FortifyTech

Security Assessment Findings Report

Business Confidential

Date: May 8th, 2021

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		
FortifyTech	Global Information Security Manager	Email: ft@fortifytech.com
CyberShield		
Heath Adams	Lead Penetration Tester	Email: heath@cybersh.com

Assessment Overview

From May 5^{th}, 2024 to May 8^{th}, 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.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Reconnaissance – To gather enough information to understand the network topology and services running on the target, so as to help in planning an effective penetration attack.
- Vulnerability Assessment – 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. 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 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

In the IPT-001 and IPT-002 test series, several key findings were identified. First, related to IPT-001, anonymous login activity on 10.15.42.36 for FTP was discovered, indicating a potential security risk due to unauthorized access. To address this, it is recommended to ensure that the FTP server configuration does not allow anonymous access, as well as implement appropriate access controls and actively monitor login activity. Furthermore, IPT-002 reveals that there are three open ports, namely 22 (SSH), 21 (FTP), and 8888 (web application or proxy), at IP 10.15.42.36. This represents a potentially significant security risk, such as unauthorized access or exploitation through these ports. To reduce risk, it is recommended to ensure proper configuration of each port, update software regularly, implement firewalls to control access, conduct active monitoring of the activity of these ports, and limit access to only authorized users and strengthen security layers to prevent potential exploitation possibilities. These steps are important to ensure overall system security and protect data stored on that IP from potential threats.

Tester Notes and Recommendations

Enhance authentication mechanisms by implementing multi-factor authentication (MFA) to mitigate the risk of unauthorized access. Strengthen firewall configuration to restrict access to critical systems and services, prioritizing user training on security best practices to minimize human error-related incidents. Conduct regular security audits, deploy intrusion detection systems (IDS), and develop an incident response plan to effectively respond to security breaches. Emphasize continuous improvement in security practices to adapt to evolving threats and mitigate emerging risks effectively.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Secure Configuration: The server configurations demonstrate a commitment to security, with appropriate access controls and encryption protocols implemented.
2. Regular Software Updates: The prompt and regular updating of software and operating systems helps to mitigate potential vulnerabilities and ensures the latest security patches are applied.

The following identifies the key weaknesses identified during the assessment:

1. Lack of Multi-Factor Authentication: The absence of multi-factor authentication mechanisms increases the risk of unauthorized access, leaving the system vulnerable to password-based attacks.
2. Inadequate Firewall Configuration: Weaknesses in the firewall configuration may allow unauthorized access to critical systems and services, potentially leading to data breaches or system compromise.

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	2	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Login activity on 10.15.42.36 as an anonymous for FTP	High	Ensure the FTP server configuration does not allow anonymous access, update the software regularly, implement firewalls to control access, and actively monitor login activity.
IPT-002: The open ports are 22, 21, and 8888 on IP 10.15.42.36	High	Strengthen security with proper configuration, software updates, firewall settings, active monitoring, and limiting access to authorized users only.

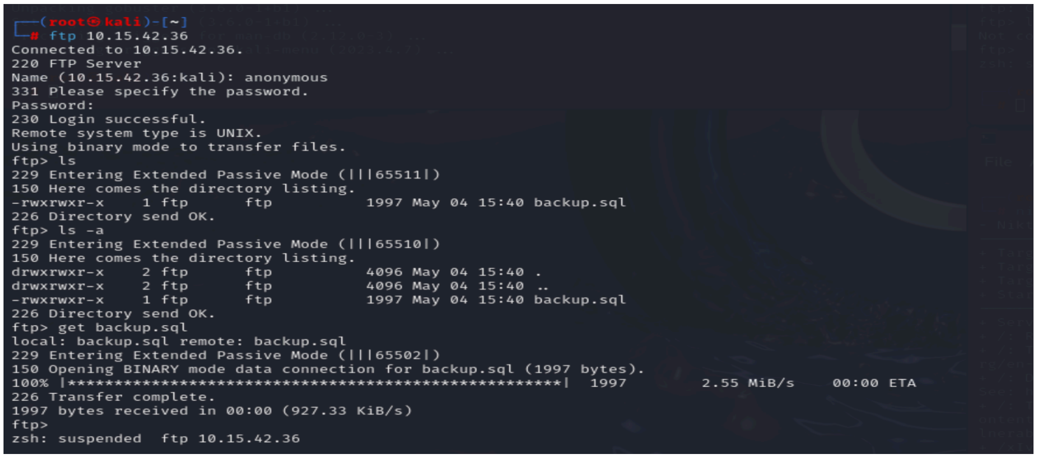
Technical Findings

Internal Penetration Test Findings

Finding IPT-001: Login activity on 10.15.42.36 as an anonymous for FTP (High)

