**Task 1 - NETWORK SCANNING**

1. Perform a comprehensive network scan using Nmap
2. Identify active hosts, open ports, and running services.
3. **nmap -sn 192.168.0.0/24**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 10:36 +0530

Nmap scan report for 192.168.0.1

Host is up (0.026s latency).

MAC Address: 50:2B:73:98:D1:A0 (Tenda Technology,Ltd.Dongguan branch)

Nmap scan report for 192.168.0.170

Host is up.

Nmap done: 256 IP addresses (2 hosts up) scanned in 33.67 seconds

1. **nmap -sS -p 1-1000 192.168.0.170**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 10:37 +0530

Nmap scan report for 192.168.0.170

Host is up (0.00098s latency).

Not shown: 994 closed tcp ports (reset)

**PORT STATE SERVICE**

135/tcp open msrpc

137/tcp filtered netbios-ns

139/tcp open netbios-ssn

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

1. **nmap -sT -p 1-65535 192.168.0.170**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 10:38 +0530

Nmap scan report for 192.168.0.170

Host is up (0.00051s latency).

Not shown: 65515 closed tcp ports (conn-refused)

**PORT STATE SERVICE**

135/tcp open msrpc

137/tcp filtered netbios-ns

139/tcp open netbios-ssn

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

2869/tcp open icslap

5040/tcp open unknown

5357/tcp open wsdapi

6183/tcp open unknown

6184/tcp open unknown

7680/tcp open pando-pub

8090/tcp open opsmessaging

49664/tcp open unknown

49665/tcp open unknown

49666/tcp open unknown

49667/tcp open unknown

49668/tcp open unknown

49680/tcp open unknown

50128/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 6.96 seconds

Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds

1. **nmap -O 192.168.0.170 –** **Operating System Detection**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 12:44 +0530

Nmap scan report for 192.168.0.170

Host is up (0.00043s latency).

Not shown: 992 closed tcp ports (reset)

**PORT STATE SERVICE**

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

2869/tcp open icslap

5357/tcp open wsdapi

8090/tcp open opsmessaging

Device type: general purpose

Running: Microsoft Windows 10

OS CPE: cpe:/o:microsoft:windows\_10

**OS details: Microsoft Windows 10 1809 - 21H2**

**Network Distance: 0 hops**

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

Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds

1. Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-17 12:28 +0530

Nmap scan report for 192.168.0.1

**Host is up (0.0095s latency).**

MAC Address: 50:2B:73:98:D1:A0 (Tenda Technology,Ltd.Dongguan branch)

Nmap scan report for 192.168.0.170

Host is up.

Nmap done: 256 IP addresses (2 hosts up) scanned in 34.48 seconds

1. **nmap -sS -p- 192.168.0.0/24 -oN ip.txt**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 13:32 +0530

**Nmap scan report for 192.168.0.1**

Host is up (0.015s latency).

Not shown: 65529 closed tcp ports (reset)

**PORT STATE SERVICE**

**80/tcp open http**

**5500/tcp open hotline**

**7547/tcp open cwmp**

**9000/tcp open cslistener**

**10004/tcp open emcrmirccd**

**52881/tcp open unknown**

**MAC Address: 50:2B:73:98:D1:A0 (Tenda Technology,Ltd.Dongguan branch)**

Nmap scan report for **192.168.0.168**

Host is up (0.017s latency).

Not shown: 65534 closed tcp ports (reset)

PORT STATE SERVICE

**37125/tcp filtered unknown**

**MAC Address: 26:B7:9B:77:2A:A2 (Unknown)**

Nmap scan report for **192.168.0.170**

Host is up (0.00043s latency).

Not shown: 65518 closed tcp ports (reset)

**PORT STATE SERVICE**

**135/tcp open msrpc**

**137/tcp filtered netbios-ns**

**139/tcp open netbios-ssn**

**445/tcp open microsoft-ds**

**902/tcp open iss-realsecure**

**912/tcp open apex-mesh**

**5040/tcp open unknown**

**5357/tcp open wsdapi**

**6183/tcp open unknown**

**6184/tcp open unknown**

**49664/tcp open unknown**

**49665/tcp open unknown**

**49666/tcp open unknown**

**49667/tcp open unknown**

**49668/tcp open unknown**

**49680/tcp open unknown**

**50128/tcp open unknown**

1. **nmap -T4 -A -v GOOGLE.COM**

**nmap utput**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-17 13:16 +0530

NSE: Loaded 158 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 13:16

Completed NSE at 13:16, 0.00s elapsed

Initiating NSE at 13:16

Completed NSE at 13:16, 0.00s elapsed

Initiating NSE at 13:16

Completed NSE at 13:16, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 13:16

Completed Parallel DNS resolution of 1 host. at 13:16, 0.01s elapsed

Initiating Ping Scan at 13:16

Scanning GOOGLE.COM (142.251.222.206) [4 ports]

Completed Ping Scan at 13:16, 0.01s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 13:16

Completed Parallel DNS resolution of 1 host. at 13:16, 0.01s elapsed

Initiating SYN Stealth Scan at 13:16

Scanning GOOGLE.COM (142.251.222.206) [1000 ports]

**Discovered open port 80/tcp on 142.251.222.206**

**Discovered open port 443/tcp on 142.251.222.206**

Completed SYN Stealth Scan at 13:16, 5.54s elapsed (1000 total ports)

Initiating Service scan at 13:16

Scanning 2 services on GOOGLE.COM (142.251.222.206)

Service scan Timing: About 50.00% done; ETC: 13:18 (0:00:59 remaining)

Completed Service scan at 13:17, 66.61s elapsed (2 services on 1 host)

Initiating OS detection (try #1) against GOOGLE.COM (142.251.222.206)

Retrying OS detection (try #2) against GOOGLE.COM (142.251.222.206)

Initiating Traceroute at 13:17

Completed Traceroute at 13:17, 3.04s elapsed

Initiating Parallel DNS resolution of 5 hosts. at 13:17

Completed Parallel DNS resolution of 5 hosts. at 13:17, 1.53s elapsed

NSE: Script scanning 142.251.222.206.

Initiating NSE at 13:17

Completed NSE at 13:18, 5.17s elapsed

Initiating NSE at 13:18

NSOCK ERROR [88.7800s] poll\_loop(): nsock\_loop error 10022: An invalid argument was supplied.

NSE: Script Engine Scan Aborted.

An error was thrown by the engine: C:\Program Files (x86)\Nmap/nse\_main.lua:1078: a fatal error occurred in nsock\_loop

stack traceback:

[C]: in function 'nmap.socket.loop'

C:\Program Files (x86)\Nmap/nse\_main.lua:1078: in upvalue 'run'

C:\Program Files (x86)\Nmap/nse\_main.lua:1488: in function <C:\Program Files (x86)\Nmap/nse\_main.lua:1435>

[C]: in ?

Nmap scan report for GOOGLE.COM (142.251.222.206)

Host is up (0.024s latency).

Other addresses for GOOGLE.COM (not scanned): 2404:6800:4007:81b::200e

rDNS record for 142.251.222.206: hkg07s55-in-f14.1e100.net

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http gws

| fingerprint-strings:

| GetRequest:

| HTTP/1.0 200 OK

| Date: Thu, 17 Jul 2025 07:46:46 GMT

| Expires: -1

| Cache-Control: private, max-age=0

| Content-Type: text/html; charset=ISO-8859-1

| Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-Kj8PeFp6fjdX3hWErdJQaQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp

| P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."

