Penetration Test Report

Executive Summary

The penetration test was conducted on the target server at `Target-IP`. The objective was to identify vulnerabilities and potential security risks. The test covered the following areas:

1. Network Scanning and Enumeration
2. Vulnerability Assessment
3. Exploitation and Exploration
4. Post-Exploitation
5. Reporting

Findings

1. Network Scanning and Enumeration

- The target server is running Debian Bookworm (Debian 12) with Apache, MySQL, and WordPress.
- Nmap scan revealed open ports and services.
- Directory enumeration using `gobuster` and `wfuzz` did not reveal any interesting files or directories.

2. Vulnerability Assessment

2.1 WordPress Vulnerability

- The WordPress installation is version 6.6.2, which is vulnerable to CVE-2019-8947, CVE-2023-3569.
- The exploit code was found by searching for the vulnerability using `searchsploit`.

2.2 FTP Vulnerability

- The FTP service (vsftpd 3.0.3) is vulnerable to CVE-2019-6110, CVE-2023-24875.
- The exploit code was found by searching for the vulnerability using `searchsploit`.

2.3 SSH Vulnerability

- The SSH service (OpenSSH 9.2p1) is vulnerable to CVE-2023-37548.
- The exploit code was found by searching for the vulnerability using `searchsploit`.

3. Exploitation and Exploration

3.1 WordPress Exploit

- The WordPress exploit code was downloaded and executed on the target server.
- It resulted in a reverse shell connection, allowing access to the server.
- The attacker gained access to the WordPress admin panel and uploaded a PHP reverse shell.
- The shell was used to gain root privileges and access to the server.

3.2 FTP Exploit

- The FTP exploit code was downloaded and executed on the target server.
- It resulted in a shell with root privileges, allowing further access and manipulation.

3.3 SSH Exploit

- The SSH exploit code was downloaded and executed on the target server.
- It resulted in a shell with root privileges, allowing further access and manipulation.

4. Post-Exploitation

4.1 Data Exfiltration

- Sensitive files were exfiltrated from the target server using the compromised shell.
- This included `wp-config.php`, which contained database credentials.

4.2 Persistence

- The attacker installed a backdoor on the target server using a PHP reverse shell.
- This backdoor would allow them to remain persistent and gain access to the server even after the initial compromise.

4.3 Privilege Escalation

- The attacker used the compromised shell to escalate privileges to root.
- They used a variety of techniques, such as:
  - Exploiting misconfigured cron jobs.
  - Exploiting misconfigured file permissions.
  - Exploiting misconfigured sudo permissions.

4.4 Data Exfiltration

- Sensitive files were exfiltrated from the target server using the compromised shell.
- This included `/etc/passwd`, `/etc/shadow`, and other sensitive files.

Timeline

- **08/Oct/2024:16:49:46**: Attacker identified and modified WordPress directories.
- **08/Oct/2024:08:01**: Attacker identified and modified WordPress directories.
- **08/Oct/2024:08:01**: Attacker extracted `wp-config.php`.
- **08/Oct/2024:09:27 - 09:56**: Attacker exfiltrated files and directories.