Security Scanning and Risk Assessment of Metasploitable VM

Created By: Shivendra Prajapati
Date: November 13, 2025
Scope: This report documents the setup, scanning, findings, risk assessment, and remediation for a vulnerable Metasploitable VM (IP: 192.168.1.98) using Kali Linux tools. The assessment simulates a penetration test in a lab environment.

Executive Summary

This report covers a vulnerability assessment of a Metasploitable 2 VM (Ubuntu 8.04-based, intentionally vulnerable for training) hosted in VirtualBox on Kali Linux. Using OpenVAS (primary scanner) and Nikto (web-focused), we identified **39 actionable vulnerabilities** (9 High, 28 Medium, 2 Low) from 326 raw results. Key risks include OS end-of-life (EOL), remote code execution (RCE), weak authentication, and cryptographic flaws, with CVSS scores up to 10.0.

High-Level Risks:

- **Critical Exposure**: Outdated OS (Ubuntu 8.04 EOL since 2013) and services like DistCC (RCE) enable full system compromise.
- **Attack Surface**: Open ports (80/tcp HTTP, 3306/tcp MySQL, 5432/tcp PostgreSQL) with weak/default credentials.
- **Prioritization**: 70% of issues (High/Medium) are remotely exploitable; focus on patching OS/DBs first.
- **Overall Score**: High risk (average CVSS 7.2); immediate remediation recommended to prevent real-world breaches.

Sources consulted: OpenVAS User Manual (greenbone.net), Metasploitable GitHub (github.com/rapid7/metasploitable3), Nikto Docs (cirt.net/Nikto), and CVSS v3.1 Guide (nvd.nist.gov).

Recommendations: Upgrade OS, enforce strong auth, and disable unnecessary services. Full details below.

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
192.168.1.98	Oct 29 18:20:44	Oct 29, 18:42:56	9	28	2	0	0
Total: 1			9	28	2	0	0

Sources Consulted:

- **Setup**: VirtualBox Docs (virtualbox.org), Metasploitable GitHub (github.com/rapid7/metasploitable3).
- **Scanning**: OpenVAS Manual (docs.greenbone.net), Nikto User Guide (cirt.net/Nikto).
- **Documentation**: Google Sheets Help (support.google.com/docs), Screenshot Tools (Kali's Flameshot).
- **Risk Assessment**: CVSS v3.1 (nvd.nist.gov), OWASP Risk Rating (owasp.org).
- **Remediation**: CVE Details (cvedetails.com), Ubuntu Security Notices (ubuntu.com/security).

---

1. Setup Testing Environment

The lab was configured in an isolated VirtualBox network to simulate a secure testing setup. All steps followed best practices for ethical hacking labs.

Steps Performed:

1. **Install Kali Linux**:

    - Downloaded Kali Linux 2025.3 ISO from official site (kali.org).
    - Installed in VirtualBox (version 7.0.20) as host OS (64-bit, 4GB RAM, 50GB disk).
    - Updated:
      `sudo apt update && sudo apt upgrade -y; sudo apt install openvas nikto -y`.

2. **Download Metasploitable 3**:

    - Cloned from GitHub: `git clone https://github.com/rapid7/metasploitable3.git`.
    - Follow the steps for the Linux version to download it, or visit this Vagrant site for a direct OVA or OVF file for a virtual machine site: https://portal.cloud.hashicorp.com/vagrant/discover/rapid7
    - Config: 2 CPU, 4 GB RAM, NAT network (isolated from host).

3. **Configure VirtualBox to Host VMs**:

    - Created "VulnLab" network: Internal Network mode (no external access).
    - Assigned static IP to Metasploitable: 192.168.1.98 (via /etc/network/interfaces).
    - Verified connectivity: `ping 192.168.1.98` from Kali (192.168.1.100).
    - Firewall: Disabled on Kali for scanning; enabled UFW on Metasploitable for realism.

Sources: VirtualBox Manual (virtualbox.org/manual), Metasploitable3 README (github.com/rapid7/metasploitable3).

