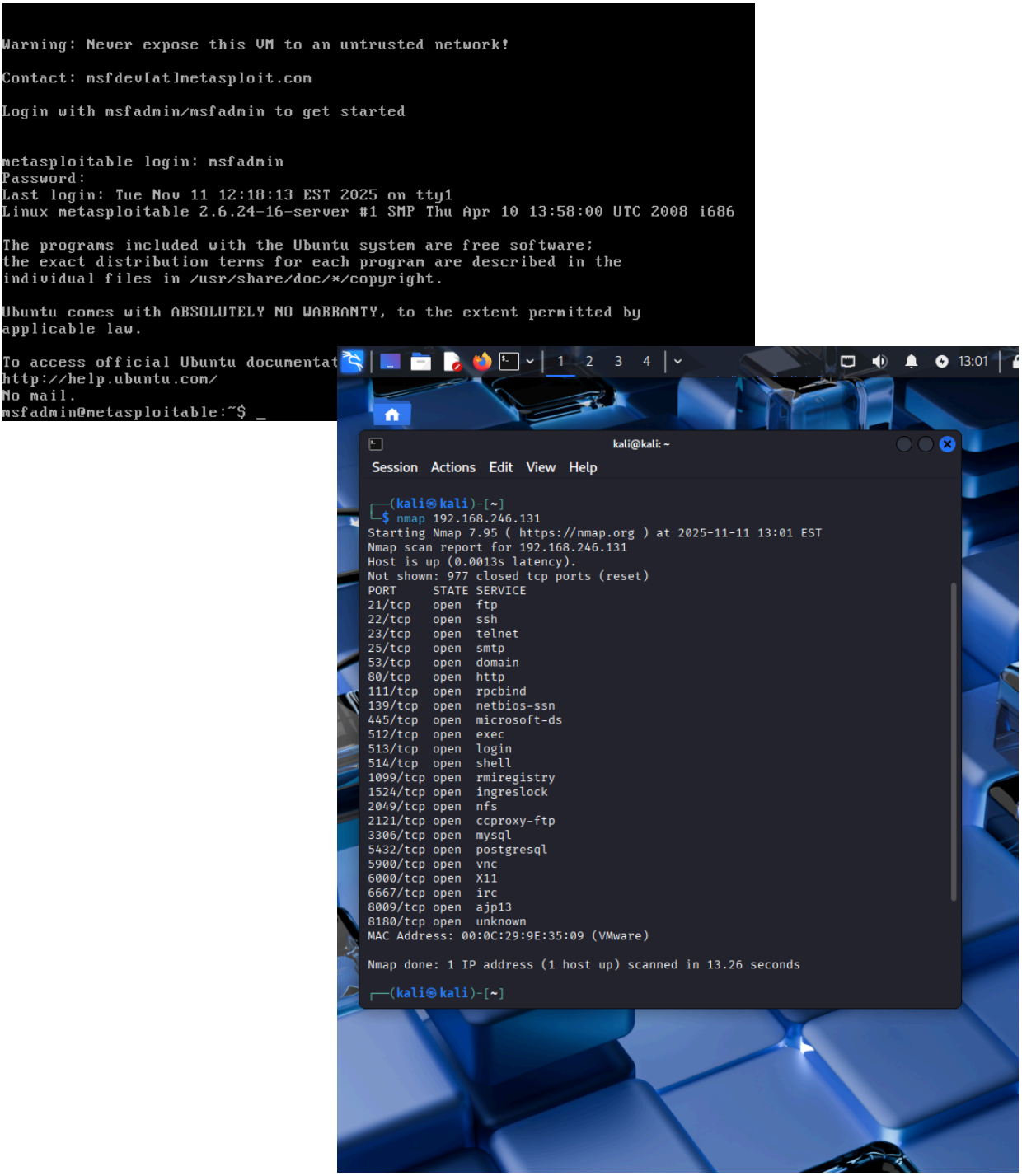
Metasploit Exploitation Workflow

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.

