Task1
Cyber Security Intern
Muhammad Ali Jarral
CID DEN9045

Security Audit Report

Objective:
To perform a comprehensive security audit of the network, identifying potential vulnerabilities and providing recommendations for enhancing security.

Target: Simple CTF (TryHackMe)

---

1. Risk Assessment & Threat Identification

Vulnerability Identification:

- **Port Scan:**
- **Number of Services:** The scan revealed that there are **two services** running on port 1000.
- **Service Running on Higher Port:** The service detected is **SSH** on a higher port.
- **CVE Vulnerability:** The application is vulnerable to **CVE-2019-9033**, which is an issue related to improper input validation leading to SQL injection.

Vulnerabilities:

- **SQL Injection (SQLi):**
  The application is vulnerable to SQL injection, which allows attackers to manipulate queries and access or modify data. This vulnerability is critical as it can lead to data breaches or system compromise.

---

2. Exploitation Details

Password Disclosure:

- **Password Identified:** The password retrieved from the system was **secret**.
- **Authentication Method:**
  Using the password, it was possible to log into the system via **SSH**.

User Flag:

- The **user flag** was retrieved after successful login, which confirmed the access gained.

Additional Users:

- **Secondary User:** Another user named **sunbath** was found in the home directory, indicating the system is multi-user and potentially has other privileges.

Privilege Escalation:

- **Privilege Escalation Vector:** The system was vulnerable to privilege escalation through the use of **vim**, which could be leveraged to spawn a root shell and gain complete control of the system.

Root Flag:

- After gaining root access, the **root flag** was successfully retrieved.

---

3. Recommendations

Security Improvements:

1. **Close Unused Ports:**
   Disable any unnecessary services running on high or non-standard ports to reduce the attack surface.
2. **Update Vulnerable Services:**
   Patch or update the services to mitigate vulnerabilities associated with CVE-2019-9033 and prevent SQL injection attacks.
3. **Implement Input Validation:**
   Ensure that all input fields in the application validate user inputs properly to avoid SQL injection attacks.
4. **Limit SSH Access:**
   Use multi-factor authentication (MFA) for SSH logins and restrict access to trusted IPs only.
5. **Review User Permissions:**
   Conduct a review of all user accounts and limit permissions based on the principle of least privilege (PoLP).
6. **Restrict Usage of Vulnerable Programs:**
   Programs like **vim** should not be given elevated privileges that could be used for privilege escalation. Regularly review system programs for such vulnerabilities.

---

4. Conclusion

The security audit identified several critical vulnerabilities in the system, including SQL injection and improper privilege handling. By addressing these vulnerabilities and implementing the recommendations provided, the security posture of the network can be significantly improved.