| Server: gws

| X-XSS-Protection: 0

| X-Frame-Options: SAMEORIGIN

| Set-Cookie: AEC=AVh\_V2hUVH8-km\_qXfTf-4ObM\_lEFjwVbdwrv4XlhRBjwseztMFXmY1uk74; expires=Tue, 13-Jan-2026 07:46:46 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax

| Set-Cookie: NID=525=iujoH2Si5xmnHGbva0wC9\_0UEIVmIEZmTFOJob-S5X7sQDw98DE-jFZY\_Ba8sUYpHKV2k3wVCOA1I3nsu0\_ka4Aq\_NG52QvVsbn0L6WOhR2uE5DUrke9qRz\_C6K8wp2MTeT6wDowsVKomSm-kJ10CueCt4Ut9MH6npWG4G5tfdzNEqbjpT1c

| HTTPOptions:

| HTTP/1.0 405 Method Not Allowed

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

| Referrer-Policy: no-referrer

| Content-Length: 1592

| Date: Thu, 17 Jul 2025 07:46:46 GMT

| <!DOCTYPE html>

| <html lang=en>

| <meta charset=utf-8>

| <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">

| <title>Error 405 (Method Not Allowed)!!1</title>

| <style>

|\_ \*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}\* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding

|\_http-server-header: gws

|\_http-title: Did not follow redirect to http://www.google.com/

| http-methods:

|\_ Supported Methods: GET HEAD

443/tcp open ssl/https gws

| fingerprint-strings:

| GetRequest:

| HTTP/1.0 200 OK

| Date: Thu, 17 Jul 2025 07:46:52 GMT

| Expires: -1

| Cache-Control: private, max-age=0

| Content-Type: text/html; charset=ISO-8859-1

| Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-ARHYpTNtxU7SBo2fQU0\_Pw' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp

| Accept-CH: Sec-CH-Prefers-Color-Scheme

| P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."

| Server: gws

| X-XSS-Protection: 0

| X-Frame-Options: SAMEORIGIN

| Set-Cookie: AEC=AVh\_V2gpRHt3AD\_rNDWCLyNw3-QAmH4dCYsPGiCe813E53EUtG6DrtzFeg; expires=Tue, 13-Jan-2026 07:46:52 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax

|\_ Set-Cookie: NID=525=ckxgKymX33cu6g4\_b6fVDDKwiJhvjrwA99bJpiHpBIhs\_YPC5lzEjugDedxtyxlytmk5cmJwXSuUZmGJ6rYSRROuI0lZnByExjRY9lRgdMHytlx\_GmldSNhnrEjPw3BpfguRY-SRJnQ2e

| ssl-cert: Subject: commonName=\*.google.com

| Subject **Alternative Name: DNS**:\*.google.com, DNS:\*.appengine.google.com, DNS:\*.bdn.dev, DNS:\*.origin-test.bdn.dev, DNS:\*.**cloud.google.com**, DNS:\*.crowdsource.google.com, DNS:\*.**datacompute.google.com**, DNS:\*.google.ca, DNS:\*.google.cl, DNS:\*.google.co.in, DNS:\*.google.co.jp, DNS:\*.**google.co.uk,** DNS:\*.google.com.ar, DNS:\*.google.com.au, DNS:\*.**google.com.br**, DNS:\*.google.com.co, DNS:\*.google.com.mx, DNS:\*.**google.com.tr,** DNS:\*.google.com.vn, DNS:\*.google.de, DNS:\*.google.es, DNS:\*.google.fr, DNS:\*.google.hu, DNS:\*.google.it, DNS:\*.google.nl, DNS:\*.google.pl, DNS:\*.google.pt, DNS:\*.googleapis.cn, DNS:\*.googlevideo.com, DNS:\*.gstatic.cn, DNS:\*.gstatic-cn.com, DNS:googlecnapps.cn, DNS:\*.googlecnapps.cn, DNS:googleapps-cn.com, DNS:\*.googleapps-cn.com, DNS:gkecnapps.cn, DNS:\*.gkecnapps.cn, DNS:**googledownloads.cn**, DNS:\*.**googledownloads.cn**, DNS:**recaptcha.net.cn**, DNS:\*.recaptcha.net.cn, DNS:recaptcha-cn.net, DNS:\*.recaptcha-cn.net, DNS:widevine.cn, DNS:\*.widevine.cn, DNS:ampproject.org.cn, DNS:\*.ampproject.org.cn, DNS:ampproject.net.cn, DNS:\*.ampproject.net.cn, DNS:google-analytics-cn.com, DNS:\*.google-analytics-cn.com, DNS:googleadservices-cn.com, DNS:\*.**googleadservices-cn.com**, DNS:googlevads-cn.com, DNS:\*.googlevads-cn.com, DNS:googleapis-cn.com, DNS:\*.googleapis-cn.com, DNS:**googleoptimize-cn.com**, DNS:\*.googleoptimize-cn.com, DNS:doubleclick-cn.net, DNS:\*.doubleclick-cn.net, DNS:\*.fls.doubleclick-cn.net, DNS:\*.g.doubleclick-cn.net, DNS:doubleclick.cn, DNS:\*.doubleclick.cn, DNS:\*.fls.doubleclick.cn, DNS:\*.g.doubleclick.cn, DNS:dartsearch-cn.net, DNS:\*.dartsearch-cn.net, DNS:**googletraveladservices-cn.com**, DNS:\*.googletraveladservices-cn.com, DNS:googletagservices-cn.com, DNS:\*.googletagservices-cn.com, DNS**:googletagmanager-cn.com**, DNS:\*.googletagmanager-cn.com, DNS:**googlesyndication-cn.com**, DNS:\*.googlesyndication-cn.com, DNS**:\*.safeframe.googlesyndication-cn.com**, DNS:app-measurement-cn.com, DNS:\*.**app-measurement-cn.com,** DNS:gvt1-cn.com, DNS:\*.gvt1-cn.com, DNS:**gvt2-cn.com**, DNS:\*.gvt2-cn.com, DNS:2mdn-cn.net, DNS:\*.2mdn-cn.net, DNS:**googleflights-cn.net**, DNS:\*.**googleflights-cn.net**, DNS:**admob-cn.com**, DNS:\*.admob-cn.com, DNS:**googlesandbox-cn.com**, DNS:\*.googlesandbox-cn.com, DNS:\*.safenup.googlesandbox-cn.com, DNS:\*.gstatic.com, DNS:\*.metric.gstatic.com, DNS:\*.gvt1.com, DNS:\*.gcpcdn.gvt1.com, DNS:\*.gvt2.com, DNS:\*.gcp.gvt2.com, DNS:\*.url.google.com, DNS:\*.youtube-nocookie.com, DNS:\*.ytimg.com, DNS:ai.android, DNS:android.com, DNS:\*.android.com, DNS:\*.flash.android.com, DNS:g.cn, DNS:\*.g.cn, DNS:g.co, DNS:\*.g.co, DNS:goo.gl, DNS:www.goo.gl, DNS:google-analytics.com, DNS:\*.**google-analytics.com**, DNS:google.com, DNS:**googlecommerce.com**, DNS:\*.**googlecommerce.com**, DNS:ggpht.cn, DNS:\*.ggpht.cn, DNS:urchin.com, DNS:\*.urchin.com, DNS:youtu.be, DNS:youtube.com, DNS:\*.youtube.com, DNS:music.youtube.com, DNS:\*.music.youtube.com, DNS:youtubeeducation.com, DNS:\*.youtubeeducation.com, DNS:youtubekids.com, DNS:\*.youtubekids.com, DNS:yt.be, DNS:\*.yt.be, DNS**:android.clients.google.com**, DNS:\*.android.google.cn, DNS:\*.**chrome.google.cn**, DNS:\*.**developers.google.cn**, DNS:\*.**aistudio.google.com**

| Issuer: commonName=WE2/organizationName=Google Trust Services/countryName=US

| Public Key type: ec

| Public Key bits: 256

| Signature Algorithm: ecdsa-with-SHA256

| Not valid before: 2025-06-23T08:40:23

| Not valid after: 2025-09-15T08:40:22

| MD5: 4e88 f59f 0006 cbf9 5e17 c72a f330 b7b4

| SHA-1: ab9e 669e c958 8170 51a3 3fa9 9314 88cb 0d6d ec50

|\_SHA-256: 2e99 1f15 dc91 3a02 8d40 3839 cfb7 3d66 d25b 44ec df46 4f5d a091 00b3 f30b de0b

| tls-alpn:

| grpc-exp

| h2

|\_ http/1.1

|\_http-server-header: gws

| tls-nextprotoneg:

| grpc-exp

| h2

|\_ http/1.1

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.97%I=7%D=7/17%Time=6878AA66%P=i686-pc-windows-windows%r(

SF:GetRequest,458F,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Thu,\x2017\x20Jul\x

