CyberShield
Security Assessment Findings Report

Academic Purposes

Praktikum 2
Ethical Hacking and Cybersecurity
Muhammad Faishal Rizqy - 5027221026

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.

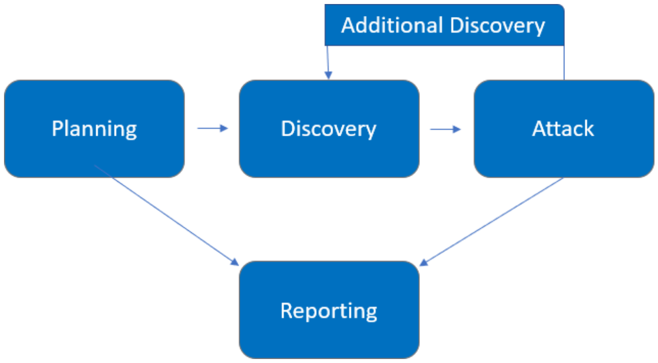
Time-limited engagements do not allow for a full evaluation of all security controls. CyberShield prioritized the assessment to identify the weakest security controls an attacker would exploit. CyberShield recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

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
Internal Penetration Test	10.15.42.36

Scope Exclusions

Per client request, CyberShield did not perform anythings that violate ethics.

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.

Attack Summary

The network assessment evaluated FortifyTech's internal network security posture.

The following table describes how CyberShield attacked FortifyTech's internal network security.

Step	Action	Reccomendation
1	Succesfully login to 10.15.42.36 port 22 and take important backup file.	Close the acces for anonymous login on ftp port

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	0	1	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Important backup file on ftp in 10.15.42.36	High	Close the open acces on port 22

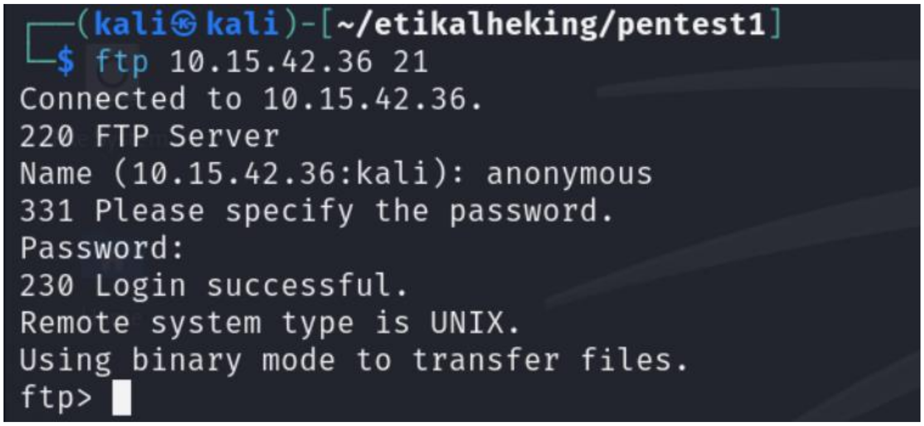
Technical Findings

Internal Penetration Test Findings

Important backup file on ftp in 10.15.42.36 (Moderate)

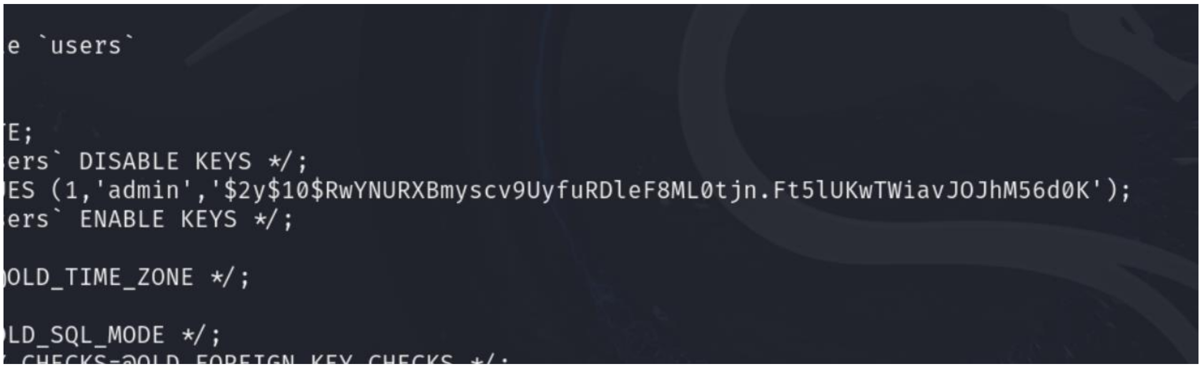
Description:	FortifyTech allows attacker to freely login to port 22 on 10.15.42.36. This allows attacker to get important file, put some malicious file, etc.
Impact:	High
System:	10.15.42.36
Tools Used:	Nmap
References:	

Evidence



```
┌──(kali㉿kali)-[~/etikalheking/pentest1]
└─$ ftp 10.15.42.36 21
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> 
```

Figure 1: Login into 10.15.42.36 ftp



```
e `users`


E;
ers` DISABLE KEYS */;
ES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
ers` ENABLE KEYS */;

OLD_TIME_ZONE */;

LD_SQL_MODE */;
```

Figure 2: backup.sql file on this open ftp port

Remediation

Disable ftp anonymous login, follow step by step here.

Last Page