MODULE 4-6 PRACTICE
Security Assessment Findings Report

Confidential

Date: May 7th, 2024

Table of Contents

Confidentiality Statement

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage or facilitate attacks against the involved parties.

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.

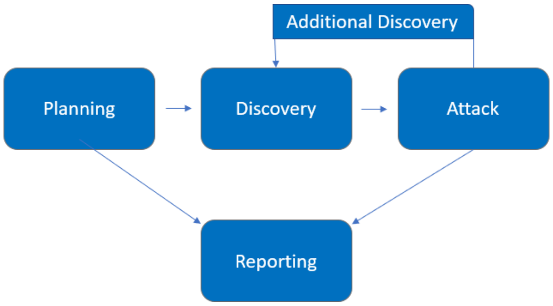
Time-limited engagements do not allow for a full evaluation of all security controls. I prioritized the assessment to identify the weakest security controls an attacker would exploit. I recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued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

Assessment Overview

From May 5th, 2024 to May 8th, 2024, FortifyTech engaged me 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

All forms of attacks were authorized

Client Allowances

FortifyTech granted me the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

I evaluated FortifyTevh 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 4 days.

Testing Summary

The network assessment evaluated FortifyTech internal network security posture. From an internal perspective, I performed vulnerability scanning against all IPs provided by FortifyTech to evaluate the overall patching health of the network. I also performed common Active Directory based attacks, attacks, such as SQL injection, Cross-Site Scripting, Path traversal, etc. Beyond vulnerability scanning and public exploit attacks, I evaluated other potential risks, such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

I found that anonymous FTP login is enabled on the network (Finding 001, particularly on 10.15.42.36), which allows unauthorized individuals to access sensitive information via FTP connection. The administrator username and hashed password were discovered, indicating a misconfiguration on the FTP server that could potentially provide expanded access to unauthorized users if the hash is successfully deciphered, which I successfully managed to do.

On 10.15.42.36, an obsolete iteration of the plugin, called forminator, was detected (version 1.2.46), allowing unauthorized users to execute Remote Code Execution by uploading any file, particularly on the feedback page authored by the administrator.

Tester Notes and Recommendations

The testing results of the FortifyTech network suggest an organization undergoing its initial penetration test, which is the situation in this case. The findings reveal vulnerabilities such as a misconfiguration on FTP and an outdated WordPress plugin version.

Throughout the testing process, the misconfiguration resulted in credential leakage and enabled remote code execution. The evidence supporting the presence of a misconfiguration on FTP is evident in my ability to log in anonymously and acquire credentials. Meanwhile, the obsolete forminator plugin resulted in complete system takeover

We suggest the client reassess their server configuration and consistently upgrade all libraries, modules, software, etc., to the most recent versions. Additionally, we advise the client team to examine the patching recommendations outlined in the Technical Findings section of the report for a comprehensive list of items requiring patches. Furthermore, we encourage the enhancement of the client's patch management policies and procedures to mitigate potential network attacks.

In general, the client network demonstrated typical performance for a first-time penetration test. We advise the client team to meticulously examine the recommendations presented in this report, address the findings through patching, and conduct annual re-testing to enhance their internal security posture further. This proactive approach will contribute significantly to strengthening their overall security resilience.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observation of scanning activity from common enumeration tools like Nuclei.
2. Unique encryption of hashed passwords for credentials.

The following identifies the key weaknesses identified during the assessment:

1. Server misconfiguration.
2. Outdated plugin.

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		
Finding 001 : Weak Security Configuration - Anonymous Login Permitted on FTP	Critical	Disable Anonymous Login, Use SFTP.
Finding 002: Outdated Forminator Plugin - Remote Code Execution	Critical	Update Forminator Plugin, Remove Forminator Plugin (If Unused), Use a Reputable Website Security Plugin.

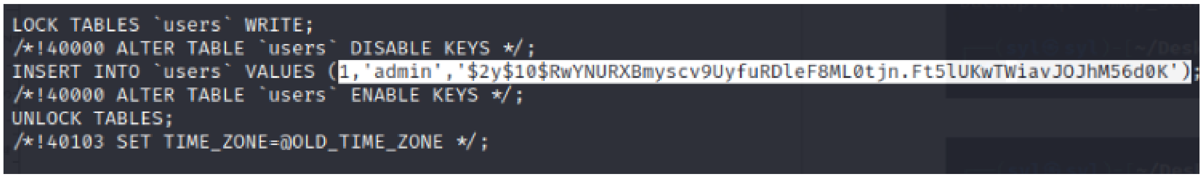
Technical Findings

Internal Penetration Test Findings

Finding 001: Weak Security Configuration - Anonymous Login Permitted on FTP

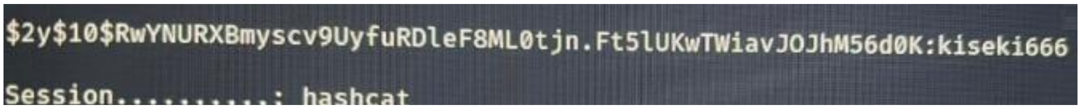
Description:	A critical security vulnerability was discovered on the client's FTP server, stemming from an improper configuration that granted unauthorized users access to the server. This misconfiguration poses a significant risk of sensitive data exposure, as unauthorized individuals could potentially download or manipulate confidential information.
Risk:	Likelihood: High - Attackers can easily exploit anonymous login to gain unauthorized access. Impact: Very High - Passwords could be leaked, and further attacks could be launched.
System:	All
Tools Used:	Nmap, Hashcat
References:	CVE-1999-0497 - Anonymous FTP

