Information:

Общие команды Linux:
https://novall.net/linux/samye-nuzhnye-i-poleznye-ssh-komandy-linux.html
IP - курс из 10 уроков:
https://proglib.io/p/ip-networks

Exercises:

In blue : a command (в качестве ответа нужно записать команду)

In green : a command output (в качестве ответа нужно записать вывод команды)

In red : a deduction, written in your own words (ответ своими словами)

Network

1. Get the list of the network interfaces of the machine without displaying any detail for these interfaces. Only the list of names.

Выведите список интерфейсов вашей машины без выведения детальной информации по этим интерфейсам. Только названия

Only IP-addresses: Вывести только IP адреса:
ifconfig | grep -o -E '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' 127.0.0.1 192.168.2*.1*2 192.168.3*.255
Only our IP: Вывести только наш IP адрес:
ifconfig | grep "inet " | grep -v 127.0.0.1 | cut -d\ -f2 192.168.2*.1*2
Only interfaces:

Только интерфейсы:

Default sort:
Без сортировки:

```
ifconfig | awk 'BEGIN{FS="\t"; OFS="\n"} {print $1}' | awk 'BEGIN{FS=":";OFS=",";
ORS="\n"} {if ($1 != NULL) print $1}'

lo0
gif0
stf0
en0
en1
en2
en3
p2p0
awdl0
bridge0
utun0
```

Ascii sort:
С сортировкой по аски:

```
ifconfig | awk 'BEGIN{FS=":"; OFS="\n"} {print $1}' | awk 'BEGIN{FS="\t"; OFS=" "} {print
$1}' | sort -n | sed '1,46d'

awdl0
bridge0
en0
en1
en2
en3
gif0
lo0
p2p0
stf0
utun0
```

Ifconfig flag:
Встроенный ifconfig флаг:

```
ifconfig -l

lo0 gif0 stf0 en0 en1 en2 en3 p2p0 awdl0 bridge0 utun0
```

2. Identify and display the Ethernet interface characteristics:
Покажите список характеристик интерфейса Ethernet
(a) Identify broadcast address (широковещательный адрес)

(b) Identify all IP adresses which are part of the same subnet (все IP адреса, которые входят в ту же подсеть)

a) ifconfig | grep broadcast | grep -o -E '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[255]{1,3}'

Where:
flag E is for extended pattern
Рассматривает ОБРАЗЕЦ как расширенное регулярное выражение.

o is for only matching
Возвращает не всю строку, где найдено соответствие ОБРАЗЦУ, а только совпадающую с ОБРАЗЦОМ часть строки.

192.168.3*.255

Broadcast and other info about IP addresses (широковещательный и иное про IP адреса):
https://habr.com/ru/post/129664/

b) ipconfig getifaddr en0
ifconfig | grep "inet " | grep -v 127.0.0.1 | cut -d\ -f2

192.168.2*.1*2

BUT can also be needed (может быть нужным):

"arp -la" saves all the addresses, that is the protocol that saves all the addresses during last 5 min
ARP (англ. Address Resolution Protocol — протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения MAC-адреса по IP-адресу другого компьютера.

ping -c 2 [your broadcast] - 2 packages to your broadcast address (кидаем 2 пакета на широковещательный адрес)
arp -a | cut -d\(-f2 | cut -d\) -f1

192.168.28.11
192.168.28.12
192.168.28.14
192.168.28.16
192.168.28.18
192.168.28.20
192.168.28.21
192.168.28.22
192.168.28.23

192.168.28.25
192.168.28.26
192.168.28.27
192.168.28.28
192.168.28.29
192.168.28.32
192.168.28.33
192.168.28.34
192.168.28.36
…
192.168.31.137
192.168.31.138
192.168.31.139
192.168.31.141
192.168.31.142
192.168.31.143
192.168.31.144
192.168.31.255

3. Identify the MAC address of the Wi-Fi card
Выявите MAC адрес сетевой карты или Wi-Fi адаптера

ifconfig en1 | grep -w "ether" | awk '{print $2}'
ifconfig en1 | grep "ether" | cut -d " " -f2

14:20:5e:0b:8c:**

4. Identifiy the default gateway in the routing table
Показать, куда по дефолту уходят пакеты, в таблице маршрутизации

netstat -rn | grep default | grep en0

default 192.168.30.1 UGSc 30 0 en0

IP address of our router is different from our MAC IP, first IP in our net is the router as the access point, lasts with .1 or .100
Первый IP в нашей сети - роутер как точка доступа, заканчивается на .1 или .100.

