Penetration Testing Report: GamingServer

Executive Summary

The purpose of this penetration test was to identify vulnerabilities within the target system at IP address 10.10.239.25. Permission for the test was granted, and it was conducted using an aggressive scan approach with NMAP, followed by directory enumeration, password cracking, and eventual privilege escalation. The report details the methodologies used, findings, and recommendations for securing the system.

Methodology and Findings

1. NMAP Scanning

An aggressive NMAP scan was conducted, revealing two open ports:

- **SSH (22/tcp):** Running OpenSSH 7.6p1 Ubuntu 4ubuntu0.3.
- **HTTP (80/tcp):** Served by Apache httpd 2.4.29 (Ubuntu).

The scan also identified potential SSH host keys and a username **john** through comments found in the website source code.

2. HTTP Enumeration

Using GoBuster, several directories were discovered:

- **/index.html:** Standard entry page.
- **/robots.txt:** Revealed the presence of the **/uploads/** directory.
- **/secret:** Contained an RSA secret key, which was stored as **rsakey**.
- **/uploads:** Contained password lists, an image, and a document.

3. Password Cracking

The RSA key from the **/secret** directory was targeted for password cracking:

- Converted for John the Ripper using **ssh2john**.
- John the Ripper found the passphrase **letmein** using the rockyou.txt wordlist.

4. SSH Enumeration

With the passphrase, an SSH session was established as user **john**. Prior to access, the RSA key permissions were secured using **chmod 600**.

5. Root Privilege Escalation

Sudo privileges were checked but required a password not known to the tester. To escalate privileges, a method involving the LXD group was chosen:

- **linpeas.sh** was uploaded using SCP to the target system.

- An LXD exploit (EDB-ID 46978) was obtained and executed.
- A tar file and an exploit script (**game.sh**) were uploaded, and the script executed with the tar file to gain root access.

6. Flag Acquisition

The final flag was located in the **/mnt/root/root** directory after obtaining root access.

Recommendations

- **SSH Service:** Update and secure SSH by disabling root login and using key-based authentication.
- **Web Service:** Remove any default content and ensure that all web directories and files have appropriate permissions.
- **User Accounts:** Investigate the presence of user **john** and ascertain if the account is legitimate.
- **Password Policy:** Implement a strong password policy and avoid using common passwords.
- **Regular Scans:** Conduct regular scans for exposed directories and files.
- **Privilege Policy:** Review user groups and privileges to avoid unauthorized privilege escalation.

Conclusion

The penetration test successfully identified several security issues, including insecure SSH and HTTP configurations, weak passwords, and privilege escalation vulnerabilities. Immediate action is recommended to address these findings to enhance the overall security posture of the system.