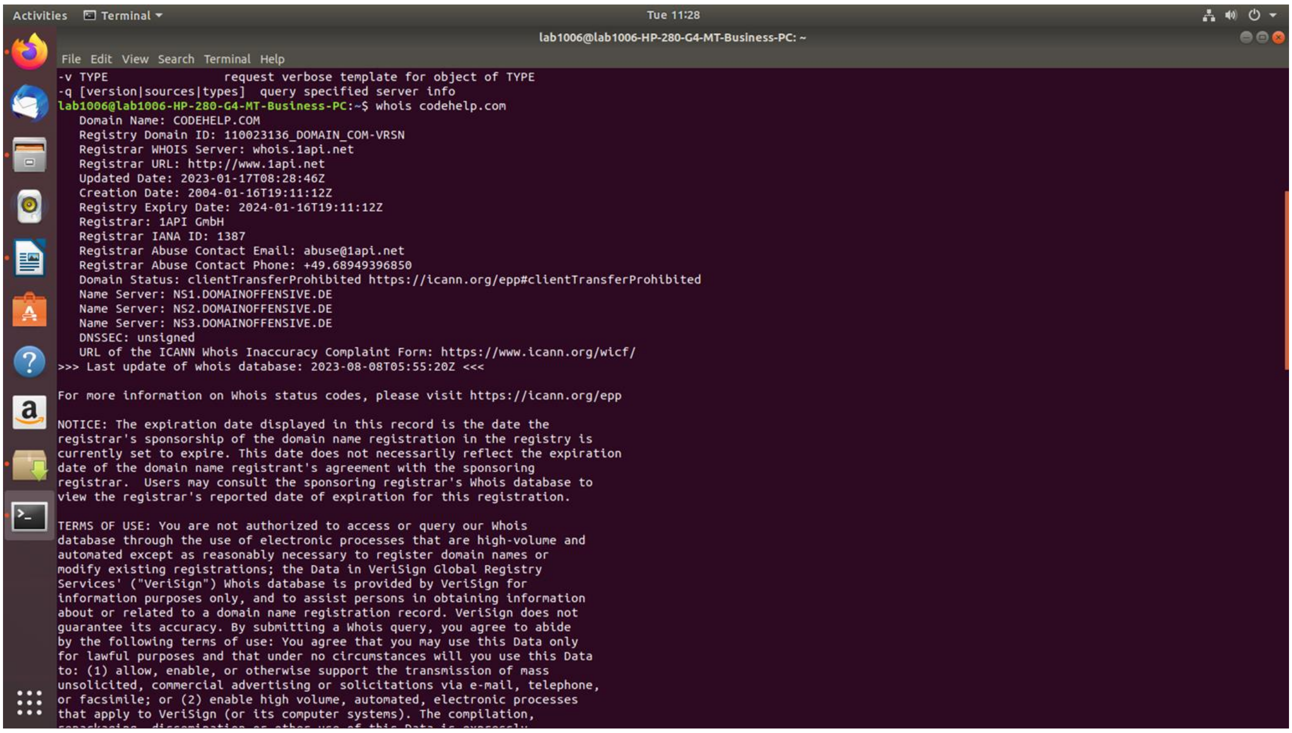
EXPERIMENT - 04

Aim : Implementation of network reconnaissance tools like WHOIS, dig, traceroute, nslookup, etc.