These are typically en0 and en1, though the port interfaces will vary slightly with Macs that don’t include ethernet ports or Wi-Fi / AirPort wireless card, and for Macs with only one form of network connectivity it will almost always be en0, though it varies per machine and per hardware.

5. Identify the IP address of the DNS that responds to the following url: slash16.org
Показать IP адрес DNS, который относится к url slash16.org

DNS: https://habr.com/ru/post/303446/

host [name] - to find the IP address of A-type

slash.org has address 162.255.119.96
slash.org mail is handled by 5 alt1.aspmx.l.google.com.
slash.org mail is handled by 10 aspmx3.googlemail.com.
slash.org mail is handled by 1 aspmx.l.google.com.
slash.org mail is handled by 10 aspmx2.googlemail.com.
slash.org mail is handled by 5 alt2.aspmx.l.google.com.

host -t ns [name] - to find the server of domain names

slash.org name server dns2.registrar-servers.com.
slash.org name server dns1.registrar-servers.com.

host -t cname [mail.google.com] - to find CNAME

mail.google.com is an alias for googlemail.l.google.com.

host -n -t mx google.com - to find mx domain

google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.

host -t txt google.com - txt domain

google.com descriptive text
"facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com descriptive text "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com descriptive text "v=spf1 include:_spf.google.com ~all"
google.com descriptive text "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com descriptive text
"globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="

dig slash16.org

; <<>> DiG 9.8.3-P1 <<>> slash.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62924
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;slash.org. IN A

;; ANSWER SECTION:
slash.org. 1577 IN A 162.255.119.96

```
;; AUTHORITY SECTION:
slash.org.              1577    IN      NS      dns1.registrar-servers.com.
slash.org.              1577    IN      NS      dns2.registrar-servers.com.

;; Query time: 2 msec
;; SERVER: 192.168.5*.2#53(192.168.5*.2)
;; WHEN: Fri Oct 18 13:15:18 2019
;; MSG SIZE  rcvd: 102
```

```
nslookup slash16.org

Server:         192.168.5*.2
Address:        192.168.5*.2#53

Non-authoritative answer:
Name: slash.org
Address: 162.255.119.96
```

My answer was: nslookup [name]

6. Get the complete path of the file that contains the IP address of the DNS server you're using

In /etc/resolv.conf there is info:

```
domain 21-school.ru
nameserver 192.168.50.2
nameserver 77.88.8.1
nameserver 77.88.8.8
nameserver 1.1.1.1
nameserver 8.8.8.8
```

7. Query an external DNS server on the slash16.org domain name (ie. : google 8.8.8.8)
Запросить внешний DNS сервер по доменному имени slash16.org

```
dig @8.8.8.8 [name]

; <<>> DiG 9.8.3-P1 <<>> @8.8.8.8 slash16.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16571
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;slash16.org.                   IN      A
```

```
;; ANSWER SECTION:
slash16.org.            59      IN      A       54.192.230.162
slash16.org.            59      IN      A       54.192.230.145
slash16.org.            59      IN      A       54.192.230.59
slash16.org.            59      IN      A       54.192.230.31

;; Query time: 46 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Oct 18 13:31:07 2019
;; MSG SIZE  rcvd: 93
```

```
nslookup [name] 8.8.8.8

Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name: slash16.org
Address: 54.192.230.145
Name: slash16.org
Address: 54.192.230.162
Name: slash16.org
Address: 54.192.230.59
Name: slash16.org
Address: 54.192.230.31
```

It is quiry to the public DNS instead of default one. We can use 8.8.8.8 or partially-public 4.2.2.2

