Praktikum Ethack Modul 2
Security Assessment Findings Report

Business Confidential

Date: October 7th,
2024 Project: DC-001
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of midashisgrade and the security assessment team. It contains proprietary and confidential information. Any duplication, redistribution, or use, in whole or in part, in any form, requires written consent from both midashisgrade and the assessment team.

Midashisgrade may share this document with authorized third parties, including auditors, under non-disclosure agreements, for the purpose of demonstrating compliance with security assessment requirements.

Disclaimer

A penetration test represents a snapshot of the system's security posture at a specific point in time. The findings and recommendations are based on the information gathered during the assessment period and do not account for any changes or modifications made after that time.

Due to the time-limited nature of this engagement, not all security controls could be fully evaluated. The assessment was prioritized to identify the most critical vulnerabilities that could be exploited by an attacker. It is recommended to conduct regular assessments, either internally or by third-party assessors, on an annual basis to ensure the continued effectiveness of security controls.

Contact Information

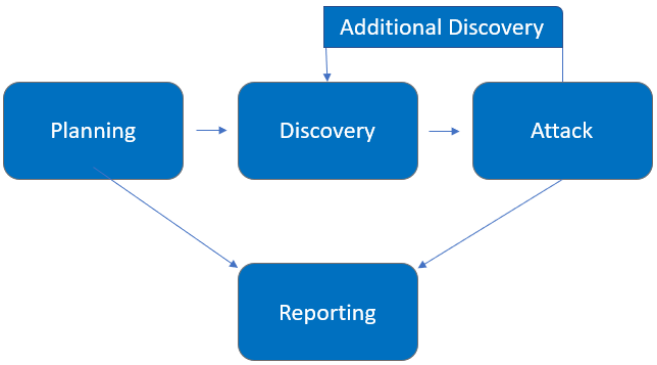
Name	Title	Contact Information
Demo Corp		
John Smith	Global Information Security Manager	Email: jsmith@democorp.com
TCM Security		
midashisgrade	Penetration Tester	Email: dimsum@tcm-sec.com

Assessment Overview

From October 4th, 2024 to October 7th, 2024, Asprak engaged praktikan 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 –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	10.15.42.245

Scope Exclusions

Per client request, Asprak 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 Asprak.

Client Allowances

Asprak provided the following allowances:

- Internal access to network

Executive Summary

midashisgrade evaluated Ethack Praktikum internal security posture through penetration testing from October 4th, 2024 to October 7th, 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

The network assessment evaluated the internal network security posture of 10.15.42.245. From an external perspective, the testing team performed comprehensive vulnerability scanning to assess the overall security health of the system. The team also explored various attack vectors, such as open FTP services, weak password policies, and web application vulnerabilities. Beyond vulnerability scanning, the team evaluated other potential risks, such as default credentials on services and sensitive information disclosure, to gain a complete picture of the network's security posture.

The team discovered that the FTP service was accessible (port 21) and allowed login with anonymous credentials, exposing sensitive files such as list.xyz containing hashed user credentials. These credentials were cracked using offline dictionary attacks, signaling weak password protection policies. Utilizing the cracked credentials, the team gained access to further system resources, indicating that user account privileges were overly permissive.

With access to user credentials, the team focused on web application vulnerabilities, particularly targeting the WordPress installation hosted on the system (port 487). The wpDiscuz plugin was found to be vulnerable to Remote Code Execution (RCE) (CVE-2020-24186). The team successfully exploited this vulnerability by uploading a malicious PHP web shell, which allowed full control over the web server, demonstrating a serious security flaw in the patch management process.

Ultimately, the team was able to exploit weak password policies and vulnerable web applications to gain extensive access to the system. The team uploaded web shells to maintain persistence and leverage the compromised system for further attacks.

In addition to the compromise listed above, the team identified that password cracking was feasible due to weak password complexity. Furthermore, the vulnerable WordPress plugin, combined with weak patch management, posed a significant risk to the integrity of the system.

The remaining findings primarily relate to patch management, including vulnerabilities in the WordPress plugin (wpDiscuz), weak password policies, and unpatched services (FTP and WordPress). These issues should be addressed as a priority to prevent exploitation.

The remainder of the findings were categorized as high, moderate, or low in terms of impact. For further information on findings, please refer to the Technical Findings section

Tester Notes and Recommendations

The testing results of the network at 10.15.42.245 indicate several significant vulnerabilities that could be easily exploited by attackers. Many of the findings discovered relate to improper configurations and weak security controls across services, such as FTP, weak password policies, and vulnerable web applications.

During testing, two key weaknesses stood out: weak password protection and vulnerable web services. The weak password protection led to the compromise of user credentials early in the engagement, and the cracked passwords enabled further access to the system. This is often the first foothold an attacker seeks when evaluating the security posture of a network. The use of simple passwords (e.g., password123) demonstrates an insufficient password policy that could be easily improved by enforcing more complex password rules and implementing multi-factor authentication (MFA).

