Information Security - INSY 8416 **06th August, 2025**

Names:

IRAKOZE Grace Vanny **ID: 26425**

Final Project (VAPT Practical Exercise).

Qn1. Vulnerability Assessment and Exploitation Report.

Qn2. VAPT Practical Exercise Report – Silky-CTF 0x02.

Qn1.

Part 1: Installation of Metasploitable 2

Introduction

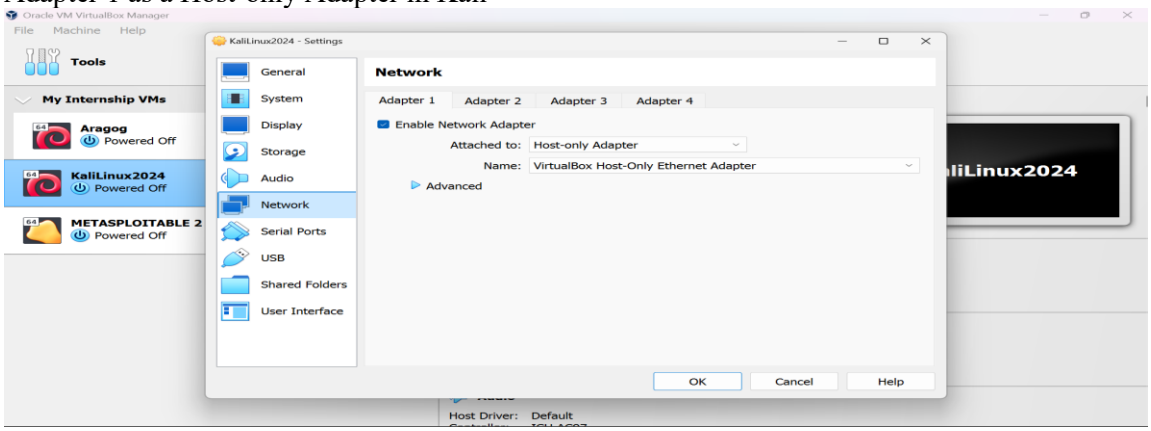
In this part, we installed the Metasploitable 2 vulnerable machine in VirtualBox using the Host-Only network adapter to safely perform penetration testing.

Steps Performed:

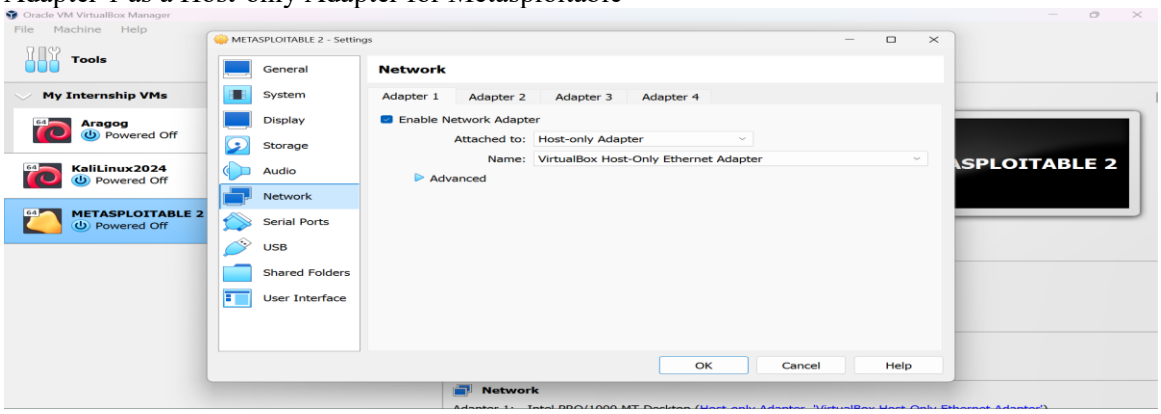
1. Downloaded Metasploitable 2 from VulnHub.
2. Imported the VM into VirtualBox.
3. Configured Adapter 1 as Host-Only (vboxnet0) for isolated lab communication.
4. Started the VM and logged in with default credentials (msfadmin/msfadmin).
5. Checked the IP address using `ifconfig`.
6. Verified network connectivity from Kali using ping