8. Find the provider of slash16.org
Найти провайдера slash16.org

Command whois [name] gives short name in (команда выводит имя в виде аббревиатуры):

```
Name Server: NS-1236.AWSDNS-26.ORG
Name Server: NS-144.AWSDNS-18.COM
Name Server: NS-686.AWSDNS-21.NET
Name Server: NS-1989.AWSDNS-56.CO.UK
```

AWS is Amazon Web Services

```
whois [IP-address]
```

Amazon Technologies Inc. AT-88-Z (NET-13-32-0-0-1) 13.32.0.0 - 13.47.255.255
Amazon.com, Inc. AMAZO-CF (NET-13-32-0-0-2) 13.32.0.0 - 13.33.255.255

gives the company - выводит компанию, чтобы сориентироваться в аббревиатурах

dig slash16.org
;; AUTHORITY SECTION:

slash16.org.	24557	IN	NS	ns-1989.awsdns-56.co.uk.
slash16.org.	24557	IN	NS	ns-144.awsdns-18.com.
slash16.org.	24557	IN	NS	ns-686.awsdns-21.net.
slash16.org.	24557	IN	NS	ns-1236.awsdns-26.org.

awsdns - Amazon Web Services DNS

9. Find the external IP of 42.fr
Внешний IP 42.fr

ping -c 2 42.fr

PING 42.fr (163.172.250.12): 56 data bytes
64 bytes from 163.172.250.12: icmp_seq=0 ttl=54 time=47.152 ms
64 bytes from 163.172.250.12: icmp_seq=1 ttl=54 time=47.177 ms

host 42.fr

42.fr has address 163.172.250.13
42.fr has address 163.172.250.12
42.fr mail is handled by 10 mx01.42.fr.
42.fr mail is handled by 10 mx02.42.fr.

Ответила: 163.172.250.12

10. Identify the network devices between your computer and the slash16.org domain
Выявить все шаги (в виде устройств), которые проходит запрос от вашей машины до домена slash16.org

dig +trace [name]

; <<>> DiG 9.8.3-P1 <<>> +trace slash16.org
;; global options: +cmd

.	73483	IN	NS	f.root-servers.net.
.	73483	IN	NS	b.root-servers.net.
.	73483	IN	NS	j.root-servers.net.
.	73483	IN	NS	d.root-servers.net.
.	73483	IN	NS	c.root-servers.net.

```
.                       73483  IN      NS      a.root-servers.net.
.                       73483  IN      NS      g.root-servers.net.
.                       73483  IN      NS      m.root-servers.net.
.                       73483  IN      NS      i.root-servers.net.
.                       73483  IN      NS      e.root-servers.net.
.                       73483  IN      NS      k.root-servers.net.
.                       73483  IN      NS      h.root-servers.net.
.                       73483  IN      NS      l.root-servers.net.
;; Received 508 bytes from 192.168.5*.2#53(192.168.50.2) in 61 ms

org.                    172800         IN      NS      a0.org.afilias-nst.info.
org.                    172800         IN      NS      a2.org.afilias-nst.info.
org.                    172800         IN      NS      b0.org.afilias-nst.org.
org.                    172800         IN      NS      b2.org.afilias-nst.org.
org.                    172800         IN      NS      c0.org.afilias-nst.info.
org.                    172800         IN      NS      d0.org.afilias-nst.org.
;; Received 431 bytes from 199.7.83.42#53(199.7.83.42) in 39 ms

slash16.org.            86400  IN      NS      ns-144.awsdns-18.com.
slash16.org.            86400  IN      NS      ns-686.awsdns-21.net.
slash16.org.            86400  IN      NS      ns-1236.awsdns-26.org.
slash16.org.            86400  IN      NS      ns-1989.awsdns-56.co.uk.
;; Received 182 bytes from 199.249.112.1#53(199.249.112.1) in 67 ms

slash16.org.            60     IN      A       54.192.230.59
slash16.org.            60     IN      A       54.192.230.145
slash16.org.            60     IN      A       54.192.230.31
slash16.org.            60     IN      A       54.192.230.162
slash16.org.            172800         IN      NS      ns-1236.awsdns-26.org.
slash16.org.            172800         IN      NS      ns-144.awsdns-18.com.
slash16.org.            172800         IN      NS      ns-1989.awsdns-56.co.uk.
slash16.org.            172800         IN      NS      ns-686.awsdns-21.net.
;; Received 230 bytes from 205.251.199.197#53(205.251.199.197) in 39 ms
```

