

Quick basic commands

cd	change directory, case sensitive (Example: Desktop)
cd	home directory
.	this directory
cd ..	go up one directory
cd -	change dir to previous working dir
pwd	print working directory
ls	list contents, -a all, -h human readable
ll	LL list directories with RW permissions
la	LA list all including hidden
sudo	super user privileges
mkdir <dirname>	create directories
cp <path and locations> .	copy contents to current directory, cp by itself will overwrite files silently
mv <item1> <item2>	move file(s) to location
rm -i <item>	delete file, -i interactive confirmation
alias	lists alias commands
alert <"message">	sends a message to notifications
> emptyDOC.txt	make an empty text file
>	standard out to .txt (will overwrite)
>>	append standard out .txt will (not overwrite)
ls -la /usr/bin	will print the directory contents to a text file
ls-output.txt	

Quick basic commands (cont)

&>	will include output and errors
apt	
apt list	grep Type a word to highlight in red
apt search	grep searchword
apt install	app name
apt remove	app name
apt update	
apt upgrade	

Permissions

id	Display user identity
chmod	Change a file's mode
umask	Set the default file permissions
su	Run a shell as another user
sudo	Execute a command as another user
chown	Change a file's owner
chgrp	Change a file's group ownership
passwd	Change a user's password

Reading, Writing, Executing -rw-r--r--

Example	-rw-r--r--
-	col1. Regular file
d	col1. Directory
l	col1. A symbolic link. Dummy values.
c	col1. A character special file. Modem
b	col1. A block special file. Ex. CD, HDD.
r	Read only
w	Write
x	Executable

iptables (firewall)

iptables -h	list commands
--list	list the rule in a chain or all chains
--verbose or -v	details
--line-numbers	print line numbers when listing
--version or -V	version number
--list-rules or -S	list rules
--numeric or -n	numeric output of addresses and ports

Permission Attribute Examples

-rwx-----	read, write, execute by file's owner only
-rw-----	read and write by owner only
-rw-r--r--	read and write owner, read group, read world
-rwxr-xr-x	read, write, execute owner. read and execute everyone else.
lrwxrwxrwx	A symbolic link with dummy permissions
drwxr-x---	Directory. read, write, execute owner. Read and execute group.

Changing passwords

passwd [user]	with sudo you can change a user password
passwd	change your password

chown

chown [owner][:group] file..	syntax use
bob	change ownership from current to bob
bob:users	change file ownership to bob and group to users

chown (cont)

:admins change group owner to admins, the owner is unchanged

bob: change the current owner to bob and change the group to the login group for bob

text editors

gedit GUI (installed in Ubuntu)

kedit KDE default

kate sudo apt install kate

nano command line based (installed in Ubuntu)

vi or vim vi IMproved (installed in Ubuntu)

emacs sudo apt install emacs-gtk

text editing basics

make a backup cp <filename> <filename.bak>

nano <filename> load a text in nano

nano text editor

^X to quit nano, ^ mean CTRL

^O CTRL-O save the file

vi or vim text editor

vi start vim

vi newdoc.txt create a blank text doc in vi from command line

:q quit

:q! quit without saving

vi starts in command mode press i to go to insert text mode

press ESC to exit insert mode exit insert mode ESC

:w save the file, or write to file

vi or vim text editor (cont)

double tap ESC if you don't know where you are in vi

Navigating Command Mode

H or left arrow left one character

J or down arrow down one line

K or up arrow up one line

L or right arrow right one character

O (zero) go to the beginning of the current line

SHIFT-6 (^) to the first non whitespace character on the current line

SHIFT-4 (\$) to the end on the current line

W to the beginning of the next word, or punctuation characters

SHIFT-W (W) to the beginning of the next word, ignore punctuation characters

B to the beginning of the previous word or character

SHIFT B (B) to the beginning of the previous word or character, ignoring punctuation

CTRL-F or page down down on page

CTRL-B or page up up one page

number-SHIFT-G to the line number, example 1G moves to the first line of the file

SHIFT-G to the last line of the file

Cutting, Copying, Pasting Text

DELETE TEXT aka CUT TEXT

vi or vim text editor (cont)

x delete the current character

3x delete the current character and the 2 after it

dd delete the current line

5dd delete the current line and the next 4 lines

dW delete from the current cursor position to the beginning of the next word

d\$ delete from the current cursor position to the end of the line

dO delete from the current cursor position to the beginning of the line

d^ delete from the current cursor location to the first non whitespace character line

dG from the current line to the end of the file

d20g from the current line to the 20th line of the file

COPYING

yy y stands for yank which is copy, yy copies the current line

vi or vim text editor (cont)

