REPORT

INFORMATION GATHERING

IP Address Resolution

Resolved IP Address: 157.240.192.18

WHOIS Lookup

Domain Information

  Domain Name: meta.com

  Registrar: RegistrarSafe, LLC

  Registrar IANA ID: 3237

  Creation Date: 1991-01-21T05:00:00Z

  Last Updated: 2024-01-24T20:05:49Z

  Expiration Date: 2033-01-22T05:00:00Z

          Domain   Statuses: clientDeleteProhibited   clientTransferProhibited

clientUpdateProhibited   serverDeleteProhibited   serverTransferProhibited

serverUpdateProhibited

  Registrant Information

  Name: Domain Admin

  Organization: Meta Platforms, Inc.

  Address: 1601 Willow Rd

  City: Menlo Park

  State: CA

  Postal Code: 94025

  Country: UNITED STATES

Phone: 16505434800

Fax: Not Available

Email: domain@fb.com

Administrative Contact

Name: Domain Admin

Organization: Meta Platforms, Inc.

State: CA

Country: UNITED STATES

Technical Contact

Name: Domain Admin

Organization: Meta Platforms, Inc.

State: CA

Country: UNITED STATES

Name Servers

D.NS.FACEBOOK.COM, A.NS.FACEBOOK.COM, C.NS.FACEBOOK.COM, B.NS.FACEBOOK.COM

Additional Information

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

InternetDB Information

InternetDB Information for IP: 157.240.192.18

Open Ports:

  80   443CPEs:

Hostnames:

  edge-star-shv-02-maa2.facebook.com

  facebook.com

  messenger.com

Tags:

Vulnerabilities: None

Geolocation Lookup

IP Information

 IP: 157.240.192.18

 Hostname: edge-star-shv-02-maa2.facebook.com

 City: Chennai

 Region: Tamil Nadu

 Country: IN

 Location: 13.0878,80.2785

 Organization: AS32934 Facebook, Inc.

 Postal: 600001

Timezone: Asia/Kolkata

Shodan Information

Shodan Information for IP: 157.240.192.18

Organization: Facebook, Inc.

Operating System: None

ISP: Facebook, Inc.

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: https://157.240.192.18/

Content-Type: text/plain

Server: proxygen-bolt

Date: Tue, 27 Aug 2024 02:38:56 GMT

Connection: keep-alive

Content-Length: 0

Port: 443

Service: N/A

Version: N/A

Banner: HTTP/1.1 400 Bad Request

Vary: Accept-Encoding

Content-Type: text/html; charset="utf-8"

X-FB-Debug:

lO0Hj1dbN2WxpqwXQbuUAr6O3lnZiIN88xGt14vkOTi+4xFZe5r1NedxEFByp8nQeNfiXuK

QJo/32o3ljGXsuA==

Date: Tue, 27 Aug 2024 02:39:00 GMT

Proxy-Status: http_request_error;

e_proxy="AcKEE_X_iUpkgfwFEdk-o2yksU6ow-Z_3JuVQN_fYYVxfrsGczwgHg70givepA4

wawK77bisxRKiX7zGkbh6";

e_fb_binaryversion="AcIY3CHGGc1akgz89OLeRwUsVHqtjvwsv-tqkknl-Hl2PCfQ5f9dGVJ

VJZUKA1mPzVSz1cEzRnpHGRA4dke2TC-MhlafQcPba6g";

e_fb_httpversion="AcJJJfGWY3g2ROsKqf3HrZvobocguDhdsVGmtQIhnAzxl4JORD31Zfl

8W_MY";

e_fb_responsebytes="AcI9bmmeQrwdhIQuZdSfrEB6ixyW5b2kSQdJpknVXwJFNd3p7oP

M-ZrUPNenfQ";

e_fb_requesttime="AcKBswmGgmkXylDz0k-g7I4OSQ3GdYcLLo5vhdBWTjpwFYmBcsqZ

XjiNMHfrXfchXF-m5ZzyRg";

e_fb_requesthandler="AcLa113yraEBmDc11GjphIg0tUMTJSGpz_sp16DPuLcI3ZRYriW4

o5mwsKuMl1bH__qMk4bP5sl";

e_fb_hostheader="AcI8wzQANvOFhyMI8r9Vy9-qTUlnzrNnUnKdvGke0yxAVA3oRVS11S
BD-tADoiudmTP3alvKxTU";

e_fb_requestsequencenumber="AcIcljM2Pj_A_T-z1ESprx3xlRgSDWrIB3ilb8J4btaJcWN-
mnQaW63B4Vn1";

e_upip="AcIls2thGoMBXl-jrWuo8WeExEB85NJA_idRr4cPLY836ttKHA_dq-mcxILC8hfBC
KnMwSe46oI5PXmRXR4KuIimDgv_rkb0sKOttdw";

e_fb_builduser="AcKUrlfGn8-xDP3i7orP7NXthPHbe0_-jBylqAVr0zIM2h7wVujdhPhxi13P
18dzXkQ";

