NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

LAB 07

LAB 07: Study the use of network reconnaissance tools like WHOIS, dig, traceroute, and nslookup to gather information about networks and domain registrars.

ROLL NO	52
NAME	Sarvesh Patil
CLASS	D15A
SUBJECT	Internet Security Lab
LO MAPPED	LO3: Explore the different network reconnaissance tools to gather information about networks

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

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

INTRODUCTION:

Active Reconnaissance is a method of collecting information about the target environment by directly interacting with the target or by sending traffic to the target. This information is further used to exploit the target. This method may be identified by Intrusion Detection System (IDS) used by the target organization. Click Here if you are interested in knowing Passive Reconnaissance techniques used by Security Experts while engagements in penetration testing.

This recon activity can be performed by using three major types of tools:

1. Port Scanning Tools: Identify open ports
2. Web Service Review Tools: Identify web-based vulnerabilities
3. Network Vulnerability Scanning Tools: Identify infrastructure-related security issues

Port Scanning Tools

Port scanning is a method of identifying open ports by connecting each port of a target system. Assume the port scanner tool identifies open port 22, which is related to secure shell ssh. An attacker might try SSH-related attacks on the target system. This is like an open window in a host where a thief may try to enter by using that open window. Below are some tools that you may use for identifying open ports.

- Nmap: Popular and free port scanner, limited vulnerability scanner by using existing Nmap scripts (/usr/share/nmap/scripts) available in the Nmap database. Refer to Nmap Cheatsheet to understand different commands.
- udp-proto-scanner: Discovers UDP services such as DNS, TFTP, NTP, NBT, SunRPC, MS SQL, DB2, SNMPv3
- Masscan: Fastest port scanner and claims to scan the internet within 6 minutes by transmitting 10 million packets per second, from a single machine.
- Angry IP Scanner - Another port scanner tool. It is absolutely free to use and you need to just provide a range of IP addresses.

Web Service Review Tools

- Nikto - Quick and terminal-based web vulnerability scanner which gives basic security issues. Click Here Nikto tutorial for usage of the tool.
- Netsparker - Commercial web application security scanning tool used by security auditing agencies.
- SQLMap - It is an open-source penetration tool that helps in detecting and exploit SQL injection issues.
- Burpsuite - The most popular tool among the people in the security community.
- HCL AppScan: Commercial application security scanning tool

- wpscan: Opensource tool used to scan vulnerabilities of WordPress websites. Click Here for a brief tutorial on the Security Audit of WordPress Applications.
- EyeWitness: This tool collects a snapshot of web pages automatically to RDP services, and opens VNC servers.
- WebInspect: Expensive commercial web application vulnerability scanning tool.
- Zed Attack Proxy (ZAP) - Open source web vulnerability scanner developed by OWASP. Click Here If you want to download OWASP ZAP and use it in your project.

Network Vulnerability Scanning Tools

- OpenVAS - opensource tool, network vulnerability scanner. It supports both authenticated and unauthenticated vulnerability scanning.
- Nessus - The most popular and widely used network vulnerability scanner. Click Here If you want to know the differences between OpenVAS and Nessus tool.
- Nexpose - This commercial tool was developed by Rapid7 and used as Vulnerability management software in big enterprises.
- Qualys - Deployed at data centers for vulnerability management, detection, and response.
- Amass - Open Source tool by OWASP

Domain name registrars:

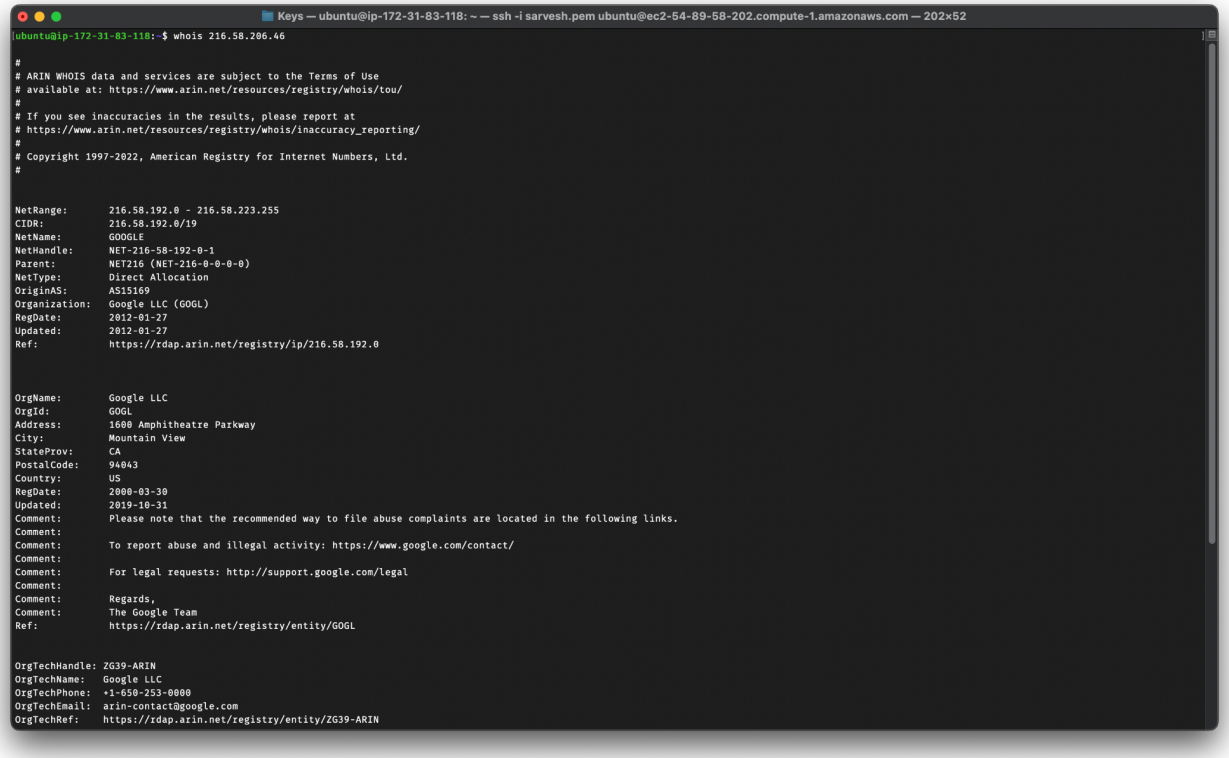
A domain name registrar is a business that handles the reservation of domain names as well as the assignment of IP addresses for those domain names. Domain names are alphanumeric aliases used to access websites; for example, Google's domain name is 'google.com' and its IP address is 192.168.1.1. Domain names make it easier to access websites without having to memorize and enter numeric IP addresses. A domain name registrar is a company that manages the reservation of Internet domain names.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

THEORY AND OUTPUT:

1. **whois**
    a. 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.
    b. 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.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.
    c. The /usr/bin/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. The whois command should be used only by users on ARPANET. Refer to RFC 812 for more complete information and recent changes to the whois command.
    d. “Note: If your network is on a national network, such as ARPANET, the hostname is hard-coded as internic.net.”
    e. The Name [. . .] parameter represents the user ID, hostname, network address, or nickname on which to perform a directory search. The whois command performs a wildcard search for any name that matches the string preceding the optional ... (three periods).
    f. WHOIS is a TCP-based query and response protocol that is commonly used to provide information services to Internet users. It returns information about the registered Domain Names, an IP address block, Name Servers, and a much wider range of information services.
    g. In Linux, the whois command line utility is a WHOIS client for communicating with the WHOIS server (or database host) which listens to requests on the well-known port number 43, which stores and delivers database content in a human-readable format.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