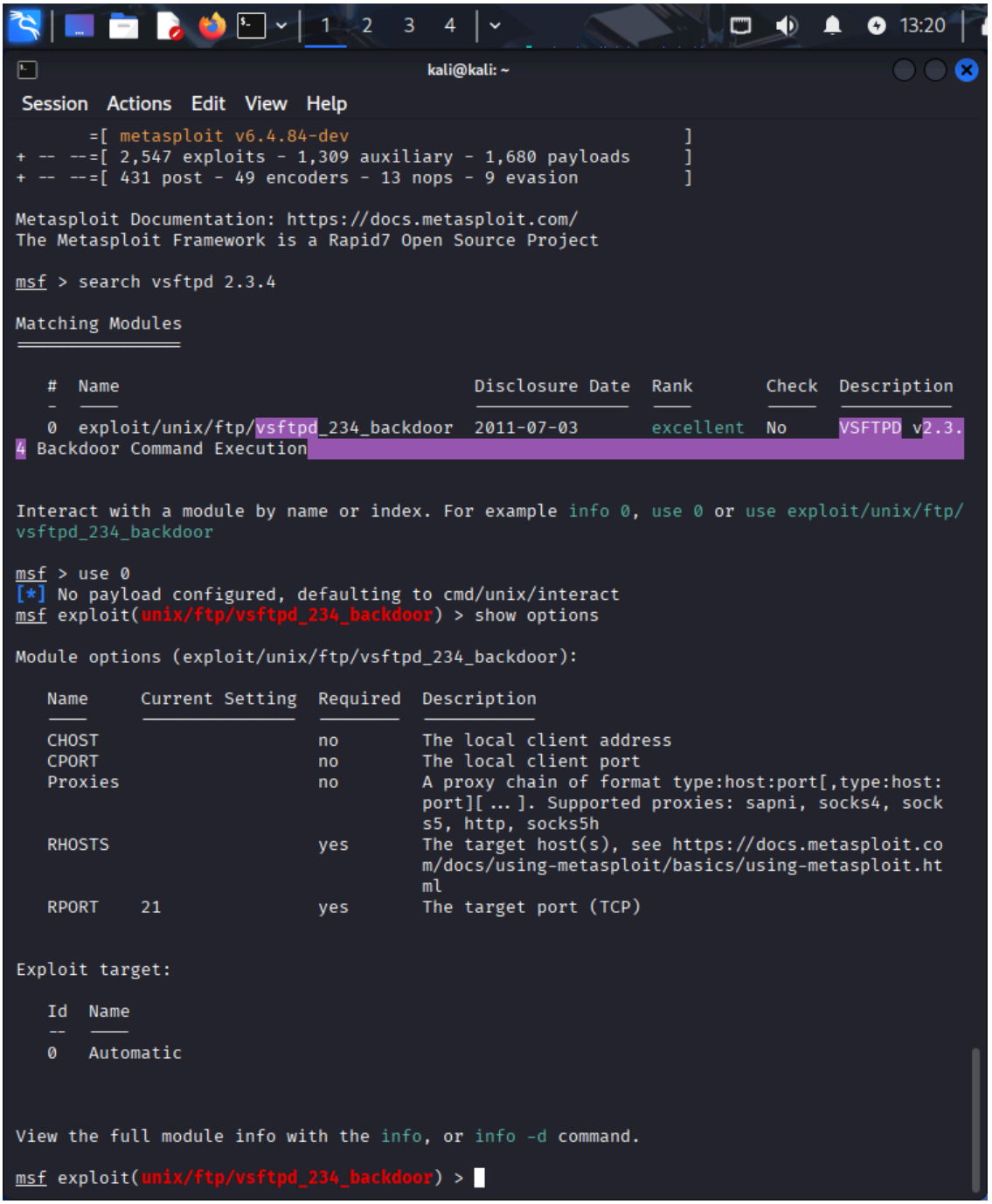
1. Starting Metasploit (msfconsole)

