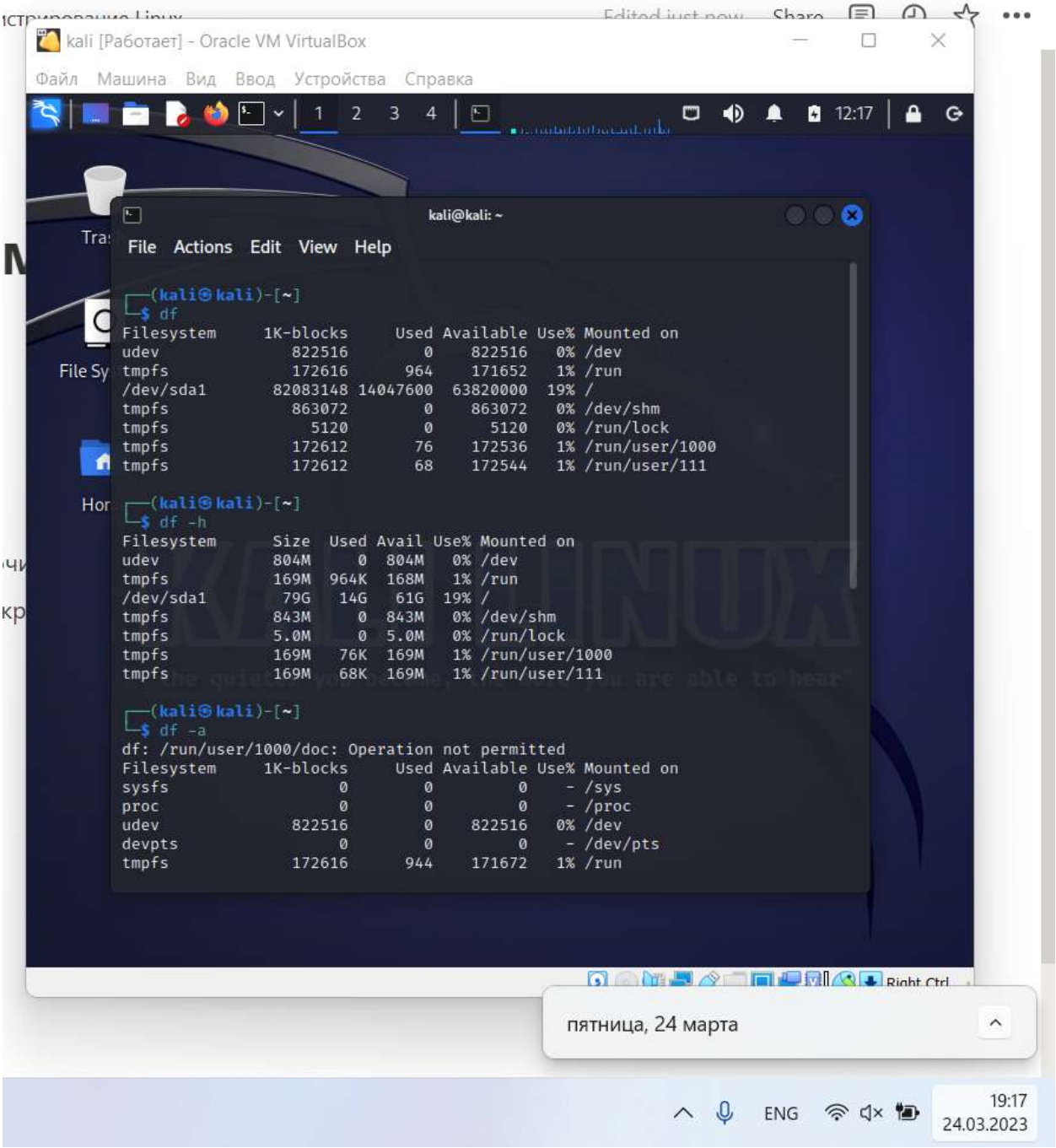
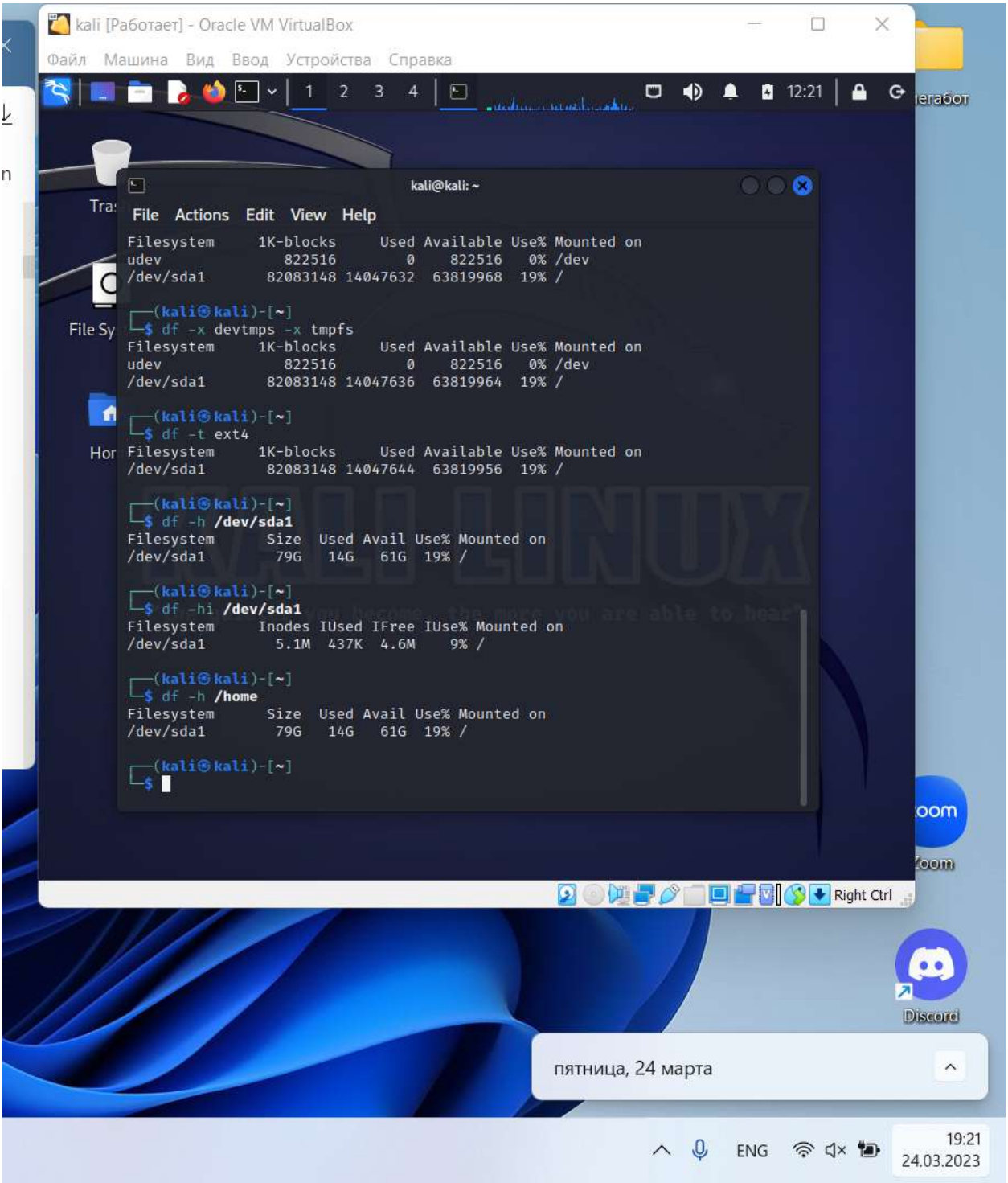
Занятие 2. Администрирование Linux

Задача:

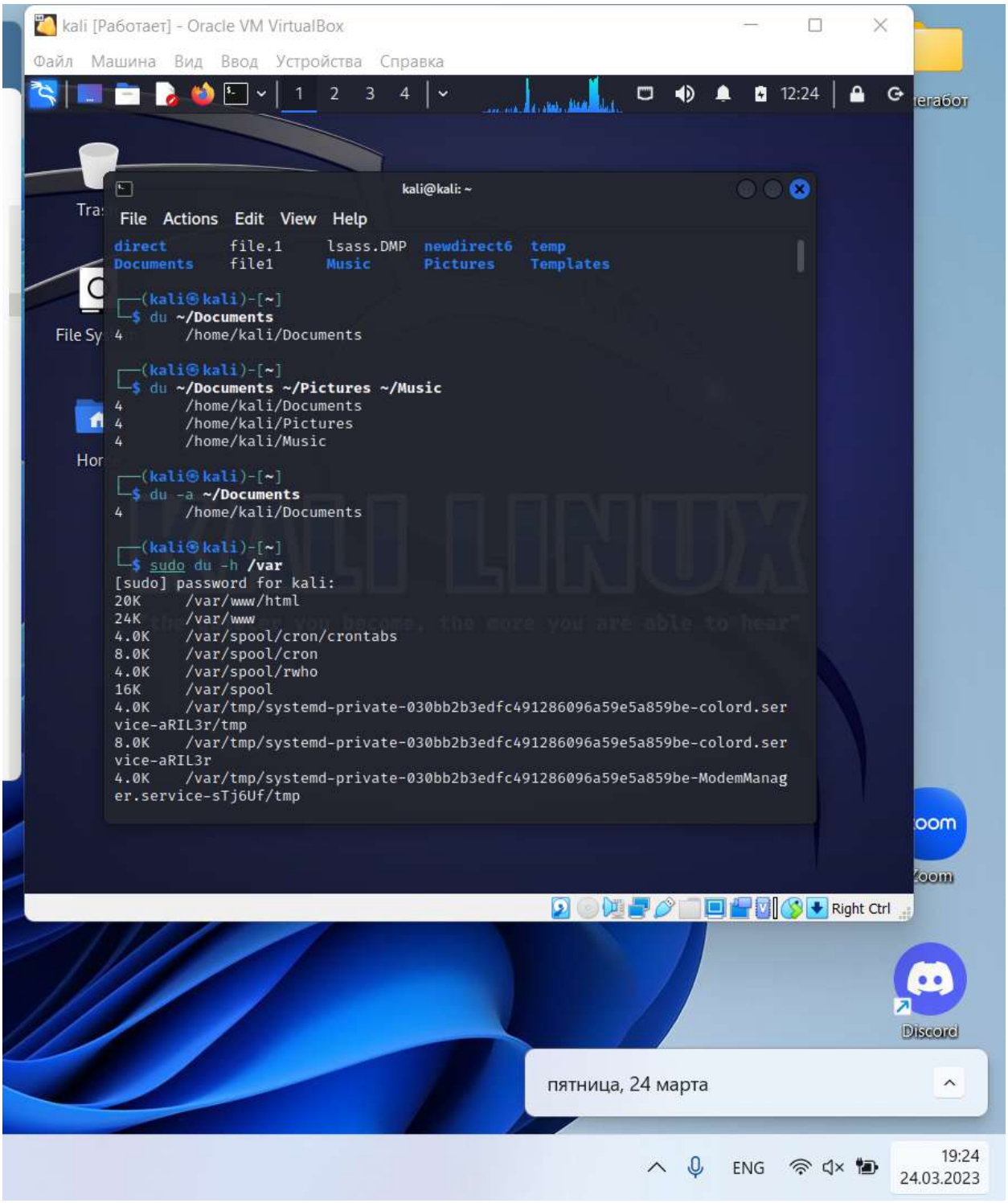
- Изучить работу всех утилит.
- Использовать при работе исключительно терминал.
- Необходимо включить в отчёт скриншоты всех указанных команд и опций в практической работе.

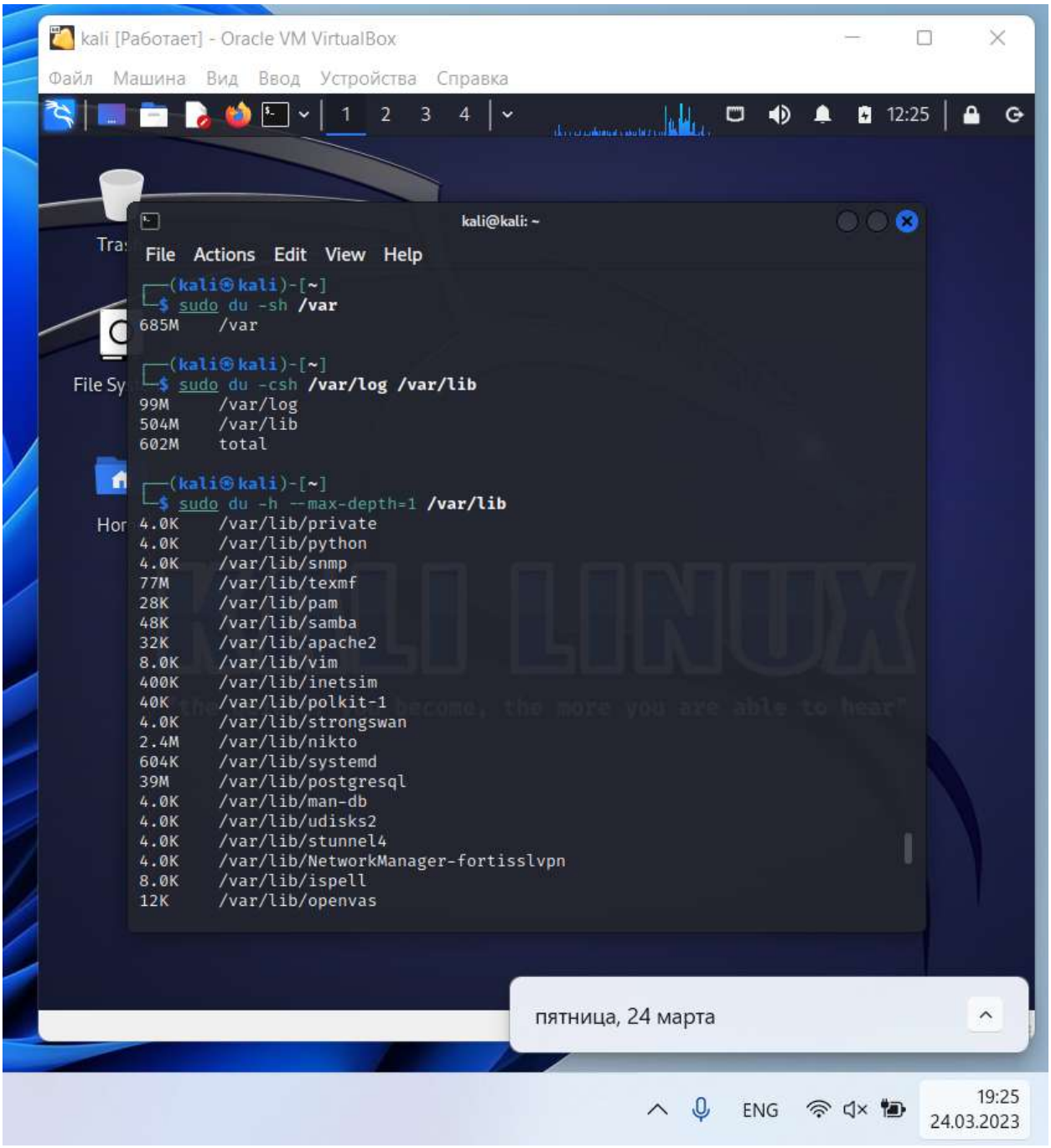
1. Команда df в linux

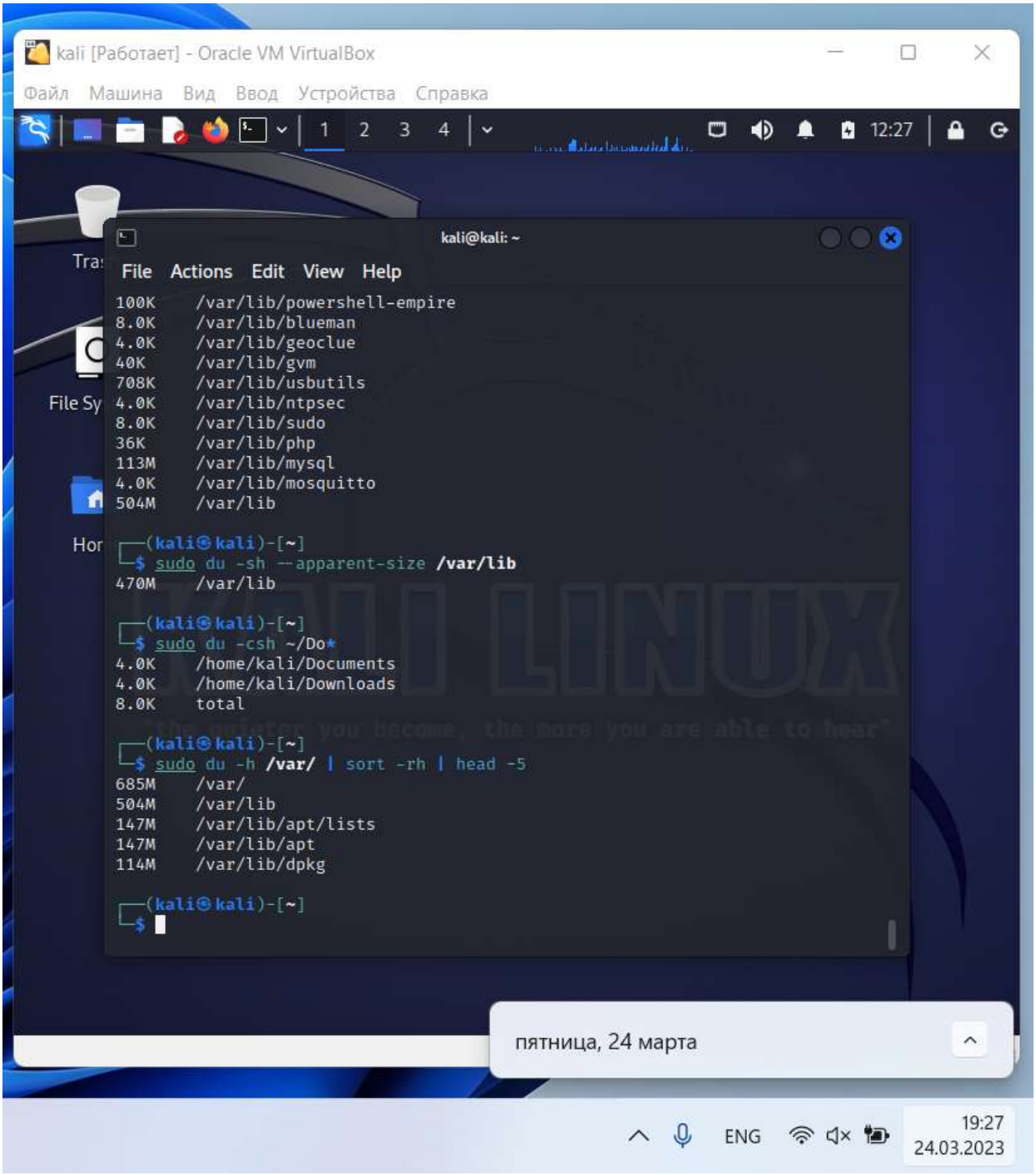

kali [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ df
Filesystem 1K-blocks Used Available Use% Mounted on
udev 822516 0 822516 0% /dev
tmpfs 172616 964 171652 1% /run
/dev/sda1 82083148 14047600 63820000 19% /
tmpfs 863072 0 863072 0% /dev/shm
tmpfs 5120 0 5120 0% /run/lock
tmpfs 172612 76 172536 1% /run/user/1000
tmpfs 172612 68 172544 1% /run/user/111
(kali㉿kali)-[~]
$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 804M 0 804M 0% /dev
tmpfs 169M 964K 168M 1% /run
/dev/sda1 79G 14G 61G 19% /
tmpfs 843M 0 843M 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 169M 76K 169M 1% /run/user/1000
tmpfs 169M 68K 169M 1% /run/user/111
(kali㉿kali)-[~]
$ df -a
df: /run/user/1000/doc: Operation not permitted
Filesystem 1K-blocks Used Available Use% Mounted on
sysfs 0 0 0 - /sys
proc 0 0 0 - /proc
udev 822516 0 822516 0% /dev
devpts 0 0 0 - /dev/pts
tmpfs 172616 944 171672 1% /run
пятница, 24 марта
ENG
19:17
24.03.2023



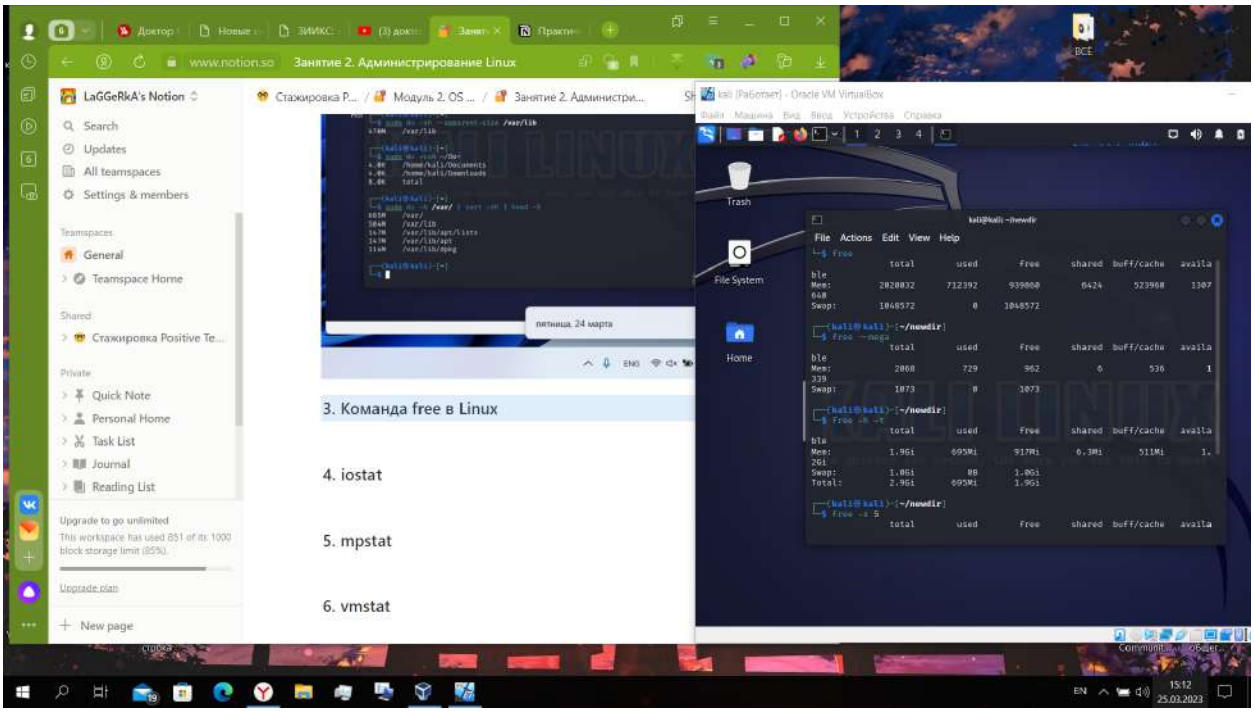
2. Команда du в Linux

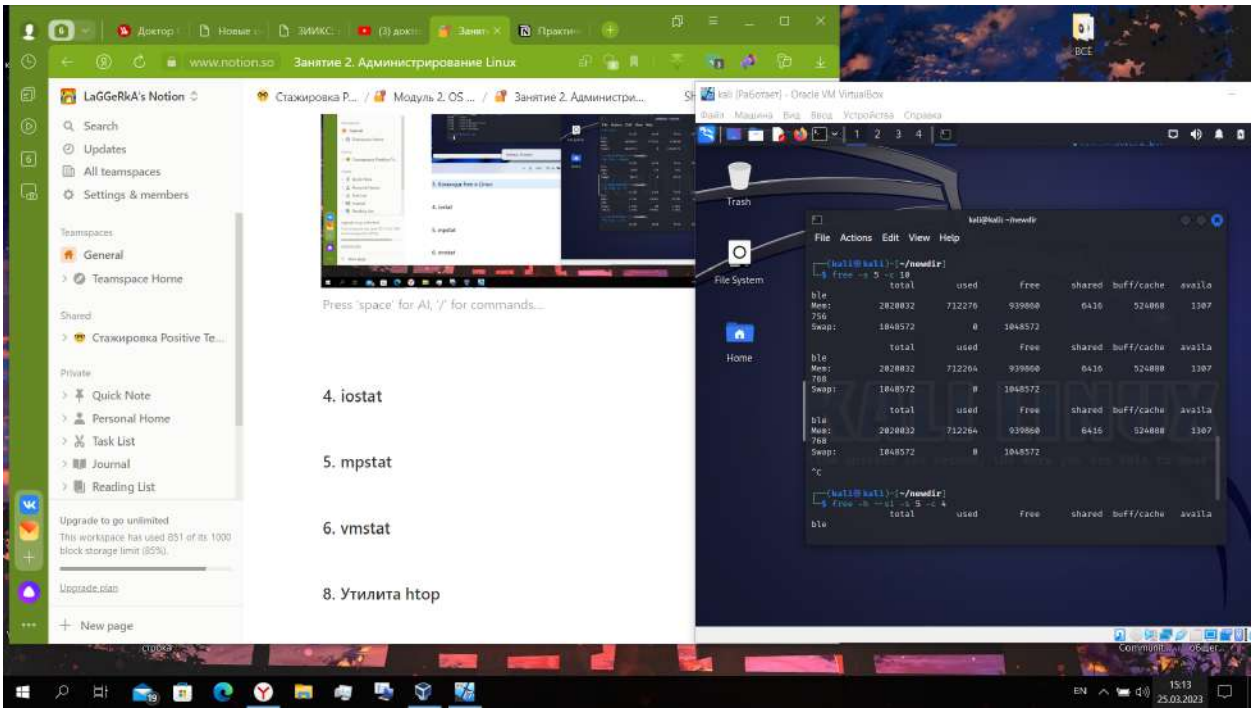

kali [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
12:24
kali@kali: ~
File Actions Edit View Help
direct file.1 lsass.DMP newdirect6 temp
Documents file1 Music Pictures Templates
(kali㉿kali)-[~]
$ du ~/Documents
4 /home/kali/Documents
(kali㉿kali)-[~]
$ du ~/Documents ~/Pictures ~/Music
4 /home/kali/Documents
4 /home/kali/Pictures
4 /home/kali/Music
(kali㉿kali)-[~]
$ du -a ~/Documents
4 /home/kali/Documents
(kali㉿kali)-[~]
$ sudo du -h /var
[sudo] password for kali:
20K /var/www/html
24K /var/www
4.0K /var/spool/cron/crontabs
8.0K /var/spool/cron
4.0K /var/spool/rwho
16K /var/spool
4.0K /var/tmp/systemd-private-030bb2b3edfc491286096a59e5a859be-colord.service-aRIL3r/tmp
8.0K /var/tmp/systemd-private-030bb2b3edfc491286096a59e5a859be-colord.service-aRIL3r
4.0K /var/tmp/systemd-private-030bb2b3edfc491286096a59e5a859be-ModemManager.service-sTj6Uf/tmp
Right Ctrl
Zoom
Discord
пятница, 24 марта
ENG
19:24
24.03.2023

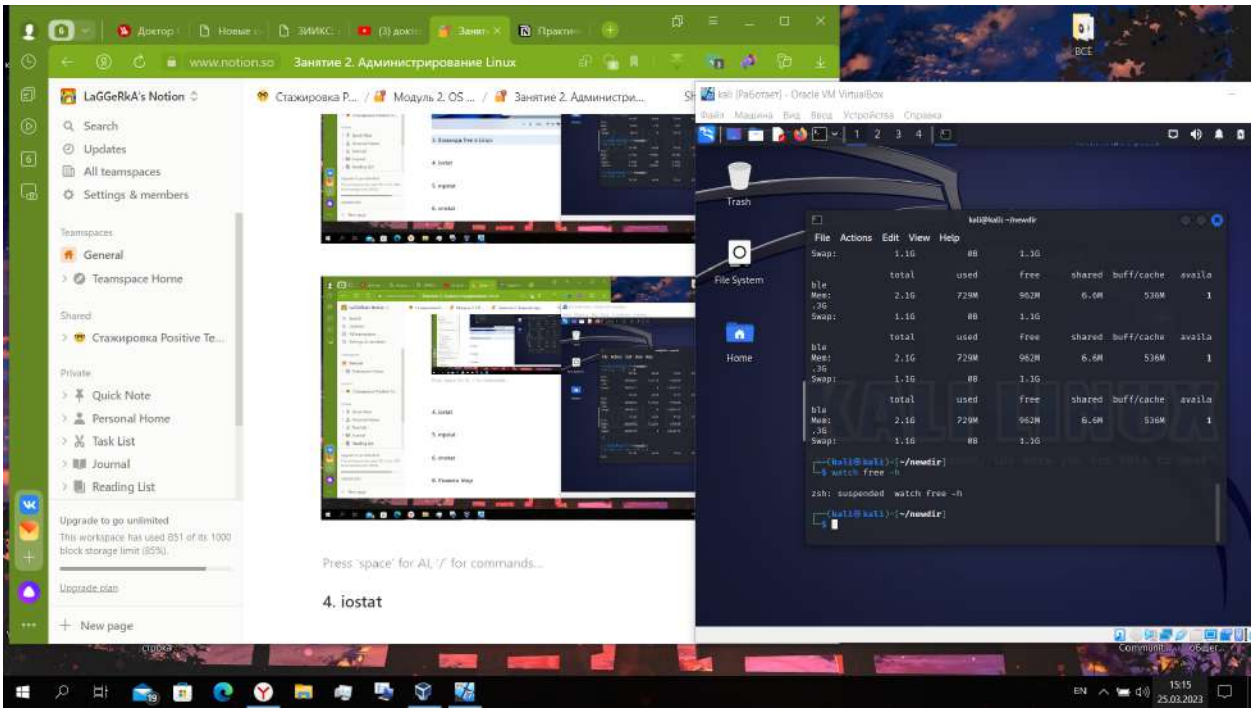

kali [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
1 2 3 4
12:25
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo du -sh /var
685M /var
(kali㉿kali)-[~]
$ sudo du -csh /var/log /var/lib
99M /var/log
504M /var/lib
602M total
(kali㉿kali)-[~]
$ sudo du -h --max-depth=1 /var/lib
4.0K /var/lib/private
4.0K /var/lib/python
4.0K /var/lib/snmp
77M /var/lib/texmf
28K /var/lib/pam
48K /var/lib/samba
32K /var/lib/apache2
8.0K /var/lib/vim
400K /var/lib/inetsim
40K /var/lib/polkit-1
4.0K /var/lib/strongswan
2.4M /var/lib/nikto
604K /var/lib/systemd
39M /var/lib/postgresql
4.0K /var/lib/man-db
4.0K /var/lib/udisks2
4.0K /var/lib/stunnel4
4.0K /var/lib/NetworkManager-fortisslvpn
8.0K /var/lib/ispell
12K /var/lib/openvas
пятница, 24 марта
ENG
19:25
24.03.2023

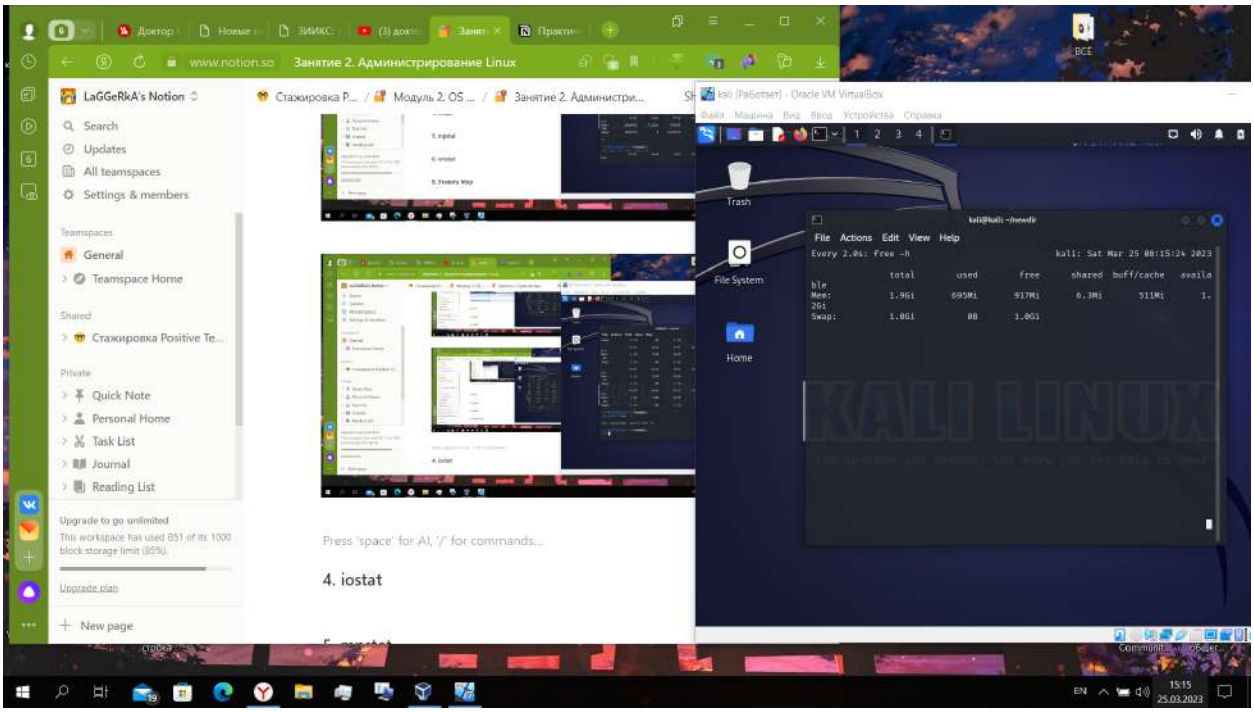


3. Команда free в Linux

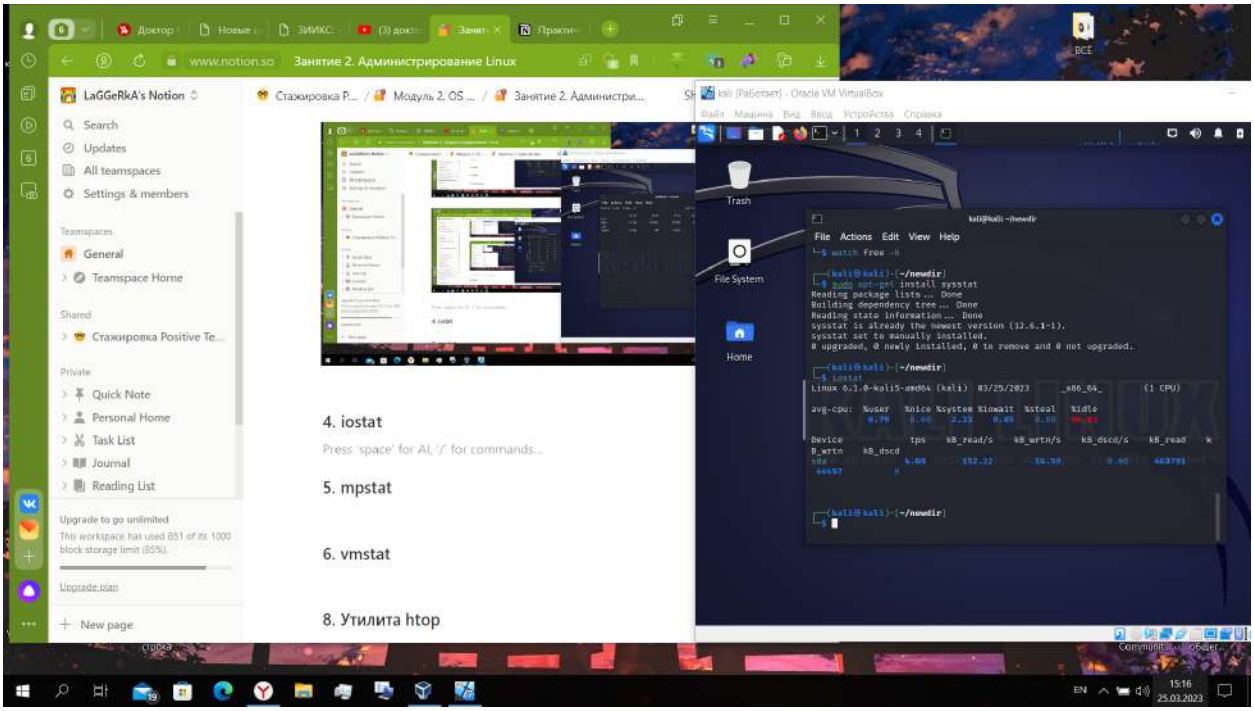

Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
General
Teamspace Home
Quick Note
Personal Home
Task List
Journal
Reading List
New page
3. Команда free в Linux
4. iostat
5. mpstat
6. vmstat
Trash
File System
Home
File Actions Edit View Help

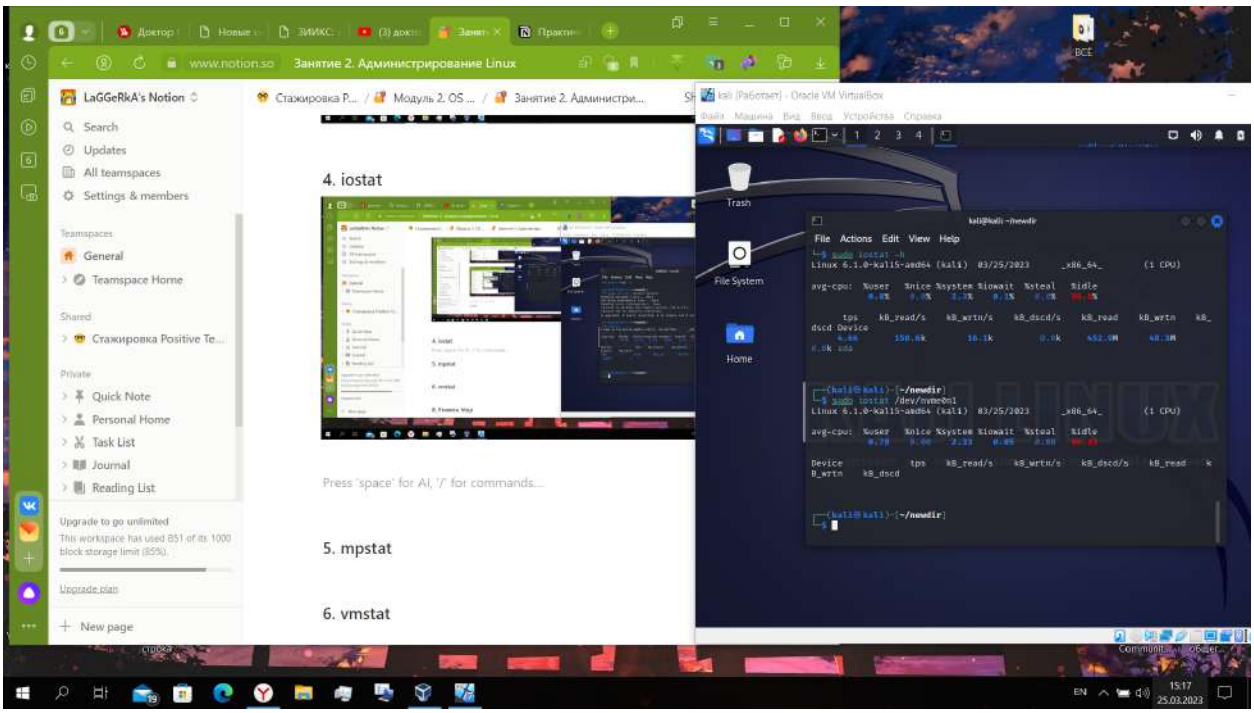

Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
General
Teamspace Home
Quick Note
Personal Home
Task List
Journal
Reading List
New page
Press 'space' for AI, '/' for commands...
4. iostat
5. mpstat
6. vmstat
8. Утилита htop
Trash
File System
Home
File Actions Edit View Help

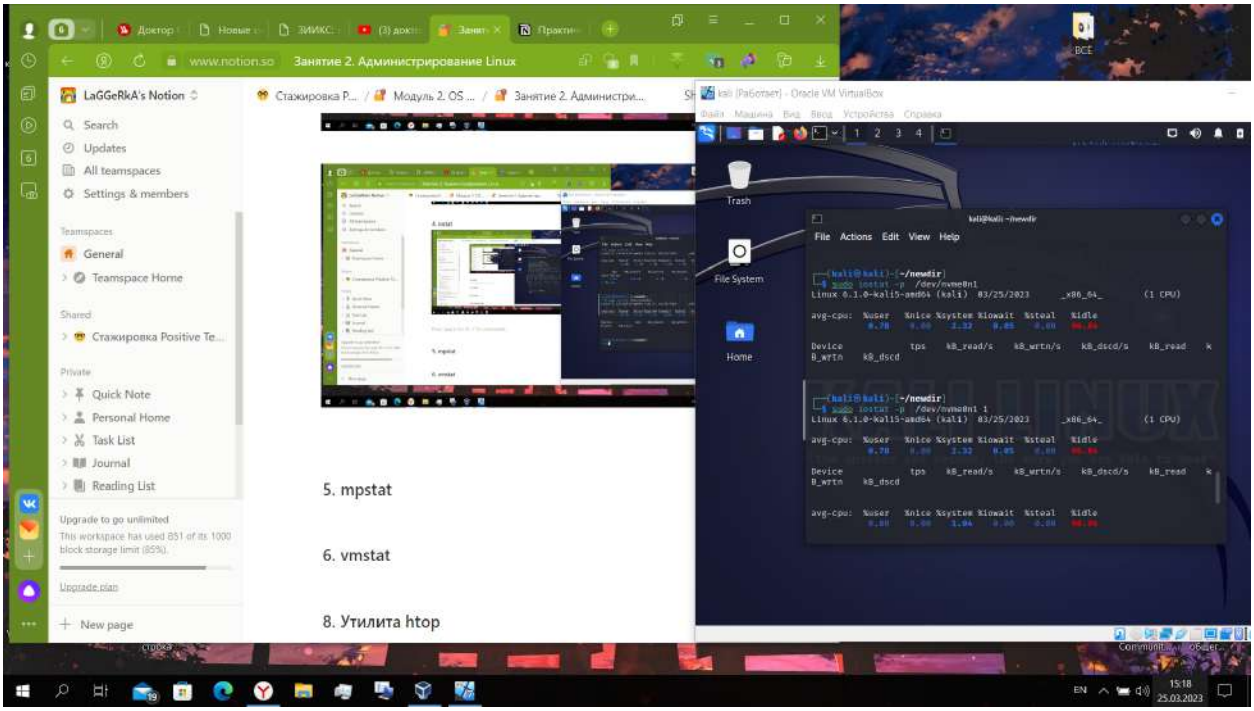

www.notion.so
Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
Teamspaces
General
Teamspace Home
Shared
Стажировка Positive Te...
Private
Quick Note
Personal Home
Task List
Journal
Reading List
Upgrade to go unlimited
This workspace has used 851 of its 1000 block storage limit (85%).
Upgrade plan
New page
Press 'space' for AI, '/' for commands...
4. iostat
Trash
File System
Home
File Actions Edit View Help
watch free -h
zsh: suspended watch free -h
15:15
25.03.2023

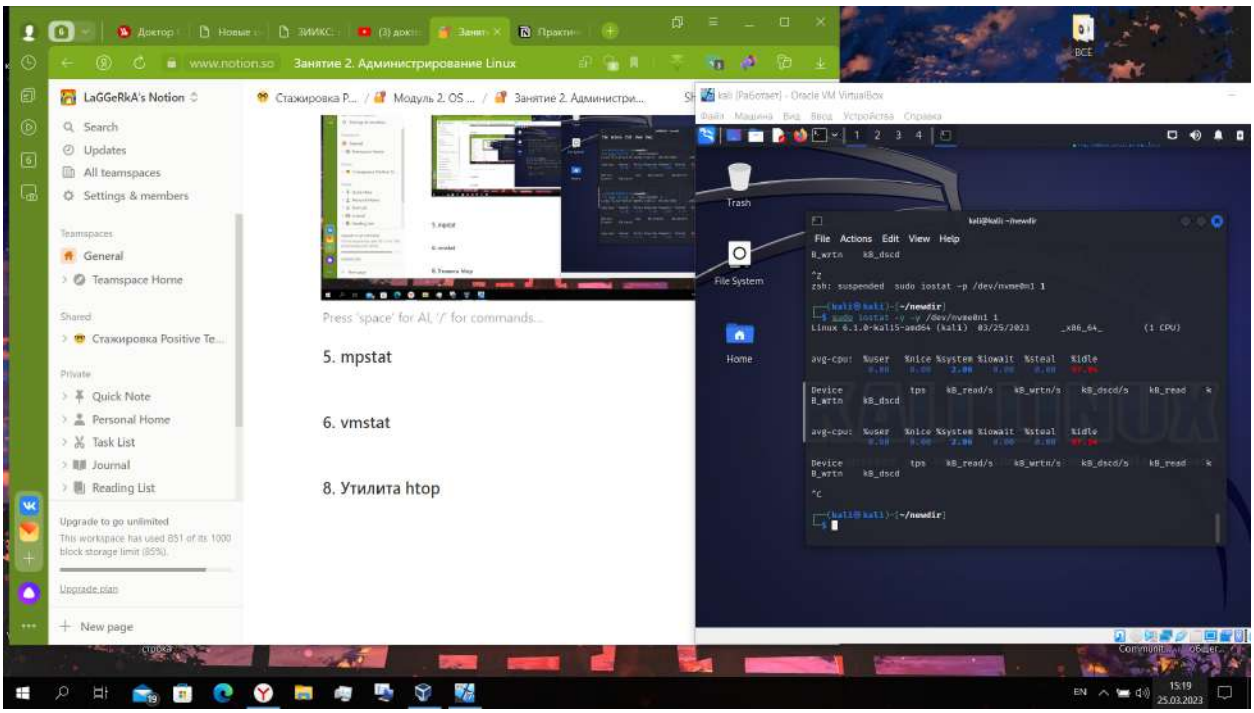

www.notion.so
Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
Teamspaces
General
Teamspace Home
Shared
Стажировка Positive Te...
Private
Quick Note
Personal Home
Task List
Journal
Reading List
Upgrade to go unlimited
This workspace has used 851 of its 1000 block storage limit (85%).
Upgrade plan
New page
Press 'space' for AI, '/' for commands...
4. iostat
Trash
File System
Home
File Actions Edit View Help
Every 2.0s: free -h
KALI LINUX
15:15
25.03.2023

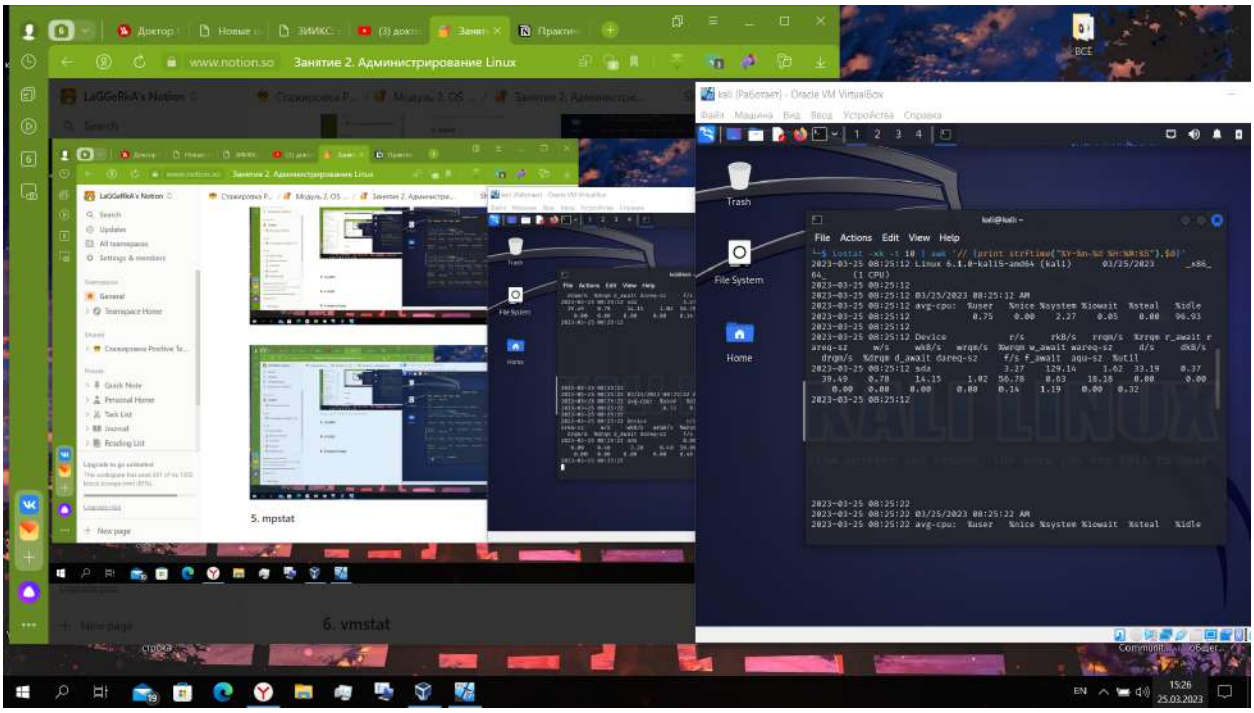
4. iostat

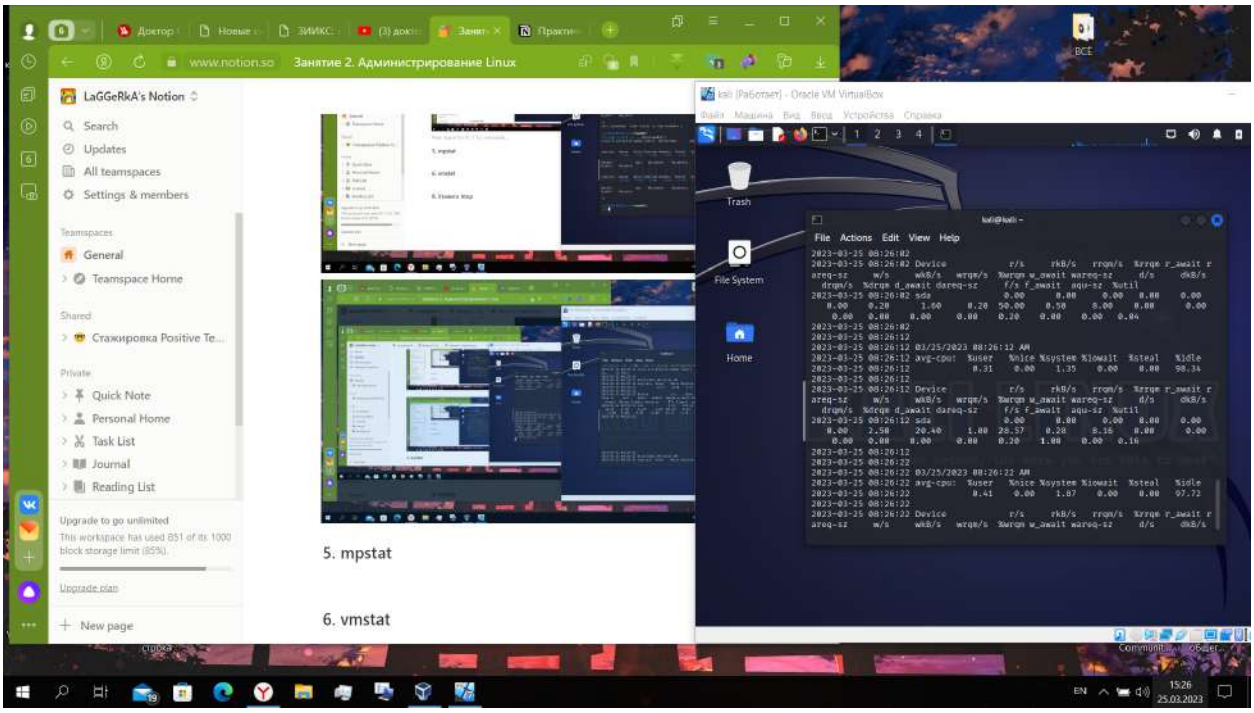

Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
General
Teamspace Home
Стажировка Positive Te...
Quick Note
Personal Home
Task List
Journal
Reading List
New page
4. iostat
5. mpstat
6. vmstat
8. Утилита htop
Trash
File System
Home
File Actions Edit View Help


Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
General
Teamspace Home
Стажировка Positive Te...
Quick Note
Personal Home
Task List
Journal
Reading List
New page
4. iostat
5. mpstat
6. vmstat
Trash
File System
Home
File Actions Edit View Help

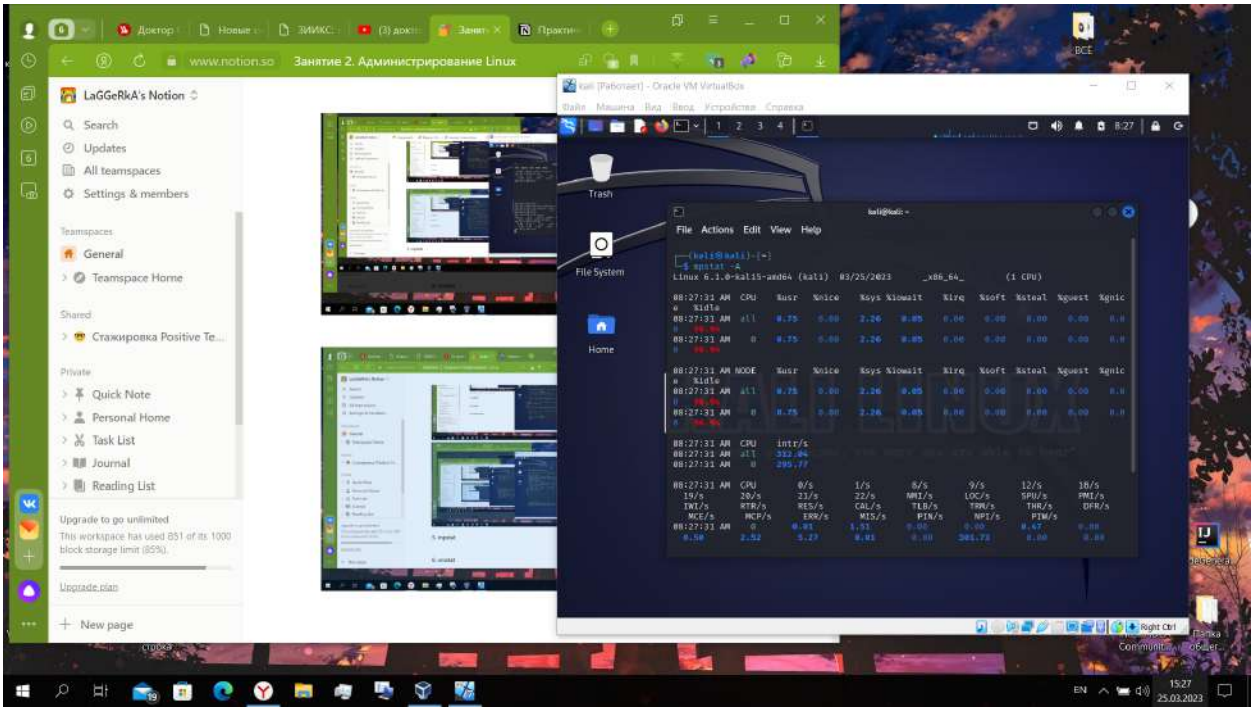

www.notion.so
Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
Teamspaces
General
Teamspace Home
Shared
Стажировка Positive Te...
Private
Quick Note
Personal Home
Task List
Journal
Reading List
Upgrade to go unlimited
Upgrade plan
New page
5. mpstat
6. vmstat
8. Утилита htop
Trash
File System
Home
File Actions Edit View Help
15:18
25.03.2023

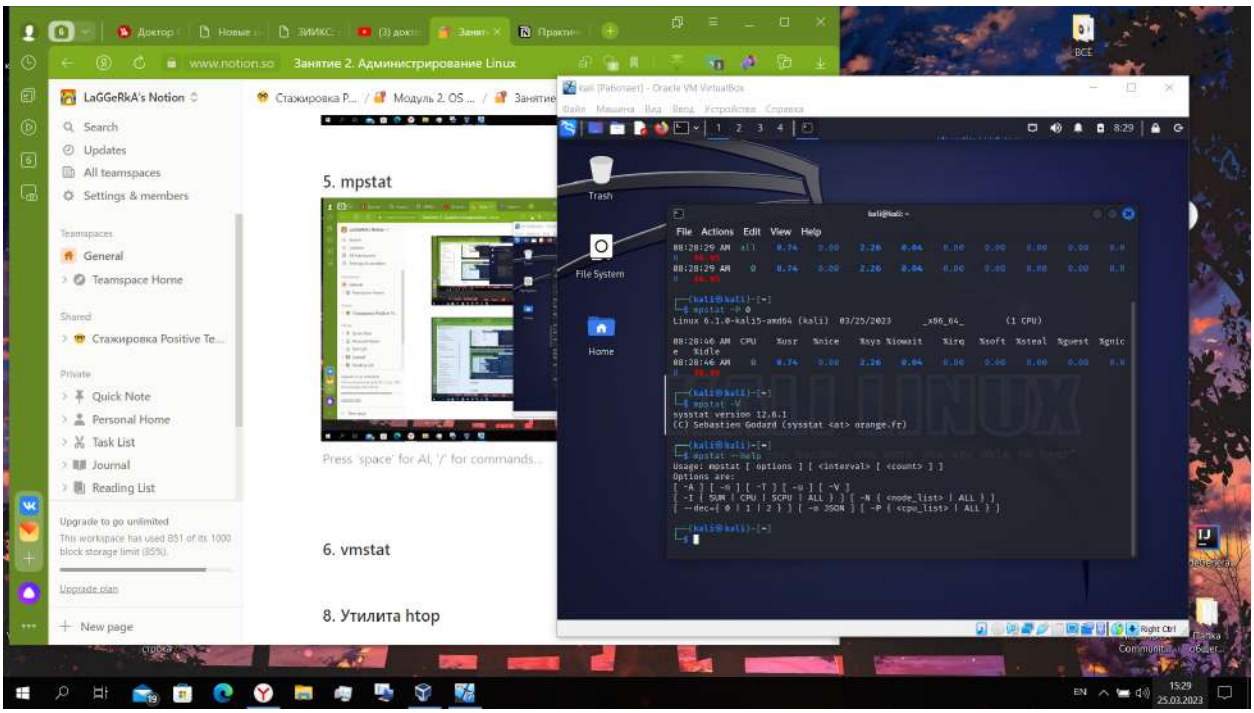

www.notion.so
Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
Teamspaces
General
Teamspace Home
Shared
Стажировка Positive Te...
Private
Quick Note
Personal Home
Task List
Journal
Reading List
Upgrade to go unlimited
Upgrade plan
New page
Press 'space' for AI, '/' for commands...
5. mpstat
6. vmstat
8. Утилита htop
Trash
File System
Home
File Actions Edit View Help
15:19
25.03.2023


www.notion.so
Занятие 2. Администрирование Linux
5. mpstat
6. vmstat

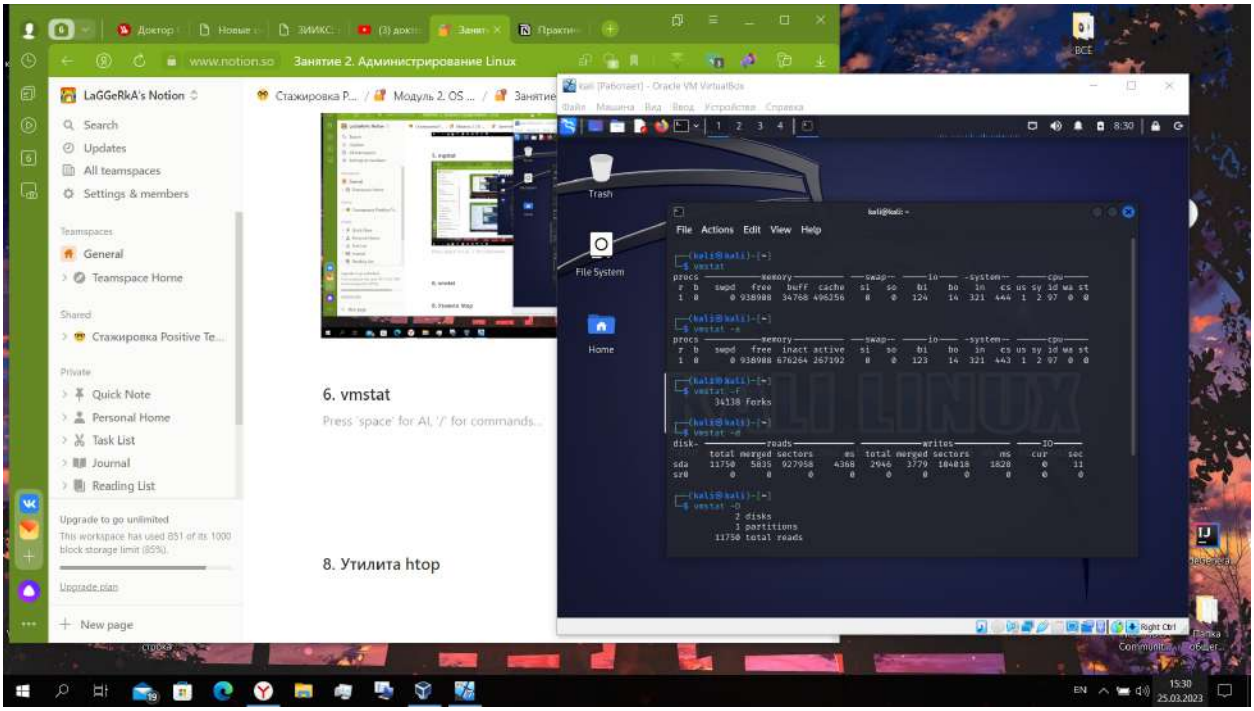

www.notion.so
Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
Teamspaces
General
Teamspace Home
Shared
Стажировка Positive Te...
Private
Quick Note
Personal Home
Task List
Journal
Reading List
Upgrade to go unlimited
This workspace has used 851 of its 1000 block storage limit (85%).
Upgrade plan
New page
5. mpstat
6. vmstat

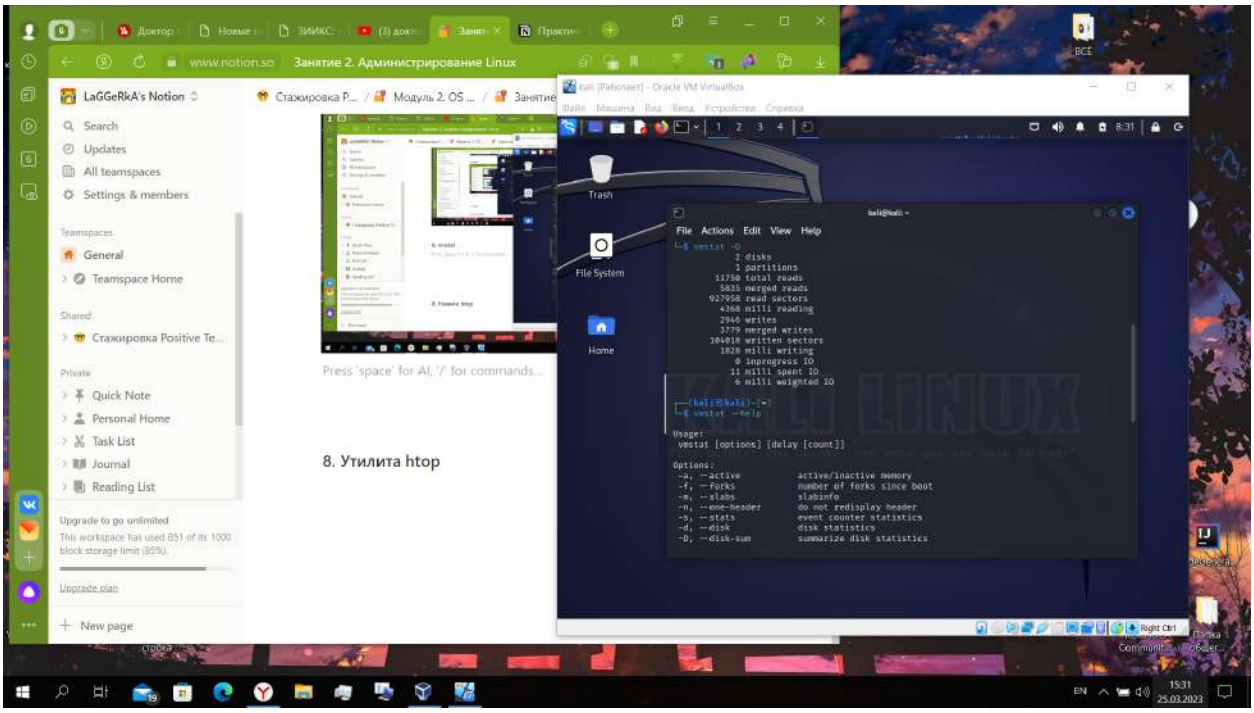
5. mpstat


www.notion.so
Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
General
Teamspace Home
Стажировка Positive Te...
Quick Note
Personal Home
Task List
Journal
Reading List
New page
Trash
File System
Home
File Actions Edit View Help

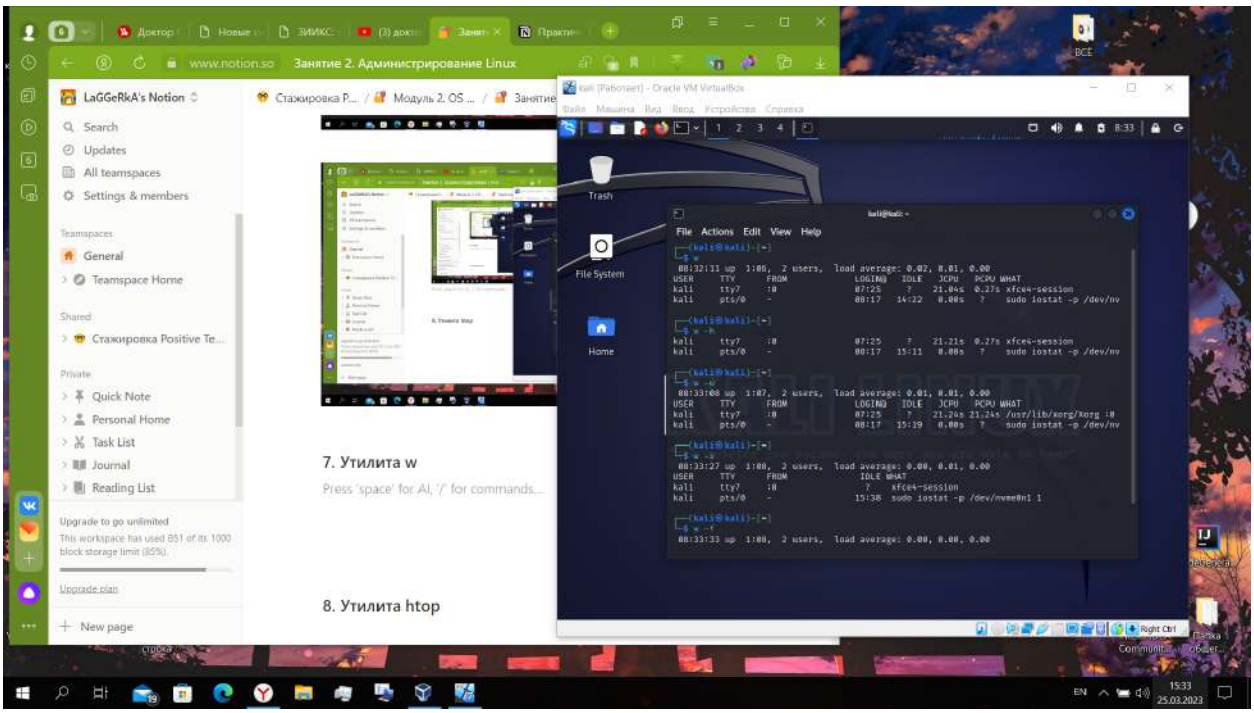

www.notion.so
Занятие 2. Администрирование Linux
LaGGeRkA's Notion
5. mpstat
6. vmstat
8. Утилита htop
Trash
File System
Home
File Actions Edit View Help

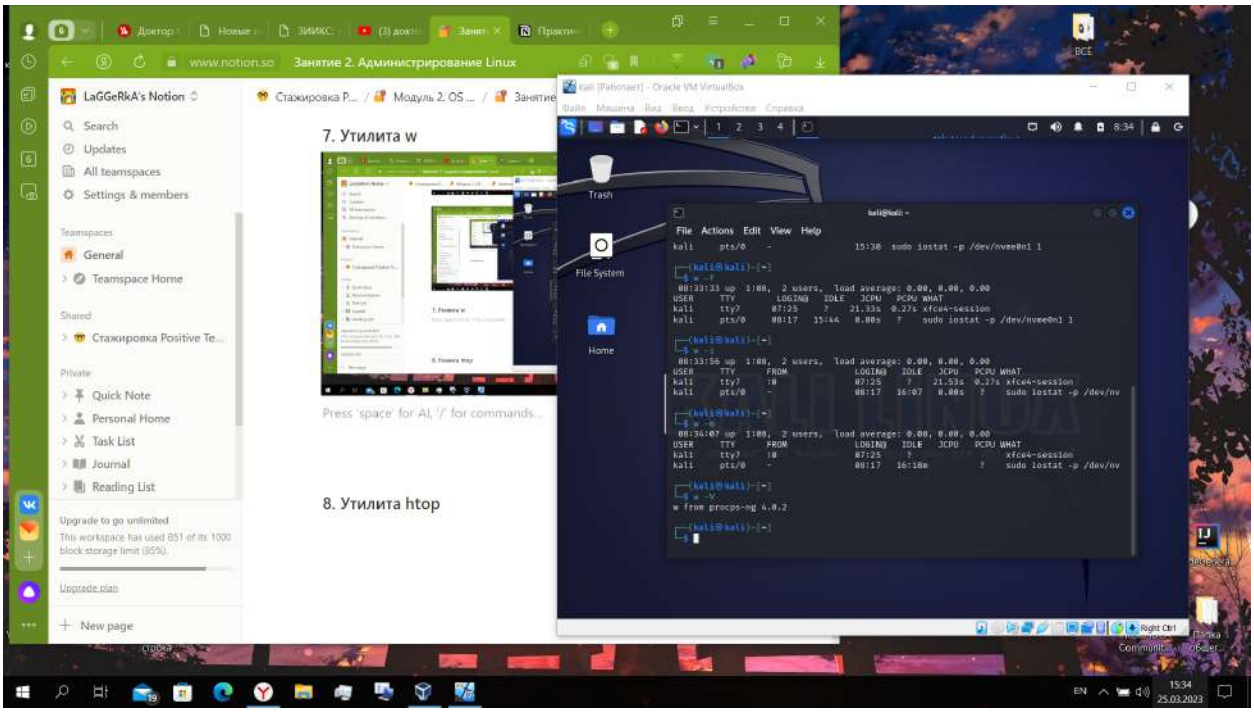
6. vmstat


www.notion.so
Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
Teamspaces
General
Teamspace Home
Shared
Стажировка Positive Te...
Private
Quick Note
Personal Home
Task List
Journal
Reading List
Upgrade to go unlimited
Upgrade plan
New page
6. vmstat
Press 'space' for AI, '/' for commands...
8. Утилита htop
Trash
File System
Home
File Actions Edit View Help
34138 forks
2 disks
3 partitions
11750 total reads

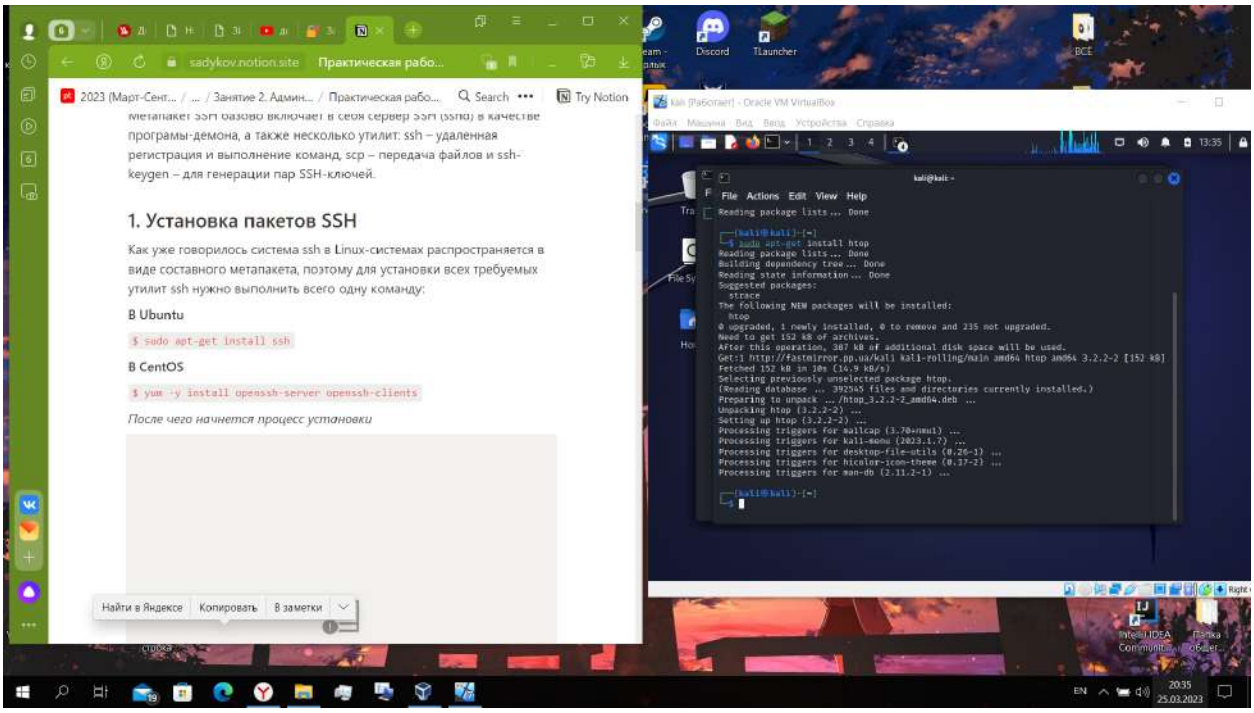

Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
General
Teamspace Home
Quick Note
Personal Home
Task List
Journal
Reading List
New page
8. Утилита htop

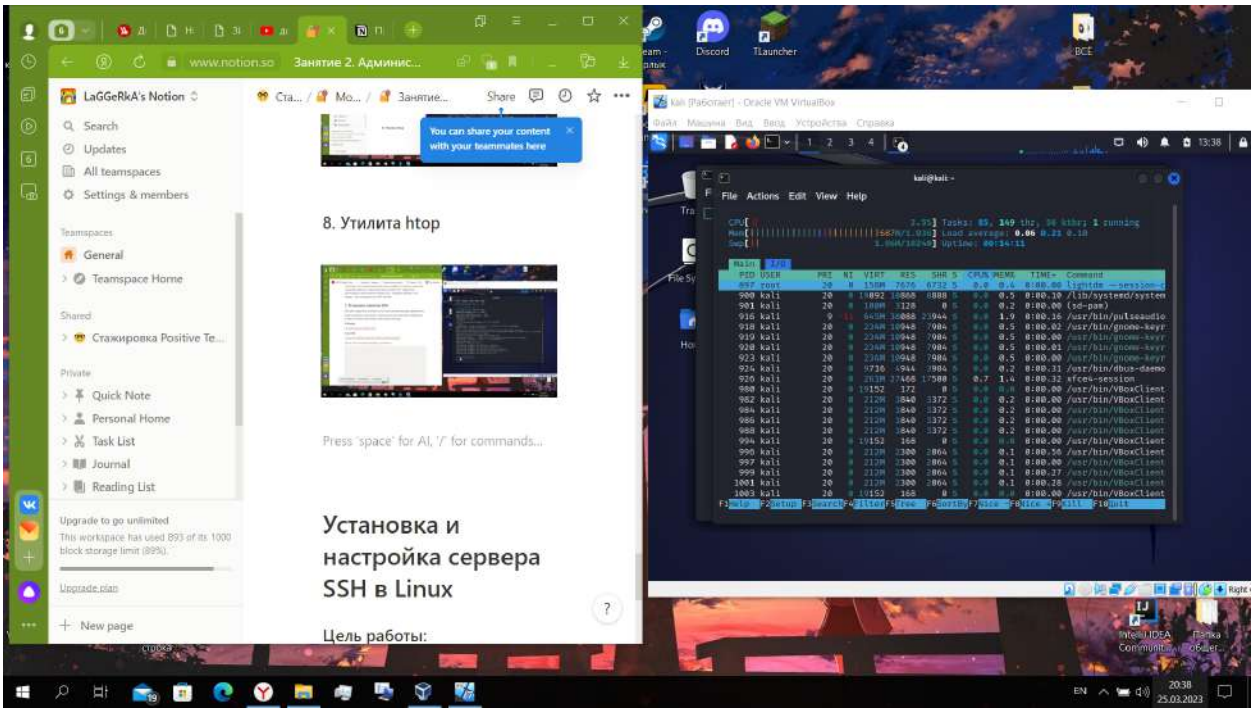
7. Утилита w

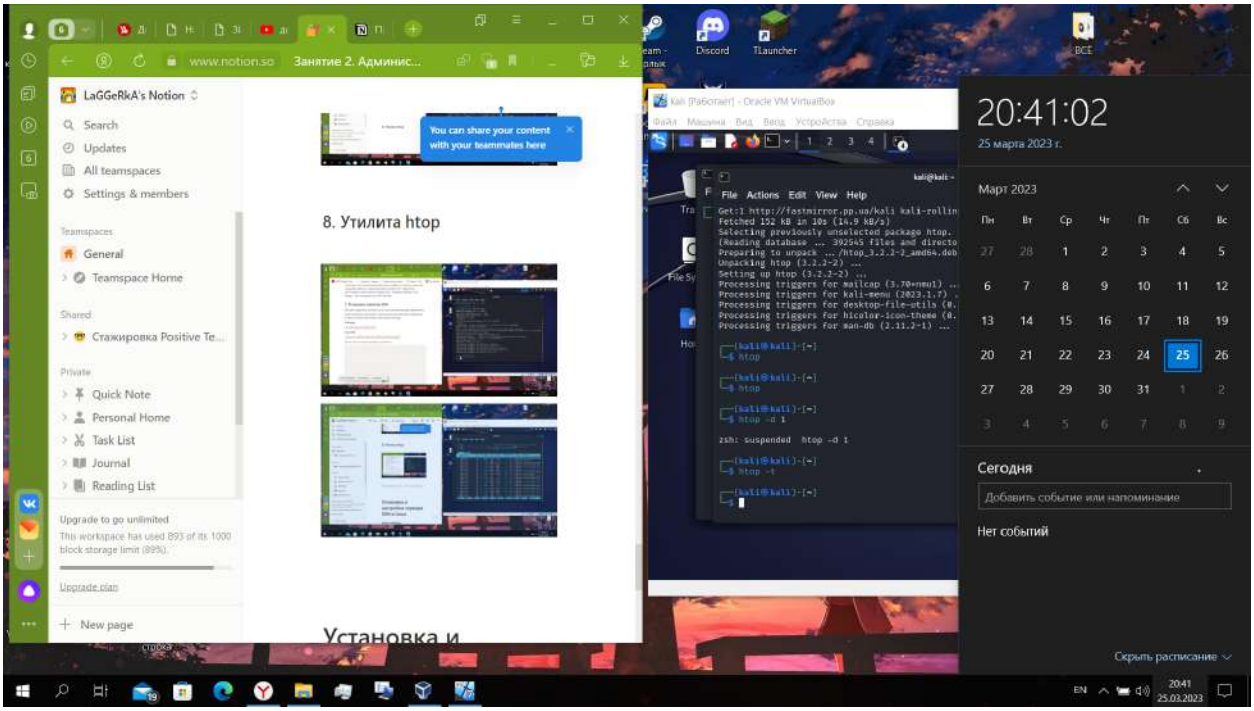

Занятие 2. Администрирование Linux
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
General
Teamspace Home
Quick Note
Personal Home
Task List
Journal
Reading List
New page
7. Утилита w
8. Утилита htop



8. Утилита htop







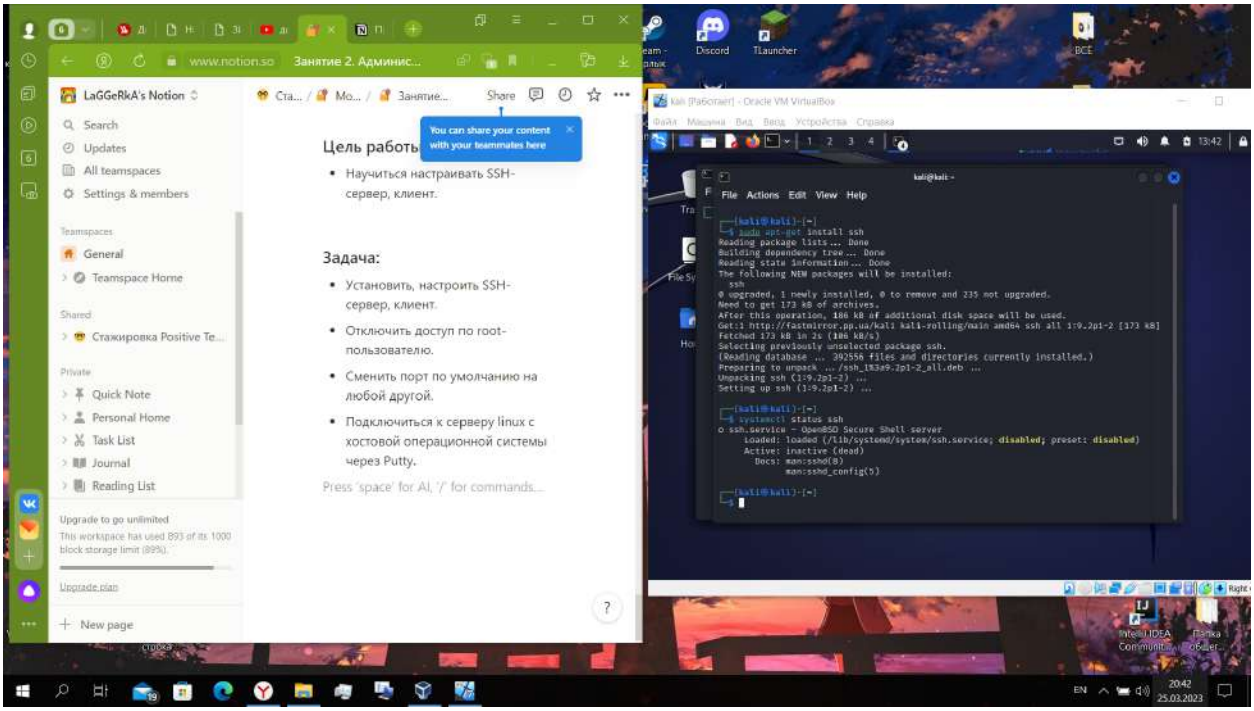
Установка и настройка сервера SSH в Linux

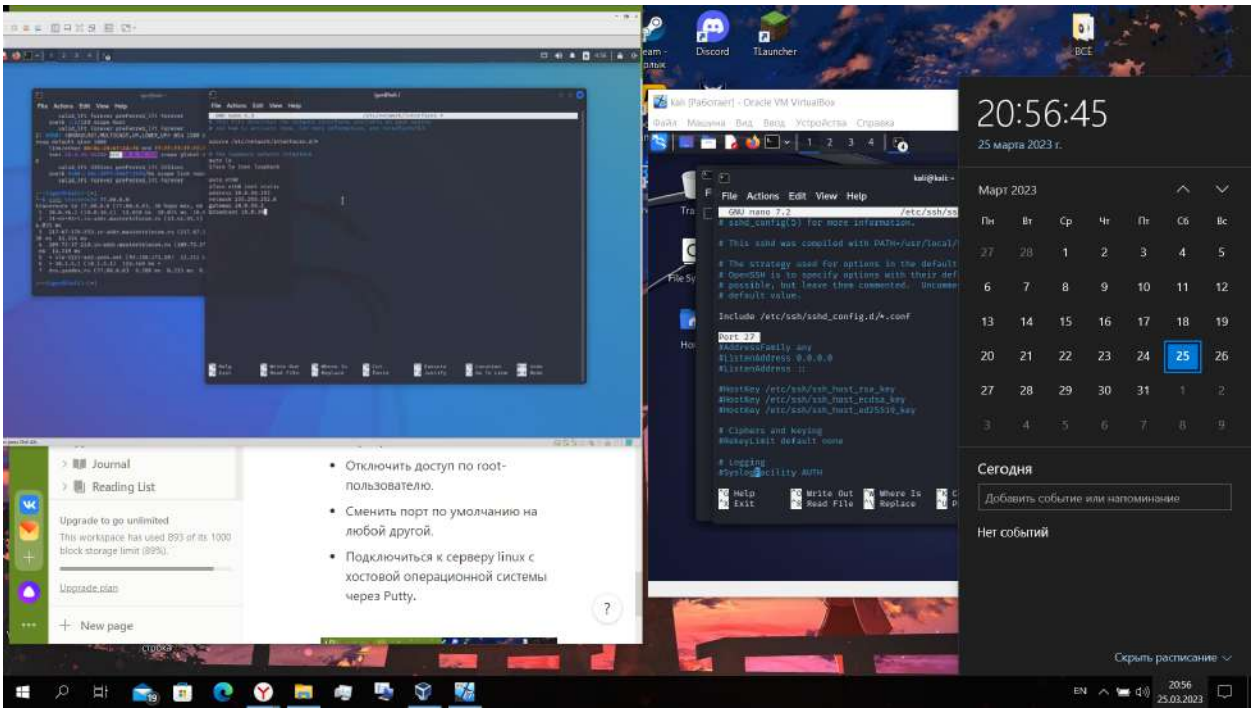
Цель работы:

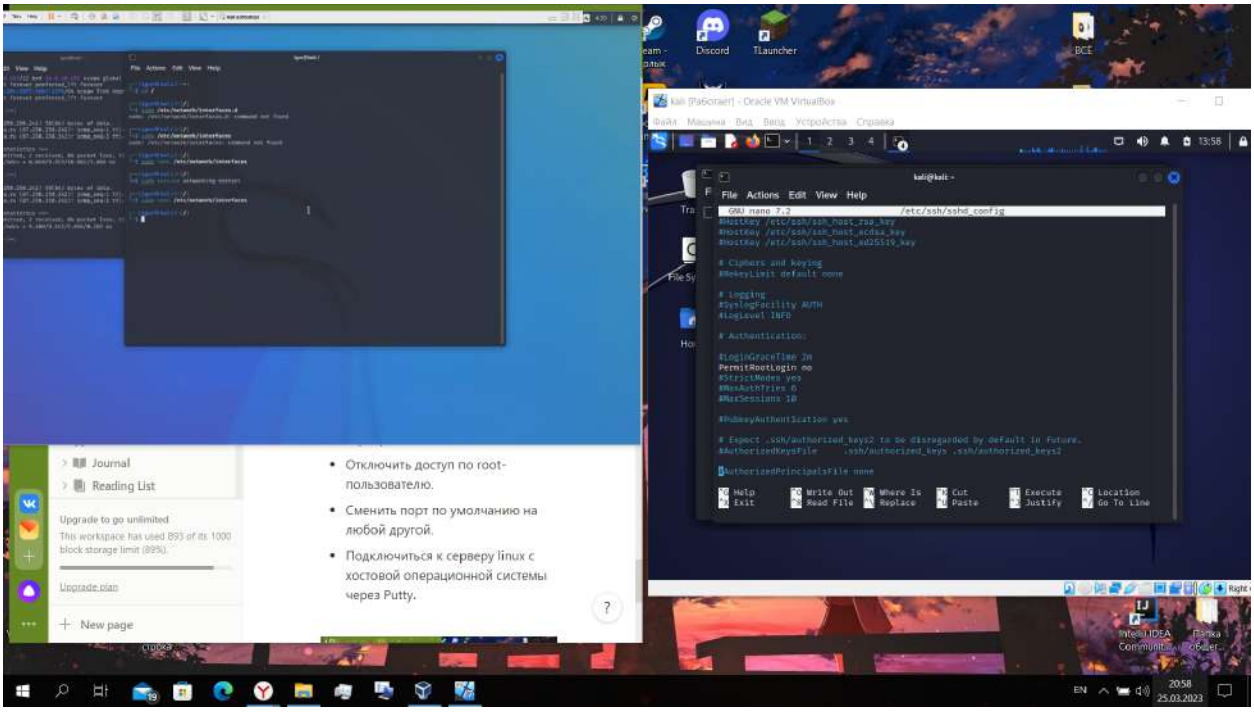
- Научиться настраивать SSH-сервер, клиент.

