Key Findings

- **[Critical] Remote Code Execution (RCE) via WebDAV:** Misconfigured WebDAV allowed arbitrary file uploads. An attacker could upload a malicious PHP shell and gain full remote control of the system.
- **[Critical] Unpatched FTP Service (vsftpd 2.3.4):** The target ran a known vulnerable version of vsftpd containing a backdoor exploit. This provided an easy entry point for attackers to obtain shell access.
- **[High] Excessive Service Exposure:** Multiple unnecessary services (FTP, HTTP) were exposed without restriction. Each exposed service increased the attack surface and provided more avenues for exploitation.
- **[Medium] Insecure System Configuration:** Sensitive files and system information were accessible post-compromise. Default configurations and insufficient hardening made exploitation easier.

Recommendations

- **Patch & Update Vulnerable Software:** Immediately update or decommission vsftpd 2.3.4 and other outdated services. Implement a formal patch management policy to ensure systems remain secure.
- **Harden Web Services:** Disable WebDAV unless required. If needed, restrict uploads to trusted, non-executable file types and enforce authentication. Deploy a Web Application Firewall (WAF) to block malicious requests.
- **Reduce Attack Surface:** Disable or firewall unnecessary services. Restrict SSH and FTP access to trusted IP ranges or secure VPN tunnels.
- **System Hardening & Defense in Depth:** Apply least-privilege principles to files and accounts. Disable unused accounts and services. Segment critical services from general access networks. Conduct regular penetration tests and vulnerability scans to maintain security posture.

Overall Risk Assessment

The target system is highly vulnerable to compromise due to critical, easily exploitable flaws. Without immediate remediation, an attacker could gain full system control, access sensitive information, and pivot to other systems within the environment.