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



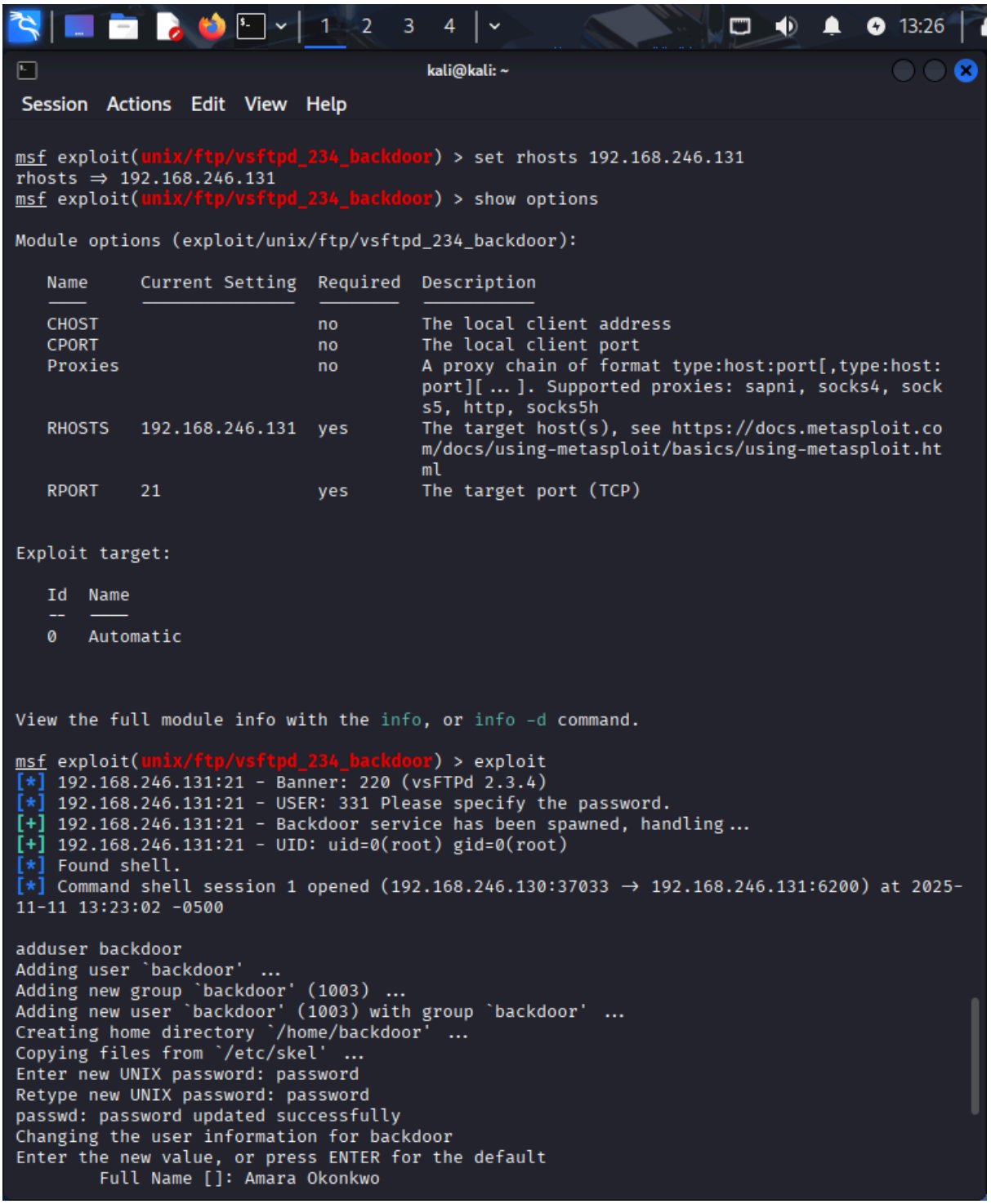
2. Searching for an Exploit Module

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.



