Fortify Tech
Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: DC-001
Version 1.0

Table of Contents

Contents

Confidentiality Statement

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

FortifyTech 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. CyberShield prioritized the assessment to identify the weakest security controls an attacker would exploit. CyberShield recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

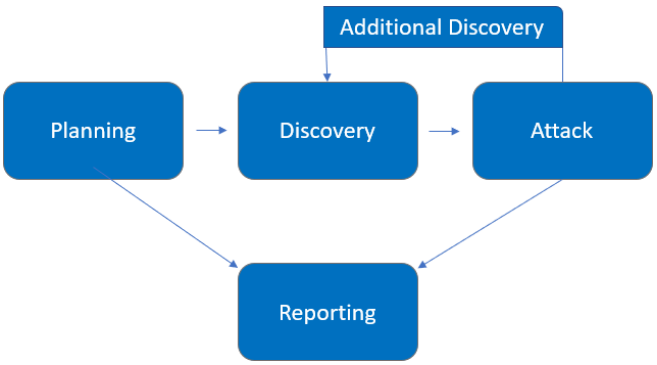
Name	Title	Contact Information
FortifyTech		
John Smith	Global Information Security Manager	Email: jsmith@fortifytech.com
CyberShield		
Gavriel Pramuda K.	Penetration Tester	Email: gavriel.k.adi12@gmail.com

Assessment Overview

From May 5th, 2024 to May 8th, 2024, Fortify Tech engaged CyberShield 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. 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 and 10.15.42.7

Scope Exclusions

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

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by FortifyTech.

Client Allowances

FortifyTech provided CyberShield the following allowances:

- Internal access to network via port allowances

Executive Summary

CyberShield evaluated Fortify Tech's internal security posture through penetration testing from May 5th, 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 three (3) business days.

Testing Summary

The CyberShield team has completed evaluating the internal network security of FortifyTech. From an internal perspective, the CyberShield team conducted vulnerability scanning against all IPs provided by FortifyTech to assess the overall patching health of the network. The team performed scanning by conducting reconnaissance, vulnerability testing, and searching for public exploits or CVEs.

From the scanning conducted, the CyberShield team discovered an endpoint named /server-status at IP 10.15.42.36 (IPT-004). The CyberShield team also found a login page (IPT-003) that allows brute force attempts to obtain credentials and access the next page. Additionally, the CyberShield team also found an open FTP located at IP 10.15.42.36 that can be accessed directly (IPT-002). From this FTP, a file containing credentials (IPT-001) to access the login page was also found.

The remainder of the findings were high, moderate, low, or informational. For further information on findings, please review the Technical Findings section.

Tester Notes and Recommendations

During the testing, one consistent finding was the presence of weak password policies. Weak password policies lead to initial compromise of accounts and are typically one of the first footholds attempted by attackers in a network.

We recommend that Fortify Tech reassess its current password policies and consider implementing a policy requiring passwords to be at least 12 characters long, including uppercase letters, symbols, and numbers to make them harder to crack.

Additionally, during the testing, a port leading to the login page was discovered that should not have been accessible. This port should not be discoverable during scanning as it represents a significant vulnerability in Fortify Tech's website.

We recommend that Fortify Tech reassess the open port leading to the login page with consideration for implementing a firewall. A firewall can act as the first line of defense by monitoring and controlling incoming and outgoing traffic, thus minimizing the risk of attacks.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Usage of comprehensive scanning techniques
2. Detection of vulnerable endpoints
3. Discovery of open FTP scanning

The following identifies the key weaknesses identified during the assessment:

1. Password is too weak
2. Network information can be easily accessed
3. Some page access is too easily accessible by anyone

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

1	0	1	1	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Insufficient Password Complexity	Critical	Implement a stronger password
IPT-002: Anonymous FTP Access	Moderate	Disable anonymous logins
IPT-003: Get status-server Page	Low	Review server-status page access
IPT-004: Get Login Page	Informational	Review action and remediation steps.

Technical Findings

Internal Penetration Test Findings

Finding IPT-001: Insufficient Password Complexity

Description:	There is a file named backup.sql in the FTP server. In that file, the CyberShield team found a SQL command that contains username and hashed password. The hashed password can be cracked using a tool named John the Ripper in approximately 2 hours.
Risk:	Likelihood: High - Simple passwords are susceptible to password cracking attacks. Encryption provides some protection, but dictionary attacks base on common word lists often crack weak passwords. Impact: Very High - Domain admin accounts with weak passwords could lead to an adversary critically impacting FortifyTech ability to operate.
System:	All
Tools Used:	Responder, John the Ripper
References:	Modul Ethical Hacking

Evidence

```
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 1: SQL command contains username and password

```
┌──(zacriel㉿Gavriel)-[~/ethack]
└─$ cat hash_sql.txt
$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K
```

Figure 2: Captured hash of "admin"