➔ Screenshot of VM Network Settings

Adapter 1 as a Host-only Adapter in Kali



Adapter 1 as a Host-only Adapter for Metasploitable



➔ Screenshot of Metasploitable IP using ifconfig
Metasploitable IP Address: **192.168.56.102**

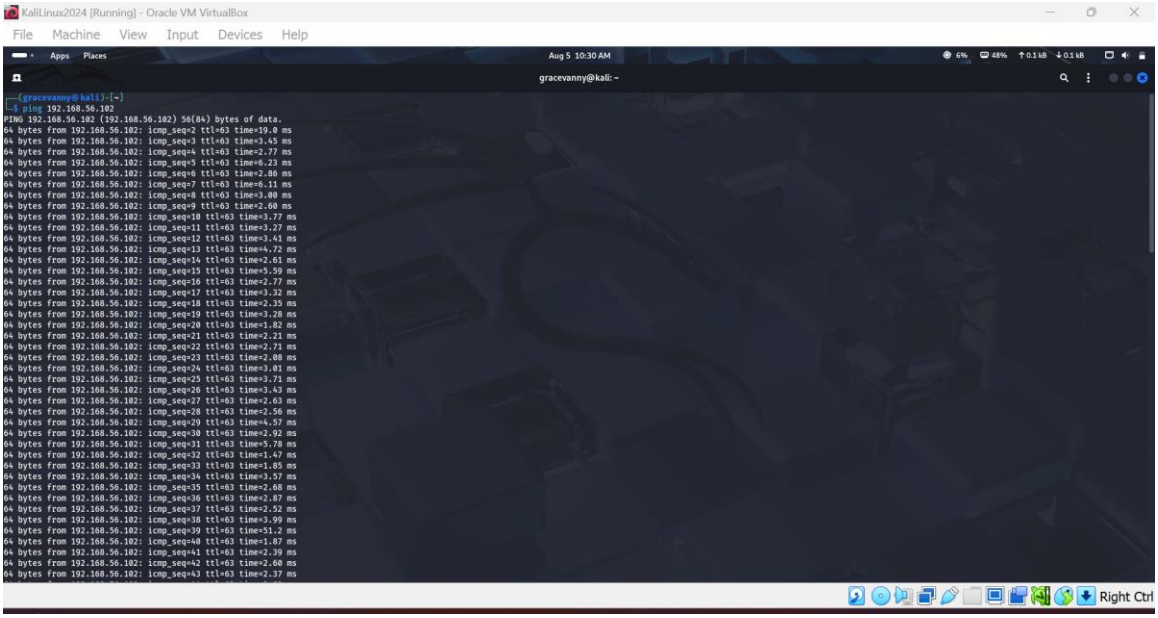
```
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:dc:28:3b
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedc:283b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

➔ Granting user privileges as a root

```
KaliLinux2024 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Apps  Places                Aug 1  8:49 AM                3%  56%  0.0 kB  0.0 kB
gracevanny@kali: ~

┌──(gracevanny㉿kali)-[~]
└─$ sudo su
[sudo] password for gracevanny:
┌──(root㉿kali)-[/home/gracevanny]
└─# usermod aG sudo gracevanny
Usage: usermod [options] LOGIN

Options:
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -b, --badname                 allow bad names (DEPRECATED)
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* files
  -r, --remove                  remove the user from only the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account
      --selinux-range SERANGE   new SELinux MLS range for the user account

┌──(root㉿kali)-[/home/gracevanny]
└─# groups gracevanny
```

```
┌──(root㉿kali)-[/home/gracevanny]
└─# groups gracevanny
gracevanny : gracevanny adm dialout cdrom floppy sudo audio dip video plugdev users netdev scanner bluetooth lpadmin wireshark vboxsf kaboxer