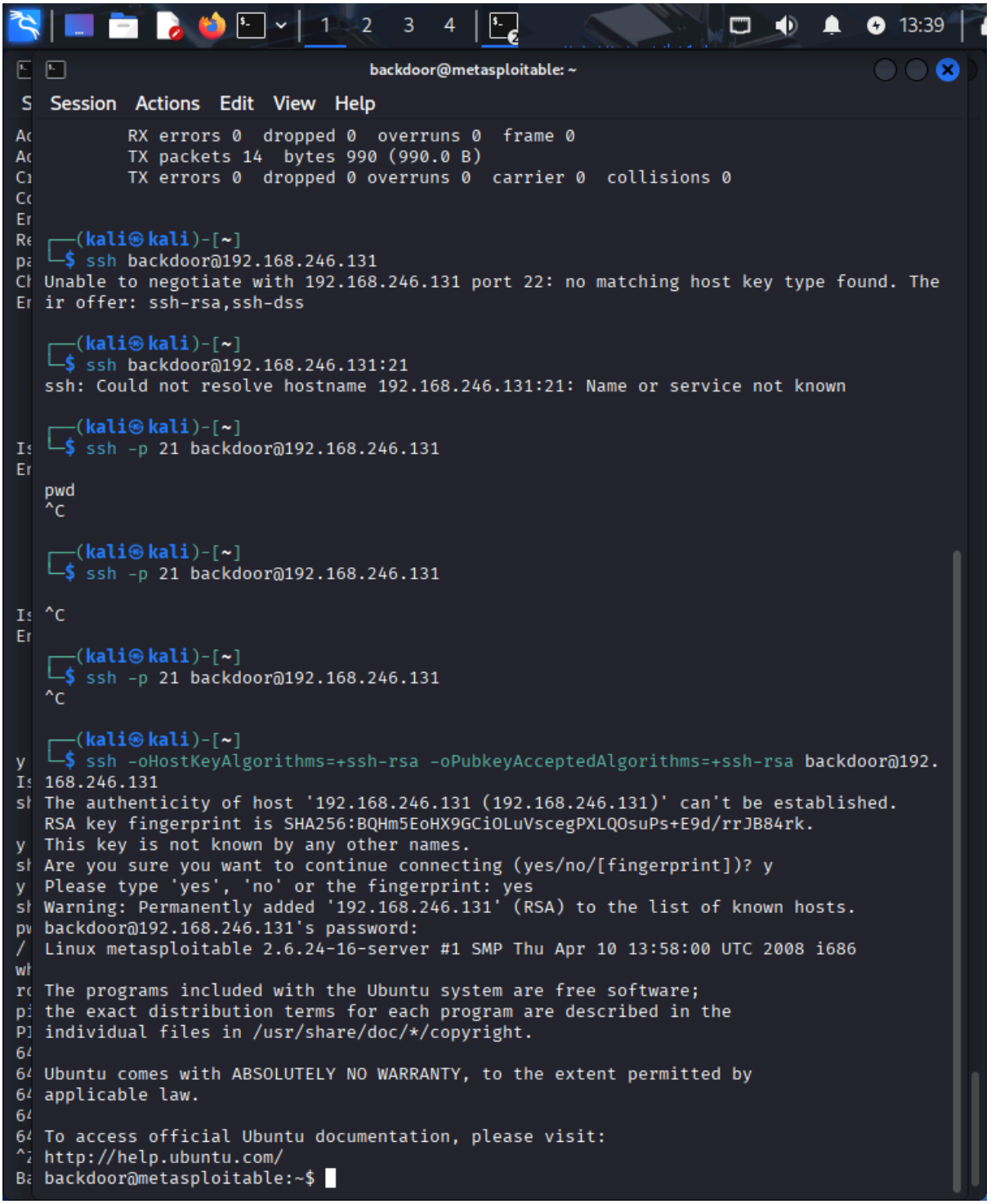
3. Loading & Configuring the Exploit

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.



