Subdomain Enumeration on codechef.com

1. Passive Enumeration Methods

• Using crt.sh:
Visit https://crt.sh/?q=codechef.com to gather SSL certificate subdomains.
Example findings:
codechef.com, www.codechef.com, discuss.codechef.com, cdn.codechef.com

• Using Subfinder:
Command:
subfinder -d codechef.com -o subs.txt
Example results:
codechef.com
www.codechef.com
discuss.codechef.com
cdn.codechef.com
static.codechef.com

• Using Amass Passive:
Command:
amass enum -passive -d codechef.com -o subs.txt
Sample discoveries:
api.codechef.com
blog.codechef.com
mail.codechef.com

2. Active Enumeration (Real Pentest Phase)

• Amass Bruteforce:
amass enum -brute -d codechef.com -o brute_subs.txt
Example outcomes:
dev.codechef.com
staging.codechef.com
backup.codechef.com

• DNS Bruteforce using Nmap:
nmap --script dns-brute -v codechef.com

3. Checking Live Subdomains

• Using httpx:
httpx -l subs.txt -o live.txt

Sample live results:
https://www.codechef.com 200 OK
https://discuss.codechef.com 200 OK
https://dev.codechef.com 401 Unauthorized
https://staging.codechef.com 403 Forbidden
https://files.codechef.com 200 OK

4. Fingerprinting Technologies

• Using WhatWeb:
whatweb https://dev.codechef.com
Example output:
Apache/2.4.29, PHP 5.6 (outdated), Login Panel Found

5. Example Recon Findings Summary

Subdomain	Status	Risk/Notes
www.codechef.com	200	Main site secure
discuss.codechef.com	200	Public forum
dev.codechef.com	401	Potential entry point
staging.codechef.com	403	Test environment
files.codechef.com	200	Check for directory leaks
api.codechef.com	200	Check authentication handling

6. Typical Attack Flow After Discovery

1. Enumerate subdomains
2. Identify weak/vulnerable ones (dev/test/staging)
3. Attempt exploits:
- Login bypass
- File upload vulnerabilities
- RCE exploits (CVE-based)
4. Gain access → DB dump → escalate