5yy	copies the current line and the next 4 lines
yW	from the cursor location to the beginning of the next word
y\$	from the cursor location to the end of the current line
y0	from the current cursor location to the beginning of the line
y^	from the current cursor location to the first non whitespace character in line
yG	from the current line to the end of the file
y20G	from the current line to the 20th line of the file

PASTING

p	pastesthe current copied text below the current line
P	pastesthe copied text above the current line
Join lines	J
vi has the ability to do search and replace	maybe I will add a cheat sheet for this later
/searchtext	searches vi
:%s/Line/-line/g	will search and replace Line with line globally

EDIT MULTIPLE FILES

vi or vim text editor (cont)

vi file1 file2 file3	
:n	switch to the next file
:N	switch to the previous file
:buffers	lists open files
:buffers 2	switch to buffer file 2
:e	open another file from vi. example :e filename.txt
:r	copy an entire file to the vi session. example :r myfile.txt

Networking commands

ping	send en ICMP echo request to network hosts
tracert	print the route packets trace to a network host
netstat	print the network connections, routing tables, interface stats, masquerade connections, and multi cast memberships
ftp	file transfer program
lftp	an improved ftp
wget	non interactive network downloader
ssh	openSSH SSH client (remote login)
scp	secure copy (remote copy program)
sftp	secure ftp

Technical commands

cat (brings files together, uses input)	CTRL-D to quit, tell cat EOF
cat > sometext.txt; this is some text to be saved	a simple way to add text to a text file

Technical commands (cont)

cat somete-xt.txt	to read the file with cat
	pipe connects input to output
ls /bin /usr/bin sort less	example sort 2 dirs binaries
sort	alphabetize a list
uniq	used with sort, removes duplicates
grep	pattern finding
head	checks the first 10 lines of a file. -n # (to adjust #)
tail	checks the last 10 lines of a file. -n#
tail -f /var/log/messages	-f is a real time log file viewer switch(CTRL-C to quit)
tee	for use with pipe
echo *D	display everything with a capital D
echo \$((2+2))	command line calculator
echo "\$(cal)"	calendar
history	a list of all commands used
history: !88	!88 will use number 88 in history

USB checking

lsusb	list connected USB devices
-------	----------------------------

dpkg

dpkg --list	list all installed packages
-r or --remove	remove a package
-P or --purge	
--log=<filename>	log changes made
-i or --install <.deb file name>	install a deb file

chmod octal chart

octal	binary - filemode
0	000 ---
1	001 --x
2	010 -w-
3	011 -wx
4	100 r--
5	101 r-x
6	110 rw-
7	111 rwx
example setting octal 600	owner, group, world
	binary seems somewhat irrelevant
chmod symbolic notation	
u	user
g	group
o	others, world
a	all
example notation	
u+x	add execute permission for the owner
u-x	remove execute permission from the owner
+x	add execute for everyone, same as a+x
o-rw	remove read and write for everyone but owner and group
u+x,go=rx	add excute for owner, group and world changed to read and execute

umask new file default permissions

umask	0022 ubuntu default
#	4000 sets program ownership to position app
0---	2000 sets group ownership for shared directories

umask new file default permissions (cont)

1000 set to a directory prevents files from being deleted in shared directory

the last three are octal permissions

system stuff

printenv less	system information
printenv	views the contents of a variable, example USER contains your user name
set less	display shell and environment variables
echo \$HOME	echo can be used to view single variables
alias	lists all alias commands
[command]; alert [message]	to get a notification when a command is done(an alias in ubuntu)
below are some variables of interest	**
DISPLAY	the name of your display enviroment
EDITOR	the default text editor
SHELL	name of the shell running
HOME	path to home directory
LANG	keyboard language
OLD_PWD	the previous working directory
PAGER	the name of the program used for paging output. Usually is app less

system stuff (cont)

PATH	a colon separated list of directories that are searched when you enter the name of an executable program
PS1	prompt string 1, defines the contents of shell prompt
PWD	current working directory
TERM	the name of your terminal type
TZ	time zone
USER	your username

Storage Media command overview

mount	mount a file system
umount	un-mount a file system (pay attention to the spelling of the command Umount)
fdisk	partition table manipulator
fsck	check and repair a filesystem
fdformat	format a floppy disk
mkfs	make a filesystem
dd	write block-oriented data directly to a device
geniso-image (mkisofs)	create an ISO 9660 image file
wodim (cdrecord)	write data to an optical storage
md5sum	calculate MD5 checksum

LISTING DEVICES AND FILESYSTEMS

/etc/fstab	is a list of devices
mount	will view a list of mounted filesystems
ls /dev	list devices



By **ralema56**

cheatography.com/ralema56/

Not published yet.