SF:202025\x2007:46:46\x20GMT\r\nExpires:\x20-1\r\nCache-Control:\x20privat

SF:e,\x20max-age=0\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-1\r\

SF:nContent-Security-Policy-Report-Only:\x20object-src\x20'none';base-uri\

SF:x20'self';script-src\x20'nonce-Kj8PeFp6fjdX3hWErdJQaQ'\x20'strict-dynam

SF:ic'\x20'report-sample'\x20'unsafe-eval'\x20'unsafe-inline'\x20https:\x2

SF:0http:;report-uri\x20https://csp\.withgoogle\.com/csp/gws/other-hp\r\nP

SF:3P:\x20CP=\"This\x20is\x20not\x20a\x20P3P\x20policy!\x20See\x20g\.co/p3

SF:phelp\x20for\x20more\x20info\.\"\r\nServer:\x20gws\r\nX-XSS-Protection:

SF:\x200\r\nX-Frame-Options:\x20SAMEORIGIN\r\nSet-Cookie:\x20AEC=AVh\_V2hUV

SF:H8-km\_qXfTf-4ObM\_lEFjwVbdwrv4XlhRBjwseztMFXmY1uk74;\x20expires=Tue,\x20

SF:13-Jan-2026\x2007:46:46\x20GMT;\x20path=/;\x20domain=\.google\.com;\x20

SF:Secure;\x20HttpOnly;\x20SameSite=lax\r\nSet-Cookie:\x20NID=525=iujoH2Si

SF:5xmnHGbva0wC9\_0UEIVmIEZmTFOJob-S5X7sQDw98DE-jFZY\_Ba8sUYpHKV2k3wVCOA1I3n

SF:su0\_ka4Aq\_NG52QvVsbn0L6WOhR2uE5DUrke9qRz\_C6K8wp2MTeT6wDowsVKomSm-kJ10Cu

SF:eCt4Ut9MH6npWG4G5tfdzNEqbjpT1c")%r(HTTPOptions,6DC,"HTTP/1\.0\x20405\x2

SF:0Method\x20Not\x20Allowed\r\nContent-Type:\x20text/html;\x20charset=UTF

SF:-8\r\nReferrer-Policy:\x20no-referrer\r\nContent-Length:\x201592\r\nDat

SF:e:\x20Thu,\x2017\x20Jul\x202025\x2007:46:46\x20GMT\r\n\r\n<!DOCTYPE\x20

SF:html>\n<html\x20lang=en>\n\x20\x20<meta\x20charset=utf-8>\n\x20\x20<met

SF:a\x20name=viewport\x20content=\"initial-scale=1,\x20minimum-scale=1,\x2

SF:0width=device-width\">\n\x20\x20<title>Error\x20405\x20\(Method\x20Not\

SF:x20Allowed\)!!1</title>\n\x20\x20<style>\n\x20\x20\x20\x20\\*{margin:0;p

SF:adding:0}html,code{font:15px/22px\x20arial,sans-serif}html{background:#

SF:fff;color:#222;padding:15px}body{margin:7%\x20auto\x200;max-width:390px

SF:;min-height:180px;padding:30px\x200\x2015px}\\*\x20>\x20body{background:

SF:url\(//www\.google\.com/images/errors/robot\.png\)\x20100%\x205px\x20no

SF:-repeat;padding-right:205px}p{margin:11px\x200\x2022px;overflow:hidden}

SF:ins{color:#777;text-decoration:none}a\x20img{border:0}@media\x20screen\

SF:x20and\x20\(max-width:772px\){body{background:none;margin-top:0;max-wid

SF:th:none;padding-right:0}}#logo{background:url\(//www\.google\.com/image

SF:s/branding");

**===========NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=============**

SF-Port443-TCP:V=7.97%T=SSL%I=7%D=7/17%Time=6878AA6C%P=i686-pc-windows-win

SF:dows%r(GetRequest,46AC,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Thu,\x2017\x

SF:20Jul\x202025\x2007:46:52\x20GMT\r\nExpires:\x20-1\r\nCache-Control:\x2

SF:0private,\x20max-age=0\r\nContent-Type:\x20text/html;\x20charset=ISO-88

SF:59-1\r\nContent-Security-Policy-Report-Only:\x20object-src\x20'none';ba

SF:se-uri\x20'self';script-src\x20'nonce-ARHYpTNtxU7SBo2fQU0\_Pw'\x20'stric

SF:t-dynamic'\x20'report-sample'\x20'unsafe-eval'\x20'unsafe-inline'\x20ht

SF:tps:\x20http:;report-uri\x20https://csp\.withgoogle\.com/csp/gws/other-

SF:hp\r\nAccept-CH:\x20Sec-CH-Prefers-Color-Scheme\r\nP3P:\x20CP=\"This\x2

SF:0is\x20not\x20a\x20P3P\x20policy!\x20See\x20g\.co/p3phelp\x20for\x20mor

SF:e\x20info\.\"\r\nServer:\x20gws\r\nX-XSS-Protection:\x200\r\nX-Frame-Op

SF:tions:\x20SAMEORIGIN\r\nSet-Cookie:\x20AEC=AVh\_V2gpRHt3AD\_rNDWCLyNw3-QA

SF:mH4dCYsPGiCe813E53EUtG6DrtzFeg;\x20expires=Tue,\x2013-Jan-2026\x2007:46

SF::52\x20GMT;\x20path=/;\x20domain=\.google\.com;\x20Secure;\x20HttpOnly;

SF:\x20SameSite=lax\r\nSet-Cookie:\x20NID=525=ckxgKymX33cu6g4\_b6fVDDKwiJhv

SF:jrwA99bJpiHpBIhs\_YPC5lzEjugDedxtyxlytmk5cmJwXSuUZmGJ6rYSRROuI0lZnByExjR

SF:Y9lRgdMHytlx\_GmldSNhnrEjPw3BpfguRY-SRJnQ2e");

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

OS fingerprint not ideal because: Missing a closed TCP port so results incomplete

No OS matches for host

Uptime guess: 0.000 days (since Thu Jul 17 13:17:49 2025)

Network Distance: 10 hops

TCP Sequence Prediction: Difficulty=262 (Good luck!)

IP ID Sequence Generation: All zeros

**TRACEROUTE (using port 80/tcp)**

**HOP RTT ADDRESS**

**1 2.00 ms 192.168.0.1**

**2 ... 5**

**6 17.00 ms 49.205.72.39.actcorp.in (49.205.72.39)**

**7 9.00 ms 72.14.223.26**

**8 9.00 ms 72.14.232.71**

**9 10.00 ms 142.251.55.239**

**10 13.00 ms pnmaaa-as-in-f14.1e100.net (142.251.222.206)**

NSE: Script Post-scanning.

Initiating NSE at 13:18

NSOCK ERROR [88.7910s] poll\_loop(): nsock\_loop error 10022: An invalid argument was supplied.

NSE: Script Engine Scan Aborted.

An error was thrown by the engine: C:\Program Files (x86)\Nmap/nse\_main.lua:1078: a fatal error occurred in nsock\_loop

stack traceback:

[C]: in function 'nmap.socket.loop'

C:\Program Files (x86)\Nmap/nse\_main.lua:1078: in upvalue 'run'

C:\Program Files (x86)\Nmap/nse\_main.lua:1488: in function <C:\Program Files (x86)\Nmap/nse\_main.lua:1435>

[C]: in ?

