Security Audit Report: Nmap Scan Results

1. Executive Summary

This report presents findings from an Nmap scan of the target ccgac.bitrix24.site (IP: 52.59.124.117). The scan aims to identify open ports, services, and potential vulnerabilities. Overall, the host exhibits both strengths in web service implementation and areas requiring immediate attention regarding security configurations.

2. Scan Overview

- **Tool**: Nmap 7.95
- **Scan Date**: September 22, 2024, 21:00 IST
- **Target**: ccgac.bitrix24.site
- **IP Address**: 52.59.124.117
- **Scan Duration**: 664.83 seconds

3. Pre-scan Findings

3.1 Profinet Devices

- **Result**: No Profinet devices detected in the subnet.

3.2 DHCP Discovery

- **Server IP**: 192.168.125.110
- **Client IP Offered**: 192.168.125.241
- **Subnet Mask**: 255.255.255.0
- **Gateway**: 192.168.125.110
- **DNS Server**: 192.168.125.110

3.3 Script Execution Errors

- Several scripts related to Robtex were disabled due to API changes.

4. Host Information

- **Host Status**: Up
- **Latency**: 0.18 seconds
- **Reverse DNS Record**: ec2-52-59-124-117.eu-central-1.compute.amazonaws.com

5. Open Ports and Services

5.1 Port 80 (HTTP)

- **State**: Open

- **Service**: HTTP (OpenResty web app server)
- **Server Header**: Bitrix24.Sites
- **Redirects**: Redirects HTTP requests to HTTPS (https://ccgac.bitrix24.site/).

5.2 Port 443 (HTTPS)

- **State**: Open
- **Service**: HTTPS (OpenResty web app server)
- **SSL Certificate**:
    - **Common Name**: *.bitrix24.site
    - **Validity**: Valid from August 29, 2024, to September 30, 2025
    - **Cipher Support**: Includes weak ciphers (e.g., 3DES), vulnerable to SWEET32 attacks.

6. Web Application Analysis

6.1 User Agent Testing

- Allowed user agents include various browsers; however, many automated agents returned a 503 error.

6.2 Security Vulnerability Testing

- **Cross-Site Scripting (XSS)**: No vulnerabilities found.
- **Cross-Site Request Forgery (CSRF)**: No vulnerabilities found.
- **Potential User Enumeration**: Usernames like root, admin, etc., detected, posing a security risk.

6.3 Security Headers

- **HSTS**: Not configured.
- **Recommendations**: Implement HSTS to strengthen security.

7. Network Analysis

7.1 Port States Summary

- **Open Ports**: 80, 443
- **Filtered Ports**: Majority of ports (1-79, 81-442, etc.) are filtered, likely due to firewall rules.
- **Closed Ports**: 1339, 1443, 8895 are closed.

7.2 SSL/TLS Security

- Weak ciphers (3DES) pose a vulnerability; upgrade to stronger alternatives is recommended.

8. Traceroute Results

- **Total Hops**: 5
- **Round Trip Times (RTT)**:

- 1st hop: 3 ms
- 2nd to 4th hops: 17-21 ms
- 5th hop: 20 ms

9. Errors and Limitations

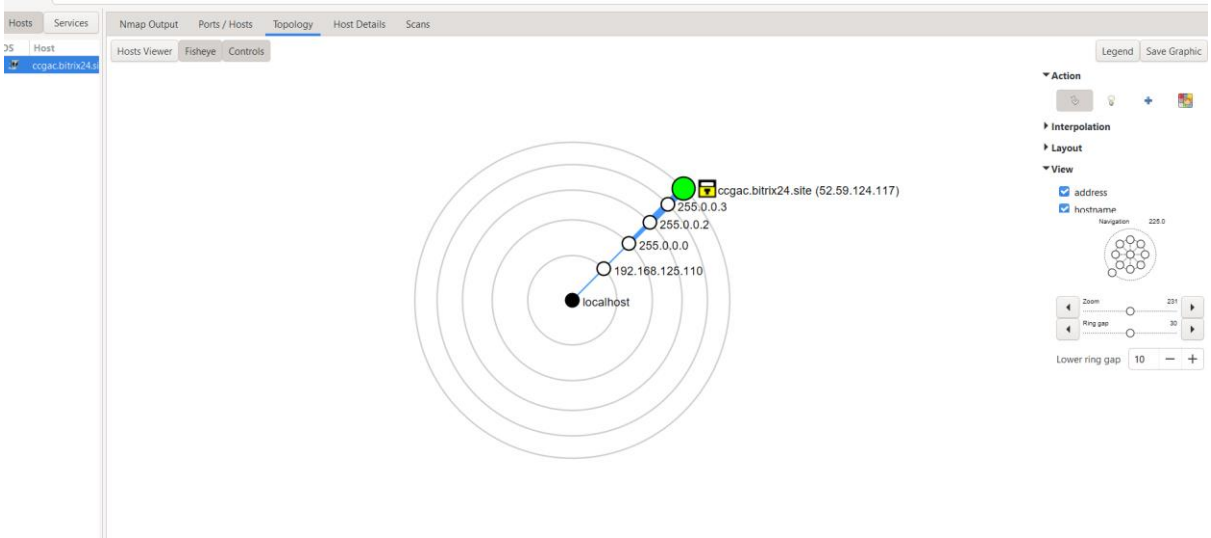
- Several scripts failed during execution, limiting detailed analysis and data collection. Future scans should ensure script compatibility and availability.

10. Recommendations

1. **Implement HSTS**: To enforce secure connections and protect user data.
2. **Upgrade Cipher Suites**: Remove weak ciphers (e.g., 3DES) to mitigate known vulnerabilities.
3. **Audit User Accounts**: Review potential user accounts for security weaknesses and implement strong password policies.
4. **Enhance Security Monitoring**: Regularly review and update firewall and server settings.
5. **Improve Logging Mechanisms**: Implement robust logging to detect and respond to unauthorized access attempts.

11. Conclusion

The Nmap scan highlights the target's current security posture, identifying both strengths and vulnerabilities. Immediate attention is required to address identified weaknesses, particularly regarding SSL/TLS configurations and the implementation of HSTS. Continuous monitoring and regular audits will help maintain a secure environment.



Summary of Findings

1. **Open Ports**:
    - **Port 80 (HTTP)**: Open; serves as an entry point but redirects to HTTPS.
    - **Port 443 (HTTPS)**: Open; SSL/TLS configurations are present but include weak cipher support.
2. **Web Application**:
    - **Server Software**: OpenResty web app server.
    - **CMS**: Bitrix24.Sites detected.
    - **No Cross-Site Scripting (XSS)** or Cross-Site Request Forgery (CSRF) vulnerabilities found.
3. **Security Headers**:
    - **HSTS**: Not configured; recommended for improving security.
    - **Weak ciphers (3DES)** detected; vulnerable to SWEET32 attacks.
4. **User Enumeration**:
    - Potential usernames like admin, root, and guest were identified, indicating possible enumeration vulnerabilities.
5. **Firewall Configuration**:
    - A large number of ports are filtered, suggesting effective firewall rules in place to block unauthorized access.
6. **DNS and Network Configuration**:
    - The server has a valid SSL certificate, but the use of weak ciphers and lack of HSTS can expose it to attacks.

Key Risks

- **Weak SSL/TLS Configurations**: The presence of vulnerable ciphers (3DES) increases the risk of data exposure.
- **Lack of HSTS**: Absence of HSTS can allow man-in-the-middle attacks.
- **User Enumeration**: Identifiable user accounts could be targeted for credential stuffing or brute-force attacks.

Recommendations

1. **Implement HSTS**: This will force HTTPS and enhance security against certain attacks.
2. **Upgrade SSL/TLS Configurations**: Remove weak ciphers and ensure strong protocols (e.g., TLS 1.2 or higher) are enabled.
3. **Audit User Accounts**: Strengthen password policies and consider implementing account lockout mechanisms.
4. **Regular Security Audits**: Continuous monitoring and regular audits will help identify and mitigate vulnerabilities proactively.