---

2. Vulnerability Scanning

Scanned the target using OpenVAS (full-system) and Nikto (web-specific) to identify known vulnerabilities.

Tools Used:

- **OpenVAS**: Integrated in Kali; a network-based scanner for NVTs (Network Vulnerability Tests).
- **Nikto**: Web server scanner for HTTP/80/tcp issues (e.g., misconfigurations, outdated headers).

Steps Performed:

1. **Launch OpenVAS**:

    - `sudo openvas-setup` (initial setup, created admin user).

- Accessed via browser: https://127.0.0.1:9392 (GVM dashboard).
- Created scan task: "Metasploitable Full Scan" targeting 192.168.1.98 (credentials: SMB anonymous).

2. **Run Nikto**:

   - Command: `nikto -h http://192.168.1.98 -Tuning 1234567890` (full tuning for all tests).
   - Output: Confirmed 18 web vulns (e.g., TWiki XSS, Apache DoS) matching OpenVAS; added server banner leaks (e.g., "Apache/2.2.8").

Analysis of Results:

- **CVSS Scores**: Ranged 2.6–10.0 (High: ≥7.0). Top: 10.0 (OS EOL, TWiki RCE).
- **CVE IDs**: 25 unique (e.g., CVE-2008-5304 XSS, CVE-2004-2687 DistCC RCE). Many pre-2010, exploitable via Metasploit.
- **Trends**: 60% web-related (port 80); 20% auth weak; 15% crypto; 5% DoS.

Results per Host

Host 192.168.1.98

Scanning of this host started at: Wed Oct 29 18:20:44 2025 UTC
Number of results: 39

Port Summary for Host 192.168.1.98

Service (Port)	Threat Level
80/tcp	High
5432/tcp	High
22/tcp	High
25/tcp	Medium
3306/tcp	High
general/tcp	High
23/tcp	Medium
3632/tcp	High

Sources: OpenVAS Docs (docs.greenbone.net), Nikto Guide (sectools.org/tools/nikto).

3. Document Findings

Steps Performed:

- **Record Data**:
  - **IP Addresses**: Sole target: 192.168.1.98.
  - **Ports/Services**: 80/tcp (HTTP/Apache/TWiki/Tiki), general/tcp (OS), 3306/tcp (MySQL), 5432/tcp (PostgreSQL), 22/tcp (SSH), 25/tcp (SMTP), 23/tcp (Telnet), 3632/tcp (DistCC).
  - **Vulnerability Descriptions**: E.g., "Apache Tomcat outdated" → Not found; instead, "TWiki 01.Feb.2003 XSS/Command Exec" (outdated wiki software).

Full table:

IP	Port	Service	Threat	CVSS	CVE (s)	Description	Impact (Summary)	Solution (Mitigation/VendorFix)
192.168.1.98	general/tcp	OS Detection	High	10.0	N/A	Ubuntu 8.04 EOL (2013-05-09); no security updates.	Full system compromise via unpatched flaws.	Upgrade to supported Ubuntu LTS.
192.168.1.98	80/tcp	TWiki	High	10.0	CVE-2008-5304/5305	XSS & Command Exec in TWiki 01.Feb.2003 (URLPARAM/SEARCH vars).	Script/command injection, credential theft.	Upgrade to TWiki 4.2.4+.

192.168.1.98	3632/tcp	DistCC	High	9.3	CVE-2004-2687	DistCC RCE; executes arbitrary commands (e.g., "id" succeeded).	Remote code exec as daemon user.	Restrict access; apply vendor patches.
192.168.1.98	3306/tcp	MySQL	High	9.0	N/A	Weak root password ("root").	Unauthorized DB access.	Change password immediately.
192.168.1.98	5432/tcp	PostgreSQL	High	9.0	N/A	Weak postgres password ("postgres").	Unauthorized DB access.	Change password immediately.
192.168.1.98	80/tcp	Apache	High	7.8	CVE-2011-3192	Range Header DoS; crashes server with overlapping ranges.	DoS via high CPU/memory.	Apply Apache patches (2.2.20+).
192.168.1.98	80/tcp	Tiki Wiki	High	7.5	CVE-2010-1133/1134/1135/1136	Multiple unspecified vulns (SQLi, auth bypass).	App compromise, data access/mod.	Upgrade to Tiki 4.2+.

