FortifyTech
Security Assessment Findings Report

Business Confidential

Date: March 9th, 2021
Project: DC-001
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Corp and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Demo Corp and TCMS.

Demo Corp 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

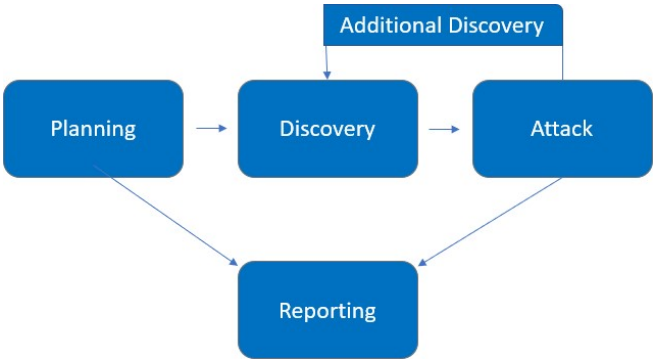
Name	Title	Contact Information
Demo Corp		
John Smith	Lab Ethical Hacking	Email: lab@ethicalhack.com
TCM Security		
Heath Adams	Lead Penetration Tester	Email: arsyathallah86@gmail.com

Assessment Overview

From February 22nd, 2021 to March 5th, 2021, Demo Corp engaged TCMS 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 dropbox and port allowances

Executive Summary

CyberShield evaluated FortifyTech's internal security posture through Vulnerability Finding 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

The Nmap scan reveals a host with the IP address 10.15.42.7, showing a low latency of 0.066 seconds. Two open TCP ports are detected: port 22 running SSH and port 80 running HTTP. The SSH service is identified as OpenSSH 8.2p1 on Ubuntu Linux, with RSA, ECDSA, and ED25519 SSH host keys. The HTTP service is running Apache httpd 2.4.59 on Debian, with WordPress 6.5.2 detected as the web application. The robots.txt file disallows access to "/wp-admin/". The title of the HTTP page is "Hello World". The operating system is determined to be Linux.

Tester Notes and Recommendations

Key Strengths and Weaknesses

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
Internal Penetration Test		
IPT-001: Enumerations on 10.15.42.7	low	

IPT-002: CVE-2023-48795 at 10.15.42.7	Moderate	
IPT-003: CVE-2023-48795 at 0.15.42.36	low	

