Vulnerability Assessment

Marlin_spike

Report of Findings

Candidate Name: Ian G. Donohue

VulnHub

October 21, 2025

Version: 1.0

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

vulnhub Contacts		
Contact	**Title**	**Contact Email**

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Ian Donohue	Security Analyst	

3 Executive Summary

MarlinSpike is a purposefully vulnerable virtual machine available on Vulnhub, a website that is reknown for education virtual machines. Ian Donohue is within his legal right to perform a Network Penetration Test and Vulnerability assessment of these virtual machines. Here within document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Ian is testing Marlinspike as a 'blackbox' without credentials or any advance knowledge of any externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Ian's assessment labs and hosted locally.

This being the vulnerability assessment and not a penetration test, the vulnerabilties and exploits eluded to can only be assured through manually penetration testing, in a sandbox environment with guidance of the vulnerability assessment.

3.2 Scope

The scope of this assessment was one internal IP address

In Scope Assets

Host/URL/IP Address	Description
10.0.2.3	internal network

3.3 Assessment Overview and Recommendations

During the penetration test against MarlinSpike, Ian identified seven findings that threaten the confidentiality, integrity, and availability of MarlinSpike's information systems. The findings were categorized by severity level, with CVE and CVSS ratings.

VulnHub should create a remediation plan based on the remediation section of this report, addressing all high findings as soon as possible according to the needs of the business. Vulnhub should also consider performing periodic vulnerability assessments if they are not already being performed.

4 Network Penetration Test Assessment Summary

Ian began all testing activities from the perspective of an unauthenticated user on the internet. Vulnhub provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

In the course of this penetration test **1 Critical**, **2 High** and **4 Medium** vulnerabilities were identified:

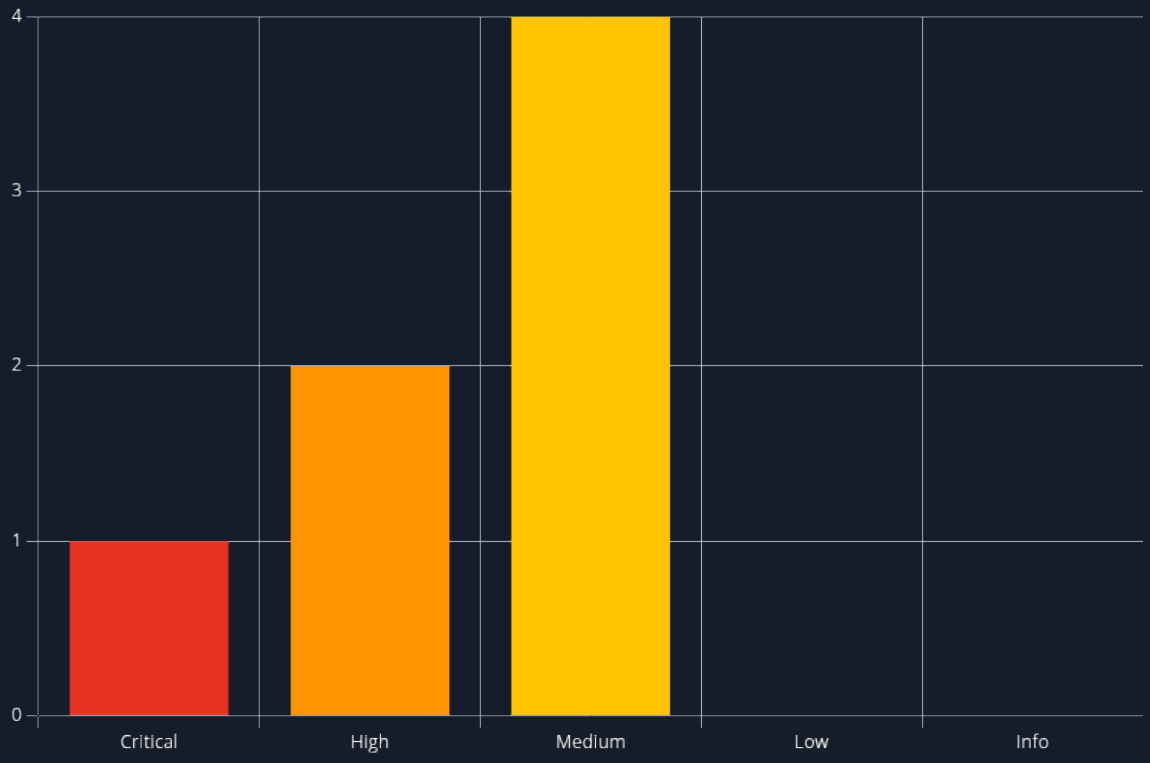

Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	10.0 (Critical)	Wordpress v4.9 exposes site to multi critical vulnerabilities	10
2	7.5 (High)	FTP Service Running Outdated ProFTPD (v1.3.3c) vulnerable to RCE	12
3	7.5 (High)	Wordpress XML-rpc interface enables brute-force and DoS attacks	13
4	5.3 (Medium)	Information disclosure via apache configuration weakness	14

