FORTIFYTECH
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 FortifyTech and TCM Security (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

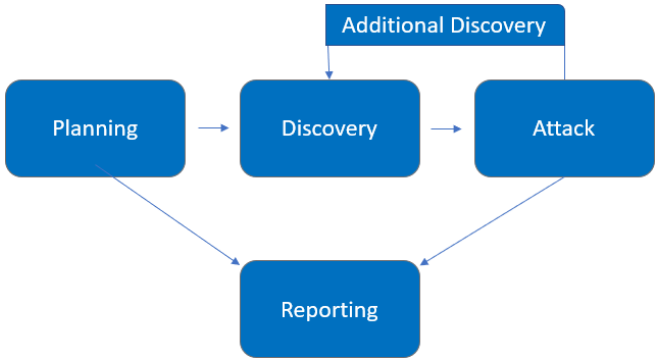
Name	Title	Contact Information
FortifyTech		
John Smith	Global Information Security Manager	Email: jsmith@democorp.com
CyberShield Security		
Monika Damelia Hutapea	Lead Penetration Tester	Email: 5027221011@student.its.ac.id.com

Assessment Overview

From May 5nd, 2024 to May 8th, 2024, FortifyTech 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:

- Anything that violates ethical hacking

All other attacks not specified above were permitted by FortifyTech.

Client Allowances

FortifyTech provided CYBERSHIELD the following allowances:

- Internal access to network via VPN ITS or ITS Network

Executive Summary

CYBERSHIELD evaluated FortifyTech's internal security posture through penetration testing from May 5th, 2024 to March 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) business days.

Testing Summary

The penetration testing of FortifyTech's infrastructure, undertaken by CyberShield security consultants, revealed several significant findings. Employing Nmap and FTP, the assessment identified vulnerabilities and potential risks within the system. Notably, examination uncovered an open FTP port with anonymous login capabilities on IP address 10.15.42.36. Despite successful access, a discrepancy in the PASV IP configuration was detected, indicating a potential security lapse. Furthermore, SSH and HTTP services were found open, suggesting various avenues for exploitation. Therefore, the focus of attention lies primarily on addressing vulnerabilities present in other parts of the infrastructure.

Tester Notes and Recommendations

To address the vulnerabilities identified during the penetration testing, CyberShield security consultants recommend prompt action in several key areas. Firstly, it is imperative to address the PASV IP mismatch detected in the FTP configuration, ensuring data connections are established securely. Secondly, a thorough review of the FTP server configuration is advised to enhance security measures, particularly concerning anonymous login permissions. Additionally, measures should be implemented to secure the HTTP login page found on port 8888/tcp to prevent unauthorized access. Lastly, regular security audits are essential to continuously evaluate and strengthen FortifyTech's infrastructure against evolving cyber threats.

Key Strengths and Weaknesses

For IP Address 10.15.42.36

The following identifies the key strengths identified during the assessment:

Strengths:

1. The scan was able to identify the open ports and services running on the target system, providing valuable information for further analysis and exploitation attempts.
2. The version information of the SSH and HTTP services was determined, allowing for research on potential vulnerabilities associated with those specific versions.

3. The operating system was guessed to be Linux, potentially running on a virtualization platform like Oracle VirtualBox or QEMU, providing insights into the target environment.

Weaknesses:

1. The FTP server (vsftpd 2.0.8 or later) is running and allows anonymous login, which is a critical security vulnerability that exposes sensitive data and potentially grants unauthorized access.
2. The PASV IP mismatch detected in the FTP configuration indicates a potential issue with the data connections, which could lead to data leakage or man-in-the-middle attacks.
3. The HTTP service running on port 8888 has a login page accessible, and if not properly secured, it could serve as an entry point for unauthorized access.
4. The scan results indicate that the test conditions were non-ideal, potentially affecting the accuracy of the operating system and service detection.

For IP Address 10.15.42.36

The following identifies the key strengths identified during the assessment:

Strengths:

1. The scan identified an open HTTP service running on port 80, indicating the presence of a web server.
2. The web server was identified as Apache httpd 2.4.59 running on Debian, providing valuable information for further analysis and potential exploitation.
3. The scan detected that the web server is running WordPress 6.5.2, which allows for researching known vulnerabilities associated with that specific version.

Weaknesses:

1. The scan revealed that the /wp-admin/ directory is disallowed in the robots.txt file, suggesting that the WordPress administration area may be accessible and could be a potential entry point for unauthorized access.
2. The test conditions were reported as non-ideal, which may affect the accuracy of the operating system and service detection.
3. No specific vulnerabilities were identified during the scan, but further testing and enumeration may be required to uncover potential weaknesses in the web server or WordPress installation.

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
IPT-001: Anonymous login via FTP on IP Address 10.15.42.36	High	Disable the anonymous login option on FTP services
IPT-002: Vulnerability in IP Address 10.15.42.7 running WordPress 6.5.2	Moderate	Update Wordpress to the latest version and implement effective security plugins to protect against xss attacks.

