1. **Ping:** Ping is a command-line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable.

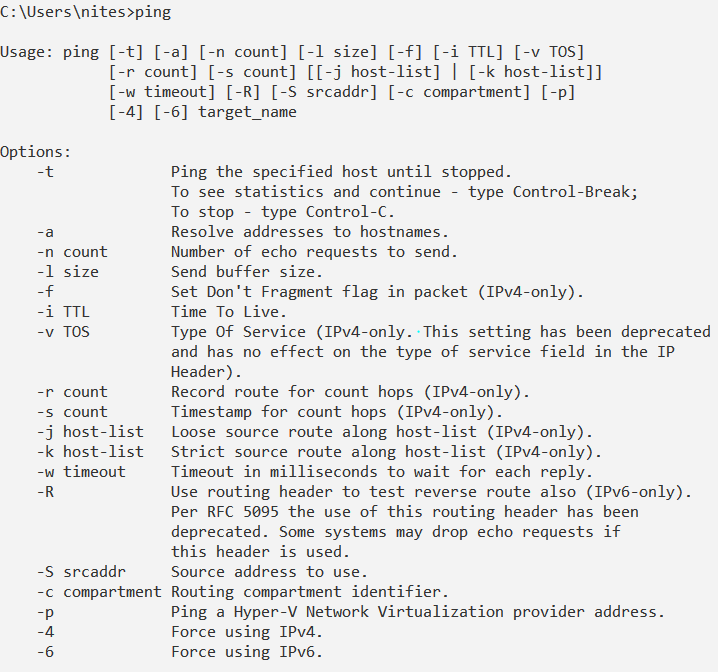
# Traceroute: The traceroute command attempts to trace the route an IP packet follows to an Internet host by launching UDP probe packets with a small maximum time-to-live (Max\_ttl variable), then listening for an ICMP TIME\_EXCEEDED response from gateways along the way.

1. **Nslookup**: The nslookup command queries internet domain name servers in two modes. Interactive mode allows you to query name servers for information about various hosts and domains, or to print a list of the hosts in a domain.
2. **Whois**: The whois command tries to reach ARPANET host internic.net where it examines a user-name database to obtain information. The whois command should be used only by users on ARPANET.
3. **Nmap:** Nmap is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators. It is used for the following purposes:

* Real time information of a network
* Detailed information of all the IPs activated on your network

**Result and Discussion**

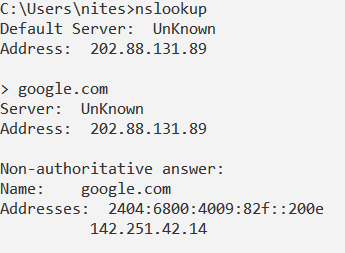
1. **Ping:**



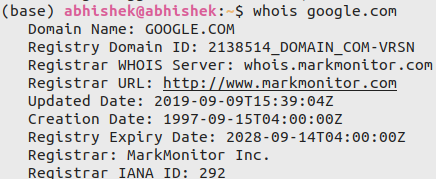
# Traceroute:

# 

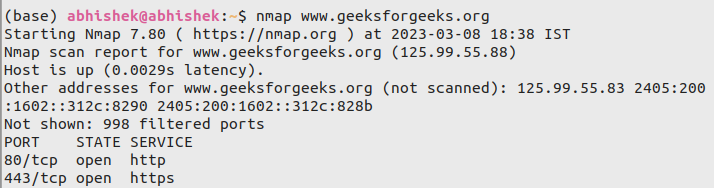
1. **Nslookup**

****

1. **Whois**



1. **Nmap**



**(**Analyze the tool nmap and use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc)