Penetration Testing Report

Client: TryHackMe: Brooklyn Nine Nine

Target IP: 10.10.253.97

Date of Test: 11/05/23

Executive Summary: The penetration test against the target IP **10.10.253.97** was conducted to identify and exploit vulnerabilities, with the aim to evaluate the security posture of the system.

1. Test Environment: The assessment was carried out within a controlled environment targeting the specified IP address.

2. Scanning and Enumeration:

- **Objective:** To discover open ports and services.
- **Method:** Conducted an Nmap scan.
- **Command Used:**

nmap -A 10.10.253.97

- **Findings:**
    - FTP Service (Port 21/tcp): vsftpd 3.0.3 with anonymous access.
    - SSH Service (Port 22/tcp): OpenSSH 7.6p1.
    - HTTP Service (Port 80/tcp): Apache httpd 2.4.29.

3. Web Service Enumeration:

- **Objective:** Identify hidden directories through the web service.
- **Method:** Performed a Gobuster directory scan.
- **Command Used:**

gobuster dir -u http://10.10.253.97 -w /usr/share/wordlists/dirb/common.txt

- **Findings:** No sensitive directories were uncovered.

4. FTP Service Enumeration:

- **Objective:** Inspect accessible files via FTP.
- **Method:** Logged in using anonymous credentials.
- **Findings:** A text file **note_to_jake.txt** indicated a potentially weak password for a user named Jake.

5. Credentials Brute Forcing:

- **Objective:** To identify the password for the user Jake.

- **Method:** Utilized Hydra for brute-forcing SSH service.
- **Command Used:**

hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.253.97

- **Findings:** The password for user Jake was identified as **987654321**.

6. System Access and User Flag:

- **Objective:** Gain user-level access and locate user flag.
- **Method:** Accessed the system via SSH with Jake's credentials.
- **Findings:** User flag was located in the Holt user's home directory.

7. Privilege Escalation:

- **Objective:** Elevate privileges to root.
- **Method:** Exploited misconfigured sudo permissions.
- **Command Sequence:**

sudo less /etc/profile !/bin/sh

- **Findings:** Successfully obtained a root shell.

8. Root Flag:

- **Objective:** Locate and secure the root flag.
- **Method:** Navigated to the root directory.
- **Findings:** Retrieved the **root.txt** flag.

Conclusion: The security assessment uncovered multiple severe vulnerabilities including unprotected FTP access, weak user password, and inappropriate sudo configurations which permitted privilege escalation.

Recommendations:

- Disable anonymous access on the FTP server or ensure it is configured properly.
- Enforce a strong password policy.
- Review and correct the sudoers file to prevent unauthorized commands execution.