┌──(root㉿kali)-[/home/gracevanny]
└─# su - gracevanny
┌──(gracevanny㉿kali)-[~]
└─$ sudo whoami
[sudo] password for gracevanny:
root
```

➔ Screenshot of Successful ping from Kali to Metasploitable



Part 2: Nmap Scan and Service Version Detection

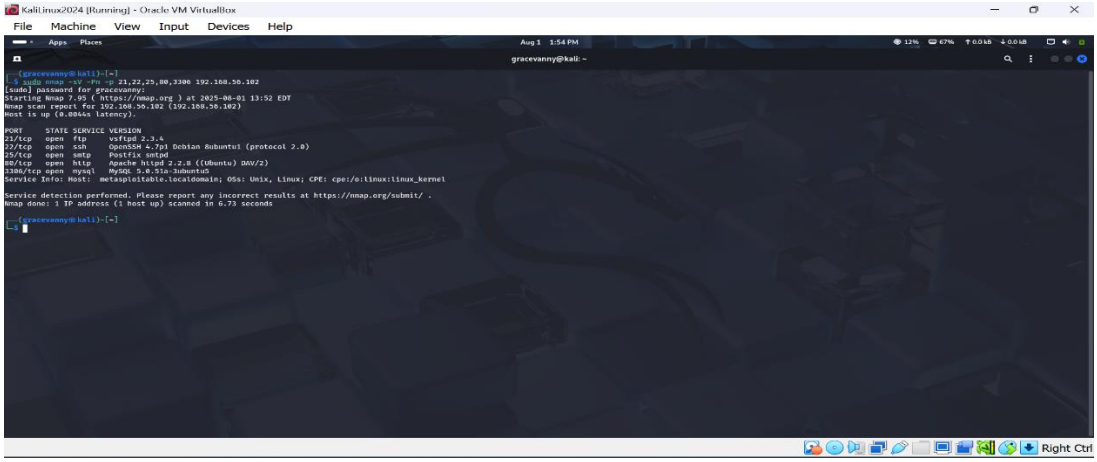
After confirming the target is reachable, we performed an Nmap scan to detect open ports and service versions.

Nmap Command Used:
sudo nmap -sV -Pn -p 21,22,25,80,3306 192.168.56.102

Output:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
25/tcp	open	smtp	Postfix smtpd (likely 2.5.x)
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5

➔ Full Nmap scan result



Vulnerability Assessment:

- FTP (vsftpd 2.3.4) → Vulnerable to CVE-2011-2523 (backdoor RCE)
- SSH (OpenSSH 4.7p1) → Outdated; weak for brute force
- SMTP (Postfix smtpd) → Could allow mail relay if misconfigured
- HTTP (Apache 2.2.8) → WebDAV directory traversal & PHP-CGI RCE
- MySQL (5.0.51a) → Potential unauthenticated remote login

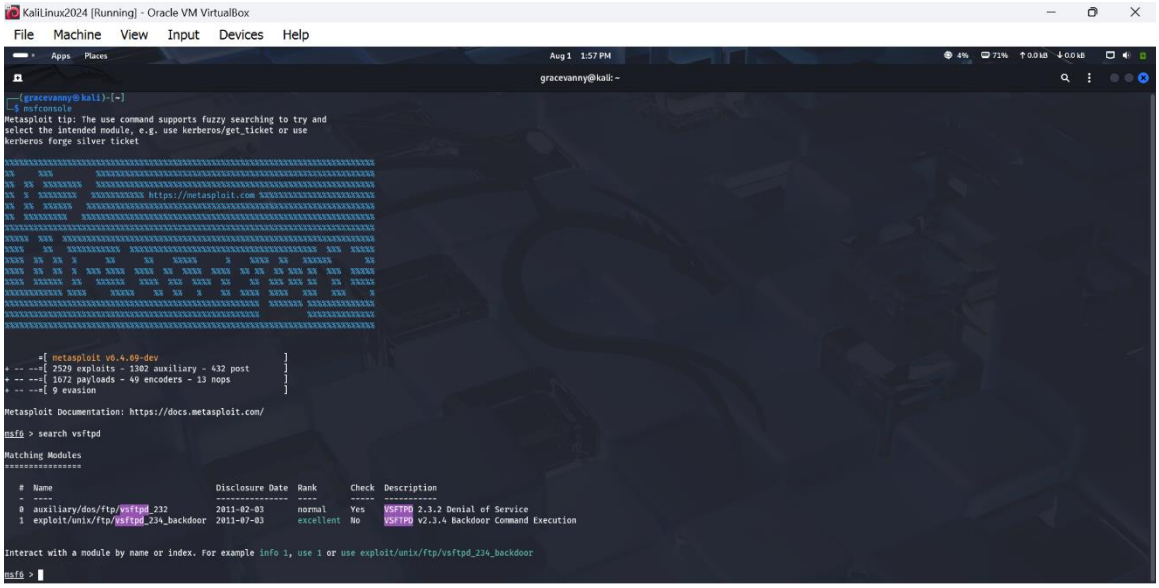
Part 3: Exploitation of Vulnerability