5 Internal Network Compromise Walkthrough

5.1 Detailed Walkthrough

6 Remediation Summary

7 Technical Findings Details

1. Wordpress v4.9 exposes site to multi critical vulnerabilities - Critical

CWE	CWE-1329 - Reliance on Component That is Not Updateable
CVSS 3.1	10.0 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Root Cause	This version of wordpress leads to a slew of problems suchs as , but not limited to: cwe 79 - xss cwe 89 - sqli cwe 434 - unrestricted file upload cwe 862 - missing auth cwe 306 - exposed admin endpoints
Impact	exposed internal directories and verbose headers provide attackers with inside tinto server configuration,potentional entry points, and system fingerprinting. this can be leveraged to identify known exploits or add to a plan of attack
Remediation	1.upgrade apache to the latest stable version 2.implement access controls or authentication on sensitive directories. 3.configure apache to suppress unncessary http headers
References	https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html

Finding Evidence

We identified an XXE injection vulnerability in the web application. The XML parser allowed the definition of XXEs, which could create a malicious XML document. The XXE contained a URL that referenced an external domain. After the XXE was dereferenced by the parser, the web application interacted with this domain, which is evident from the DNS requests.

Extensible Markup Language (XML) is a standardized markup language and file format for storing, transmitting, and reconstructing arbitrary data. The language encodes data in a format that is readable by both humans and machines. The structure of an XML document is defined in the XML standard. The standard provides for a concept called an entity. Entities provide the ability to reference content that is provided remotely by a server or resides locally on the server. When the XML parser evaluates the XML document, the entity it contains is replaced with the referenced value. Entities are defined in so-called Document Type Definitions (DTDs).

DTDs define the structure and composition of an XML document. They can either be completely contained in the XML document itself, so-called internal DTDs, or they can be loaded from another location, so-called external DTDs. A combination of both variants is also possible. XML External Entities (XXE) are a special form of XML entities whose contents are loaded from outside the DTD in which they are declared.

An XXE is declared in the DTD with the SYSTEM keyword and a URI from where the content should be loaded. For example:

```
<!DOCTYPE dtd [ <!ENTITY xxe SYSTEM "http://syslifters.com" > ]>
```

The URI can also use the `file://` protocol scheme. Content can be loaded from local files as a result. For example:

```
<!DOCTYPE dtd [ <!ENTITY xxe SYSTEM "file:///path/to/local/file" > ]>
```

When evaluating XML documents, the XML parser replaces occurring XXEs with the contents by dereferencing the defined URIs. If the URI contains manipulated data, this could have serious consequences. An attacker can exploit this to perform server-side request forgery (SSRF) attacks and compromise the underlying server or other backend infrastructure. XXE injection vulnerabilities can also be exploited to cause service/application downtime (denial of service) or expose sensitive data such as local system files.

2. FTP Service Running Outdated ProFTPD (v1.3.3c) vulnerable to RCE - High

CWE	CWE-912 - Hidden Functionality
CVSS 3.1	7.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Root Cause	CVE-2015-3306 ProFTPD 1.3.5 contains a remote code execution vulnerability via the mod_copy module which allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands. CVE-2010-20103 This vulnerability was the result of a malicious backdoor being embedded in the official ProFTPD 1.3.3c source code. The affected source tarballs were available for download between November 28 and December 2, 2010, after the project's distribution server was compromised
Impact	Unauthorized access via a backdoor as awell as the ability to access a remote code execution
Remediation	Upgrade ProFTPD to the latest secure version or disable FTP if not required. Consider replacing it with SFTP.", "references": ["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4221", "https://www.exploit-db.com/exploits/15150"
References	-

Finding Evidence

3. Wordpress XML-rpc interface enables brute-force and DoS attacks - High

CWE	CWE-307 - Improper Restriction of Excessive Authentication Attempts
CVSS 3.1	7.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Root Cause	The XML-RPC interface is enabled and publicly accessible. This feature is often exploited for brute force attacks or DDoS amplification via pingbacks. Although legitimate, it increases the attack surface if not actively used.
Impact	brute-force enumeration leads to expansion of attack surface and increase visibility and vulnerabilty of target by informaton gleaned.
Remediation	disable xml rpc if it is not being used - if it is being used, restrict use through the IP
References	-

