

Expansion

<code>ls \$(which cp)</code>	Command expansion
<code>ls `which cp`</code>	Command expansion
<code>mkdir {2017...2-020}-{01-12}</code>	Brace expansion
<code>echo text ~/.*.txt</code>	Variable expansion
<code>{a,b} \$USER</code>	Variable expansion
<code>echo "text ~/.*.txt"</code>	" expansion
<code>{a,b} \$USER"</code>	" expansion
<code>echo 'text ~/.*.txt'</code>	' expansion
<code>{a,b} \$USER'</code>	(NONE)

Redirection & Commands

<code>ls > file.txt</code>	Standard Out
<code>ls 2> file.txt</code>	Standard Error
<code>ls > file.txt 2>&1</code>	Standard Out & Error
<code>ls &> file.txt</code>	Standard Out & Error
<code>ls tee file wc -l</code>	Read stdin & writes stdout
<code>cmd1 ; cmd2</code>	Run cmd1 then cmd2
<code>cmd1 && cmd2</code>	Run cmd2 if cmd1 is OK
<code>cmd1 cmd2</code>	Run cmd2 if cmd1 is KO

su / sudo

```
su [-l] [user]
| Become another user, ROOT by default. If
| - or -l, load user envs and working dir.

su [user] -c 'command'
| Execute command as user. Default
| root

sudo [-u user] command
| Execute command as user. Default
| root

sudo -ll
| Which commands I'm allowed to execute
```

```
visudo
| Edit /etc/sudoers file. Example
| teralco ALL=(root) NOPASSWD:
| /etc/init.d/jboss
| teralco ALL=(jboss) NOPASSWD:
| /bin/kill
```

UFW

```
ufw status [verbose|numbered]
| Show status and rules
```

```
ufw default deny incoming
ufw default allow outgoing
| Deny all incoming traffic by default
| Allow all outgoing traffic by default
```

```
ufw [allow|deny] from IP to
[any|interface_name] [proto
tcp|udp] port PORT
| Full allow/deny rule
```

```
ufw [allow|deny] service_name
| Allow/deny a service (ssh www ftp
...)
```

```
ufw [enable|disable]
```

```
ufw delete [rule|number]
```

Alt commands

```
/var/log/messages & /var/log/-
syslog
```

```
| System log files
```

```
script file
```

```
| Record session commands in file
```

```
nohup command &
```

```
| Keep command running even after close
session
```

```
tar -Jxvf file.tar.xz [-C
dest_folder]
```

```
| Extract xz (higher compress ratio)
```

```
zip -FF x.zip --out Y.zip &&
unzip Y.zip
```

```
| Merge zip files (x.zip, x.z01, x.z02)
```

```
ps aux --sort -rss
```

```
| Higher memory consumption processes
```

```
fdisk -l
```

```
| List partition tables
```

```
dd bs=4M if=input.iso of=/de-
v/sd? conv=fdatasync
```

```
| Burn iso in device
```

Searches

```
find path -name *.log -type f -
mtime +5 -exec rm -rvf {} \;
```

```
| Find and delete files older than 5 days
```

```
find path -type f -printf "%s-
\t%p\n" | sort -rn | head -10
```

```
| Find the 10 biggest files
```

```
grep -rli 'pattern' path
```

```
| Find files with pattern content
```

```
du -cks path/* | sort -rn | head
-10
```

```
| Find biggest dirs
```



By **culebrino**

cheatography.com/culebrino/

Published 4th May, 2020.

Last updated 4th May, 2020.

Page 1 of 2.

Sponsored by **CrosswordCheats.com**

Learn to solve cryptic crosswords!

<http://crosswordcheats.com>

Searches (cont)

du -sh path

Dir size

Permissions

chmod [u|g|o] [+|-|=] [rwx]
dir_file

Change permissions

chmod u[+|-]s file

Set uid. File is always exec as owner user

chmod g[+|-]s dir

Set gid. New files in folder are always owned by folder owner

chmod [+|-]t dir

Sticky Bit. Files in dir can only be renamed or removed by owner or root

umask xxxx

Set default permissions to dirs

Enviroment

/etc/profile Global env config files

/etc/bash.bashrc User env config file

printenv Print defined env vars

alias Show defined aliases

export VAR Make a VAR available to child process

source script Load a file into current script or shell session

. script

Network

ip addr

Show ips

ifup | **ifdown** interface_name

Up or down an interface

/etc/network/interfaces

File interfaces are defined

hostnamectl [set-hostname hostname]

Manage hostname (/etc/hostname) without restarting

netstat -tuln

All tcp and udp listening ports

ss -tuln

All tcp and udp listening ports

nc -vz host port

Scan port in host

SSH

ssh-keygen [-f /etc/ssh/ssh_host_rsa_key] -t rsa -b 4096

Generate ssh rsa key. By default ~/.ssh/id_rsa

ssh-copy-id [-i ~/.ssh/mykey] user@host

Copy ssh key in remote host (~/.ssh/authorized_keys). By default ~/.ssh/id_rsa.

ssh user@host command

Exec command in host

ssh -J hostA hostB

Connect to hostB through hostA (Jumping). Identification in localhost. Can use **ProxyJump** in ~/.ssh/config

SSH (cont)

ssh -D port -fCqN user@host

Proxy socket (HTTP and HTTPS traffic) through port.

ssh -nNT -L 9000:remote_server:80 user@host

Tunneling (Local port forwarding). Map remote_server:80 into localhost:9000 through host

ssh -nNT -R 9000:localhost:3000 user@host

Tunneling (Remote port forwarding). Map localhost:3000 into host:-9000



By **culebrinoo**

cheatography.com/culebrinoo/

Published 4th May, 2020.

Last updated 4th May, 2020.

Page 2 of 2.

Sponsored by **CrosswordCheats.com**

Learn to solve cryptic crosswords!

<http://crosswordcheats.com>