INFORMATION GATHERING REPORT

(Ethical Hacking)

Information Gathering Challenge

Organized By

Inlighn Tech

Prepared By

Name : S Sudharna

Intern ID : ITID5418

Course / Program : Ethical Hacking Intern

Company : InLighnX Global Pvt. Ltd.

Submission Date

Date:15.12.2025

ABSTRACT

Information gathering is the foundational phase of ethical hacking and cybersecurity assessment. It involves the systematic collection of publicly available information about a target without performing any unauthorized or intrusive actions. This project focuses on conducting an ethical information gathering exercise on Google (google.com) using passive reconnaissance and legal active techniques.

The objective of this study is to analyze the publicly accessible domain, network, and technological infrastructure of Google while strictly adhering to ethical hacking guidelines. Various industry-standard tools and Open Source Intelligence (OSINT) techniques were employed to collect information related to domain details, DNS records, hosting infrastructure, subdomains, technologies in use, open ports, and public digital presence.

The results indicate that Google follows strong security practices, including secure DNS configurations, restricted port exposure, extensive use of encryption, and advanced firewall protections. Most reconnaissance attempts revealed only intentionally public information, demonstrating Google's minimal attack surface and robust defense-in-depth strategy.

This project highlights the importance of information gathering in understanding an organization's security posture and emphasizes how effective security controls can significantly limit information leakage. The study was conducted solely for educational purposes and within legal and ethical boundaries.

Information Gathering on a Target – Overview

Target: Google (google.com)

1.Target Overview

Target Organization : Google LLC

Target Domain : google.com

Industry : Technology / Internet Services

Parent Company : Alphabet Inc.

Google is a multinational technology company providing search engine services, cloud computing, advertising platforms, and software products. Due to its global infrastructure, only passive and legal reconnaissance is permitted.

2.Objective

The objective of this information gathering exercise is to collect publicly available information related to Google's domain and infrastructure using ethical and legal reconnaissance techniques, without attempting any exploitation, intrusion, or unauthorized access.

The main objectives of this project are:

- To collect maximum publicly available information about the given target

- To understand the target's domain, hosting environment, and network structure
- To identify subdomains, DNS records, and technologies used by the target
- To perform passive and limited legal active reconnaissance within ethical boundaries
- To analyze the collected data to understand the target's security posture
- To document all findings in a clear, structured, and professional manner

3.**Scope and Ethical Compliance**

The scope of this information gathering project is defined to ensure ethical conduct and legal compliance throughout the assessment. The activities performed in this project strictly follow responsible cybersecurity practices.

- The key aspects of the scope and ethical compliance are:
- To perform passive reconnaissance without directly interacting with the target systems
- To conduct legal and limited active scanning in a non-intrusive manner
- To use only Open Source Intelligence (OSINT) and publicly accessible data
- To avoid any form of exploitation or vulnerability testing
- To ensure no brute-force attacks are attempted on any service
- To refrain from bypass attempts involving authentication, authorization, or security controls

- To comply with ethical hacking standards and legal guidelines at all stages of the project

4. Basic Information Gathering

Basic information gathering is the initial step in the reconnaissance process. In this phase, publicly available details about the target domain and its ownership are collected in order to understand the overall structure, administrative control, and security posture of the target.

4.1 Domain Information

Domain information provides essential details related to the identity, registration, and management of the target domain.

Domain Name : google.com
Top-Level Domain (TLD) : .com
Organization : Google LLC
Registrar : MarkMonitor Inc.

Google operates on a highly distributed and secure DNS infrastructure that is frequently updated to ensure high availability, scalability, and protection against domain-based attacks.

4.2 WHOIS Information

WHOIS analysis was performed to collect publicly available domain registration and administrative details.
Tool Used:
whois

Command Executed
whois google.com

Information Identified

Registrar : MarkMonitor Inc.
Organization : Google LLC
Domain Status: Client Transfer Prohibited
Name Servers : Multiple Google-managed name servers

WHOIS privacy and protection mechanisms are enabled, indicating strong domain security practices and preventing unauthorized access to sensitive registration and contact information.