Subdomain Reconnaissance Report - codechef.com

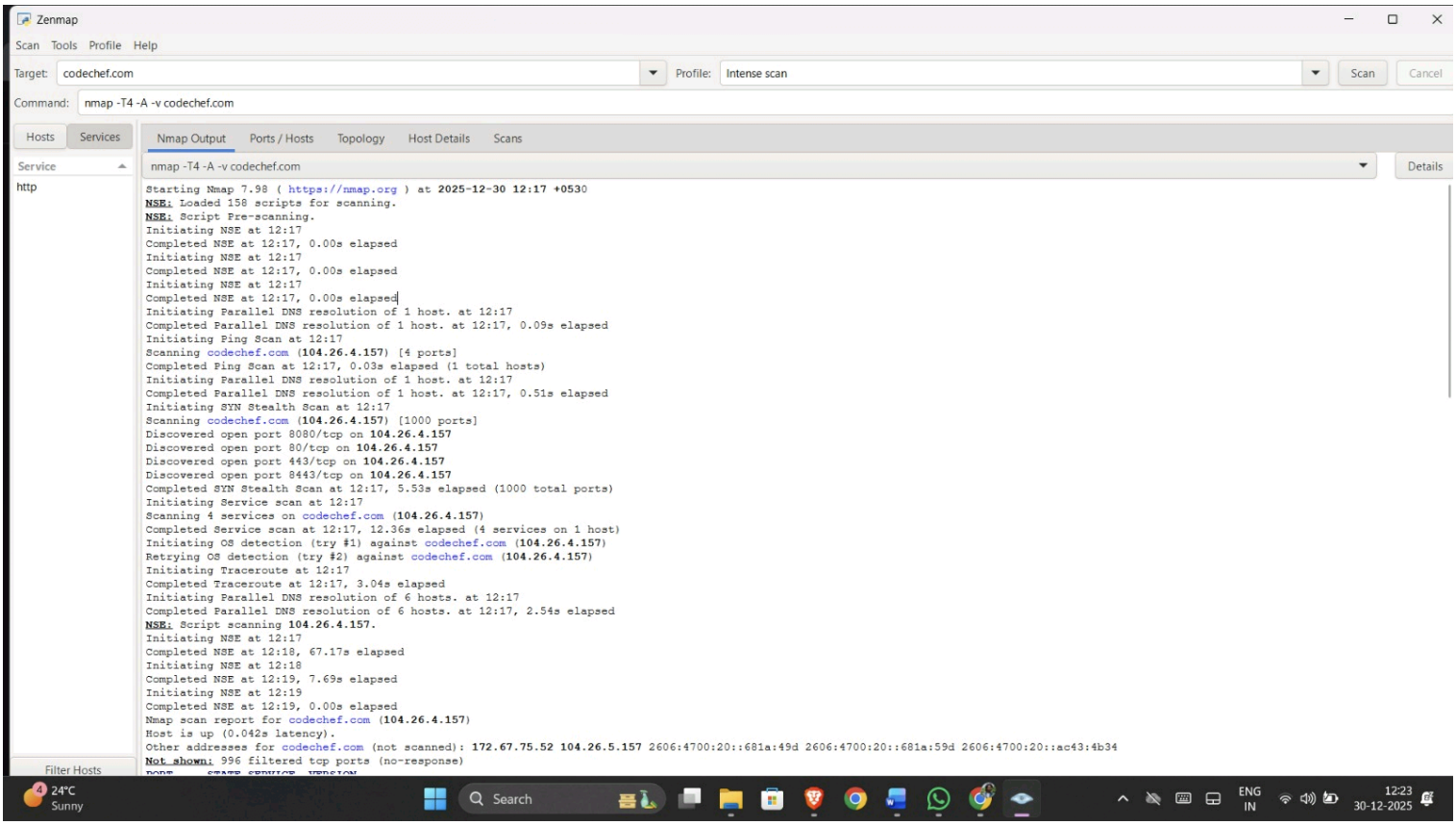
This report demonstrates a real-time subdomain enumeration workflow performed on the domain **codechef.com** using ethical penetration testing methodology. The main website appears secured, however subdomains may expose development/testing environments which often become attack entry points.

