VAPT Report for 212.83.142.84 (Born2Root VM)

Author: Alok Kumar Sahu
Environment: Kali Linux (Attacker), Born2Root VM (Target)
Date: 2025-12-03

1. Executive Summary

This report documents the vulnerability assessment and penetration testing (VAPT) conducted on the Born2Root VM (IP: 212.83.142.84). The objective was to identify potential vulnerabilities, assess their severity, and suggest remediation steps for mitigating risks.

Due to **RAM limitations**, I was unable to use **Metasploitable 3** for the assessment, which was originally intended. As a result, I used the **Born2Root VM**, a vulnerable machine that allows for similar testing scenarios. This environment provided sufficient opportunities to assess security weaknesses effectively.

The report provides:

- Detailed vulnerability findings from tools like OpenVAS, Nmap, and Nikto.
- Evidence in the form of screenshots and tool outputs.
- Actionable remediation steps to mitigate the identified vulnerabilities.

2. Tools & Environment

2.1 Primary Tools Used

- **Kali Linux (Attacker & Host):** Nmap, OpenVAS, Nikto
- **Born2Root VM (Target):** Vulnerable system to be tested
- **Supporting Tools:**
  - OpenVAS for vulnerability scanning
  - Nmap for network exploration and vulnerability discovery
  - Nikto for web server scanning

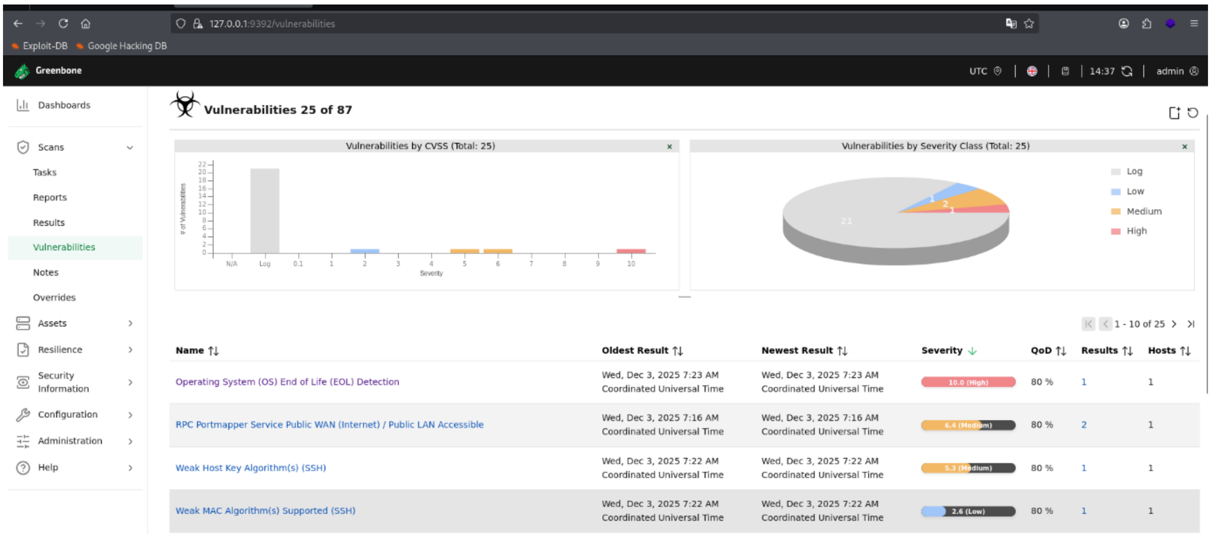
2.2 Files Captured & Provided

- **openvas_scan_report.xml:** OpenVAS vulnerability scan report
- **nmap_scan_report.txt:** Nmap scan results
- **nikto_scan_report.txt:** Nikto scan results
- **Screenshots**: Provided as evidence for each vulnerability found

3. Vulnerabilities Breakdown

3.1 Operating System (OS) End of Life (EOL) Detection

- **Affected IP:** 212.83.142.84
- **Service:** N/A
- **Risk Level:** High (CVSS: 10.0)
- **Description:** The target system is running an EOL OS (Debian), which no longer receives security updates or patches. This presents a critical security risk.
- **Evidence:**