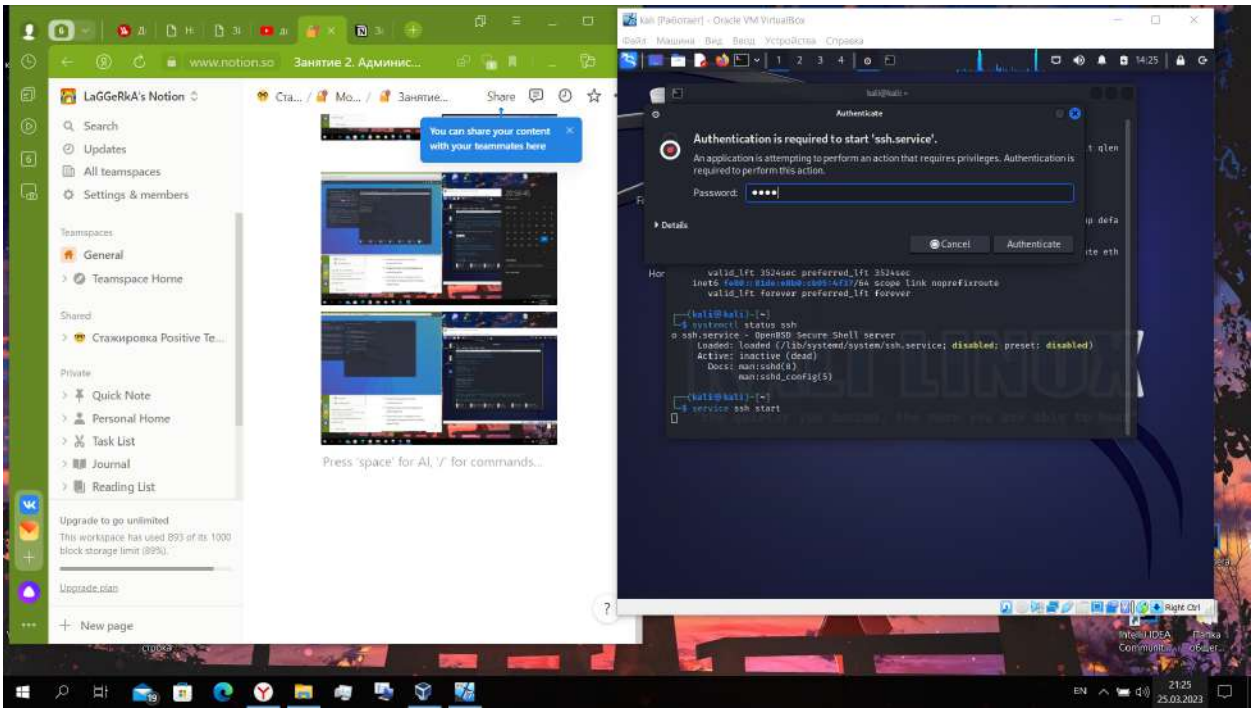
Задача:

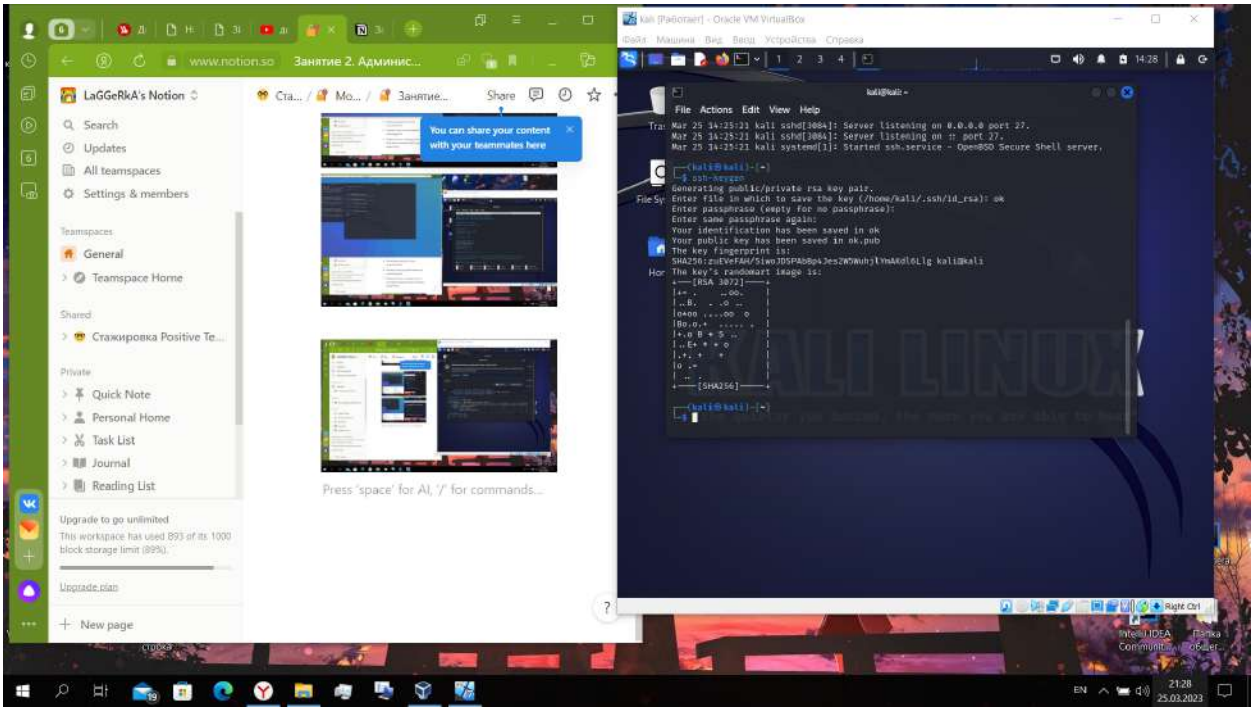
- Установить, настроить SSH-сервер, клиент.
- Отключить доступ по root-пользователю.
- Сменить порт по умолчанию на любой другой.
- Подключиться к серверу linux с хостовой операционной системы через Putty.

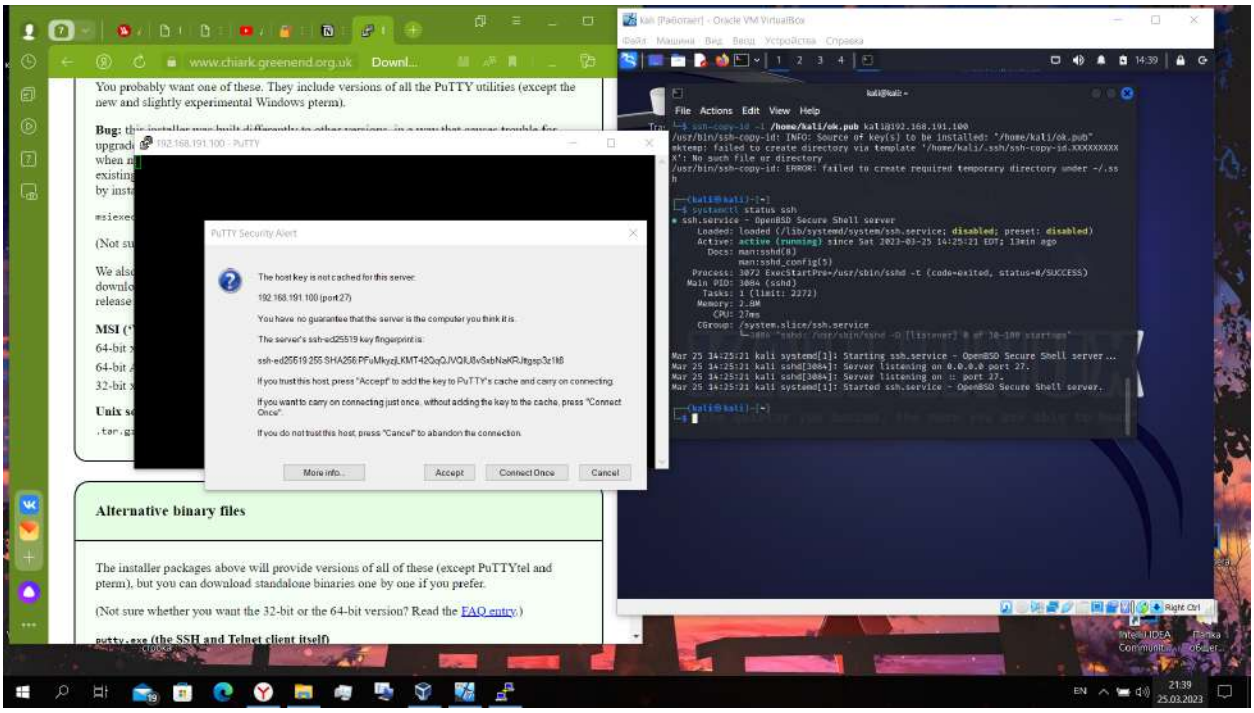


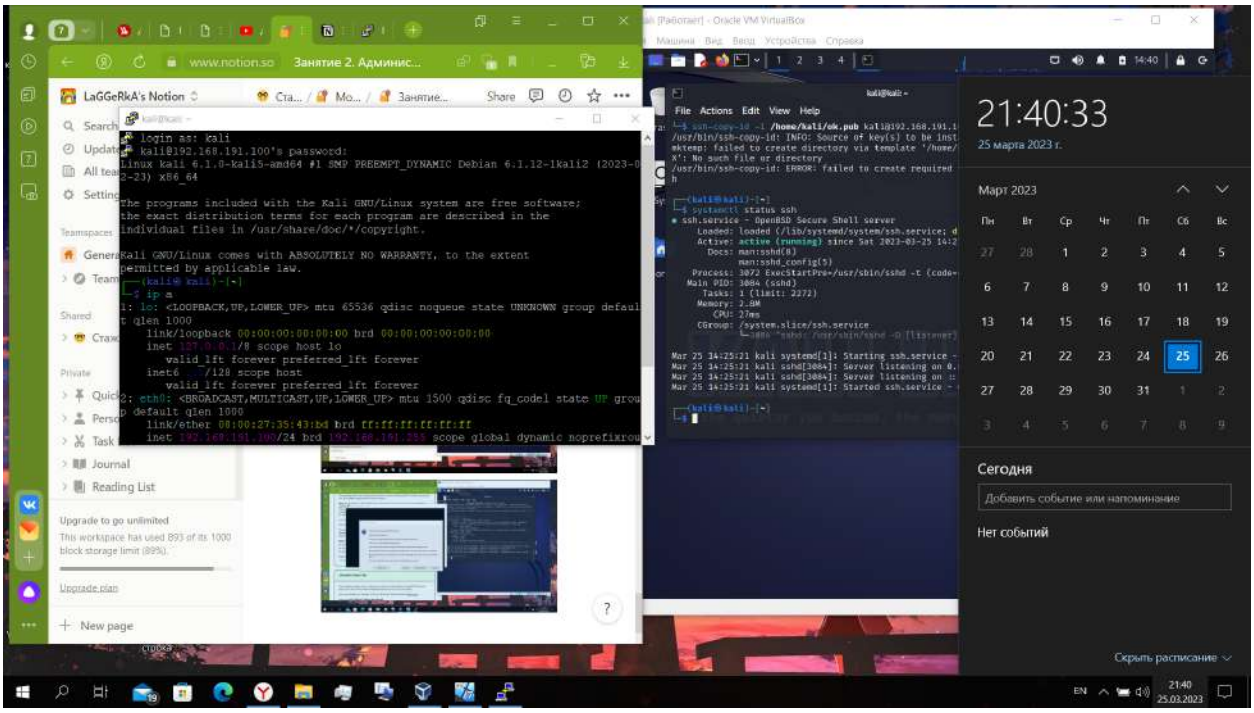

Journal
Reading List
Upgrade to go unlimited
This workspace has used 893 of its 1000 block storage limit (89%).
Upgrade plan
New page
• Отключить доступ по root-пользователю.
• Сменить порт по умолчанию на любой другой.
• Подключиться к серверу linux с хостовой операционной системы через Putty.
20:56:45
25 марта 2023 г.
Март 2023
Сегодня
Добавить событие или напоминание
Нет событий
Скрыть расписание


Journal
Reading List
Upgrade to go unlimited
This workspace has used 893 of its 1000 block storage limit (89%).
Upgrade plan
New page
• Отключить доступ по root-пользователю.
• Сменить порт по умолчанию на любой другой.
• Подключиться к серверу linux с хостовой операционной системы через Putty.


Занятие 2. Администр...
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
General
Teamspace Home
Quick Note
Personal Home
Task List
Journal
Reading List
New page
You can share your content with your teammates here
Press 'space' for AI, '/' for commands...
Authentication is required to start 'ssh.service'.
An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.
Password:
Cancel
Authenticate
service ssh start


Занятие 2. Администр...
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
General
Teamspace Home
Quick Note
Personal Home
Task List
Journal
Reading List
New page
You can share your content with your teammates here
Press 'space' for AI, '/' for commands...
ssh-keygen
Generating public/private rsa key pair.
Your identification has been saved in ok
Your public key has been saved in ok.pub
The key fingerprint is:
The key's randomart image is:


www.chiark.greenend.org.uk
You probably want one of these. They include versions of all the PuTTY utilities (except the new and slightly experimental Windows pterm).
PuTTY Security Alert
The host key is not cached for this server:
192.168.191.100 (port 27)
You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:PFuMkyzjLKMT42QcQJVQILl0vSxbNaKFJtgsp3z1h8
If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".
If you do not trust this host, press "Cancel" to abandon the connection.
More info...
Accept
Connect Once
Cancel
Alternative binary files
The installer packages above will provide versions of all of these (except PuTTYtel and pterm), but you can download standalone binaries one by one if you prefer.
(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)
putty.exe (the SSH and Telnet client itself)
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
systemctl status ssh
ssh.service - OpenBSD Secure Shell server
Mar 25 14:25:21 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Mar 25 14:25:21 kali sshd[3084]: Server listening on 0.0.0.0 port 27.
Mar 25 14:25:21 kali sshd[3084]: Server listening on :: port 27.
Mar 25 14:25:21 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.


www.notion.so
Занятие 2. Администр...
LaGGeRkA's Notion
login as: kali
kali@192.168.191.100's password:
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
21:40:33
25 марта 2023 г.
Март 2023
Сегодня
Добавить событие или напоминание
Нет событий
Скрыть расписание
Journal
Reading List
New page

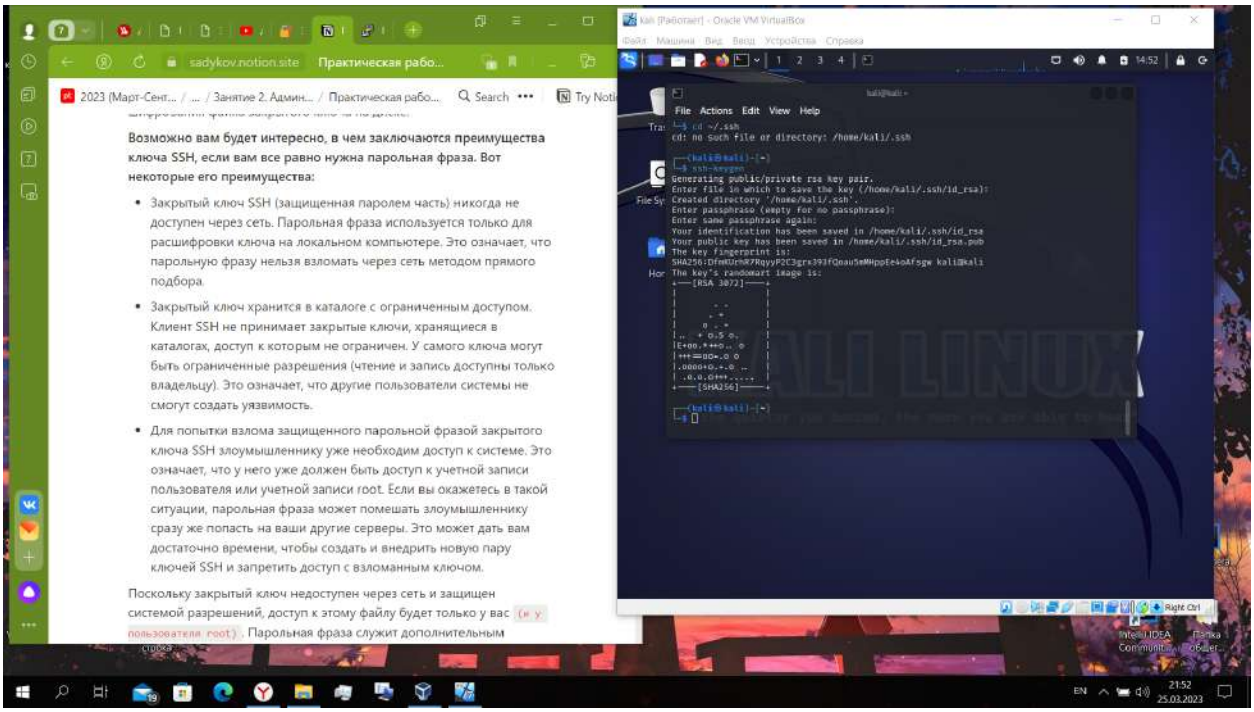
Практическая работа "Установка и настройка SSH-authorized_keys"

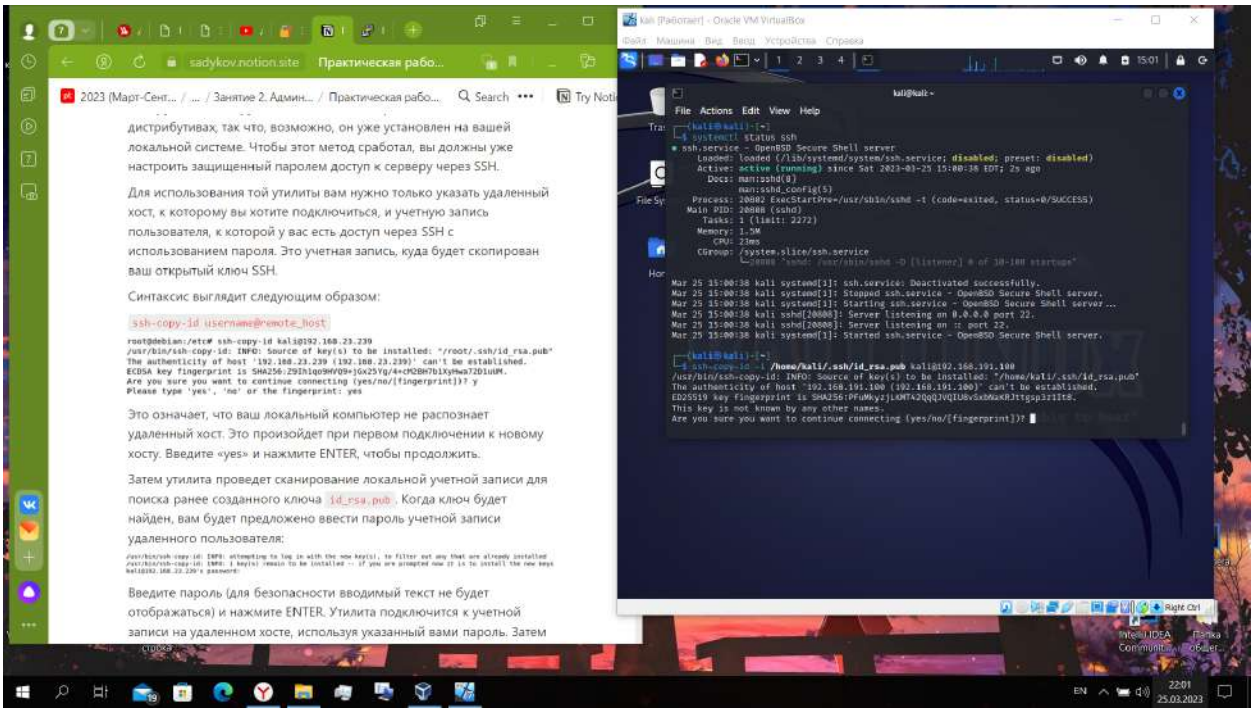
Цель работы:

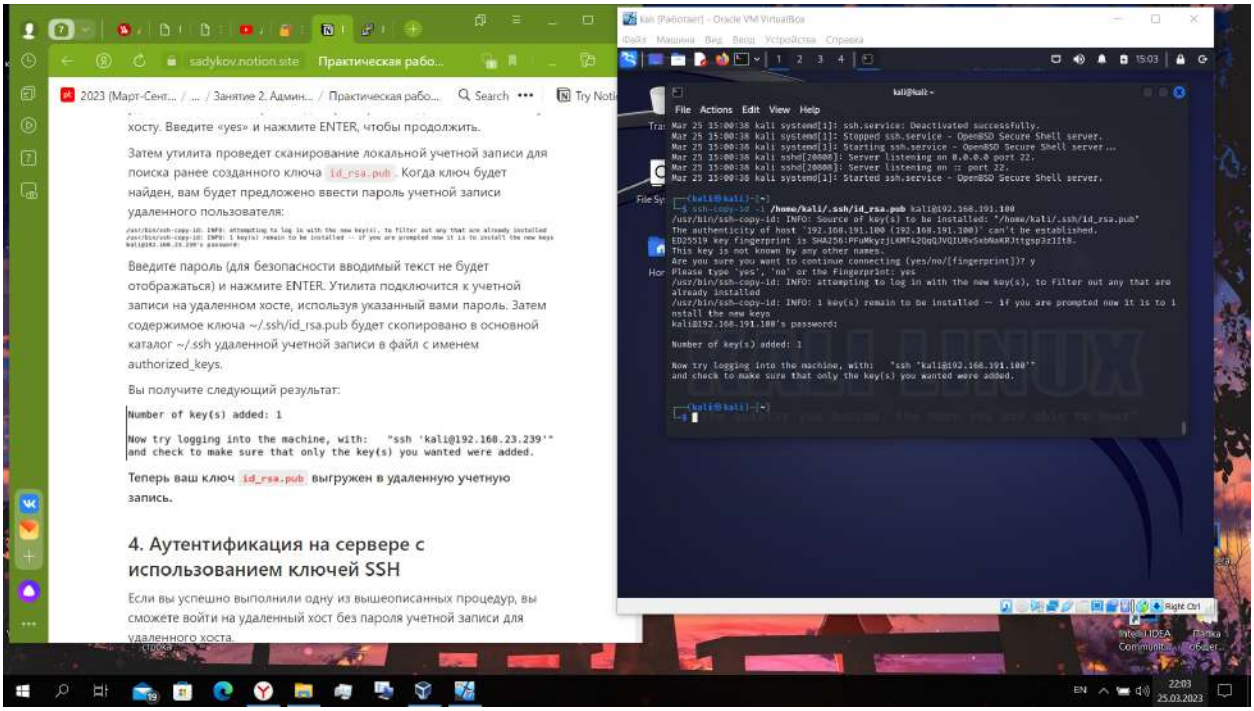
- научиться настраивать SSH-authorized_keys.
- научиться работать с ключами SSH.

