



# REPORT

INFORMATION GATHERING





## IP Address Resolution

Resolved IP Address: 142.250.77.164

## WHOIS Lookup

### Domain Information

-----

- Domain Name: google.com
- Registrar: MarkMonitor, Inc.
- Registrar IANA ID: 292
- Creation Date: 1997-09-15T07:00:00+0000
- Last Updated: 2024-08-02T02:17:33+0000
- Expiration Date: 2028-09-13T07:00:00+0000

- Domain Statuses: clientUpdateProhibited clientTransferProhibited

clientDeleteProhibited serverUpdateProhibited serverTransferProhibited

serverDeleteProhibited

### Registrant Information

-----

- Name: Not Available
- Organization: Google LLC
- Address: Not Available
- City: Not Available
- State: CA
- Postal Code: Not Available
- Country: UNITED STATES





- Phone: Not Available
- Fax: Not Available
- Email: Not Available

#### Administrative Contact

-----

- Name: Not Available
- Organization: Google LLC
- State: CA
- Country: UNITED STATES

#### Technical Contact

-----

- Name: Not Available
- Organization: Google LLC
- State: CA
- Country: UNITED STATES

#### Name Servers

-----

- ns2.google.com, ns1.google.com, ns4.google.com, ns3.google.com

#### Additional Information

-----





- Domain Protection: The domain is safeguarded under multiple prohibitive statuses.

## InternetDB Information

InternetDB Information for IP: 142.250.77.164

Open Ports:

- 80
- 443

CPEs:

Hostnames:

- maa05s17-in-f4.1e100.net

Tags:

- self-signed

Vulnerabilities: None

## Geolocation Lookup

IP Information

-----

- IP: 142.250.77.164
- Hostname: maa05s17-in-f4.1e100.net
- City: Chennai
- Region: Tamil Nadu
- Country: IN
- Location: 13.0878,80.2785
- Organization: AS15169 Google LLC
- Postal: 600001





- Timezone: Asia/Kolkata

## Shodan Information

Shodan Information for IP: 142.250.77.164

Organization: Google LLC

Operating System: None

ISP: Google LLC

Country: India

City: Chennai

Latitude: 13.08784

Longitude: 80.27847

Open Ports:

Port: 80

Service: N/A

Version: N/A

Banner: HTTP/1.1 301 Moved Permanently

Location: <http://www.google.com/>

Content-Type: text/html; charset=UTF-8

Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-jwa7H8HCg5wF\_wdfYeMJig' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp

Permissions-Policy: unload=()

Date: Sun, 25 Aug 2024 03:35:47 GMT

Expires: Tue, 24 Sep 2024 03:35:47 GMT





Cache-Control: public, max-age=2592000

Server: gws

Content-Length: 219

X-XSS-Protection: 0

X-Frame-Options: SAMEORIGIN

-----  
Port: 443

Service: N/A

Version: N/A

Banner: HTTP/1.1 301 Moved Permanently

Location: <http://www.google.com/>

Content-Type: text/html; charset=UTF-8

Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src  
'nonce-k0HJSJvxJnR6Y5WnDGQjhnw' 'strict-dynamic' 'report-sample' 'unsafe-eval'  
'unsafe-inline' https: http;;report-uri https://csp.withgoogle.com/csp/gws/other-hp

Cross-Origin-Opener-Policy: same-origin-allow-popups; report-to="gws"

Report-To:

{"group":"gws","max\_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gws/other"}]}

Permissions-Policy: unload=()

Date: Mon, 26 Aug 2024 17:16:29 GMT

Expires: Wed, 25 Sep 2024 17:16:29 GMT





Cache-Control: public, max-age=2592000

Server: gws

Content-Length: 219

X-XSS-Protection: 0

X-Frame-Options: SAMEORIGIN

Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

-----

## Nmap Scan

Starting Nmap 7.95 ( <https://nmap.org> ) at 2024-08-27 12:59 India Standard Time

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

| After NULL UDP avahi packet DoS (CVE-2011-1002).

|\_ Hosts are all up (not vulnerable).

Nmap scan report for maa05s17-in-f4.1e100.net (142.250.77.164)

Host is up (0.025s latency).

PORT	STATE	SERVICE
------	-------	---------

21/tcp	filtered	ftp
--------	----------	-----

22/tcp	filtered	ssh
--------	----------	-----





23/tcp filtered telnet

25/tcp filtered smtp

80/tcp open http

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|\_http-dombased-xss: Couldn't find any DOM based XSS.

|\_http-csrf: Couldn't find any CSRF vulnerabilities.

110/tcp filtered pop3

139/tcp filtered netbios-ssn

443/tcp open https

|\_http-csrf: Couldn't find any CSRF vulnerabilities.

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|\_http-dombased-xss: Couldn't find any DOM based XSS.

445/tcp filtered microsoft-ds

3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 636.82 seconds

## Conclusion

-----

No critical vulnerabilities were detected in the Nmap scan, but regular scans are advised to ensure ongoing security. Shodan identified 2 open ports, which could serve as potential entry points for attackers. It is recommended to review these open ports and secure or close them if they are not needed. Disabling unnecessary services can minimize







exposure to threats. WHOIS lookup provided detailed information about the domain ownership. This information can be used to understand the entity behind the domain and assess potential risks associated with it. The IP is located in IN, which could indicate the origin of the services and provide insights into potential regional threats. The system is detected as vulnerable. Immediate action is advised to mitigate the identified risks.

