**Practical No : 7** Name : Roshan Naicker

**Network reconnaissance tool.**  Roll No : 5021137

**Aim:** Execute network reconnaissance tools like WHOIS, traceroute, nslookup to gather information about networks and domain registrars.

**Objectives:** To know how to gather information about the networks by using different n/w

reconnaissance tools.

**Course outcome:** CO3

**Theory:**

Reconnaissance is a process of gathering information about a system to identify vulnerabilities. Originally an ethical hacking technique, it allowed network owners to better secure their systems after identifying their security loopholes. Reconnaissance generally follows seven steps:

* Collect initial information
* Determine the network range
* Identify active machines
* Find access points and open ports
* Fingerprint the operating system
* Discover services on ports
* Map the network

Reconnaissance generally follows seven steps:

* Collect initial information
* Determine the network range
* Identify active machines
* Find access points and open ports
* Fingerprint the operating system
* Discover services on ports
* Map the network

One of the most common techniques involved with reconnaissance is port scanning, which sends data to various TCP and UDP (user datagram protocol) ports on a device and evaluates the response. Over the years, reconnaissance has grown from an ethical hacking procedure to a cyberattack mechanism. A reconnaissance attack is a process whereby a hacker plays the role of an undercover detective to fish for information about their target systems and then use that information to identify vulnerabilities ahead of their attacks.

**Types of Reconnaissance Attacks**

There are two types of reconnaissance attacks: active and passive.

* **Active Reconnaissance**

In active reconnaissance, the attacker engages with the target actively. They communicate with you just to get information about your system. Active reconnaissance is quite effective as it gives the attacker valuable information about your system.

The following are active reconnaissance techniques:

1. **Social Engineering**

Social engineering is a process where a cyber threat actor manipulates targets to reveal confidential information to them. They may contact you online via instant chats, emails, and other interactive means to build a connection with you. Once they win you over, they will make you divulge sensitive information about your system or lure you to open a malware-infected file that will compromise your network.

1. **Active Footprinting**

Active footprinting is a method that involves an intruder taking deliberate steps to gather information about your system, its security infrastructure and user engagement. They retrieve your IP addresses, active email addresses, domain name system (DNS) information, etc. Active footprinting can be automated.

1. **Port Scanning**

Ports are areas through which information passes from one computer program or device to another. In port scanning, the threat actor scans the ports within your network to identify the open ones. They use a port scanner to detect the active services on your network such as the hosts and IP addresses and then break in through the open ports.

## **Passive Reconnaissance**

In passive reconnaissance, the attacker doesn’t engage with you or your system directly. They do their investigation from a distance, monitoring the traffic and the interactions on your network. A threat actor in passive reconnaissance turns to public platforms such as search engines and online repositories for information about your system.

Passive reconnaissance strategies include the following:.

1. **Open Source Intelligence**

Open source intelligence (OSINT), refers to the gathering and analysis of data from public locations. People and networks spread their information across the web either intentionally or unintentionally. A reconnaissance actor could use OSINT to retrieve valuable information about your system.

### **Passive Footprinting**

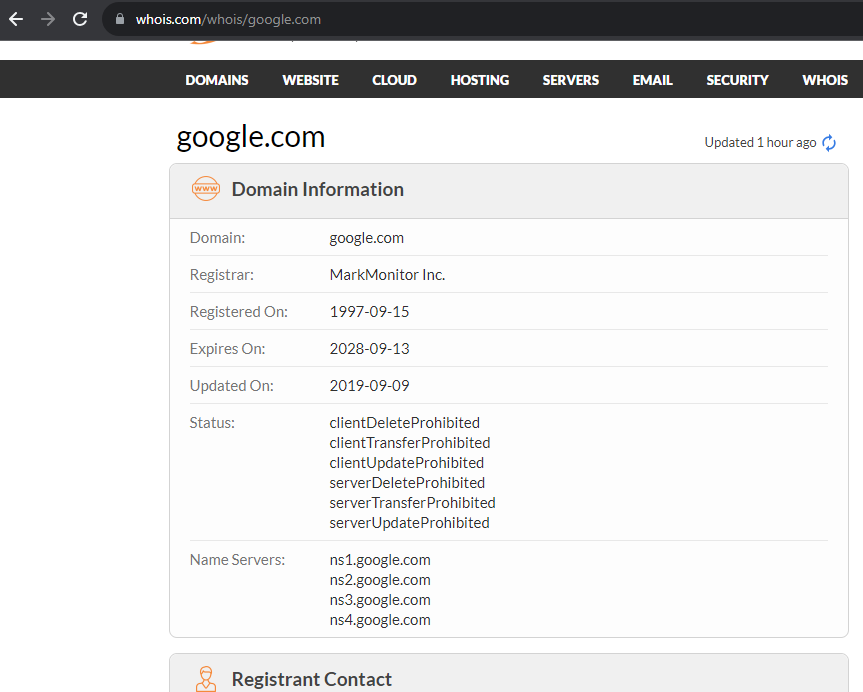
Footprinting is a technique for gathering information about a target. But in this case, the activities are passive, meaning there’s no direct interaction or engagement. The attacker does their investigation from afar, checking you out on search engines, social media, and other online repositories.To get concrete information from passive footprinting, an attacker doesn’t only rely on popular platforms like search engines and social media. They use tools like Wireshark and Shodan to get additional information that may not be available on popular platforms.

