StartUp

Penetration Testing Report

Executive Summary: A penetration test was conducted on the target IP to evaluate the security posture of its network services and web applications. The test revealed several critical vulnerabilities that could potentially be exploited by an unauthorized party to gain access to sensitive information or compromise the integrity and availability of the system.

Test Parameters:

- **Target:** 10.10.183.157
- **Testing Tool:** Nmap with the **-A** option for aggressive scan

Findings:

1. **FTP Service Analysis:**
    - Port 21 was found to be open, running vsftpd 3.0.3.
    - Anonymous FTP login was allowed, leading to the discovery of two files: **important.jpg** and **notice.txt**.
    - **important.jpg** was identified as an Among Us meme image, and **notice.txt** contained a message indicating internal frustration over the misuse of the FTP server for sharing memes.
2. **Web Application Review:**
    - HTTP service running on port 80 presented a placeholder page indicating the site was under development.
    - A job listing suggested that the web development team was seeking new personnel.
    - Directory brute-forcing with Gobuster only revealed a **/files** directory, which was already known.
3. **Exploitation:**
    - A PHP reverse shell was successfully uploaded to the **/ftp** directory via the FTP service.
    - A Netcat listener was set up on port 666, and the PHP reverse shell was executed by accessing the file through the web server, granting shell access to the tester.
    - Directory traversal led to the discovery of a **recpie.txt** file and an **incidents** directory containing a **suspicious.pcapng** file.
    - The **.pcapng** file was analyzed with Wireshark, revealing a previous shell session with clear text HTTP login credentials for a user named lennie.
4. **Privilege Escalation:**

- A stable shell was established using Python to upgrade from the initial Netcat shell.
- Credentials obtained from the Wireshark analysis were used to switch to the lennie user account.
- The user flag was retrieved from the **user.txt** file.
- The **pspy64** tool was uploaded and executed, revealing a background script **planner.sh**, which interacted with **print.sh**.
- A reverse shell was inserted into **print.sh**, and upon its execution by the system's cron job, a root shell was obtained on the listener.
- The root flag was captured from the **root.txt** file.

Conclusion: The target IP was found to be vulnerable due to misconfigured FTP services allowing anonymous access, poor handling of sensitive information, and insufficient privilege separation. Immediate action is recommended to address these issues. The following measures should be taken:

- Disable anonymous FTP access and ensure that sensitive files are not accessible without proper authentication.
- Implement content filtering to prevent the misuse of the FTP service.
- Review and harden cron job scripts to prevent unauthorized modifications.
- Enforce strong password policies and secure transmission protocols to protect credentials.
- Conduct a comprehensive review of system access controls and user permissions.

Recommendations: For remediation and to prevent future breaches, it is advised to:

- Conduct regular security audits of network services.
- Employ file integrity monitoring on critical system files.
- Provide security awareness training to staff to prevent internal misuse.
- Hire a qualified web developer to secure the web application.
- Establish comprehensive logging and monitoring to detect and respond to malicious activities swiftly.

By addressing the vulnerabilities discovered during this penetration test, the security posture of the target system will be significantly improved, reducing the risk of successful cyberattacks.