Commands :

1) WHOIS :

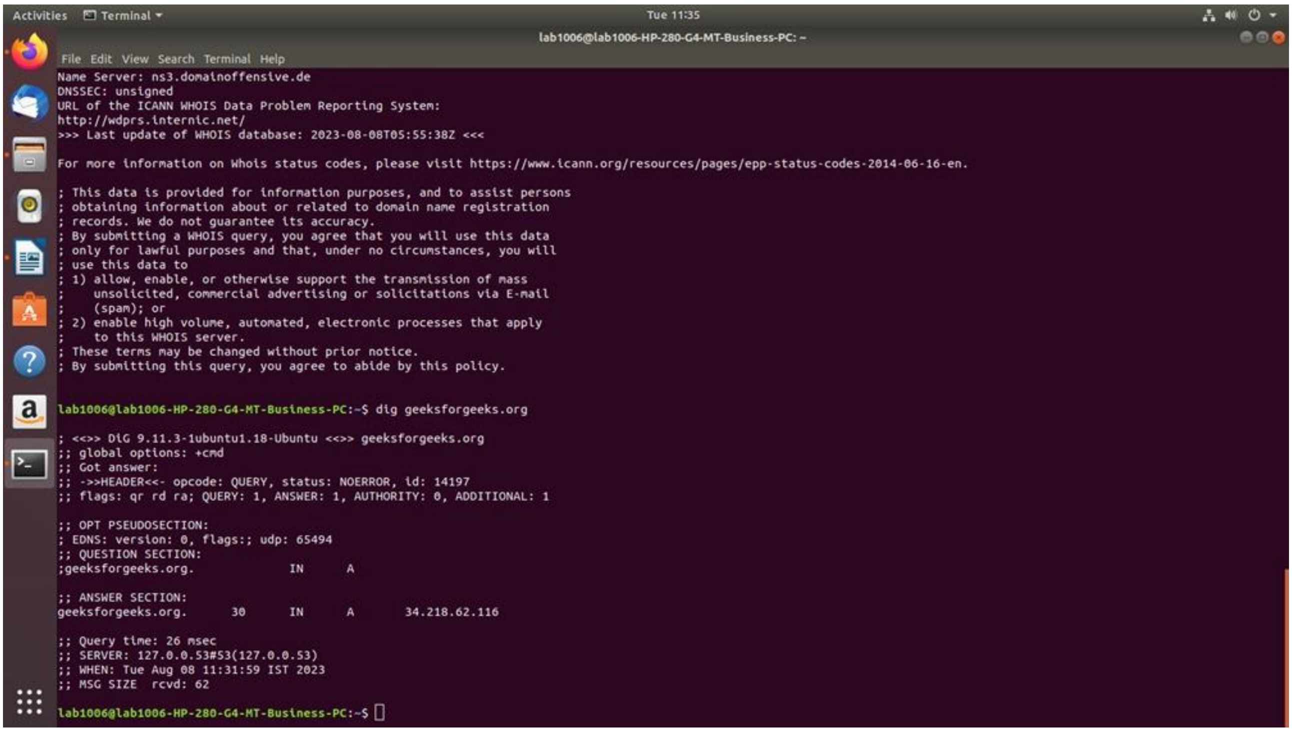
The whois command displays information about a website's record. You may get all the information about a website regarding its registration and owner's information.


Activities
Terminal
Tue 11:28
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
-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:~$ whois codehelp.com
   Domain Name: CODEHELP.COM
   Registry Domain ID: 110023136_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.1api.net
   Registrar URL: http://www.1api.net
   Updated Date: 2023-01-17T08:28:46Z
   Creation Date: 2004-01-16T19:11:12Z
   Registry Expiry Date: 2024-01-16T19:11:12Z
   Registrar: 1API GmbH
   Registrar IANA ID: 1387
   Registrar Abuse Contact Email: abuse@1api.net
   Registrar Abuse Contact Phone: +49.68949396850
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.DOMAINOFFENSIVE.DE
   Name Server: NS2.DOMAINOFFENSIVE.DE
   Name Server: NS3.DOMAINOFFENSIVE.DE
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-08T05:55:20Z <<<