Detailed Domain Registration Information

Domain : google.com
Registered On : 1997-09-15
Expires On : 2028-09-14
Updated On : 2019-09-09

Domain Status:
client delete prohibited
client transfer prohibited
client update prohibited
server delete prohibited
server transfer prohibited
server update prohibited
These status flags collectively protect the domain from unauthorized deletion, transfer, or modification.

Name Servers
ns1.google.com
ns2.google.com
ns3.google.com

ns4.google.com

The use of multiple name servers ensures redundancy, fault tolerance, and resilience against DNS failures or attacks.

Registrar Information
Registrar :MarkMonitor Inc.
IANA ID : 292

Registrar Contact Email:
https://www.markmonitor.com/contact-us/

Abuse Email:
abusecomplaints@markmonitor.com

Abuse Phone:
+1.2086851750

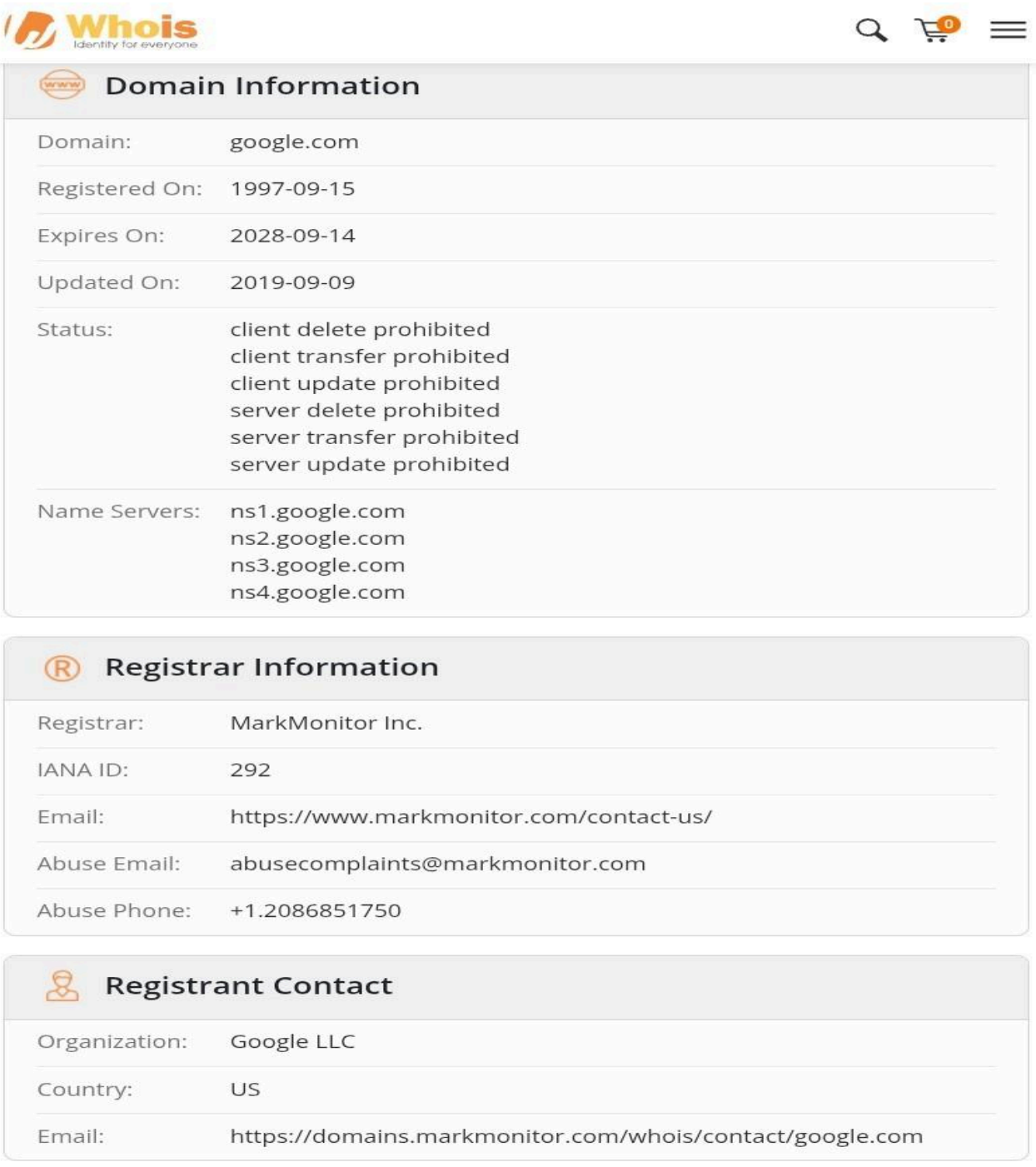
Registrant Contact Information

Organization:Google LLC
Country:United States (US)

Registrant Contact Email:
https://domains.markmonitor.com/whois/contact/google.com

Technical Contact Information
Technical Contact Email:
https://domains.markmonitor.com/whois/contact/google.com

Direct email addresses are masked using secure contact URLs, indicating the use of WHOIS privacy protection to reduce exposure to spam, phishing, and social engineering attacks.



5.Hosting Provider and Location

This section identifies the hosting environment and geographical distribution of the target infrastructure.

Hosting Provider:
Google Cloud Infrastructure

IP Distribution:
Global (Anycast-based)

Data Centers:
Worldwide (United States, Europe, Asia)

Google uses Anycast routing, a network addressing and routing methodology in which the same IP address is advertised from multiple geographical locations. As a result, user requests are automatically routed to the nearest or best-performing data center based on geographic location and network conditions. This approach improves performance, availability, scalability, and resistance to Distributed Denial-of-Service (DDoS) attacks.

6. DNS Information Analysis

Tools Used:

nslookup google.com
dig google.com

DNS Records Identified:

- A Records: Multiple rotating IP addresses

- MX Records: Google Mail Servers (aspmx.l.google.com)
- NS Records: Google-controlled name servers