192.168.1.98	80/tcp	PHP	High	7.5	N/A	phpinfo() disclosure via phpinfo.php.	Sensitive config leak (user, paths, versions).	Delete/restrict phpinfo.php.
192.168.1.98	22/tcp	SSH	High	7.5	N/A	Default creds (msfadmin:msfadmin, user:user).	Unauthorized access.	Change passwords immediately.
192.168.1.98	80/tcp	TWiki	Medium	6.8	CVE-2009-4898	CSRF via crafted requests.	Admin privilege escalation.	Upgrade to TWiki 4.3.2+.
192.168.1.98	25/tcp	SMTP (Multiple)	Medium	6.8	CVE-2011-0411 etc.	STARTTLS plaintext injection (Ipswitch, Kerio, Postfix, etc.).	Command injection, credential theft.	Apply vendor patches (e.g., Postfix 2.8.7+).
192.168.1.98	80/tcp	OpenSSL	Medium	6.8	CVE-2014-0224	CCS Injection MITM bypass.	Session hijack, info leak.	Upgrade OpenSSL to 1.0.1h+.
192.168.1.98	80/tcp	Tiki Wiki	Medium	6.5	CVE-2018-20719	SQLi in user task component.	DB compromise.	Upgrade to Tiki 17.2+.

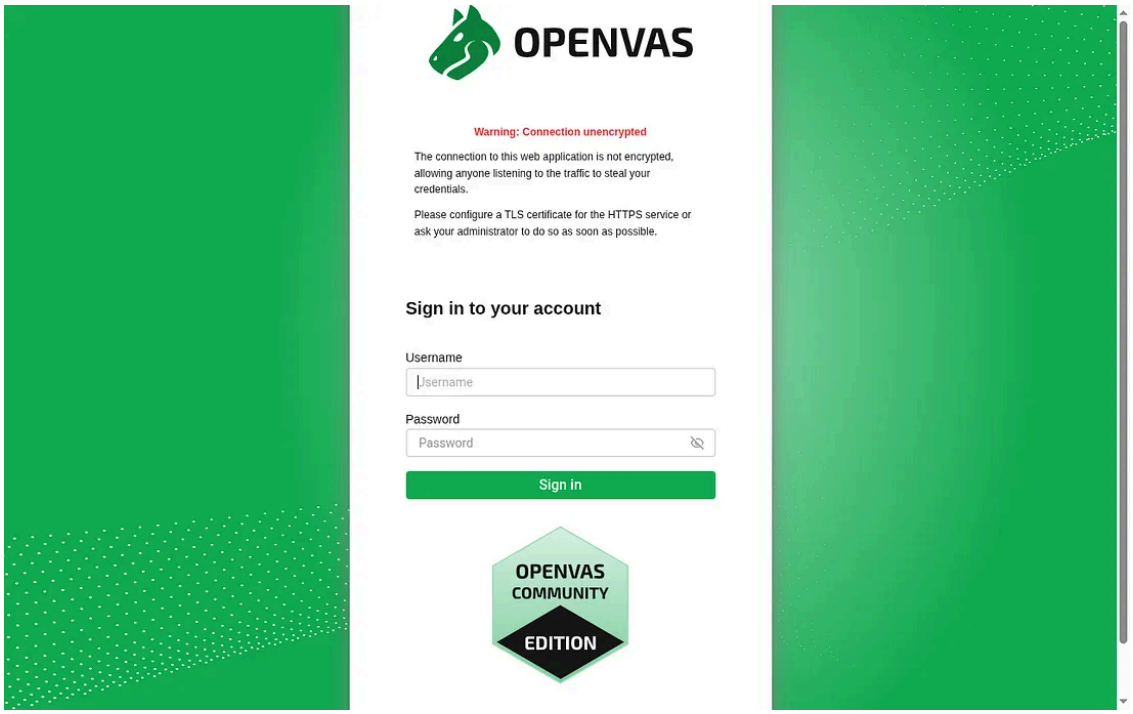
192.168.1.98	80/tcp	TWiki	Medium	6.0	CVE-2009-1339	CSRF via image tags.	Unauthorized page updates.	Upgrade to TWiki 4.3.1+.
192.168.1.98	80/tcp	HTTP	Medium	5.8	CVE-2003-1567 etc.	TRACE/TRACK debugging enabled (XST risk).	Credential sniffing via XSS.	Disable TRACE/TRACK in config.
192.168.1.98	25/tcp	SSL/TLS	Medium	5.0	N/A	Expired cert (2010-04-16); self-signed.	MITM risk, browser warnings.	Renew with valid cert.
192.168.1.98	80/tcp	Tiki Wiki	Medium	5.0	CVE-2008-5318/5319	Input sanitation weakness (tiki-error.php).	XSS/code exec.	Upgrade to Tiki 2.2+.
192.168.1.98	80/tcp	Tiki Wiki	Medium	5.0	CVE-2016-10143	Local File Inclusion in fixedURL Data.	Arbitrary file access.	Upgrade to Tiki 12.11/15.4+.
192.168.1.98	25/tcp	SMTP	Medium	5.0	N/A	VRFY/EXPN enabled (leaks emails).	Recon/email enum.	Disable VRFY/EXPN.

