**Vulnerability Assessment Report**

**By Youssef Ahmed Hany**

Uneeq Interns – Cyber Security Internship

**Target System:** Virtual Machine (IP: 172.17.0.1)  
**Scanning Tool Used:** Nmap  
**Objective:** Identify open ports, services, and associated vulnerabilities on the local network.

**-Summary**

The vulnerability assessment was conducted on the virtual machine (172.17.0.1) using the Nmap tool. The scan revealed several open ports and services with associated vulnerabilities. The most critical issue identified is a high-severity vulnerability in the OpenSSH service, with multiple CVEs linked to potential exploits. Additionally, services such as FTP (vsftpd) and Telnet are running, which may expose the system to security risks if not properly secured.

**-Host Information**

* **IP Address:** 172.17.0.1
* **Operating System:** Linux

### **-Identified Vulnerabilities**

#### **OpenSSH (Port 22)**

#### **Service Version:** OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; Protocol 2.0) **Severity:** Critical **Associated Vulnerabilities:**

* **CVE-2023-38408** - Score: 9.8 (Critical)  
  An issue in OpenSSH could allow a remote attacker to execute arbitrary code on the system. Exploits are available for this vulnerability.
  + Exploit: [GitHub Exploit](https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23)
* **CVE-2020-15778** - Score: 7.8 (High)  
  This vulnerability affects the scp client in OpenSSH, which could be exploited by a malicious server.
  + Exploit: [Seebug Exploit](https://vulners.com/seebug/SSV:92579)
* **CVE-2021-41617** - Score: 7.0 (High)  
  A privilege escalation vulnerability that could allow an attacker to execute unauthorized commands on the system.
  + Details: [CVE Report](https://vulners.com/cve/CVE-2021-41617)
* **CVE-2020-14145** - Score: 5.9 (Medium)  
  Vulnerability allowing the bypass of security restrictions under specific conditions.
  + Details: [CVE Report](https://vulners.com/cve/CVE-2020-14145)
* **CVE-2023-48795** - Score: 5.9 (Medium)  
  A vulnerability that can be exploited remotely, allowing attackers to potentially disrupt service.
  + Details: [CVE Report](https://vulners.com/cve/CVE-2023-48795)

#### **FTP (Port 21)**

#### **Service Version:** vsftpd 3.0.5 **Severity:** Low **Details:** No specific vulnerabilities were identified for this version during the scan, but FTP as a protocol is inherently insecure due to the transmission of credentials in clear text.

#### **Telnet (Port 23)**

#### **Service Version:** Linux telnetd **Severity:** High **Details:** The Telnet protocol is widely considered insecure as it transmits data, including passwords, in plaintext. This service can be exploited by attackers to intercept sensitive information or gain unauthorized access to the system.

### **-Recommendations**

1. **SSH (Port 22)**
   * **Immediate Action:** Upgrade OpenSSH to the latest version to mitigate critical vulnerabilities (CVE-2023-38408 and CVE-2020-15778).
   * **Mitigation:** Disable SSH password authentication and use key-based authentication. Implement IP whitelisting to restrict access. Regularly monitor SSH logs for suspicious activity.
2. **FTP (Port 21)**
   * **Recommendation:** Replace FTP with a secure alternative like SFTP or FTPS to encrypt data in transit and protect user credentials.
   * **Mitigation:** If FTP must be used, ensure that anonymous login is disabled and enforce strong password policies.
3. **Telnet (Port 23)**
   * **Recommendation:** Disable Telnet and replace it with a secure protocol such as SSH. Telnet’s plaintext transmission of data makes it a major security risk.
   * **Mitigation:** If Telnet cannot be disabled, use it over a secure VPN to encrypt data in transit.
4. **General System Hardening:**
   * Keep all software, including the operating system and services, updated with the latest security patches.
   * Disable unused services and ports to reduce the attack surface.
   * Use firewall rules to limit access to necessary services and block unauthorized access.
   * Implement intrusion detection/prevention systems (IDS/IPS) to monitor network traffic for suspicious activity.