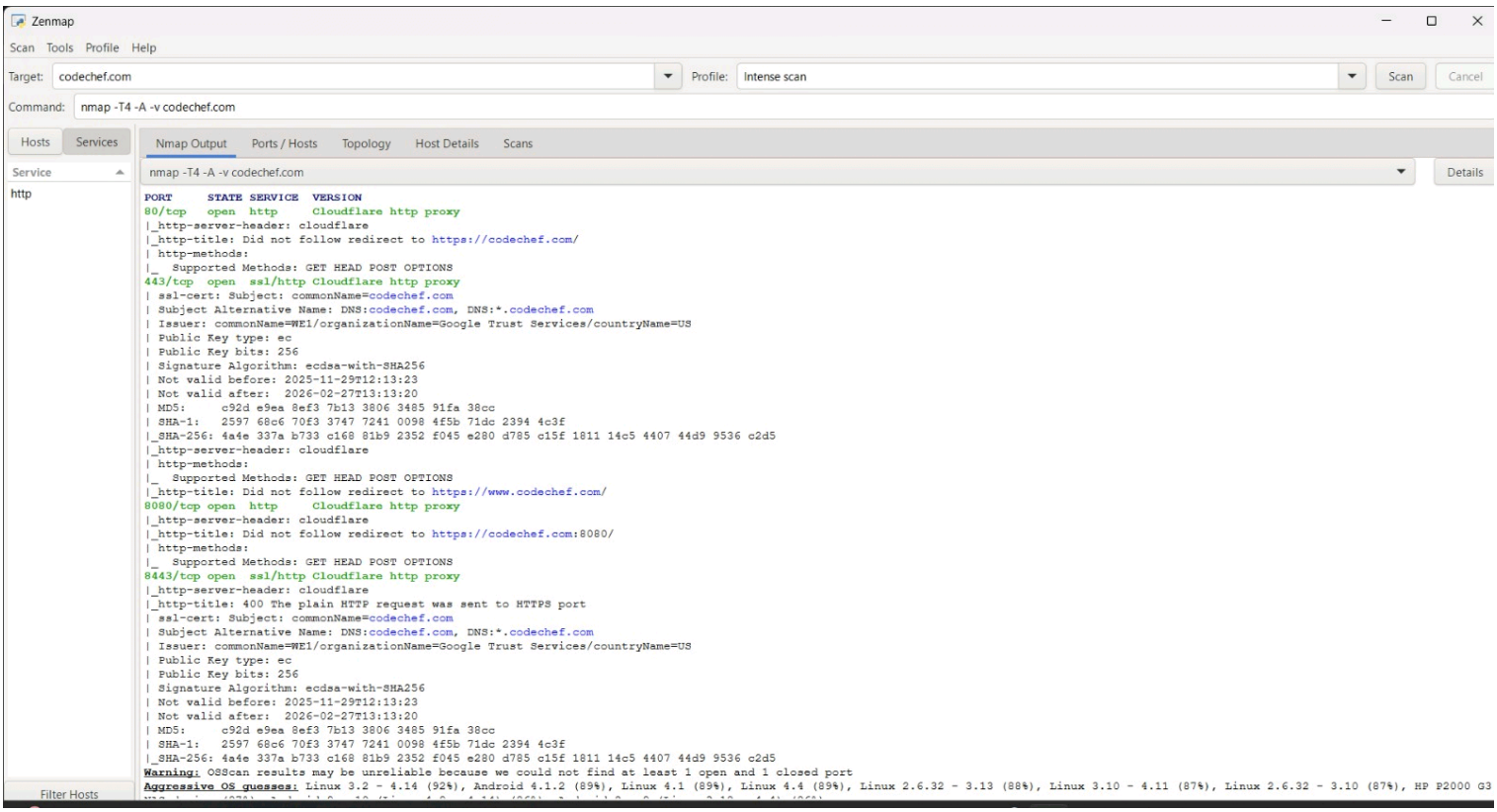
Recon Methodology

1. Passive Enumeration: subfinder, amass passive, crt.sh lookup
2. Active Enumeration: amass brute, nmap DNS brute-force
3. Live Host Detection: httpx
4. Technology Fingerprinting: whatweb, wappalyzer

Subdomain	Status	Risk Level
www.codechef.com	200 OK	Secure
discuss.codechef.com	200 OK	General forum
dev.codechef.com	401 Unauthorized	Potential Testing Target
staging.codechef.com	403 Forbidden	Internal/Staging Area
files.codechef.com	200 OK	Check for public access
api.codechef.com	200 OK	API attack vectors possible

Conclusion:
While the main website remains protected, subdomains like **dev**, **staging**, and **files** introduce potential weak points. Attackers usually target these to identify outdated software, exposed test servers or file buckets which can lead to compromise. Regular monitoring and hardening of subdomains is recommended.