Задача:

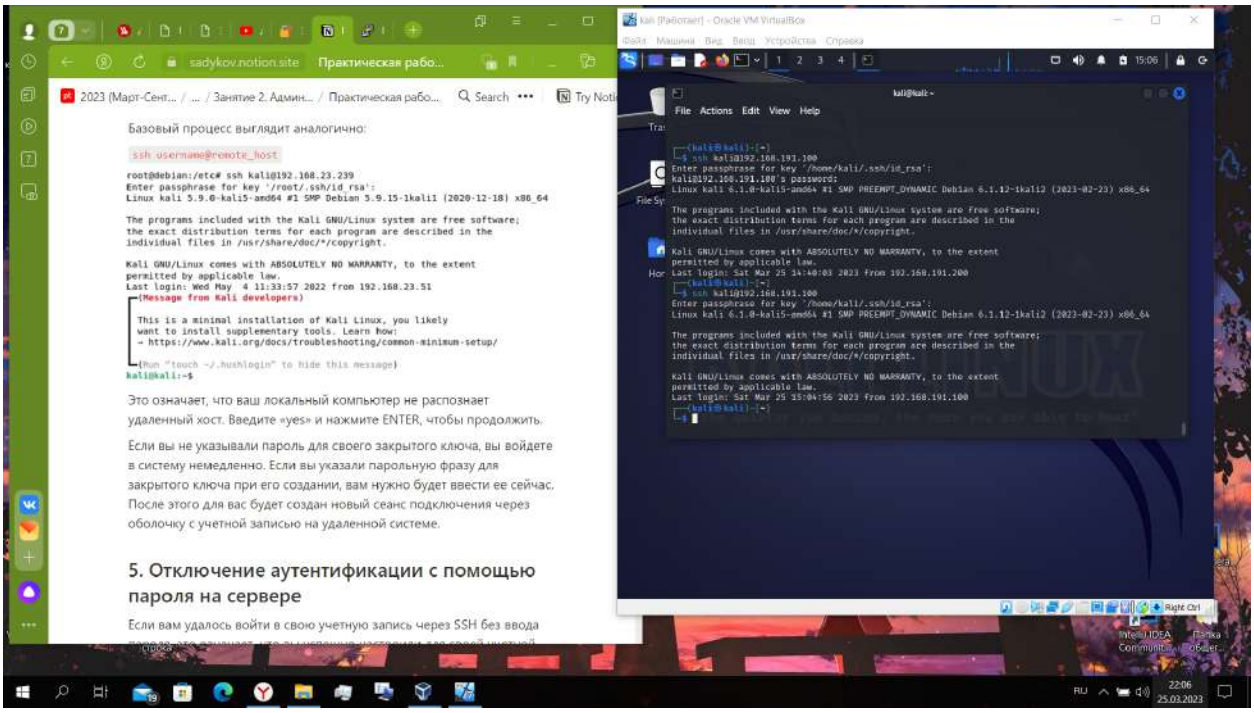
- Разобраться как работает доступ по ключам.
- Организовать аутентификацию к серверу linux через ключи.
- Организовать аутентификацию к серверу linux через ключи без пароля.







Выгрузка открытого ключа в удалённый аккаунт



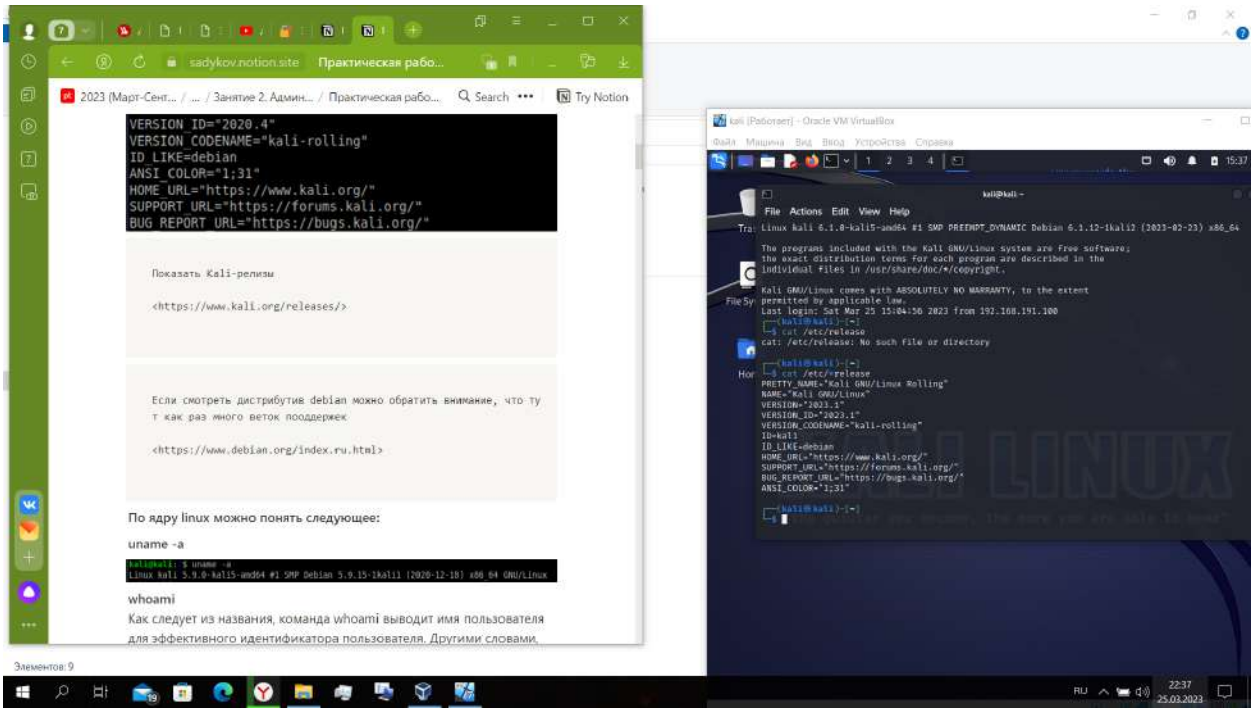
Практическая работа "Сбор информации о Linux и WGET"

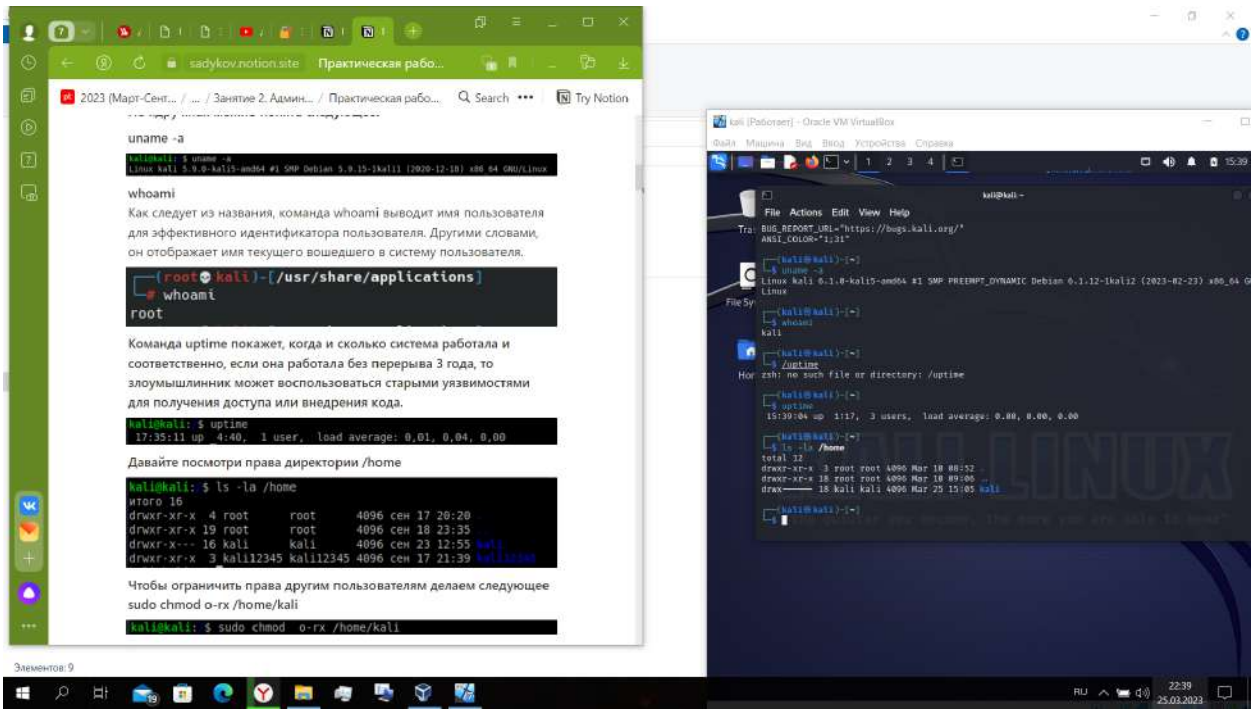
Цель работы:

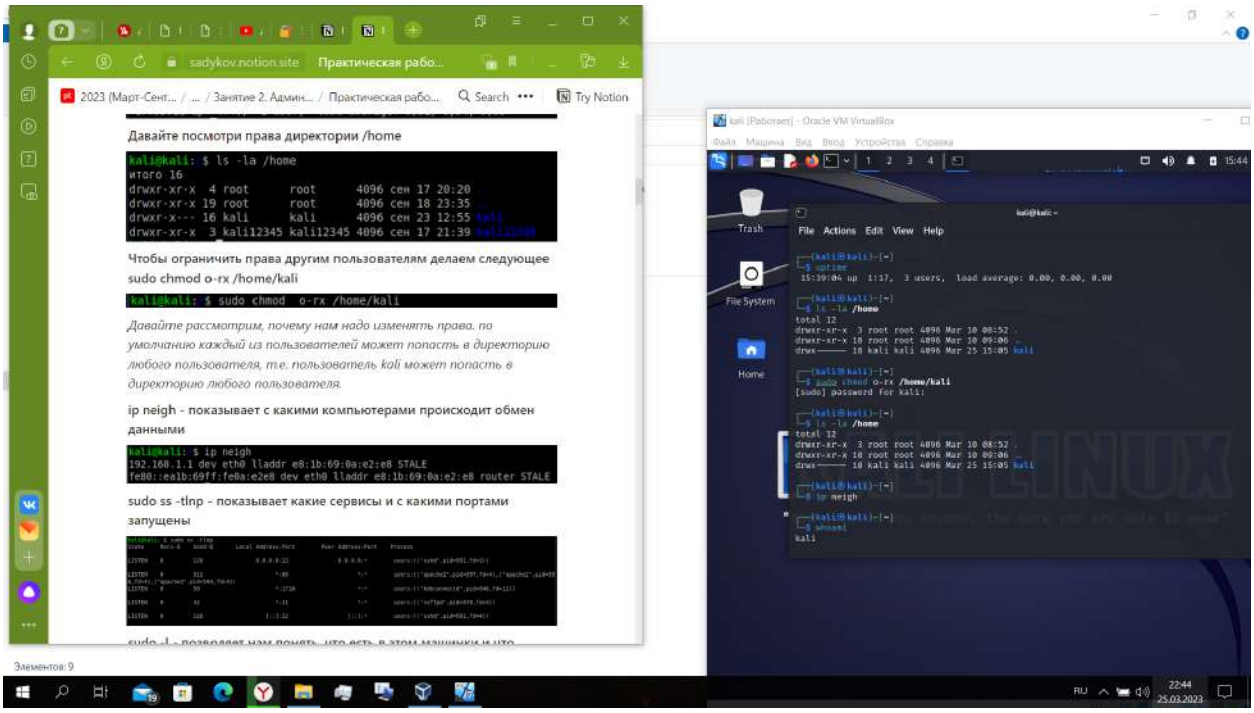
- Научиться базовому сбору информации о Linux системах.

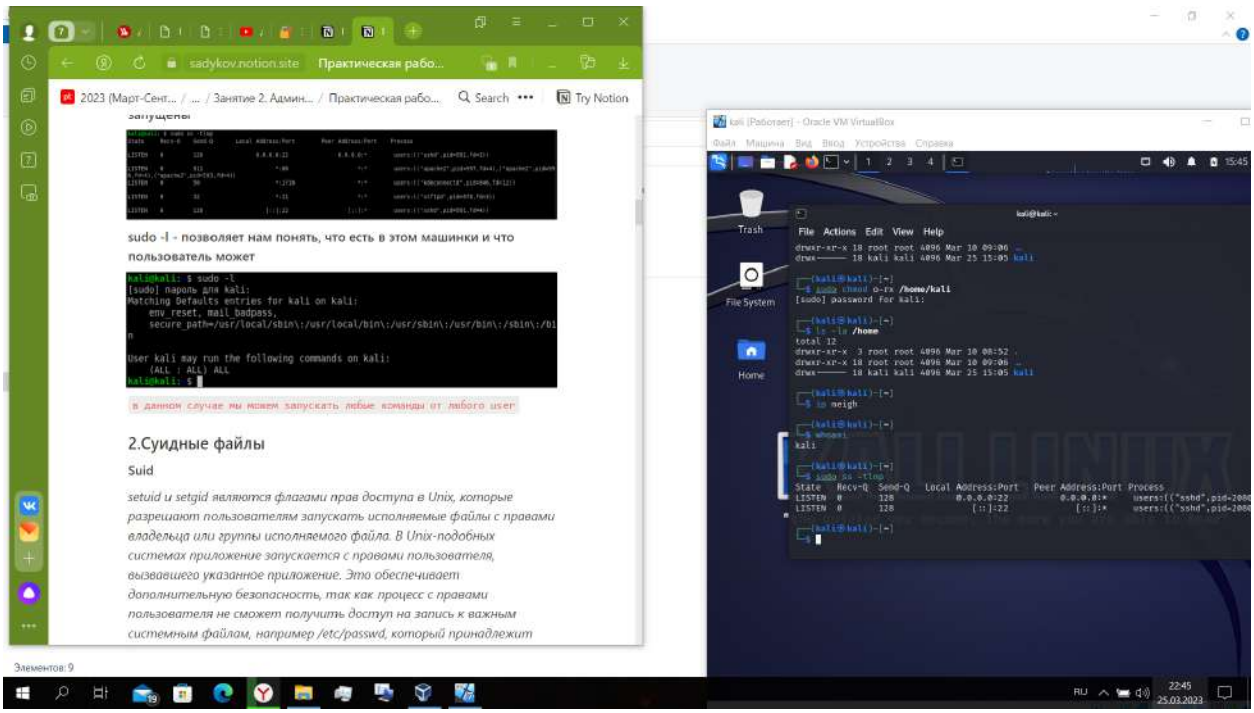
Задача:

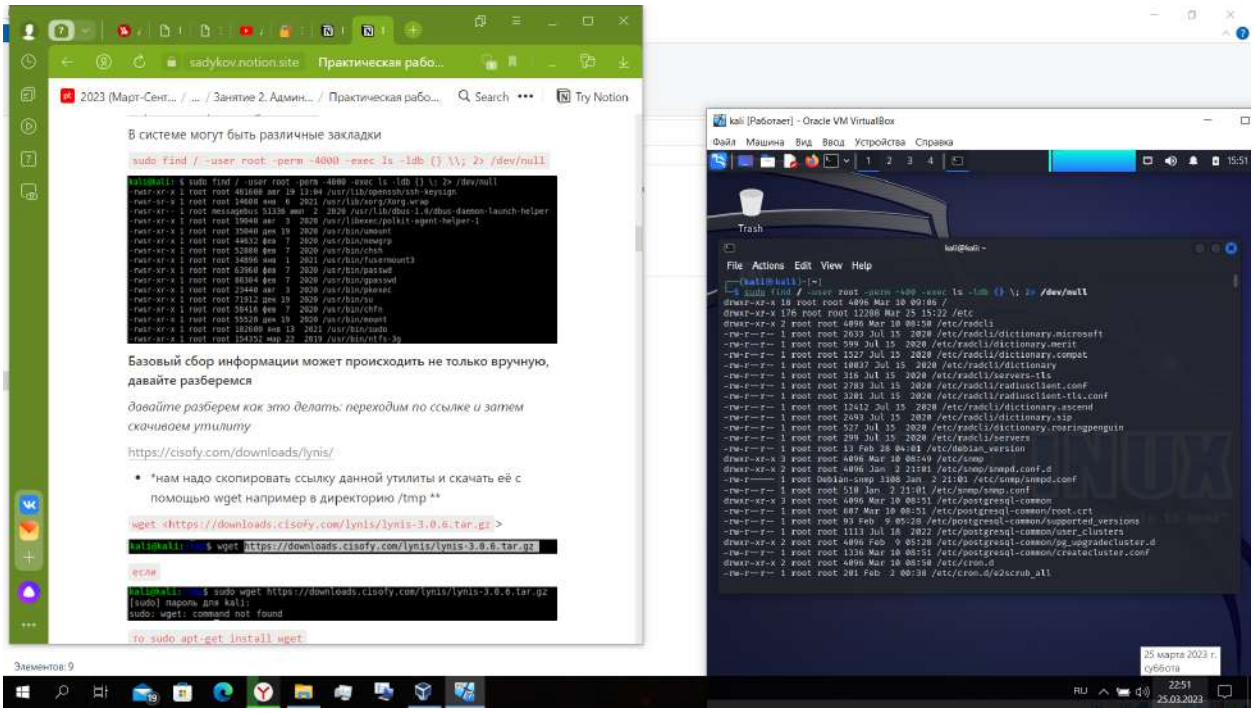
- Научитесь скачивать файлы с помощью утилиты wget.
- Научиться проверять пакеты на целостность.