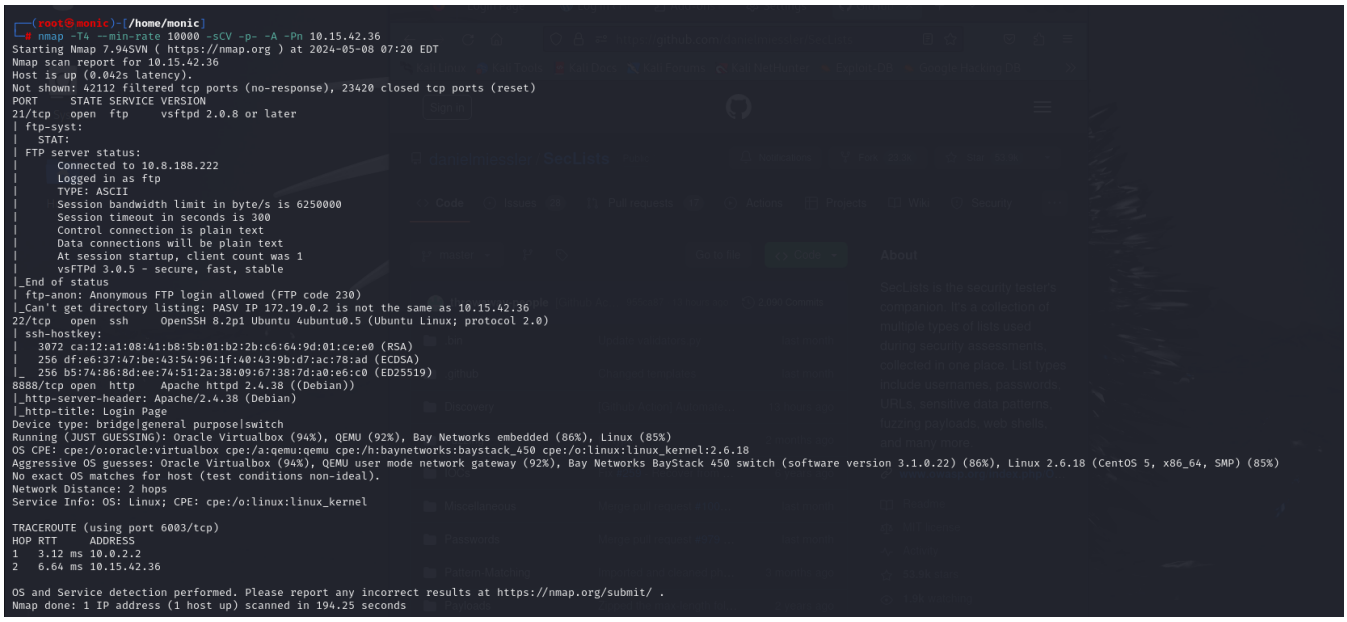
Technical Findings

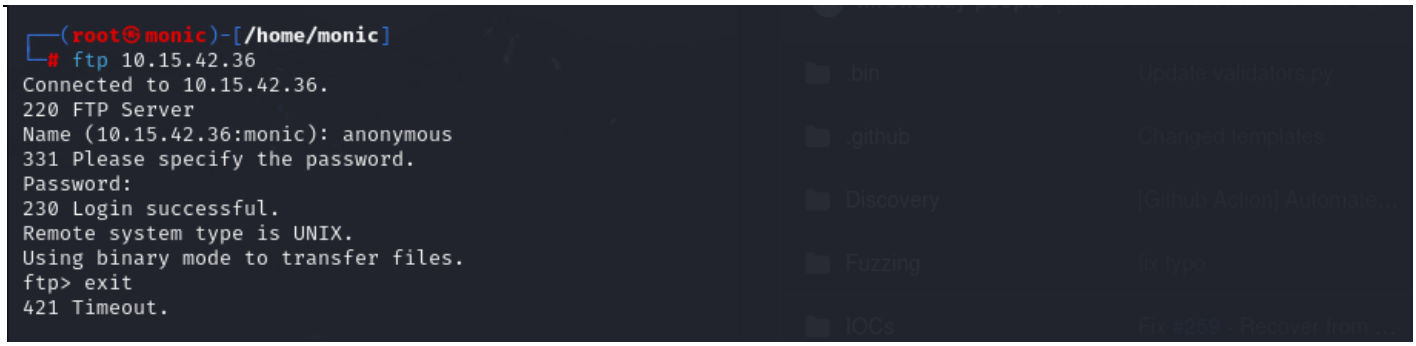
Internal Penetration Test Findings

Finding IPT-001: Anonymous login via FTP on IP Address 10.15.42.36 (High)

Description:	The Nmap scan revealed that the FTP server (vsftpd 2.0.8 or later) running on port 21 of the host with IP 10.15.42.36 allows anonymous login. This configuration bypasses authentication mechanisms and grants unrestricted access to the FTP server, potentially exposing sensitive data and system files.
Risk:	Likelihood: Moderate – Allowing anonymous FTP access is a significant security risk, as it is a common attack vector that is easily exploitable by malicious actors but need higher skills to exploit attacks. Impact: High – Anonymous FTP access permits unauthorized access to the system, enabling attackers to explore and potentially compromise sensitive data, exfiltrate files, distribute malware, and gain a foothold for pivoting and lateral movement within the network..
System:	All
Tools Used:	Nmap on Kali Linux

