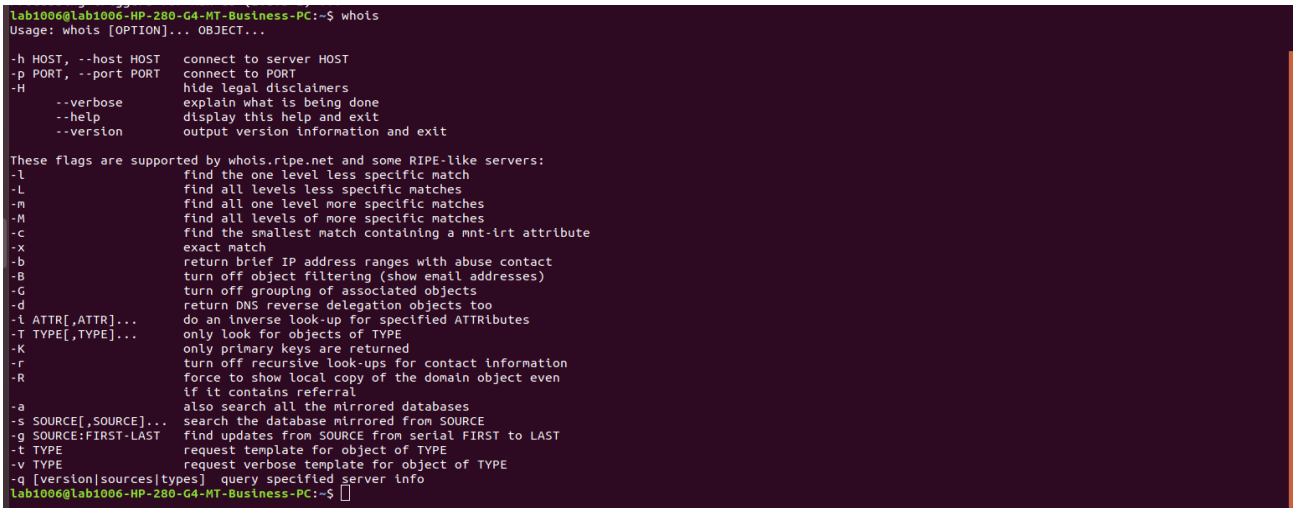
YUVRAJ UPADHYAY
BATCH: T22
ROLL NO: 96

ASSIGNMENT 6

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

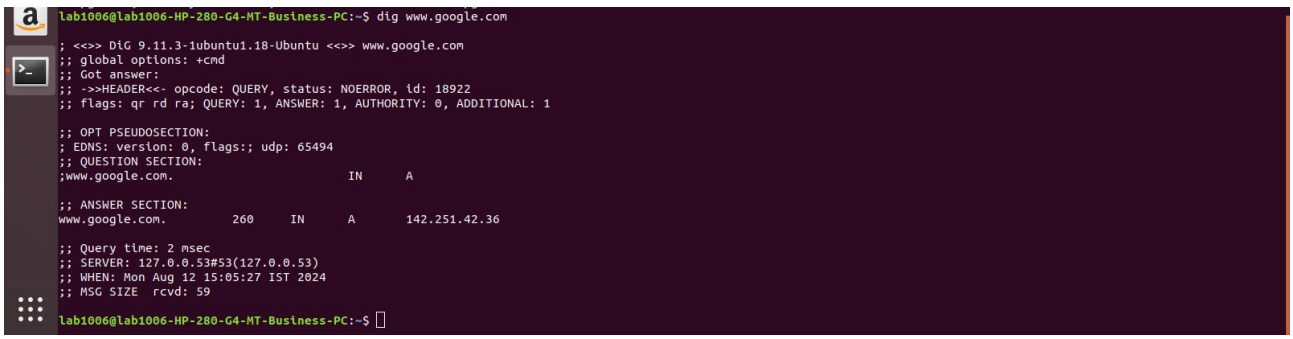
1.whois

whois command searches a user name directory and displays information about the user ID or nickname specified in the Name parameter. The whois command tries to reach ARPANET host internic.net where it examines a user-name database to obtain information.



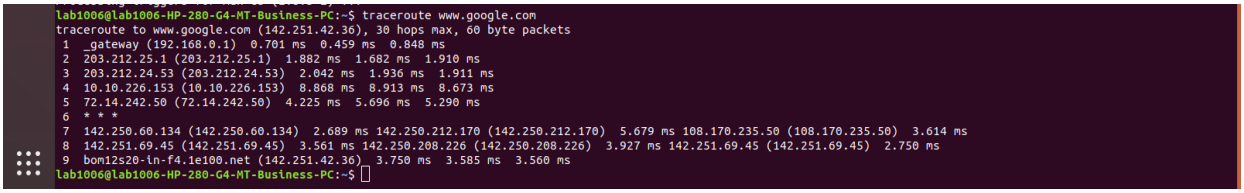
2.dig

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. Dig command replaces older tools such as nslookup and the host.



3.traceroute

The `traceroute` command is a network diagnostic tool used to trace the route taken by packets from a source to a destination over an IP network. It provides valuable insights into the network path, including the number of hops (routers) between the source and destination, and the round-trip time (RTT) for each hop.



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.

5.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

6.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.