Vulnerability Assessment and Penetration Testing (VAPT) of Metasploitable Using OpenVAS

Executive Summary

This VAPT assessment was conducted on the vulnerable Metasploitable machine using Kali Linux and OpenVAS in a controlled lab environment. The scan showed many high-risk vulnerabilities, outdated services, default credentials, RCE (Remote code Execution), and misconfigurations. Across services such as FTP, SSH, HTTP, and SMB. These issues show how easy it is for an attacker to gain unauthorized access and execute malicious programs/software on a system.

Overall, the system's security posture is rated as highly vulnerable. Immediate remediation—such as applying updates, removing backdoored services, and enforcing stronger authentication—is necessary to reduce the risk of exploitation.

Setup & Environment

The testing environment was created using **Kali Linux** as the attacker machine and **Metasploitable** as the vulnerable target system. Both virtual machines were hosted in VirtualBox and configured under a Host-Only network so they could communicate securely without internet exposure. Kali Linux provided the required VAPT tools such as OpenVAS, while Metasploitable offered intentionally vulnerable services for assessment. This isolated setup ensured safe testing and accurate vulnerability identification.

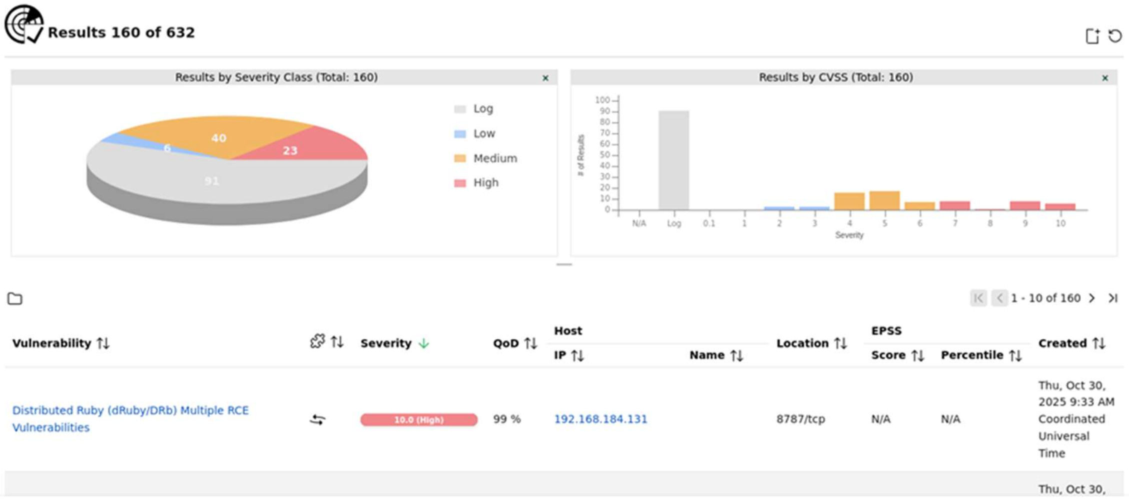
- Installed Kali Linux (attacker VM)
- Downloaded and imported Metasploitable (target VM)
- Configured VirtualBox Host-Only Adapter
- Verified connectivity using ping
- Started OpenVAS on Kali for scanning

Vulnerability Scanning (OpenVAS)

Setup Summary:

- PostgreSQL initialized successfully
- Scanner configured with SSH credential (authenticated scan)
- Target: Metasploitable
- Config: “Full and Fast”

Report Screenshot:



Results 160 of 632

Vulnerability ⇅	⇅	Severity ↓	QoD ⇅	Host		Location ⇅	EPSS		Created ⇅
				IP ⇅	Name ⇅		Score ⇅	Percentile ⇅	
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	⇆	10.0 (High)	99 %	192.168.184.131		8787/tcp	N/A	N/A	Thu, Oct 30, 2025 9:33 AM Coordinated Universal Time
									Thu, Oct 30,

Key Findings

The OpenVAS scan on the Metasploitable 2 machine revealed multiple high-risk vulnerabilities including default credentials, outdated software versions, remote code execution flaws, and insecure configurations. These weaknesses affect critical services such as MySQL, PostgreSQL, FTP, Apache, OpenSSL, Tomcat, and SMB. The following table summarizes the most significant findings discovered during the assessment.

Vulnerability Assessment Table

Finding / CVE	Severity	Port	Description	CVSS
MySQL Default Credentials	High	3306	Root login allowed with no password.	9.8
PostgreSQL Default Credentials	High	5432	Weak default password 'postgres'.	9
FTP Default Creds (msfadmin)	High	21 / 2121	Known username/password allow access.	7.5
vsftpd Backdoor (CVE-2011-2523)	High	21 / 6200	Backdoored version opens shell on port 6200.	9.8
PHP CGI Argument Injection (CVE-2012-1823)	High	80	PHP CGI allows execution via crafted parameters.	9.8
Ghostcat AJP RCE (CVE-2020-1938)	High	8009	Apache Tomcat AJP file inclusion / RCE.	9.8
OpenSSL CCS Injection (CVE-2014-0224)	High	TLS	Allows MITM attack altering handshake.	7.4
DistCC Remote Code Execution (CVE-2004-2687)	High	3632	Remote shell execution via distcc daemon.	9.8
Unencrypted Telnet Service	Medium	23	Login credentials transmitted in cleartext.	6.5
Outdated Apache HTTP Server	Medium	80	Running vulnerable, unpatched Apache version.	5.8
SSL Weak Cipher Suites Enabled	Medium	443	Supports export-grade and weak ciphers.	6

