Intermediate Linux

jens::link

$whoami

- Freelance Consultant
- started Linux when it shipped on 35 3.5" disks
- 1st IPv6 presentation in 2007
- 1st large IPv6 project in 2012
- Besides IPv6: networking, automation, monitoring

Intro

Rules

- YMMV - Your Milage May Vary
- TMTOWTDI - There is More Then One Way To Do IT

Structure

- sometimes I'll mention alternative tools
- brief example
- every couple of slide you get some time to play with the tools
- you'll be missing a lot of tools

Notes

- Tools should all work on Linux, MacOS and WSL
- Note: WSL 2 does not work with IPv6 (out of the box)
- not all tools are available via your distributions package manager
- $ - normal user
- # - root

RTFM

- Read the fine|f**king manual
- There is a book by a Spanish guy called Manual. You should read it.
- At least on Debian: A command without a decent man page is considered a bug

```
$ man man
```

- Also for GNU commands:

```
$ info
```

First things first

- If you want to document your terminal session use the *script* command

```
$ script [file]
```

- If you want animations: https://asciinema.org/

bash vs zsh

- On Linux you will most likely have a bash as default
- On MacOS zsh is the default
- I will use bash, but everything should work on zsh as well
- If you want to dive really deep into the working with the shell learn zsh

history

- Your shell keeps a history
- stored in .bash_history
- Use the up arrow to scroll to previous commands
- Use !<number> to select command <number> from bash history
- Use CTRL-R and start typing to search your history
- If you don't want a command in the history add a " " in front
- Note: Some distribution delete the history after lockout

```
$ history
```

Keyboard shortcuts

- CTRL-L - clear (the screen)
- CTRL-R - search history
- CTRL-W - one word back

Making you shell look nicer

- liquidpromt

  Liquid Prompt gives you a nicely displayed prompt with useful information when you need it.

deprecated commands on Linux

- ifconfig - replaced by ip
- route - replaced by ip
- arp - replaced by ip
- netstat - replaced by ss

ip

- Not only for ip

```
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | address | addrlabel | route | rule |
                   neigh | ntable | tunnel | tuntap | maddress |
                   mroute | mrule | monitor | xfrm | netns |
                   l2tp | fou | macsec | tcp_metrics | token |
                   netconf | ila | vrf | sr | nexthop }
```

Define your own commands

- alias

```
alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l='ls -CF'
alias la='ls -A'
alias ll='ls -alF'
alias ls='ls --color=auto'
alias ls='ip --color=auto'
```

How long is a command running?

```
$ time tar -xf linux-6.11.8.tar.xz

real    0m11.749s
user    0m10.281s
sys     0m4.801s
```

Run a program every n second

```
$ watch -n 60 ls
```

Speaking of time

```
$ date
$ alias TS=date "+%Y%m%d%H%M"
```

Command substitution

- Use the output of an command

```
$ touch $(TS)
$ ls
202411151557
```

sudo

- *sudo -s* - get a root shell
- *sudo -i* - get root login

Configure your editor

- Take some time to configure your editor
- If your using Ansible integrate *ansible-lint* and *yamlint*
- for shell scripting: *shellcheck*
- There are many more tools and checks

ssh

- ssh is probably the most used tools
- it has more to offer then just logging into other hosts

ssh config

```
cat ~/.ssh/config
Host *.example.com
    ProxyJump jump.example.net
    USER    jlink
```

ssh-keys

- DO NOT USE PASSWORDS
- can be used to run only certain commands
- you can have multiple keys
- protect your key with a passphrase
- use ssh-agent so you don't have to enter your passphrase everytime
- be careful which algorithm you use, the remote system also needs to support it (looking at Cisco)

ssh jump server

- ssh -J
- ssh -A

ssh socks proxy

```
$ ssh -D 1234 -q -C -N www.example.com
```

- Firefox: foxyproxy or manual configuration

screen / tmux

- tmux — terminal multiplexer
- screen - screen manager with VT100/ANSI terminal emulation

mosh

- mosh - mobile shell with roaming and intelligent local echo
- Important if you travel by train ;-)

serial console

- screen
- minicom
- picoterm
- ser2net

```
$ screen /dev/ttyUSB0 TD
```

The Web

- wget - download files
- curl
- w3m / lynx - shell web browser

Measuring time with curl:

```
$ curl -w '%{time_namelookup}\n%{time_connect}' www.example.com
```

git

- Tip: tig
- Tipp: Clone to a directory .git

```
for i in *.git
do
  cd $i
  git pull
  cd ..
done
```

grepcidr

- grepcidr — Filter IPv4 and IPv6 addresses matching CIDR patterns

working with (log) files

- grep
- sort
- uniq
- wc

Working with json / csv

- jq - jq is like sed for JSON data
- mlr - Miller is like awk, sed, cut, join, and sort for data formats such as CSV, TSV, JSON, JSON Lines, and positionally-indexed

Networking

aggregate

- aggregate6 will aggregate an unsorted list of IP prefixes (both IPv4 and IPv6)

small demo (I)

```
$ wget https://ip-ranges.amazonaws.com/ip-ranges.json
$ jq '.prefixes[] | select(.region=="eu-west-1")'  < ip-ranges.j
```

small demo (II)

```
$ jq '.prefixes[] | select(.region=="eu-west-1")'  < ip-ranges.j
```

jens::link

small demo (III)

```
$ jq '.prefixes[] | select(.region=="eu-west-1")'  < ip-ranges.j
```

jens::link

sipcalc

- sipcalc - IP subnet calculator

iptraf

- iptraf - Interactive Colorful IP LAN Monitor

DNS

- dig
- host
- drill
- zonemater

traceroute and co.

- traceroute
- tracepath
- mtr

testssl.sh

- https://www.testssl.sh

tcpdump & co

- tcpdump
- tshark
- sshdump - Provide interfaces to capture from a remote host through SSH using a remote capture binary.

Misc

- lynis
- etckeeper
- make

The End

jens::link