This is how domain resolution works. You can get valuable information about the speed and accuracy of the answer.
Можно получить информацию также по быстроте и ответам при прохождении через устройства.

```
traceroute slash16.org

traceroute to slash16.org (13.32.43.171), 64 hops max, 52 byte packets
 1  192.168.2*.1 (192.168.20.1)  1.679 ms  1.013 ms  1.006 ms
 2  192.168.2.9 (192.168.2.9)  0.317 ms  0.281 ms  0.214 ms
 3  217-67-187-49.in-addr.mastertelecom.ru (217.67.187.49)  5.688 ms  3.223 ms  4.665 ms
 4  mail.neoresurs.ru (217.67.176.130)  0.497 ms  0.524 ms  0.474 ms
 5  217-67-176-205.in-addr.mastertelecom.ru (217.67.176.205)  1.891 ms  4.899 ms 4.840 ms
 6  ae11-227.rt.mr.msk.ru.retn.net (87.245.253.69)  1.237 ms  1.182 ms  1.328 ms
```

```
 7  ae5-8.rt.rad.hki.fi.retn.net (87.245.233.174)  15.392 ms  15.707 ms  15.424 ms
 8  52.46.167.62 (52.46.167.62)  16.678 ms  17.281 ms  17.159 ms
 9  * * *
 10  * * *
 11  * * *
 12  * * *
 13  * * *
 14  * * *
 15  * * *
 16  server-13-32-43-171.hel50.r.cloudfront.net (13.32.43.171)  16.051 ms  17.101 ms
17.128 ms
```

Using this DNS tool, you send a packet of data to an internet host, and it gives you back a result for every hop your query makes in seconds. If your website has a slow response, using this tool you can see where exactly it is the problem.

Для определения промежуточных маршрутизаторов traceroute отправляет целевому узлу серию ICMP-пакетов (по умолчанию 3 пакета), с каждым шагом увеличивая значение поля TTL («время жизни») на 1. Это поле обычно указывает максимальное количество маршрутизаторов, которое может быть пройдено пакетом. Первая серия пакетов отправляется с TTL, равным 1, и поэтому первый же маршрутизатор возвращает обратно ICMP-сообщение «time exceeded in transit», указывающее на невозможность доставки данных. Traceroute фиксирует адрес маршрутизатора, а также время между отправкой пакета и получением ответа (эти сведения выводятся на монитор компьютера). Затем traceroute повторяет отправку серии пакетов, но уже с TTL, равным 2, что заставляет первый маршрутизатор уменьшить TTL пакетов на единицу и направить их ко второму маршрутизатору. Второй маршрутизатор, получив пакеты с TTL=1, так же возвращает «time exceeded in transit».
Процесс повторяется до тех пор, пока пакет не достигнет целевого узла. При получении ответа от этого узла процесс трассировки считается завершённым.

11. Use the output of the previous command to find the name and IP address of the device that makes the link between you (local network) and the outside world
Благодаря прошлой команде найдите IP адрес устройства, которое соединяет вашу локальную сеть и сеть интернет

It is done through NAT, NAT transfers local addresses into external ones.
Все работает через NAT.
https://wiki.merionet.ru/seti/13/nat-na-palcax-chto-eto/

12. Find the IP that was assigned to you by DHCP server
Найдите IP, который был вам дан DHCP сервером

DHCP - https://wiki.merionet.ru/seti/11/vse-chto-vam-nuzhno-znat-pro-dhcp/
ifconfig | grep "inet " | grep -v 127.0.0.1 | cut -d\ -f2
ipconfig getifaddr en0