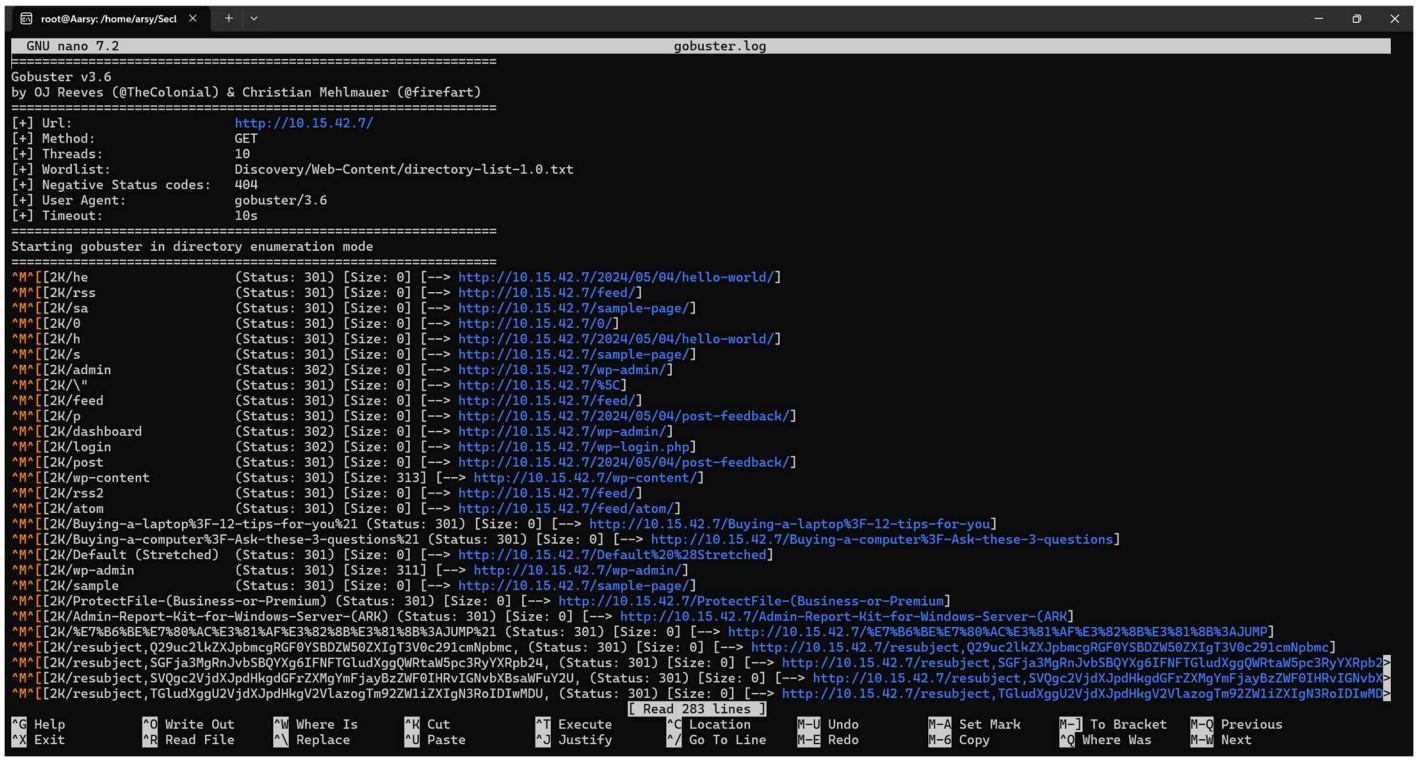
Technical Findings

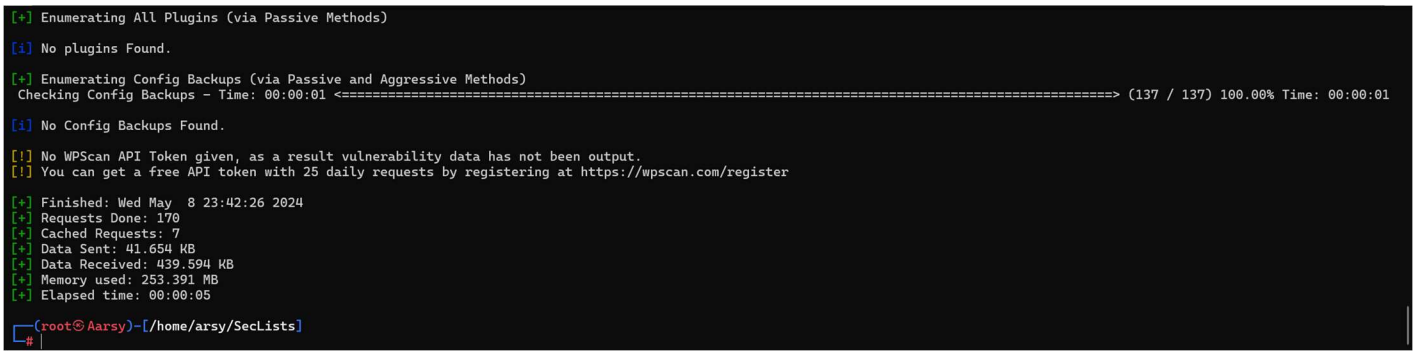
Internal Penetration Test Findings

Finding IPT-001: Enumerations on 10.15.42.7

Description:	After installing the seclist we can see there are so many web that has 0 size. Then using WPScan to find something but unfortunately I didn't find something important.
Risk:	No risk at all
System:	
Tools Used:	Gobuster, Nmap, WPScan