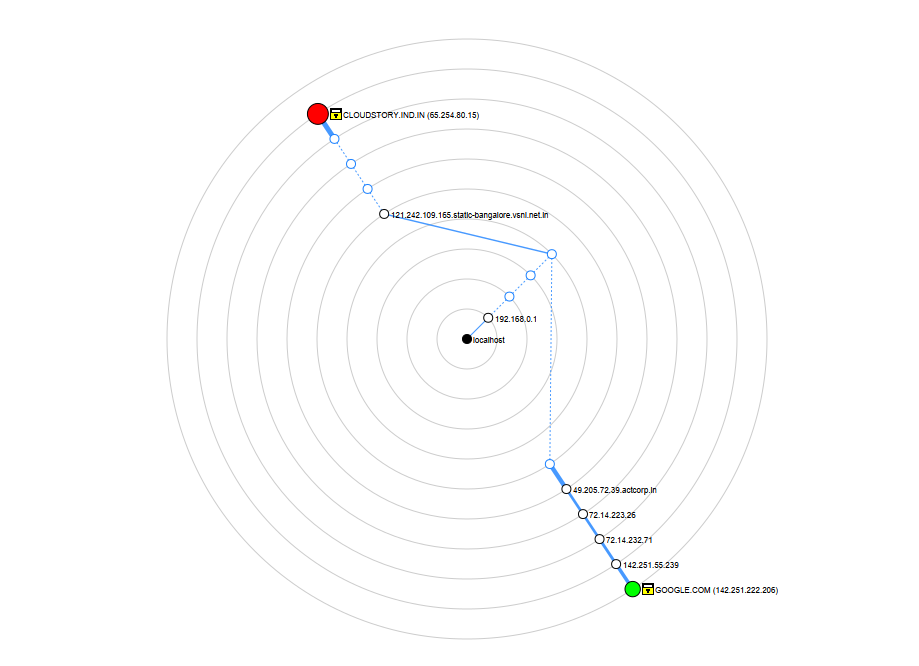
Read data files from: C:\Program Files (x86)\Nmap

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

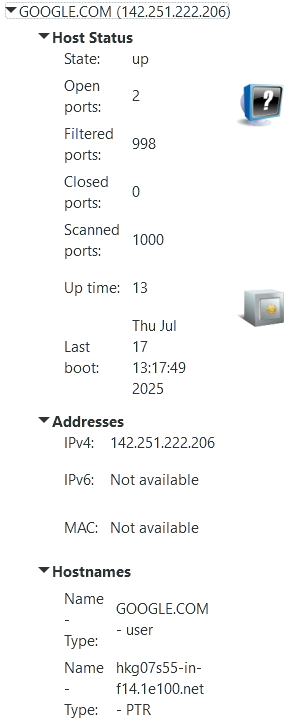
Nmap done: 1 IP address (1 host up) scanned in 88.79 seconds

Raw packets sent: 2103 (96.840KB) | Rcvd: 47 (4.286KB)

* 1. **ports open**
     1. **80 - tcp – open – http -gws**
     2. **443 – tcp – open – https – gws**
  2. **Topology**



* 1. **Host details**



* + 1. **Active Host - GOOGLE.COM (142.251.222.206)**
    2. **Open Ports – 80, 443**
    3. **Running Services**
       1. **http**
       2. **https**

1. **nmap -T4 -A -v cloudstory.ind.in**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-17 13:16 +0530

NSE: Loaded 158 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 13:16

Completed NSE at 13:16, 0.00s elapsed

Initiating NSE at 13:16

Completed NSE at 13:16, 0.00s elapsed

Initiating NSE at 13:16

Completed NSE at 13:16, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 13:16

Completed Parallel DNS resolution of 1 host. at 13:16, 0.50s elapsed

Initiating Ping Scan at 13:16

Scanning CLOUDSTORY.IND.IN (65.254.80.15) [4 ports]

Completed Ping Scan at 13:16, 0.04s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 13:16

Completed Parallel DNS resolution of 1 host. at 13:16, 0.55s elapsed

Initiating SYN Stealth Scan at 13:16

Scanning CLOUDSTORY.IND.IN (65.254.80.15) [1000 ports]

Discovered open port 110/tcp on 65.254.80.15

Discovered open port 993/tcp on 65.254.80.15

Discovered open port 22/tcp on 65.254.80.15

Discovered open port 443/tcp on 65.254.80.15

Discovered open port 143/tcp on 65.254.80.15

Discovered open port 53/tcp on 65.254.80.15

Discovered open port 587/tcp on 65.254.80.15

Discovered open port 995/tcp on 65.254.80.15

Discovered open port 80/tcp on 65.254.80.15

Discovered open port 3306/tcp on 65.254.80.15

Discovered open port 465/tcp on 65.254.80.15

Completed SYN Stealth Scan at 13:16, 10.45s elapsed (1000 total ports)

Initiating Service scan at 13:16

Scanning 11 services on CLOUDSTORY.IND.IN (65.254.80.15)

Completed Service scan at 13:16, 18.08s elapsed (11 services on 1 host)

Initiating OS detection (try #1) against CLOUDSTORY.IND.IN (65.254.80.15)

Retrying OS detection (try #2) against CLOUDSTORY.IND.IN (65.254.80.15)

Initiating Traceroute at 13:16

Completed Traceroute at 13:16, 3.10s elapsed

Initiating Parallel DNS resolution of 2 hosts. at 13:16

Completed Parallel DNS resolution of 2 hosts. at 13:16, 0.51s elapsed

NSE: Script scanning 65.254.80.15.

Initiating NSE at 13:16

Completed NSE at 13:16, 9.16s elapsed

Initiating NSE at 13:16

NSOCK ERROR [49.2120s] poll\_loop(): nsock\_loop error 10022: An invalid argument was supplied.

NSE: Script Engine Scan Aborted.

An error was thrown by the engine: C:\Program Files (x86)\Nmap/nse\_main.lua:1078: a fatal error occurred in nsock\_loop

stack traceback:

[C]: in function 'nmap.socket.loop'

C:\Program Files (x86)\Nmap/nse\_main.lua:1078: in upvalue 'run'

C:\Program Files (x86)\Nmap/nse\_main.lua:1488: in function <C:\Program Files (x86)\Nmap/nse\_main.lua:1435>

[C]: in ?

Nmap scan report for CLOUDSTORY.IND.IN (65.254.80.15)

Host is up (0.027s latency).

rDNS record for 65.254.80.15: 65-254-80-15.webhostbox.net

Not shown: 913 filtered tcp ports (no-response), 16 filtered tcp ports (admin-prohibited), 60 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.0 (protocol 2.0)

| ssh-hostkey:

| 3072 19:62:79:d8:cd:5a:c6:86:61:19:cf:b7:4c:42:08:da (RSA)

| 256 f7:81:86:d3:77:e3:50:44:32:40:9f:1b:11:ad:e3:b4 (ECDSA)

|\_ 256 ab:51:ae:09:e3:55:08:bd:3d:90:43:3c:be:fb:26:e2 (ED25519)

53/tcp open domain PowerDNS Authoritative Server 4.9.5

| dns-nsid:

| NSID: 65-254-80-15.cprapid.com (36352d3235342d38302d31352e637072617069642e636f6d)

| id.server: 65-254-80-15.cprapid.com

|\_ bind.version: PowerDNS Authoritative Server 4.9.5 (built May 12 2025 13:41:30 by root@bh-centos-8.dev.cpanel.net)

80/tcp open http Apache httpd

|\_http-server-header: Apache

| http-methods:

|\_ Supported Methods: HEAD GET POST OPTIONS

|\_http-title: Cloudstory

|\_http-favicon: Unknown favicon MD5: 1FBDF735A0DD3E8321C5E0828A45A4D5

110/tcp open pop3 Dovecot pop3d

| ssl-cert: Subject: commonName=cloudstory.ind.in

| Subject Alternative Name: DNS:cloudstory.ind.in, DNS:cpanel.cloudstory.ind.in, DNS:cpcalendars.cloudstory.ind.in, DNS:cpcontacts.cloudstory.ind.in, DNS:mail.cloudstory.ind.in, DNS:webdisk.cloudstory.ind.in, DNS:www.cloudstory.ind.in

| Issuer: commonName=R10/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2025-06-22T22:28:47

| Not valid after: 2025-09-20T22:28:46

| MD5: 107b e017 dfdb c929 0c13 3191 167a ae05

| SHA-1: 5e54 4d61 e34d 4e6f 312f dbb6 e765 42b0 37d7 bc9e

|\_SHA-256: 2bea 3dcc 1372 cf85 e51b 6f22 9a72 418a 982a f76c 4aaa 0e60 c293 5b51 81fc 86bc

|\_pop3-capabilities: UIDL TOP PIPELINING CAPA USER SASL(PLAIN LOGIN) STLS AUTH-RESP-CODE RESP-CODES

143/tcp open imap Dovecot imapd

|\_imap-capabilities: SASL-IR Pre-login post-login OK listed IDLE capabilities AUTH=LOGINA0001 STARTTLS AUTH=PLAIN more IMAP4rev1 have ID LITERAL+ ENABLE NAMESPACE LOGIN-REFERRALS