The vulnerability in the WordPress plugin (wpDiscuz) further exacerbated the system's security risks. The exploitation of this Remote Code Execution (RCE) vulnerability allowed the team to upload a web shell, giving full access to the web server. This, combined with weak patch management, could easily lead to the compromise of the entire system if left unaddressed.

We recommend re-evaluating the current password policies and enforcing a minimum password length of at least 12 characters with a combination of uppercase, lowercase, numbers, and special characters. Additionally, implementing MFA and password blacklisting would further improve the security posture. For the WordPress instance, we recommend updating or replacing vulnerable plugins and ensuring regular patching to prevent further exploitation.

On the positive side, our testing revealed that the FTP service, while misconfigured, did not contain highly sensitive information other than hashed user credentials. However, the exposure of any sensitive data still poses a risk to the organization and should be addressed promptly.

Overall, this testing engagement revealed critical vulnerabilities that need immediate remediation. The weak password protection and vulnerable web applications created several attack vectors, which could be exploited in future attacks if not patched. We recommend the team follows the recommendations outlined in the Technical Findings section, patches the vulnerabilities, and improves overall system security by adopting better password and patch management policies.

Finally, once remediations are implemented, we suggest conducting periodic penetration tests to ensure that security improvements are effective and to stay ahead of evolving threats.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. **FTP Service Detected**: The system responded quickly to FTP enumeration and allowed file listing, suggesting that service identification tools are effective.
2. **No Highly Sensitive Information Exposed in FTP**: Although user credentials were accessible, no highly classified or critical system files were immediately exposed.
3. **Prompt Response to FTP Connections**: The server responded with correct FTP protocol messages and logins, indicating active and functional services.

The following identifies the key weaknesses identified during the assessment:

1. **Insufficient Password Policy:** Weak passwords such as password123 were easily cracked, highlighting the need for stronger password complexity requirements.
2. **FTP Misconfiguration:** The FTP service allowed anonymous login and access to sensitive files, representing a serious security misconfiguration.
3. **Exposed User Credentials:** Credentials stored in list.xyz were accessible and cracked, leading to unauthorized access to the system.
4. **Vulnerable WordPress Plugin:** The wpDiscuz plugin was outdated and vulnerable to Remote Code Execution (CVE-2020-24186), allowing the upload of a malicious web shell.
5. **Weak Patch Management:** The WordPress plugin and potentially other services were not updated, creating a critical entry point for attackers.
6. **No Multi-Factor Authentication (MFA):** The absence of MFA allowed simple password-based attacks to succeed.
7. **Potential for Further Exploitation:** Once initial access was gained, there were no apparent protections to prevent lateral movement or privilege escalation through the compromised services.
8. **No Intrusion Detection or Alerts:** No evidence was found of alerts triggered by the attacks, indicating a lack of monitoring or intrusion detection capabilities.
9. **Lack of File System Permissions:** Directory and file access were overly permissive, exposing files like list.xyz without adequate security controls

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

3	1	0	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
VULN-001: Weak Password Policy	Critical	Enforce a strong password policy, including a minimum length and complexity requirements. Implement MFA.
VULN-002: FTP Misconfiguration	Critical	Disable anonymous login and enforce strong authentication for FTP services.
VULN-003: Vulnerable WordPress Plugin	Critical	Update wpDiscuz to the latest version to patch the Remote Code Execution (RCE) vulnerability (CVE-2020-24186).
VULN-004: Exposed User Credentials	High	Protect sensitive files like list.xyz with proper file permissions and restrict access.
VULN-005: Unrestricted Directory Access	Informational	Review directory permissions and restrict access to critical resources.

Technical Findings

Internal Penetration Test Findings

Finding VULN-001: Weak Password Policy (Critical)

