Executive Summary

A penetration test was conducted on the Metasploitable VM with the IP address 192.168.1.4. The goal was to identify and analyze vulnerabilities by simulating real-world cyber-attacks.

The test identified a critical vulnerability on the target machine: an outdated FTP service (Vsftpd 2.3.4). This weakness was successfully exploited using the exploit/unix/ftp/vsftpd_234_backdoor Metasploit payload, allowing the tester to gain root access. This finding highlights a significant security risk due to the use of unpatched, vulnerable software.

Project Scope and Findings

The scope of this engagement was limited to the single in-scope device, the Metasploitable VM. The initial port scan revealed two key services with known vulnerabilities:

Port	Service	Version	Vulnerable?
21	ftp	Vsftpd 2.3.4	Yes
139	smb	samba	Yes

The most critical finding was the successful exploitation of the FTP service. This was due to the service running an outdated version that contained a backdoor. The exploit provided full administrative (root) control of the system, a critical finding that could lead to complete system compromise if exploited by a malicious actor.

Recommendations

To address the identified vulnerabilities and mitigate future risks, the following actions are recommended:

- **Update the FTP Service:** The Vsftpd service must be updated immediately to a secure, patched version to remove the backdoor vulnerability.
- **Patch Other Services:** The Samba service should also be updated to a secure version to prevent exploitation of the SMB vulnerability.
- **Regular Security Audits:** Implement a schedule for regular port scans and vulnerability assessments to proactively identify and patch new weaknesses.

- **System Hardening:** Review and update all system configurations, disable unnecessary services, and apply the principle of least privilege to minimize the attack surface.