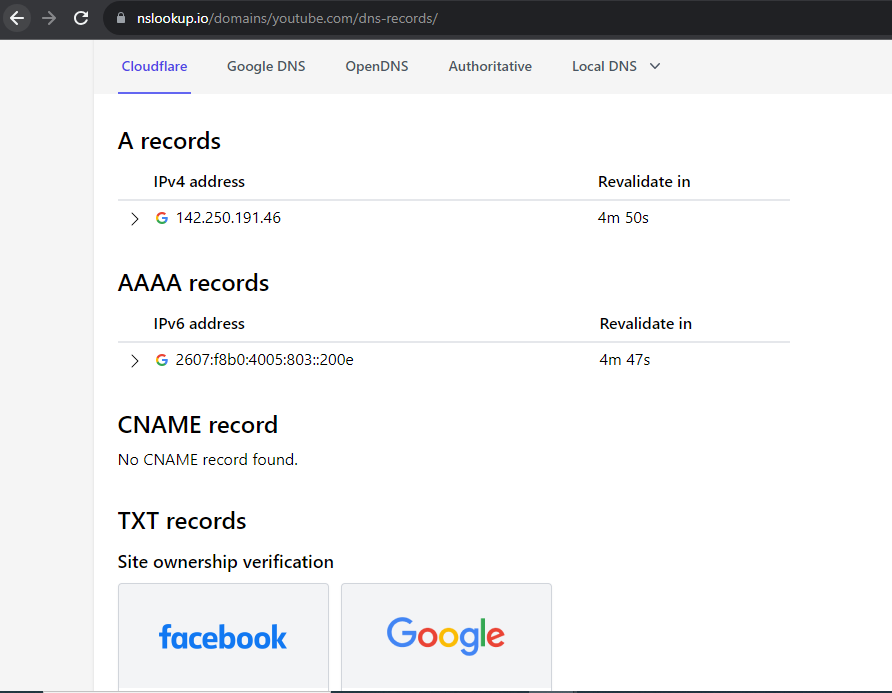
**Network reconnaissance tools**

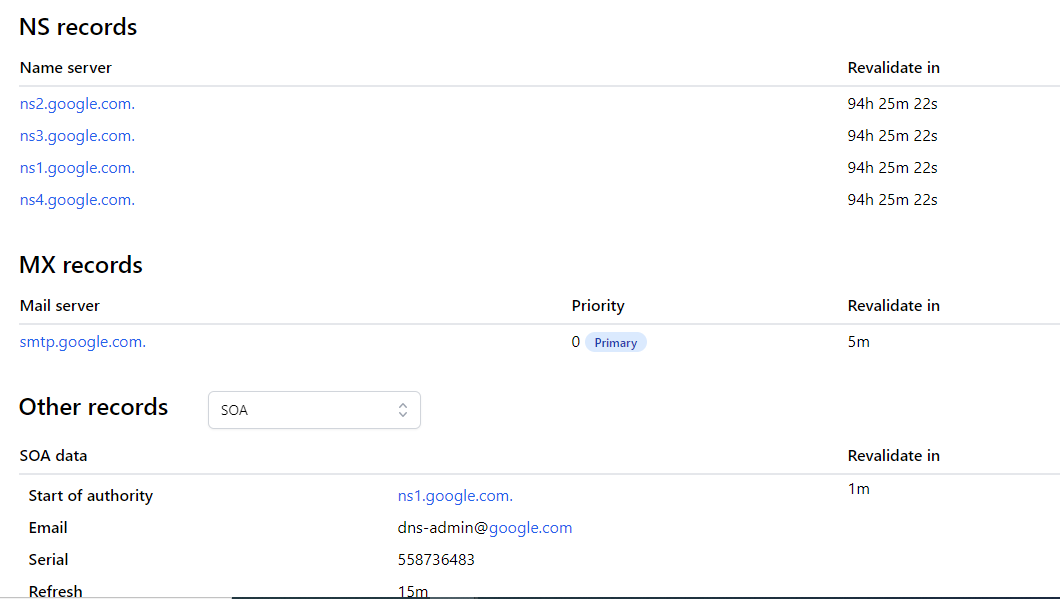
Network reconnaissance tools are used to gather information about target networks, devices, and services. They assist in assessing the security posture of a network, identifying vulnerabilities, and making informed decisions for network management and cybersecurity. Here are some commonly used network reconnaissance tools:

* **Nmap (Network Mapper):** A versatile and powerful open-source tool for network discovery and scanning. It can perform host discovery, port scanning, version detection, and more.
* **Wireshark:** A popular packet analyzer that captures and analyzes network traffic. It helps understand the communication patterns and potentially identify vulnerabilities
* A **WHOIS** tool is a software or online service that provides information about domain names and their registered owners. The WHOIS database contains details about domain registrations, including the domain's creation and expiration dates, registrant contact information, name servers, and more. WHOIS tools are commonly used for domain research, troubleshooting, and cybersecurity purposes.
* **NSlookup (Name Server lookup)** is a command-line tool and network utility used to query the Domain Name System (DNS) to obtain information about domain names, IP addresses, and DNS records. It's available on most operating systems, including Windows, macOS, and Linux. NSlookup is particularly helpful for troubleshooting DNS-related issues, checking DNS records, and verifying DNS configurations

**Results:**







**Conclusion:** Various reconnaissance tools are studied and executed and used to gather primary network information.