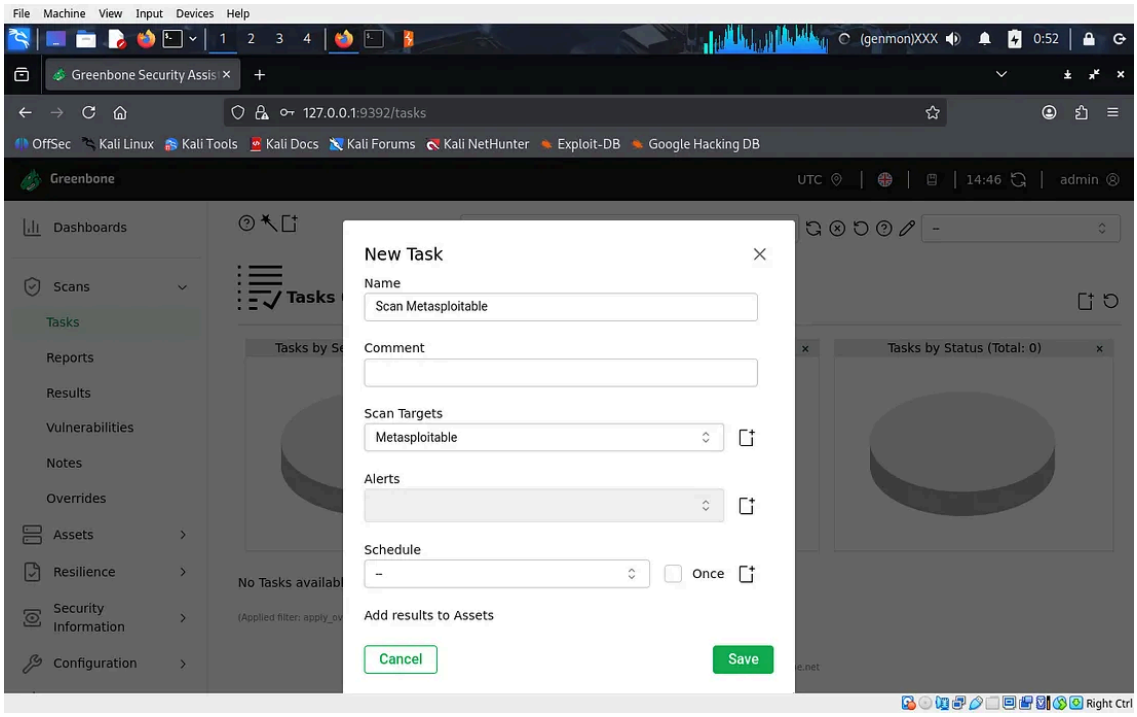
192.168.1.98	23/tcp	Telnet	Medium	4.8	N/A	Unencrypted cleartext login.	Credential sniffing.	Replace with SSH.
192.168.1.98	80/tcp	HTTP	Medium	4.8	N/A	Sensitive info (usernames/passwords) in cleartext HTTP.	MITM credential theft.	Enforce HTTPS/SSL.
192.168.1.98	80/tcp	SSL/TLS	Medium	4.8	CVE-2015-0204	FREAK (RSA_EXPORT downgrade).	Weak encryption, MITM.	Disable RSA_EXPORT ciphers.
192.168.1.98	80/tcp	SSL/TLS	Medium	4.3	N/A	Weak ciphers (RC4, 64-bit) supported.	Encryption breakable.	Disable weak ciphers.
192.168.1.98	80/tcp	SSL/TLS	Medium	4.3	CVE-2014-3566	POODLE (SSLv3 CBC disclosure).	Plaintext recovery.	Disable SSLv3/CBC ciphers.
192.168.1.98	80/tcp	SSL/TLS	Medium	4.3	N/A	Deprecated SSLv2/SSLv3 enabled.	Known exploits (POODLE/DROWN).	Disable SSLv2/SSLv3.