Evidence



```
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

Figure 1: Captured hash of "admin"



```
$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K:kiseki666
Session..........: hashcat
```

Figure 2: Hash "Cracked"

Remediation

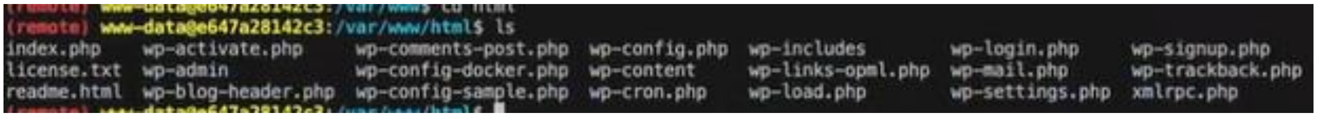
- Disable Anonymous Login: This eliminates the ability for unauthorized users to access the FTP server.
- Implement SFTP: SFTP (SSH File Transfer Protocol) encrypts data transfer, providing a more secure alternative to FTP.

- Review and Harden FTP Configuration: Carefully review the remaining FTP server configuration and implement best practices to further strengthen security.

Finding 002: Outdated Forminator Plugin - Remote Code Execution

Description:	The security flaw present in Forminator version 1.2.46 is specifically targeted at the feedback page associated with posts authored by the administrator. Exploiting this vulnerability involves the unauthorized uploading of arbitrary files, consequently facilitating remote code execution. Such an exploit poses a critical risk, potentially leading to the complete takeover of the system.
Risk:	Likelihood: High - Attacker gains complete control over website content. Impact: Very High - Severe disruption, page deletion/modification.
System:	All
Tools Used:	Nuclei
References:	https://www.exploit-db.com/exploits/51664

Evidence



```
(remote) www-data@e647a28142c3:/var/www$ cd html
(remote) www-data@e647a28142c3:/var/www/html$ ls
index.php    wp-activate.php      wp-comments-post.php   wp-config.php  wp-includes         wp-login.php     wp-signup.php
license.txt  wp-admin             wp-config-docker.php   wp-content     wp-links-opml.php   wp-mail.php      wp-trackback.php
readme.html  wp-blog-header.php   wp-config-sample.php   wp-cron.php    wp-load.php         wp-settings.php  xmlrpc.php
(remote) www-data@e647a28142c3:/var/www/html$
```

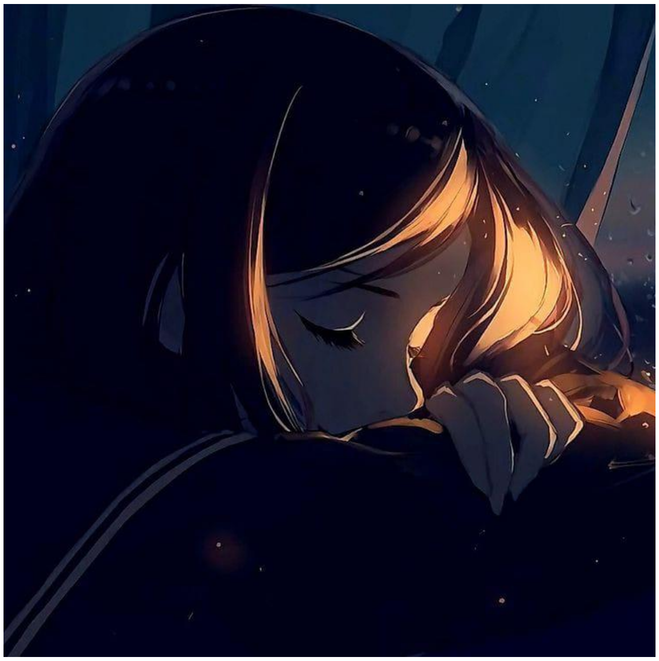
Figure 3: Shell access

Remediation

- Update Forminator Plugin: This remains a perfect way to phrase this action.
- Remove Forminator Plugin (If Unused): Here's an alternative phrasing with slightly stronger language: If Forminator is no longer needed, completely remove it from your website.
- Use a Reputable Website Security Plugin: This is another well-phrased action. Here's an option with a bit more emphasis: Consider implementing a reputable website security plugin to enhance overall website protection.

Additional Scans and Reports

I provide all clients with all report information gathered during testing. This includes full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by me. The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depthopportunities.



Last Page