Eshan K027

Lab 10 : Report Creation lab 8 & 9

Contents

1. Summary

This report is aimed to enumerate the vulnerability assessment and pen testing activities performed on corrosion2 machine. The assessment was divided into two phases: initial scanning and enumeration (Lab8) and subsequent exploitation with privilege escalation (Lab9). Critical vulnerabilities were identified, including misconfigured services, password-protected backup files, and exploitable weak credentials. The findings highlight the risks posed by these vulnerabilities and underscore the necessity for immediate remediation measures.

2. Introduction

The objective of this VAPT exercise was to identify, exploit, and analyze vulnerabilities within the target system (corrosion machine). The findings documented in Lab8 and Lab9 are consolidated in this report to provide a clear understanding of the security posture of the system, the methods used in testing, and the impact of the discovered vulnerabilities. The intended audience includes technical teams responsible for remediation as well as management requiring an executive overview of risks.

3. Methodology

The testing followed a structured approach:

- **Reconnaissance and Scanning:**
  Tools such as netdiscover and nmap were utilized to identify the target IP address and enumerate open ports on the machine.

- **Enumeration:**
  Directory enumeration tools (dirb) and file analysis (fcrackzip) were employed to detect sensitive files and analyze file protections.

- **Exploitation:**
  The Tomcat exploit in the Metasploit framework was used to leverage weak credentials, leading to a reverse shell. This phase involved user enumeration and extraction of hashed passwords.

- **Privilege Escalation:**
  After obtaining user credentials, further exploitation was performed using a Python library hijacking technique to modify the base64 module and escalate privileges to root.

4. Findings and Observations

4.1. Network Scanning & Enumeration

- **IP Address Discovery:**
  The vulnerable machine was identified with the IP address **10.0.2.5** using network scanning tools (nmap, netdiscover).

- **Open Ports:**
  A port scan revealed that the following ports were open:
  - **SSH (22):** Facilitates remote shell access.
  - **HTTP (80):** Hosts web services.
  - **HTTP Proxy (8080):** Likely used for forwarding traffic.

- **File Enumeration:**
  Directory scanning identified a file named **backup.zip** on the server. Analysis indicated that the file was password-protected.
  - **Password for backup.zip:** hi5
    This file likely contained sensitive configurations or credentials, emphasizing a potential information leakage risk.

- **Additional Credentials:**
  Extraction from the backup file revealed administrative credentials, specifically for the admin user:
  - **Admin Password:** melehifokivai

4.2. Exploitation & Privilege Escalation

- **Exploitation Phase:**
  Utilizing the Metasploit Framework, the Tomcat exploit was executed to take advantage of weak credentials. This exploit involved deploying a malicious WAR file, resulting in a reverse shell connection.

- **User Enumeration & Credential Discovery:**
  Post-exploitation, two user accounts were discovered:
  - **User 1:** jaye with password melehifokivai
  - **User 2:** randy with password 07051986randy
    Additional investigation included navigating to the home directories and extracting the /etc/shadow file.
- **Privilege Escalation:**
  With the cracked password for user randy, the next step was to escalate privileges. The assessment involved:
  - Using the sudo -l command to list allowed commands.
  - Exploiting the Python library hijacking vulnerability via manipulation of the randombase64.py and corresponding base64 module file.
  - The modified Python script enabled execution of system commands as root, ultimately yielding full control over the machine and capturing the root flag.

5. Impact Analysis

- **Unauthorized Access:**
  The discovery of weak credentials and exploitable services could allow unauthorized users remote access to critical systems, potentially leading to data breaches or further compromise.
- **Information Disclosure:**
  The presence of sensitive files (e.g., backup.zip) and plaintext credentials signifies a high risk for information leakage.

- **Privilege Escalation Risks:**
  The ability to escalate privileges via Python library hijacking demonstrates a critical vulnerability that can lead to complete system takeover.

- **Operational Impact:**
  These vulnerabilities, if exploited by a malicious actor, can result in severe operational disruption and loss of data integrity, thereby affecting both technical operations and executive management decision-making.

6.Security Audit Analysis

The security assessment of the Corrosion 2 machine identified critical and high-severity vulnerabilities. By exploiting weak authentication, improper access controls, and a Python library hijacking vulnerability, the system was fully compromised.

Graphical Summary of Vulnerabilities:

Vulnerability Severity	Number of Vulnerabilities Found
Critical	1
High	2
Medium	1
Low	0
Total	**4**

List of Vulnerabilities:

#	Vulnerability	Severity	CVSS Score	Status
1	Weak Tomcat Manager Credentials	High	8.0	Closed
2	Insecure File Access (.program)	Medium	6.5	Closed
3	Weak Password Hashing	High	7.5	Closed
4	Python Library Hijacking	Critical	9.8	Closed

7. Conclusion

The VAPT exercise on the corrosion machine revealed multiple security weaknesses, from weak credentials and misconfigured services to a critical privilege escalation vulnerability via Python library hijacking. Immediate remediation steps are necessary to safeguard the system against potential breaches. This report provides a roadmap for addressing these vulnerabilities and emphasizes the importance of continual security assessments to protect organizational assets.

The assessment highlights the importance of addressing weak authentication mechanisms, enforcing proper access controls, and securing third-party dependencies to prevent future exploitation. All identified vulnerabilities have been mitigated and marked as closed, ensuring a more secure environment.