Common Linux Commands

Command	Meaning	What it does
ls	listing	List files in directory
cd dirname	change dir	Change directory to dirname
cd ..		Go back one directory (the parent directory)
pwd	present working dir	Shows you what directory are you in
cat filename	concatenate	Print the contents of the file to the screen (don't do this with binary files, zips, etc)
cat file1 file2 file3		Prints all the files back to back like they were single file, they are concatenated together
less filename	less	Print the contents of a file, but you can PgDown/PgUp to read a large file
gedit filename	Gnome Edit	Open text editor gedit (easy to use) to edit file (only good for ASCII / text files)
nano filename	Small Editor	Text editor, command line (not a GUI), easy to use
vi filename	Visual Edit	Text editor. NOT EASY TO USE! If something tells you to use vi, try using gedit or nano instead!
rm filename	Remove	Remove a file
mv filenameold fnnew	Move	Moves / Renames a file from old name to new name (there is no rename command in Linux)
cp src dest	Copy	Copies a file from source location to destination location
mkdir dirname	Make dir	Makes a directory
rmdir dirname	Remove dir	Removes a directory (must be empty)
rm -rf listoffiles	rm recursive	Removes files / directories recursively, with force (ignore permissions / warnings if possible)
whoami	Who am I	Tells you what username is currenty on system
which command	Which	Tells you the full path of a command
basename path [-s .ext]	Basename	Strips path and extensions of a filename
history	History	Lists previous commands run
touch filename	Touch	Creates an empty file with the given name
man command	Manual	Shows manual page about the command, shows you the options, similar commands
man -k topic		Searches for man pages pertaining to topic (see below)
reset	Reset	If you terminal is acting weird, try reset to fix it
exit	Exit	Exit shell (logout of server)
head [filename]	Head	List the first few lines of a file (or stdin)
sort [filename]	Sort	Sorts file (or stdin) line by line
uniq [filename]	Unique	Removes CONSECUTIVE redundant lines from a file
wc [filename]	Word Count	Counts number of words in a file (or stdin)
tail [filename]	Tail	List the last few lines of a file (or stdin)
tee filename	Tee (pipe)	Writes the standard output piped into command into a file, while displaying the output
base64 [filename]	Base 64	Converts files (including binary) to / from simple ASCII text
rot13	rotate 13	Rotates characters in string +13 chars. A->N, B->O
file	File	Tells you what type of file something is (based on file signatures, can be tricked)
df	Disk free	Lists disc drives mounted, and how much free space
du	Disk usage	Lists how much space is being used by files
watch [command]	Watch	Run (watch) a command over and over (every 2s)
!!	last cmd	Run last command again
~	Home	Home directory (/home/username)
*	Splat, Star	Matches all files in a directory, *.txt is all files ending in .txt
?		Matches all files with any char, ex: ls part??.bin matches part09.bin, but not part1.bin

Process Management

Command	Meaning	What it does
kill [-9] pid	Kill	Kills a running process (-9 is KILL signal, which is sometimes required)
killall processname	Kill All	Kills all processes with the given name ex: killall chrome\
top	Top	Lists processes running (interactive)
htop	H Top	Fancier version of top (bar graphs, easy sorting)
ps [aux]	Process List	Dumps list of running processes
pstree	ps tree	Lists all process in tree format (see which process started others)

Files / permissions

Command	Meaning	What it does
ll	long list	List file, file length, and file permissions (ls -l)
sudo command	Superuser do	Runs the command as root user (administration commands). Requires sudo permissions
chmod permissions filename	Channge mode	Changes read (+r), write (+w), execute (+x), or sticky bits (+s) for a file. a=all, u=user, g=group, o=other
chown user:group filename	Change owner	Changes who owns a file

```
ls -l                          # Lists type of file, rwx for user, rwx for group, rwx for other, owner, group, length, etc
chmod a+rx filenames           # All user can read / execute
                               # Dirs need execute permission to cd into
chmod 744 filename             # Set permission with octal (for rwx bits)
```

Searching / investigation

Command	What it does
file	Determines what the file is based on sig / magic bytes
grep needle [filenames]	Searches for needle in the list of files (or stdin)
find	Find files. Has insane amount of options
binwalk	Looks all through a file to find file signatures / hidden files. Many false positives!
lsof	List open files on the system
strings	Shows all ASCII strings contained in a binary that are atleast 5 chars long
hexdump -C [filename]	Shows hexdump of a file next to ASCII representation
xxd	Similar to hexdump, can also convert hex to binary (be careful of endianness)

Image / Stegenography tools

Command	What it does
exiftool [filename]	Shows the EXIF / metadata for an image
steghide info [filename]	Will seach for steg information in the file

Find examples

```
# Find files accessed 10 days ago
find ./ -atime 10

# Find directories created in your home folder in the last 2 hours
find ~ -type d -cmin -120

# Delete all files over 100MB that have name starting with tmp
find ./ -type f -name "tmp*" -size +100M -exec rm {} \;
```