Vulnerabilities 25 of 87

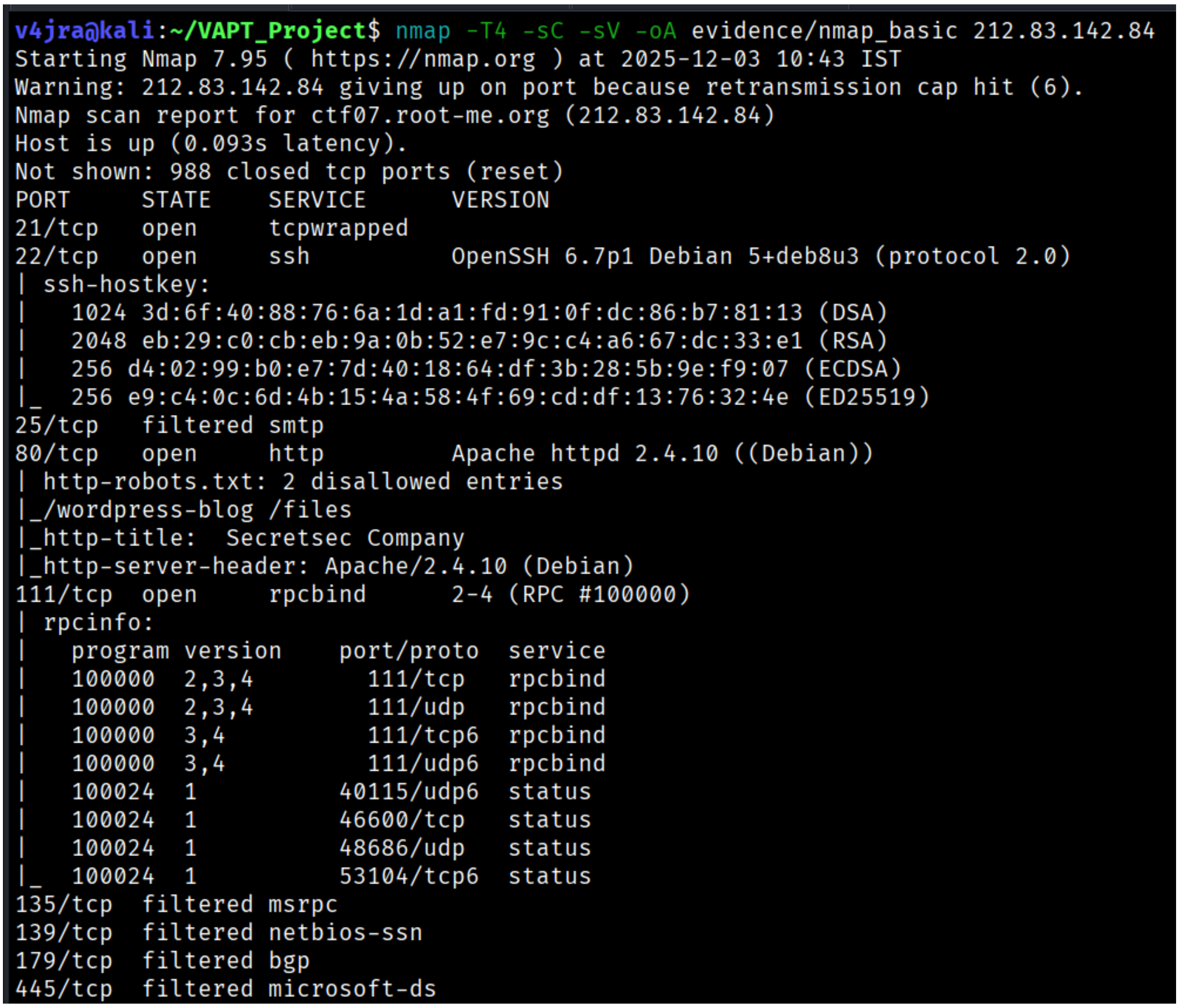
Name	Oldest Result	Newest Result	Severity	QoD	Results	Hosts
Operating System (OS) End of Life (EOL) Detection	Wed, Dec 3, 2025 7:23 AM Coordinated Universal Time	Wed, Dec 3, 2025 7:23 AM Coordinated Universal Time	10.0 (High)	80 %	1	1
RPC Portmapper Service Public WAN (Internet) / Public LAN Accessible	Wed, Dec 3, 2025 7:16 AM Coordinated Universal Time	Wed, Dec 3, 2025 7:16 AM Coordinated Universal Time	6.4 (Medium)	80 %	2	1
Weak Host Key Algorithm(s) (SSH)	Wed, Dec 3, 2025 7:22 AM Coordinated Universal Time	Wed, Dec 3, 2025 7:22 AM Coordinated Universal Time	5.3 (Medium)	80 %	1	1
Weak MAC Algorithm(s) Supported (SSH)	Wed, Dec 3, 2025 7:22 AM Coordinated Universal Time	Wed, Dec 3, 2025 7:22 AM Coordinated Universal Time	2.6 (Low)	80 %	1	1

Figure 1: OpenVAS EOL detection report showing the vulnerability

- **Remediation:**
  - Upgrade the OS to a supported version or migrate to a newer, secure operating system.

