TCET

DEPARTMENT OF COMPUTER ENGINEERING (COMP)

(Accredited by NBA for 3 years, 3rd Cycle Accreditation w.e.f. 1st July 2019)

Choice Based Credit Grading System with Holistic Student Development (CBCGS - H 2019)

Under TCET Autonomy Scheme - 2019

Name: Deep Kothari

Class: TECOMP-B

Roll No: 23

CSS Experiment 1 -A

AIM:

Understand the use of network reconnaissance tools like WHOIS, dig, trace route, nslookup to gather information about network and domain registers.

THEORY:

1. Whois - Whois searches for an object in a WHOIS database. WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block, but is also used for a wider range of other information. Most modern versions of whois try to guess the right server to ask for the specified object. If no guess can be made, whois will connect to whois.network solutions.com for NIC handles orwhois.arin.netforIPv4addresses and network names.

   Importance of WHOIS:
   - Helps network administrators find and fix system problems and maintain Internet stability.
   - Manages registration status of domain names.
   - Assists in fighting abusive use of internet.

   Examples:
   - Obtaining the domain WHOIS record for computersolutions.com
   - WHOIS record by IP querying
   - Querying WHOIS in google search engine

2. **Dig** -Dig is a networking tool that can query DNS servers for information. It can be very helpful for diagnosing problems with domain pointing and is a good way to verify that your configuration is working. The most basic way to use dig is to specify the domain we wish to query: dig example.com.

3. **Trace Route** – When you connect with a website, the data you get must travel across multiple devices and networks along the way, particularly routers. A traceroute provides a map of how data on the internet travels from its source to its destination. A traceroute plays a different role than other diagnostic tools, such as packet capture,

which analyses data. Traceroute differs in that it examines how the data moves through the internet. A traceroute works by sending Internet Control Message Protocol (ICMP) packets, and every router involved in transferring the data gets these packets. The ICMP packets provide information about whether the routers used in the transmission are able to effectively transfer the data. An Internet Protocol (IP) tracer is helpful for figuring out the routing hops data has to go through, as well as response delays as it travels across nodes, which are what send the data toward its destination. Traceroute also enables you to locate where the data was unable to be sent along, known as points of failure. You can also perform a visual traceroute to get a visual representation of each hop.

The traceroute report lists data pertaining to every router the packets pass through as they head to their destination. The hops get numbered on the left side of the report window. Each line in the report has the domain name—if that was included—as well as the IP address belonging to the router. There are also three measurements of time, displayed in milliseconds. These tell you the length of time to send the ICMP packets from your computer to that router and back.

The primary difference between ping and traceroute is that while ping simply tells you if a server is reachable and the time it takes to transmit and receive data, traceroute details the precise route info, router by router, as well as the time it took for each hop.

4. **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. In noninteractive mode, the names and requested information are printed for a specified host or domain. The **nslookup** command enters interactive mode when no arguments are given, or when the first argument is a - (minus sign) and the second argument is the host name or internet address of a name server. When no arguments are given, the command queries the default name server. The **nslookup** command enters non-interactive mode when you give the name or internet address of the host to be looked up as the first argument. The optional second argument specifies the host name or address of a name server. You can specify options on the command line if they precede the arguments and are prefixed with a hyphen

RESULT AND DISCUSSION:

We were able to:-

• Understand, identify, analyse and design the problem, implement the same using current techniques, skills, and tools and validate the solution including both hardware and software.

• Use network-based tools for network analysis

CONCLUSION:

It was understood how to obtain information about network and domain registers using network reconnaissance tools such as WHOIS, dig, trace route and nslookup.