Description:	The system uses weak passwords, such as password123, which were easily cracked using basic dictionary attacks. The weak password policy allows attackers to gain unauthorized access to the system. Lack of password complexity requirements and multi-factor authentication (MFA) further exposes the system to brute force and credential stuffing attacks
Risk:	Likelihood: High – Weak passwords are one of the most commonly exploited vulnerabilities in modern systems. Impact: Very High – If exploited, attackers can gain unauthorized access to sensitive accounts, allowing lateral movement within the network.
System:	All
Tools Used:	John the Ripper
References:	https://owasp.org/www-community/vulnerabilities/Weak_password_policy https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Evidence

```
┌──(kali㉿dimzandhk)-[/mnt/d]
└─$ john --wordlist=dictionary.txt pwethack.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 16384 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:30 2.30% (ETA: 14:21:53) 0g/s 32.93p/s 32.93c/s 32.93C/s UJM/4/+t..+.A@d8B>
0g 0:00:10:27 40.61% (ETA: 14:25:54) 0g/s 32.14p/s 32.14c/s 32.14C/s 3xttx&T$..n3z3J73*
0g 0:00:11:12 43.49% (ETA: 14:25:56) 0g/s 32.13p/s 32.13c/s 32.13C/s &dPXN5pn..3Tvjnv@[
6DMfLv(9         (?)
1g 0:00:15:33 DONE (2024-10-06 14:15) 0.001071g/s 31.94p/s 31.94c/s 31.94C/s %CxTR2=Z..2_h6haQe
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Figure 1: Successfully Cracking Password

Remediation

Enforce a strong password policy with a minimum of 12-16 characters, requiring a mix of uppercase, lowercase, numbers, and special characters. Implement Multi-Factor Authentication (MFA) to reduce reliance on passwords alone. Consider using password blacklisting to prevent the use of commonly breached passwords. Additionally, educate users on safe password practices and enforce periodic password changes. For full mitigation and detection guidance, refer to the NIST Password Policy Guidelines.

Finding VULN-002: FTP Misconfiguration (Critical)

Description:	The FTP service was misconfigured, allowing anonymous access without proper authentication. Sensitive files, such as list.xyz, containing hashed credentials were accessible. This exposure significantly increases the risk of unauthorized access to critical information.
Risk:	Likelihood: High – Anonymous FTP access is commonly exploited by attackers for reconnaissance and data theft. Impact: Very High – Unauthorized access to sensitive files can lead to credential theft, privilege escalation, and further exploitation of the network.
System:	All
Tools Used:	Nmap (for service detection and port scanning)
References:	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45ver2.pdf https://cwe.mitre.org/data/definitions/532.html

Evidence

```
┌──(kali㉿dimzandhk)-[~]
└─$ cat awikwok.log
# Nmap 7.94SVN scan initiated Sun Oct  6 13:38:04 2024 as: nmap -p- -T4 -oN awikwok.log 10.15.42.245
Nmap scan report for 10.15.42.245
Host is up (0.0097s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
487/tcp open  saft

# Nmap done at Sun Oct  6 13:38:19 2024 -- 1 IP address (1 host up) scanned in 15.15 seconds
```

Figure 2: Port Scanning

Remediation

Disable anonymous access to the FTP service and require strong authentication (username and password) for all users. Use FTPS (FTP over SSL) to encrypt the communication between client and server. Apply proper file permissions to sensitive directories and limit access to authorized users only. Consider replacing FTP with a more secure file transfer protocol, such as SFTP.
For further guidance, refer to the NIST Guide to Secure FTP Configuration.

Finding VULN-003: Vulnerable WordPress Plugin (Critical)

Description:	The wpDiscuz plugin installed on the WordPress site was outdated and vulnerable to Remote Code Execution (RCE) (CVE-2020-24186). Exploiting this vulnerability, the attacker was able to upload a malicious PHP web shell, gaining complete control over the web server.
Risk:	Likelihood: High – Outdated plugins are easy targets for attackers due to publicly available exploit information. Impact: Very High – Successful exploitation allows attackers to execute arbitrary code on the web server, leading to full control over the server.
System:	All
Tools Used:	WPScan (WordPress vulnerability scanner) Python Script (wpDiscuz_RemoteCodeExec.py) (for exploiting the RCE vulnerability)
References:	https://nvd.nist.gov/vuln/detail/CVE-2020-24186 https://owasp.org/www-project-top-ten/2017/A9-Using-Components-with-Known-Vulnerabilities

Evidence

```
Fingerprinting the version - Time: 00:00:26 <==========================================>
[i] The WordPress version could not be detected.