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
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
```

2) dig :

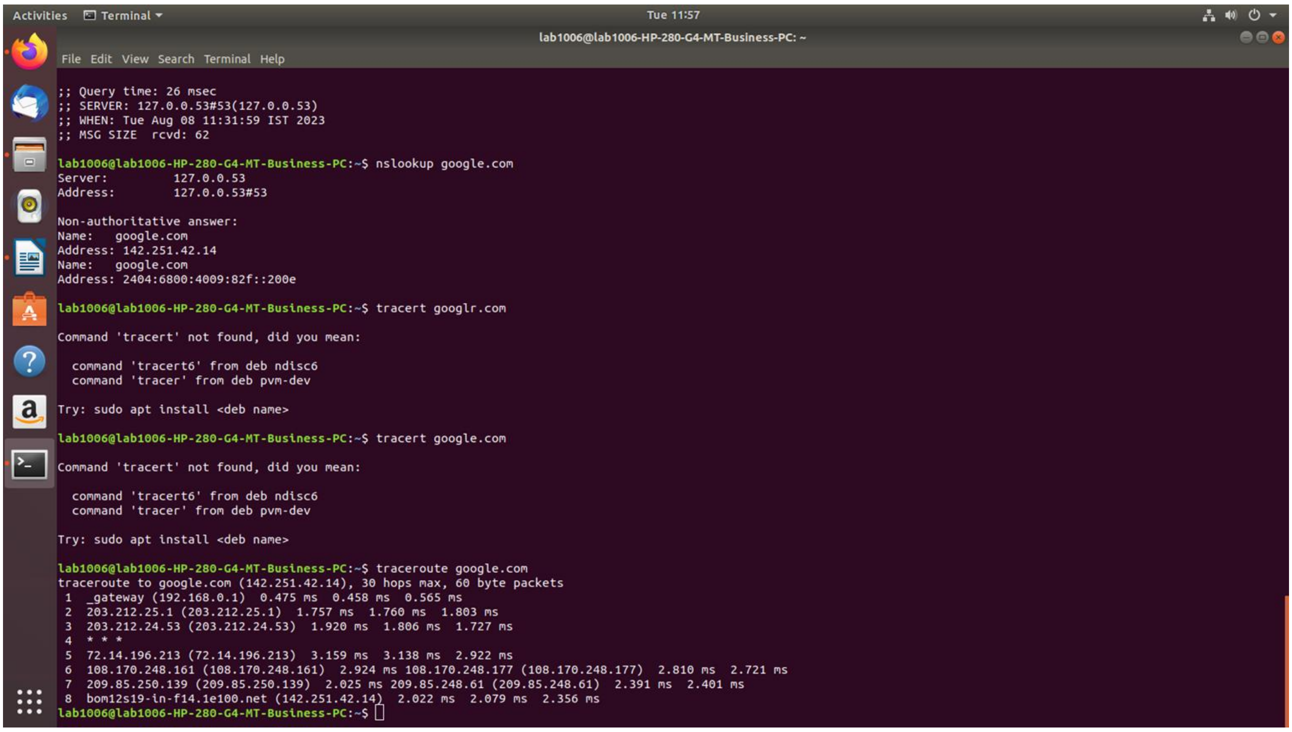
dig command stands for ***Domain Information Groper***. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups.


Activities
Terminal
Tue 11:35
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
Name Server: ns3.domainoffensive.de
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-08-08T05:55:38Z <<<

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

; This data is provided for information purposes, and to assist persons
; obtaining information about or related to domain name registration
; records. We do 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, you will
; 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 this WHOIS server.
; These terms may be changed without prior notice.
; By submitting this query, you agree to abide by this policy.


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: 14197
;; 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: 26 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Aug 08 11:31:59 IST 2023
;; MSG SIZE  rcvd: 62

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

3) traceroute :

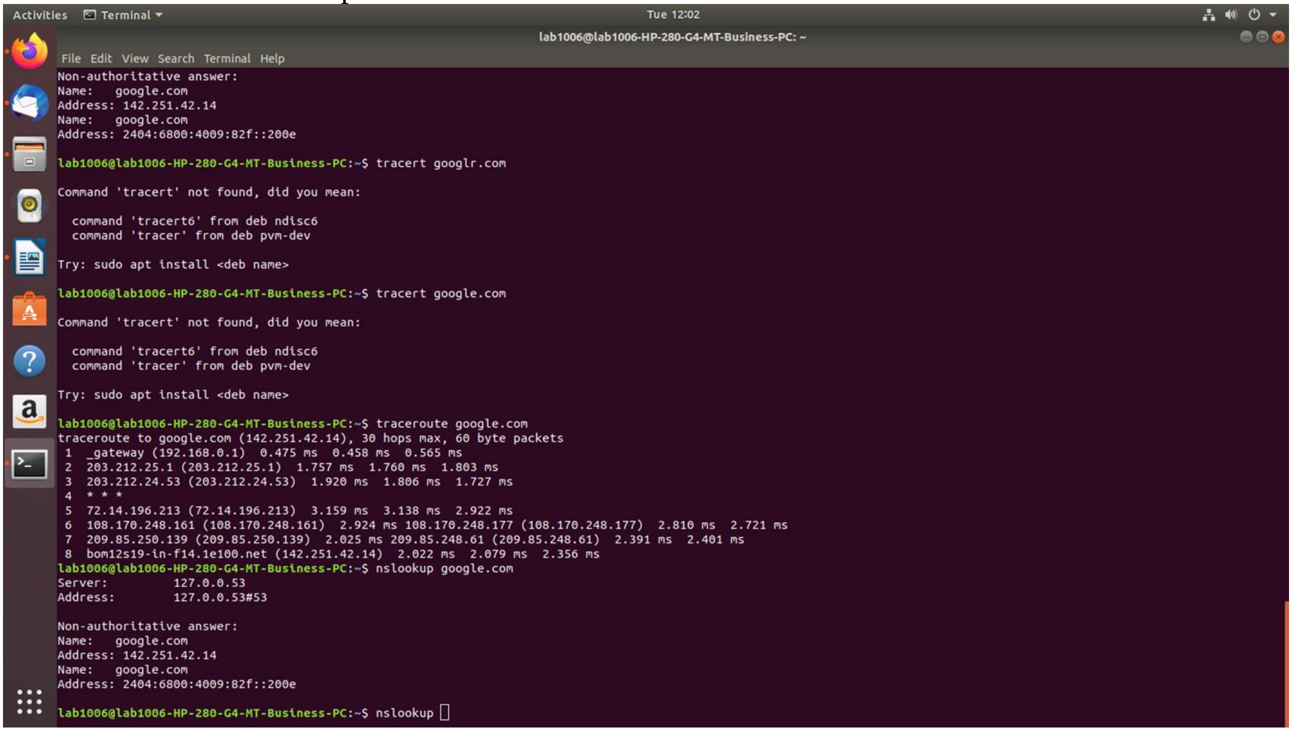
Traceroute is a widely used command-line utility available in almost all operating systems. It shows you the complete route to a destination address. It also shows the time is taken (or delays) between intermediate routers.