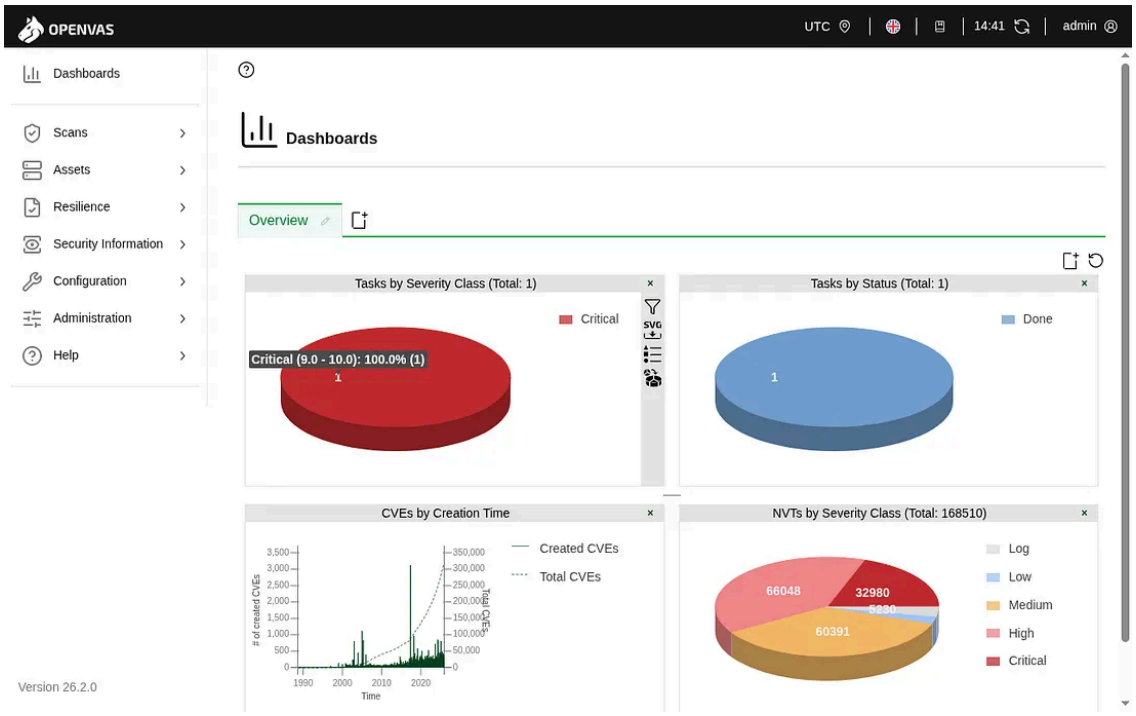
192.168.1.98	80/tcp	Apache	Medium	4.3	CVE-2003-1418	ETag header leaks inode/size (67575/45).	File recon for attacks.	Disable FileETag or hash inodes.
192.168.1.98	80/tcp	SSL/TLS	Medium	4.3	CVE-2015-0204	FREAK (RSA_EXPORT downgrade, duplicate).	Weak encryption, MITM.	Disable RSA_EXPORT ciphers.
192.168.1.98	80/tcp	SSL/TLS	Medium	4.3	N/A	Weak ciphers (duplicate).	Encryption breakable.	Disable weak ciphers.
192.168.1.98	80/tcp	SSL/TLS	Medium	4.3	CVE-2014-3566	POODLE (duplicate).	Plaintext recovery.	Disable SSLv3/CBC ciphers.
192.168.1.98	80/tcp	TWiki	Medium	4.3	CVE-2009-1204	Multiple XSS in pages (orphan_pages.php etc.).	Script injection.	Upgrade to Tiki 2.4+.
192.168.1.98	80/tcp	SSL/TLS	Medium	4.0	N/A	DH group <2048 bits (1024-bit temp key).	Offline decryption.	Use ECDHE or 2048+ DH.
192.168.1.98	80/tcp	SSL/TLS	Medium	4.0	N/A	Weak signature	Cert forgery risk.	Use SHA-2+ certs.

