FortifyTech

Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project:
Version 1.0

Table of Contents

Confidentiality Statement

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

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

Contact Information

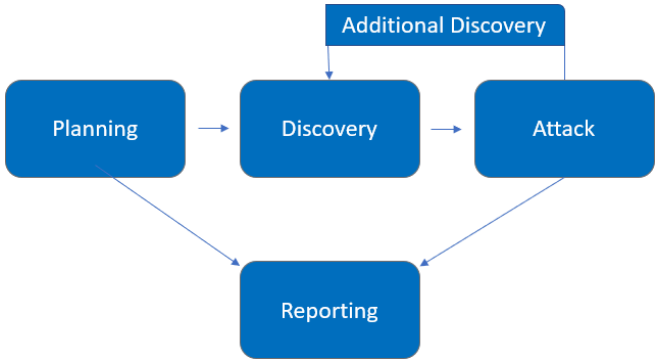
Name	Title	Contact Information
FortifyTech		
Aslab Ethack		Email:
Practitioner		
Rehana Putri Salsabilla	an ethical hacking practitioner	NRP : 5027221015 Email: rehanaputri814@gmail.com

Assessment Overview

From May 5nd, 2024 to May 8th, 2024, FortifyTech engaged Practitioner 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 - used as login purposes • 10.15.42.7 - used as a landing page with wordpress as it's framework

Scope Exclusions

During the testing phase, FortifyTech did not enforce restrictions against certain types of attacks.

Client Allowances

FortifyTech tidak mengadakan program apapun yang memberikan CyberShield sebagai tambahan keuntungan kepada karyawannya.

Executive Summary

Practitioner evaluated FortifyTech 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 business days.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools (Nessus)
2. Mimikatz detected on some machines
3. Service accounts were not running as domain administrators
4. Demo Corp local administrator account password was unique to

each device The following identifies the key weaknesses identified during

the assessment:

1. Password policy found to be insufficient
2. Critically out-of-date operating systems and weak patching exist within the network
3. Passwords were observed in cleartext due to WDigest
4. LLMNR is enabled within the network
5. SMB signing is disabled on all non-server devices in the work
6. IPv6 is improperly managed within the network
7. User accounts can be impersonated through token delegation
8. Local admin accounts had password re-use and were overly permissive
9. Default credentials were discovered on critical infrastructure, such as iDRACs
10. Unauthenticated share access was permitted
11. User accounts were found to be running as service accounts
12. Service accounts utilized weak passwords
13. Domain administrator utilized weak passwords

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

External Penetration Test		
Anonymous FTP is enabled	Medium	Disable anonymous FTP access on the FTP server to prevent unauthorized users from accessing the system without authentication
Vulnerable to Terrapin	Medium	ensure WordPress is updated to version 4.7.1 or later to patch the vulnerability.
WordPress Username Enumeration	Medium	update affected SSH implementations, including OpenSSH, to version 9.6 or later, or apply patches provided by vendors as soon as they become available

Technical Findings

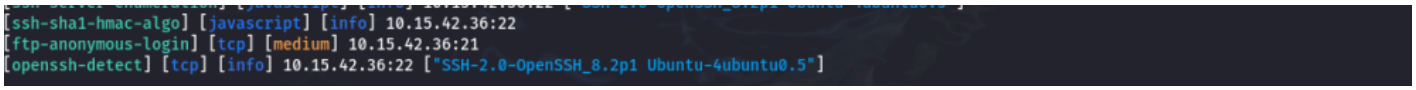
FTP Server Detection

An FTP server is listening on a remote port. It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Vulnerable to Terappin

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack.

Evidence

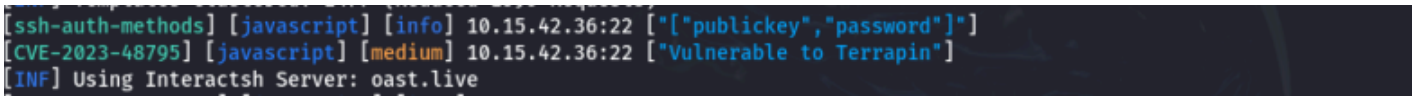


Exploitation Proof of Concept

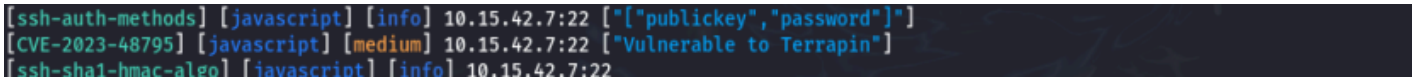
- I successfully gained access to the FTP server of 10.15.42.36 using the command [ftp 10.15.42.36]

Evidence

Evidence



Evidence



CVE-2023-48795 - Vulnerable to Terappin (Medium)

• **Description:**	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2

	6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.
• **Impact:**	Medium
• **System:**	10.15.42.7 10.15.42.36:22
• **References:**	

FTP Server Detection (Medium)

• **Description:**	An FTP server is listening on a remote port.
• **Impact:**	Medium
• **System:**	10.15.42.36
• **References:**	

Server Leaks Version Information via "Server" HTTP Response Header Field (Low)

• **Description:**	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
• **Impact:**	Low
• **System:**	10.15.42.7 10.15.42.36:8888
• **References:**	

Additional Scans and Reports

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

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