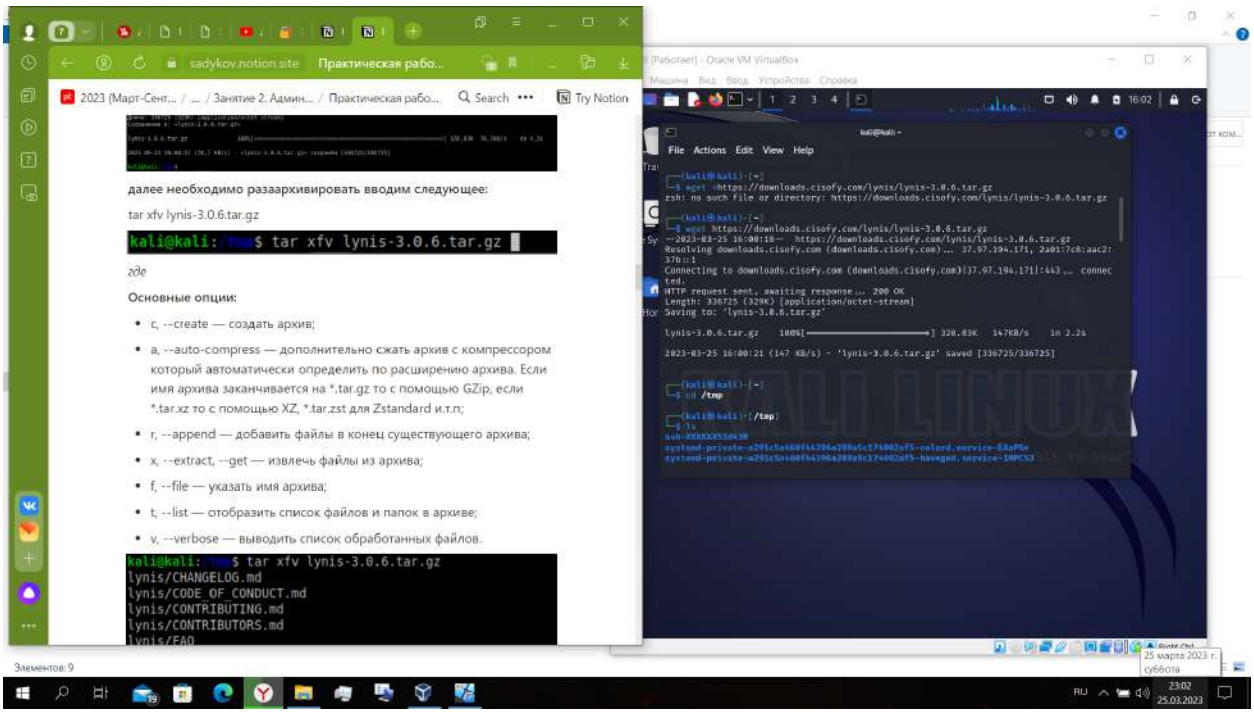

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
VERSION_ID="2020.4"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
Показать Kali-релизы
<https://www.kali.org/releases/>
Если смотреть дистрибутив debian можно обратить внимание, что ту
т как раз много веток поддержек
<https://www.debian.org/index.ru.html>
По ядру linux можно понять следующее:
uname -a
whoami
Как следует из названия, команда whoami выводит имя пользователя
для эффективного идентификатора пользователя. Другими словами,
Элементов: 9
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
cat /etc/release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION="2023.1"
VERSION_ID="2023.1"
VERSION_CODENAME="kali-rolling"
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
RU
22:37
25.03.2023

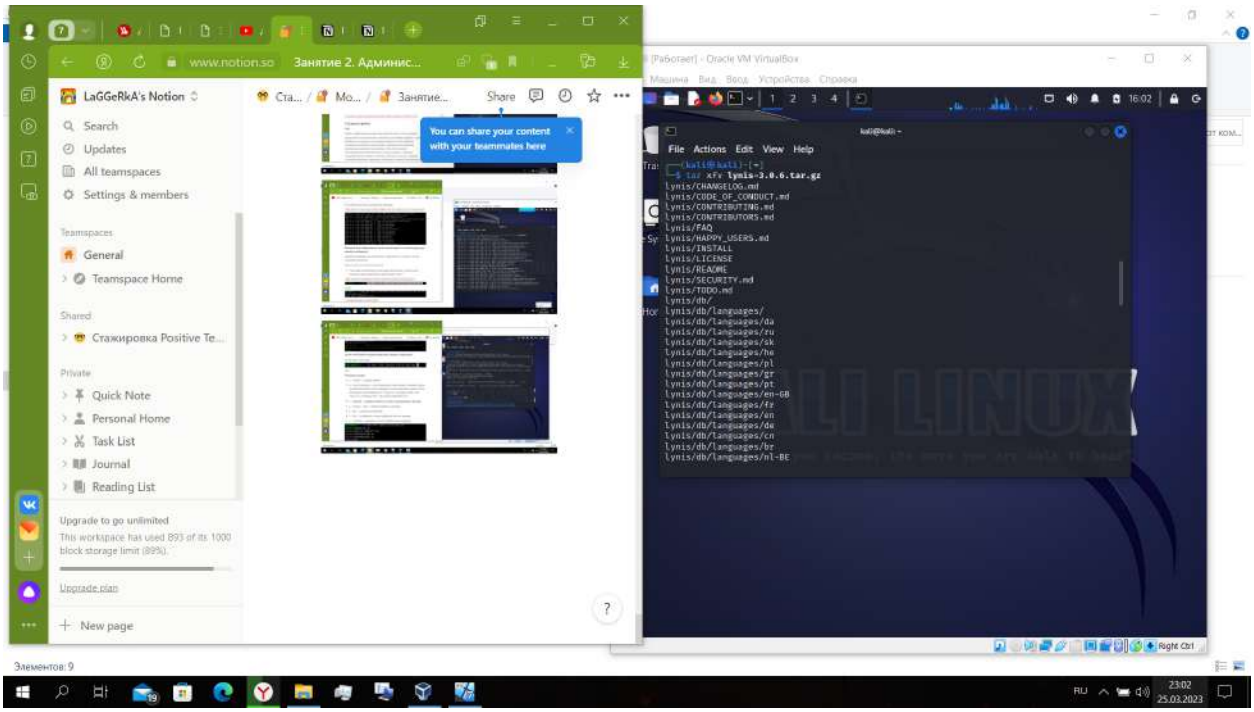

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
uname -a
whoami
Как следует из названия, команда whoami выводит имя пользователя
для эффективного идентификатора пользователя. Другими словами,
он отображает имя текущего вошедшего в систему пользователя.
root
Команда uptime покажет, когда и сколько система работала и
соответственно, если она работала без перерыва 3 года, то
злоумышлинник может воспользоваться старыми уязвимостями
для получения доступа или внедрения кода.
kali@kali: $ uptime
17:35:11 up 4:40, 1 user, load average: 0,01, 0,04, 0,00
Давайте посмотри права директории /home
kali@kali: $ ls -la /home
итого 16
drwxr-xr-x 4 root root 4096 сен 17 20:20
drwxr-xr-x 19 root root 4096 сен 18 23:35
drwxr-x--- 16 kali kali 4096 сен 23 12:55 kali
drwxr-xr-x 3 kali12345 kali12345 4096 сен 17 21:39 kali12345
Чтобы ограничить права другим пользователям делаем следующее
sudo chmod o-rx /home/kali
kali@kali: $ sudo chmod o-rx /home/kali
Элементов: 9
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
Linux kali 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23) x86_64 G
Linux
kali
zsh: no such file or directory: /uptime
15:39:04 up 1:17, 3 users, load average: 0.08, 0.00, 0.00
total 12
drwxr-xr-x 3 root root 4096 Mar 10 08:52 .
drwxr-xr-x 18 root root 4096 Mar 10 09:00 ..
drwx------ 18 kali kali 4096 Mar 25 15:05 kali
RU
22:39
25.03.2023

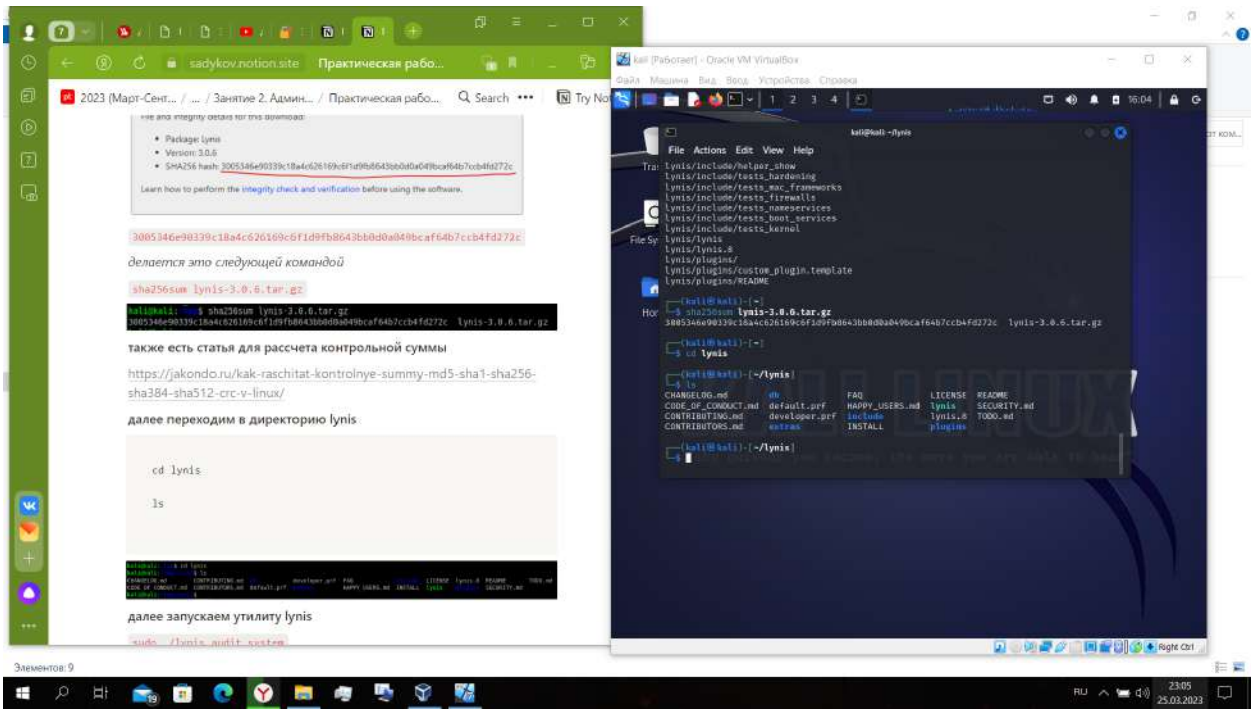

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
Давайте посмотри права директории /home
kali@kali: $ ls -la /home
итого 16
drwxr-xr-x 4 root   root   4096 сен 17 20:20
drwxr-xr-x 19 root   root   4096 сен 18 23:35
drwxr-x--- 16 kali   kali   4096 сен 23 12:55 kali
drwxr-xr-x 3 kali12345 kali12345 4096 сен 17 21:39 kali12345
Чтобы ограничить права другим пользователям делаем следующее
sudo chmod o-rx /home/kali
kali@kali: $ sudo chmod o-rx /home/kali
Давайте рассмотрим, почему нам надо изменять права. по умолчанию каждый из пользователей может попасть в директорию любого пользователя, т.е. пользователь kali может попасть в директорию любого пользователя.
ip neigh - показывает с какими компьютерами происходит обмен данными
kali@kali: $ ip neigh
192.168.1.1 dev eth0 lladdr e8:1b:69:0a:e2:e8 STALE
fe80::ea1b:69ff:fe8a:e2e8 dev eth0 lladdr e8:1b:69:0a:e2:e8 router STALE
sudo ss -tlnp - показывает какие сервисы и с какими портами запущены
Элементов: 9
kali (Работает) - Oracle VM VirtualBox
Trash
File System
Home
File Actions Edit View Help
kali@kali: ~
15:20:04 up 1:17, 3 users, load average: 0.00, 0.00, 0.00
[sudo] password for kali:
kali
RU
22:44
25.03.2023

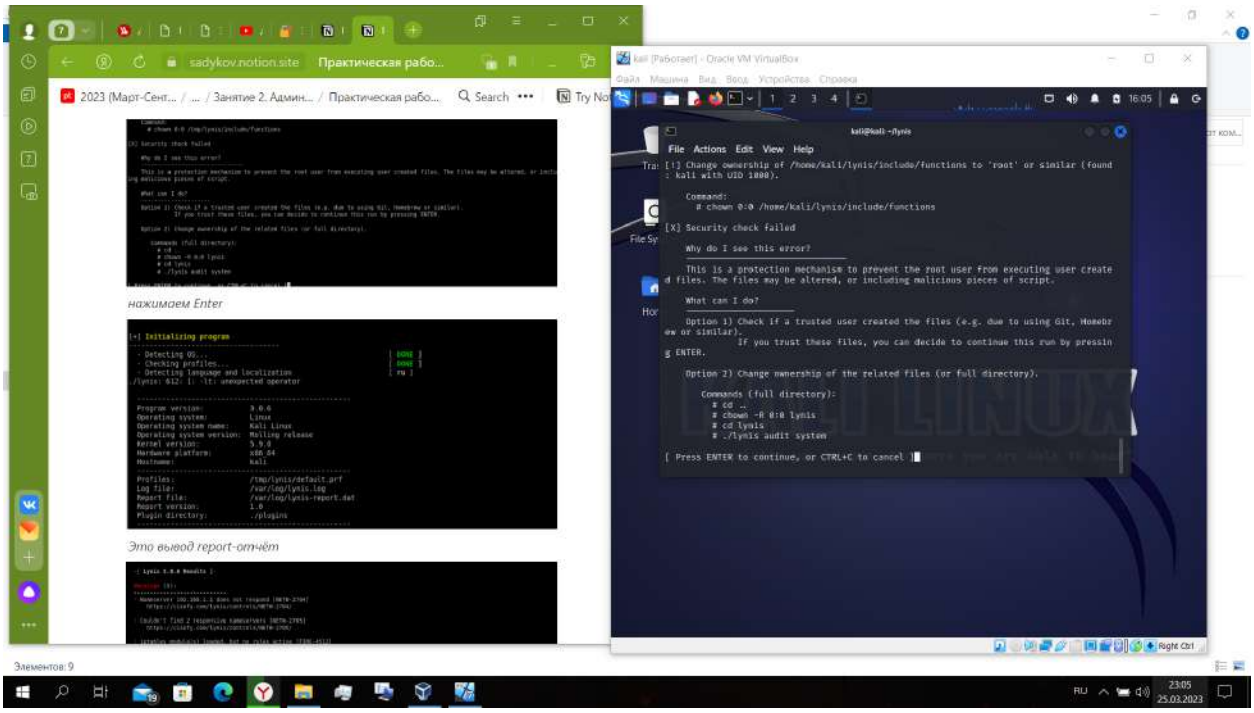

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
sudo -l - позволяет нам понять, что есть в этом машинки и что пользователь может
kali@kali: $ sudo -l
[sudo] пароль для kali:
Matching Defaults entries for kali on kali:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User kali may run the following commands on kali:
(ALL : ALL) ALL
kali@kali: $
в данном случае мы можем запускать любые команды от любого user
2.Суидные файлы
Suid
setuid и setgid являются флагами прав доступа в Unix, которые разрешают пользователям запускать исполняемые файлы с правами владельца или группы исполняемого файла. В Unix-подобных системах приложение запускается с правами пользователя, вызвавшего указанное приложение. Это обеспечивает дополнительную безопасность, так как процесс с правами пользователя не сможет получить доступ на запись к важным системным файлам, например /etc/passwd, который принадлежит
Элементов: 9
kali (Работает) - Oracle VM VirtualBox
Trash
File System
Home
File Actions Edit View Help
kali@kali: ~
[sudo] password for kali:
kali
RU
22:45
25.03.2023

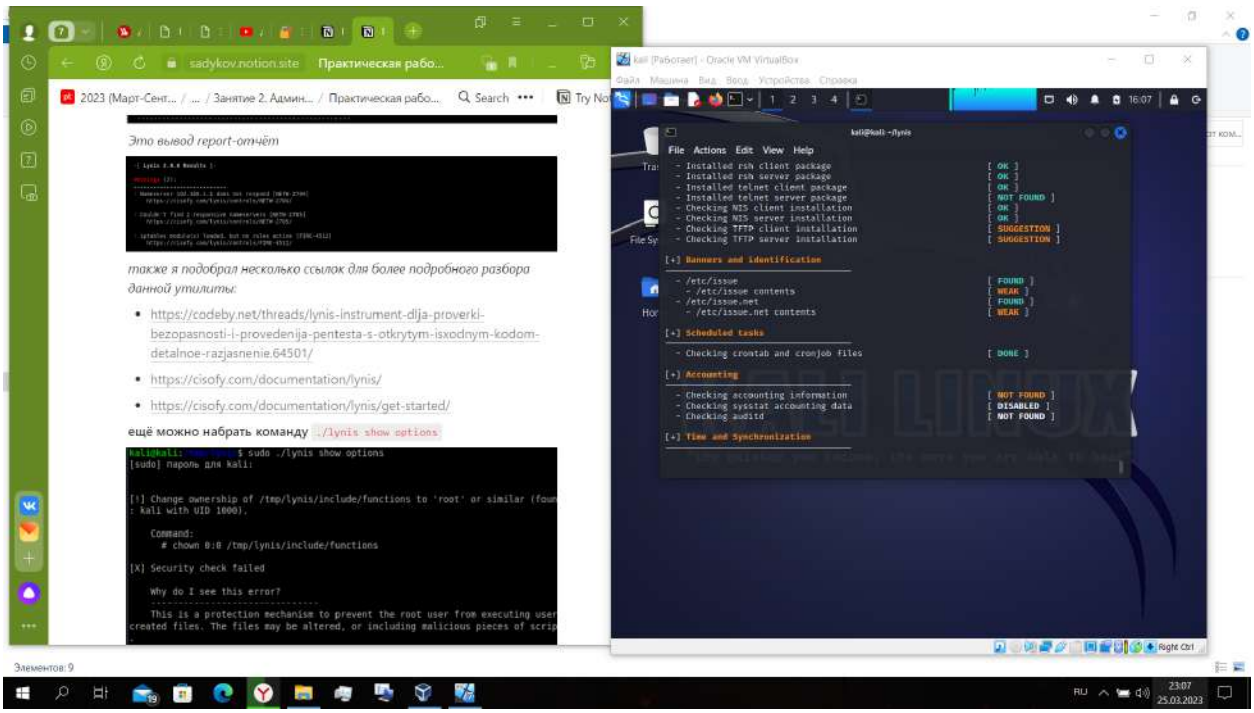

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
В системе могут быть различные закладки
sudo find / -user root -perm -4000 -exec ls -ldb {} \; 2> /dev/null
Базовый сбор информации может происходить не только вручную, давайте разберемся
давайте разберем как это делать: переходим по ссылке и затем скачиваем утилиту
https://cisofy.com/downloads/lynis/
*нам надо скопировать ссылку данной утилиты и скачать её с помощью wget например в директорию /tmp **
wget <https://downloads.cisofy.com/lynis/lynis-3.0.6.tar.gz >
kali@kali: /tmp$ wget https://downloads.cisofy.com/lynis/lynis-3.0.6.tar.gz
если
kali@kali: /tmp$ sudo wget https://downloads.cisofy.com/lynis/lynis-3.0.6.tar.gz
[sudo] пароль для kali:
sudo: wget: command not found
то sudo apt-get install wget
Элементов: 9
kali [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Trash
File Actions Edit View Help
25 марта 2023 г.
суббота
22:51
25.03.2023

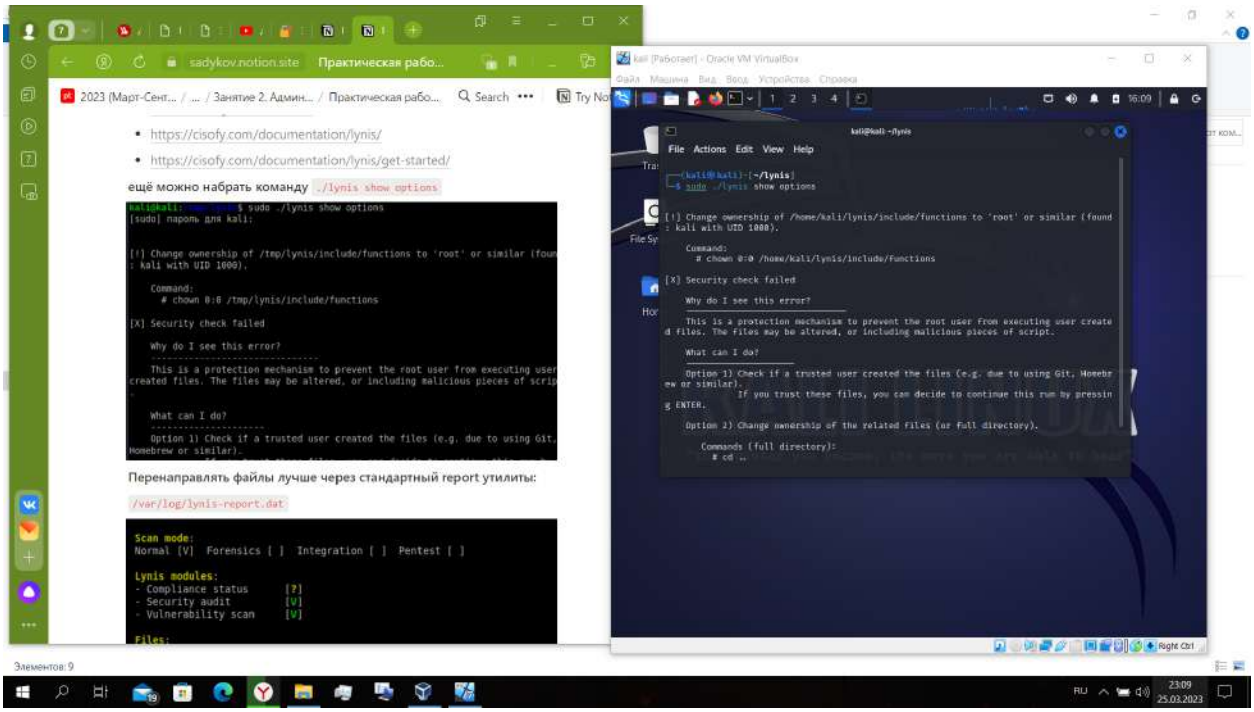

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
далее необходимо разаархивировать вводим следующее:
tar xfv lynis-3.0.6.tar.gz
kali@kali: /tmp$ tar xfv lynis-3.0.6.tar.gz
где
Основные опции:
c, --create — создать архив;
a, --auto-compress — дополнительно сжать архив с компрессором который автоматически определить по расширению архива. Если имя архива заканчивается на *.tar.gz то с помощью GZip, если *.tar.xz то с помощью XZ, *.tar.zst для Zstandard и.т.п;
r, --append — добавить файлы в конец существующего архива;
x, --extract, --get — извлечь файлы из архива;
f, --file — указать имя архива;
t, --list — отобразить список файлов и папок в архиве;
v, --verbose — выводить список обработанных файлов.
kali@kali: /tmp$ tar xfv lynis-3.0.6.tar.gz
lynis/CHANGELOG.md
lynis/CODE_OF_CONDUCT.md
lynis/CONTRIBUTING.md
lynis/CONTRIBUTORS.md
lynis/FAQ
Элементов: 9
File Actions Edit View Help
zsh: no such file or directory: https://downloads.cisofy.com/lynis/lynis-3.0.6.tar.gz
Resolving downloads.cisofy.com (downloads.cisofy.com)... 37.97.194.171, 2a01:7c8:aac2:
Connecting to downloads.cisofy.com (downloads.cisofy.com)|37.97.194.171|:443... connec
ted.
HTTP request sent, awaiting response... 200 OK
Length: 336725 (329K) [application/octet-stream]
Saving to: 'lynis-3.0.6.tar.gz'
lynis-3.0.6.tar.gz 100%[===========>] 328.83K 147KB/s in 2.2s
2023-03-25 16:00:21 (147 KB/s) - 'lynis-3.0.6.tar.gz' saved [336725/336725]
25 марта 2023 г.
суббота
23:02
25.03.2023