Description:	"Anonymous login via FTP" refers to a configuration where users can access an FTP (File Transfer Protocol) server without providing any authentication credentials, such as a username or password. Instead, users can log in using a default username (often "anonymous" or "ftp") and typically use their email address as the password. While anonymous FTP can be convenient for allowing public access to certain files or directories, it also poses security risks if not properly configured. By carefully configuring and managing anonymous FTP access, organizations can provide convenient file sharing capabilities while minimizing security risks. However, it's essential to regularly review and update the configuration to address any emerging security threats or vulnerabilities.
Risk:	Likelihood: Medium – If the FTP server is properly configured with strict access controls and monitoring mechanisms, the likelihood of unauthorized access decreases. Impact: High – The impact of unauthorized access via anonymous FTP can be severe, especially if sensitive or confidential information is exposed or tampered with.
System:	All
Tools Used:	Nuclei and Nmap on Kali Linux

Evidence



```
┌──(root㉿kali)-[~]
└─# ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65511|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> ls -a
229 Entering Extended Passive Mode (|||65510|)
150 Here comes the directory listing.
drwxrwxr-x    2 ftp      ftp          4096 May 04 15:40 .
drwxrwxr-x    2 ftp      ftp          4096 May 04 15:40 ..
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> get backup.sql
local: backup.sql remote: backup.sql
229 Entering Extended Passive Mode (|||65502|)
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% |***************************************************|  1997        2.55 MiB/s    00:00 ETA
226 Transfer complete.
1997 bytes received in 00:00 (927.33 KiB/s)
ftp>
zsh: suspended  ftp 10.15.42.36
```

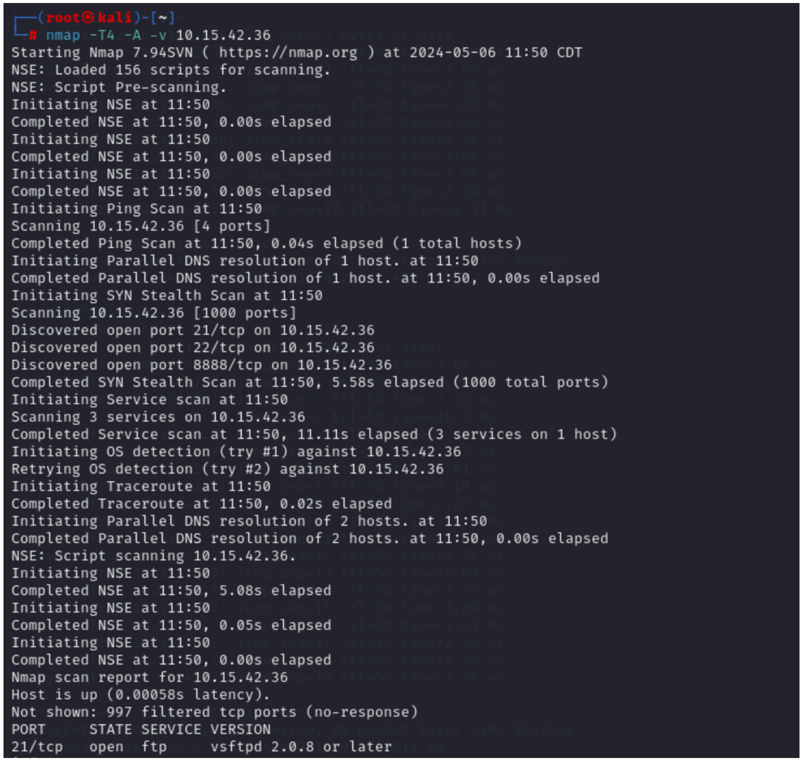
Remediation

To reduce the risk of unauthorized access via anonymous FTP, remediation steps include ensuring proper configuration of the FTP server by disabling unnecessary anonymous access, implementing strong authentication, conducting regular monitoring of FTP server activity, managing file and directory permissions by be thorough, update software regularly, perform periodic security scans, provide training to users on good security practices, use firewalls to control access, classify data based on its sensitivity, and conduct regular audits of FTP server configurations to ensure compliance with security policies.

