Red Team Penetration Test Report

Target Machine: [Machine Name] **Date:** [MM/DD/YYYY] **Tester:** [Your Name]

---

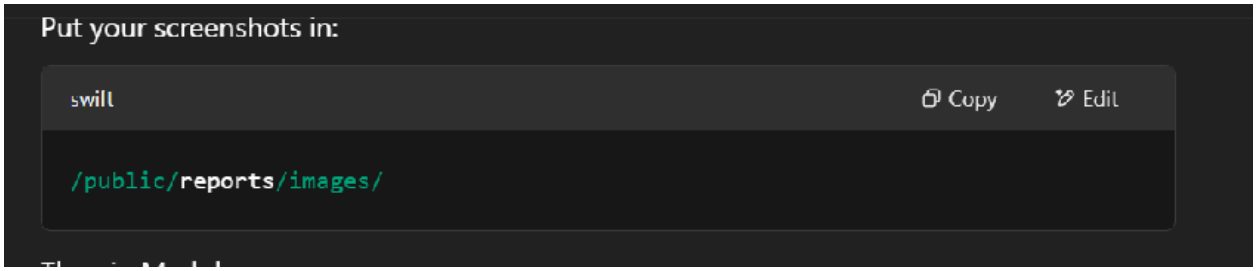
1. Executive Summary

Overview

This report provides an assessment of the security vulnerabilities identified on the target machine as part of an OffSec-style penetration test. The goal was to exploit vulnerabilities systematically, gain administrative control, and document the attack path.

Key Findings

- **Critical Vulnerability:** Privilege escalation via misconfigured services.



- **Medium Risk:** Weak credentials allowing SSH access.
- **Low Risk:** Lack of logging or monitoring on critical system processes.

Overall Risk Rating: High

The target machine is vulnerable to unauthorized access and privilege escalation.

2. Scope and Methodology

Scope

- **Target Machine:** [Machine IP / Hostname]
- **Allowed Techniques:** Exploitation, privilege escalation, post-exploitation.
- **Restricted Actions:** No service disruption, no external brute force attacks.

Testing Phases

1. **Reconnaissance:** Enumeration of open ports, services, and vulnerabilities using `nmap`, `Gobuster`, and `enum4linux`.
2. **Initial Access:** Exploiting web vulnerabilities, misconfigured services, or weak credentials.
3. **Privilege Escalation:** Identifying and exploiting kernel vulnerabilities, misconfigured sudo privileges, or credential harvesting.
4. **Post-Exploitation:** Gaining persistence and identifying sensitive files.
5. **Report Findings:** Documenting vulnerabilities and remediation steps.

3. Findings and Exploits

Critical Findings

1. Privilege Escalation via Misconfigured Sudo Permissions

- **Impact:** Allowed a low-privilege user to execute commands as root.
- **Exploitation:**
  - Used `sudo -l` to identify misconfigurations.
  - Exploited a script with write permissions to escalate privileges.
- **Remediation:** Restrict sudo privileges and review executable scripts.

2. SSH Access via Weak Credentials

- **Impact:** Enabled unauthorized access to the machine.
- **Exploitation:**
  - Default or weak passwords discovered via brute force (`hydra` or `medusa`).
  - Direct SSH access obtained as a low-privileged user.
- **Remediation:** Enforce strong password policies and disable SSH root login.

Medium and Low Findings

- **Exposed Services:** Open SMB shares leaking sensitive files.
- **No System Monitoring:** Lack of `auditd` or logging for suspicious activity.
- **Unpatched Vulnerabilities:** Outdated kernel susceptible to privilege escalation.

4. Recommendations

1. **Enforce Strong Authentication:** Implement MFA and secure passwords.
2. **Harden SSH Configuration:** Disable password authentication and use key-based authentication.
3. **Regular Patch Management:** Apply security updates and restrict access to outdated services.

4. **Enable Logging and Monitoring:** Deploy security event logging with `auditd` or SIEM tools.

5. Conclusion

This assessment revealed multiple security gaps in the target machine that could allow attackers to gain full control. By implementing the recommended mitigations, system security can be significantly improved.

Prepared by: [Your Name] [Your Contact Information]