Conclusion

The audit reveals that while the server is operational with valid security measures, immediate attention is required to address the identified vulnerabilities, particularly in SSL/TLS configurations and the implementation of security headers. Addressing these issues will significantly enhance the overall security posture of the application.

Scan Result

Starting Nmap 7.95 (https://nmap.org) at 2024-09-22 21:00 India Standard Time

No profinet devices in the subnet

Pre-scan script results:

|_multicast-profinet-discovery: 0

| broadcast-listener:

| udp

| DHCP

| srv ip cli ip mask gw dns vendor

|_ 192.168.125.110 192.168.125.241 255.255.255.0 192.168.125.110 192.168.125.110 -

|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/

|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/

| targets-asn:

|_ targets-asn.asn is a mandatory parameter

| broadcast-dhcp-discover:

| Response 1 of 1:

| Interface: eth3

| IP Offered: 192.168.125.241

| Server Identifier: 192.168.125.110

| Subnet Mask: 255.255.255.0

| Broadcast Address: 192.168.125.255

| Router: 192.168.125.110

|_ Domain Name Server: 192.168.125.110

|_eap-info: please specify an interface with -e

Failed to resolve "nmap".

Nmap scan report for ccgac.bitrix24.site (52.59.124.117)

Host is up (0.18s latency).

rDNS record for 52.59.124.117: ec2-52-59-124-117.eu-central-1.compute.amazonaws.com

Not shown: 65530 filtered tcp ports (no-response)

Bug in http-security-headers: no string output.

PORT STATE SERVICE VERSION

80/tcp open http OpenResty web app server

|_http-fetch: Please enter the complete path of the directory to save data in.

|_http-server-header: Bitrix24.Sites

| http-useragent-tester:

| Status for browser useragent: 200

| Redirected To: https://ccgac.bitrix24.site/

| Allowed User Agents:

| Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)

| libwww

| lwp-trivial

| Python-urllib/2.5

| GT::WWW

| Snoopy

| Zend_Http_Client

| PECL::HTTP

| Change in Status Code:

| http client: 503

| URI::Fetch: 503

| WWW-Mechanize/1.34: 503

| PHP/: 503

| MFC_Tear_Sample: 503
| libcurl-agent/1.0: 503
| PHPCrawl: 503
| HTTP::Lite: 503
|_ Wget/1.13.4 (linux-gnu): 503
|_http-mobileversion-checker: No mobile version detected.
|_http-title: Did not follow redirect to https://ccgac.bitrix24.site/
| http-headers:
| Date: Sun, 22 Sep 2024 15:39:30 GMT
| Content-Type: text/html
| Content-Length: 158
| Connection: close
| Location: https://ccgac.bitrix24.site/
| Server: Bitrix24.Sites
|
|_ (Request type: GET)
| http-sitemap-generator:
| Directory structure:
| Longest directory structure:
| Depth: 0
| Dir: /
| Total files found (by extension):
|_
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-vhosts:
| noc.bitrix24.site
| pbx.bitrix24.site
| syslog.bitrix24.site
| cdn.bitrix24.site : 403

|_124 names had status 302

|_http-feed: Couldn't find any feeds.

|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.

|_http-xssed: No previously reported XSS vuln.

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

|_http-comments-displayer: Couldn't find any comments.

|_http-chrono: Request times for /; avg: 439.60ms; min: 362.00ms; max: 595.00ms

|_http-errors: Couldn't find any error pages.

|_http-date: Sun, 22 Sep 2024 15:39:19 GMT; +5s from local time.

