



CyberShield

Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: Praktikum 2
Version 1.0



Confidentiality Statement

This document is the exclusive property of CyberShield and TCM Security (FORTIFYTECH). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both CyberShield and FORTIFYTECH.

CyberShield may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. FORTIFYTECH prioritized the assessment to identify the weakest security controls an attacker would exploit. FORTIFYTECH recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

Name	Title	Contact Information
CyberShield		
John	Global Information Security Manager	Email: jsmith@democorp.com
Fortifytech Security		
Jeany Aurellia	Lead Penetration Tester	Email: heath@tcm-sec.com

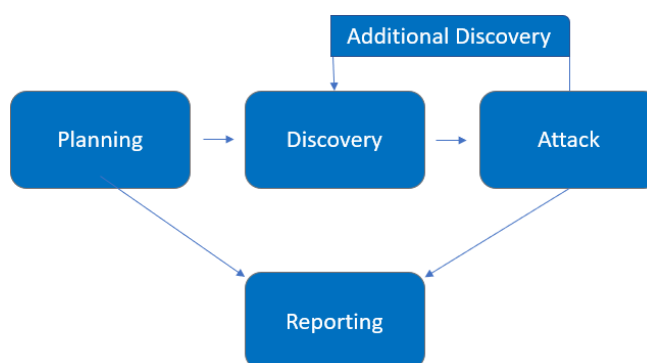


Assessment Overview

From May 5th, 2024 to May 8th, 2024, CyberShield engaged FORTIFYTECH to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment*, OWASP Testing Guide (v4), and customized testing frameworks.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man-in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.



Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.



Scope

Assessment	Details
Internal Penetration Test	10.15.42.36 10.15.42.7

Scope Exclusions

Per client request, FORTIFYTECH did not perform any of the following attacks during testing:

Client Allowances

CyberShield provided FORTIFYTECH the following allowances:

- Internal access to network via ITS VPN or ITS network



Executive Summary

FORTIFYTECH evaluated CyberShield's internal security posture through penetration testing from May 5nd, 2024 to May 8th, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for four (4) days.

Testing Summary

Fortifytech conducted a security assessment of CyberShield's network by performing a comprehensive scan using the Nmap and Nuclei software tools. The purpose of this scan was to identify all open ports on the system, the services running on each port, and potential vulnerabilities that may exist within those services.

Nmap was used to scan all TCP and UDP ports on CyberShield's target system, detect which ports were open, what services were running on each port, and other information such as the operating system and software versions. With this information, Fortifytech could identify potential vulnerabilities based on the software versions and services running. Nuclei, on the other hand, was used to automatically scan for vulnerabilities across various detected web services on CyberShield's system, such as Apache, Nginx, WordPress, and others. Nuclei has a large and continuously updated vulnerability database, allowing it to detect various latest security holes in web applications.

The results from the scans using both tools were then thoroughly analyzed by the Fortifytech team to provide appropriate mitigation recommendations and security improvements to CyberShield. With this comprehensive and structured approach, Fortifytech can assist CyberShield in identifying and addressing vulnerabilities before they can be exploited by malicious actors.



Tester Notes and Recommendations

The Nmap scan on the host with IP 10.15.42.36 revealed some critical security findings. One of the findings was an FTP server running on port 21 that allows anonymous login. This means anyone can connect to the FTP server without any credentials. Even more alarmingly, in the FTP directory, there is a file named "backup.sql" that can be accessed and downloaded by all anonymous users as it has read-write-execute (rwxrwxr-x) permissions. This file potentially contains sensitive or proprietary backup data such as databases storing customer information, financial data, or even critical application source code. This vulnerability exposes the risk of unauthorized access to confidential information by attackers and should be immediately mitigated by disabling anonymous FTP access and protecting critical files such as "backup.sql".

Anonymous access to the FTP server is a high-risk practice and is not recommended at all in a production environment. It provides an avenue for attackers to explore the system and obtain sensitive information with ease. Furthermore, overly permissive read-write-execute access on critical files also increases the risk of data misuse or modification by unauthorized parties. Companies should immediately revise their security policies and implement strict controls to limit access to critical resources only to legitimate users with the required authority. Information security is a shared responsibility and must be prioritized to protect valuable corporate assets.

Key Strengths and Weaknesses

For scoop 10.15.42.7

The following identifies the key strengths identified during the assessment:

1. Open Ports Identified: The scan successfully identified two open ports (22/tcp and 80/tcp) on the target system, which can provide valuable information for further analysis and potential exploitation.
2. Service Versions Detected: The scan detected the specific versions of the services running on the open ports, which can help in identifying potential vulnerabilities associated with those versions.
3. OS Detection: The scan was able to detect the operating system running on the target system, which can provide insights into potential vulnerabilities and assist in tailoring further attacks or exploits.
4. Host Discovery: The scan effectively discovered the target host and its network distance, which can be useful for network mapping and understanding the network topology.

