Fortify Tech
Security Assessment Findings Report

Business Confidential

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

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

Contact Information

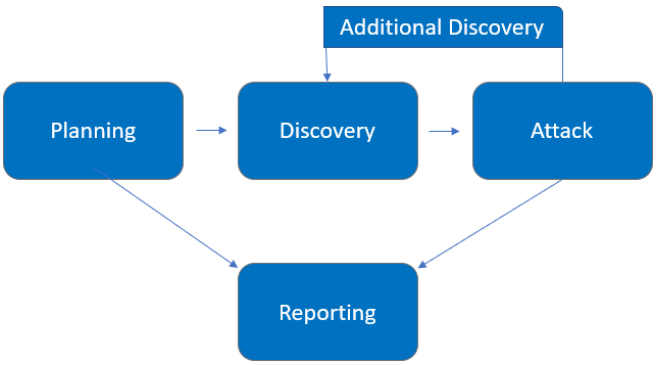
Name	Title	Contact Information
FortifyTech		
John Smith	Global Information Security Manager	Email: jsmith@fortifytech.com
CyberShield		
Muhammad Harvian Dito Syahputra	Penetration Tester	Email: harviandito20@gmail.com

Assessment Overview

From May 22 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, 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, 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

0	0	1	1	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Anonymous FTP Access	Moderate	Disable anonymous logins
IPT-002: Get status-server Page	Low	Review server-status page access
IPT-003: Get Login Page	Informational	Review action and remediation steps.

Technical Findings

Internal Penetration Test Findings

Finding IPT-001: 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

```
┌──(root㉿kali)-[/home/aveee]
└─# cat backup.sql
-- MySQL dump 10.13  Distrib 8.0.36, for Linux (x86_64)
--
-- Host: localhost    Database: db
-- ------------------------------------------------------
-- Server version       8.0.36-0ubuntu0.22.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `users`
--

DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int NOT NULL,
  `username` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `users`
--

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: The information in backup.sql

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-002: 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:	Module Ethical Hacking

Evidence

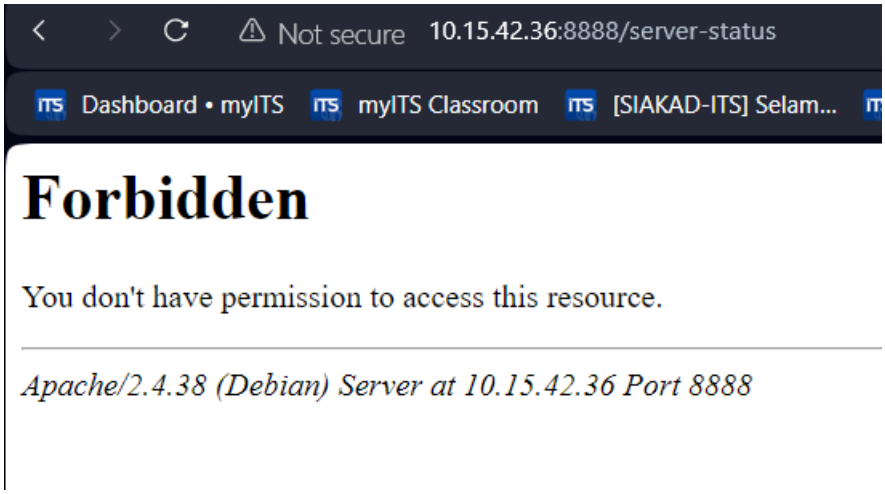


Figure 2: Access for status-server page

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-003: 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