Penetration Testing Report: Source

Executive Summary

This report details the findings from a Capture the Flag (CTF) exercise performed on a target IP **10.10.225.221**. The exercise involved an aggressive scan using Nmap, identification of open ports, discovery of a critical vulnerability (CVE-2019-15107) in a Webmin service, and subsequent exploitation using Metasploit to gain root access.

Objective

The objective of the CTF exercise was to identify and exploit vulnerabilities within the target system to gain unauthorized access and escalate privileges.

Methodology

1. **Nmap Aggressive Scan**:
    - An aggressive scan (**nmap -A**) was executed against the target IP **10.10.225.221**.
    - Two open ports were discovered:
        - Port 22/tcp (SSH service)
        - Port 10000/tcp (Webmin HTTP service, version 1.890)
2. **Vulnerability Assessment**:
    - A Webmin login interface was found on port 10000.
    - Using AttackerKB and Searchsploit, a significant vulnerability, CVE-2019-15107 (a backdoor in Webmin), was identified.
3. **Exploitation**:
    - Metasploit's **msfconsole** was used to exploit CVE-2019-15107.
    - The exploit module was set with appropriate options:
        - **RHOSTS**: 10.10.225.221
        - **RPORT**: 10000
        - **SSL**: true
        - **LHOST** and **LPORT**: Configured for reverse shell
    - The exploit was successfully executed, gaining root access on the target.
4. **Post-Exploitation**:
    - A stable shell was established using Python's **pty** module.
    - Full system access was achieved, and flags were captured.

Key Findings

1. **Critical Vulnerability in Webmin (CVE-2019-15107)**:
    - The target system was running a vulnerable version of Webmin, allowing for remote code execution and privilege escalation.
2. **Inadequate Security Measures**:
    - The target system lacked adequate protections against known vulnerabilities, highlighting a significant oversight in patch management and security hardening.

Recommendations

1. **Immediate Patching**:
    - Update the Webmin service to the latest version to mitigate the CVE-2019-15107 vulnerability.
2. **Regular Vulnerability Scanning and Patch Management**:
    - Implement a routine for regular vulnerability scanning and timely application of security patches.
3. **Enhanced Security Configurations**:
    - Review and strengthen security configurations for services running on exposed ports, especially those accessible over the network.

Conclusion

The exercise demonstrated a critical vulnerability in the Webmin service, leading to full system compromise. It underscores the importance of regular vulnerability assessments and prompt patching of identified vulnerabilities to maintain robust security postures in networked environments.