REPORT

INFORMATION GATHERING

IP Address Resolution

Resolved IP Address: 104.16.103.112

WHOIS Lookup

Domain Information

- Domain Name: canva.com

- Registrar: GANDI SAS

- Registrar IANA ID: 81

- Creation Date: 2001-05-04T22:03:52Z

- Last Updated: 2024-05-17T07:26:12Z

- Expiration Date: 2025-05-05T00:03:52Z

- Domain Statuses: clientTransferProhibited

Registrant Information

- Name: REDACTED FOR PRIVACY

- Organization: Canva Pty. Ltd.

- Address: REDACTED FOR PRIVACY

- City: REDACTED FOR PRIVACY

- State: New South Wales

- Postal Code: REDACTED FOR PRIVACY

- Country: AUSTRALIA

- Phone: Not Available

- Fax: Not Available

- Email: 7bd96a5bc65905fe8dd1f642d591b0b7-12873969@contact.gandi.net

Administrative Contact

- Name: REDACTED FOR PRIVACY

- Organization: REDACTED FOR PRIVACY

- State: REDACTED FOR PRIVACY

- Country: REDACTED FOR PRIVACY

Technical Contact

- Name: REDACTED FOR PRIVACY

- Organization: REDACTED FOR PRIVACY

- State: REDACTED FOR PRIVACY

- Country: REDACTED FOR PRIVACY

Name Servers

- NS1.CANVA.COM, NS2.CANVA.COM

Additional Information

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

InternetDB Information

InternetDB Information for IP: 104.16.103.112

Open Ports:

- 80
- 443
- 2052
- 2082
- 2083
- 2086
- 2087
- 2095
- 8080
- 8443
- 8880

CPEs:

Hostnames:

- canva.com

Tags:

- cdn

Vulnerabilities: None

Geolocation Lookup

IP Information

- IP: 104.16.103.112

- Hostname: Not Available

- City: San Francisco

- Region: California

- Country: US

- Location: 37.7621,-122.3971

- Organization: AS13335 Cloudflare, Inc.

- Postal: 94107

- Timezone: America/Los_Angeles

Shodan Information

Shodan Information for IP: 104.16.103.112

Organization: Cloudflare, Inc.

Operating System: None

ISP: Cloudflare, Inc.

Country: United States

City: San Francisco

Latitude: 37.7621

Longitude: -122.3971

Open Ports:

Port: 80

Service: N/A

Version: N/A

Banner: HTTP/1.1 301 Moved Permanently

Date: Tue, 27 Aug 2024 01:46:24 GMT

```
Content-Type: text/html

Content-Length: 167

Connection: keep-alive

Cache-Control: max-age=3600

Expires: Tue, 27 Aug 2024 02:46:24 GMT

Location: https://designschool.canva.com/

Report-To:

{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=FcmQ%2FBheznLk0y%2B

rezEJtlODN2nj8%2BxkJlZjgcAAO%2BfdqYel2n35B1FGHKCYERTYrgU7SXgo%2FQYOt

5tymZhYVJZARH6yecbmigjeW5%2Bq2GtU2mnLbT%2FzOJd789qiWIvw8Xzj7wqIueU%

3D"}],"group":"cf-nel","max_age":604800}

NEL: {"success_fraction":0.01,"report_to":"cf-nel","max_age":604800}

Vary: Accept-Encoding

X-Content-Type-Options: nosniff

Server: cloudflare

CF-RAY: 8b98633f9db97c33-LAX




----------------------------------------

Port: 443

Service: CloudFlare

Version: N/A

Banner: HTTP/1.1 403 Forbidden

Server: cloudflare
```

```
Date: Tue, 27 Aug 2024 04:39:39 GMT

Content-Type: text/html

Content-Length: 553

Connection: keep-alive

CF-RAY: 8b996105395d4244-EWR



----------------------------------------

Port: 2052

Service: N/A

Version: N/A

Banner: HTTP/1.1 403 Forbidden

Date: Fri, 02 Aug 2024 04:26:33 GMT

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

Content-Length: 5895

Connection: close

X-Frame-Options: SAMEORIGIN

Referrer-Policy: same-origin

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Vary: Accept-Encoding

Server: cloudflare

CF-RAY: 8acb4f781b39b963-AMS
```

```
----------------------------------------
Port: 2053
Service: N/A
Version: N/A
Banner: HTTP/1.1 400 Bad Request
Server: cloudflare
Date: Sat, 24 Aug 2024 05:19:45 GMT
Content-Type: text/html
Content-Length: 655
Connection: close
CF-RAY: -


----------------------------------------
Port: 2082
Service: N/A
Version: N/A
Banner: HTTP/1.1 403 Forbidden
Date: Tue, 27 Aug 2024 01:48:29 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5895
Connection: close
```

```
X-Frame-Options: SAMEORIGIN

Referrer-Policy: same-origin

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Vary: Accept-Encoding

Server: cloudflare

CF-RAY: 8b9866493f80176a-SJC



----------------------------------------

Port: 2083

Service: N/A

Version: N/A

Banner: HTTP/1.1 403 Forbidden

Server: cloudflare

Date: Tue, 27 Aug 2024 05:47:59 GMT

Content-Type: text/html

Content-Length: 553

Connection: keep-alive

CF-RAY: 8b99c51fbe50f9ea-SJC



----------------------------------------
```

```
Port: 2086

Service: N/A

Version: N/A

Banner: HTTP/1.1 403 Forbidden

Date: Mon, 26 Aug 2024 17:34:44 GMT

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

Content-Length: 5894

Connection: close

X-Frame-Options: SAMEORIGIN

Referrer-Policy: same-origin

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Vary: Accept-Encoding

Server: cloudflare

CF-RAY: 8b959305694b93f0-LHR



----------------------------------------

Port: 2087

Service: N/A

Version: N/A

Banner: HTTP/1.1 400 Bad Request

Server: cloudflare
```

```
Date: Tue, 27 Aug 2024 03:21:26 GMT
Content-Type: text/html
Content-Length: 155
Connection: close
CF-RAY: -

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>cloudflare</center>
</body>
</html>

----------------------------------------
Port: 2095
Service: N/A
Version: N/A
Banner: HTTP/1.1 403 Forbidden
Date: Wed, 07 Aug 2024 23:14:38 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5895
Connection: close
X-Frame-Options: SAMEORIGIN
```

```
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 8afaf6d08a8a415a-AMS


----------------------------------------
Port: 8080
Service: CloudFlare
Version: N/A
Banner: HTTP/1.1 403 Forbidden
Date: Mon, 26 Aug 2024 15:52:32 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5895
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
```

```
Server: cloudflare

CF-RAY: 8b94fd561be95c1d-SJC




----------------------------------------

Port: 8443

Service: CloudFlare

Version: N/A

Banner: HTTP/1.1 403 Forbidden

Server: cloudflare

Date: Tue, 27 Aug 2024 02:23:14 GMT

Content-Type: text/html

Content-Length: 553

Connection: keep-alive

CF-RAY: 8b9899318dcb9e50-SJC




----------------------------------------

Port: 8880

Service: N/A

Version: N/A

Banner: HTTP/1.1 403 Forbidden

Date: Mon, 26 Aug 2024 16:12:27 GMT

Content-Type: text/plain; charset=UTF-8
```

```
Content-Length: 16
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Server: cloudflare
CF-RAY: 8b951a809b4e2349-SJC

error code: 1003
----------------------------------------
```

Nmap Scan

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-27 13:29 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 104.16.103.112
Host is up (0.019s 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-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS 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 636.67 seconds
```

Conclusion

No critical vulnerabilities were detected in the Nmap scan, but regular scans are advised to ensure ongoing security.Shodan identified 12 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 US, 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.