## 💧 Top Critical Vulnerabilities Identified

### 📋 Target Details

**IP dress:** 192.168.152.129 (Metasploitable2)

**SystAdem Type:** Linux Ubuntu 8.04 LTS (vulnerable VM)

**Purpose:** Ethical hacking training & vulnerability scanning

### 1. vsftpd 2.3.4 Backdoor Command Execution

- **CVSS Score**: 10.0 (Critical)
- **Description**: A backdoored version of vsftpd allows unauthenticated remote code execution when a smiley :) is used in the username.
- **Affected Service**: FTP (Port 21)
- **Remediation**: Uninstall vsftpd 2.3.4 immediately and replace with a trusted, updated FTP server (or disable FTP altogether if not needed).

### 2. Samba smbd 3.x - Remote Code Execution

- **CVSS Score**: 10.0 (Critical)
- **Description**: Vulnerable Samba versions allow attackers to execute arbitrary code via crafted SMB packets.
- **Affected Service**: SMB (Port 445)
- **Remediation**: Upgrade Samba to a secure version (≥ 4.x). Disable SMBv1 if not required.

### 3. MySQL Privilege Bypass

- **CVSS Score**: 10.0 (Critical)
- **Description**: MySQL is configured with weak access controls, allowing attackers to escalate privileges.

- **Affected Service**: MySQL (Port 3306)
- **Remediation**: Harden MySQL configurations, disable remote root login, update MySQL to a secure version, and enforce strong authentication.

### 4. Unencrypted HTTP Services

- **CVSS Score**: 7.5 (High)
- **Description**: Apache is running over HTTP, exposing credentials and session info in plaintext.
- **Affected Service**: HTTP (Port 80)
- **Remediation**: Enable HTTPS using SSL/TLS certificates. Redirect all HTTP traffic to HTTPS.

### 5. OpenSSH with Weak Ciphers

- **CVSS Score**: 7.5 (High)
- **Description**: SSH is configured to support outdated and weak encryption algorithms.
- **Affected Service**: SSH (Port 22)
- **Remediation**: Edit /etc/ssh/sshd_config to disable weak ciphers (e.g., arcfour, cbc modes) and enable only secure algorithms.