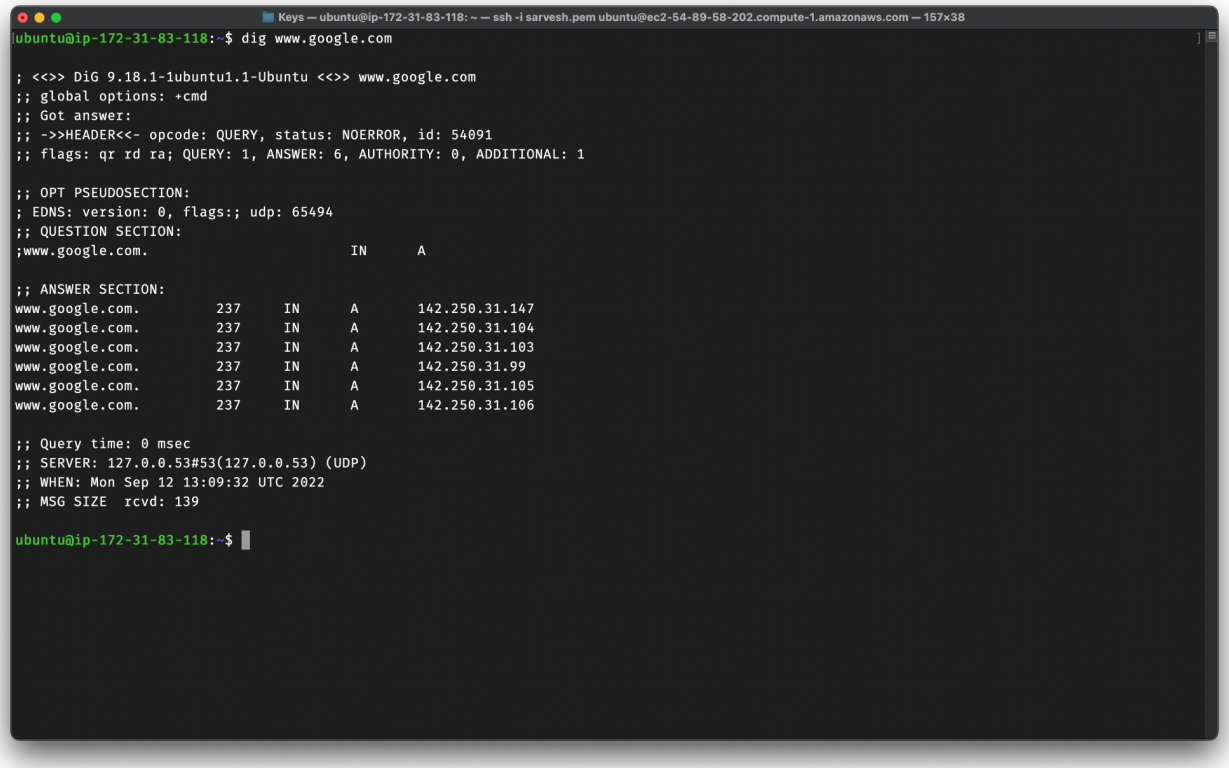


NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

2. dig

a. The dig command in Linux is used to gather DNS information. It stands for Domain Information Groper, and it collects data about Domain Name Servers.
b. The dig command is helpful for diagnosing DNS problems but is also used to display DNS information.
c. The first column lists the name of the server that was queried. The second column is Time to Live, a set time frame after which the record is refreshed. The third column shows the class of the query, in this case, IN stands for Internet. The fourth column shows the type of query, in this case, A stands for Address record. The final column displays the IP address associated with the domain name.
d. dig command stands for Domain Information Groper. It is used for retrieving information about DNS name servers.
e. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and performing DNS lookups.
f. Dig command replaces older tools such as nslookup and the host.
g. The dig (domain information groper) command is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the queried name server(s). Most DNS administrators use the dig command to troubleshoot DNS problems because of its flexibility, ease of use, and clarity of output.
h. The dig command, allows you to query information about various DNS records, including host addresses, mail exchanges, and name servers. It is the most commonly used tool among system administrators for troubleshooting DNS problems because of its flexibility and ease of use.
i. This tutorial explains how to use the dig utility through practical examples and detailed explanations of the most common dig options.
j. Dig (Domain Information Groper) is a Linux command line utility that performs DNS lookup by querying name servers and displaying the result to you.
k. A command dig is a tool for querying DNS nameservers for information about host addresses, mail exchanges, nameservers, and related information. This tool can be used from any Linux (Unix) or Macintosh OS X operating system. The most typical use of dig is to simply query a single host.