443/tcp open ssl/http Apache httpd

|\_http-server-header: Apache

|\_ssl-date: TLS randomness does not represent time

| http-methods:

|\_ Supported Methods: HEAD GET POST OPTIONS

|\_http-title: Cloudstory

|\_http-favicon: Unknown favicon MD5: 1FBDF735A0DD3E8321C5E0828A45A4D5

465/tcp open ssl/smtp Exim smtpd 4.98.2

|\_ssl-date: TLS randomness does not represent time

| smtp-commands: 65-254-80-15.cprapid.com Hello CLOUDSTORY.IND.IN [49.207.233.30], SIZE 52428800, LIMITS MAILMAX=1000 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, HELP

|\_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP

587/tcp open smtp Exim smtpd 4.98.2

| ssl-cert: Subject: commonName=65-254-80-15.cprapid.com

| Subject Alternative Name: DNS:65-254-80-15.cprapid.com

| Issuer: commonName=R10/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2025-07-17T04:52:15

| Not valid after: 2025-10-15T04:52:14

| MD5: b73f 6353 442d 78ee 2ae0 ec70 fa6b c936

| SHA-1: 79d7 60ce e9ec f29b a89f d990 bee3 bdf0 aac3 20ea

|\_SHA-256: bd09 6203 adba d7e5 63e9 226e 56f0 f497 e181 e576 f3f9 e9e3 65fb 5fd3 b8dc 0511

| smtp-commands: 65-254-80-15.cprapid.com Hello CLOUDSTORY.IND.IN [49.207.233.30], SIZE 52428800, LIMITS MAILMAX=1000 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP

|\_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP

993/tcp open imaps?

|\_ssl-date: TLS randomness does not represent time

|\_imap-capabilities: SASL-IR Pre-login post-login OK listed IDLE capabilities AUTH=LOGINA0001 AUTH=PLAIN more IMAP4rev1 NAMESPACE ID LITERAL+ have LOGIN-REFERRALS ENABLE

995/tcp open pop3s?

| ssl-cert: Subject: commonName=cloudstory.ind.in

| Subject Alternative Name: DNS:cloudstory.ind.in, DNS:cpanel.cloudstory.ind.in, DNS:cpcalendars.cloudstory.ind.in, DNS:cpcontacts.cloudstory.ind.in, DNS:mail.cloudstory.ind.in, DNS:webdisk.cloudstory.ind.in, DNS:www.cloudstory.ind.in

| Issuer: commonName=R10/organizationName=Let's Encrypt/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2025-06-22T22:28:47

| Not valid after: 2025-09-20T22:28:46

| MD5: 107b e017 dfdb c929 0c13 3191 167a ae05

| SHA-1: 5e54 4d61 e34d 4e6f 312f dbb6 e765 42b0 37d7 bc9e

|\_SHA-256: 2bea 3dcc 1372 cf85 e51b 6f22 9a72 418a 982a f76c 4aaa 0e60 c293 5b51 81fc 86bc

|\_ssl-date: TLS randomness does not represent time

|\_pop3-capabilities: CAPA SASL(PLAIN LOGIN) UIDL USER TOP RESP-CODES AUTH-RESP-CODE PIPELINING

3306/tcp open mysql MariaDB 5.5.5-10.11.13

| mysql-info:

| Protocol: 10

| Version: 5.5.5-10.11.13-MariaDB

| Thread ID: 174

| Capabilities flags: 63486

| Some Capabilities: DontAllowDatabaseTableColumn, ConnectWithDatabase, Support41Auth, ODBCClient, Speaks41ProtocolNew, SupportsTransactions, IgnoreSigpipes, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolOld, FoundRows, InteractiveClient, SupportsLoadDataLocal, LongColumnFlag, SupportsCompression, SupportsAuthPlugins, SupportsMultipleStatments, SupportsMultipleResults

| Status: Autocommit

| Salt: ~Y#A[\*ZgyJCQOw-s~Cm}

|\_ Auth Plugin Name: mysql\_native\_password

Aggressive OS guesses: Linux 4.15 (92%), Linux 4.19 - 5.15 (92%), Linux 3.4 (91%), Linux 3.11 - 4.9 (87%), Linux 3.2 - 3.8 (87%), Android TV OS 11 (Linux 4.19) (85%), IPFire 2.25 firewall (Linux 4.14) (85%), IPFire 2.27 (Linux 5.15 - 6.1) (85%), Linux 2.6.32 (85%), Linux 2.6.32 or 3.10 (85%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 6.847 days (since Thu Jul 10 16:57:30 2025)

Network Distance: 9 hops

TCP Sequence Prediction: Difficulty=258 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: Host: 65-254-80-15.cprapid.com

TRACEROUTE (using port 8080/tcp)

HOP RTT ADDRESS

1 1.00 ms 192.168.0.1

2 ... 4

5 3.00 ms 121.242.109.165.static-bangalore.vsnl.net.in (121.242.109.165)

6 ... 8

9 20.00 ms 65-254-80-15.webhostbox.net (65.254.80.15)

NSE: Script Post-scanning.

Initiating NSE at 13:16

NSOCK ERROR [49.2200s] poll\_loop(): nsock\_loop error 10022: An invalid argument was supplied.

NSE: Script Engine Scan Aborted.

An error was thrown by the engine: C:\Program Files (x86)\Nmap/nse\_main.lua:1078: a fatal error occurred in nsock\_loop

stack traceback:

[C]: in function 'nmap.socket.loop'

C:\Program Files (x86)\Nmap/nse\_main.lua:1078: in upvalue 'run'

C:\Program Files (x86)\Nmap/nse\_main.lua:1488: in function <C:\Program Files (x86)\Nmap/nse\_main.lua:1435>

[C]: in ?

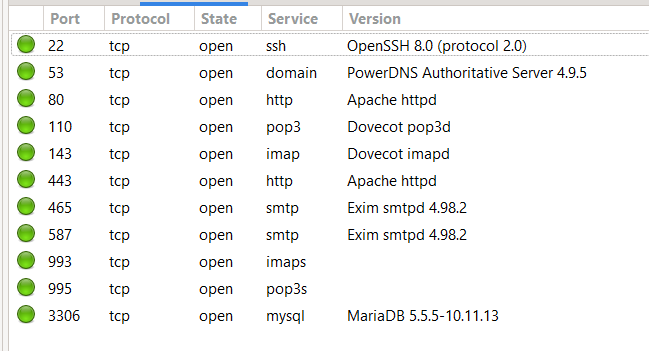
Read data files from: C:\Program Files (x86)\Nmap

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

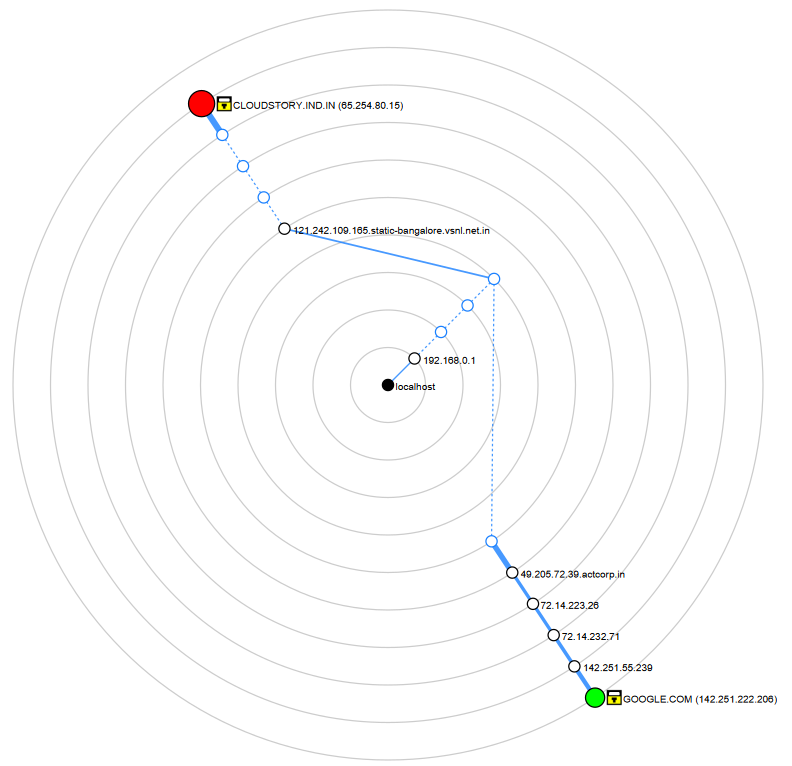
Nmap done: 1 IP address (1 host up) scanned in 49.22 seconds