The following identifies the key weaknesses identified during the assessment:

1. Potential Misconfigurations: The warning about unreliable OS scan results due to the inability to find at least one open and one closed port suggests potential misconfigurations or missing security updates on the target system.
2. Limited Information Gathering: While the scan provided some useful information, it may not have gathered comprehensive details about the target system's configuration, running services, and potential vulnerabilities, which could limit the effectiveness of further security assessments or exploitation attempts.



For scoop 10.15.42.36

The following identifies the key strengths identified during the assessment: No major strengths were identified.

The following identifies the key weaknesses identified during the assessment:

1. Port 21 (FTP) is open and running the vsftpd 2.0.8 or later service, which allows anonymous login (FTP code 230).
2. In the FTP directory, there is a file named "backup.sql" that can be accessed and downloaded by all anonymous users as it has read-write-execute (rwxrwxr-x) permissions. This file potentially contains sensitive or proprietary backup data.
3. Port 8888 is open and running Apache httpd 2.4.38, displaying a login page, which could be a target for brute-force attacks or exploitation of vulnerabilities in that Apache version.

To mitigate these security weaknesses, it is recommended to:

1. Disable anonymous FTP access and protect critical files such as "backup.sql".
2. Tighten access controls and follow security best practices in managing the SSH service.
3. Update the Apache version or disable the service if it is not required.
4. Perform regular vulnerability scanning and address any identified vulnerabilities.
5. Implement additional security controls such as firewalls, IPS/IDS, and other security solutions.



Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

13	5	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
<u>Internal Penetration Test</u>		
Anonymous FTP access allowed with sensitive file exposure	High	<ul style="list-style-type: none">• Disable anonymous FTP access immediately.• Remove or restrict access to sensitive files like "backup.sql".• Implement secure file transfer mechanisms with proper access controls.
Outdated Apache HTTP Server version	Moderate	<ul style="list-style-type: none">• Update Apache HTTP Server to the latest stable version• Apply latest security patches and configurations• Disable the service if it is not required.
Potential Misconfiguration or Missing Updates	Moderate	<ul style="list-style-type: none">• Review the system configuration and ensure that all required ports are properly configured and accessible as intended.• Regularly apply security updates and patches to the operating system and all installed software to mitigate potential vulnerabilities.• Implement a robust patch management process to ensure timely installation of security updates.• Consider implementing additional security controls, such as a firewall or intrusion detection/prevention system (IDS/IPS), to enhance the overall security posture.



Technical Findings

Internal Penetration Test Findings

Anonymous FTP access allowed with sensitive file exposure (High)

Description:	The scan revealed that the FTP server allows anonymous access without any credentials. Furthermore, a sensitive file named "backup.sql" with read-write-execute permissions can be accessed and downloaded by anonymous users through this FTP server.
Risk:	<p>Likelihood: High – This attack is effective in environments where anonymous FTP access is allowed and sensitive files are exposed.</p> <p>Impact: Very High – Anonymous FTP access with sensitive file exposure can lead to unauthorized access to confidential data, intellectual property theft, and potential data breaches, resulting in significant financial and reputational damage.</p>
System:	10.15.42.36
Tools Used:	Nmap, Nuclei
References:	OWASP Top 10 2021 - A5: Security Misconfiguration CIS Controls v8 - Control 14: Access Control Management

Evidence

```
➜ $ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:rea): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Figure 1 : Login as anonymous

```
ftp> ls
229 Entering Extended Passive Mode (|||65506|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
```

Figure 2 : Access file backup.sql



```
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

Figure 3 : contents of backup.sql

Remediation

- Disable anonymous FTP access entirely if it's not required for business operations.
- If anonymous FTP access is required, configure the FTP server to restrict access to specific directories and files that do not contain sensitive information.
- Implement strict file permissions and ownership on the FTP server to prevent unauthorized access to sensitive files.



Outdated Apache HTTP Server version

Description:	An outdated version of the Apache HTTP Server is being used, which may contain known vulnerabilities and security flaws that have been addressed in later versions. Failing to keep the web server software up-to-date exposes the system to potential attacks and exploits.
Risk:	<p>Likelihood: High – Outdated software is a common attack vector, and hackers actively scan for and exploit known vulnerabilities in older versions.</p> <p>Impact: High – A successful attack on an outdated web server can lead to data breaches, website defacement, remote code execution, and other severe consequences.</p>
System:	Apache HTTP Server is a widely used open-source web server software, powering a significant portion of websites on the internet.
Tools Used:	Nmap, Nuclei
References:	https://httpd.apache.org/security/ https://www.cvedetails.com/product/66/Apache-Http-Server.html?vendor_id=45

Evidence

```
|_http-title: Login Page
|_http-server-header: Apache/2.4.38 (Debian)
```