Last updated 15th March, 2019.

Page 4 of 8.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>

Storage Media command overview (cont)

/dev/fd* floppy disks

/dev/hd* hard drives

/dev/lp* printers

/dev/sd* SCSI disks

/dev/sr* Optical drives CD/DVD readers and burners

sudo tail -f to see real time device

/var/log/- changes in the system
syslog

MOVING DEV MOUNT LOCATIONS

sudo mkdir make a dir to mount flash
/mnt/flash drive

sudo moves the location to the new
mount one (use the proper device
/dev/sdb1 name before moving)
/mnt/flash

df display disk space df -h for
human readable

system startup stuff

/etc/p- a global configuration script that
rofile applies to all users

~/.bas- a users personal startup file. can
h_profile override the global config script

~/.bas- if ~/.bash_profile is not found,
h_login bash attempts to read this one

~/.profile if neither bash profile or login
are found this is run. this is the
default in Ubuntu

/etc/b- a global config script that applies
ash/bas to all users
hrc

system startup stuff (cont)

~/.bashrc a users personal
startup file

files that start with a is -a option when
period are hidden searching with ls

fdisk commands

sudo umount unmount the partition
/dev/sdb1

sudo fdisk mount the entire drive
/dev/sdb

fdisk commands

p print partition tables

l list known partition
types

t change a partitions
system id

w write partition changes

q quit fdisk

creating a new filesystem with mkfs

sudo mkfs -t make an ext3 filesystem
ext3 on device sdb1 partition
/dev/sdb1

sudo mkfs -t make a fat32 filesystem
vfat /dev/sdb1 on device sdb1

testing and repairing filesystems with fsck

sudo fsck checks the filesystem on
/dev/sdb1 sdb1 partition

Moving data directly to and from devices with dd

dd raw copy tool (dd
has 2 names, data
definition and destroy
disk)

dd if=input_file syntax to dd raw
of=output_file copy
[bs=block_size
[count=blocks]]

Moving data directly to and from devices with dd (cont)

dd if=/dev/sdb copy 2 identical usb
of=/dev/sdc drives that are the same
size

dd if=/dev/sdb make a raw image of the
of=flash_dri- drive
ve.img

creating CD-ROM images

dd if=/de- copy the contents of a cd to
v/cdrom an image file
of=ubu-
ntu.iso

cdrdao is used for audio cds

creating an iso from a collection of files

genisoimage if you had a directory called
-o cd- /cd-rom-files, you could use
rom.iso -R - this command to make an
J ~/cd-rom-- image of the directory
files

the -R -J the allow the use of long
options filenames
defined

mounting an iso image directly

using the -o loop with mount

mkdir /mnt/i- then the next line down
so_image

mount -t mounts the iso as a virtual
iso9660 -o drive
loop
image.iso
/mnt/iso_ -
image

blanking a RW CD

wodim there are other types of
dev=/d- blanking
ev/cdrw
blank=fast

writing an image file

wodim writes an image to cd
dev=/d-
ev/cdrw
image.iso

MD5 checksum

md5sum image.iso	will give you the md5 checksum value
md5sum /dev/cdrom	a cd-r write in disc at once can be checked like this

lynis (auditing,hardening)

sudo apt install lynis	install it
lynis audit system	perform local security scan
lynis show version	version
--verbose	details
--pentest	non privileged scan

systemctl (services)

systemctl -all or -a	see all loaded processes
list-units	list units currently in memory
list-sockets	list sockets currently in memory
list-unit-files	list installed unit files
poweroff	turn the computer off
reboot	shutdown and restart
is-system-running	checks to see if the system is running
--type service --state running	searching for running services

ps (running processes)

ps -e	all running processes
ps aux grep telnet	search for telnet running
ps #####	# = number for PID to view
ps -aux	custom running process search
ps --help all	list more commands
ps	report a snapshot of the current running processes

ps (running processes) (cont)

top	display tasks with the top active ones
jobs	list active jobs
bg	place a job in the background
fg	place a job in the foreground
kill	send a signal to a process via PID
killall	kill process by name
shutdown	shut down or reboot the system
xlogo	creates a nonsense xlogo app for debugging and testing ps controls
[CTRL-c]	terminates programs started in terminal
xlogo &	& will make a program start in the background
fg %1	will bring the program to the foreground
[CTRL-z]	stops or pauses a process
bg %1	put program in background
killall [process name]	killall xlogo for example if multiples are running
pstree	outputs a process list in a tree pattern
vmstat	system resource snapshot [vmstat5] for continuous feed
xload	GUI draws a graph, showing sys stats overtime
tload	a terminal version of xload
tload	a terminal version of xload

netstat

netstat	-tulpn
-l (L)	display listening sockets
-n	don't resolve names
-p	display PID
-s	an overview - statistics
-g	group memberships
-r	router table
-i	interface table