Activities
Terminal
Tue 11:57
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
;; Query time: 26 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Aug 08 11:31:59 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:~$ tracert googlr.com

Command 'tracert' not found, did you mean:

  command 'tracert6' from deb ndisc6
  command 'tracer' from deb pvm-dev

Try: sudo apt install <deb name>

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ tracert google.com

Command 'tracert' not found, did you mean:

  command 'tracert6' from deb ndisc6
  command 'tracer' from deb pvm-dev

Try: sudo apt install <deb name>

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute google.com
traceroute to google.com (142.251.42.14), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  0.475 ms  0.458 ms  0.565 ms
 2  203.212.25.1 (203.212.25.1)  1.757 ms  1.760 ms  1.803 ms
 3  203.212.24.53 (203.212.24.53)  1.920 ms  1.806 ms  1.727 ms
 4  * * *
 5  72.14.196.213 (72.14.196.213)  3.159 ms  3.138 ms  2.922 ms
 6  108.170.248.161 (108.170.248.161)  2.924 ms 108.170.248.177 (108.170.248.177)  2.810 ms  2.721 ms
 7  209.85.250.139 (209.85.250.139)  2.025 ms 209.85.248.61 (209.85.248.61)  2.391 ms  2.401 ms
 8  bom12s19-in-f14.1e100.net (142.251.42.14)  2.022 ms  2.079 ms  2.356 ms
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ 
```