443/tcp open   ssl/http   OpenResty web app server

|_http-chrono: Request times for /; avg: 1720.40ms; min: 1236.00ms; max: 2037.00ms

| ssl-cert: Subject: commonName=*.bitrix24.site

| Subject Alternative Name: DNS:*.bitrix24.site, DNS:bitrix24.site

| Not valid before: 2024-08-29T17:21:45

|_Not valid after: 2025-09-30T17:21:45

|_http-server-header: Bitrix24.Sites

|_http-fetch: Please enter the complete path of the directory to save data in.

|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.

| http-wordpress-enum:

| Search limited to top 100 themes/plugins

| themes

| twentytwelve

| twentyten

| twentythirteen

| twentyfourteen

| twentyfifteen

| responsive

| customizr

| zerif-lite

| virtue

| storefront
| atahualpa
| twentysixteen
| vantage
| hueman
| spacious
| evolve
| colorway
| graphene
| sydney
| ifeature
| mh-magazine-lite
| generatepress
| mantra
| omega
| onetone
| coraline
| pinboard
| thematic
| sparkling
| catch-box
| make
| colormag
| enigma
| custom-community
| mystique
| alexandria
| delicate
| lightword
| attitude
| inove

| magazine-basic
| raindrops
| minamaze
| zbench
| point
| eclipse
| portfolio-press
| twentyseventeen
| travelify
| swift-basic
| iconic-one
| arcade-basic
| bouquet
| pixel
| sliding-door
| pilcrow
| simple-catch
| tempera
| destro
| p2
| sunspot
| sundance
| dusk-to-dawn
| onepress
| moesia
| dynamic-news-lite
| parabola
| optimizer
| one-page
| chaostheory
| business-lite

| duster
| constructor
| nirvana
| sixteen
| esquire
| minimatica
| radiate
| accelerate
| oxygen
| accesspress-parallax
| swift
| spun
| wp-creativix
| suevafree
| hemingway
| pink-touch-2
| motion
| fruitful
| steira
| news
|_ llorix-one-lite
| http-useragent-tester:
| Status for browser useragent: 200
| Allowed User Agents:
| libwww
| Snoopy
| MFC_Tear_Sample
| PHPCrawl
| Wget/1.13.4 (linux-gnu)
| Change in Status Code:
| http client: 503

| Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html): 400
| URI::Fetch: 503
| GT::WWW: 503
| PHP/: 503
| HTTP::Lite: 503
| libcurl-agent/1.0: 503
| Zend_Http_Client: 503
| WWW-Mechanize/1.34: 503
| PECL::HTTP: 503
| Python-urllib/2.5: 503
|_ lwp-trivial: 503
| ssl-enum-ciphers:
| TLSv1.0:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
| TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
| compressors:
| NULL
| cipher preference: server
| warnings:
| 64-bit block cipher 3DES vulnerable to SWEET32 attack
| TLSv1.1:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
| TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
| compressors:
| NULL

```
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|_  least strength: C
|_http-date: Sun, 22 Sep 2024 15:39:15 GMT; +4s from local time.
|_http-title: Cloud Counselage Pvt. Ltd.
| http-backup-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=ccgac.bitrix24.site
|   https://ccgac.bitrix24.site:443/favicon.ico~
|_  https://ccgac.bitrix24.site:443/favicon.ico.~1~
| http-grep:
|   (1) https://ccgac.bitrix24.site:443/:
|     (1) email:
|_      + info@giftacareer.in
|_http-feed: Couldn't find any feeds.
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

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

| http-aspnet-debug:

|_ status: DEBUG is enabled

| http-vhosts:

| corp.bitrix24.site : 400

| test.bitrix24.site : 503

| ssl.bitrix24.site : 502

| 98 names had status 410

| test2.bitrix24.site : 404

| home.bitrix24.site : 404

| pbx.bitrix24.site : 404

| erp.bitrix24.site : 404

| log.bitrix24.site : 404

| development.bitrix24.site : 403

| internet.bitrix24.site : 403

| testing.bitrix24.site : 403

| intra.bitrix24.site : 403

| cdn.bitrix24.site : 403

| eshop.bitrix24.site : 403

| 15 names had status 200

|_www.bitrix24.site : 302 -> https://www.bitrix24.in/

|_http-xssed: No previously reported XSS vuln.

| http-sitemap-generator:

| Directory structure:

| Longest directory structure:

| Depth: 0

| Dir: /

| Total files found (by extension):

|_

| http-errors:

| Spidering limited to: maxpagecount=40; withinhost=ccgac.bitrix24.site

| Found the following error pages:

|

| Error Code: 400

|_ https://ccgac.bitrix24.site:443/

|_http-referer-checker: Couldn't find any cross-domain scripts.

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

|_http-comments-displayer: Couldn't find any comments.

|_http-userdir-enum: Potential Users: root, admin, administrator, webadmin, sysadmin, netadmin, guest, user, web, test

|_http-traceroute: ERROR: Script execution failed (use -d to debug)

| http-waf-detect: IDS/IPS/WAF detected:

|_ccgac.bitrix24.site:443/?p4yl04d3=<script>alert(document.cookie)</script>

| http-headers:

| Date: Sun, 22 Sep 2024 15:39:24 GMT

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

| Connection: close

| Vary: Accept-Encoding

| Server: Bitrix24.Sites

| X-Powered-CMS: Bitrix24.Sites

|

|_ (Request type: HEAD)

| http-robots.txt: 2 disallowed entries

|_/pub/site/* /preview/*

|_http-mobileversion-checker: No mobile version detected.

| http-security-headers:

| Strict_Transport_Security:

|_ HSTS not configured in HTTPS Server

1339/tcp closed kjtsiteserver

1443/tcp closed ies-lm

8895/tcp closed unknown

OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU

No OS matches for host

Network Distance: 5 hops

Host script results:

|_fcrdns: PASS (ec2-52-59-124-117.eu-central-1.compute.amazonaws.com)

|_clock-skew: mean: 4s, deviation: 0s, median: 3s

| resolveall:

| Host 'ccgac.bitrix24.site' also resolves to:

| Use the 'newtargets' script-arg to add the results as targets

|_ Use the --resolve-all option to scan all resolved addresses without using this script.

|_qscan: ERROR: Script execution failed (use -d to debug)

|_path-mtu: ERROR: Script execution failed (use -d to debug)

|_firewalk: ERROR: Script execution failed (use -d to debug)

| port-states:

| tcp:

| open: 80,443

| filtered: 1-79,81-442,444-1338,1340-1442,1444-8894,8896-65535

|_ closed: 1339,1443,8895

|_ipidseq: ERROR: Script execution failed (use -d to debug)

| asn-query:

| BGP: 52.58.0.0/15 | Country: US

| Origin AS: 16509 - AMAZON-02, US

|_ Peer AS: 174 1299 2914 3257 6461

| traceroute-geolocation:

| HOP RTT ADDRESS GEOLOCATION

| 1 3.00 192.168.125.110 - ,-

| 2 21.00 255.0.0.0 - ,-

| 3 17.00 255.0.0.2 - ,-

| 4 19.00 255.0.0.3 - ,-

|_ 5 20.00 ec2-52-59-124-117.eu-central-1.compute.amazonaws.com (52.59.124.117) - ,-

Bug in ip-geolocation-geoplugin: no string output.

| dns-brute:

| DNS Brute-force hostnames:

| cdn.bitrix24.site - 54.217.250.34

|_   *A: 52.59.124.117

| dns-blacklist:

| SPAM

|_   l2.apews.org - FAIL

| whois-ip: Record found at whois.arin.net

| netrange: 52.58.0.0 - 52.59.255.255

| netname: AMAZO-ZFRA

| orgname: A100 ROW GmbH

| orgid: RG-123

|_country: DE

| whois-domain:

|

| Domain name record found at whois.nic.site

|_The queried object does not exist: DOMAIN NOT FOUND\x0D

TRACEROUTE (using port 80/tcp)

HOP RTT   ADDRESS

1   3.00 ms 192.168.125.110

2   21.00 ms 255.0.0.0

3   17.00 ms 255.0.0.2

4   19.00 ms 255.0.0.3

5   20.00 ms ec2-52-59-124-117.eu-central-1.compute.amazonaws.com (52.59.124.117)

Post-scan script results:

| reverse-index:

| 80/tcp: 52.59.124.117

|_ 443/tcp: 52.59.124.117

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 664.83 seconds