

Metasploit Exploitation Lab: vsftpd 2.3.4 Backdoor

Kevin Goates

Personal Cybersecurity Home Lab

Offensive Security / Penetration Testing Practice

August 1, 2025

Introduction

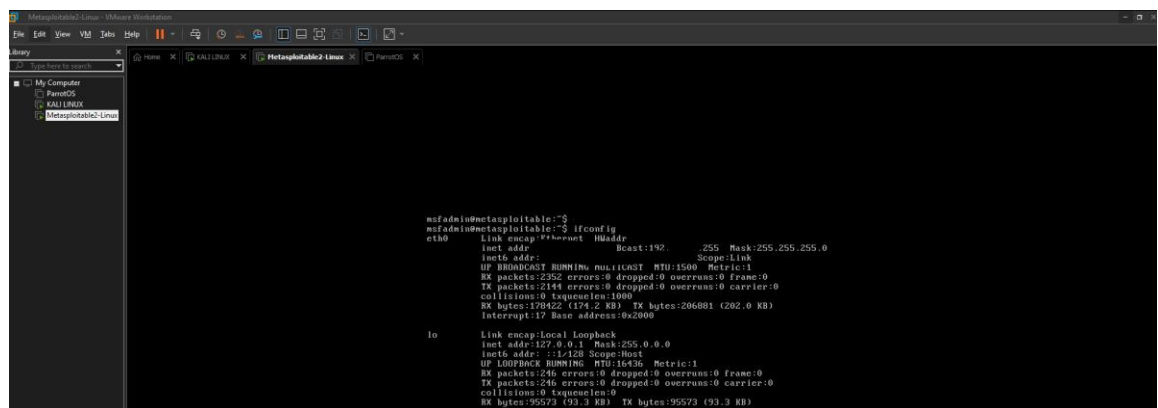
This lab demonstrates the exploitation of a known vulnerability in the vsftpd 2.3.4 service running on Metasploitable 2 using the Metasploit Framework. The purpose of this exercise is to practice penetration testing techniques in a safe, controlled environment.

Tools Used

- VMware Workstation
- Kali Linux (attacker machine)
- Metasploitable 2 (target machine)
- Metasploit Framework
- Nmap (network scanning tool)