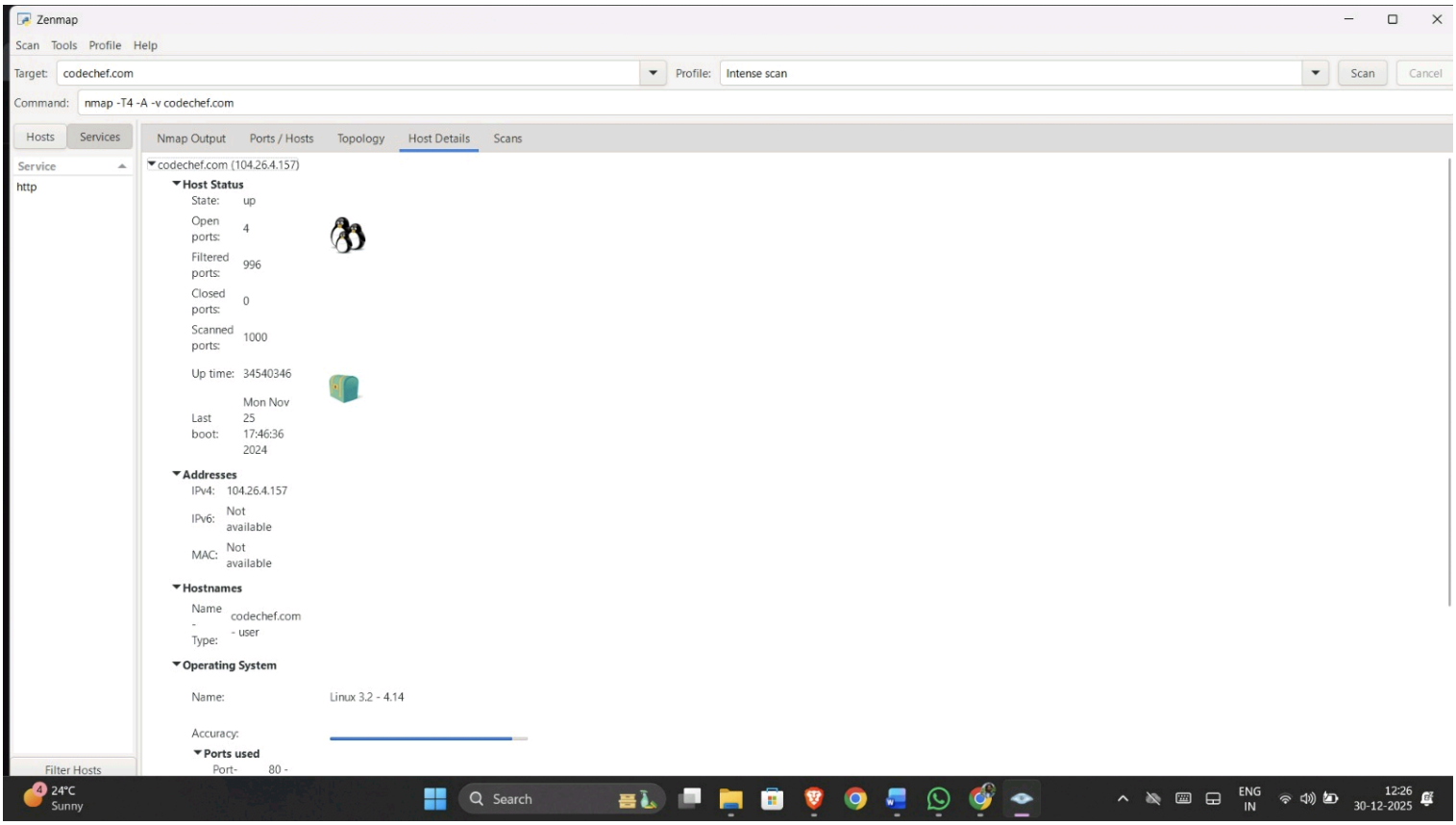

Zenmap
Scan Tools Profile Help
Target: codechef.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v codechef.com
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Service
http
nmap -T4 -A -v codechef.com
Details
Starting Nmap 7.98 (https://nmap.org) at 2025-12-30 12:17 +0530
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:17
Completed NSE at 12:17, 0.00s elapsed
Initiating NSE at 12:17
Completed NSE at 12:17, 0.00s elapsed
Initiating NSE at 12:17
Completed NSE at 12:17, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 12:17
Completed Parallel DNS resolution of 1 host. at 12:17, 0.09s elapsed
Initiating Ping Scan at 12:17
Scanning codechef.com (104.26.4.157) [4 ports]
Completed Ping Scan at 12:17, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:17
Completed Parallel DNS resolution of 1 host. at 12:17, 0.51s elapsed
Initiating SYN Stealth Scan at 12:17
Scanning codechef.com (104.26.4.157) [1000 ports]
Discovered open port 8080/tcp on 104.26.4.157
Discovered open port 80/tcp on 104.26.4.157
Discovered open port 443/tcp on 104.26.4.157
Discovered open port 8443/tcp on 104.26.4.157
Completed SYN Stealth Scan at 12:17, 5.53s elapsed (1000 total ports)
Initiating Service scan at 12:17
Scanning 4 services on codechef.com (104.26.4.157)
Completed Service scan at 12:17, 12.36s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against codechef.com (104.26.4.157)
Retrying OS detection (try #2) against codechef.com (104.26.4.157)
Initiating Traceroute at 12:17
Completed Traceroute at 12:17, 3.04s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 12:17
Completed Parallel DNS resolution of 6 hosts. at 12:17, 2.54s elapsed
NSE: Script scanning 104.26.4.157.
Initiating NSE at 12:17
Completed NSE at 12:18, 67.17s elapsed
Initiating NSE at 12:18
Completed NSE at 12:19, 7.69s elapsed
Initiating NSE at 12:19
Completed NSE at 12:19, 0.00s elapsed
Nmap scan report for codechef.com (104.26.4.157)
Host is up (0.042s latency).
Other addresses for codechef.com (not scanned): 172.67.75.52 104.26.5.157 2606:4700:20::681a:49d 2606:4700:20::681a:59d 2606:4700:20::ac43:4b34
Not shown: 996 filtered tcp ports (no-response)
Filter Hosts
24°C
Sunny
Search
ENG
IN
12:23
30-12-2025