4. Information disclosure via apache configuration weakness - Medium

CWE	CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
CVSS 3.1	5.3 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
Root Cause	The Apache 2.4.18 web server on port 80 reveals sensitive information due to the exposure of internal directories (e.g., '/secret/') and default verbose HTTP headers. These misconfigurations could aid attackers in reconnaissance or exploitation.", 1.Apache version: Apache/2.4.18 (Ubuntu)\nDiscovered via directory enumeration: /secret/ 2.HTTP Headers disclosed: Server, X-Powered-By 3.Supported Methods: GET, HEAD, POST, OPTIONS
Impact	This allows bad actors to gather more valuable information abou the target
Remediation	• The application should send all sensitive data in the body of an HTTP message, e.g. in the body of a POST request. • Furthermore, the transmission should be secured via encrypted communication via HTTPS.
References	-

Finding Evidence

5. OpenSSH 7.2p2 Detected - Medium

CWE	CWE-1104 - Use of Unmaintained Third Party Components
CVSS 3.1	5.3 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Root Cause	disclosure possible due to outdated version, no direct rce demonstrated
Impact	it may be vulnerable known attack as mitm downgrade attacks or integrity bypass via terrapin older versions use weak cipher suites, increasing availability during brute force deprecated versions may allow attackers to bypass authentication or execute code remotely
Remediation	upgrade openssh to the latest stable version support by the operating system, ideally version 8.9 or later
References	-

Finding Evidence

6. Sensitive Directories Discovered via Directory Enumeration - Medium

CWE	CWE-548 - Exposure of Information Through Directory Listing
CVSS 3.1	5.3 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Root Cause	CWE-548: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') This weakness occurs when an application uses user-supplied input to access files or directories without properly neutralizing "dot-dot-slash" (`../`) sequences
Impact	exposure of sensitive data and exposing the contents of a directory can lead to an attacker gaining access to source code or providing useful information for the attacker to devise exploits, such as creation times of files or any information that may be encoded in file names. The directory listing may also compromise private or confidential data.
Remediation	Remediate directory listing exposure • **Disable directory listing on the web server:** Configure your web server (e.g., Nginx, Apache, IIS) to prevent it from generating directory listings when no index file is present. • **Use default index files:** Place a default file, such as `index.html`, in each directory to be displayed instead of a listing of its contents. • **Restrict access:** Use file permissions to restrict access to sensitive directories, ensuring that only authorized users can view their contents. • **Remove sensitive files:** Ensure that sensitive files, such as configuration files, backup files, or crash dumps, are not stored in web-accessible directories. • **Follow security best practices:** Avoid placing important files in publicly accessible locations and adopt a "need to know" requirement for both the document and the server root
References	-

Finding Evidence

7. Weak SSH Configuration Detected - Medium

CWE	-
CVSS 3.1	4.8 / CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
Root Cause	OpenSSH version: 7.2p2 Ubuntu-4ubuntu2.2\nFailing KEX: ecdh-sha2-nistp256, nistp384, nistp521, diffie-hellman-group14-sha1\nFailing Host Key: ssh-rsa (2048-bit, SHA-1)\nWarnings on RSA SHA2-256/512 due to key length. The SSH service is using a combination of outdated and weak cryptographic algorithms. Key exchange algorithms such as `ecdh-sha2-nistp256/384/521` and `diffie-hellman-group14-sha1` are either deprecated, use weak hashes (SHA-1), or are suspected of being compromised. The host key algorithm `ssh-rsa` uses SHA-1 and is deprecated as of OpenSSH 8.8. Additionally, 2048-bit RSA keys offer only 112 bits of symmetric strength, which is below modern recommended thresholds. https://latacora.micro.blog/2018/04/03/ssh.html https://www.openssh.com/txt/release-8.8 https://infosec.mozilla.org/guidelines/openssh.html
Impact	
Remediation	Upgrade OpenSSH to the latest stable version. Disable SHA-1 based algorithms and NIST curves suspected of being compromised. Use only strong, modern cryptography such as curve25519-sha256 and ed25519 host keys with >= 3072-bit RSA or ECDSA keys where needed.
References	-

Finding Evidence

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of vulnhub's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

sudo nmap -A -O -sV -sC 10.0.2.3 -Pn Starting Nmap 7.95 (https://nmap.org) at 2025-10-21 01:33 EDT Nmap scan report for 10.0.2.3 Host is up (0.0012s latency). Not shown: 997 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp ProFTPD 1.3.3c 22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0) | ssh-hostkey: | 2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c: 54:7e:54 (RSA) | 256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA) |_ 256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519) 80/tcp open http Apache httpd 2.4.18 ((Ubuntu)) |_http-title: Site doesn't have a title (text/html). |_http-server-header: Apache/2.4.18 (Ubuntu) MAC Address: 08:00:27:F9:22:5B (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Device type: general purpose Running: Linux 3.X|4.X OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/ o:linux:linux_kernel:4 OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16 Network Distance: 1 hop Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE HOP RTT ADDRESS 1 1.17 ms 10.0.2.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds

End of Report

This report was rendered
by SysReptor with
♥