FortifyTech
Security Assessment Findings Report

BUSINESS CONFIDENTIAL

Date: May 8th, 2021
Project: Modul-1
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. 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

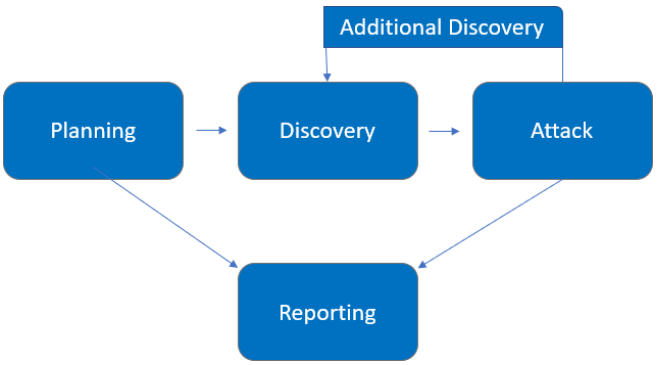
Name	Title	Contact Information
FortifyTech		
John Smith	Global Information Security Manager	Email: jsmith@democorp.com
CyberShield		
Ilhan Ahmad Syafa	Lead Penetration Tester	Email: ilhan@cybershield.com

Assessment Overview

From May 5th, 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	10.15.42.7 10.15.42.36

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:

- Access to IP Adress via ITS network Wi-Fi

Executive Summary

CyberShield evaluated FortifyTech'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 four (4) business days.

Testing Summary

I've identified a vulnerability in an IP address where an external party can gain access through a port. This breach poses a potential security risk, as it could allow unauthorized individuals to infiltrate the system and potentially compromise sensitive information. It's crucial to address this vulnerability promptly by implementing appropriate security measures and patching the port to prevent any unauthorized access and safeguard the integrity of the system.

Tester Notes and Recommendations

After identifying a vulnerability in an IP address allowing external access through a specific port, it's critical to promptly patch the port to prevent unauthorized entry. Implementing a firewall configuration to restrict access solely to authorized connections can significantly reduce the risk of exploitation. Regular security audits and vulnerability assessments should be conducted to proactively identify and address any potential weaknesses. Robust access control measures, including strong authentication mechanisms and least privilege principles, must be implemented to limit access to sensitive systems. Continuous monitoring of network traffic and system logs is essential to detect and respond to any suspicious activities promptly. Comprehensive employee training on cybersecurity best practices and the importance of promptly reporting vulnerabilities is crucial. Additionally, developing an incident response plan and engaging cybersecurity experts can further enhance the security posture of the system.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Slug readme cannot accessed publicly, so the attacker didn't get enough detail informations about the wordpress template

The following identifies the key weaknesses identified during the assessment:

1. Slug login can be known and accessed publicly by accessing port 8888
2. A username "admin" known as the only one credentials. So, in order to get the password, attackers can simply brute force it

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	0	0	1	7
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Found http://10.15.42.7/robots.txt		
Found http://10.15.42.7/license.txt		
Found http://10.15.42.7/ [http://10.15.42.7/wp-includes/blocks/navigation/view.min.js?ver=6.5.2]		
Found http://10.15.42.7/xmlrpc.php		
Found http://10.15.42.7/readme.html		

Found http://10.15.42.7/wp-json/wp/v2/users/ [admin]		
Found http://10.15.42.7/wp-login.php		
Found http://10.15.42.7/?author=1 [author/admin]		

Technical Findings

Internal Penetration Test Findings

Found openssh address

Description:	Upon investigation, we have discovered an open access point to OpenSSH on the IP address 10.15.42.7, specifically through port 22. This revelation poses a significant security concern as OpenSSH, a widely used remote administration tool, could potentially provide unauthorized individuals with a gateway to the system. Such access could lead to a variety of malicious activities, including unauthorized data retrieval, system manipulation, or even complete network compromise. Given the critical role of SSH in remote system administration, securing this access point is paramount to safeguarding the integrity and confidentiality of the system's data and operations. Immediate action is required to address this vulnerability, including implementing stringent access controls, patching any known security flaws in the SSH configuration, and monitoring network traffic for any suspicious activities. Additionally, it is essential to conduct a comprehensive security audit to identify any other potential vulnerabilities within the system and to ensure that appropriate measures are in place to mitigate them effectively. Failure to address this issue promptly could leave the system vulnerable to exploitation and compromise its overall security posture.
Risk:	Likelihood: High – This attack potentially intended to brute force password in order to get accessed by OpenSSH to that IP address and port Impact: Very High – Attackers can take over a website and destroy the contents for their own benefit.
System:	All
Tools Used:	OpenSSH
References:	