```
┌──(root㉿Gavriel)-[/home/zacriel/ethack]
└─# john hash_sql.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:18:19 1.23% (ETA: 2024-05-09 00:59) 0g/s 190.2p/s 190.2c/s 190.2C/s 123abc*..12101978
0g 0:00:18:20 1.24% (ETA: 2024-05-09 01:00) 0g/s 190.2p/s 190.2c/s 190.2C/s 12101976..112374
0g 0:00:18:22 1.24% (ETA: 2024-05-09 01:00) 0g/s 190.2p/s 190.2c/s 190.2C/s 08800880..071609
0g 0:00:18:24 1.24% (ETA: 2024-05-09 01:00) 0g/s 190.3p/s 190.3c/s 190.3C/s 03042529..0123210
0g 0:00:18:25 1.24% (ETA: 2024-05-09 00:59) 0g/s 190.3p/s 190.3c/s 190.3C/s zxcvbnm...yovanka
0g 0:00:39:47 2.61% (ETA: 2024-05-09 01:38) 0g/s 182.4p/s 182.4c/s 182.4C/s aliosha..alexparks
0g 0:00:40:13 2.63% (ETA: 2024-05-09 01:57) 0g/s 181.5p/s 181.5c/s 181.5C/s MONEY14..MARYFER
0g 0:00:40:16 2.63% (ETA: 2024-05-09 01:58) 0g/s 181.4p/s 181.4c/s 181.4C/s Love1234..LISALISA
0g 0:00:42:23 2.71% (ETA: 2024-05-09 02:31) 0g/s 177.9p/s 177.9c/s 177.9C/s 041068..03282008
0g 0:00:45:34 2.96% (ETA: 2024-05-09 02:07) 0g/s 180.1p/s 180.1c/s 180.1C/s limonnkim..lilrob14
kiseki666        (admin)
1g 0:02:16:56 DONE (2024-05-08 02:44) 0.000121g/s 196.7p/s 196.7c/s 196.7C/s kiseki666..kirstyleanne
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Figure 3: Password cracking

Remediation

Leaked username and hashed password in backup.sql are a security risk. Secure the file and rotate passwords. Two-factor authentication and data encryption can add further protection.

Finding IPT-002: Anonymous FTP Access

Description:	The CyberShield team discovered an open FTP that can be accessed directly, When connected to this FTP, the team found a file named *backup.sql* that can be downloaded. Inside the file, there are credentials including a username and hashed password, which can be used on the login page described earlier.
Risk:	Likelihood: High – With the simple access for FTP, it can be access easily by any attacker Impact: High – If the attacker can access and get the file from FTP, it can be encrypted so the password for user can be accessed
System:	10.15.42.36
Tools Used:	nmap, ftp
References:	Modul Ethical Hacking

Evidence

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.33.1.240
|      Logged in as ftp
|      TYPE: ASCII
|      Session bandwidth limit in byte/s is 6250000
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.18.0.3 is not the same as 10.15.42.36
```

Figure 4: Using nmap for scanning

```
┌──(zacriel㉿Gavriel)-[~]
└─$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:zacriel): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||65506|)
150 Here comes the directory listing.
drwxrwxr-x    2 ftp      ftp          4096 May 04 15:40 .
drwxrwxr-x    2 ftp      ftp          4096 May 04 15:40 ..
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> mget *
mget backup.sql [anpqy?]? y
229 Entering Extended Passive Mode (|||65507|)
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% |*****************************************************************************************************|  1997        8.98 MiB/s    00:00 ETA
226 Transfer complete.
1997 bytes received in 00:00 (22.33 KiB/s)
ftp> quit
221 Goodbye.
```

Figure 5: Opening the FTP server

Remediation

To enhance security, it's advisable to disable anonymous logins, which would prevent unauthorized users from accessing the system without proper authentication.

Finding IPT-003: Get status-server Page

Description:	The status-server page was found on IP 10.15.42.36 with port 8888 on the system. The page can be accessed using the server-status endpoint. However, higher access is required to view the contents of the page.
Risk:	Likelihood: Moderate – Status server may be not important and interesting for every attacker Impact: Moderate – With status server, attacker may be getting some information for this system
System:	10.15.42.36
Tools Used:	Gobuster
References:	Modul Ethical Hacking

Evidence

```
┌──(root㉿Gavriel)-[/home/zacriel/KaliLists/dirbuster]
└─# gobuster dir -u http://10.15.42.36:8888/ -w /home/zacriel/KaliLists/dirbuster/directory-list-2.3-medium.txt -o /
home/zacriel/output.log
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.15.42.36:8888/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/zacriel/KaliLists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 403) [Size: 278]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

Figure 6: Found another directory named "server-status"

Remediation

Please conduct a thorough review of access permissions and security measures related to the server-status page to ensure that it is adequately protected from unauthorized access or exploitation.

Finding IPT-004: Steps to Get Login Page (Informational)

The steps below describe how the penetration tester obtained login page access. Each step also provides remediation recommendations to help mitigate risk.

Step	Action	Remediation
1	Nmap for open port	Add firewall
2	Access the open port with 10.15.42.38:port	Add firewall

Remediation

Review action and remediation steps.

Last Page