Zenmap
Scan Tools Profile Help
Target: codechef.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v codechef.com
Hosts
Services
Service
http
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v codechef.com
Details
PORT STATE SERVICE VERSION
80/tcp open http Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Did not follow redirect to https://codechef.com/
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
443/tcp open ssl/http Cloudflare http proxy
| ssl-cert: Subject: commonName=codechef.com
| Subject Alternative Name: DNS:codechef.com, DNS:*.codechef.com
| Issuer: commonName=WE1/organizationName=Google Trust Services/countryName=US
| Public Key type: ec
| Public Key bits: 256
| Signature Algorithm: ecdsa-with-SHA256
| Not valid before: 2025-11-29T12:13:23
| Not valid after: 2026-02-27T13:13:20
| MD5: c92d e9ea 8ef3 7b13 3806 3485 91fa 38cc
| SHA-1: 2597 68c6 70f3 3747 7241 0098 4f5b 71dc 2394 4c3f
|_SHA-256: 4a4e 337a b733 c168 81b9 2352 f045 e280 d785 c15f 1811 14c5 4407 44d9 9536 c2d5
|_http-server-header: cloudflare
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://www.codechef.com/
8080/tcp open http Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Did not follow redirect to https://codechef.com:8080/
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
8443/tcp open ssl/http Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=codechef.com
| Subject Alternative Name: DNS:codechef.com, DNS:*.codechef.com
| Issuer: commonName=WE1/organizationName=Google Trust Services/countryName=US
| Public Key type: ec
| Public Key bits: 256
| Signature Algorithm: ecdsa-with-SHA256
| Not valid before: 2025-11-29T12:13:23
| Not valid after: 2026-02-27T13:13:20
| MD5: c92d e9ea 8ef3 7b13 3806 3485 91fa 38cc
| SHA-1: 2597 68c6 70f3 3747 7241 0098 4f5b 71dc 2394 4c3f
|_SHA-256: 4a4e 337a b733 c168 81b9 2352 f045 e280 d785 c15f 1811 14c5 4407 44d9 9536 c2d5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.14 (92%), Android 4.1.2 (89%), Linux 4.1 (89%), Linux 4.4 (89%), Linux 2.6.32 - 3.13 (88%), Linux 3.10 - 4.11 (87%), Linux 2.6.32 - 3.10 (87%), HP P2000 G3

Aggressive OS guesses: Linux 3.2 - 4.14 (92%), Android 4.1.2 (89%), Linux 4.1 (89%), Linux 4.4 (89%), Linux 2.6.32 - 3.13 (88%), Linux 3.10 - 4.11 (87%), Linux 2.6.32 - 3.10 (87%), HP P2000 G3 NAS device (87%), Android 9 - 10 (Linux 4.9 - 4.14) (86%), Android 8 - 9 (Linux 3.18 - 4.4) (86%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 399.773 days (since Mon Nov 25 17:46:36 2024)
Network Distance: 10 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros