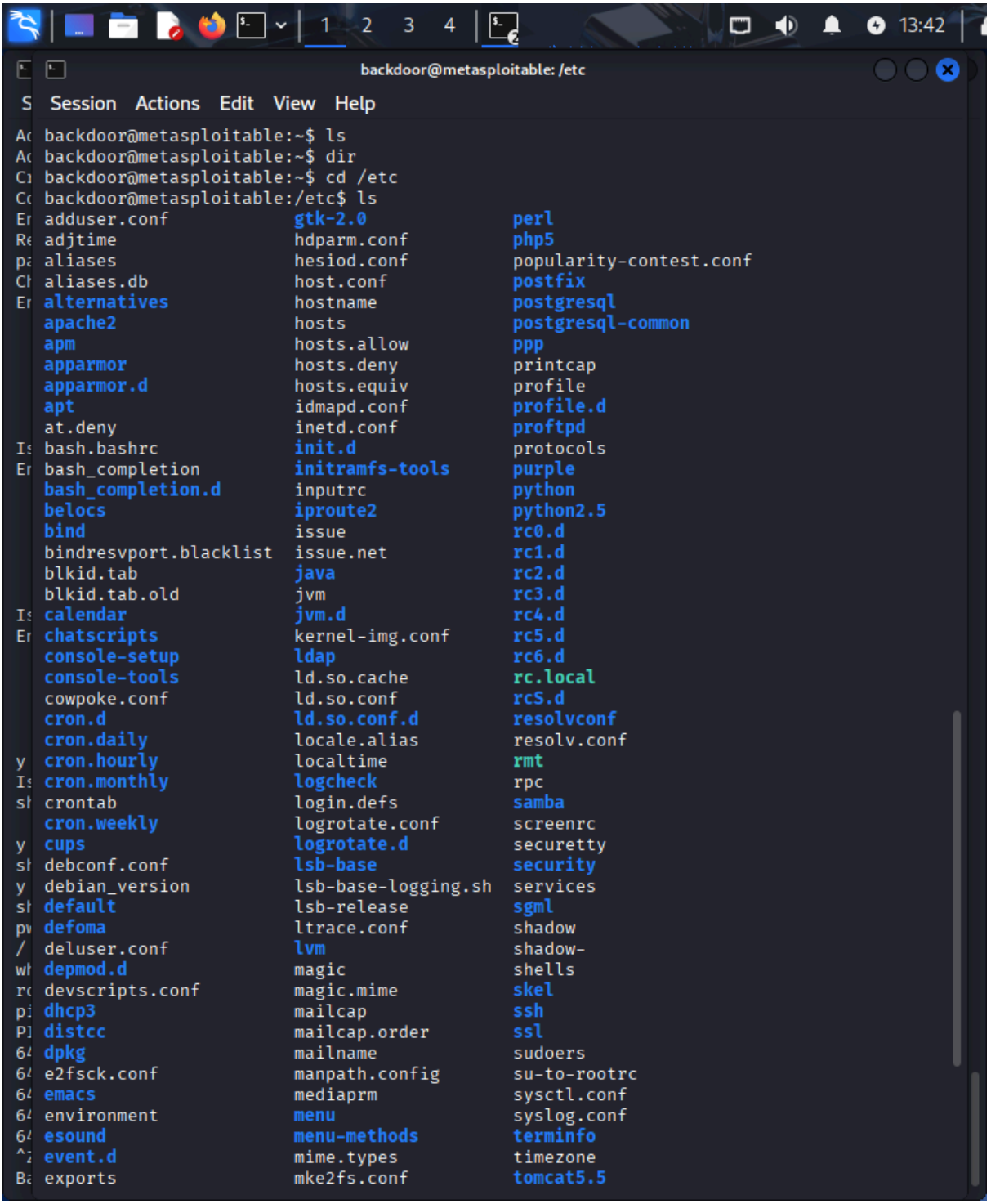
4. Running the Exploit

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.


1 2 3 4
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