Linux Command-line interface

Table of Contents

Last updated: Mon 28 Nov 2022 16:26 IST

Package management

Debian

apt

```
apt install packagename
apt remove packagename
apt purge packagename
apt update
apt upgrade
```

dpkg

```
dpkg -i package.deb
```

Red Hat (RHEL, CentOS, Fedora)

dnf

```
dnf install packagename
dnf remove packagename
dnf update
```

rpm

```
rpm -i package.rpm
```

Arch

pacman

```
pacman -S packagename
pacman -Syu
```

Shell

echo

```
echo -e "line1\nline2" #enable interpretation of backslash escapes
echo -n #do not output trailing newline
echo *.log #print all .log files in dir
```

man

history

Filesystem navigation

pwd

ls

```
ls -R #recursive list
ls -r #reverse order while sorting
ls -S #sort by size
ls -shal #print size, human-readable, all, long listing format
```

tree

```
tree -a -L 1 #tree 1 level all files, says "x directories, y files"
```

cd

Directory and file operations

mkdir

```
mkdir test logs #two seperate dirs
mkdir -p test/logs #create by path, logs subdir (inside) of test dir
```

rmdir

touch

```
touch newfile.txt #creates newfile.txt
touch newfile.txt #if newfile.txt exists: updates time, no overwrite
```

nano

rm

```
rm -r directory/ #recursive dir removal
```

cp

```
cp -R mydir/ destination/ #recursive dir copy
cp -v file.txt destination/ #verbose
```

mv

File reading and manipulation

less

more

```
more -2 file.txt
```

tail

```
tail -n 3 file.txt #last 3 lines
```

head

```
head -n 20 file.txt #first 20 lines
head -c 5k file.txt #first 5k bytes in size
```

cat

```
cat -n file.txt #show line numbers
```

grep

```
grep -r login /var/log/apache2 #recursive
grep -v login /var/log/apache2/access.log #select non-matching lines
grep -R #follow all symlinks
grep -l #print only names of FILEs with selected lines
grep -A 2 #print NUM lines of trailing context
grep -B 3 #print NUM lines of leading context
grep -A 2 -B 2 login /var/log/apache2/access.log #2 lines after, 2 before
```

cut

```
cut -b 5 file.txt #get first 5 bytes in each line
cut -c 2,5,7 file.txt #get chars at 2nd, 5th, 7th place in each line
```

sort

```
sort -n nums.txt #ascending sort
sort -nr nums.txt #descending sort
sort -hr nums.txt #descending sort
sort -nu #numeric unique sort
```

uniq

```
uniq -c nums.txt #unique lines count, requires sorted list
```

watch

find

```
find / -name myfile.txt
```

file

stat

wc

```
wc -c file.txt #byte count
wc -m file.txt #character count
wc -w file.txt #word count
wc -l file.txt #line count
```

Archives and encryption

tar

```
tar -czvf output.tar.gz input-dir/ #create gzip file verbose
tar -xvf file.tar.gz #extract file verbose
```

zip

unzip

```
unzip latest.zip
unzip file.zip -d /path/to/dir
```

mcrypt

```
mcrypt backup.txt
rm backup.txt
mcrypt -d backup.txt.nc
```

Users and groups

adduser

useradd

groupadd

userdel

groupdel

usermod

```
usermod -a -G grpname username
usermod -aG sudo username #add user to sudo group
```

sudo

su

id

whoami

who

w

last

passwd

Permissions, ownership, and groups

chmod

```
chmod +x file.sh #give execution permission
chmod 777 file.sh #give all permissions
```

chown

```
chown userowner:usergrp file.sh #change file owner
```

chgrp

```
chgrp staff /u #change the group of /u to "staff"
chgrp -hR staff /u  #change the group of /u and subfiles to "staff"
```