We exploited the FTP service running vsftpd 2.3.4 using the known backdoor vulnerability (CVE-2011-2523) to gain root access on Metasploitable 2.

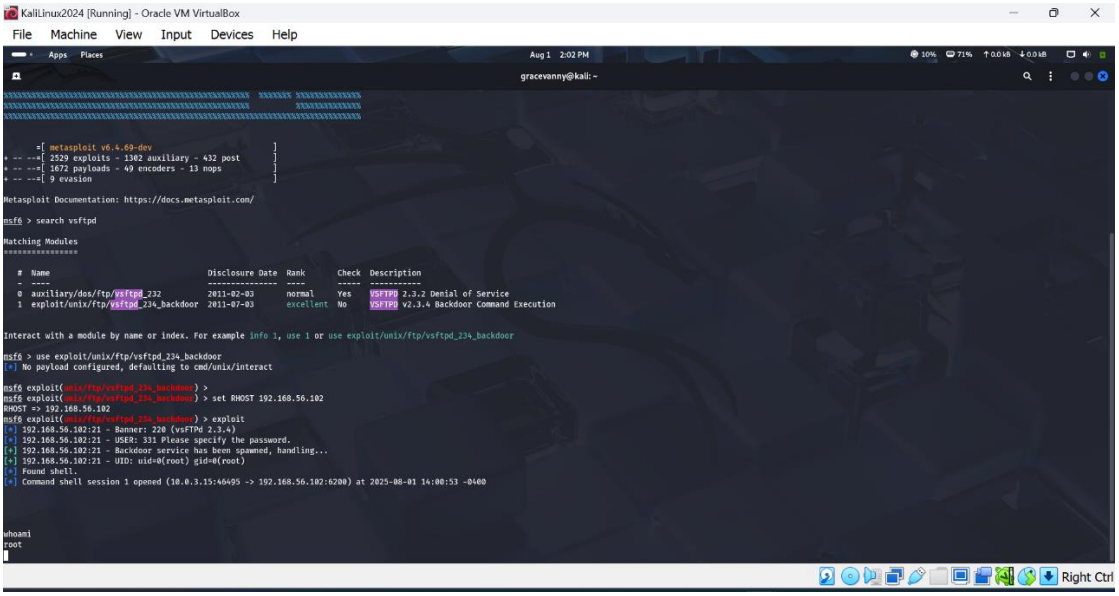
Exploitation Steps:

1. Launch Metasploit Framework: `msfconsole`
2. Search for the exploit: `search vsftpd`
3. Use the exploit module: `use exploit/unix/ftp/vsftpd_234_backdoor`
4. Set the target IP: `set RHOSTS 192.168.56.102`
5. Run the exploit: `run`
6. Verify root access in the session: `whoami` → root

➔ Metasploit exploit execution



➔ Root shell access verification



Conclusion

All in all, we successfully installed and scanned Metasploitable 2, identified vulnerable services, and exploited vsftpd 2.3.4 to gain root access. This demonstrates the risk of outdated software and the importance of regular patching.

Qn 2.

1

1. Introduction

The purpose of this practical exercise was to perform a Vulnerability Assessment and Penetration Testing (VAPT) on the virtual machine from VulnHub.

2. Methodology & Steps

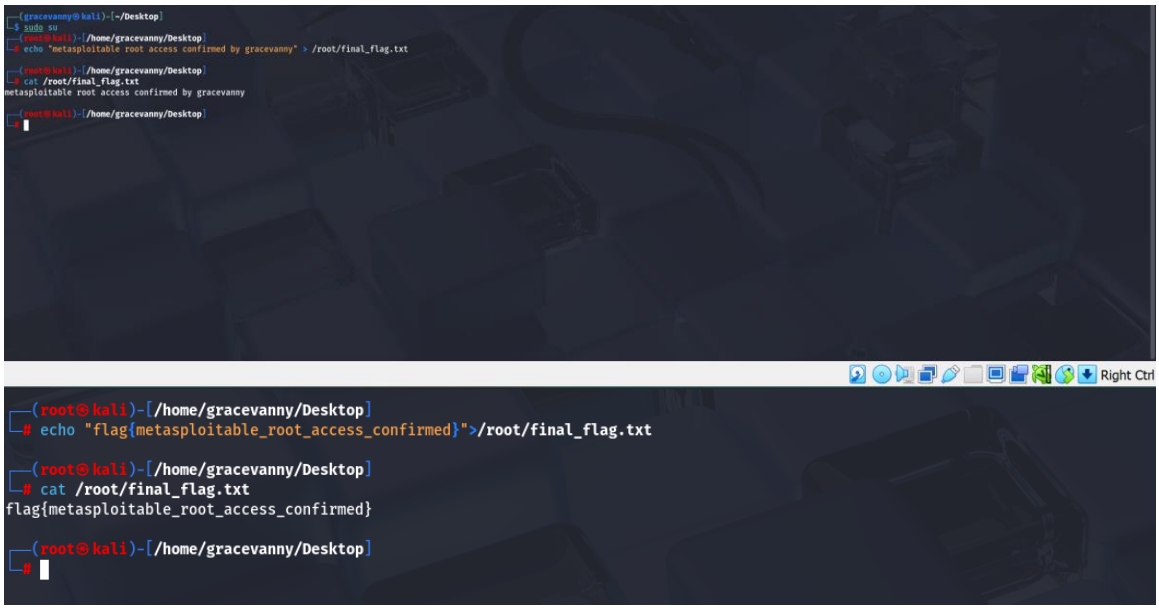
1. Network Discovery: Used net discover to identify the target VM IP address.
2. Port Scanning: Performed Nmap scans to detect open ports and services.
3. Service Enumeration: Enumerated web services and Samba shares for potential vulnerabilities.
4. Exploitation: Exploited discovered vulnerabilities to gain shell access.
5. Privilege Escalation: Escalated privileges to root and accessed the final flag.

3. Findings & Analysis

During the VAPT exercise, the following findings were made:
- Open services were identified, including SSH (22), HTTP (80), and SMB (445).
- A misconfigured Samba share allowed unauthorized access and file enumeration.
- Weak credentials enabled remote login and system compromise.
- Privilege escalation was achieved using misconfigured sudo permissions.

4. Proof of Concept Screenshots

The following screenshots were captured during the assessment as proof of concept:
- Nmap Scan Results
- Service Enumeration Output
- Initial Shell Access
- Privilege Escalation Proof
- Final Flag Capture



5. Conclusion

The Machine was successfully compromised using network scanning, service enumeration, and privilege techniques. Misconfigured services and weak credentials were the key vulnerabilities exploited to capture the final flag.