3.2 Weak SSH Host Key Algorithm(s)

- **Affected IP:** 212.83.142.84
- **Service:** SSH
- **Risk Level:** Medium (CVSS: 6.4)
- **Description:** The system is using weak SSH host key algorithms that can be exploited by attackers.
- **Evidence:**



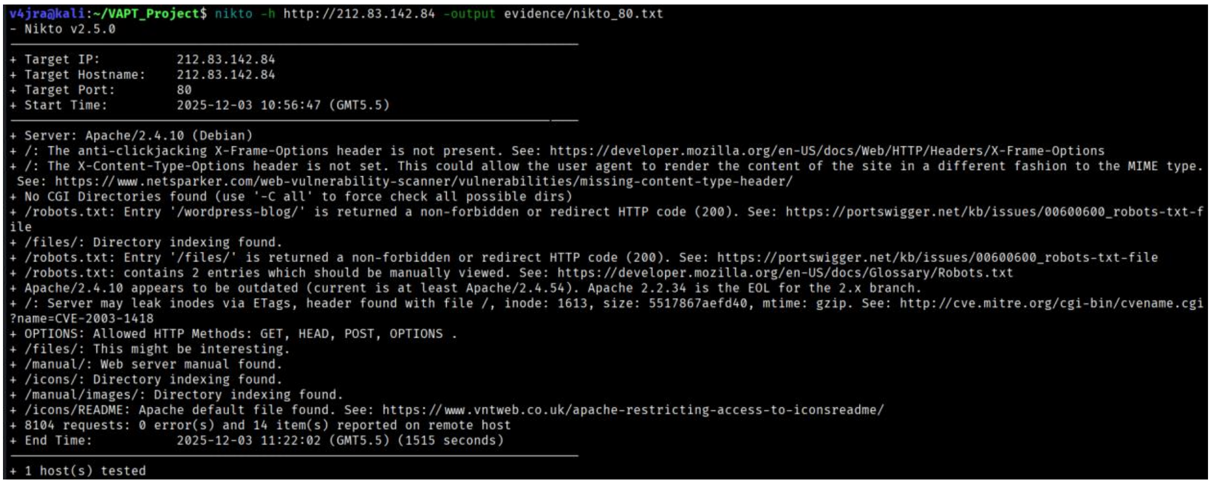
```
v4jra@kali:~/VAPT_Project$ nmap -T4 -sC -sV -oA evidence/nmap_basic 212.83.142.84
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 10:43 IST
Warning: 212.83.142.84 giving up on port because retransmission cap hit (6).
Nmap scan report for ctf07.root-me.org (212.83.142.84)
Host is up (0.093s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     tcpwrapped
22/tcp   open     ssh          OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 3d:6f:40:88:76:6a:1d:a1:fd:91:0f:dc:86:b7:81:13 (DSA)
|   2048 eb:29:c0:cb:eb:9a:0b:52:e7:9c:c4:a6:67:dc:33:e1 (RSA)
|   256 d4:02:99:b0:e7:7d:40:18:64:df:3b:28:5b:9e:f9:07 (ECDSA)
|_  256 e9:c4:0c:6d:4b:15:4a:58:4f:69:cd:df:13:76:32:4e (ED25519)
25/tcp   filtered smtp
80/tcp   open     http         Apache httpd 2.4.10 ((Debian))
| http-robots.txt: 2 disallowed entries
|_/wordpress-blog /files
|_http-title:  Secretsec Company
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp  open     rpcbind      2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          40115/udp6  status
|   100024  1          46600/tcp   status
|   100024  1          48686/udp   status
|_  100024  1          53104/tcp6  status
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
179/tcp  filtered bgp
445/tcp  filtered microsoft-ds
```

Figure 2: Nmap output showing weak SSH algorithms

- **Remediation:**
  - Disable weak SSH algorithms in the /etc/ssh/sshd_config file.
  - Use ECDSA or ED25519 algorithms for enhanced security.