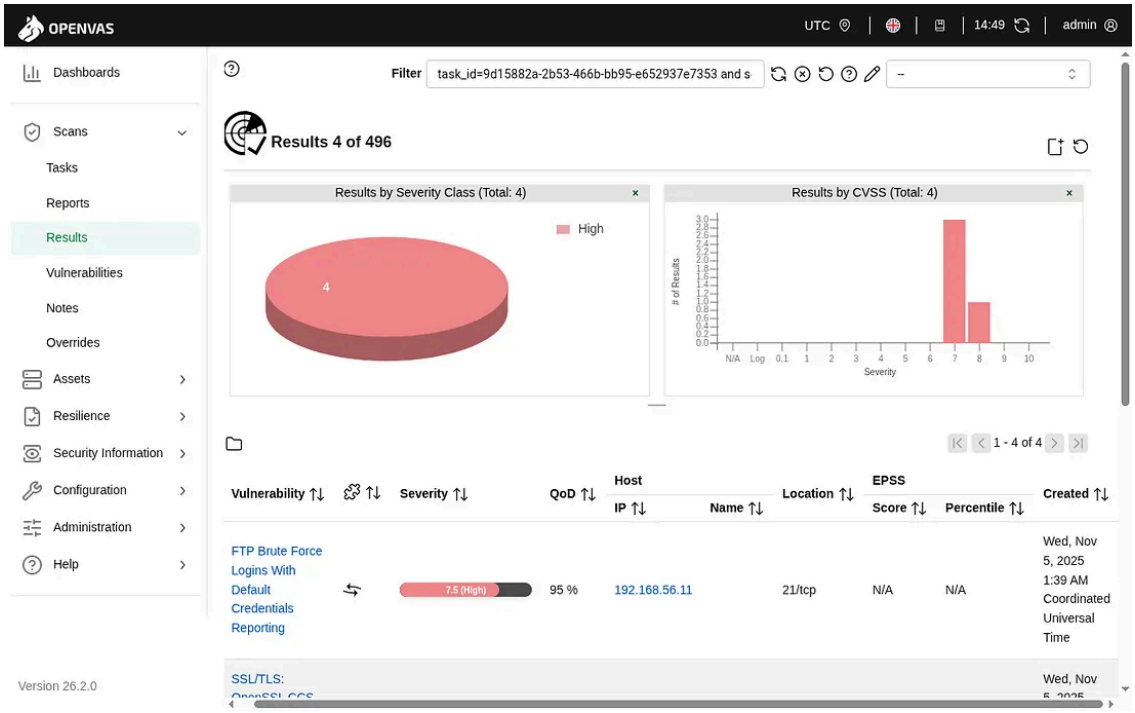
						algo (SHA-1).		
192.168.1.98	80/tcp	Tiki Wiki	Low	3.5	CVE-2018-7188	XSS via SVG image in filegals.	Admin privilege escalation if opened.	Upgrade to Tiki 18.0+.
192.168.1.98	22/tcp	SSH	Low	2.6	N/A	Weak MAC algos (MD5, 96-bit SHA1).	Message integrity compromise.	Disable weak MACs.

