PENETRATION TEST REPORT

Metasploitable 2 Vulnerability Assessment

CONFIDENTIAL

Prepared by:
Paul Umeh
Junior Penetration Tester

Target System:

192.168.2.143 (Metasploitable 2)

Date: February 18–20, 2026

1. Executive Summary

This report documents a penetration test conducted against Metasploitable 2, a deliberately vulnerable Linux virtual machine, between February 18–20, 2026. The assessment was performed in a controlled, isolated lab environment for educational purposes.

The assessment identified multiple critical vulnerabilities that would allow an unauthenticated attacker to gain complete control of the target system. The most severe finding — a backdoor embedded in vsftpd 2.3.4 — was successfully exploited to obtain root-level access, after which encrypted user credentials were extracted and partially cracked using offline techniques.

A subsequent defensive investigation using Splunk SIEM revealed that the exploitation left zero traces in the system authentication logs, highlighting a significant detection gap that would allow a real attacker to operate undetected.

Critical	High	Medium
2	1	1

2. Scope & Methodology

2.1 Scope

- **Target IP:** 192.168.2.143
- **Target System:** Metasploitable 2 (Linux Ubuntu)
- **Environment:** Isolated VMware lab network
- **Test Date:** February 18–20, 2026
- **Tester:** Paul Umeh

2.2 Methodology

The assessment followed a standard penetration testing methodology consisting of the following phases:

- Reconnaissance — Network scanning using nmap to identify open ports and running services
- Enumeration — Service version detection to identify outdated and vulnerable software
- Vulnerability Research — Cross-referencing discovered versions against the NIST National Vulnerability Database (NVD)
- Exploitation — Using Metasploit Framework to exploit identified vulnerabilities
- Post-Exploitation — Credential extraction, password cracking, and privilege assessment
- Detection Analysis — Defensive investigation using Splunk SIEM to assess detection capability

2.3 Tools Used

- nmap 7.98 — Port scanning and service enumeration
- Metasploit Framework 6.4 — Exploitation framework
- John the Ripper — Offline password cracking
- Splunk Enterprise 10.2 — SIEM log analysis
- dirb — Web directory enumeration

3. Reconnaissance

3.1 Port Scan Results

An nmap service version scan was conducted against the target, revealing 22 open TCP ports running multiple outdated and vulnerable services. This represents an extremely large attack surface for any internet-facing system.

Command used: nmap -sV 192.168.2.143

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.2.143
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-18 13:47 +0100
Nmap scan report for 192.168.2.143
Host is up (0.0046s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
ernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.96 seconds
```

Figure 1: nmap -sV scan revealing 22 open ports and vulnerable service versions

Key findings from the reconnaissance phase:

- Port 21 — vsftpd 2.3.4 (backdoored version, CVE-2011-2523)
- Port 22 — OpenSSH 4.7p1 (outdated, multiple known CVEs)
- Port 23 — Telnet enabled (transmits credentials in plaintext)
- Port 80 — Apache httpd 2.2.8 (outdated web server)
- Port 1524 — Metasploitable root shell (open backdoor)
- Port 3306 — MySQL 5.0.51a exposed to network
- Port 6667 — UnrealIRCd (contains backdoor vulnerability)

4. Findings

Finding 1 — vsftpd 2.3.4 Backdoor Command Execution

VULN-001 — vsftpd 2.3.4 Backdoor Command Execution	
Severity	**CRITICAL**
CVSS Score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVE Reference	CVE-2011-2523
Description	vsftpd version 2.3.4 contains a malicious backdoor that was secretly inserted into the software's source code between June 30 and July 1, 2011. When a username containing the string ':)' is submitted during FTP authentication, the backdoor opens a root shell on port 6200, granting the attacker complete unauthenticated access to the system.
Impact	An unauthenticated remote attacker can obtain full root-level command execution on the target system without requiring any credentials. This represents complete compromise of the affected system including full access to all data, system configuration, and user credentials.
Remediation	Immediately update vsftpd to the latest stable version. Implement network-level firewall rules to restrict FTP access to authorized IP addresses only. Consider replacing FTP with SFTP (SSH File Transfer Protocol) for secure file transfers.

Evidence of successful exploitation:

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.2.143:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.2.143:21 - USER: 331 Please specify the password.
[+] 192.168.2.143:21 - Backdoor service has been spawned, handling...
[+] 192.168.2.143:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:44497 -> 192.168.2.143:6200) at 2026-02-19 03:44:58 +0100

whoami
root
pwd
/
hostname
metasploitable
```

Figure 2: Metasploit exploitation of CVE-2011-2523 confirming root access (uid=0)

