Penetration Testing and Vulnerability Management

Steel Mountain Room

1. Penetration Testing Scope Document

Scope:

- Target:

The target machine is an emulated corporate environment named *Steel Mountain*, which involves simulating a security breach into a company network.

- IP Address:

(10.10.203.69).

- Goals:

- Perform reconnaissance and enumerate the target machine.
- Identify and exploit vulnerabilities in services or applications running on the machine.
- Escalate privileges to gain full access to the system, ideally root/admin privileges.
- Document all findings, proof of concepts , and provide risk analysis.

2. Tool Configuration Report

Tools Used:

1. Nmap

- Purpose:

Network scanning and enumeration.

2. Gobuster

- Purpose:

Directory brute-forcing to find hidden web directories or files.

3. Metasploit Framework

- Purpose:

Exploitation framework used for gaining access.

4. Netcat

- Purpose: Used for reverse shells and network connectivity tests.

3. Penetration Testing Report

Findings:

1. Vulnerability #1: Outdated Web Application

- Proof of Concept :

An nmap scan revealed that the server was running an outdated version of Apache . A known vulnerability (CVE- 2014-6287) was used to gain an initial foothold by exploiting an RCE vulnerability.

- Exploit Steps:

  - Used Metasploit to run a remote code execution exploit on the vulnerable service.

  - Result: Gained a low-privilege shell.

2. Vulnerability #2: Weak Credentials for Web Interface

- Proof of Concept :

Using Gobuster, hidden directories were discovered on the web server, leading to an admin login page. Default credentials were used to access the panel (admin:admin).

- Exploit Steps:
  - Logged in to the admin panel.
  - Uploaded a reverse shell to gain access to the system.

3. Privilege Escalation: Sudo Vulnerability

- Proof of Concept :

Running linpeas.sh revealed that the user could run a vulnerable binary with sudo permissions. Exploiting this, privilege escalation to root was achieved.

- Exploit Steps:
  - Result: Gained root access to the system.

4. Risk Assessment Document

Vulnerability 1: Outdated Web Application

- Risk Level: High

- Impact: Remote code execution allows attackers to gain unauthorized access to the system.

- Mitigation: Update the application to the latest version, apply patches regularly.

Vulnerability 2: Weak Credentials

- Risk Level: High

- Impact: Easy access to admin functions, enabling malicious actions like file uploads or configuration changes.

- Mitigation: Enforce stronger password policies, implement 2FA for web admin logins.

Vulnerability 3: Privilege Escalation

- Impact: Complete system compromise.

- Mitigation: Review sudo permissions regularly, and limit access to sensitive binaries.

5. Prioritization Report

1. Critical: Privilege escalation vulnerability via misconfigured sudo permissions.

2. High: Weak admin credentials allowing easy access to web admin panel.

3. Medium: Outdated software (Apache) with known RCE vulnerabilities.

6. Vulnerability Management Plan

Step 1:

- Immediate Action: Update all software versions to the latest patch releases, particularly the vulnerable web application.

Step 2:

- Access Control Review:

  - Ensure that sudo access is limited to necessary users only.

  - Remove unnecessary or outdated binaries with sudo permissions.

Step 3:

- Credential Management:

  - Enforce a strong password policy.

  - Enable two-factor authentication (2FA) where applicable.

Step 4:

- Ongoing Monitoring:

  - Implement continuous monitoring tools to detect future vulnerabilities and unauthorized access attempts.

7. Verification Report

- Evidence of Fixes:

  - After the vulnerabilities were identified, the web application was updated to the latest secure version.

  - Default admin credentials were replaced with strong, complex passwords.

  - Privilege escalation vectors were mitigated by limiting sudo access and removing the vulnerable binary.

8. Final Project Report

- Testing Overview:
  - Reconnaissance: Open port and service detection using nmap.
  - Vulnerability identification through directory brute forcing and weak credential detection.
  - Exploitation using Metasploit and manual techniques.

- Findings:
  - Discovered multiple vulnerabilities, including RCE through outdated web services, weak admin credentials, and a privilege escalation flaw in sudo permissions.

- Management Plan:
  - Implemented fixes to update software, improve access control, and enforce stronger password policies.

- Outcomes:
  - All identified vulnerabilities were successfully remediated.
  - System hardened against future attacks.