Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Experiment No. : 7

Name : Avadhoot Pawaskar
Rollno.: 43

Date: 10/09/2024

Title : Network Reconnaissance tools/commands

Problem Definition : Use following Network Reconnaissance tools/commands to gather information about network and domain registrars.

WHOIS, dig, traceroute, nslookup

Pre-requisite : Networking commands

Theory :

WHOIS: It searches for an object in a RFC 3912 database. This version of the whois client tries to guess the right server to ask for the specified object. If no guess can be made it will connect to whois.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.

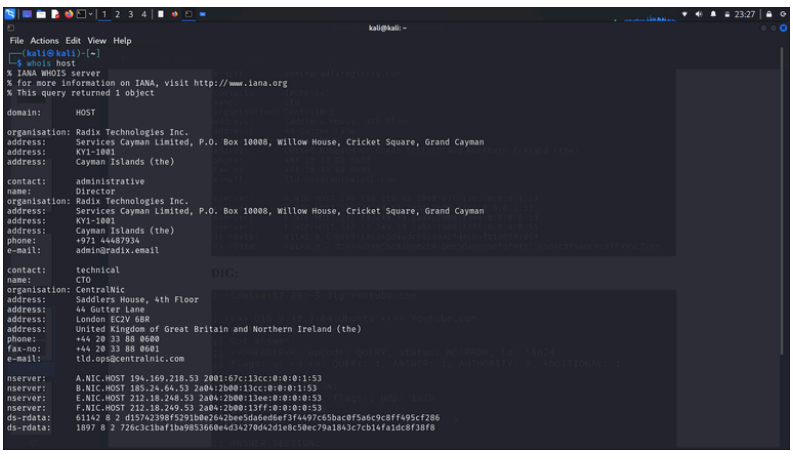
dig (domain information groper): It is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig.

Traceroute: It tracks the route packets taken from an IP network on their way to a given host. It utilizes the IP protocol's time to live (TTL) field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to the host.

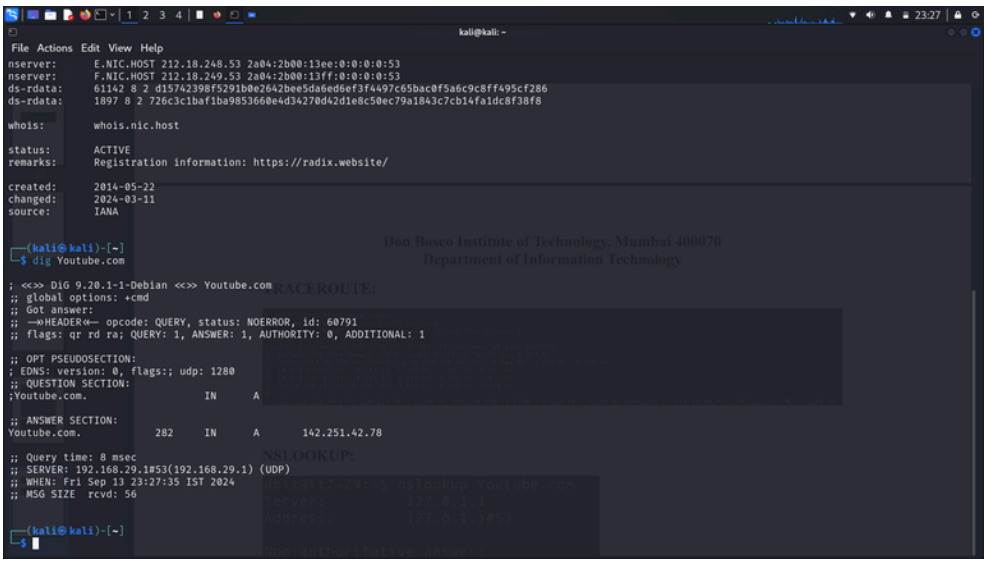
Nslookup: It is a program to query Internet domain name servers. Nslookup has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Noninteractive mode is used to print just the name and requested information for a host or domain.