192.168.2*.1*2

13. Thanks to the previous question and the reverse DNS find the name of your host

14. What file contains the local DNS entries?
В каком файле лежат локальные разметки IP-домен (DNS записи)

/etc/hosts

15. Make the intra.42.fr address reroute to 46.19.122.85
Сделайте так, чтобы домен intra.42.fr приводил на 46.19.122.85

We do not have rights (у нас нет прав), but we should do:
When we ask for connection to some IP-address, first fo all, our mashine looks in the file-
Если мы запрашиваем сайт по доменному имени, сперва машина смотрит на локальный файл /etc/hosts.

e2r9p6% vi /etc/hosts
192.168.5*.1* cdn.42.fr
192.168.5*.1* cdn.intra.42.fr
127.0.0.1 localhost
255.255.255.255 broadcasthost
::1 localhost

46.19.122.85 intra.42.fr

Then if i try to connect to domain name "intra.42.fr" i will be redirected to IP-address 46.19.122.85 and domain "prod1-hadopi-web.integra.fr."

System

Installation (Установка виртуалки)
Virtual Box, debian
ISO image:
https://cdimage.debian.org/debian-cd/current-live/amd64/iso-hybrid/

СОВЕТ: ничего еще не понимая в этом мире ставила live версию - не стоит этого делать, слетает все каждый раз. Однако, можно хорошенько заучить все основные команды. И еще: лучше делать Snapshots - снимки системы после определенных настроек. Если этого не делать, есть возможность убить машину и начать делать все заново. Благодаря же Snapshots можно восстановить версию уже с какими-либо настройками.

1. In what file can you find the installed version of your Debian?
В каком файле можно узнать версию установленного Debian

The installed version of the system we are in (here with Debian we need to look for file in system architecture on the virtual machine) you can find the version in /etc/debian_version (it is a file and will contain numbers meaning the version)

"9.7"

2. What command can you use to rename your system?
Какой командой можно переименовать систему

hostnamectl (Control the System hostname) on VM
--static, --transient, --pretty

sudo hostnamectl set-hostname "NAME" - if not root user (если не под рутом)
To change to the root user: su [Enter] and password input

При установке виртуальной машины будет также назначаться пароль для root юзера.
Под рутом все намного проще делать, чтобы постоянно не писать sudo. Переход: su [Enter]

hostname on MAC - just to see (чтобы только увидеть)

Just info:
On VM:

hostname -i
fe80::e126:98f9:3773:8a37%enp0s3 10.0.2.15

hostname -I
10.0.2.15

To see the domain DNS name, we use flag -d:
hostname -d
sschmele

hostname -f shows FQDN name - fully qualified domain name:
hostname -f
sschmele.com

hostname -A shows all the data of FQDN host:

hostname -A
mail.sschmele.com

3. What file has to be modified to make it permanent?
Какой файл нужно изменить, чтобы сделать имя постоянным

/etc/hosts
Then reboot the system by "systemctl restart networking" or "service networking restart" (Debian or Ubuntu) - потом перезапустить систему с использованием команд выше

4. What command gives you the time since your system was last booted?
Время, когда ваша машина была запущена последний раз

The command "top" shows all the processes running in the system
Все процессы, которые запущены в системе

top

17:44 up 1 day, 6:45, 4 users, load averages: 1.33 1.42 1.40
Tasks: 119 total, 1 running, 118 sleeping, 0 stopped, 0 zombie
%Cpu(s) :
KiB Mem :
KiB Swap :
Detalization

The command "w" shows the system time, how long it works and how many users are there
Время, как долго система работает, какие юзеры есть

w

10:03:10 up 20 min, 2 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

uptime

17:44 up 1 day, 6:45, 4 users, load averages: 1.33 1.42 1.40

5. Name the command that determines the state of the SSH service.

sudo service ssh status - check (проверка существования сервиса)

sudo apt-get update -y && sudo apt-get upgrade -y - package installer on Debian and Ubuntu (Linux systems), установщик пакетов на Линукс системах

https://help.ubuntu.ru/wiki/%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE_%D0%BF%D0%BE_ubuntu_server/%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0%D0%BC%D0%B8/apt-get

sudo apt-get install openssh-server

sudo service ssh start - старт сервиса

Проверка работы (answer here, ответ на задание):

sudo service ssh status
sudo /etc/init.d/ssh status
systemctl status sshd

It should be Active: active (running) since ...