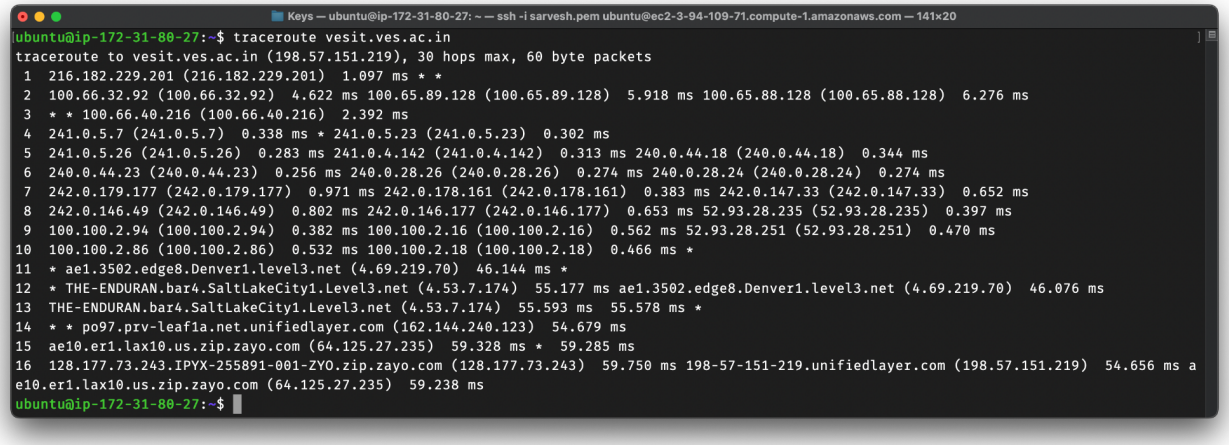
NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52



NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

3. traceroute

a. traceroute command in Linux prints the route that a packet takes to reach the host.
b. This command is useful when you want to know about the route and about all the hops that a packet takes.
c. The below image depicts how the traceroute command is used to reach the Google(172.217.26.206) host from the local machine and it also prints detail about all the hops that it visits in between.
d. The first column corresponds to the hop count.
e. The second column represents the address of that hop and after that, you see three space-separated times in milliseconds.
f. 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.
g. Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Traceroute also records the time taken for each hop the packet makes during its route to the destination.
h. Traceroute most commonly uses Internet Control Message Protocol (ICMP) echo packets with variable time to live (TTL) values. The response time of each hop is calculated. To guarantee accuracy, each hop is queried multiple times (usually three times) to better measure the response of that particular hop. Traceroute uses ICMP messages and TTL fields in the IP address header to function. Traceroute tools are typically included as a utility by operating systems such as Windows and Unix. Traceroute utilities based on TCP are also available.
i. Traceroute is a useful tool for determining the response delays and routing loops present in a network pathway across packet-switched nodes. It also helps to locate any points of failure encountered while en route to a certain destination.
j. However, on the Internet, Traceroute messages are often blocked by routers in various Autonomous Systems (AS), making Traceroute highly inaccurate in many cases.
k. The Traceroute command sends three packets to the hop and each of the times refers to the time taken by the packet to reach the hop.
l. Syntax: traceroute [options] host_address [pathLength]