Steps Taken

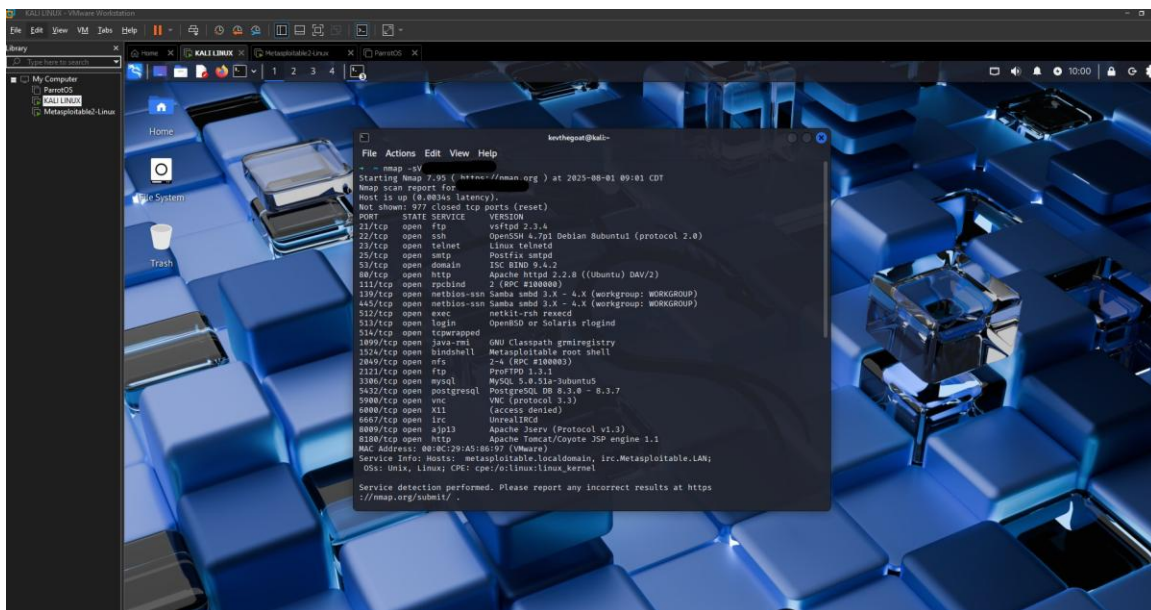
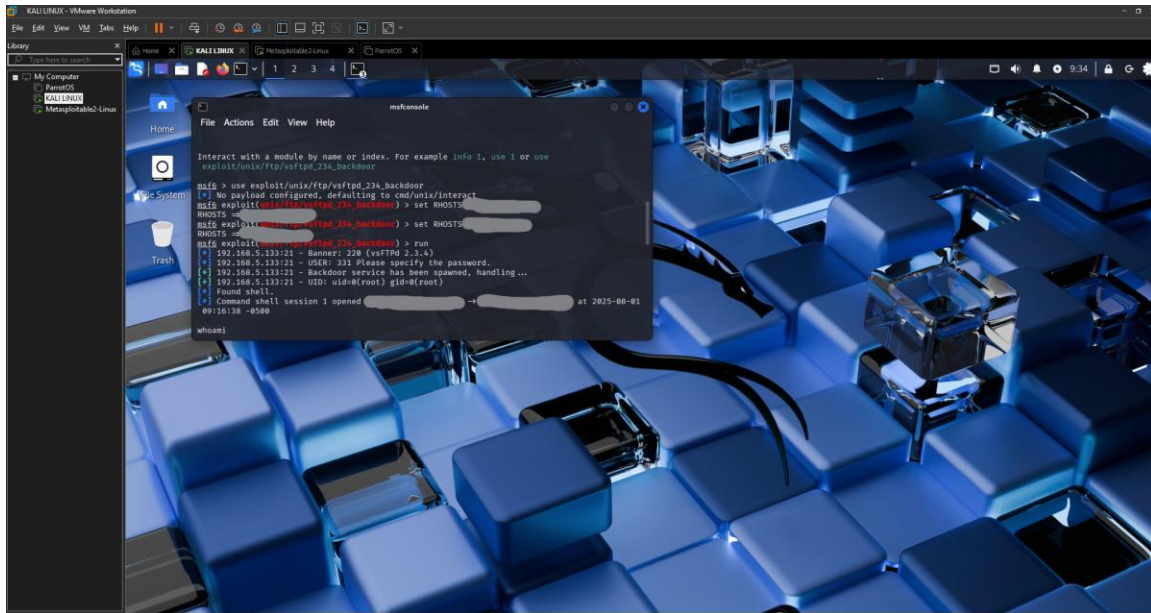
Step 1: Identified the IP address of the Metasploitable target using ifconfig.



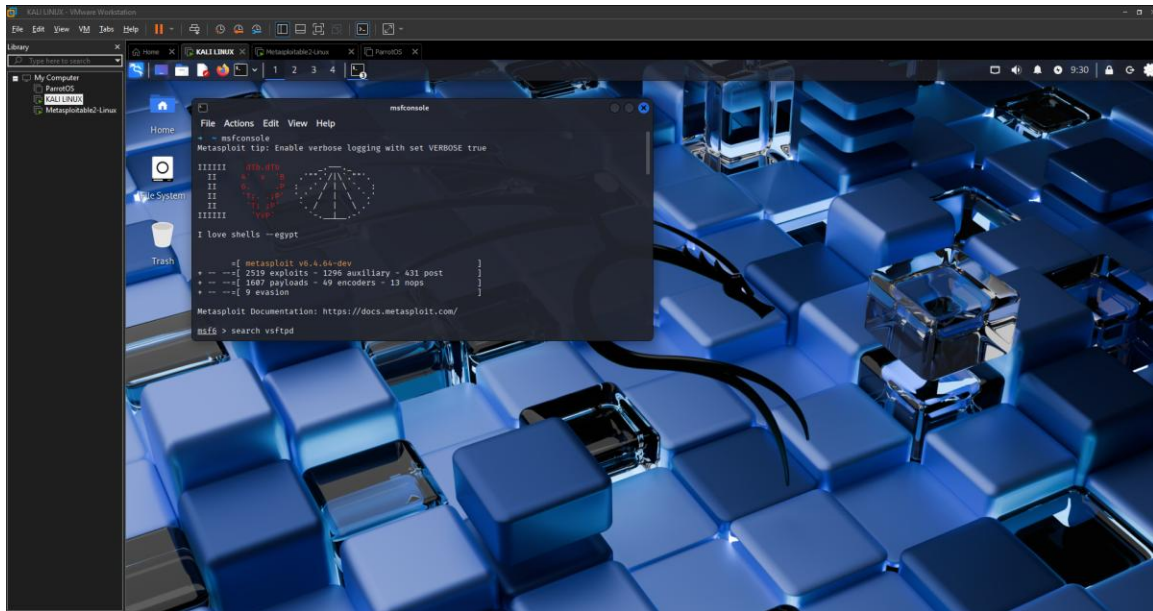
```
msfadmin@metasploitable:~$ ifconfig
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:06:27:00:00
          inet addr:192.168.1.154  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::200:6:27:0:0:0:0:0  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2352 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:178422 (174.2 KB)  TX bytes:206081 (202.0 KB)
          Interrupt:17 Base address: 0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1:1  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:246 errors:0 dropped:0 overruns:0 frame:0
          TX packets:246 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:95573 (93.3 KB)  TX bytes:95573 (93.3 KB)
```