6. Name the command that reboots the SSH service.

sudo service ssh restart
sudo service sshd reload

7. Figure out the PID of the SSHD service.

PID сервиса ssh

pidof sshd

2209

ps aux | grep root | grep sshd (потому что демон)

root 2209 0.0 0.0 66224 1184 ? Ss 17:46 0:00 /usr/sbin/sshd

pgrep -u [user] - watch all the processes of the user (все процессы юзера)

8. What file contains the RSA keys of systems that are authorized to connect via SSH?

В каком файле лежат RSA ключи, которые позволяют подключаться по ssh

All the authorized keys for the remote server lie in the file ~/.ssh/authorized_keys

9. What command lets you know who is connected to the System?
Посмотреть, кто еще подключен к системе

who

skyline console Mar 23 10:59
skyline ttys000 Mar 24 17:04

10. Name the command that lists the partition tables of drives?
Команда, которая показывает деление диска

sudo fdisk -l
sudo sfdisk -l

sudo cfdisk /dev/sdb
Shows one partition at a time (1 деление за раз)

df -h
Only the file systems that start with a /dev are actual devices or partitions.

Fdisk adn cfdisk are used for the disk segmentation (используются для деления диска)
fdisk - manipulate disk partition table and fdisk -- DOS partition maintenance program
lsblk

11. Name the command that displays the available space left and used on the system in an humanly understandable way
Показывает, сколько места осталось и было использовано в адекватном формате - с обозначением измерений (K, Mb …)

df -h

df - display free disk space
df -h - "Human-readable" output.

12. Figure out the exact size of each folder of /var in a humanly understandable way followed by the path of it.
Узнать вес каждой папки в адекватном формате - с обозначением измерений (K, Mb …)

du -h
Shows all the folders with ./work/... and their size in a "Human-readable" way

du -h *
Shows all the folders without ./

13. Name the command that find, in real time, currently running processes
Команда, которая позволяет увидеть все процессы системы в реальном времени

top

14. Run the ‘tail -f /var/log/syslog‘ command in background
Запустить команду в фоне

tail is needed to give the tail part of the file (показывает конец файла, может работать сразу с несколькими файлами - перечисление через пробел)
tail -n 20 /var/log/syslog last 20 lines of the file
[command] & - does all the commands in the background (в фон)
sudo tail -f /var/log/syslog & [5] 2050 (pid)
fg - see the background processes and bring it back to the foreground (посмотреть процессы в фоне и перевести вперед)

15. Find the command that kills the background command’s process
Команда, которая помогает завершить фоновый процесс

kill -l - list of signals
jobs shows you processes you called in a human understandible way
ps aux all the processes

kill [pid]
pkill [process_name]

16. Find the service which makes it possible to run specific tasks following a regular schedule
Сервис, который помогает установить выполнение каких-либо задач на регулярной основе

cron is used to perform tasks at some special time, for ex. do a backup of our system
the main configuration file is /etc/crontab
https://help.ubuntu.ru/wiki/cron

crontab -l shows for user
sudo crontab -l shows for root
sudo crontab -e makes it possible to create a task (создание задания)

17. Find the command that allows you to connect via ssh on the VM.(In parallel with the graphic session)
Команда, которая позволяет подключиться по ssh к виртуалке - с сохранением графической сессии

You need to create a new key:
Создание rsa ключа:

sudo ssh-keygen -t rsa -b 2048

The default is 2048, the minimum is 1024, "-t" specify the type of key (тип ключа)
It asks you where to save your keys, default in the file /home/user/.ssh/id_rsa and the public in /home/user/.ssh/id_rsa.pub (спрашивает, куда сохранить, по дефолту - эти папки)
Shows you the fingerprint: SHA256: TyQZnNrw8… (показывает отпечаток)
And shows the key's randomart image (и образ)

ssh [user_name]@[public IP-address]
OR
sudo ssh -p [port_nb] [user_name]@[public IP-address]

Default port nb is 22
Port is stated in /etc/ssh/sshd_config

check port: sudo netstat -tulpan | grep ssh
check all the users: "awk -F: '{ print $1}' /etc/passwd" or "getent passwd | awk -F: '{print $1}'

If you want to connect to VM, in settings->network do bridge instead of NAT and then:
On VM there will be new IP-address (проброс портов на VM)

18. Find the command that kills ssh service
Завершение работы ssh сервиса

exit stops the session (останавливает сессию)
sudo kill [PID ssh] - kills it with pid (убивает по pid)

Connection to [IP-address] closed by remote host (if we close form the main user)
Connection to [IP-address] closed.