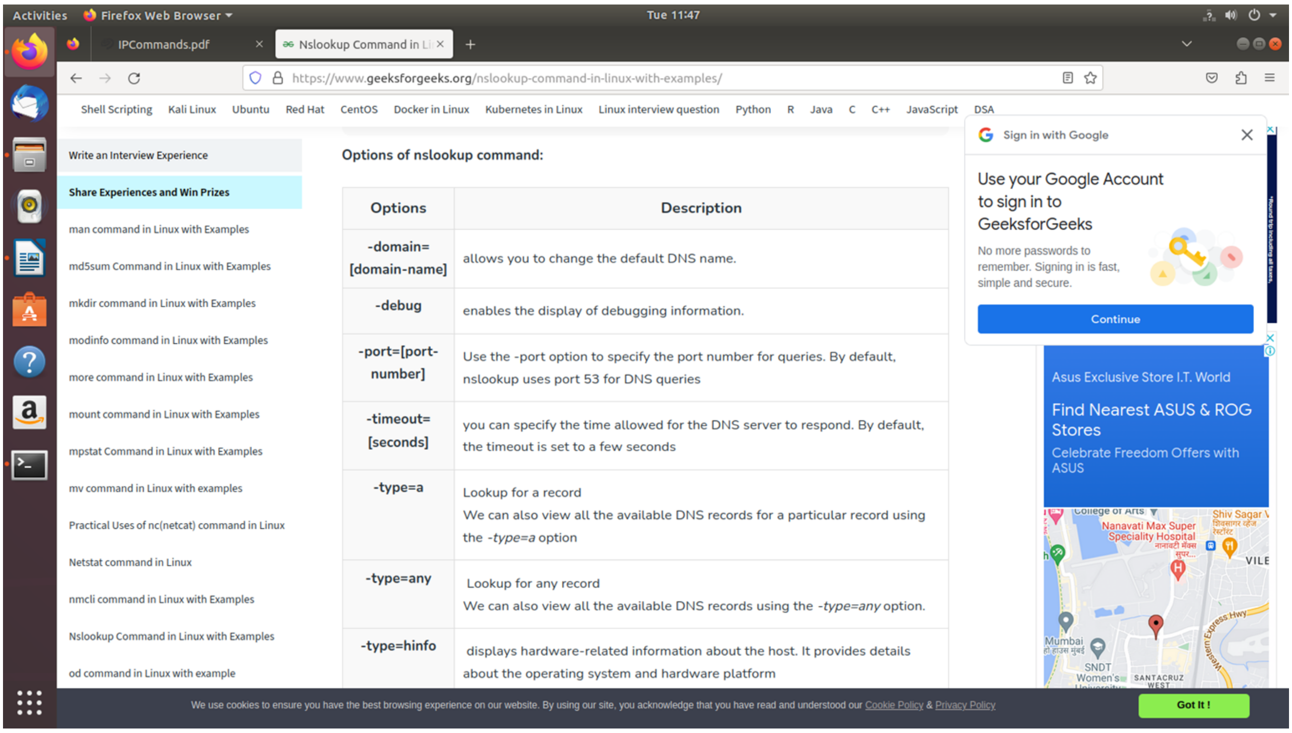
4) nslookup :