Results :

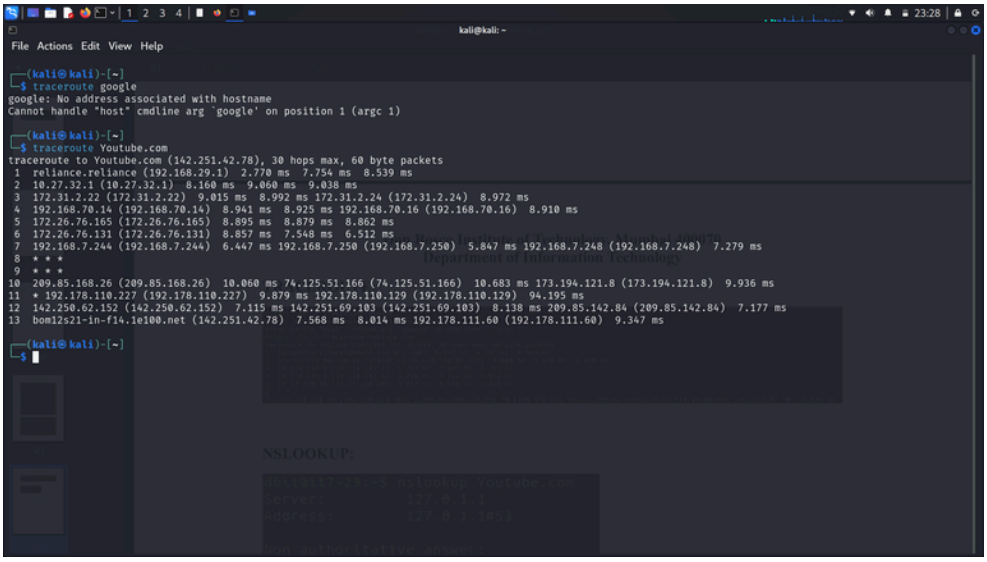
1. WHOIS



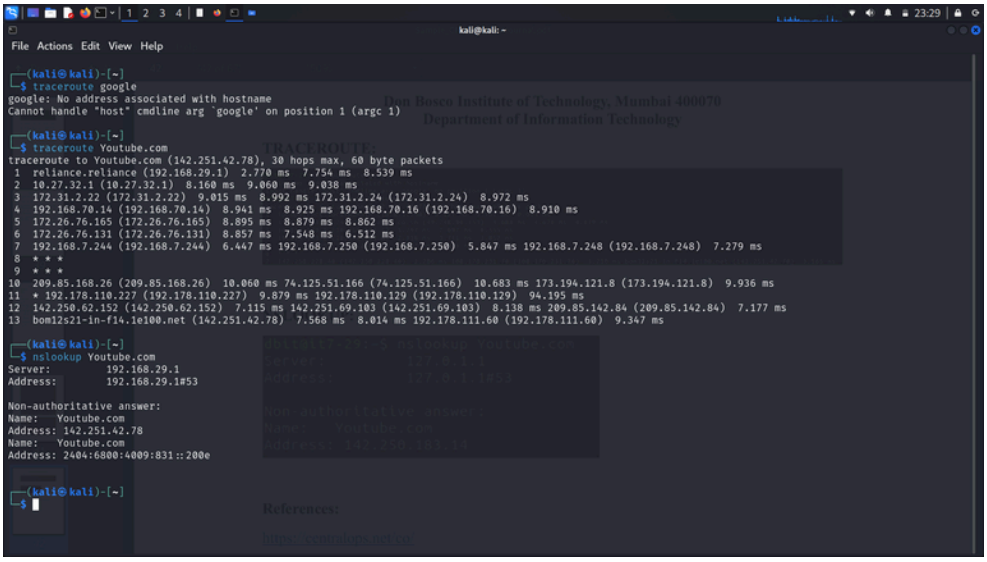
2. DIG



3. TRACEROUTE



4. NSLOOKUP



References:
https://centralops.net/co/
https://www.howtogeek.com/190148/8-common-network-utilities-explained/