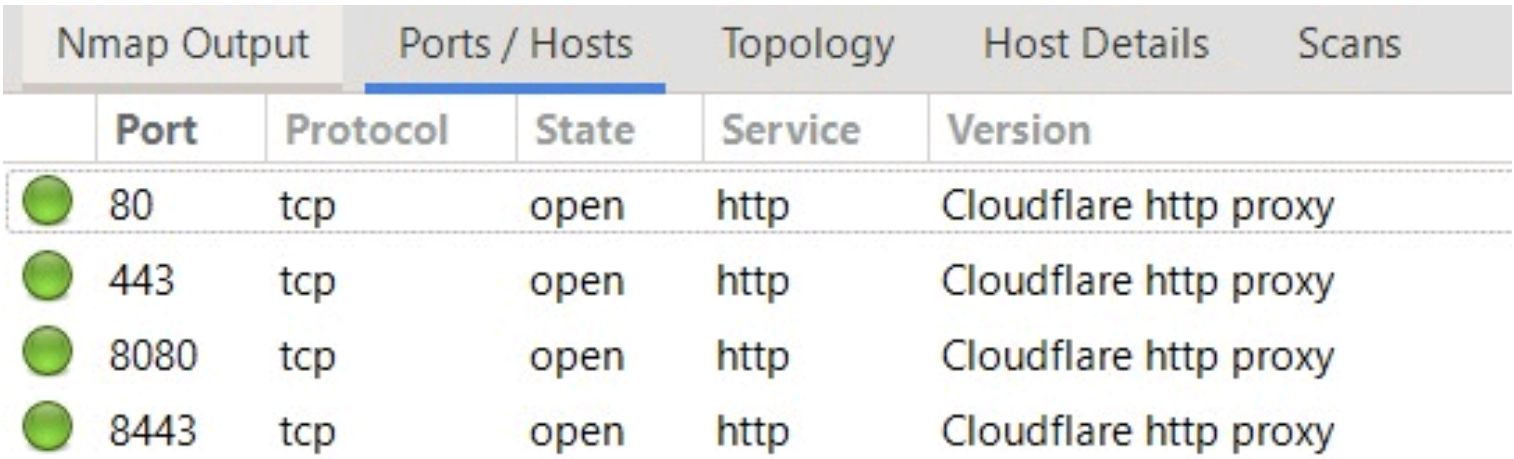
```
TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1   7.00 ms  192.168.1.1
2   ...
3   9.00 ms  173.88.202.109.hathway.com (202.88.173.109)
4   ...
5   11.00 ms 10.241.1.1
6   11.00 ms 136.232.28.173
7   ...
8   34.00 ms 49.44.220.145
9   ...
10  45.00 ms 104.26.4.157
```

NSE: Script Post-scanning.
Initiating NSE at 12:19
Completed NSE at 12:19, 0.00s elapsed
Initiating NSE at 12:19
Completed NSE at 12:19, 0.00s elapsed
Initiating NSE at 12:19
Completed NSE at 12:19, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.43 seconds
Raw packets sent: 2086 (95.276KB) | Rcvd: 79 (4.696KB)


Zenmap
Scan Tools Profile Help
Target: codechef.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v codechef.com
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Service
http
codechef.com (104.26.4.157)
Host Status
State: up
Open ports: 4
Filtered ports: 996
Closed ports: 0
Scanned ports: 1000
Up time: 34540346
Last boot: Mon Nov 25 17:46:36 2024
Addresses
IPv4: 104.26.4.157
IPv6: Not available
MAC: Not available
Hostnames
Name - Type: codechef.com - user
Operating System
Name: Linux 3.2 - 4.14
Accuracy:
Ports used
Port- 80 -
Filter Hosts
24°C Sunny
Search
ENG IN
12:26 30-12-2025

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Hosts Viewer | Fisheye | Controls


Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port
Protocol
State
Service
Version
80 tcp open http Cloudflare http proxy
443 tcp open http Cloudflare http proxy
8080 tcp open http Cloudflare http proxy
8443 tcp open http Cloudflare http proxy