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.



Activities
Terminal
Tue 12:02
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
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:~$ tracert googlr.com

Command 'tracert' not found, did you mean:

  command 'tracert6' from deb ndisc6
  command 'tracer' from deb pvm-dev

Try: sudo apt install <deb name>

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ tracert google.com

Command 'tracert' not found, did you mean:

  command 'tracert6' from deb ndisc6
  command 'tracer' from deb pvm-dev

Try: sudo apt install <deb name>

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ traceroute google.com
traceroute to google.com (142.251.42.14), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  0.475 ms  0.458 ms  0.565 ms
 2  203.212.25.1 (203.212.25.1)  1.757 ms  1.760 ms  1.803 ms
 3  203.212.24.53 (203.212.24.53)  1.920 ms  1.806 ms  1.727 ms
 4  * * *
 5  72.14.196.213 (72.14.196.213)  3.159 ms  3.138 ms  2.922 ms
 6  108.170.248.161 (108.170.248.161)  2.924 ms 108.170.248.177 (108.170.248.177)  2.810 ms  2.721 ms
 7  209.85.250.139 (209.85.250.139)  2.025 ms 209.85.248.61 (209.85.248.61)  2.391 ms  2.401 ms
 8  bom12s19-in-f14.1e100.net (142.251.42.14)  2.022 ms  2.079 ms  2.356 ms
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:~$ nslookup 
```



Activities
Firefox Web Browser
Tue 11:47
IPCommands.pdf
Nslookup Command in Li
https://www.geeksforgeeks.org/nslookup-command-in-linux-with-examples/
Shell Scripting
Kali Linux
Ubuntu
Red Hat
CentOS
Docker in Linux
Kubernetes in Linux
Linux interview question
Python
R
Java
C
C++
JavaScript
DSA
Write an Interview Experience
Share Experiences and Win Prizes
man command in Linux with Examples
md5sum Command in Linux with Examples
mkdir command in Linux with Examples
modinfo command in Linux with Examples
more command in Linux with Examples
mount command in Linux with Examples
mpstat Command in Linux with Examples
mv command in Linux with examples
Practical Uses of nc(netcat) command in Linux
Netstat command in Linux
nmcli command in Linux with Examples
Nslookup Command in Linux with Examples
od command in Linux with example
Sign in with Google
Continue
Asus Exclusive Store I.T. World
Find Nearest ASUS & ROG Stores
Celebrate Freedom Offers with ASUS