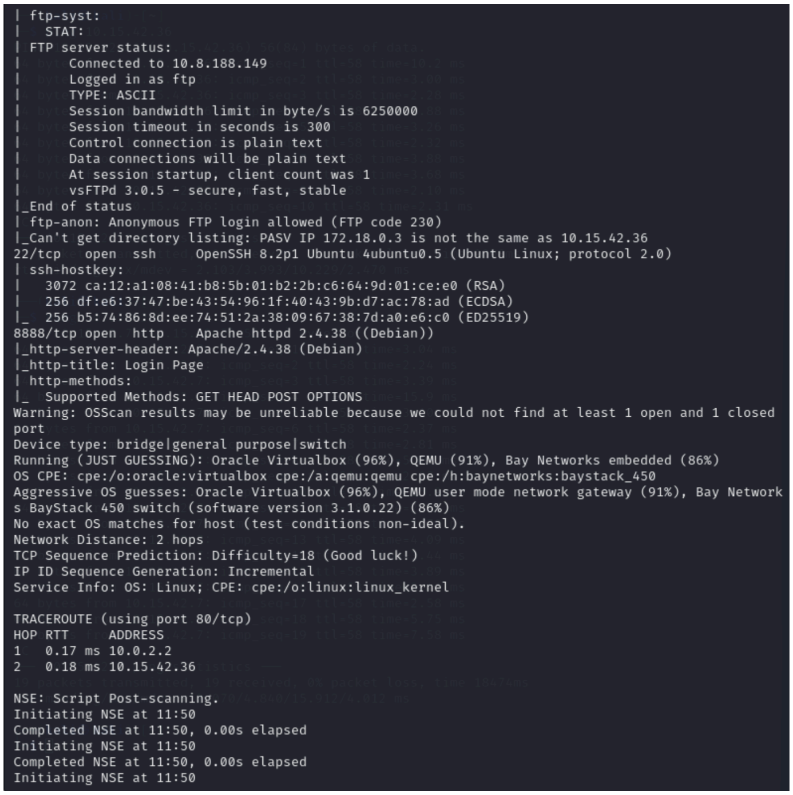
Finding IPT-002: The open ports are 22, 21, and 8888 on IP 10.15.42.36 (High)

Description:	With ports 21 (FTP), 22 (SSH), and 8888 (commonly used for web applications or proxies), it is important to ensure that any open ports are properly configured and have adequate security layers. For port 21, ensure the FTP configuration does not allow anonymous access unless necessary, and enforce strong authentication. For port 22, ensure that the SSH protocol is running with a secure version and using strong credentials. Port 8888 requires further inspection to understand what applications or services are running on it, and ensure that its security configuration is adequate, including proper authentication and regular software updates. Moreover, monitoring activity on these three ports and performing regular security scans are important preventive measures to ensure overall system security.
Risk:	Likelihood: Medium to High – The availability of these three ports provides an opportunity for attackers to try to find security gaps. Impact: High – This could include access to sensitive data, misuse of web services, or even use of the port as an entry point for further attacks into the internal network.
System:	All
Tools Used:	Nmap on Kali Linux

Evidence



```
┌──(root㉿kali)-[~]
└─# nmap -T4 -A -v 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 11:50 CDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Initiating Ping Scan at 11:50
Scanning 10.15.42.36 [4 ports]
Completed Ping Scan at 11:50, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:50
Completed Parallel DNS resolution of 1 host. at 11:50, 0.00s elapsed
Initiating SYN Stealth Scan at 11:50
Scanning 10.15.42.36 [1000 ports]
Discovered open port 21/tcp on 10.15.42.36
Discovered open port 22/tcp on 10.15.42.36
Discovered open port 8888/tcp on 10.15.42.36
Completed SYN Stealth Scan at 11:50, 5.58s elapsed (1000 total ports)
Initiating Service scan at 11:50
Scanning 3 services on 10.15.42.36
Completed Service scan at 11:50, 11.11s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 10.15.42.36
Retrying OS detection (try #2) against 10.15.42.36
Initiating Traceroute at 11:50
Completed Traceroute at 11:50, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 11:50
Completed Parallel DNS resolution of 2 hosts. at 11:50, 0.00s elapsed
NSE: Script scanning 10.15.42.36.
Initiating NSE at 11:50
Completed NSE at 11:50, 5.08s elapsed
Initiating NSE at 11:50
Completed NSE at 11:50, 0.05s elapsed
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Nmap scan report for 10.15.42.36
Host is up (0.00058s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
```



```
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.8.188.149
|      Logged in as ftp
|      TYPE: ASCII
|      Session bandwidth limit in byte/s is 6250000
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.18.0.3 is not the same as 10.15.42.36
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RSA)
|   256 df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
|_  256 b5:74:86:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25519)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Page
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Network
s BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=18 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.17 ms 10.0.2.2
2   0.18 ms 10.15.42.36

NSE: Script Post-scanning.
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Initiating NSE at 11:50
Completed NSE at 11:50, 0.00s elapsed
Initiating NSE at 11:50
```

Remediation

To reduce the risk of unauthorized access through ports 21 (FTP), 22 (SSH), and 8888 (web applications or proxies), remediation steps include ensuring that proper security configurations are implemented for each port, such as using strong authentication, updating software regularly, actively monitors port activity, and uses firewalls to control access. Additionally, it is recommended to limit access to these ports to authorized users only and ensure that adequate layers of security are implemented to prevent potential exploits.

Last Page