Vulnerability Assessment and Pentesting Report

Ch.Jatin

Aug 18, 2025

Executive Summary:

A security test was performed on the Metasploitable2 server, revealing numerous critical vulnerabilities that allow an attacker to easily gain complete control of the system. We discovered several backdoors and services with weak default passwords. Using these weaknesses, we successfully took control of the server, proving that the system is at a high risk of compromise. Immediate patching and password changes are required to secure the server and protect any data it might hold. This summary highlights the severe risk and the need for urgent action.

1. Reconnaissance

- **Objective:** To perform Open-Source Intelligence (OSINT) to gather information about the target environment without direct interaction.
- **Process and Findings:** Standard reconnaissance techniques were used to gather information. A whois lookup was performed to identify domain registration details. Subdomain enumeration was conducted using Sublist3r to identify potential attack surfaces. Finally, the Wappalyzer browser extension was used to identify the technology stack of the web applications.

Domain Info	Subdomains	Exposed Services
Domain Name: google.com Registry Domain ID: 2138514_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.markmonitor.com Registrar URL: http://www.markmonitor.com Updated Date: 2024-08-02T02:17:33+0000 Creation Date: 1997-09-15T07:00:00+0000 Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000	accounts.google.com admanager.google.com admin.google.com admob.google.com	Analyzed the target http://192.168.56.102/twiki/bin/view/Main/WebHome Found techstack: Apache 2.2.8 HTTP Server Ubuntu OS

Checklist:

Check WHOIS	Enumerate Subdomains	Tech Stack
Done	Done	Done

2. Discovery & Vulnerability Scanning

- Objective: To identify all open ports, running services, and known vulnerabilities on the target host to map out the potential attack surface.
- Analysis and Findings: Manual scanning with Nmap and automated analysis with OpenVAS were conducted. Both scans confirmed the presence of numerous critical vulnerabilities, indicating a severely compromised security posture.

Key Critical-Risk Vulnerabilities:

  - Ingreslock Backdoor (Port 1524): A backdoor service providing immediate, unauthenticated root access (CVSS 10.0).
  - vsftpd v2.3.4 Backdoor (Port 21): A known backdoor in the FTP server that can be triggered to gain a root-level command shell (CVSS 9.8).
  - Apache Tomcat Manager (Port 8180): The administrative interface was accessible via weak default credentials (tomcat/tomcat), allowing for remote code execution (CVSS 9.8).
  - MySQL Unauthenticated Access (Port 3306): The database server allows root login with a blank password, granting full administrative control over all databases (CVSS 9.8).

3. Exploitation & Post-Exploitation

- **Objective:** To gain unauthorized shell access to the target system and perform post-exploitation to collect evidence.
- **Process and Analysis:** The assessment involved two successful exploitation scenarios. First, the **vsftpd v2.3.4 backdoor** was exploited using the exploit/unix/ftp/vsftpd_234_backdoor Metasploit module, which immediately provided a root-level command shell.
  Separately, the **Apache Tomcat Manager** was exploited using the exploit/multi/http/tomcat_mgr_upload module. After manually setting the default credentials (tomcat/tomcat) and the correct LHOST, a Meterpreter session was successfully established.

During post-exploitation, the /etc/shadow file, which contains user password hashes, was collected as evidence of the full system compromise.

4. Capstone Project: Full VAPT Cycle on DVWA

A full VAPT cycle was performed against the Damn Vulnerable Web Application (DVWA). Following the Penetration Testing Execution Standard (PTES), the engagement began with information gathering, followed by vulnerability analysis where an SQL Injection vulnerability was identified in the "SQL Injection" page. The sqlmap tool was used to confirm and exploit this vulnerability during the exploitation phase. The attack was successful, allowing for the enumeration of the backend databases and the dumping of the users table, which contained usernames and hashed passwords. This represents a critical information disclosure vulnerability. The post-exploitation phase confirmed the extent of the data exposure. Remediation steps, including the implementation of parameterized queries (prepared statements) to prevent SQL injection, were documented. A final report was compiled detailing the findings, and a non-technical summary was drafted for management, completing the VAPT cycle.

Non-Technical Summary:

A security test was conducted on the DVWA web application. The test discovered a critical flaw that allowed our team to bypass security measures and access the application's underlying database. This vulnerability enabled the extraction of sensitive user information, including usernames and password hashes. This type of flaw poses a significant risk of a data breach. We have provided detailed technical recommendations to the development team to fix the issue. It is crucial that this vulnerability is patched to protect user accounts and ensure the integrity of the application's data.