Raw packets sent: 2935 (132.728KB) | Rcvd: 139 (10.027KB)

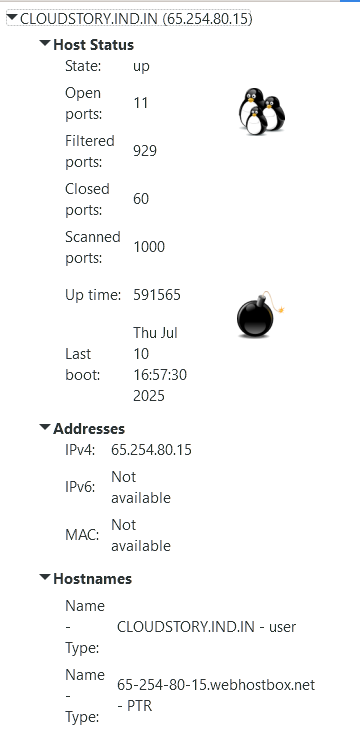
* 1. **PORTS OPEN**

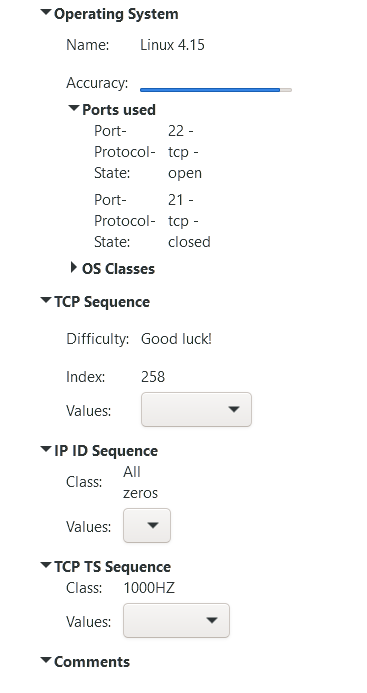


* 1. **TOPOLOGY**



* 1. HOST DETAILS





* 1. Identify active hosts, open ports, and running services.
     1. **Active Host** - CLOUDSTORY.IND.IN (65.254.80.15)
     2. **Open Ports – 22, 53, 80, 110, 143, 443, 465, 587, 993, 995, 3306**
     3. **Running Services**
        1. http, https - Required
        2. ssh, DNS, pop3, pop3s, imap, imaps, smtp & mysql ports are open which can be blocked.

1. **nmap -p 1-65535 -T4 -A -v 192.168.0.0/24**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-19 12:31 +0530

NSE: Loaded 158 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 12:31

Completed NSE at 12:31, 0.00s elapsed

Initiating NSE at 12:31

Completed NSE at 12:31, 0.00s elapsed

Initiating NSE at 12:31

Completed NSE at 12:31, 0.00s elapsed

Initiating ARP Ping Scan at 12:31

Scanning 255 hosts [1 port/host]

Completed ARP Ping Scan at 12:31, 4.47s elapsed (255 total hosts)

Initiating Parallel DNS resolution of 255 hosts. at 12:31

Completed Parallel DNS resolution of 255 hosts. at 12:31, 27.27s elapsed

Nmap scan report for 192.168.0.0 [host down]

Nmap scan report for 192.168.0.2 [host down]

Nmap scan report for 192.168.0.3 [host down]

Nmap scan report for 192.168.0.4 [host down]

Nmap scan report for 192.168.0.5 [host down]

Nmap scan report for 192.168.0.6 [host down]

Nmap scan report for 192.168.0.7 [host down]

Nmap scan report for 192.168.0.8 [host down]

Nmap scan report for 192.168.0.9 [host down]

Nmap scan report for 192.168.0.10 [host down]

Nmap scan report for 192.168.0.11 [host down]

Nmap scan report for 192.168.0.12 [host down]

Nmap scan report for 192.168.0.13 [host down]

Nmap scan report for 192.168.0.14 [host down]

Nmap scan report for 192.168.0.15 [host down]

Nmap scan report for 192.168.0.16 [host down]

Nmap scan report for 192.168.0.17 [host down]

Nmap scan report for 192.168.0.18 [host down]

Nmap scan report for 192.168.0.19 [host down]

Nmap scan report for 192.168.0.20 [host down]

Nmap scan report for 192.168.0.21 [host down]

Nmap scan report for 192.168.0.22 [host down]

Nmap scan report for 192.168.0.23 [host down]

Nmap scan report for 192.168.0.24 [host down]

Nmap scan report for 192.168.0.25 [host down]

Nmap scan report for 192.168.0.26 [host down]

Nmap scan report for 192.168.0.27 [host down]

Nmap scan report for 192.168.0.28 [host down]

Nmap scan report for 192.168.0.29 [host down]

Nmap scan report for 192.168.0.30 [host down]

Nmap scan report for 192.168.0.31 [host down]

Nmap scan report for 192.168.0.32 [host down]

Nmap scan report for 192.168.0.33 [host down]

Nmap scan report for 192.168.0.34 [host down]

Nmap scan report for 192.168.0.35 [host down]

Nmap scan report for 192.168.0.36 [host down]

Nmap scan report for 192.168.0.37 [host down]

Nmap scan report for 192.168.0.38 [host down]

Nmap scan report for 192.168.0.39 [host down]

Nmap scan report for 192.168.0.40 [host down]

Nmap scan report for 192.168.0.41 [host down]

Nmap scan report for 192.168.0.42 [host down]

Nmap scan report for 192.168.0.43 [host down]

Nmap scan report for 192.168.0.44 [host down]

Nmap scan report for 192.168.0.45 [host down]

Nmap scan report for 192.168.0.46 [host down]

Nmap scan report for 192.168.0.47 [host down]

Nmap scan report for 192.168.0.48 [host down]

Nmap scan report for 192.168.0.49 [host down]

Nmap scan report for 192.168.0.50 [host down]

Nmap scan report for 192.168.0.51 [host down]

Nmap scan report for 192.168.0.52 [host down]

Nmap scan report for 192.168.0.53 [host down]

Nmap scan report for 192.168.0.54 [host down]

Nmap scan report for 192.168.0.55 [host down]

Nmap scan report for 192.168.0.56 [host down]

Nmap scan report for 192.168.0.57 [host down]

Nmap scan report for 192.168.0.58 [host down]

Nmap scan report for 192.168.0.59 [host down]

Nmap scan report for 192.168.0.60 [host down]

Nmap scan report for 192.168.0.61 [host down]

Nmap scan report for 192.168.0.62 [host down]

Nmap scan report for 192.168.0.63 [host down]

Nmap scan report for 192.168.0.64 [host down]

Nmap scan report for 192.168.0.65 [host down]

Nmap scan report for 192.168.0.66 [host down]

Nmap scan report for 192.168.0.67 [host down]

Nmap scan report for 192.168.0.68 [host down]

Nmap scan report for 192.168.0.69 [host down]

Nmap scan report for 192.168.0.70 [host down]

Nmap scan report for 192.168.0.71 [host down]

Nmap scan report for 192.168.0.72 [host down]

Nmap scan report for 192.168.0.73 [host down]

Nmap scan report for 192.168.0.74 [host down]

Nmap scan report for 192.168.0.75 [host down]

Nmap scan report for 192.168.0.76 [host down]

Nmap scan report for 192.168.0.77 [host down]

Nmap scan report for 192.168.0.78 [host down]

Nmap scan report for 192.168.0.79 [host down]

Nmap scan report for 192.168.0.80 [host down]

Nmap scan report for 192.168.0.81 [host down]

Nmap scan report for 192.168.0.82 [host down]

Nmap scan report for 192.168.0.83 [host down]

Nmap scan report for 192.168.0.84 [host down]

Nmap scan report for 192.168.0.85 [host down]

Nmap scan report for 192.168.0.86 [host down]

Nmap scan report for 192.168.0.87 [host down]

Nmap scan report for 192.168.0.88 [host down]

Nmap scan report for 192.168.0.89 [host down]

Nmap scan report for 192.168.0.90 [host down]

Nmap scan report for 192.168.0.91 [host down]

Nmap scan report for 192.168.0.92 [host down]

Nmap scan report for 192.168.0.93 [host down]

Nmap scan report for 192.168.0.94 [host down]

Nmap scan report for 192.168.0.95 [host down]

Nmap scan report for 192.168.0.96 [host down]

