Vulnerability Disclosure Policy

Maryam Khan

Oct 14, 2024

Introduction

As a Cyber Security professional, I conduct security research with the intention of improving the security and integrity of systems. This policy outlines the process for discovering and reporting vulnerabilities in the Metasploitable system, a deliberately vulnerable environment designed for penetration testing and security research.

Scope

This policy applies to vulnerabilities discovered in the Metasploitable system, which includes the following services and endpoints:

- Web Server: Apache 2.2.8 (Ubuntu)
- http://192.168.100.48/dvwa
- http://192.168.100.48/mutillidae
- http://192.168.100.48/dav/
- http://192.168.100.48/twiki/
- http://192.168.100.48/phpMyAdmin/

Out of Scope

- Any third-party services not operated within the Metasploitable environment.
- Denial of Service (DoS) or brute-force attacks.
- Physical security testing, including office access.
- Any real-world production systems, servers, or networks that exist outside of Metasploitable2 are not covered under this policy

Vulnerabilities Identified

These vulnerabilities were identified during my security assessment of the Metasploitable system and are categorized based on their severity.

Apache Outdated Version (Apache 2.2.8)

- **Description:** The system is running an outdated version of Apache (2.2.8), which has reached its End of Life (EOL).

- **Risk Factor:** High exploitation risk due to known vulnerabilities in outdated versions.
- **Severity:** Critical

PHP Info Disclosure (`phpinfo.php` found)

- **Description:** The `phpinfo.php` script exposes sensitive system information, such as PHP environment settings.
- **Risk Factor:** High potential for information leakage, aiding attackers in further exploitation.
- **Severity:** Critical

FTP (vsftpd 2.3.4) Vulnerability

- **Description:** An outdated version of vsftpd (2.3.4) is running, which is known to have a backdoor vulnerability.
- **Risk Factor:** High chance of unauthorized access through the backdoor.
- **Severity:** Critical

OpenSSH (OpenSSH 4.7p1 Debian 8ubuntu1)

- **Description:** An outdated version of OpenSSH is running, making it susceptible to multiple exploits.
- **Risk Factor:** High potential for system compromise via SSH access.
- **Severity:** Critical

Cross-Site Tracing (HTTP TRACE Enabled)

- **Description:** The HTTP TRACE method is active, making the system vulnerable to Cross-Site Tracing (XST) attacks.
- **Risk Factor:** High risk of sensitive information, such as cookies, being stolen.
- **Severity:** High

phpMyAdmin Directory Unprotected

- **Description:** The `/phpMyAdmin/` directory is accessible without restrictions, potentially allowing unauthorized users to manage databases.
- **Risk Factor:** High risk of unauthorized database access and manipulation.
- **Severity:** High

Apache `mod_negotiation` MultiViews Enabled

- **Description:** MultiViews is enabled, allowing attackers to brute-force file names.
- **Risk Factor:** Potential risk of discovering and accessing sensitive files.

- **Severity:** Medium

Directory Indexing Enabled (Multiple Directories)

- **Description:** Directory indexing is enabled for /doc/, /icons/, and /test/, exposing the system structure.
- **Risk Factor:** Moderate risk of information disclosure assisting attackers in mapping the system.
- **Severity:** Medium

Reporting Guidelines

I encourage researchers to review these findings and address the vulnerabilities based on their severity. To report future vulnerabilities or collaborate on resolving these issues, please follow these guidelines:

- **Proof of Concept (PoC):** Include clear instructions or screenshots that demonstrate the vulnerability.
- **Description of the Issue:** Explain the vulnerability, its impact, and how it could be exploited.
- **Supporting Evidence:** Provide HTTP requests, responses, or code snippets that help reproduce the issue.

Reporting a Vulnerability

All vulnerability reports should be submitted via email to **metasploitable@disclosure.com**. Please refrain from publicly disclosing any information about the vulnerability until it has been verified and fixed.

Responsible Disclosure

I request that vulnerabilities are reported privately and not disclosed to third parties or the public without explicit permission. I will work to address the issues and provide regular updates on the remediation process.

What You Can Expect from Me

When you share your contact information with me, I commit to:

- Acknowledging your report within 3 business days.
- Confirming the existence of the vulnerability and being transparent about remediation efforts.
- Maintaining open communication to resolve any issues.

Questions

For any questions or suggestions regarding this policy, please contact me at **metasploitable@disclosure.com**.