NMAP Results:

Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-03 17:36 UTC

Nmap scan report for cseds.co (104.21.12.24)

Host is up (0.0017s latency).

Other addresses for cseds.co (not scanned): 172.67.151.81 2606:4700:3033::ac43:9751

2606:4700:3036::6815:c18

Not shown: 996 filtered tcp ports (no-response)

PORT   STATE SERVICE VERSION

80/tcp   open http   Cloudflare http proxy

|_http-server-header: cloudflare

|_http-title: Did not follow redirect to https://cseds.co/

443/tcp open ssl/http Cloudflare http proxy

| ssl-cert: Subject: commonName=cseds.co

| Subject Alternative Name: DNS:cseds.co, DNS:*.cseds.co

| Not valid before: 2024-11-28T22:58:47

|_Not valid after: 2025-02-26T22:58:46

|_http-title: SoIT CSEDS

|_http-server-header: cloudflare

8080/tcp open http   Cloudflare http proxy

|_http-server-header: cloudflare

8443/tcp open ssl/http Cloudflare http proxy

| ssl-cert: Subject: commonName=cseds.co

| Subject Alternative Name: DNS:cseds.co, DNS:*.cseds.co

| Not valid before: 2024-11-28T22:58:47

|_Not valid after: 2025-02-26T22:58:46

|_http-server-header: cloudflare

|_http-title: 400 The plain HTTP request was sent to HTTPS port

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 92.62 seconds

SSLSCAN Results:

Version: [32m2.1.2 [0m

OpenSSL 3.0.13 30 Jan 2024

 [0m

 [32mConnected to 172.67.151.81 [0m

Testing SSL server [32mcseds.co [0m on port [32m443 [0m using SNI name [32mcseds.co [0m

  [1;34mSSL/TLS Protocols: [0m

SSLv2   [32mdisabled [0m

SSLv3   [32mdisabled [0m

TLSv1.0   [33menabled [0m

TLSv1.1   [33menabled [0m

TLSv1.2   enabled

TLSv1.3   [32menabled [0m

  [1;34mTLS Fallback SCSV: [0m

Server [32msupports [0m TLS Fallback SCSV

  [1;34mTLS renegotiation: [0m

 [32mSecure [0m session renegotiation supported

TLS Compression:

OpenSSL version does not support compression

Rebuild with zlib1g-dev package for zlib support

Heartbleed:

TLSv1.3 not vulnerable to heartbleed

TLSv1.2 not vulnerable to heartbleed

TLSv1.1 not vulnerable to heartbleed

TLSv1.0 not vulnerable to heartbleed

Supported Server Cipher(s):

Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253

Accepted TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253

Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253

Preferred TLSv1.2 256 bits ECDHE-ECDSA-CHACHA20-POLY1305 Curve 25519 DHE 253

Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-GCM-SHA256 Curve 25519 DHE 253

Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-SHA Curve 25519 DHE 253

Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-GCM-SHA384 Curve 25519 DHE 253

Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-SHA Curve 25519

DHE 253

Accepted TLSv1.2 [32m128 [0m bits ECDHE-ECDSA-AES128-SHA256   Curve [32m25519 [0m

DHE 253

Accepted TLSv1.2 [32m256 [0m bits ECDHE-ECDSA-AES256-SHA384   Curve [32m25519 [0m

DHE 253

 [32mPreferred [0m [33mTLSv1.1 [0m   [32m128 [0m bits   ECDHE-ECDSA-AES128-SHA

Curve [32m25519 [0m DHE 253

Accepted   [33mTLSv1.1 [0m   [32m256 [0m bits   ECDHE-ECDSA-AES256-SHA   Curve

 [32m25519 [0m DHE 253

 [32mPreferred [0m [33mTLSv1.0 [0m   [32m128 [0m bits   ECDHE-ECDSA-AES128-SHA

Curve [32m25519 [0m DHE 253

Accepted   [33mTLSv1.0 [0m   [32m256 [0m bits   ECDHE-ECDSA-AES256-SHA   Curve

 [32m25519 [0m DHE 253

   [1;34mServer Key Exchange Group(s): [0m

TLSv1.3   [32m128 [0m bits secp256r1 (NIST P-256) [0m

TLSv1.3   [32m192 [0m bits secp384r1 (NIST P-384) [0m

TLSv1.3   [32m260 [0m bits secp521r1 (NIST P-521) [0m

TLSv1.3   [32m128 [0m bits   [32mx25519 [0m

TLSv1.2   [32m128 [0m bits secp256r1 (NIST P-256) [0m

TLSv1.2   [32m192 [0m bits secp384r1 (NIST P-384) [0m

TLSv1.2   [32m260 [0m bits secp521r1 (NIST P-521) [0m

TLSv1.2   [32m128 [0m bits   [32mx25519 [0m

   [1;34mSSL Certificate: [0m

Signature Algorithm: ecdsa-with-SHA256

ECC Curve Name: prime256v1

ECC Key Strength: 128 [0m

Subject: cseds.co

Altnames: DNS:cseds.co, DNS:*.cseds.co

Issuer: WE1

Not valid before: [32mNov 28 22:58:47 2024 GMT [0m

Not valid after: [32mFeb 26 22:58:46 2025 GMT [0m

DIG Results:

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> cseds.co

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33690

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 65494

;; QUESTION SECTION:

;cseds.co.   IN A

;; ANSWER SECTION:

cseds.co. 299 IN A 172.67.151.81

cseds.co. 299 IN A 104.21.12.24

;; Query time: 1 msec

```
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)

;; WHEN: Tue Dec 03 17:37:37 UTC 2024

;; MSG SIZE  rcvd: 69
```