3.3 HTTP Directory Indexing Found

- **Affected IP:** 212.83.142.84
- **Service:** Apache HTTP
- **Risk Level:** Medium (CVSS: 5.3)
- **Description:** The Apache HTTP server on the target system allows directory indexing, which can expose sensitive files and directories to unauthorized users.
- **Evidence:**



```
v4jra@kali:~/VAPT_Project$ nikto -h http://212.83.142.84 -output evidence/nikto_80.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          212.83.142.84
+ Target Hostname:    212.83.142.84
+ Target Port:        80
+ Start Time:         2025-12-03 10:56:47 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
 See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/wordpress-blog/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-f
ile
+ /files/: Directory indexing found.
+ /robots.txt: Entry '/files/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 1613, size: 5517867aefd40, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi
?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /files/: This might be interesting.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /manual/images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8104 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2025-12-03 11:22:02 (GMT5.5) (1515 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 3: Nikto output showing directory indexing vulnerability

- **Remediation:**
  - Disable directory indexing in the Apache configuration by setting Options -Indexes in the Apache server config.

4. Conclusion

This report has identified several vulnerabilities within the Born2Root VM:

- Critical risk due to the EOL OS that requires immediate action to mitigate the threat of unpatched vulnerabilities.
- Medium risks involving weak SSH algorithms and HTTP directory indexing, which can be exploited to gain unauthorized access or exposure of sensitive data.

It is recommended to:

- Upgrade the OS to a supported version to eliminate the EOL risk.
- Configure SSH to use stronger algorithms.
- Secure the Apache HTTP server by disabling directory indexing.

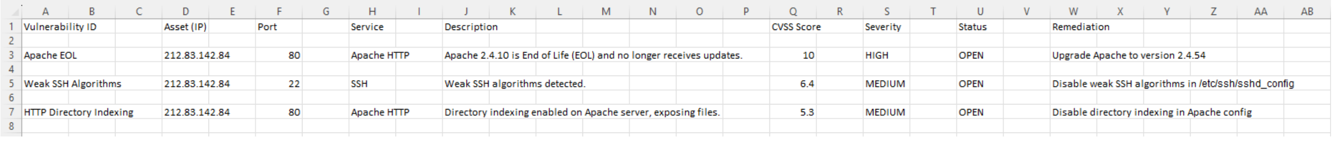
5. Key Learnings

1. **Vulnerability Detection:** Learned how to use OpenVAS, Nmap, and Nikto for effective vulnerability scanning.
2. **Risk Mitigation:** Understanding how to configure and patch systems to reduce exposure to known vulnerabilities.
3. **Security Best Practices:** Emphasized the importance of maintaining up-to-date operating systems and securing SSH and web server configurations.

6. References

Nmap: https://nmap.org
OpenVAS: https://www.openvas.org
Nikto: https://cirt.net/Nikto2
CVE Database: https://cve.mitre.org

7. Appendix: Vulnerability Tracking Spreadsheet



Vulnerability ID	Asset (IP)	Port	Service	Description	CVSS Score	Severity	Status	Remediation
Apache EOL	212.83.142.84	80	Apache HTTP	Apache 2.4.10 is End of Life (EOL) and no longer receives updates.	10	HIGH	OPEN	Upgrade Apache to version 2.4.54
Weak SSH Algorithms	212.83.142.84	22	SSH	Weak SSH algorithms detected.	6.4	MEDIUM	OPEN	Disable weak SSH algorithms in /etc/ssh/sshd_config
HTTP Directory Indexing	212.83.142.84	80	Apache HTTP	Directory indexing enabled on Apache server, exposing files.	5.3	MEDIUM	OPEN	Disable directory indexing in Apache config

8. Key Learnings from Theoretical Knowledge

1. **Security Assessment & Tools**:
   - Gained practical experience using open-source tools like **OpenVAS**, **Nmap**, and **Nikto** for vulnerability scanning and exploitation.
   - Understood how to evaluate systems effectively without relying on paid tools, following frameworks like **NIST**.
2. **VAPT Methodology:**
   - Learned the four key phases: **Planning**, **Discovery**, **Attack**, and **Reporting**, which ensure thorough testing and proper documentation of findings.
3. **Risk Assessment**:
   - Gained insights into how to assess vulnerabilities using **CVSS** scores and categorize risks using a **Risk Matrix** to prioritize remediation efforts.
4. **Security Standards & Compliance**:
   - Understanding **OWASP Top 10** and **CIS Benchmarks** helped prioritize vulnerabilities and align the testing with industry standards.
5. **Documentation & Reporting**:
   - Learned how to document findings clearly and concisely using tools like **Dradis CE**, ensuring actionable remediation steps and professional reporting.