

To	↳ Person ↳ Person ↳ Person manager-cyart
Cc	↳ Person
Bcc	↳ Person
Subject	Critical Vulnerabilities Identified During VAPT Assessment – Immediate Attention Required

Hi Team,

During the recent Vulnerability Assessment and Penetration Testing (VAPT) exercise conducted on the target system (Metasploitable2 – 192.168.71.128), multiple **high and critical severity security vulnerabilities** were identified that pose a significant risk to system confidentiality, integrity, and availability.

The most critical finding includes **Samba usermap script Remote Code Execution (CVE-2007-2447)** with a CVSS score of **9.8 (Critical)**, which was successfully exploited to obtain a root-level shell on the target system. This confirms that an unauthenticated attacker can fully compromise the server remotely.

Additional high-risk issues observed include:

- **Anonymous FTP access enabled**, allowing unauthorized file access.
- **Telnet service enabled**, transmitting credentials in cleartext.
- **Outdated Apache HTTP Server (2.2.8)** with known vulnerabilities.
- **phpMyAdmin exposed without access restrictions**, increasing the risk of database compromise.
- **MySQL service exposed on port 3306**, accessible without network-level restrictions.
- Multiple unnecessary and legacy services running, expanding the overall attack surface.

Web application scanning using Nikto further revealed directory indexing, information disclosure via phpinfo pages, insecure HTTP headers, and exposed administrative interfaces. SQL injection testing using sqlmap did not confirm exploitable injection points; however, exposed parameters and weak configurations remain a concern.

Recommended Immediate Actions:

- Patch or remove vulnerable services, especially Samba and Apache.
- Disable anonymous FTP and replace Telnet with SSH.
- Restrict access to phpMyAdmin and database services using authentication, IP whitelisting, and firewall rules.
- Remove unnecessary services and enforce the principle of least privilege.
- Perform a full rescan after remediation to validate fixes.

Given the **critical nature of these vulnerabilities**, immediate remediation is strongly recommended to prevent potential exploitation in a real-world environment.

Please let me know if you need detailed logs, proof-of-concept screenshots, or assistance with remediation validation.

Regards,
Mustafa Syed

VAPT Analyst