- TXT Records: SPF, DKIM, DMARC for email security

Zone Transfer Attempt:

❌ Not allowed (secured DNS configuration)

7. Subdomain Enumeration

Tools Used:

subfinder
amass
assetfinder

Publicly Known Subdomains:

mail.google.com
maps.google.com
drive.google.com
accounts.google.com
cloud.google.com
> Google uses a very large subdomain ecosystem, many of which are intentionally public-facing.

8. Technology Fingerprinting

Tools Used:

whatweb
Wappalyzer
BuiltWith

Identified Technologies:

Web Server: Google Frontend (GFE)
Programming Languages: C++, Java, Go, Python
JavaScript Frameworks: Internal Google frameworks
CDN: Google Global Load Balancer
Security Headers: Strongly implemented

Google hides most backend technologies to reduce fingerprinting risks.

9. Directory and File Discovery

Tools Used:
dirsearch
gobuster
Result:
No sensitive directories exposed.

> Google actively blocks directory enumeration and uses advanced rate limiting and WAF protections.

10. Open Ports and Services

Tool Used:

nmap google.com

Observed Open Ports:

Port	Service
80	HTTP (Redirects to HTTPS)
443	HTTPS

All other ports are filtered or blocked by firewalls.

11. Email Harvesting

Tools Used:

theHarvester
Google Dorking

Findings:
Public emails are limited
Uses role-based emails (support@, press@)
Strong protection against email scraping

12. Google Dorking

Sample dorks used without accessing sensitive content:

site:google.com filetype:pdf
site:google.com intitle:"privacy"
site:google.com inurl:careers

Purpose:
To locate public documentation, policies, and career pages.

13. OSINT & Social Media Presence

Platforms:

LinkedIn
Twitter (X)
YouTube
GitHub

Findings:

- Employee roles publicly listed
- Open-source projects on GitHub
- Public blogs revealing technology trends

14. Security Observations

- Strong DNS security
- Strict firewall rules
- No zone transfer allowed
- Minimal attack surface exposure

- Heavy use of encryption and load balancing

15. Conclusion

This information gathering exercise demonstrates that Google has one of the most secure and well-architected infrastructures in the world. Even with advanced reconnaissance tools, only limited publicly intended information is available.

The exercise highlights the importance of:

- Defense-in-depth
- DNS security
- Attack surface reduction