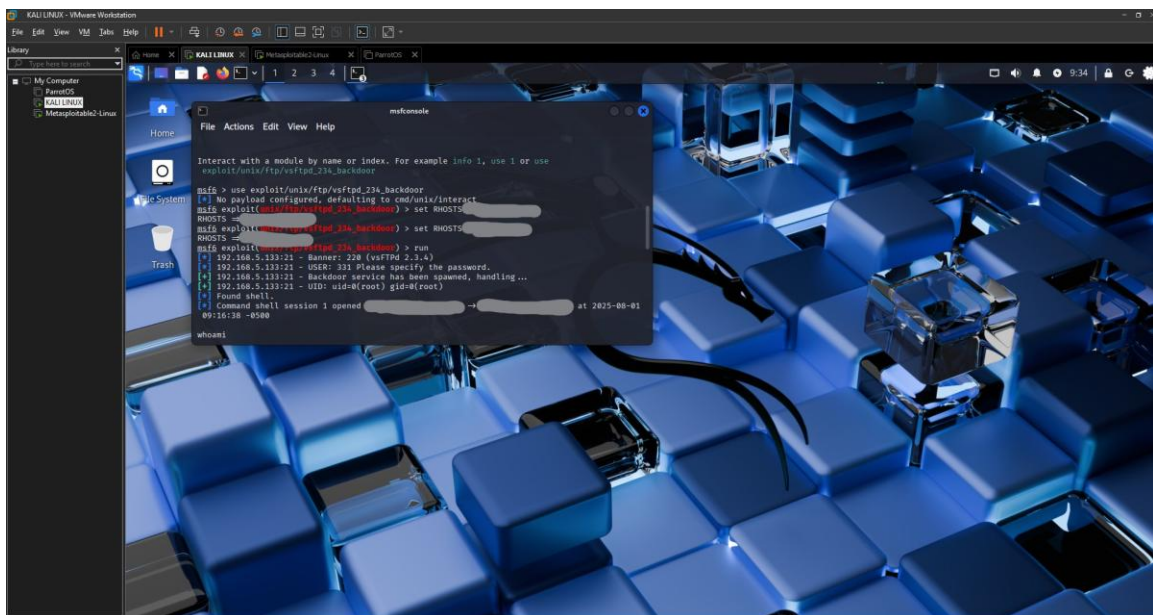
Step 2: Scanned the target with nmap to verify vsftpd service was running on port