Figure 4 : Apache version outdate

Remediation

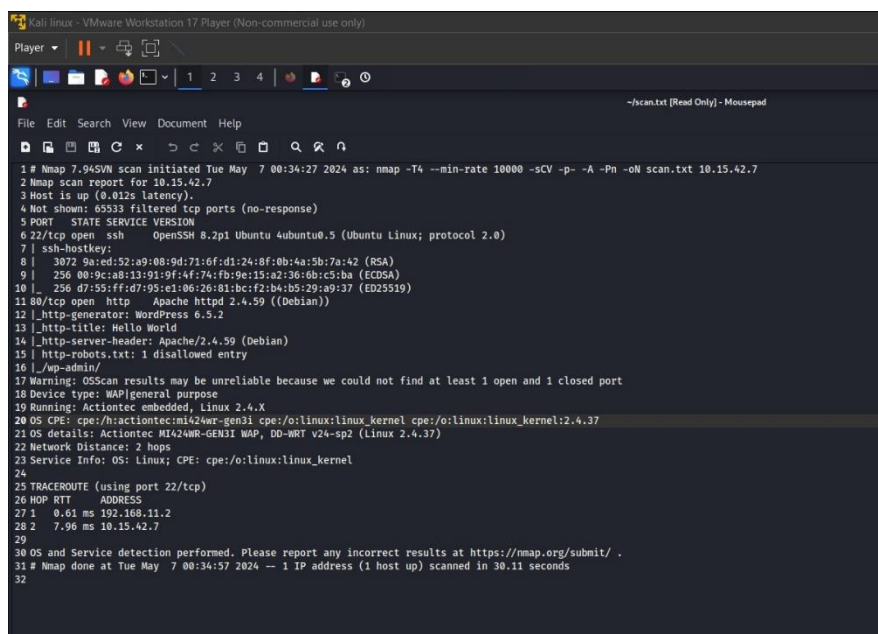
- Regularly update the Apache HTTP Server to the latest stable version, which includes security patches and bug fixes.
- Enable automatic updates or set up a process for regularly monitoring and installing updates as soon as they are released.
- Review the Apache HTTP Server release notes and security advisories for any specific configuration changes or additional steps required after updating.
- Disable or remove any unnecessary modules or features from the Apache HTTP Server to reduce the attack surface



Potential Misconfiguration or Missing Updates

Description:	A potential misconfiguration or missing security updates can leave a system vulnerable to various security threats. When a system is not configured properly or lacks the latest security patches, attackers can exploit known vulnerabilities to gain unauthorized access, execute malicious code, or compromise the system's integrity.
Risk:	<p>Likelihood: High - Misconfigured systems and outdated software are common targets for attackers, as they provide easy entry points for exploitation.</p> <p>Impact: High - A successful exploitation can lead to data breaches, system compromise, unauthorized access, and other severe consequences, potentially causing significant financial and reputational damage.</p>
System:	All
Tools Used:	Nmap, Nuclei
References:	https://www.cisa.gov/uscert/ncas/tips/ST04-006

Evidence



```
1 # Nmap 7.94SVN scan initiated Tue May 7 00:34:27 2024 as: nmap -T4 --min-rate 10000 -sCV -p- -A -Pn -oN scan.txt 10.15.42.7
2 Nmap scan report for 10.15.42.7
3 Host is up (0.012s latency).
4 Not shown: 65533 filtered tcp ports (no-response)
5 PORT      STATE SERVICE VERSION
6 22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
7 | ssh-hostkey:
8 |   3072 9a:ed:07:a9:08:9d:71:0f:d1:24:8f:0b:4a:5b:7a:52 (RSA)
9 |   256 00:9c:a8:33:91:9f:4f:76:9e:15:a2:36:6b:c5:ba (ECDSA)
10 |   256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:37 (ED25519)
11 80/tcp    open  http     Apache httpd 2.4.59 ((Debian))
12 |_http-generator: WordPress 6.5.2
13 |_http-title: Hello World
14 |_http-server-header: Apache/2.4.59 (Debian)
15 |_http-robots.txt: 1 disallowed entry
16 |_wp-admin/
17 Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
18 Device type: WAP|general purpose
19 Running: Actiontec embedded, Linux 2.4.X
20 OS CPE: cpe:/o:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37
21 OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37)
22 Network Distance: 2 hops
23 Service Info: OS: Linux; CPE: o:linux:linux_kernel
24
25 TRACEROUTE (using port 22/tcp)
26 HOP RTT ADDRESS
27 1 0.61 ms 192.168.11.2
28 2 7.96 ms 10.15.42.7
29
30 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
31 # Nmap done at Tue May 7 00:34:57 2024 -- 1 IP address (1 host up) scanned in 30.11 seconds
32
```

Figure 5: nmap scan of IP 10.15.42.7

Remediation

- Regularly review system configurations and ensure that all required ports are properly configured and accessible as intended.
- Implement a robust patch management process to ensure timely installation of security updates and patches for the operating system, applications, and all installed software.
- Subscribe to security advisories and vulnerability notifications from vendors and trusted sources to stay informed about the latest threats and available updates.



-
- Conduct regular vulnerability assessments and penetration testing to identify potential misconfigurations or missing updates.
 - Consider implementing additional security controls, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and security information and event management (SIEM) solutions, to enhance the overall security posture.
 - Develop and enforce strong security policies and procedures, including regular system hardening, least privilege principles, and secure configuration guidelines.

Additional Scans and Reports

FORTIFYTECH provides all clients with all report information gathered during testing. This includes Nmap files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by TCM Security.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled “Additional Scans and Reports”.



Last Page