Ethical Hacking
FortifyTech Penetration Testing

Academic Purposes

Date: May 8th, 2024
Project: Praktikum 2
Version 1.0

Table of Contents

Contents

Confidentiality Statement

This document is the exclusive property of CyberShield and FortifyTech. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both CyberShield and FortifyTech.

CyberShield and 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.

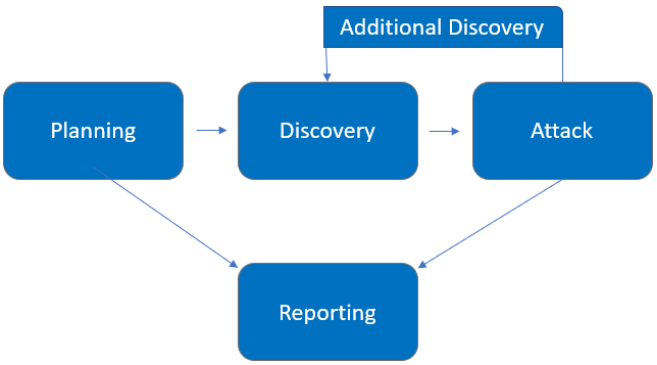
Time-limited engagements do not allow for a full evaluation of all security controls. CyberShield prioritized the assessment to identify the weakest security controls an attacker would exploit.

Assessment Overview

From May 5th, 2024 to May 8th, 2024, CyberShield engaged FortifyTech 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
Internal Penetration Test	10.15.42.7

Scope Exclusions

Per client request, CyberShield did not perform any non-ethical attacks nor actions that may violate the contract.

Client Allowances

FortifyTech provided CyberShield the following allowances:

- Internal access to network via Virtual Private Network (VPN) & 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) days.

Testing Summary

The network assessment evaluated FortifyTech's internal network security posture. From an internal perspective, the CyberShield team performed vulnerability scanning against all IPs provided by FortifyTech to evaluate the overall patching health of the network. CyberShield did a Directoral Scan of each IP and port that are provided, but sadly only turned up with one possible vulnerability, an OpenSSH exploit that occurs because of using an older version of OpenSSH that allows attackers to bypass integrity checks.

Overall, the FortifyTech network performed as expected for a first-time penetration test. We recommend that the FortifyTech team thoroughly review the recommendations made in this report, patch the findings, and re-test annually to improve their overall internal security posture.

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: Open FTP port accessable via anonymous user	High	Disable or remove guest/anonymous access to port

Technical Findings

Internal Penetration Test Findings

Finding IPT-001: Open FTP port accessable via anonymous user (High)

Description:	FortifyTech allows an open FTP port (Port 21) to be accessable via anonymous mode login (user:anonymous, password:*blank*) which allows attackers to take advantage of this opening and upload malicious files that can harm the system. There is also a possibility of the attacker not having a need to authenticate themselves to use this exploit
Risk:	Likelihood: High – This attack is effective to be exploited. Impact: Very High – By sending a large number of TELNET_IAC escape sequence, a remote attacker will be able to corrupt the stack and execute arbitrary code.
System:	All
Tools Used:	Nmap
References:	Nmap - Script ftp-vuln-cve2010-4221 CVE – CVE2010-4221

Evidence

```
┌──(kali㉿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 (|||65503|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> cat backup.sql
?Invalid command.
ftp> ls -a
229 Entering Extended Passive Mode (|||65515|)
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.
```

Figure 1: Found an exploit by authenticating as anonymous to be able to upload or delete files

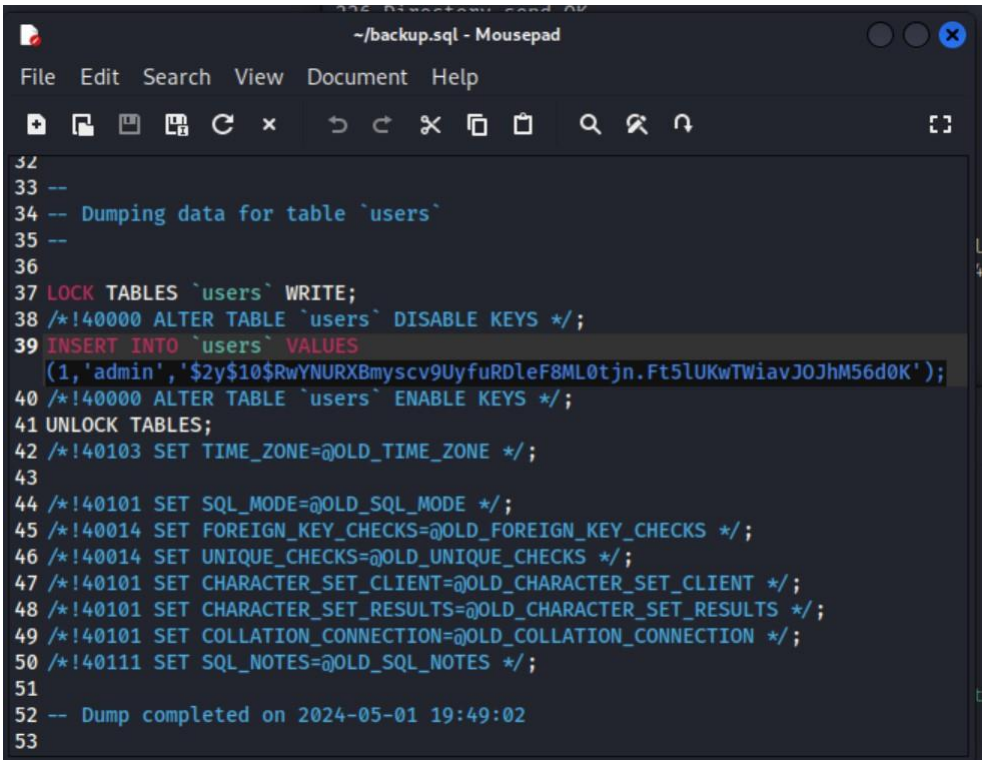


Figure 2: Cracked hash of "production"

Remediation

Disable access of FTP port as anonymous or even better yet, remove port 21 as a whole to counteract this issue and make use of a workaround to avoid creating an open port 21 as it can lead to more exploits.

Remediation

Review action and remediation steps.

Additional Scans and Reports

CyberShield 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 TCM Security.

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