Compression Tools

Command	Compress	Extract	Notes
zip	zip filename.zip -r dir	unzip filename.zip	Compatible with windows
tar	tar -cvf filname dir	tar -xvf filename	Tape ARchive
gzip	gzip filename	gunzip filename	.gz extension (very common, fast)
bzip2	bzip2 filename	bunzip2 filename	.bz or .bz2 extension (slower, but better compression)
rar	rar a filename dir	rar x filename	.rar (compatible with WinRAR)
tar / gzip	tar -czvf filename dir	tar -xzvf filename	Combines tar (many files to single file) and gzip (compression) .tar.gz or .tgz extension
tar / bzip2	tar -cjvf filename dir	tar -xjvf filename	Combines tar (many files to single file) and bzip2 (compression) .tar.bz2 or .tbz

Networking

Command	Meaning	What it does
ip addr show	ip	Lists IP address of interfaces (NIC card, wifi, virtual interfaces for VMs)
ifconfig	interface config	Old version of ip addr show
ping [ip/host]	ping	Sends ICMP packet, waits for response. Is this server online?

netstat -ant	network status	Lists all current network connections
netstat -lnp		Lists all listening connections
nmap	network map	Lists devices / ports on network. Be very careful, don't use at school!
nc	net cat	Connects to a TCP port on a devices to send / receive text (no authentication / encryption)
socat	stream cat	Fancier (more complicated) version of netcat
wget [url]	www get	Download file from internet
curl	client url	Transfer data from a server (many uses, search for usages on web)
wireshark	Wireshark	Capture (or view) network traffice (pcap files)
tcpdump	TCP dump	Command line tool to create pcaps

Commands for system maintenance

Command	Purpose
adduser username	Adds a user to the system
deluser username	Deletes a user from the system
addgroup groupname	Adds a group to the sytem
adduser username groupname	Adds an existing user to the group
passwd	Change your password
passwd username	Changes the password of another user (must run as root)
sudo command	Runs the command as root (if the current user has sudo privledges)
sudo -i	Create a root shell (don't need to sudo every root command / worry about passwords). BE CAREFUL WITH THIS.
exit	Exit shell (exit root shell if you started a root shell)

Other tools

sed is stream editor

```
sed s/oldstring/newstring [filename]
```

Sed can search and replace in a file

```
sed -i 's/oldstring/newstring/g' filename
```

cut can take output and filter certain columns

```
# Show only columns (comma separated) 2, 5, and 7 from document
cat document | cut -d ',' -f 2,5,7
```

tr and awk are advanced tools for editting files from the command line, but are to complex for this cheatsheet.

Package Manager (Ubuntu and Debian)

Thousands of free open-source tools are available to install on Ubuntu through the package manager. You can only run one package manager software at a time, but you can usually do other things while packages are installing or udpating.

```
sudo apt-get update   # Updates repository, cache of package list.  Do this first before everything else
```

Search for packages using synaptic (GUI package browser) or

```
apt-cache search keyword
```

Install a package via synaptic or from command line:

```
sudo apt install package1 [package2 package3 etc]
```

To update system with latest patches / security updates (not neccessarily latest version). This could take a long time, prevent you from installing a package needed for another challenge, so be careful...

```
sudo apt-get upgrade
sudo apt-get dist-upgrade
```

Command	Purpose
dpkg -i filename.pkg	Install a single package
dpkg -l	Lists all installed packages
dpkg -S filepath	Shows which package file came from

sudo apt remove pkgname Removes package from system

Useful packages to add to a system

Package	Purpose
synaptic	GUI package manager / browser
vlc, smplayer	Media players
audacity	Audio editor / visualizer
gimp, kolourpaint	Photo editting
libreoffice	Producity tools (documents, spreadsheet, presentations)
okular	PDF viewer (fast, handles larged PDFs)
gedit, geany	Simple / minimal text editors
ghex	Hex editor
wireshark	Network capture
binwalk	Detects files based on signature / magic bytes
gcc, g++	C and C++ compiler
git	Version control
forensics-full	Metapackage that includes 100+ forensic tools
guake	terminal that pops down from top of screen via F12
openssh-server	SSH server (allows you to remotely connect to system)
remmina	RDP client (connecting to Windows machines)
vmplayer	Emulation / Install other OS

man (Manual)

Sometimes a single command / topic will have many different manual pages. For example, if you search for printf

```
man -k printf
printf (1)           - format and print data
printf (3)           - formatted output conversion
```

The number in parens is the "page". Page 1 for printf is the printf shell command. Page 3 printf is the printf command from C/C++. There are man instances where a single topic has more than 1 man page. Press Q to quit

Useful man pages

- man ascii: shows you the ASCII table

Pipes

You can send the output of 1 command into a second command. Unix/Linux philososphy is to have many simple commands or applications that do 1 simple task. But the user can combine them using pipes for much more powerful uses.

```
netstat -lp | less
ls | grep jpg
find . -name "*secret*" -exec md5sum {} \; | tee logfile.txt
```

The output of netstat would only be shown 1 page at a time because less paginates the output.
The ls command would only show files/dirs that have jpg in them because grep is searching for jpg in output of ls

Shell Notes

- Directories or files that start with a dot / period are hidden. You must use ls with the -a switch to see hidden files
- If your shell changes prompt, you may have started an unterminated quote or something, press ctrl-c to cancel command
- If a command is taking forever, ctrl-c to cancel command
- If shell acting weird, or changes to unreadable text, you can try reset command to fix, else just close terminal and start new one