FortifyTech
Security Assessment Findings Report

Business Confidential

FortifyTech – 897-19
BUSINESS CONFIDENTIAL

Date: May 7th, 2024
Project: 897-19
Version 1.0

Table of Contents

Confidentiality Statement

This report is confidential and contains proprietary information of Pentester. The Report is provided solely for the use of authorized personnel of Pentester and its affiliates, and may not be disclosed to any third party without the prior written consent of Pentester.

By accessing or reviewing the Report, the recipient acknowledges that the Report contains confidential and proprietary information of Pentester, including but not limited to:

- Sensitive security information and vulnerabilities identified during the penetration testing;
- Proprietary methodologies and tools used during the engagement;
- Confidential business information and trade secrets of Pentester;
- Information about Pentester's systems, networks, and infrastructure.

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.

The Report is a snapshot of the Client's security posture at the time of the Engagement and may not reflect the current security state. The Report is based on the Tester's observations, testing, and analysis, and may not be exhaustive or definitive.

Contact Information

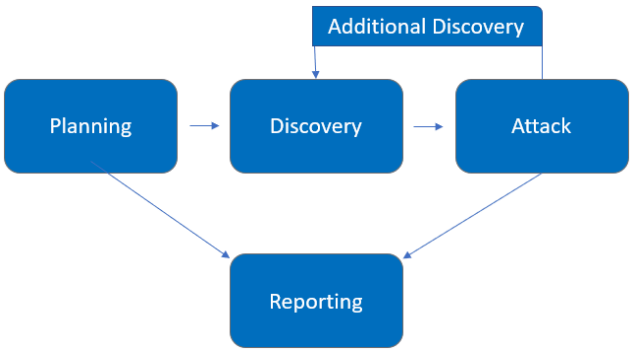
Name	Title	Contact Information
Pentester		
Arsyad Rizantha Maulana Salim	Information technology Student	Office: (081) 234-567-890 Email: arsyad.rizantha@gmail.com

Assessment Overview

From May 06th, 2019 to May 08th, 2024, FortifyTech engaged Pentester to evaluate the security posture of its infrastructure compared to current industry best practices that included an external 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

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A Pentester engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

The following table defines levels of severity and corresponding Pentester score range that are used throughout the document to assess vulnerability and risk impact.

Severity	FT 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.

Scope

Assessment	Details
External Penetration Test	10.15.42.36/ 10.15.42.7/

Client Allowances

Tester did not provide any allowances to assist the testing.

Executive Summary

Pentester evaluated FortifyTech's external security posture through an external network penetration test from May 05th, 2019 to May 08th, 2019. By leveraging a series of attacks, Pentester found critical level vulnerabilities that allowed full internal network access to the FortifyTech headquarter office. It is highly recommended that FortifyTech address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Attack Summary

The following table describes how Pentester gained internal network access, step by step:

Step	Action	Recommendation
1	Obtained historical breached account credentials to leverage against all company login pages.	Discourage employees from using work emails and usernames as login credentials to other services unless necessary.
2	Attempted a "credential stuffing" attack against Outlook Web Access (OWA), which was unsuccessful. However, OWA provided username enumeration, which allowed Pentester to gather a list of valid usernames to leverage in further attacks.	Synchronize valid and invalid account messages.
3	Performed a "password spraying" attack against OWA using the usernames discovered in step 2. Pentester used the password of Summer2018! (season + year + special character) against all valid accounts and gained access into the OWA application.	OWA permitted authenticated with valid credentials. Pentester recommends FortifyTech implement Multi-Factor Authentication (MFA) on all external services. OWA permitted unlimited login attempts. Pentester recommends FortifyTech restrict logon attempts against their service.

4	Leveraged valid credentials to log into VPN.	OWA permitted authenticated with valid credentials. Pentester recommends FortifyTech implement Multi-Factor Authentication (MFA) on all external services.

Security Strengths

SIEM alerts of vulnerability scans

During the assessment, the FortifyTech security team alerted Pentester engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the Pentester engineer's attacker IP address within minutes of scanning and was capable of blacklisting Pentester from further scanning actions.

Security Weaknesses

Missing Multi-Factor Authentication

Pentester leveraged multiple attacks against FortifyTech login forms using valid credentials harvested through open-source intelligence. Successful logins included employee email accounts through Outlook Web Access and internal access via Active Directory login on the VPN. The use of multi-factor authentication would have prevented full access and required Pentester to utilize additional attack methods to gain internal network access.