Evidence





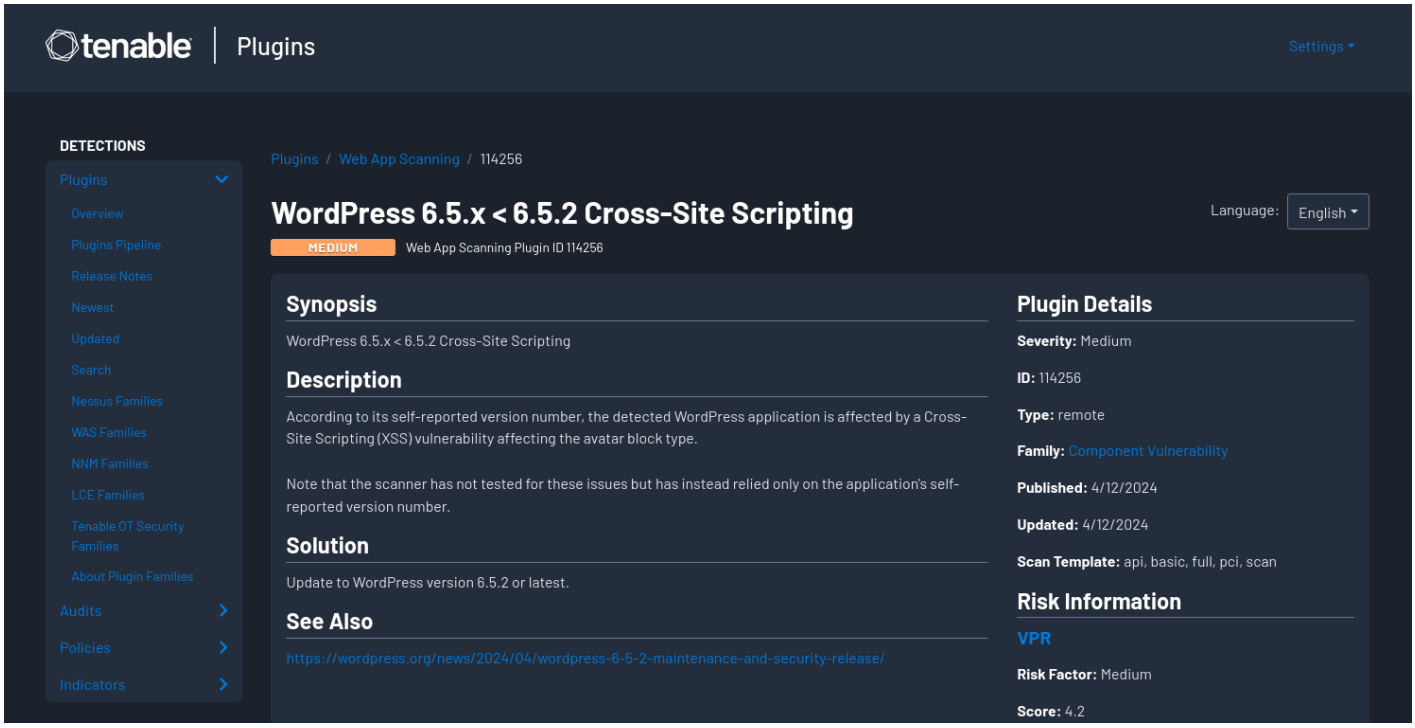
Remediation

To remediate the anonymous FTP login vulnerability on 10.15.42.36, FortifyTech must promptly disable anonymous access, enforce strong authentication, restrict FTP access, harden the server configuration, enable secure protocols, regularly patch and update, implement logging and monitoring, enforce least privilege access controls, and conduct routine security audits..

Finding IPT-002: XSS vulnerability in 10.15.42.7 running WordPress 6.5.2(Moderate)

Description:	The Nmap scan revealed an HTTP service running on port 80, identified as Apache httpd 2.4.59 (Debian). The server is hosting a WordPress installation, version 6.5.2, as indicated by the "http-generator" header. The scan also detected that the "/wp-admin/" directory is disallowed in the robots.txt file, suggesting that the WordPress administration area may be accessible.
Risk:	Likelihood: Moderate – WordPress installations are commonly targeted by attackers due to their widespread use and the availability of various exploit techniques and tools. Impact: Moderate – If the WordPress installation is not properly secured and updated, it could be vulnerable to various attacks such as data loss or takeover of control by other system.
System:	All
Tools Used:	Nmap on Kali Linux

Evidence



Remediation

To remediate the risks associated with the WordPress installation on the host with IP 10.15.42.7, FortifyTech should promptly implement the following measures: ensure the WordPress core, plugins, and themes are up-to-date with the latest security patches; enforce strong authentication mechanisms and access controls; configure a web application firewall to protect against common attacks; regularly review and update WordPress security configurations; and conduct routine security audits and vulnerability assessments to identify and address any emerging threats.

Last Page