Nmap scan report for 192.168.0.97 [host down]

Nmap scan report for 192.168.0.98 [host down]

Nmap scan report for 192.168.0.99 [host down]

Nmap scan report for 192.168.0.100 [host down]

Nmap scan report for 192.168.0.101 [host down]

Nmap scan report for 192.168.0.102 [host down]

Nmap scan report for 192.168.0.103 [host down]

Nmap scan report for 192.168.0.104 [host down]

Nmap scan report for 192.168.0.105 [host down]

Nmap scan report for 192.168.0.106 [host down]

Nmap scan report for 192.168.0.107 [host down]

Nmap scan report for 192.168.0.108 [host down]

Nmap scan report for 192.168.0.109 [host down]

Nmap scan report for 192.168.0.110 [host down]

Nmap scan report for 192.168.0.111 [host down]

Nmap scan report for 192.168.0.112 [host down]

Nmap scan report for 192.168.0.113 [host down]

Nmap scan report for 192.168.0.114 [host down]

Nmap scan report for 192.168.0.115 [host down]

Nmap scan report for 192.168.0.116 [host down]

Nmap scan report for 192.168.0.117 [host down]

Nmap scan report for 192.168.0.118 [host down]

Nmap scan report for 192.168.0.119 [host down]

Nmap scan report for 192.168.0.120 [host down]

Nmap scan report for 192.168.0.121 [host down]

Nmap scan report for 192.168.0.122 [host down]

Nmap scan report for 192.168.0.123 [host down]

Nmap scan report for 192.168.0.124 [host down]

Nmap scan report for 192.168.0.125 [host down]

Nmap scan report for 192.168.0.126 [host down]

Nmap scan report for 192.168.0.127 [host down]

Nmap scan report for 192.168.0.128 [host down]

Nmap scan report for 192.168.0.129 [host down]

Nmap scan report for 192.168.0.130 [host down]

Nmap scan report for 192.168.0.131 [host down]

Nmap scan report for 192.168.0.132 [host down]

Nmap scan report for 192.168.0.133 [host down]

Nmap scan report for 192.168.0.134 [host down]

Nmap scan report for 192.168.0.135 [host down]

Nmap scan report for 192.168.0.136 [host down]

Nmap scan report for 192.168.0.137 [host down]

Nmap scan report for 192.168.0.138 [host down]

Nmap scan report for 192.168.0.139 [host down]

Nmap scan report for 192.168.0.140 [host down]

Nmap scan report for 192.168.0.141 [host down]

Nmap scan report for 192.168.0.142 [host down]

Nmap scan report for 192.168.0.143 [host down]

Nmap scan report for 192.168.0.144 [host down]

Nmap scan report for 192.168.0.145 [host down]

Nmap scan report for 192.168.0.146 [host down]

Nmap scan report for 192.168.0.147 [host down]

Nmap scan report for 192.168.0.148 [host down]

Nmap scan report for 192.168.0.149 [host down]

Nmap scan report for 192.168.0.150 [host down]

Nmap scan report for 192.168.0.151 [host down]

Nmap scan report for 192.168.0.152 [host down]

Nmap scan report for 192.168.0.153 [host down]

Nmap scan report for 192.168.0.154 [host down]

Nmap scan report for 192.168.0.155 [host down]

Nmap scan report for 192.168.0.156 [host down]

Nmap scan report for 192.168.0.157 [host down]

Nmap scan report for 192.168.0.158 [host down]

Nmap scan report for 192.168.0.159 [host down]

Nmap scan report for 192.168.0.160 [host down]

Nmap scan report for 192.168.0.161 [host down]

Nmap scan report for 192.168.0.162 [host down]

Nmap scan report for 192.168.0.163 [host down]

Nmap scan report for 192.168.0.164 [host down]

Nmap scan report for 192.168.0.165 [host down]

Nmap scan report for 192.168.0.166 [host down]

Nmap scan report for 192.168.0.167 [host down]

Nmap scan report for 192.168.0.168 [host down]

Nmap scan report for 192.168.0.169 [host down]

Nmap scan report for 192.168.0.171 [host down]

Nmap scan report for 192.168.0.172 [host down]

Nmap scan report for 192.168.0.173 [host down]

Nmap scan report for 192.168.0.174 [host down]

Nmap scan report for 192.168.0.175 [host down]

Nmap scan report for 192.168.0.176 [host down]

Nmap scan report for 192.168.0.177 [host down]

Nmap scan report for 192.168.0.178 [host down]

Nmap scan report for 192.168.0.179 [host down]

Nmap scan report for 192.168.0.180 [host down]

Nmap scan report for 192.168.0.182 [host down]

Nmap scan report for 192.168.0.183 [host down]

Nmap scan report for 192.168.0.184 [host down]

Nmap scan report for 192.168.0.185 [host down]

Nmap scan report for 192.168.0.186 [host down]

Nmap scan report for 192.168.0.187 [host down]

Nmap scan report for 192.168.0.188 [host down]

Nmap scan report for 192.168.0.189 [host down]

Nmap scan report for 192.168.0.190 [host down]

Nmap scan report for 192.168.0.191 [host down]

Nmap scan report for 192.168.0.192 [host down]

Nmap scan report for 192.168.0.193 [host down]

Nmap scan report for 192.168.0.194 [host down]

Nmap scan report for 192.168.0.195 [host down]

Nmap scan report for 192.168.0.196 [host down]

Nmap scan report for 192.168.0.197 [host down]

Nmap scan report for 192.168.0.198 [host down]

Nmap scan report for 192.168.0.199 [host down]

Nmap scan report for 192.168.0.200 [host down]

Nmap scan report for 192.168.0.201 [host down]

Nmap scan report for 192.168.0.202 [host down]

Nmap scan report for 192.168.0.203 [host down]

Nmap scan report for 192.168.0.204 [host down]

Nmap scan report for 192.168.0.205 [host down]

Nmap scan report for 192.168.0.206 [host down]

Nmap scan report for 192.168.0.207 [host down]

Nmap scan report for 192.168.0.208 [host down]

Nmap scan report for 192.168.0.209 [host down]

Nmap scan report for 192.168.0.210 [host down]

Nmap scan report for 192.168.0.211 [host down]

Nmap scan report for 192.168.0.212 [host down]

Nmap scan report for 192.168.0.213 [host down]

Nmap scan report for 192.168.0.214 [host down]

Nmap scan report for 192.168.0.215 [host down]

Nmap scan report for 192.168.0.216 [host down]

Nmap scan report for 192.168.0.217 [host down]

Nmap scan report for 192.168.0.218 [host down]

Nmap scan report for 192.168.0.219 [host down]

Nmap scan report for 192.168.0.220 [host down]

Nmap scan report for 192.168.0.221 [host down]

Nmap scan report for 192.168.0.222 [host down]

Nmap scan report for 192.168.0.223 [host down]

Nmap scan report for 192.168.0.224 [host down]

Nmap scan report for 192.168.0.225 [host down]

Nmap scan report for 192.168.0.226 [host down]

Nmap scan report for 192.168.0.227 [host down]

Nmap scan report for 192.168.0.228 [host down]

Nmap scan report for 192.168.0.229 [host down]

Nmap scan report for 192.168.0.230 [host down]

Nmap scan report for 192.168.0.231 [host down]

Nmap scan report for 192.168.0.232 [host down]

Nmap scan report for 192.168.0.233 [host down]

Nmap scan report for 192.168.0.234 [host down]

Nmap scan report for 192.168.0.235 [host down]

Nmap scan report for 192.168.0.236 [host down]

Nmap scan report for 192.168.0.237 [host down]

Nmap scan report for 192.168.0.238 [host down]

Nmap scan report for 192.168.0.239 [host down]

Nmap scan report for 192.168.0.240 [host down]

Nmap scan report for 192.168.0.241 [host down]

Nmap scan report for 192.168.0.242 [host down]

Nmap scan report for 192.168.0.243 [host down]

Nmap scan report for 192.168.0.244 [host down]

Nmap scan report for 192.168.0.245 [host down]

Nmap scan report for 192.168.0.246 [host down]

Nmap scan report for 192.168.0.247 [host down]

Nmap scan report for 192.168.0.248 [host down]

Nmap scan report for 192.168.0.249 [host down]

Nmap scan report for 192.168.0.250 [host down]

