wgel

Executive Summary

During a penetration test conducted on the target IP 10.10.230.243, a series of vulnerabilities were identified which led to the successful compromise of the system. The test included network scanning, service enumeration, website analysis, and exploitation of insecure file permissions and misconfigurations. The findings are detailed below.

Vulnerability Assessment and Exploitation

1. Initial Scan and Service Enumeration

An Nmap scan was conducted with the following command:

```
nmap -A 10.10.230.243
```

The results of the scan revealed the following open services:

- SSH (22/tcp) running OpenSSH 7.2p2 Ubuntu 4ubuntu2.8
- HTTP (80/tcp) running Apache httpd 2.4.18 (Ubuntu)

The presence of an outdated SSH version suggests potential vulnerabilities, and the Apache server's default page indicates possible neglect in maintenance or updates.

2. Website Analysis

Upon inspecting the source code of the web server's default page, a comment was discovered which hints at a possible username "Jessie" and suggests that the website may not be up-to-date with security patches.

3. Directory and File Enumeration

A directory brute-force attack was performed using Gobuster, which revealed a hidden directory:

http://10.10.230.243/sitemap/.ssh

Within this directory, an **id_rsa** private key file was discovered, likely belonging to the user "Jessie."

4. SSH Access and Privilege Escalation

Using the acquired private key, SSH access to the target system was established as user "Jessie":

```
ssh -i id_rsa jessie@10.10.230.243
```

Post-access enumeration revealed that the user "Jessie" had sudo privileges to run all commands and specifically to execute **/usr/bin/wget** without a password.

5. User Flag Acquisition

Navigating to Jessie's document directory led to the discovery of **user_flag.txt**, which presumably contains user-level access confirmation.

6. **Root Flag Acquisition and System Compromise**

The sudo permissions allowed the upload of a modified **/etc/passwd** file to gain root access. The following steps were taken:

- The **/etc/passwd** file was copied to a writable location for editing.
- A new root password hash was generated using Python's **crypt** module.
- The new hash was inserted into the copied **passwd** file in place of the root's existing hash.
- A simple HTTP server was set up on the attacker's machine to serve the modified **passwd** file.
- Using **wget**, the modified **passwd** file was transferred to replace the system's **/etc/passwd**.
- The password for the root user was successfully changed, and root access was obtained by switching to the root user with **su - root**.
- The **root_flag.txt** file was then accessible, confirming full system compromise.

Conclusion and Recommendations

The test concluded with the successful penetration of the target system due to outdated services, insecure permissions, and poor system management practices. It is recommended to:

- Update all services to their latest stable versions.
- Remove any unnecessary comments and sensitive information from production websites.
- Restrict write permissions on critical system files and directories.
- Implement stricter access controls and monitoring to detect anomalous activities.
- Regularly audit system and file permissions as well as user privileges.
- Conduct security awareness training for staff to avoid similar security lapses in the future.

The system should be thoroughly cleaned, and all passwords and keys should be changed post-remediation to prevent further unauthorized access.