Got It !

Use your Google Account to sign in to GeeksforGeeks

No more passwords to remember. Signing in is fast, simple and secure.

Options of nslookup command:

Options	Description
-domain=[domain-name]	allows you to change the default DNS name.
-debug	enables the display of debugging information.
-port=[port-number]	Use the -port option to specify the port number for queries. By default, nslookup uses port 53 for DNS queries
-timeout=[seconds]	you can specify the time allowed for the DNS server to respond. By default, the timeout is set to a few seconds
-type=a	Lookup for a record We can also view all the available DNS records for a particular record using the *-type=a* option
-type=any	Lookup for any record We can also view all the available DNS records using the *-type=any* option.
-type=hinfo	displays hardware-related information about the host. It provides details about the operating system and hardware platform

We use cookies to ensure you have the best browsing experience on our website. By using our site, you acknowledge that you have read and understood our Cookie Policy & Privacy Policy

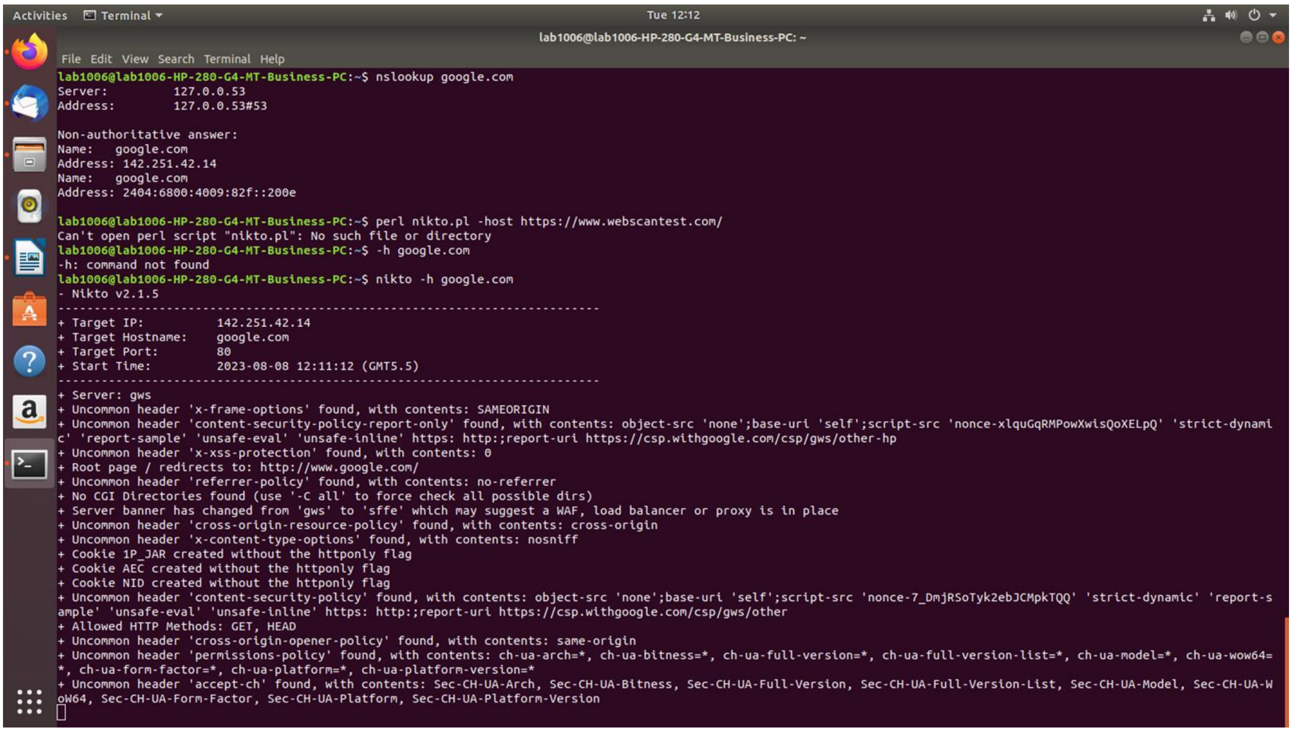
NIKTO:

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. It can also check for outdated version details of 1200 server and can detect problems with specific version details of over 200 servers. It can also fingerprint server using favicon.ico files present in the server. It is not designed to be a particularly a stealth tool rather than it is designed to be fast and time-efficient to achieve the task in very little time. Because of this, a web admin can easily detect that its server is being scanned by looking into the log files.

It can also show some items that do not have security problem but are info only which shows how to take full use of it to secure the web-server more properly.

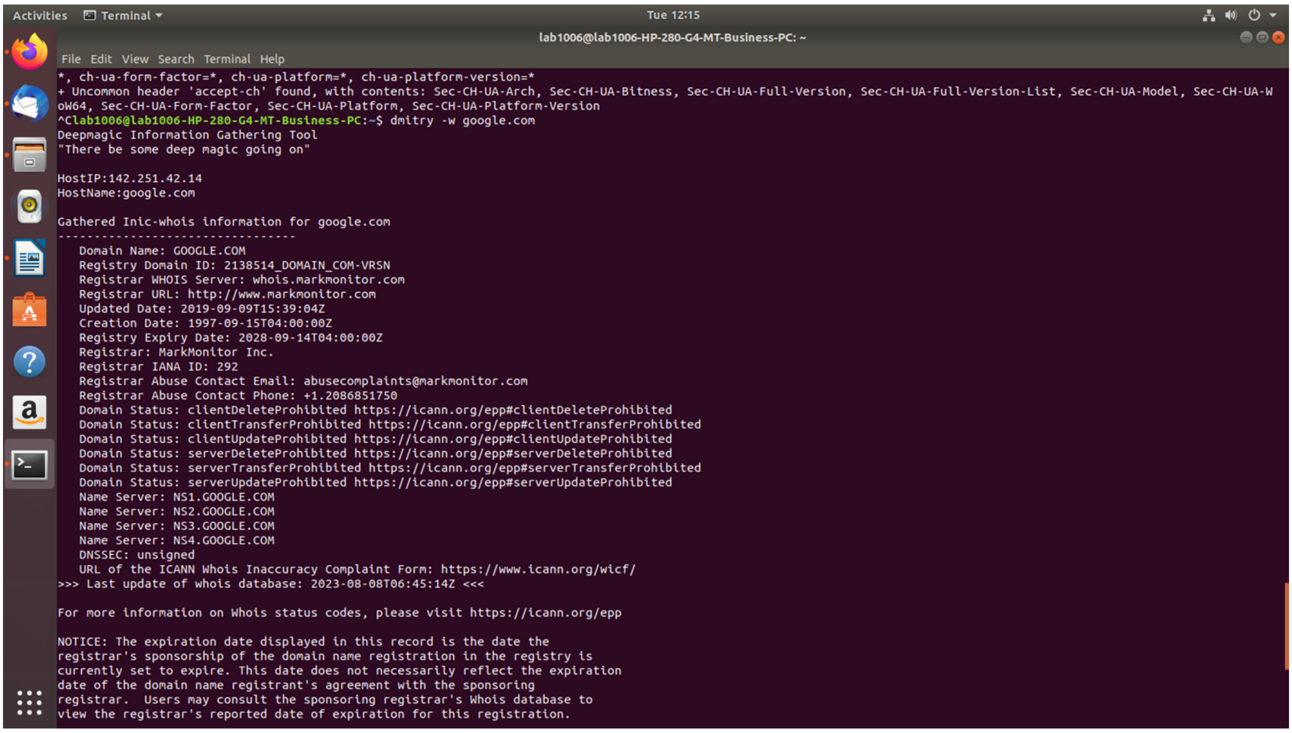
Features:

- Full support for SSL
- Finds sub-domain
- Supports full HTTP Proxy
- Outdated component report
- Result saved in multiple format (xml, csv etc)
- Username guessing
- Gives details of installed software
- Takes Nmap file as input to scan port in a web-server.
- Able to perform dictionary attack.
- Updated easily


Activities
Terminal
Tue 12:12
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