Finding 2 — Weak Password Policy / Credential Exposure

VULN-002 — Weak Passwords and MD5 Password Hashing	
Severity	**CRITICAL**
CVSS Score	9.1 (AV:N/AC:L/Au:N/C:C/I:C/A:N)
CVE Reference	CWE-521, CWE-916
Description	Following root access, the /etc/shadow file was extracted containing password hashes for all system accounts. The system uses the MD5crypt (1) hashing algorithm, which is considered cryptographically weak by modern standards. Offline password cracking using John the Ripper with the rockyou.txt wordlist successfully cracked 3 of 7 hashes within 13 minutes.
Impact	Attackers with access to the shadow file can recover plaintext passwords through offline cracking. Cracked credentials can be used for lateral movement across the network, credential stuffing attacks, and persistent access even after the initial vulnerability is patched.
Remediation	Migrate all password hashing to bcrypt or SHA-512 (yescrypt). Enforce a strong password policy requiring minimum 12 characters with complexity requirements. Implement multi-factor authentication for all accounts. Regularly audit accounts and disable unnecessary system accounts.

Evidence — /etc/shadow file contents extracted:

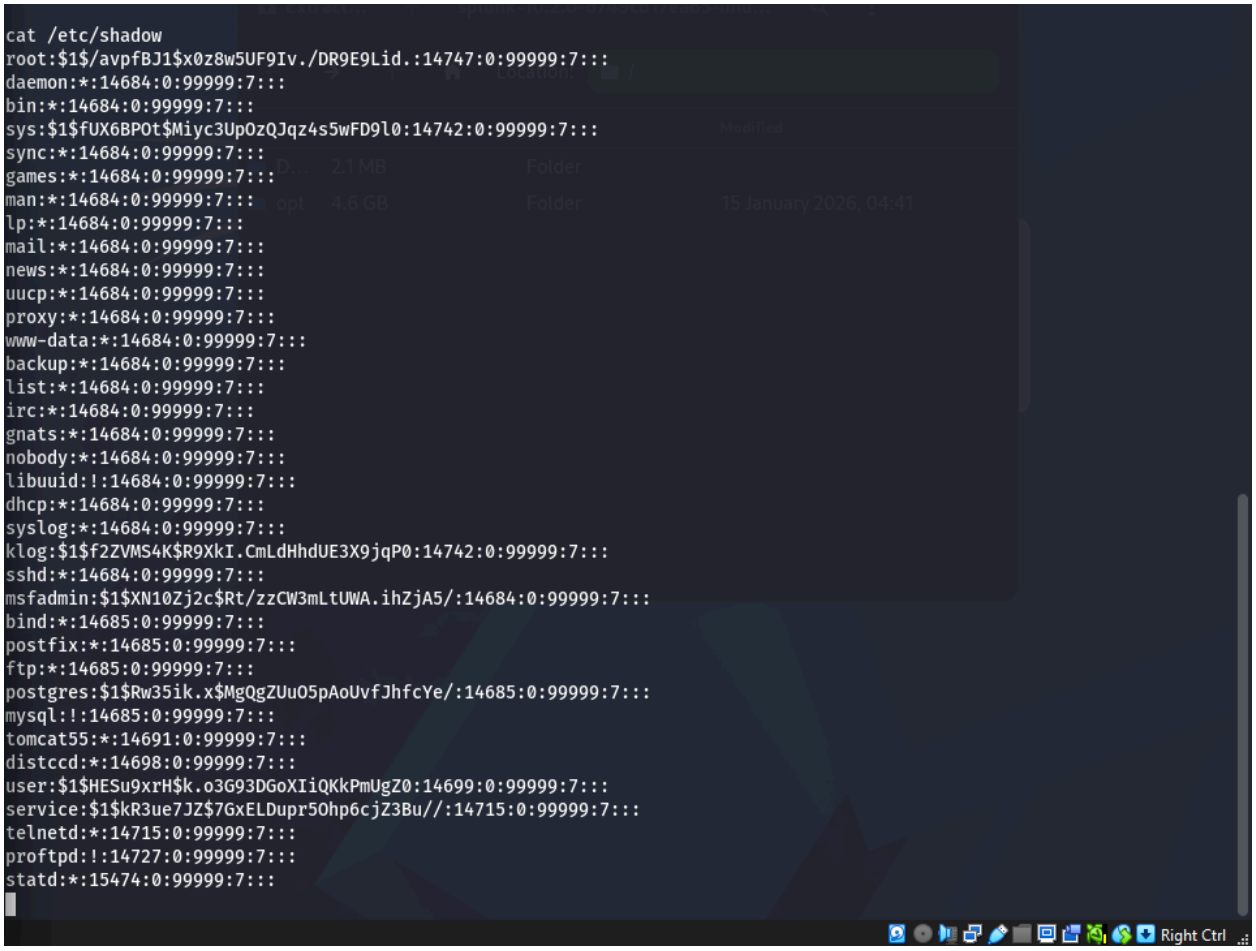

Figure 3: /etc/shadow file exposed — MD5 password hashes for all system accounts

Evidence — Password cracking results:

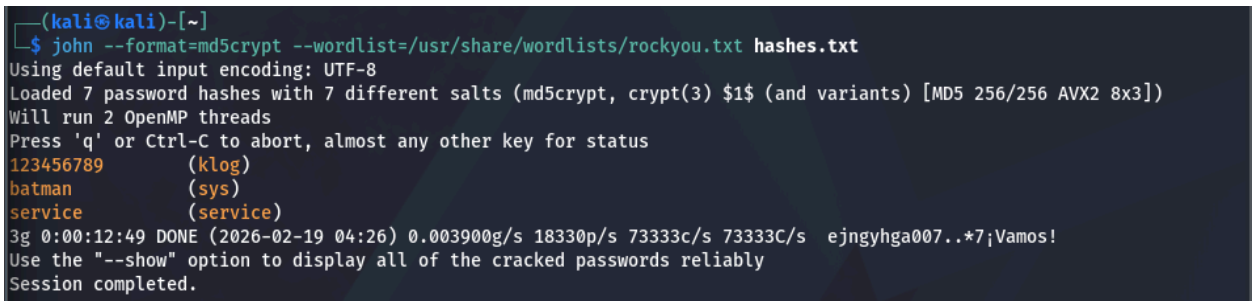

Figure 4: John the Ripper cracking 3 passwords in under 13 minutes using rockyou.txt

Username	Password	Status
klog	123456789	**CRACKED**
sys	batman	**CRACKED**

service	service	CRACKED
root	********	NOT CRACKED
msfadmin	********	NOT CRACKED

Finding 3 — Telnet Service Enabled

VULN-003 — Unencrypted Telnet Service	
Severity	**HIGH**
CVSS Score	7.5 (AV:N/AC:L/Au:N/C:C/I:N/A:N)
CVE Reference	CWE-312
Description	Telnet is enabled on port 23. Telnet transmits all data including usernames and passwords in plaintext over the network. Any attacker with network access can intercept Telnet sessions using packet capture tools and retrieve credentials without any decryption.
Impact	An attacker with network access can capture authentication credentials and session data in plaintext, enabling account takeover and unauthorized access to the system.
Remediation	Disable Telnet immediately. Replace with SSH (port 22) for all remote administration tasks. SSH provides strong encryption for all session data.

Finding 4 — Detection Gap: Exploitation Invisible in Auth Logs

VULN-004 — Insufficient Logging and Monitoring	
Severity	**MEDIUM**
CVSS Score	6.5 (AV:N/AC:L/Au:N/C:C/I:N/A:N)
CVE Reference	CWE-778, OWASP A09:2021
Description	A SIEM investigation using Splunk Enterprise confirmed that the vsftpd backdoor exploitation generated zero entries in the system authentication log (/var/log/auth.log). The backdoor bypasses the standard PAM

	authentication stack entirely, opening a raw shell on port 6200 without triggering any authentication events.
Impact	An attacker exploiting this vulnerability can maintain complete root access to the system for an extended period without being detected by security teams monitoring authentication logs. This represents a critical gap in the organisation's ability to detect and respond to incidents.
Remediation	Implement comprehensive logging across all log sources including FTP service logs, network flow data, and system call auditing. Deploy a SIEM with correlation rules to detect anomalous port activity, particularly unexpected connections on non-standard ports. Implement network-based intrusion detection (Snort or Suricata) to detect malformed FTP packets characteristic of this exploit.

Evidence — Splunk investigation showing zero exploitation traces in attack window:

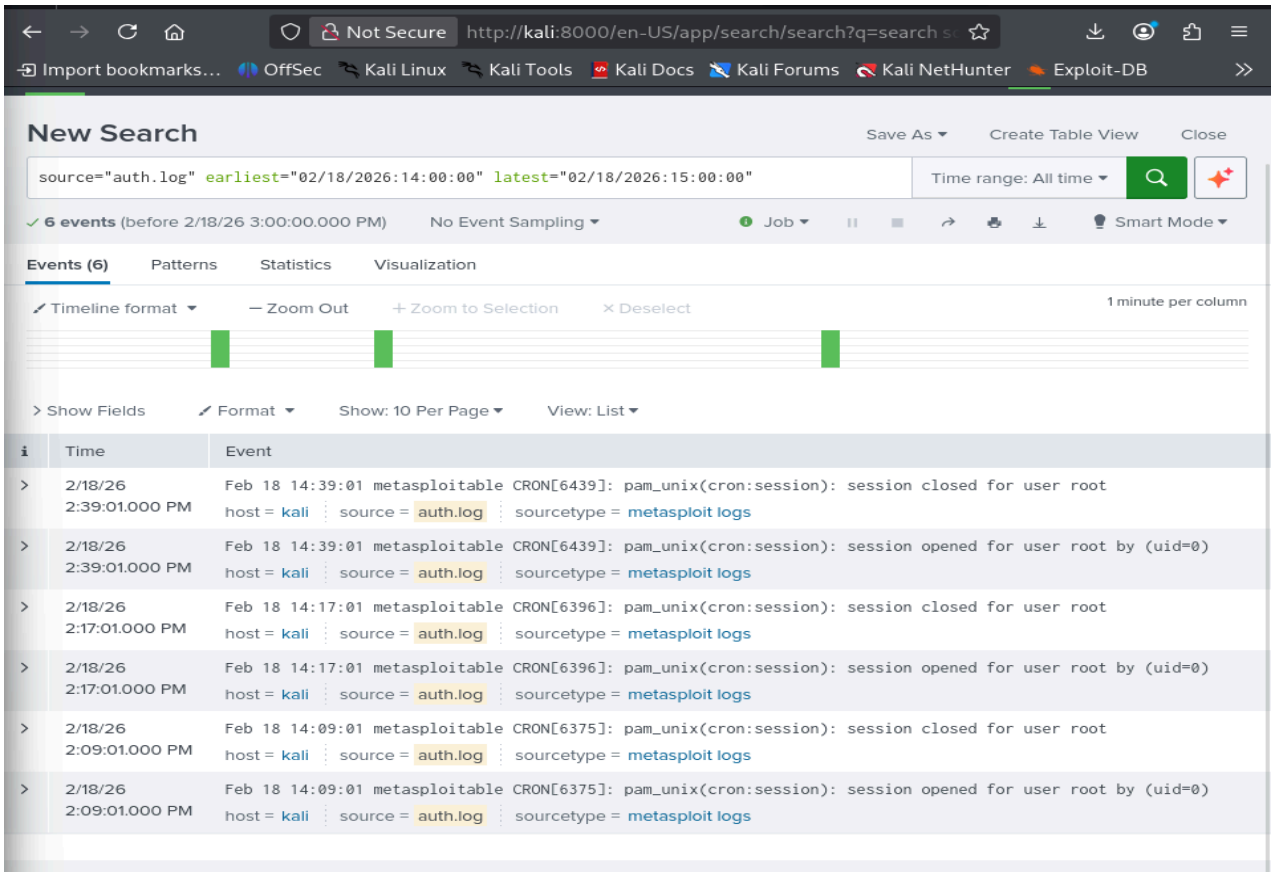

Figure 5: Splunk SIEM search showing only CRON activity during exploitation window — attack was completely undetected

5. Recommendations

The following remediation actions are recommended in order of priority:

#	Recommendation	Priority	Effort
1	Update vsftpd to latest stable version and remove backdoored binary	CRITICAL	Low — 1 hour
2	Disable Telnet service and replace with SSH	CRITICAL	Low — 30 minutes
3	Migrate password hashing from MD5 to bcrypt/SHA-512	HIGH	Medium — 1 day
4	Enforce strong password policy (12+ chars, complexity)	HIGH	Low — 2 hours
5	Implement multi-source SIEM logging with correlation rules	HIGH	High — 1 week
6	Deploy network IDS/IPS (Snort or Suricata)	MEDIUM	Medium — 2 days
7	Close unnecessary open ports via firewall rules	MEDIUM	Low — 2 hours

6. Conclusion

The penetration test of Metasploitable 2 revealed a system with a critically poor security posture. Multiple severe vulnerabilities were identified and successfully exploited, resulting in complete system compromise including root access and credential exposure.

The most significant finding was not the exploitation itself, but the subsequent SIEM investigation which confirmed that the attack was entirely invisible to a defender monitoring authentication logs. This highlights the critical importance of defence-in-depth — no single log source or security tool is sufficient to detect all attack techniques.

Immediate action should be taken to patch the vsftpd backdoor and disable Telnet. Medium-term investment in a properly configured SIEM with multi-source log correlation and network-based intrusion detection will significantly improve the organisation's ability to detect and respond to future attacks.

Paul Umeh | Junior Penetration Tester | February 2026