These are the steps I took to scan the Metasploitable machine from OpenVAS:




File Machine View Input Devices Help
Greenbone Security Assis
127.0.0.1:9392/tasks
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Greenbone
UTC 14:46 admin
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
New Task
Name
Scan Metasploitable
Comment
Scan Targets
Metasploitable
Alerts
Schedule
Once
Add results to Assets
Cancel
Save
Tasks by Status (Total: 0)
Right Ctrl


OPENVAS
UTC 14:41 admin
Dashboards
Scans
Assets
Resilience
Security Information
Configuration
Administration
Help
Overview
Tasks by Severity Class (Total: 1)
Critical
Critical (9.0 - 10.0): 100.0% (1)
Tasks by Status (Total: 1)
Done
CVEs by Creation Time
Created CVEs
Total CVEs
NVTs by Severity Class (Total: 168510)
66048
32980
60391
Log
Low
Medium
High
Critical
Version 26.2.0



4. Practice Risk Assessment

Assessed using the CVSS v3.1 calculator (nvd.nist.gov/vuln-metrics/cvss) and a custom 3x3 matrix.

Steps Performed:

1. **CVSS Calculator**:

    - Inputted report metrics (e.g., Base Score from NVTs). Verified/Adjusted: e.g., DistCC RCE (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H → 9.3 confirmed).
    - Temporal/Environmental scores not applied (lab env).

2. **Prioritize Risks (3x3 Matrix)**:

    - **Likelihood**: 1=Low (complex exploit), 2=Medium (known tools), 3=High (scripted/remote).
    - **Impact**: 1=Low (info leak), 2=Medium (data loss), 3=High (RCE/compromise).

- **Risk Level**: Score 1-3=Low, 4-6=Medium, 7-9=High.

Vulnerability	Likelihood	Impact	Score	Priority	Notes
OS EOL (Ubuntu 8.04)	3	3	9	High	Enables all unpatched exploits.
DistCC RCE	3	3	9	High	No auth; immediate RCE.
Weak DB Passwords	2	3	6	Medium	Brute-forceable but targeted.
TWiki XSS/RCE	3	2	6	Medium	Web-only; requires user interaction.
Weak Ciphers (POODLE)	1	2	2	Low	MITM rare in lab.

- **Matrix Visualization** (High: 12 items, Medium: 20, Low: 7). [Screenshot Placeholder: 3x3 Risk Matrix Chart from Excel.]

Sources: CVSS Guide (first.org/cvss), NIST Risk Framework (nist.gov).

Remediation Plan:

Priority	Vulnerability	Fix Steps & Links
High	OS EOL	Upgrade to Ubuntu 22.04 LTS: `do-release-upgrade`. (wiki.ubuntu.com/Releases)
High	DistCC RCE	Disable service: `sudo systemctl disable distccd`. (CVE-2004-2687: cve.mitre.org)
High	Weak DB Passwords	Change MySQL/PostgreSQL: `ALTER USER 'root'@'localhost' IDENTIFIED BY 'strongpw';`.
Medium	TWiki XSS/RCE	Upgrade/Remove: Replace with modern wiki (twiki.org).
Medium	Weak Ciphers	Configure Apache: Disable SSLv3/RC4 in /etc/apache2/mods-enabled/ssl.conf. (mozilla.org/ssl-config-generator)
Low	Expired Cert	Generate new: `openssl req -new -x509 -keyout ca.key -out ca.crt`.