PENETRATION TEST REPORT

Internal Network Security Assessment – Metasploitable 2

1. Executive Summary

An internal penetration test was conducted against a vulnerable lab environment (Metasploitable 2). The objective was to identify security weaknesses that could allow unauthorized access, privilege escalation, and lateral movement.

The system was fully compromised through exposed services, weak credential storage, and insecure configurations.

Overall Risk Rating: CRITICAL

2. Scope

Target System:

Metasploitable 2 (Linux-based vulnerable VM)
Internal IP: 192.168.100.11

Testing Environment:

Kali Linux (attacker machine)

Testing Type:

Internal network penetration test

---

3. Methodology

The assessment followed industry-standard penetration testing methodology aligned with:

OWASP Testing Guide
PTES (Penetration Testing Execution Standard)
Offensive Security penetration testing practices

Testing phases included:

1. Reconnaissance
2. Service Enumeration
3. Exploitation
4. Post-Exploitation

5. Credential Dumping
6. Password Cracking
7. Lateral Movement

4. Findings

4.1 Remote Code Execution via Backdoor Service

Severity: Critical
Port: 6200
Service: Unauthenticated shell access

An open service running on TCP port 6200 provided direct shell access without authentication.

Exploit method:

nc 192.168.100.11 6200

Result:

Immediate interactive shell access to the target system.

Impact:

Full remote command execution
Complete system compromise
Ability to access sensitive files

4.2 Credential Dumping

Severity: High

After obtaining shell access, sensitive credential data was extracted from system files.

Example:
cat /etc/shadow

Password hashes for multiple users were obtained.

Impact:
Exposure of all local user password hashes
Enables offline password cracking attacks

4.3 Password Cracking

Severity: High

Extracted hashes were cracked using an offline password cracking tool.

The hash format identified:

> md5crypt

Multiple user passwords were successfully recovered.

Impact:

> Compromise of legitimate user accounts
> Ability to authenticate via SSH
> Increased attack surface

4.4 Lateral Movement via SSH

Severity: High

Using cracked credentials, SSH access was attempted:

ssh msfadmin@192.168.100.11

Initial SSH negotiation errors related to deprecated algorithms were resolved by adjusting client-side SSH options.

Result:

Successful authenticated SSH session.

Impact:

> Legitimate user-level access
> Ability to pivot within the system
> Foundation for privilege escalation

5. Risk Assessment Summary

Vulnerability	Severity	Impact
Unauthenticated Backdoor (Port 6200)	Critical	Full system compromise
Weak Password Hashing (md5crypt)	High	Credential exposure
Weak SSH Configuration	Medium	Facilitates lateral movement

Overall Risk Level: **CRITICAL**

6. Technical Impact

An attacker on the internal network can:

Gain remote shell access without credentials
Extract password hashes
Crack weak passwords offline
Log in via SSH as legitimate users
Fully compromise the system

The attack requires minimal sophistication and no zero-day vulnerabilities.

7. Recommendations

1. Remove and disable unauthorized or backdoor services (close port 6200).
2. Upgrade password hashing algorithms to modern standards (bcrypt, Argon2).
3. Enforce strong password policies.
4. Restrict SSH to key-based authentication only.
5. Disable deprecated SSH algorithms.
6. Implement network segmentation and firewall rules.
7. Apply regular patching and system hardening.

---

8. Conclusion

The Metasploitable 2 system was fully compromised through:

Exposed unauthenticated services
Weak credential storage mechanisms
Insecure service configurations

The findings demonstrate the critical importance of secure configuration management, strong authentication mechanisms, and service exposure control.

The system in its current state should not be deployed in any production environment.