Nmap scan report for 192.168.0.251 [host down]

Nmap scan report for 192.168.0.252 [host down]

Nmap scan report for 192.168.0.253 [host down]

Nmap scan report for 192.168.0.254 [host down]

Nmap scan report for 192.168.0.255 [host down]

Initiating Parallel DNS resolution of 1 host. at 12:31

Completed Parallel DNS resolution of 1 host. at 12:31, 0.50s elapsed

Initiating SYN Stealth Scan at 12:31

Scanning 2 hosts [65535 ports/host]

Discovered open port 80/tcp on 192.168.0.1

Discovered open port 10004/tcp on 192.168.0.1

SYN Stealth Scan Timing: About 14.78% done; ETC: 12:35 (0:02:59 remaining)

Discovered open port 7547/tcp on 192.168.0.1

Discovered open port 52881/tcp on 192.168.0.1

SYN Stealth Scan Timing: About 30.73% done; ETC: 12:35 (0:02:18 remaining)

Discovered open port 5500/tcp on 192.168.0.1

SYN Stealth Scan Timing: About 45.45% done; ETC: 12:35 (0:01:49 remaining)

Discovered open port 9000/tcp on 192.168.0.1

SYN Stealth Scan Timing: About 60.26% done; ETC: 12:35 (0:01:20 remaining)

SYN Stealth Scan Timing: About 75.79% done; ETC: 12:35 (0:00:48 remaining)

Completed SYN Stealth Scan against 192.168.0.1 in 197.69s (1 host left)

Completed SYN Stealth Scan at 12:35, 198.55s elapsed (131070 total ports)

Initiating Service scan at 12:35

Scanning 6 services on 2 hosts

WARNING: Service 192.168.0.1:5500 had already soft-matched rtsp, but now soft-matched sip; ignoring second value

1. **nmap -sC -sV -p- 192.168.0.170**

nmap -sC -sV -p- 192.168.0.170

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 19:24 +0530

Nmap scan report for 192.168.0.170

Host is up (0.00032s latency).

Not shown: 65517 closed tcp ports (reset)

**PORT STATE SERVICE VERSION**

135/tcp open msrpc Microsoft Windows RPC

137/tcp filtered netbios-ns

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

912/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)

5040/tcp open unknown

5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Service Unavailable

6183/tcp open msrpc Microsoft Windows RPC

6184/tcp open msexchange-logcopier Microsoft Exchange 2010 log copier

8090/tcp open tcpwrapped

49664/tcp open msrpc Microsoft Windows RPC

49665/tcp open msrpc Microsoft Windows RPC

49666/tcp open msrpc Microsoft Windows RPC

49667/tcp open msrpc Microsoft Windows RPC

49678/tcp open msrpc Microsoft Windows RPC

50128/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Bad Request

50756/tcp open msrpc Microsoft Windows RPC

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-security-mode:

| 3.1.1:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2025-07-20T13:56:09

|\_ start\_date: N/A

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

Nmap done: 1 IP address (1 host up) scanned in 105.04 seconds

1. REPORT

**🛡️ Banner Grabbing & Vulnerability Analysis Report**

**Target IP:** 192.168.0.170  
**Scan Method:** nmap -sC -sV -p-  
**Scan Date:** July 20, 2025  
**Operating System:** Microsoft Windows (Based on service banners)  
**MAC Address:** Not reported  
**Host Status:** Up (0.00032s latency)

**1️⃣ Active Host Summary**

* **Total Hosts Scanned:** 1
* **Active Hosts Detected:** 1
* **Host IP:** 192.168.0.170
* **Host OS:** Windows (CPE: cpe:/o:microsoft:windows)

**2️⃣ Open Ports and Banner Grabbing Results**

| **Port** | **Protocol** | **Service** | **Version / Banner** | **Potential Vulnerabilities / Notes** |
| --- | --- | --- | --- | --- |
| 135 | TCP | MSRPC | Microsoft Windows RPC | RCE via DCOM (e.g., **CVE-2021-26414**) |
| 137 | TCP | netbios-ns | **Filtered** | Possible firewall or IDS rule |
| 139 | TCP | netbios-ssn | Microsoft NetBIOS Session Service | Can allow SMB relay, NetBIOS spoofing |
| 445 | TCP | microsoft-ds | Unknown version | Target for **SMBv1 RCE (EternalBlue – CVE-2017-0144)** |
| 902 | TCP | SSL/VMware-auth | VMware Authentication Daemon 1.10 | Possible remote access risk, VNC/Soap interface |
| 912 | TCP | vmware-auth | VMware Authentication Daemon 1.0 | May leak VMware environment info |
| 5040 | TCP | unknown | No banner detected | Further manual probing required |
| 5357 | TCP | HTTP | Microsoft HTTPAPI httpd 2.0 | Known SSRF bugs in some versions, shows "Service Unavailable" |
| 6183 | TCP | MSRPC | Microsoft Windows RPC | Ephemeral RPC endpoint |
| 6184 | TCP | Exchange log copier | Microsoft Exchange 2010 log copier | Vulnerable to post-auth RCE (**CVE-2021-26855**, ProxyLogon) |
| 8090 | TCP | tcpwrapped | Service behind wrapper | Could indicate WAF or firewall |
| 49664 | TCP | MSRPC | Microsoft Windows RPC | High port range used by RPC |
| 49665 | TCP | MSRPC | Microsoft Windows RPC | — |
| 49666 | TCP | MSRPC | Microsoft Windows RPC | — |
| 49667 | TCP | MSRPC | Microsoft Windows RPC | — |
| 49678 | TCP | MSRPC | Microsoft Windows RPC | — |
| 50128 | TCP | HTTP | Microsoft HTTPAPI httpd 2.0 | Returns "Bad Request" — unusual |
| 50756 | TCP | MSRPC | Microsoft Windows RPC | — |

**3️⃣ Host Script Results**

| **Script** | **Result** |
| --- | --- |
| smb2-security-mode | SMB v3.1.1: Message signing enabled, **but not required** (risk: downgrade attacks) |
| smb2-time | Time: 2025-07-20T13:56:09 (Used to detect domain controller time drift) |

**4️⃣ Analysis of Vulnerabilities and Risks**

| **Service** | **Risk Level** | **Vulnerabilities / CVEs** |
| --- | --- | --- |
| **SMB on 445** | 🔴 High | CVE-2017-0144 (EternalBlue), CVE-2020-0796 (SMBGhost) |
| **Exchange (6184)** | 🔴 High | CVE-2021-26855 (ProxyLogon), CVE-2021-34473 |
| **NetBIOS (139)** | 🟠 Medium | NBNS spoofing, LLMNR relay, pass-the-hash |
| **VMware-auth (902/912)** | 🟠 Medium | Information disclosure or service misuse |
| **HTTPAPI (5357/50128)** | 🟡 Low | No major CVEs but may leak internal config |
| **Filtered port 137** | 🟡 Info | May be blocked by host firewall — investigate further |

**5️⃣ Recommendations**

| **Area** | **Recommendation** |
| --- | --- |
| 🔒 SMB & NetBIOS | Disable SMBv1, enforce SMB signing, restrict NetBIOS usage |
| 🔧 Exchange Services | Immediately update Exchange Server; verify CVE patches |
| 🔐 VMware Interfaces | Restrict access to 902/912; use strong authentication |
| 🔥 Firewalling | Block unused high ports and NetBIOS externally |
| 🕵️ Manual Testing | Probe port 5040 and 8090 manually using telnet, nc, or browser tools |
| 📈 Monitoring | Log and alert on RPC/SMB/Exchange access from untrusted IPs |
| 🔄 Patching | Keep Windows services and components up to date using WSUS/SCCM/Manual |

**6️⃣ Unusual / Unexpected Findings**

* **Port 5040** is open but unidentified — possibly a custom or legacy app.
* **Port 8090** is TCP-wrapped — may be intentionally hidden behind a proxy/WAF.
* **SMB signing not required** — opens door for relay attacks if not protected by other layers.

**✅ Conclusion**

The system is **active**, running **Windows RPC, SMB, VMware, HTTPAPI, and Exchange services**, some of which are **outdated or vulnerable**.  
Focus should be on securing **SMB**, **Exchange**, and **VMware** services, **hardening RPC**, and **investigating unidentified ports (5040, 8090)**.