Evidence

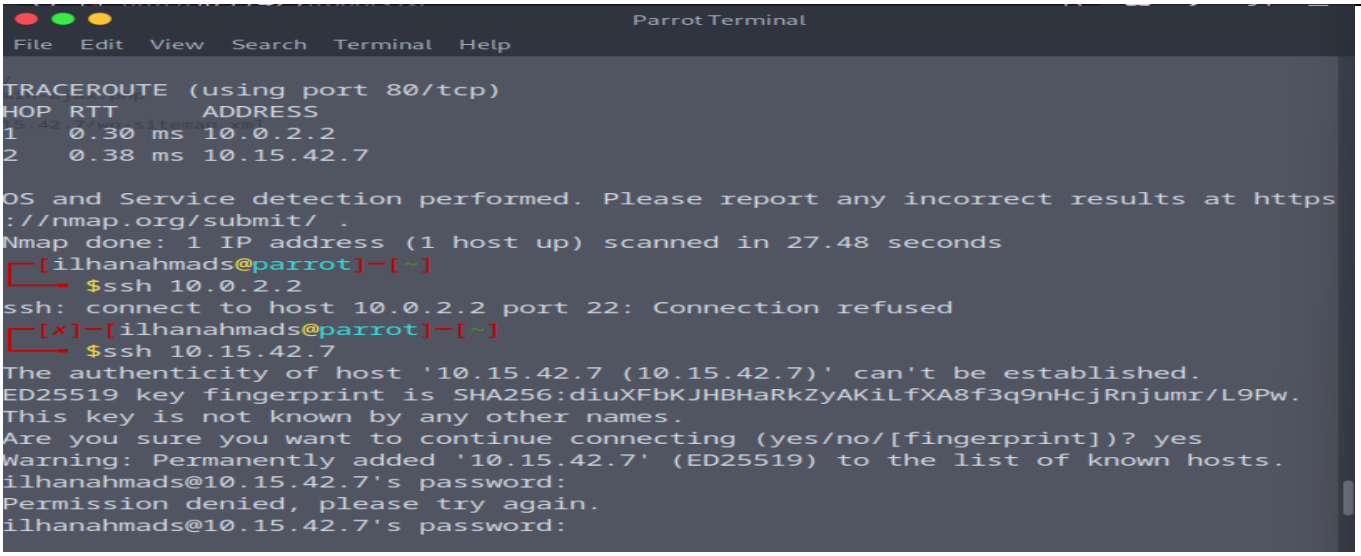


Figure 1: OpenSSH Access to 15.42.7 Port 22

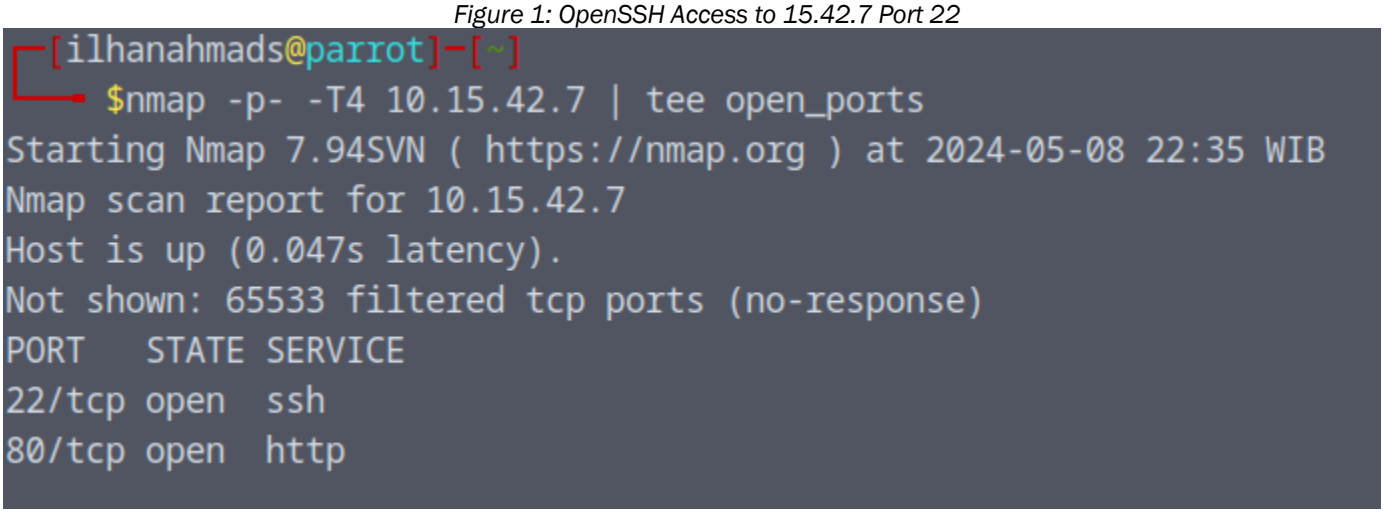


Figure 2: The Command

Remediation

To remediate and prevent unauthorized access through OpenSSH on the IP address 10.15.42.7 port 22, several steps can be taken. Firstly, it's crucial to maintain up-to-date patches for the OpenSSH software to mitigate known vulnerabilities effectively. Regularly checking for updates and applying them promptly ensures a secure configuration. Secondly, implement access controls to restrict SSH access solely to authorized users. Utilize SSH keys for authentication instead of passwords and enforce strong passphrase policies. Consider incorporating two-factor authentication for an additional layer of security. Thirdly, configure firewall rules to limit access to the SSH port (port 22) to specific IP addresses or ranges, thereby allowing only authorized users to connect remotely. Furthermore, consider network segmentation to isolate critical systems accessible via SSH from less sensitive areas, containing potential breaches and limiting unauthorized access impact. Additionally, set up monitoring tools to detect and alert on suspicious SSH activity, such as multiple failed login attempts or unusual access patterns. Enable detailed logging of SSH sessions for forensic analysis and audit purposes. Regular security audits

and vulnerability assessments should also be conducted to identify and address any weaknesses in the SSH configuration or server setup. This includes reviewing SSH server configuration files for any misconfigurations and ensuring compliance with best practices. Moreover, provide training to employees on secure SSH usage practices, emphasizing the importance of protecting SSH keys, recognizing phishing attempts, and promptly reporting any suspicious activity. Lastly, develop and maintain an incident response plan outlining the steps to be taken in the event of a security incident involving unauthorized SSH access. Ensure that all stakeholders are aware of their roles and responsibilities in responding to and mitigating such incidents. By implementing these comprehensive measures, organizations can effectively remediate existing vulnerabilities and prevent unauthorized access through OpenSSH, enhancing the overall security posture of their systems and networks.

Last Page