[+] WordPress theme in use: default
 | Location: http://10.15.42.245:487/2024/10/03/trial/wp-content/themes/default/
 | Latest Version: 1.7.2 (up to date)
 | Last Updated: 2020-02-25T00:00:00.000Z
 | Style URL: http://10.15.42.245:487/wp-content/plugins/wpdiscuz/themes/default/style.css?ver=7.0.4
 | Style Name: Default
 | Author: gVectors team
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 7.0.0 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.15.42.245:487/wp-content/plugins/wpdiscuz/themes/default/style.css?ver=7.0.4, Match: 'Version: 7.0.0'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] wpdiscuz
 | Location: http://10.15.42.245:487/2024/10/03/trial/wp-content/plugins/wpdiscuz/
 | Latest Version: 7.6.24
 | Last Updated: 2024-08-31T08:29:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | The version could not be determined.
```

Figure 3

Remediation

Update the wpDiscuz plugin to the latest version or remove it if no longer in use. Regularly check for updates and security patches for all WordPress plugins. Implement a Web Application Firewall

(WAF) to monitor and block potential malicious requests. Regularly scan WordPress sites for vulnerabilities using tools like WPScan and ensure secure configuration settings.
Refer to OWASP's WordPress Security Hardening Guide.

Finding VULN-004: Exposed User Credentials (High)

Description:	Sensitive user credentials were found in the list.xyz file on the FTP server. These credentials were hashed but were cracked using basic password-cracking techniques due to weak passwords. The exposed credentials allow unauthorized access to the system.
Risk:	Likelihood: Moderate – Cracking weak password hashes is common and easily accomplished with publicly available tools. Impact: High – Exposed credentials can be used to compromise user accounts and escalate privileges within the network.
System:	All
Tools Used:	John the Ripper (to crack the hashed credentials) FTP Client (to retrieve the list of exposed credentials)
References:	https://cwe.mitre.org/data/definitions/200.html https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

Evidence

Remediation: Remove sensitive files like list.xyz from publicly accessible directories and ensure that all sensitive information is stored securely. Implement proper file permissions to restrict access only to authorized users. Store user credentials securely using stronger hashing algorithms (e.g., bcrypt, Argon2) with salt and pepper techniques. Regularly audit stored data for the presence of sensitive information.
For more details on secure storage practices, refer to OWASP's Password Storage Cheat Sheet.

Finding VULN-005: Unrestricted Directory Access (Informational)

Description:	Directory permissions on the system were not properly restricted, allowing access to sensitive files such as list.xyz. Although no critical files were exposed, the lack of directory-level access controls presents an unnecessary risk.
Risk:	Likelihood: Low – Directory access requires some level of unauthorized access, but once obtained, the permissions issue can be exploited. Impact: Moderate – Exposure of non-sensitive but useful information can assist in further reconnaissance and attacks.
System:	All
Tools Used:	FTP Client (to explore the directory and retrieve files)
References:	https://cwe.mitre.org/data/definitions/732.html https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45ver2.pdf

Evidence

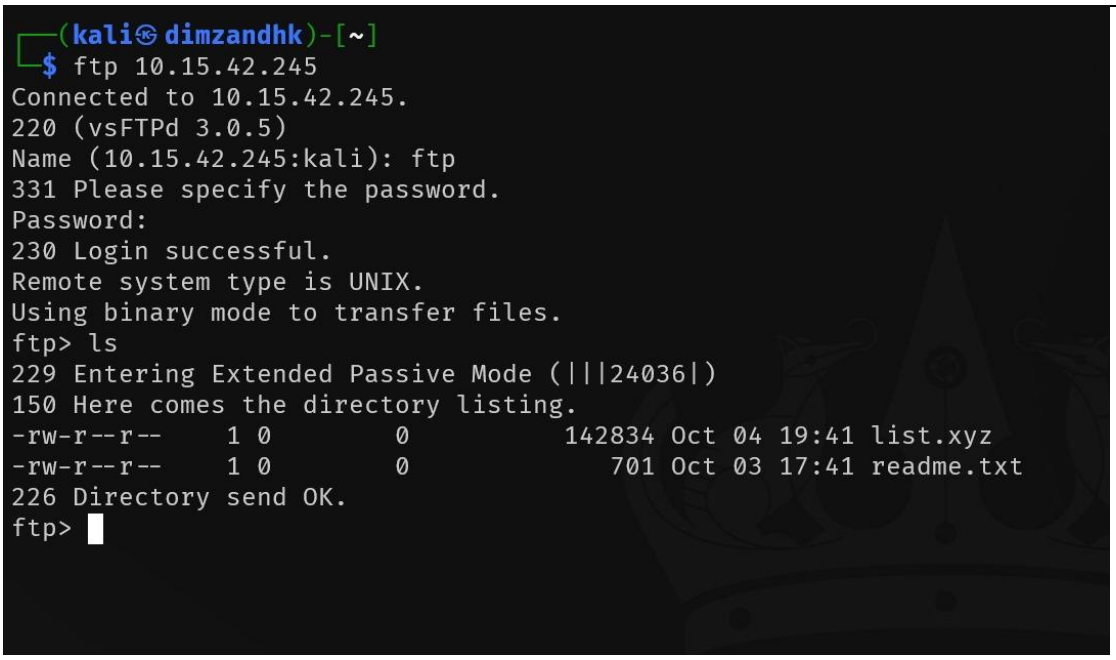


Figure 5: Directory Access

Remediation

Implement proper directory access controls by setting file and folder permissions based on the principle of least privilege. Ensure that sensitive directories are not publicly accessible and restrict access to authenticated and authorized users only. Use file system monitoring tools to track access to sensitive directories.
For more details, refer to the NIST Guide on File and Directory Permissions.

Last Page