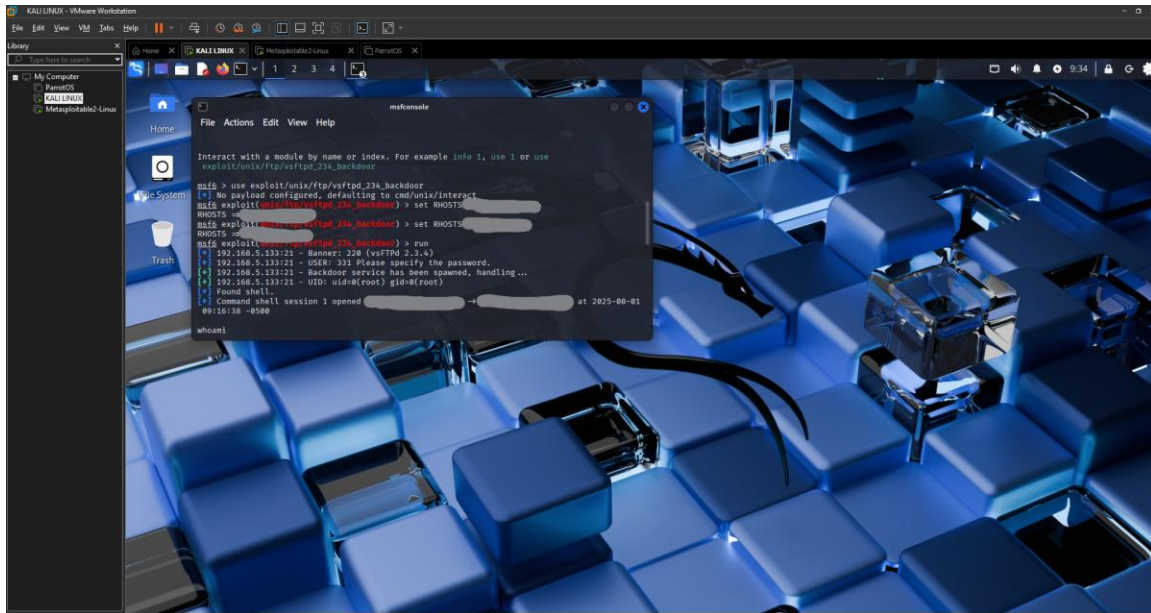
Step 3: Launched Metasploit and searched for the vsftpd 2.3.4 backdoor exploit.



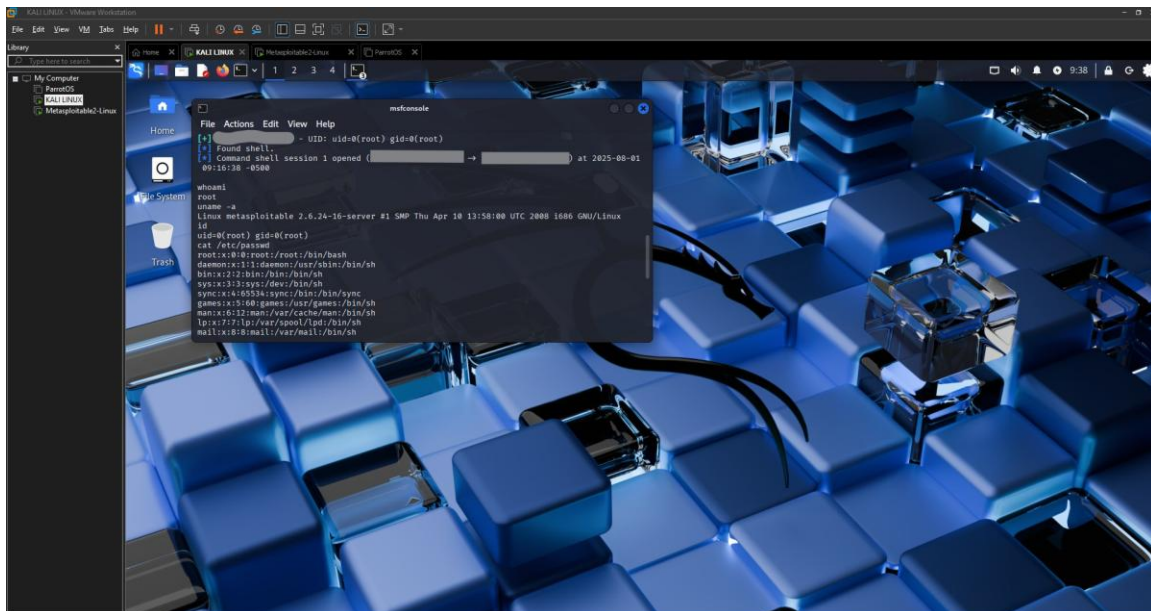
Step 4: Configured the exploit by setting RHOSTS to the target IP.



Step 5: Executed the exploit using the run command.



Step 6: Opened a shell session and verified access using whoami, uname -a, and id.



Results

The vsftpd 2.3.4 backdoor was successfully exploited, resulting in remote shell access to the Metasploitable machine with root privileges. Screenshots of each step demonstrate the process and outcome.

Reflection

This lab provided practical experience in exploiting a known vulnerability using Metasploit. It reinforced understanding of network scanning, module selection, and exploitation workflows. The exercise also emphasized the importance of maintaining security patches to prevent such vulnerabilities.

References

Rapid7. (n.d.). Metasploitable download.
<https://information.rapid7.com/metasploitable-download.html>
Rapid7. (n.d.). Metasploit documentation. <https://docs.rapid7.com/metasploit/>