Processes and system

ps

```
ps -a #show processes for all users
ps -u #display process user/owner
ps -x #show processes not attached to a terminal
```

free

```
free -h #free and used memory (RAM) in system human-readable
```

top

kill

```
kill 12345 #by process ID
kill -9 12345 #force kill by process ID
```

systemctl

```
systemctl reboot #reboot machine
systemctl status sshd #status of ssh daemon service
systemctl stop sshd
systemctl start sshd
systemctl enable sshd
```

service

```
service sshd status #status of ssh daemon service
service sshd stop
service sshd start
service sshd restart
```

reboot

shutdown

```
shutdown -h now #halt, time
```

date

uptime

uname

```
uname -a
```

hostname

locale

dmesg

df

```
df -h #file system space usage human-readable
```

fdisk

```
fdisk -l
fdisk /dev/sdb
```

mkfs

```
mkfs.ext4 /dev/sdb1
```

lsblk

mount

```
mount /dev/sdb1 /media/usb
```

Networking

ping

host

wget

```
wget -O /dev/null http://speedtest.wdc01.softlayer.com/downloads/test100.zip #wget speed test
wget file.sh | sh #download shell script and run it
```

curl

```
curl -o file.tar.gz http://server/file2.tar.gz #Write to file instead of stdout
curl -u username:password ftp://server/
```

traceroute

ifconfig

```
ifconfig eth0
ifconfig eth0 up
ifconfig eth0 down
```

Setting up NIC to use DHCP

```
echo "iface eth0 inet dhcp" >> /etc/network/interfaces
ifconfig eth0 down
ifconfig eth0 up
```

Setting up NIC to use static IP

```
ifconfig eth0 down
```

```
nano /etc/network/interfaces
```

```
iface eth0 inet static
    address 192.168.44.33
    netmask 255.255.255.0
    gateway 192.168.44.2
ifconfig eth0 up
```

ip

```
ip a
```

dhclient

iftop

netstat

```
netstat -at #all tcp
netstat -au #all udp
netstat -p #show process
```

ssh

```
ssh user@host
```

scp

```
scp user@host:/home/user/file.txt destination/
```

nc

See exploitation#nc

```
nc -l -p 4444 #listen for inbound connections, local port
nc 10.8.22.123 4444 #tcp connection to ip and port
nc -lvp 7777 -e /bin/bash
```

Reconnaissance tools

nmap

```
nmap -sn 10.8.22.0/24 #host discovery
nmap -sS -p 1234 10.8.22.0/24 #TCP SYN scan
nmap -sT -p 1234 10.8.22.0/24 #TCP connect scan test connection 3-way-handshake
nmap -sU --top-ports 100 10.8.22.0/24 #UDP scans
nmap -sS -sV 10.8.22.123 #SYN stealth scan, service and version detection
nmap -sS -O 10.8.22.123 #OS detection
nmap -sS -T4 -p 1-1024 10.8.22.123 #timing and performance
nmap -A 10.8.22.123 #OS and version detection, script scanning, traceroute
```

masscan

```
masscan -p0-1024 --interface eth0 172.16.127.0/24
masscan -p -4000 --interface eth0 127.0.0.1
```

whois

theHarvester

```
theHarvester -d google.com -l 300 -b all #domain, limit, source
```

recon-ng

```
help
marketplace info all
marketplace search all
marketplace install recon/domains-hosts/hackertarget
modules load recon/domains-hosts/hackertarget
info
options set SOURCE yahoo.com
run
show hosts
```

sublist3r

```
sublist3r -d google.com #finds subdomains
```

dig

dirsearch

```
dirsearch -u google.com #directory search
```

fping

```
fping -gaq 192.168.1.0/24 #ping connectivity test
```

netdiscover

Metasploit Framework

See exploitation#metasploit-framework

msfdb

```
msfdb init
msfdb start
msfdb stop
```

msfconsole

See exploitation#msfconsole

```
help
search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor
```

msfvenom

See exploitation#msfvenom

```
msfvenom -h
msfvenom -l payloads
msfvenom -l formats
```