01 CRITICAL WE VULNERABILITIES

EXECUTIVE SUMMARY

A vulnerability scan of host **192.168.96.128** identified multiple critical findings that collectively expose the system to full compromise. High-risk issues include unauthenticated remote services (rlogin, rexec), default credentials, known remote code execution vectors in web components (TWiki, PHP CGI, Tomcat AJP), tainted/compromised packages (vsftpd backdoor), and an end-of-life operating system (Ubuntu 8.04). Immediate containment, remediation, and forensic investigation are recommended.

SCOPE & METHODOLOGY

Scope: Single host: 192.168.96.128

Tools used:

- Nmap (service/version discovery)
- OpenVAS / Greenbone (vulnerability enumeration and CVSS)
- Nikto (web application scanning)

Methodology:

1. Discovery with Nmap (service enumeration and versions).
2. Web-focused scans (Nikto) and full vulnerability scans with OpenVAS.
3. Collation of findings, mapping to CVEs where applicable, and prioritization by CVSS scores.
4. Sanitize outputs for reporting.

FINDINGS

Notation: CVSS scores and severity levels are those reported by the scanning tools and/or mapped from referenced CVEs.

1. rlogin — Passwordless Login

- **Host:** 192.168.96.128
- **Service/Port:** rlogin
- **CVSS / Severity:** 10.0 — Critical

- **Description:** rlogin permits remote root login without password authentication, enabling full system takeover.
- **Remediation:** Disable rlogin, remove inetd/xinetd entry, block the service via firewall, and migrate remote access to SSH with key-based authentication.
- **Notes:** Treat as immediate P0 — isolate host if seen in production.

2. TWiki XSS and Command Execution (CVE-2008-5304, CVE-2008-5305)

- **Host:** 192.168.96.128
- **Port:** 80/tcp
- **CVSS / Severity:** 10.0 — Critical
- **Description:** TWiki instances prior to v4.2.4 are vulnerable to XSS and eval injection via %URLPARAM{} and %SEARCH{} allowing script injection and possible command injection.
- **Remediation:** Upgrade TWiki to v4.2.4 or later. If immediate upgrade not possible, restrict access, apply web application firewall rules, or disable the application until patched.

3. Possible Backdoor: Ingreslock

- **Host:** 192.168.96.128
- **Port:** 1524/tcp
- **CVSS / Severity:** 10.0 — Critical
- **Description:** Service responds as root (uid=0), indicating a probable installed backdoor enabling arbitrary command execution.
- **Remediation:** Isolate host, conduct incident response and forensic analysis, rebuild from known-good images if compromise confirmed, rotate all credentials, and block the port.

4. rexec (unencrypted remote exec) — CVE-1999-0618 referenced

- **Host:** 192.168.96.128
- **Port:** 512/tcp
- **CVSS / Severity:** 10.0 — Critical

- **Description:** rexec transmits credentials in cleartext and permits remote command execution.
- **Remediation:** Disable rexec, remove inetd entry, firewall the port, and require SSH for remote execution.

5. Operating System End-of-Life — Ubuntu 8.04

- **Host:** 192.168.96.128
- **CVSS / Severity:** 10.0 — Critical
- **Description:** OS is EOL and no longer receives security updates, leaving many unpatched vulnerabilities.
- **Remediation:** Rebuild or upgrade the host to a supported distribution and apply a hardened baseline.

6. Distributed Ruby (DRb) — Multiple RCE Vectors

- **Host:** 192.168.96.128
- **Port:** 8787/tcp
- **CVSS / Severity:** 10.0 — Critical
- **Description:** DRb accepts serialized objects/commands leading to potential remote code execution.
- **Remediation:** Disable DRb if unused, restrict access to trusted networks, apply application-level ACLs, and run services with least privilege.

7. MySQL / MariaDB Default Credentials

- **Host:** 192.168.96.128
- **Port:** 3306/tcp
- **CVSS / Severity:** 9.8 — Critical
- **Description:** Database root accessible with empty password allowing full DB compromise.
- **Remediation:** Immediately set strong passwords, remove anonymous accounts, restrict DB access via firewall and host-based controls, and rotate any potentially exposed credentials.

8. Apache Tomcat AJP (Ghostcat) — CVE-2020-1938

- **Host:** 192.168.96.128
- **Port:** 8009/tcp
- **CVSS / Severity:** 9.8 — Critical
- **Description:** AJP connector can disclose webapp resources (e.g., /WEB-INF/web.xml) and may enable RCE on vulnerable configurations.
- **Remediation:** Apply vendor patches, disable AJP if unused, or bind AJP to localhost and restrict via firewall.

9. PHP CGI (php-cgi) Vulnerabilities

- **Host:** 192.168.96.128
- **Port:** 80/tcp (cgi-bin/php)
- **CVSS / Severity:** 9.8 — Critical
- **Description:** Vulnerable php-cgi configurations allow passing command-line switches leading to source disclosure or RCE.
- **Remediation:** Upgrade PHP to fixed versions, remove CGI configuration, apply WAF rules, and restrict access to cgi-bin.

10. vsftpd 2.3.4 Backdoor (CVE-2011-2523)

- **Host:** 192.168.96.128
- **Ports:** 21/tcp and 6200/tcp
- **CVSS / Severity:** 9.8 — Critical
- **Description:** Compromised vsftpd package contains a backdoor spawning a shell on port 6200.
- **Remediation:** Remove affected package, reinstall vendor-signed fixed package, verify package integrity, block backdoor port, and rebuild host if needed.

PRIORITIZATION & SCORING

Use CVSS as primary numeric score. Suggested priority mapping (use in Google Sheets):

- CVSS $\geq 9.0 \rightarrow$ **Critical**
- $7.0 \leq$ CVSS $< 9.0 \rightarrow$ **High**
- $4.0 \leq$ CVSS $< 7.0 \rightarrow$ **Medium**

- CVSS < 4.0 → **Low**

RECOMMENDED IMMEDIATE ACTIONS

1. Isolate 192.168.96.128 from production networks.
2. Rotate all credentials and revoke any exposed keys.
3. Remove/disable insecure services (rlogin, rexec, unauthenticated DB access, DRb, vsftpd tainted package).
4. Rebuild or upgrade OS (Ubuntu 8.04) to a supported release and apply vendor patches.
5. Apply specific vendor fixes for Tomcat AJP, PHP CGI, and TWiki; apply WAF rules and host-based firewall restrictions.

VERIFICATION & RETEST PLAN

After remediation:

1. Re-run Nmap and OpenVAS scans and compare outputs to identify resolved items.
2. Verify that previously exposed services no longer allow unauthorized access.
3. Document verification evidence and update the Google Sheet remediation status.

ESCALATION EMAIL

Subject: Urgent Security Escalation – Critical Vulnerabilities Detected on Host 192.168.96.128

Dear Development Team,

A security scan identified multiple critical vulnerabilities on host **192.168.96.128**, including unauthenticated remote access, default DB credentials, known RCE vectors (TWiki, PHP CGI, Tomcat AJP), and an EOL operating system. CVSS scores range from 9.8–10.0. I have attached sanitized scan outputs and screenshots demonstrating the issues. Please isolate the host, apply critical patches, and remove insecure services immediately. Confirm remediation plan and timeline; I will assist with verification and retesting.

Regards,

ARYAKRISHNA K U