e_fb_vipport="AcIZLpSW3rJ1nqmd2G6s1RXxSKEsJb6mDZYC5gY7XJLNZs7joX-FB81B
XpCY";

e_clientaddr="AcIUC65eDeWke2XntzGsrGiOvHUSvP1dXw5ZMF8mp-UKLzIbXngxiSZfJ
1J6l6h3mrPr2dNTAZ1Go2EPula28XqCQWYR2J2bJeVNSLfWXoYuyLh-EA";

e_fb_vipaddr="AcLjQxaZxFkhLZ6dl5ompxsZRh3sjTi5h0iUi8J1f5cVZ9prrXXj-XrYrDjRAcr
A5l0RifzIBFuB8RfkMJqiQPt5v-tja-ty6w";

e_fb_configversion="AcLerGns2pcOw7K1efmt1U3dS-2WqtfkXjZXXFQ3QZIssrPip3xyHIY
vOHprEg",   http_request_error;

e_proxy="AcJQaUf2DcTkS7fSmP0AVO-3eQOWfymQ8MNLrHALBVoRwZ1vG4LARIAnz
9YF-MjfMrOl9oZlu8rdLwA";

e_fb_binaryversion="AcKo3tjGVDR_zbAPpzOoOwHf3N8ujsJ70mvH6akE95R7zHpRsSW
9Gv5dSs28ZZN9uKi8mI48t7k7FMahqpKBB1IVO-j8eLSOimc";

e_fb_httpversion="AcI4NS8QYuO2_0GURrluRSO_P5Gn9L4xlDTa-S-zZsJOXUKztBEjjpd
Z3N2k";

e_fb_responsebytes="AcJq7rAL71NEWrkWQDXha7Yu22cYkdEKQ5sTwv9ECIantz5CB1
kJR4V9TafTZg";

e_fb_requesttime="AcJEDh0RN50GqbikxYvTOJhqiRe1VqpAHenmZ7URq82zxtyXqEPl-x xifwipbiDrQpYr3emX8w";

e_fb_requesthandler="AcIQ2XaWy38Kh_9xxfGIY8W0rsEplcE5iH_SjOTn8SeV0Ta0ZNt9 MM9hXSQinR2idw_yNkFkG_Sd3sZLk1rdje7D";

e_fb_hostheader="AcLIXdHTf4yzVwbjeIIzeIh4ana9Ycac8Wdn3s7DeoRK3yNDXbqXE_fA kfv-975Iph6miBWIuJ4";

e_fb_requestsequencenumber="AcLaf527pH-qBF9uKB69vv1rBSb4fCMAmmZx0140Hy_ VCfvD_xi_umHqBw";

e_upip="AcI6XHPofxjpSvfF6SViQ_tLpnjjmoGqByqEyNDV8T6jktcYu9QWSErz0-fTRBkfu4 XooOcjgJHyfgQOz3BLk89qqdScwFn3qQ";

e_fb_builduser="AcJLGEqrY8rFXMT6liN9yMopqrUG8E3nfj5beFHBUiICdrpWABFJ1p-8Lf 6hIRV4H5Y";

e_fb_vipport="AcJ1SzziOka_Jp_WNd11QGJlsHsQrV8WIzso-qHWS_nNRCK1DmasinaC uquS";

e_clientaddr="AcLI4dnDPx0-UXakKy9KgF3AfRRExVuDtq3tWj1zvmE9BTHVl9GMSuPT6 2gaEunkLz0HZvSbujR94__DH_g";

e_fb_vipaddr="AcJem3tS196erWBOVmGNPYLFIR4AmPu6LUCtNj1ZnuPSROqKfOTGV 0iNrk_mTEomXJFJZQIbMUA";

e_fb_configversion="AcJz_fpFfcNTVNVgtx2Gr8CTJ5l6ZOeV39QCvysoY6AoEovOoHIE7 YIxJM5DBQ"

X-FB-Connection-Quality: MODERATE; q=0.3, rtt=178, rtx=0, c=10, mss=1380, tbw=3223, tp=-1, tpl=-1, uplat=231, ullat=0

Alt-Svc: h3=":443"; ma=86400

Connection: keep-alive

Content-Length: 1542

Nmap Scan

Starting Nmap 7.95 (https://nmap.org) at 2024-08-28 13:07 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 edge-star-shv-02-maa2.facebook.com (157.240.192.18)

Host is up (0.028s latency).

PORT   STATE   SERVICE

21/tcp   filtered ftp

22/tcp   filtered ssh

23/tcp   filtered telnet

25/tcp   filtered smtp

53/tcp   filtered domain

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

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

143/tcp filtered imap

443/tcp open   https

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

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

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

445/tcp filtered microsoft-ds

3306/tcp filtered mysql

3389/tcp filtered ms-wbt-server

8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 104.10 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.No vulnerabilities were detected . Consider using other tools or methods, as our scan did not find any issues.