Customizing the Prompt

adjust how the prompt is displayed and operates

echo \$PS1	display the current prompt setup
ps1_old="PS1"	make a backup before making changes called ps1_old. check with echo \$ps1_old
PS1="\$ps1_old"	restore the original
PS1=	clear all prompt data (no visible prompt)
PROMPT VALUES	ubuntu default value is: [u@h \W]\$
PS1="\\$ "	a minimal prompt
\a	ASCII bell. Makes the computer beep
\d	current date in day, month, date format
\h	hostname of the local machine minus the domain
\H	full hostname
\j	number of jobs in the current shell
\l	name of the current terminal device
\n	a newline character
\r	a carriage return
\s	name of the shell program
\t	current time in 24hour H:M:S
\T	current time in 12hour format

Customizing the Prompt (cont)

\@	current time in 12hour am/pm format
\A	current time in 24 hour H:M
\u	username of the current user
\v	version number of the shell
\V	version and release number of the shell
\w	name of the current working directory
\W	last part of the working directory
\!	history number of the current command
\#	number of commands entered in shell
\\$	displays the \$ character unless you have root, in that case it displays #
\[the start of a series of one or more non-printing characters
\]	the end of a non-printing character sequence

COLOR TEXT

\033[0;30m	black
\033[0;31m	red
\033[0;32m	green
\033[0;33m	brown
\033[0;34m	blue
\033[0;35m	purple
\033[0;36m	cyan
\033[0;37m	light grey
\033[1;30m	dark grey
\033[1;31m	light red
\033[1;32m	light green
\033[1;33m	yellow
\033[1;34m	light blue
\033[1;35m	light purple
\033[1;36m	light cyan

Customizing the Prompt (cont)

\033[1;37m	white
BACKGROUND COLOR	
\033[0;40m	black
\033[0;41m	red
\033[0;42m	green
\033[0;43m	brown
\033[0;44m	blue
\033[0;45m	purple
\033[0;46m	cyan
\033[0;47m	light gray

Searching for files commands

locate	find files by name
find	search for files in directory hierarchy
xargs	build and execute command lines from standard input
touch	change file times
stat	display file or filesystem status

locate (find files the easy way)

locate	locate will search for any string
bin/zip	with bin and zip
locate zip	and fancier search
grep bin	

find (find files the hard way)

find ~	a list of directories in our home dir
find ~ wc -l	use word count to find how many files
find ~ -type d wc -l	find how many directories with word count
find ~ -type f wc -l	find regular files with word count

Searching for files commands (cont)

find ~ type f	find files with the name .jpg
-name "*.J-PG" -size +1M wc -l	larger than 1 mb and count them

find test

-cmin n	match files of dirs whose content was modified exactly n minutes ago
-cnewer file	match files or directories whose content was last modified more recently than the file named
-ctime	match files or dirs that were modified within the last 24hours
-empty	match empty files or dirs
-group name	match files or dirs belonging to a group
-iname pattern	like name but case sensitive pattern
-inum n	match files with inode number n
-mmin n	match files of dir whose contents were modified n mins ago
-mtime n	match files or dirs whose contents were modified n 24 hours ago
-name pattern	match files with wildcard pattern
-newer file	match files or dirs whose content was modified more recently than specified file

Searching for files commands (cont)

-nouser match files or dirs that do not belong to a user

-nogroup match files that do not belong to a group

-perm mode match files that have permission set to a specific mode

-samefile match files with the same name
inode number, similar to -inum test

-size n match file of size n

-type c match files of c type

-user name match files or dir belonging to user name

find logical operators

-and match if both sides are true, also known as -a

-or match if one side is true also known as -o

-not match if the following test is false, also known as -!

() group tests together to form larger expressions

examples

-type f -and testing for bad permissions
-not -perms 0600 by testing for good ones

Searching for files commands (cont)

find ~ (-type f -not -perms 0600) -or (-type d -not -perms 0700) test for bad files and directories

actions for find

-delete delete the currently matching file(see warning)

-ls perform the equivalent of ls -dils on the matching file.

-print output the full pathname of the file

-print0 used to correctly print file names with spaces

-quit quit once a match has been made

warning for delete

always use -print as a substitute for -delete to see what will be deleted

find ~ -type f -name '*.BAK' -print -print the files to output before deleting

find ~ -type f -name '*.BAK' -delete then proceed if you wish to delete still