Get the PID (узнать pid):

ps -aux | grep ssh
pidof ssh

pkill ssh

19. List all services which are started at boot time and name this kind of services
Перечисление всех сервисов, которые были запущены с момента загрузки системы

sudo service --status-all - only the names with [+] or [-]
systemctl list-units --type service --all - full names with all the info and description (полное описание)
systemctl -at service - full names with all the info and description (полное описание)

20. List all existing users on the VM
Перечисление всех существующих юзеров

awk -F: '{ print $1}' /etc/passwd
getent passwd | cut -d: -f1

21. List all real users on the VM
Перечисление всех реальных юзеров

All real users have UIDs starting with 1000 and till 59999 or in the directory /home
У всех реальных юзеров UID лежит в промежутке от 1000 до 59999. ВАЖНО - директория /home устанавливается не всегда, зависит от файловой системы

cat /etc/passwd | grep '/home' | cut -d: -f1 - is not always valid because we can create a user without home dir (не всегда сработает через директорию /home)

getent passwd | cut -d: -f1,3 | egrep ':[0-9]{4}$' | cut -d: -f1 - but the last limit is 59999 (in the file /etc/adduser_conf) - но не обозначен лимит в 59999
getent - get entries from Name Service Switch libraries

Answered: getent passwd {1000..6000} | cut -d: -f1

22. Find the command that add a new local user

Команда для добавления локального юзера

sudo adduser [name]

OR

sudo useradd -m -d /home/[name] -s /bin/bash [name]
sudo passwd [name]

23. Explain how connect yourself as new user. (With graphic session and ssh session)
Объясните, как подключиться по ssh в качестве нового пользователя (с графической сессией)

The creation of a new user:
Создаем нового юзера:

sudo adduser [name]

Will create /bin/bash and ask for creating the password + other info about the new user
Создаст юзера, домашнюю директорию и запросит установку пароля, а также другую информацию о юзере

OR

sudo useradd -m -d /home/[name] -s /bin/bash [name]

In order to be sure that home and bin/bash are done and then
Чтобы убедиться и прописать самому, а далее

sudo passwd [name]

The creation of a public key (not necessary):
Создаем ключи для ssh

sudo ssh-keygen -t rsa -b 2048

Then copy the public key from the /root/.ssh/id_rsa.pub
Копируем ключ из файла
Then switch to the test user
Переключаемся на тестового юзера

su - [name]
mkdir .ssh
chmod 700 .ssh
touch .ssh/authorized_keys
chmod 600 .ssh/authorized_keys

echo "ssh-rsa [full public key]" > /home/[name]/.ssh/authorized_keys

The connection:
Само подключение:

from the main user:
sudo ssh -p [port_nb] [name]@[IP-address]
You need to allow the new user ssh access: /etc/ssh/sshd_config
Нужно позволить пользователю подключаться по ssh

Command "id" shows info:
uid=1004(new_user) gid=1004(new_user) groups=1004(new_user)

Info:
1) ssh: https://habr.com/ru/post/331348/
2) ssh connection: https://mordeniuss.ru/enable-ssh-debian/

24. Find the command that list all packages
Команда, которая выводит все установленные пакеты

apt list --installed

Scripts

Info:

https://habr.com/ru/post/47163/
https://rtfm.co.ua/bash-opisanie-ciklov-for-while-until-i-primery-ispolzovaniya/
полная инструкция (+ awk и sed): https://habr.com/ru/company/ruvds/blog/325928/
https://habr.com/ru/post/158971/

