Task 3 – OpenVAS Vulnerability Scan Mitigation Strategies

A proper mitigation strategy involves three phases: **Immediate Triage, System Hardening, and Policy Implementation.**

Phase 1: Immediate Triage (Critical Fixes)

These issues must be resolved first as they represent the highest CVSS scores and the easiest avenues for compromise.

1. Patching and Upgrading

Vulnerability	CVSS Score	Mitigation Action
OS End Of Life Detection (Ubuntu 8.04)	10.0	**Urgent OS Migration:** Immediately migrate this system to a **current, supported Linux distribution** (e.g., a recent Long-Term Support version). Running EOL software is the biggest security risk.
TWiki XSS and Command Execution	10.0	**Upgrade TWiki:** Update TWiki to version **4.2.4 or later** (or the latest stable release).
Tiki Wiki CMS Groupware Vulns	7.5	**Upgrade Tiki Wiki:** Update Tiki Wiki CMS Groupware to version **18.0 or later** (as indicated in the report snippet) to fix known SQL injection and XSS flaws.
Apache HTTPD DoS	7.8	**Patch Apache:** Apply vendor patches or upgrade Apache to a version that fixes the Range Header DoS vulnerability (versions after 2.0.64 and 2.2.19).

2. Password and Credential Management

Vulnerability	Port	Mitigation Action
MySQL/MariaDB Weak Password	3306/tcp	**Change Passwords:** Immediately set **strong, unique, complex passwords** for the root user in MySQL/MariaDB.

Vulnerability	Port	Mitigation Action
PostgreSQL Weak Password	5432/tcp	**Change Passwords:** Immediately set **strong, unique, complex passwords** for the postgres user.
SSH Brute Force (Default Credentials)	22/tcp	**Disable/Remove Accounts:** For users like msfadmin and user, either **delete the accounts** or **force password resets** with strong, complex passwords. Ideally, switch to **key-based authentication** for SSH and disable password-based login entirely.

3. Service Removal and Cleanup

Vulnerability	Port	Mitigation Action
phpinfo() Output Reporting	80/tcp	**Delete the File:** The file phpinfo.php is a severe information leak. **Delete this file** immediately from the web root.
DistCC Remote Code Execution	3632/tcp	**Disable or Restrict:** If DistCC is not essential, **disable the service**. If it is required, configure a **strict firewall rule** to only allow access from trusted internal IP addresses.

Phase 2: System Hardening (Mitigating Medium/Low Issues)

These steps address lower-risk issues that reduce the overall attack surface.

1. **SSL/TLS Certificates: Renew and install valid certificates** for services on ports 25/tcp (SMTP) and 5432/tcp (PostgreSQL) to replace the expired certificates from 2010.
2. **SSH Configuration:** Modify the SSH configuration (sshd_config) to **disable weak MAC algorithms** (like MD5) and disable outdated ciphers to prevent the **SSH Weak MAC Algorithms Supported** issue.
3. **HTTP Configuration:** Disable the HTTP **TRACE and TRACK** methods in the web server configuration to prevent Cross-Site Tracing (XST) attacks.
4. **Mail Server Hardening:** Ensure the mail server on port 25/tcp is updated and configured to securely handle STARTTLS to mitigate the **Arbitrary Command Injection** vulnerability.

Phase 3: Policy and Continuous Monitoring

To ensure the system remains secure after the initial fixes, these policies must be implemented.

1. **Network Segmentation and Firewall:**
    - Implement a **firewall policy** to strictly limit external (and internal) access to services. Block public access to management ports like 22, 3306, 5432, and 3632.
    - **Disable all unnecessary services and open ports** to minimize the attack surface.
2. **Continuous Vulnerability Management (VM):**
    - Establish a **regular, automated scanning schedule** (e.g., weekly or daily) using OpenVAS or similar tools to catch new vulnerabilities as soon as they emerge.
    - Implement an **emergency patching policy** for vulnerabilities rated 8.0 CVSS or higher.
3. **Principle of Least Privilege (PoLP):**
    - Ensure all applications and services (especially databases, web servers, and compilation tools like DistCC) run using **non-root, least-privileged service accounts**. This prevents an attacker who compromises a service from gaining control of the entire system.
4. **Audit and Logging:**
    - Ensure all critical service actions (SSH logins, database access, web server errors) are **logged and centrally monitored** for suspicious activity.