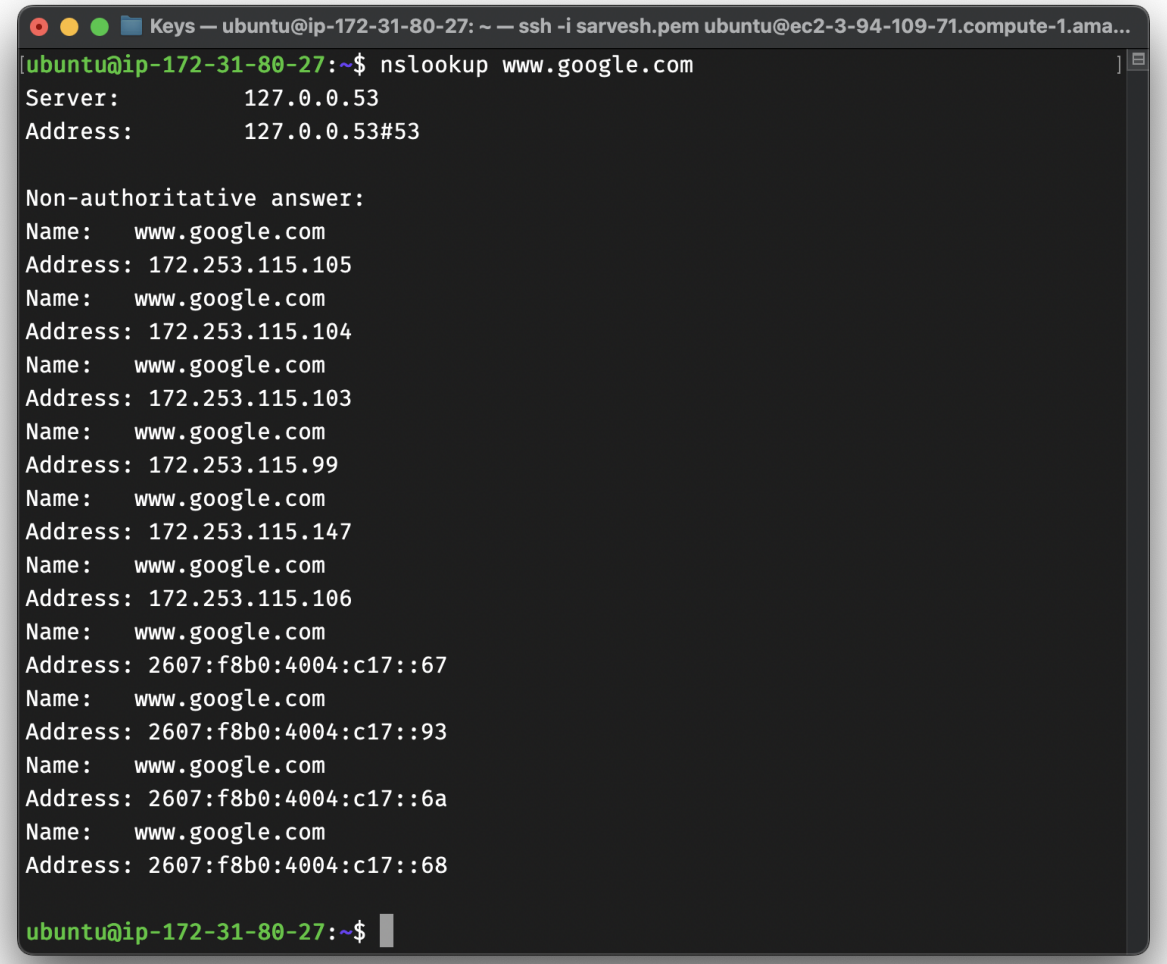


NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

4. nslookup

a. Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The nslookup command-line tool is available only if you have installed the TCP/IP protocol.
b. The nslookup command-line tool has two modes: interactive and non-interactive.
c. If you need to look up only a single piece of data, we recommend using the non-interactive mode. For the first parameter, type the name or IP address of the computer that you want to look up. For the second parameter, type the name or IP address of a DNS name server. If you omit the second argument, nslookup uses the default DNS name server.
d. Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from a DNS server.
e. NsLookup queries the specified DNS server and retrieves the requested records that are associated with the domain name you provided. These records contain information like the domain name’s IP addresses.
f. 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.
g. It is also used to troubleshoot DNS-related problems.
h. nslookup followed by the domain name will display the “A Record” (IP Address) of the domain.
i. Use this command to find the address record for a domain. It queries domain name servers and gets the details.
j. nslookup is the name of a program that lets an Internet server administrator or any computer user enter a hostname (for example, "whatis.com") and find out the corresponding IP address or domain name system (DNS) record. The user can also enter a command for it to do a reverse DNS lookup and find the hostname for an IP address that is specified.
k. You can also do the reverse DNS look-up by providing the IP Address as an argument to nslookup.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52



CONCLUSION:
Thus all the given commands were studied and implemented.