Evidence

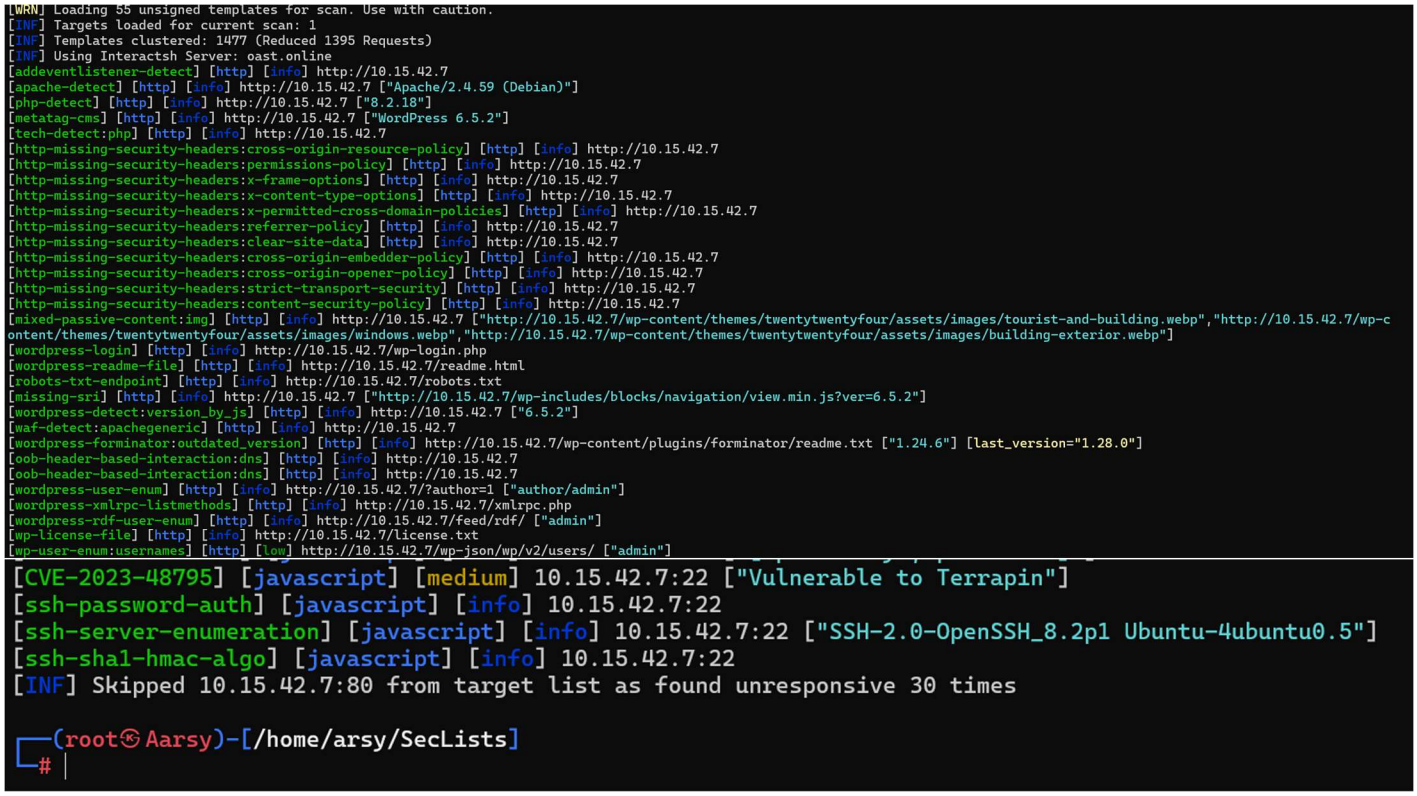




Finding IPT-002: CVE-2023-48795 at 10.15.42.7

Description:	
Risk:	
System:	
Tools Used:	Nuclei,Nmap

Evidence



Finding IPT-003: CVE-2023-48795 at 0.15.42.36

Description:	
Risk:	
System:	
Tools Used:	Nuclei,Nmap

Evidence

Additional Scans and Reports

FortifyTech 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 FortifyTech.

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