Weak Password Policy

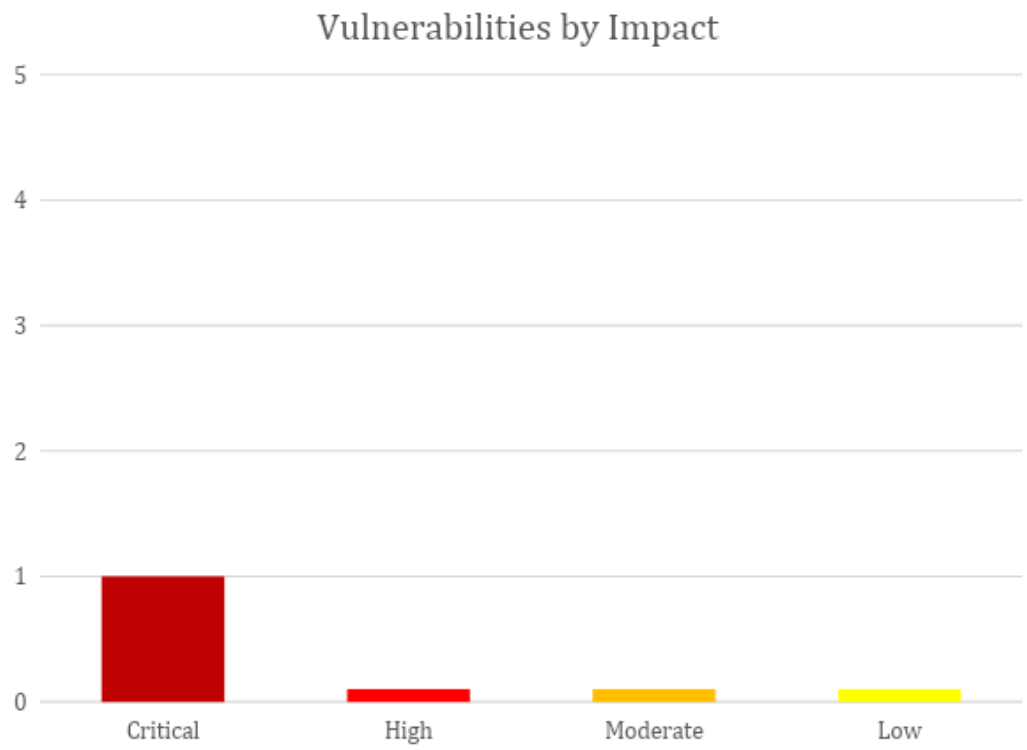
Pentester successfully performed password guessing attacks against FortifyTech login forms, providing internal network access. A predictable password format of Summer2018! (season + year + special character) was attempted and successful.

Unrestricted Logon Attempts

During the assessment, Pentester performed multiple brute-force attacks against login forms found on the external network. For all logins, unlimited attempts were allowed, which permitted an eventual successful login on the Outlook Web Access application.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



External Penetration Test Findings

Insufficient Lockout Policy

Description:	FortifyTech allowed unlimited login attempts against their Outlook Web App (OWA) services. This configuration allowed brute force and password guessing attacks in which TCMS used to gain access to FortifyTech's internal network.
Impact:	Critical
System:	http://10.15.42.36/

Exploitation Proof of Concept

First of all, in IP **10.15.42.36,** we have to do the nmap the scope using:

```
nmap --unprivileged -sV -sC -oN nmap1.log -Pn 10.15.42.36
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-08 20:48 SE Asia Standard Time
Nmap scan report for 10.15.42.36
Host is up (0.059s 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 10.33.3.205
|      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 2
|      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 172.19.0.2 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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.50 seconds
```

The result is as follows:

- Port 21/tcp: Open, running FTP service using vsftpd version 3.0.5. This service allows anonymous FTP login (FTP code 230) and provides information about the FTP server status, including current connections and other information.
- Port 22/tcp: Open, running SSH service using OpenSSH version 8.2p1 on the Ubuntu Linux operating system. Host SSH key information (RSA, ECDSA, ED25519) is also provided.
- Port 8888/tcp: Open, running HTTP service using Apache HTTP Server version 2.4.38 on the Debian operating system.

It appears that port 8888 on that IP address can be accessed, which leads to a login page. Additionally, the IP address has an FTP (File Transfer Protocol) service that we can access.

```
└─# ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:root): 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.
```

Further investigation using **ftp 10.15.42.36**, it revealed that the FTP server's history is vulnerable to unauthorized access, as the username was discovered using Nmap and, surprisingly, it doesn't require a password.

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.15.42.36
+ Target Hostname:    10.15.42.36
+ Target Port:        8888
+ Start Time:         2024-05-08 21:17:18 (GMT7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: Retrieved x-powered-by header: PHP/7.2.34.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2024-05-08 21:26:53 (GMT7) (575 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

A vulnerability scan using **`nikto -h http://10.15.42.36:8888/`** on port 8888 revealed several issues with the web server:

- The server is running Apache/2.4.38 (Debian), which discloses the web server version.
- The X-Powered-By Header indicates that the server uses PHP 7.2.34 as its backend programming language.
- The presence of X-Frame-Options and X-Content-Type-Options Headers is detected.
- The Apache version, Apache/2.4.38, is outdated and may pose a security risk.
- A README Apache file was found at /icons/README, which could provide hackers with insight into the server's structure or default configuration, potentially leading to exploitation.
- The server responds to invalid HTTP methods, which could be a security concern.

Remediation

Who:	IT Team
Vector:	Remote
Action:	Item 1: VPN and OWA login with valid credentials did not require Multi-Factor Authentication (MFA). Pentester recommends FortifyTech implement and enforce MFA across all external-facing login services. Item 2: OWA permitted unlimited login attempts. Pentester recommends FortifyTech restrict logon attempts against their service. Item 3: FortifyTech permitted a successful login via a password spraying attack, signifying a weak password policy. Pentester recommends the following password policy, per the Center for Internet Security (CIS): ▪ 14 characters or longer ▪ Use different passwords for each account accessed ▪ Do not use words and proper names in passwords, regardless of language Item 4: OWA permitted user enumeration. Pentester recommends FortifyTech synchronize valid and invalid account messages. Additionally, Pentester recommends that FortifyTech: ▪ Train employees on how to create a proper password ▪ Check employee credentials against known breached passwords ▪ Discourage employees from using work emails and usernames as login credentials to other services unless absolutely necessary

Last Page