Samba SMBv2 Insecure Configuration	Medium	139 / 445	Older SMB version exposed to attacks.	5.5
Anonymous FTP Login Enabled	Medium	21	Allows login without authentication.	5.3
SSLv3 Protocol Supported	Low	443	Outdated SSLv3 susceptible to POODLE.	4.3
Expired SSL Certificate	Low	443	Certificate validity expired; not trusted.	3.5

Risk Assessment (CVSS + Likelihood/Impact)

CVSS-Based Severity Overview

Severity	Count	Examples
High (CVSS > 7.0)	8	RCE (vsftpd backdoor, PHP CGI), Ghostcat (AJP), MySQL root
Medium (4.0 - 6.9)	5	Telnet enabled, weak ciphers, outdated Apache
Low (< 4.0)	2	SSLv3 enabled, expired certificate

The CVSS severity table shows how serious the vulnerabilities are. Most findings are High severity, meaning they can be easily exploited and cause major damage. Medium issues are less dangerous but still weaken security, while Low issues have minimal impact but should still be fixed when possible.

Likelihood vs. Impact Matrix

Impact ↓ / Likelihood →	**Low**	**Medium**	**High**
High Impact	–	OpenSSL CCS Injection	vsftpd Backdoor, Ghostcat RCE, PHP CGI RCE, MySQL Default Root
Medium Impact	–	Weak SSL Ciphers, Outdated Apache	Anonymous FTP, SMB Insecure
Low Impact	Expired SSL Cert	SSLv3 Enabled	Telnet Enabled

The Likelihood vs. Impact matrix shows how each vulnerability compares in terms of how easy it is to exploit and how much damage it can cause. High-likelihood and high-impact issues are the most dangerous because they are easy to exploit and lead to serious compromise. Medium and low categories help show which vulnerabilities are less urgent but still important to fix, allowing the risks to be prioritized clearly.

Risk Evaluation Summary

- **High-risk vulnerabilities** are those that provide remote execution, full authentication bypass, or sensitive data access (e.g., MySQL root, Ghostcat, vsftpd backdoor).
- **Medium-risk issues** weaken the security posture but require additional conditions for exploitation (e.g., outdated Apache, weak ciphers).
- **Low-risk issues** do not directly allow compromise but degrade encryption trust (SSLv3, expired certificate).

Remediation Recommendations

1. High Severity Remediation

High-severity remediation focuses on fixing the most dangerous vulnerabilities first, especially those that allow remote code execution, default logins, or full system compromise. Addressing these issues immediately reduces the highest risks and prevents attackers from easily gaining control of the system.

- **Change all default credentials** for MySQL, PostgreSQL, FTP, and Telnet.
- **Patch high-risk RCE vulnerabilities**: vsftpd backdoor, DistCC, PHP CGI, and Ghostcat.
- **Update all outdated services** (Apache, Tomcat, OpenSSL).
- **Disable or restrict dangerous services**: AJP, distcc, Telnet, FTP, anonymous login.
- **Apply strong authentication** for all exposed ports.

2. Medium Severity Remediation

Medium-severity remediation focuses on fixing vulnerabilities that do not cause immediate system compromise but still weaken security and increase the attack surface. Addressing these issues helps prevent attackers from exploiting misconfigurations or outdated services and strengthens the overall security posture.

- Disable **weak SSL/TLS ciphers** and enforce TLS 1.2/1.3.
- Upgrade **Samba/SMB** and disable SMBv1.
- Restrict guest/anonymous access.
- Harden Apache configuration and remove unnecessary modules.

3. Low Severity Remediation

Low-severity remediation focuses on minor issues that do not pose an immediate threat but still affect system trust and best practices. Fixing these helps improve overall security hygiene and prevents small weaknesses from becoming bigger problems over time.

- Disable **SSLv3 entirely** to prevent POODLE attacks.
- Renew **expired SSL certificates** and apply modern CA-signed certificates.

General Best Practices

General best practices help maintain long-term security by ensuring the system stays updated, properly configured, and monitored. Following these practices reduces future risks, prevents recurring vulnerabilities, and keeps the overall environment more resilient against attacks.

- Perform regular patch cycles.
- Apply least privilege access control.
- Segregate internal services with firewall rules.
- Monitor logs for abnormal access.

Conclusion

This VAPT assessment demonstrated how multiple vulnerabilities across default credentials, outdated services, and insecure configurations can significantly weaken a system’s security posture. The findings clearly show that Metasploitable contains high-risk issues that could lead to full system compromise if left unresolved. By applying the recommended remediation steps and following security best practices, these weaknesses can be effectively reduced and the overall environment made more secure. This exercise also reinforces the importance of regular scanning, timely patching, and continuous monitoring to maintain strong cybersecurity hygiene.

Key Takeaways

- High-severity issues must be fixed immediately to prevent compromise.
- Medium/low issues still affect overall security hygiene.
- Continuous patching and monitoring are essential for long-term protection.

References

1. **OpenVAS Documentation**, Greenbone Networks.
   https://docs.greenbone.net
2. **CVSS v3.1 Specification**, FIRST Organization.
   https://www.first.org/cvss
3. **Apache HTTP Server Documentation.**
   https://httpd.apache.org/docs/
4. **MySQL Security Best Practices**, Oracle.
   https://dev.mysql.com/doc/
5. **NIST National Vulnerability Database (NVD).**
   https://nvd.nist.gov/
6. **OpenVAS Tutorials & Troubleshooting Resources (YouTube)**

- https://www.youtube.com/watch?v=GS2zrZIMnaY
- https://www.youtube.com/watch?v=QSu-WNwn6cY
- https://www.youtube.com/watch?v=XQ3DaSw5dbA
- https://www.youtube.com/watch?v=DoNaGI1XHYE&t=655s