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:~$ perl nikto.pl -host https://www.webscantest.com/
Can't open perl script "nikto.pl": No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ -h google.com
-h: command not found
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:         2023-08-08 12:11:12 (GMT5.5)
---------------------------------------------------------------------------
+ Server: gws
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'content-security-policy-report-only' found, with contents: object-src 'none';base-uri 'self';script-src 'nonce-xlquGqRMPowXwisQoXELpQ' 'strict-dynami
c' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ 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 'cross-origin-resource-policy' found, with contents: cross-origin
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ 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-7_DmjRSoTyk2ebJCMpkTQQ' '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
+ Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin
+ Uncommon header 'permissions-policy' found, with contents: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=
*, ch-ua-form-factor=*, ch-ua-platform=*, ch-ua-platform-version=*
+ Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-W
oW64, Sec-CH-UA-Form-Factor, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version
```

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
Tue 12:15
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
*, ch-ua-form-factor=*, ch-ua-platform=*, ch-ua-platform-version=*
+ Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-W
oW64, Sec-CH-UA-Form-Factor, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version
^Clab1006@lab1006-HP-280-G4-MT-Business-PC:~$ dmitry -w google.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:142.251.42.14
HostName:google.com

Gathered Inic-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: 2023-08-08T06:45:14Z <<<

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.
```

CONCLUSION:-

We have successfully made use of reconnaissance tools like WHOIS, dig, traceroute etc. and gathered information about the networks and domain registers which maps to **LO3.**

LO3 : To explore different network reconnaissance tools to gather information about networks.