Ex00

Write a script which displays only the login, UID and Path of each entry of the /etc/passwd file

```
#!/bin/bash
file="/etc/passwd"
nb=1
i=0
IFS=$'\n'
```

```
if [ -f $file ]
then
	for line in $(cat $file | grep -v '#')
	do
		echo "$nb"
		IFS=:
		for value in $line
		do
			if [ $i -eq 0 ]
			then
				echo -e "\033[32mLOGIN is $value\033[0m"
			elif [ $i -eq 3 ]
			then
				echo "UID is $value"
			elif [ $i -eq 6 ]
			then
				echo "PATH is $value"
			elif [ $i -gt 6 ]
			then
				break
			fi
			i=$(($i + 1))
		done
		(( nb++ ))
		i=0
	done
else
	echo -e "\033[37;1;41mThe file does not exist\033[0m"
fi
```

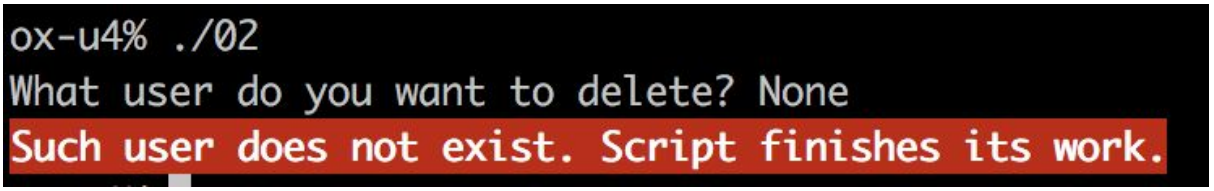
Output:

```
88
LOGIN is _findmydevice
UID is 03
PATH is Find My Device Daemon
89
LOGIN is _datadetectors
UID is 03
PATH is DataDetectors
90
LOGIN is _captiveagent
UID is 03
PATH is captiveagent
91
LOGIN is _ctkd
UID is 03
PATH is ctkd Account
92
LOGIN is _applepay
UID is 03
PATH is applepay Account
93
LOGIN is _hidd
UID is 03
PATH is HID Service User
```

Ex01

```
#!/bin/bash
i=0
read -p "What user do you want to delete? " answer
name=$answer
$(cat /etc/passwd | grep $name > /dev/null 2>&1)
if [ $? -eq 0 ]
then
        while [ $i -ne 1 ]
        do
                read -p "Do you really want to delete the user $name? y/n " answer
                if [ $answer = "y" ]
                then
                        echo "Ok. Deleting all the processes of the user $name."
                        i=1
                        sudo pkill -u $name
                        echo "Deleting the user $name."
                        sudo userdel -f $name
                        echo "User $name deleted. If you want to check, enter the
command: cat /etc/passwd | grep -w [user name]"
                elif [ $answer = "n" ]
                then
                        echo "It is your decision. Script finishes its work."
                        i=1
                else
                        echo -e "\033[31;1mYou gave the wrong answer.\033[0m"
                fi
        done
else
        echo -e "\033[37;1;41mSuch user does not exist. Script finishes its work.\033[0m"
fi
```

Output:



Ex02

```
#!/bin/bash
name=$1
if [ -n "$1" ]
then
        search=$(ldapsearch -Q "uid=$name" | grep -w "# numResponses:" | cut -d: -f2)
```

```
        if [ $search -eq 2 ]
        then
                str=$(ldapsearch -Q "uid=$name" | grep mobile)
                if [ -n "$str" ]
                then
                        echo -e "\033[32;1m$(ldapsearch -Q "uid=$name" | grep
mobile)\033[0m"
                else
                        echo -e "\033[31;1mUser $name keeps his/her phone number in
secret\033[0m"
                fi
        else
                echo -e "\033[37;1;41m Such user does not exist\033[0m"
        fi
#       echo "$(ldapsearch -Q "uid=$name" | grep mobile)"
else
        echo -e "\033[36mPlease, write the user name. Try once more.\033[0m"
fi
```

Output:

```
ox-u4% ./03
Please, write the user name. Try once more.
ox-u4% ./03 sschmele
mobile: 89265989621
ox-u4% ./03 drestles
User drestles keeps his/her phone number in secret
ox-u4%
```