Penetration Testing Report: Lian Yu

Target IP: 10.10.37.40

Tools Used: Nmap, Gobuster, Steghide, Hex Editor, SSH Client, pkexec

Executive Summary: The penetration test began with an Nmap scan revealing multiple open ports and services including FTP, SSH, HTTP, and rpcbind. Further enumeration on the HTTP service using Gobuster exposed hidden directories and potential steganographic clues.

Key Findings:

1. **Service Enumeration:**
    - FTP running vsftpd 3.0.2 on port 21.
    - SSH running OpenSSH 6.7p1 on port 22.
    - HTTP running Apache with an interesting title "Purgatory" on port 80.
    - rpcbind running on port 111 with various RPC services.
2. **HTTP Service Analysis:**
    - The HTTP service did not reveal significant findings initially.
    - Steganographic analysis hinted at further hidden data.
    - Gobuster uncovered a directory **/island** and a suggestive codeword "vigilante".
    - Additional Gobuster scans with numerical wordlists exposed a directory **/2100** with a cryptic message hinting at a **.ticket** extension.
    - Discovery of **/green_arrow.ticket** led to a token **RTy8yhBQdscX** and a suggestion to use cyberchef, yielding a password **!#th3h00d**.
3. **FTP Enumeration:**
    - Successful access to the FTP server using the credentials "vigilante" and **!#th3h00d**.
    - Acquisition of multiple files including **Leave_me_alone.png**, **Queen's_gambit.png**, **aa.jpg**, and a hidden file **.other_user**.
    - Correcting the header of a corrupted PNG file revealed another password "password".
    - Steghide extraction on **aa.jpg** using the new password produced a zip file containing **shado** & **passwd.txt**, with **shado** containing the passphrase "M3tahuman".
4. **SSH Enumeration:**
    - Access gained to the SSH server with the username "Slade Wilson" and the passphrase "M3tahuman".

- Discovery of **user.txt** and a mysterious **.Important** file suggesting a search for "Secret_Mission".

5. **Root Privilege Escalation:**
    - Sudo permissions check indicated the user "Slade" could run **/usr/bin/pkexec** as root.
    - A search for "Secret_Mission" led to **/usr/src/Secret_Mission**, containing ambiguous text related to "Mirakuru" and superpowers.
    - Utilization of **pkexec** allowed for root privilege escalation, leading to the acquisition of **root.txt**.

Conclusion: The system's vulnerabilities, primarily through misconfigurations and hidden data, allowed for full system compromise. Recommendations for hardening include strict file permissions, secure password policies, and the removal of unnecessary services.

Acknowledgments: This report summarizes the penetration test conducted and does not include all commands and outputs for brevity. Full technical logs are available upon request.