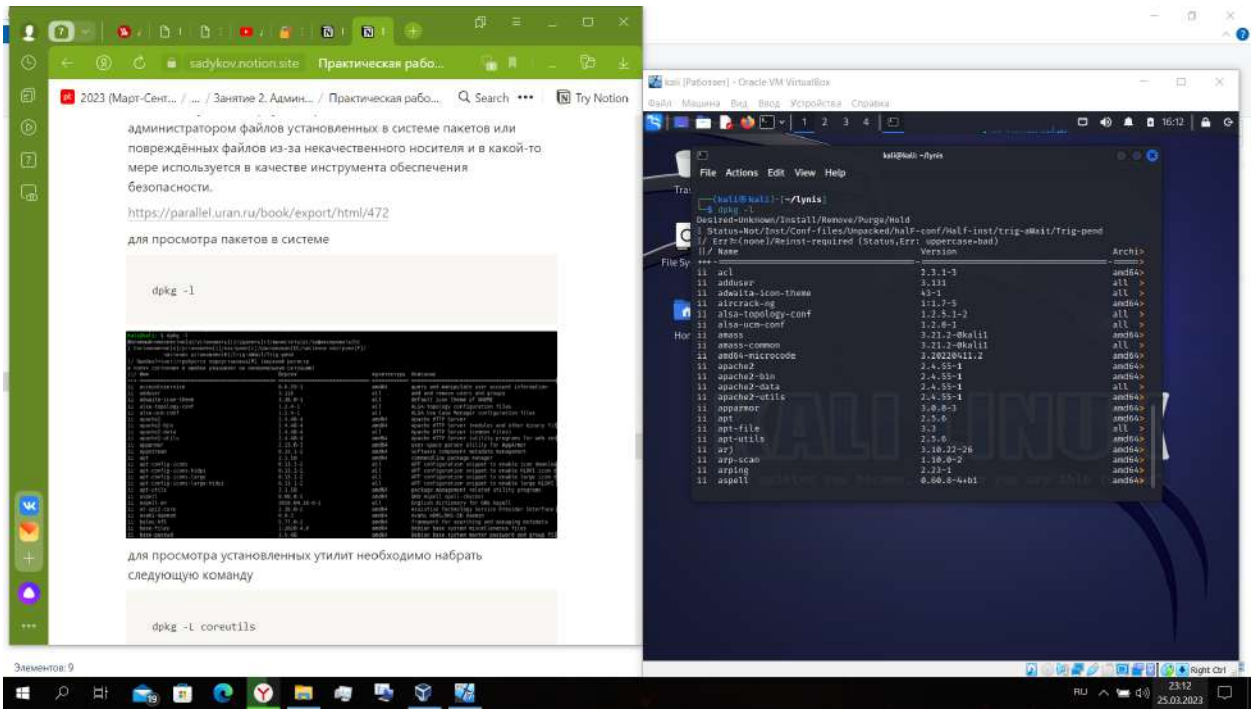

www.notion.so
Занятие 2. Администр...
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
Teamspaces
General
Teamspace Home
Shared
Стажировка Positive Te...
Private
Quick Note
Personal Home
Task List
Journal
Reading List
Upgrade to go unlimited
Upgrade plan
New page
Share
You can share your content with your teammates here
[Работает] - Oracle VM VirtualBox
File Actions Edit View Help
lynis/CHANGELOG.md
lynis/CODE_OF_CONDUCT.md
lynis/CONTRIBUTING.md
lynis/CONTRIBUTORS.md
lynis/FAQ
lynis/HAPPY_USERS.md
lynis/INSTALL
lynis/LICENSE
lynis/README
lynis/SECURITY.md
lynis/TODO.md
lynis/db/
lynis/db/languages/
lynis/db/languages/da
lynis/db/languages/ru
lynis/db/languages/sk
lynis/db/languages/he
lynis/db/languages/pl
lynis/db/languages/gr
lynis/db/languages/pt
lynis/db/languages/en-GB
lynis/db/languages/fr
lynis/db/languages/en
lynis/db/languages/de
lynis/db/languages/cn
lynis/db/languages/br
lynis/db/languages/nl-BE
Элементов: 9
RU
23:02
25.03.2023

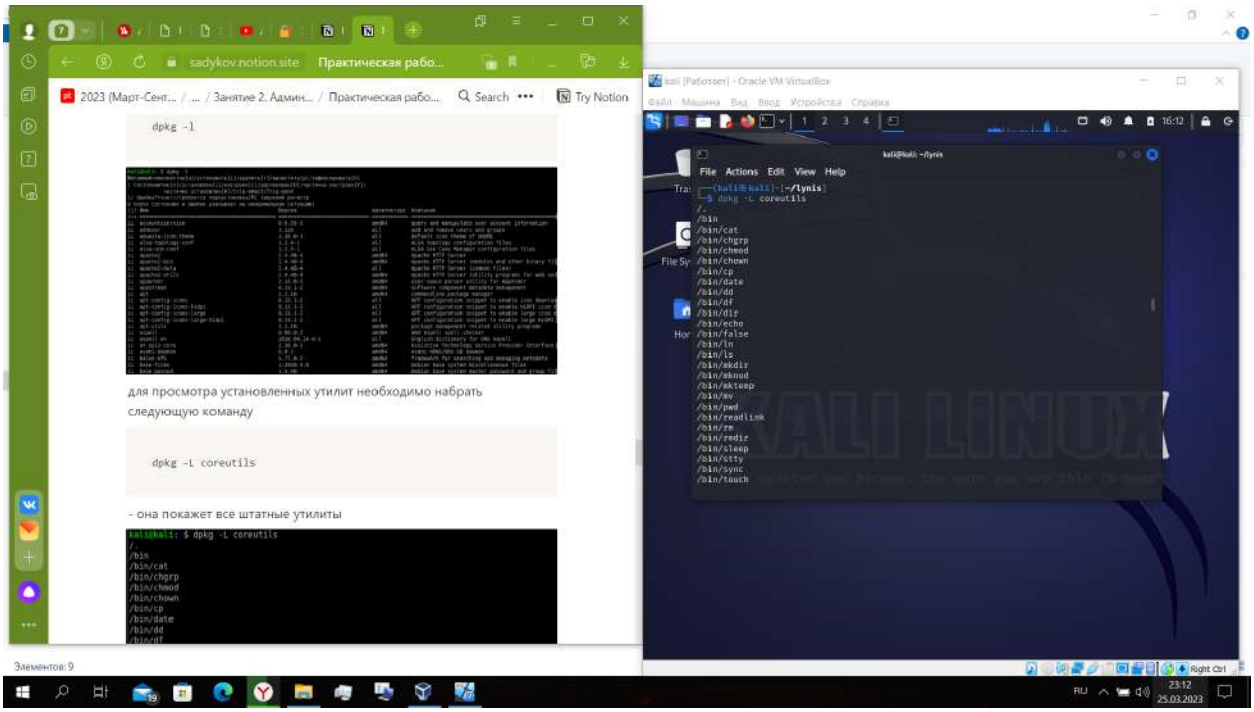

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Package: lynis
Version: 3.0.6
SHA256 hash: 3005346e90339c18a4c626169c6f1d9fb8643bb0d0a049bcaf64b7ccb4fd272c
Learn how to perform the integrity check and verification before using the software.
3005346e90339c18a4c626169c6f1d9fb8643bb0d0a049bcaf64b7ccb4fd272c
делается это следующей командой
sha256sum lynis-3.0.6.tar.gz
kali@kali: ~ $ sha256sum lynis-3.0.6.tar.gz
3005346e90339c18a4c626169c6f1d9fb8643bb0d0a049bcaf64b7ccb4fd272c lynis-3.0.6.tar.gz
также есть статья для рассчета контрольной суммы
https://jakondo.ru/kak-raschitat-kontrolnye-summy-md5-sha1-sha256-sha384-sha512-crc-v-linux/
далее переходим в директорию lynis
cd lynis
ls
далее запускаем утилиту lynis
sudo ./lynis audit system
Kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
lynis/include/helper_show
lynis/include/tests_hardening
lynis/include/tests_mac_frameworks
lynis/include/tests_firewalls
lynis/include/tests_nameservices
lynis/include/tests_boot_services
lynis/include/tests_kernel
lynis/lynis
lynis/lynis.8
lynis/plugins/
lynis/plugins/custom_plugin.template
lynis/plugins/README
lynis-3.0.6.tar.gz
CHANGELOG.md
CODE_OF_CONDUCT.md
CONTRIBUTING.md
CONTRIBUTORS.md
db
default.prf
developer.prf
extras
FAQ
HAPPY_USERS.md
include
INSTALL
LICENSE
lynis
lynis.8
README
SECURITY.md
TODO.md
plugins
Элементов: 9
RU
23:05
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try No
нажимаем Enter
Это вывод report-отчёт
kali@kali: ~/lynis
File Actions Edit View Help
[!] Change ownership of /home/kali/lynis/include/functions to 'root' or similar (found : kali with UID 1000).
Command:
chown 0:0 /home/kali/lynis/include/functions
[X] Security check failed
Why do I see this error?
This is a protection mechanism to prevent the root user from executing user created files. The files may be altered, or including malicious pieces of script.
What can I do?
Option 1) Check if a trusted user created the files (e.g. due to using Git, Homebrew or similar). If you trust these files, you can decide to continue this run by pressing ENTER.
Option 2) Change ownership of the related files (or full directory).
Commands (full directory):
cd ..
chown -R 0:0 lynis
cd lynis
./lynis audit system
[Press ENTER to continue, or CTRL+C to cancel]
Элементов: 9
RU
23:05
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try No
Это вывод report-отчёт
также я подобрал несколько ссылок для более подробного разбора данной утилиты:
https://codeby.net/threads/lynis-instrument-dlja-proverki-bezopasnosti-i-provedenija-pentesta-s-otkrytym-isxodnym-kodom-detalnoe-razjasnenie.64501/
https://cisofy.com/documentation/lynis/
https://cisofy.com/documentation/lynis/get-started/
ещё можно набрать команду ./lynis show options
kali@kali: ~/lynis$ sudo ./lynis show options
[sudo] пароль для kali:
[!] Change ownership of /tmp/lynis/include/functions to 'root' or similar (found : kali with UID 1000).
Command:
chown 0:0 /tmp/lynis/include/functions
[X] Security check failed
Why do I see this error?
This is a protection mechanism to prevent the root user from executing user created files. The files may be altered, or including malicious pieces of script.
kali@kali: ~/lynis
File Actions Edit View Help
- Installed rsh client package [OK]
- Installed rsh server package [OK]
- Installed telnet client package [OK]
- Installed telnet server package [NOT FOUND]
- Checking NIS client installation [OK]
- Checking NIS server installation [OK]
- Checking TFTP client installation [SUGGESTION]
- Checking TFTP server installation [SUGGESTION]
[+] Banners and identification
- /etc/issue [FOUND]
- /etc/issue contents [WEAK]
- /etc/issue.net [FOUND]
- /etc/issue.net contents [WEAK]
[+] Scheduled tasks
- Checking crontab and cronjob files [DONE]
[+] Accounting
- Checking accounting information [NOT FOUND]
- Checking sysstat accounting data [DISABLED]
- Checking auditd [NOT FOUND]
[+] Time and Synchronization
Элементов: 9
RU
23:07
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
https://cisofy.com/documentation/lynis/
https://cisofy.com/documentation/lynis/get-started/
ещё можно набрать команду ./lynis show options
sudo ./lynis show options
Перенаправлять файлы лучше через стандартный report утилиты:
/var/log/lynis-report.dat
Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]
Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]
Files:
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
Элементов: 9
RU
23:09
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
администратором файлов установленных в системе пакетов или повреждённых файлов из-за некачественного носителя и в какой-то мере используется в качестве инструмента обеспечения безопасности.
https://parallel.uran.ru/book/export/html/472
для просмотра пакетов в системе
dpkg -l
для просмотра установленных утилит необходимо набрать следующую команду
dpkg -L coreutils
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
Элементов: 9
RU
23:12
25.03.2023



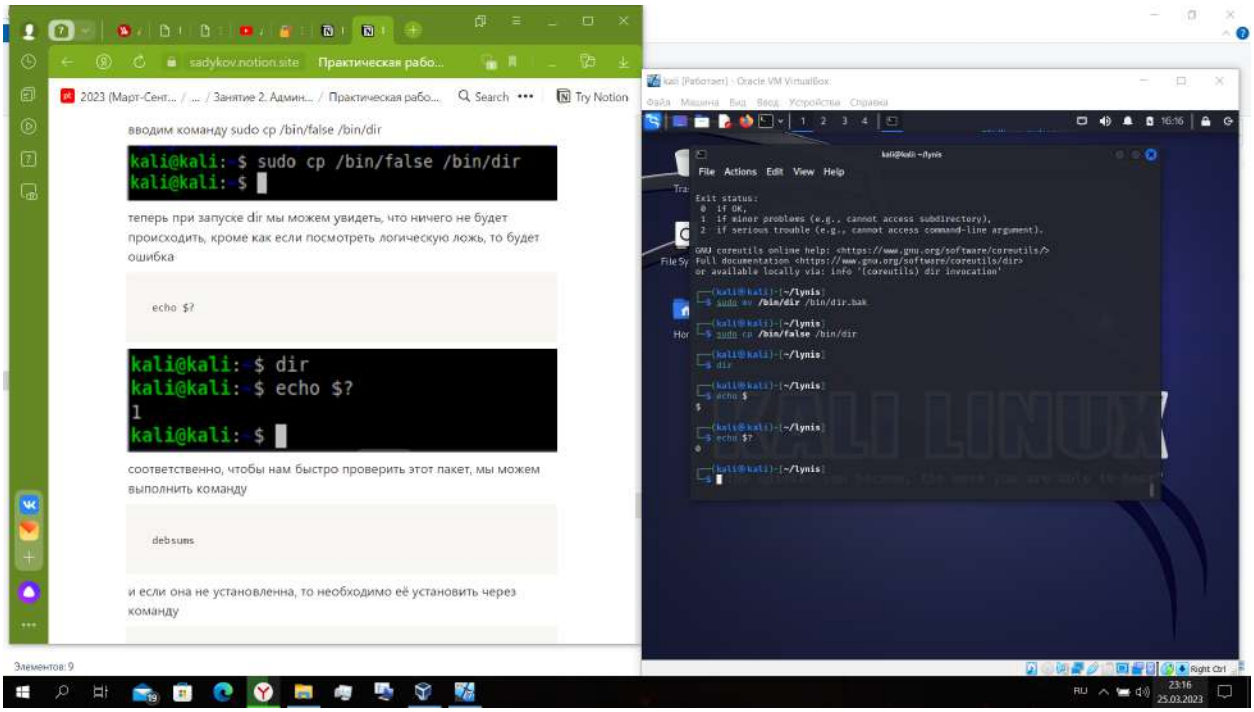
например, рассмотрим утилиту /bin/dir
/bin/dir --help
которая позволяет нам работать по сути как ls

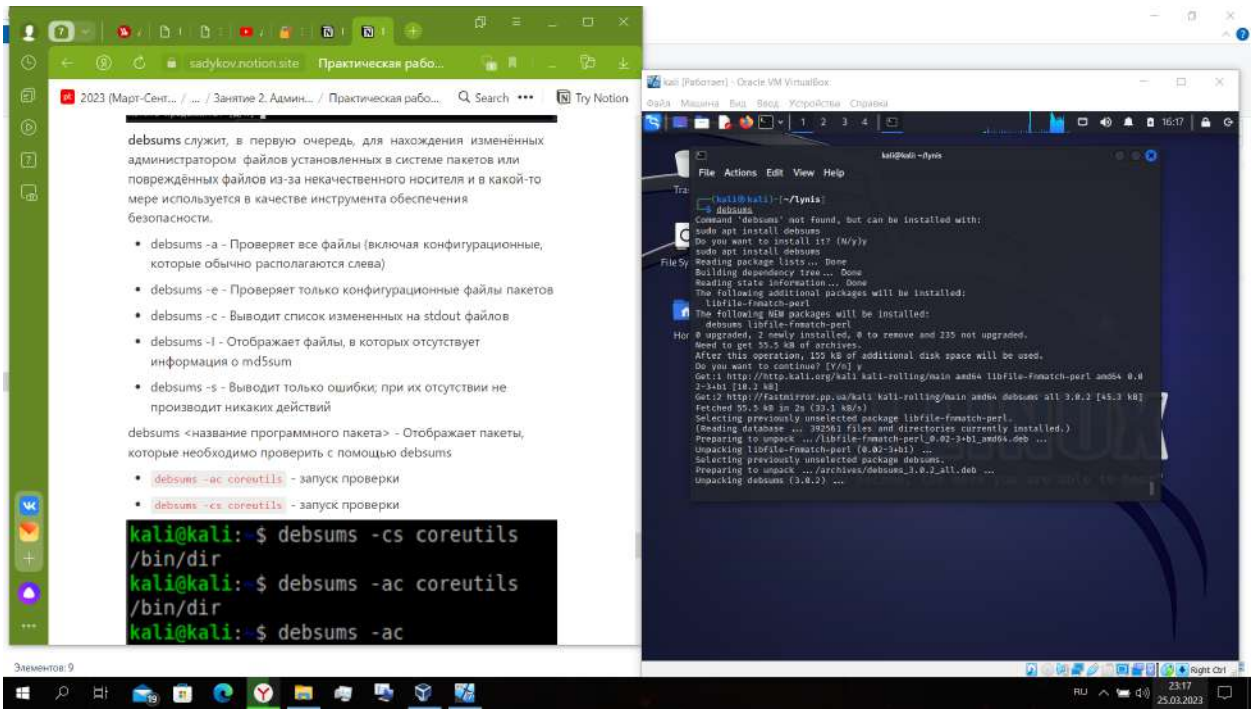
что будет, если мы поменяем /bin/false на /bin/dir, тем самым
сымитируем подмену или правку кода программы
сделаем backup sudo mv /bin/dir /bin/dir.bak

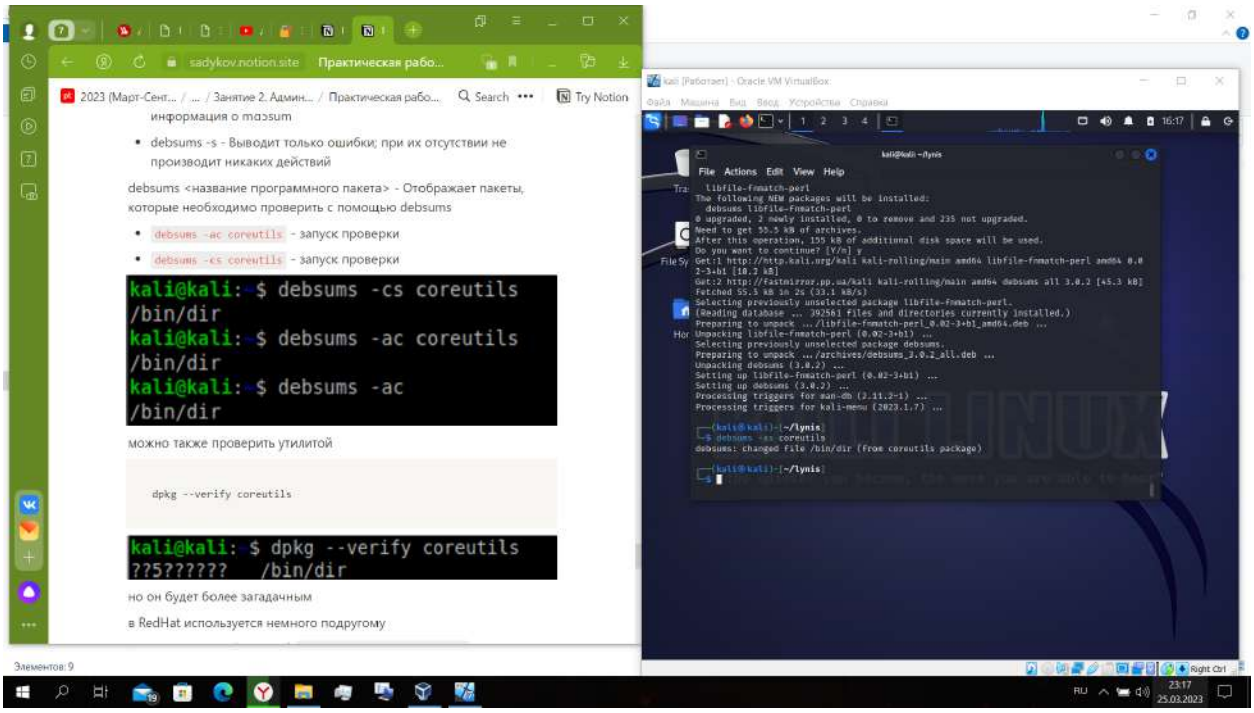
```
kali@kali: $ sudo mv /bin/dir /bin/dir.bak
[sudo] пароль для kali:
kali@kali: $
```

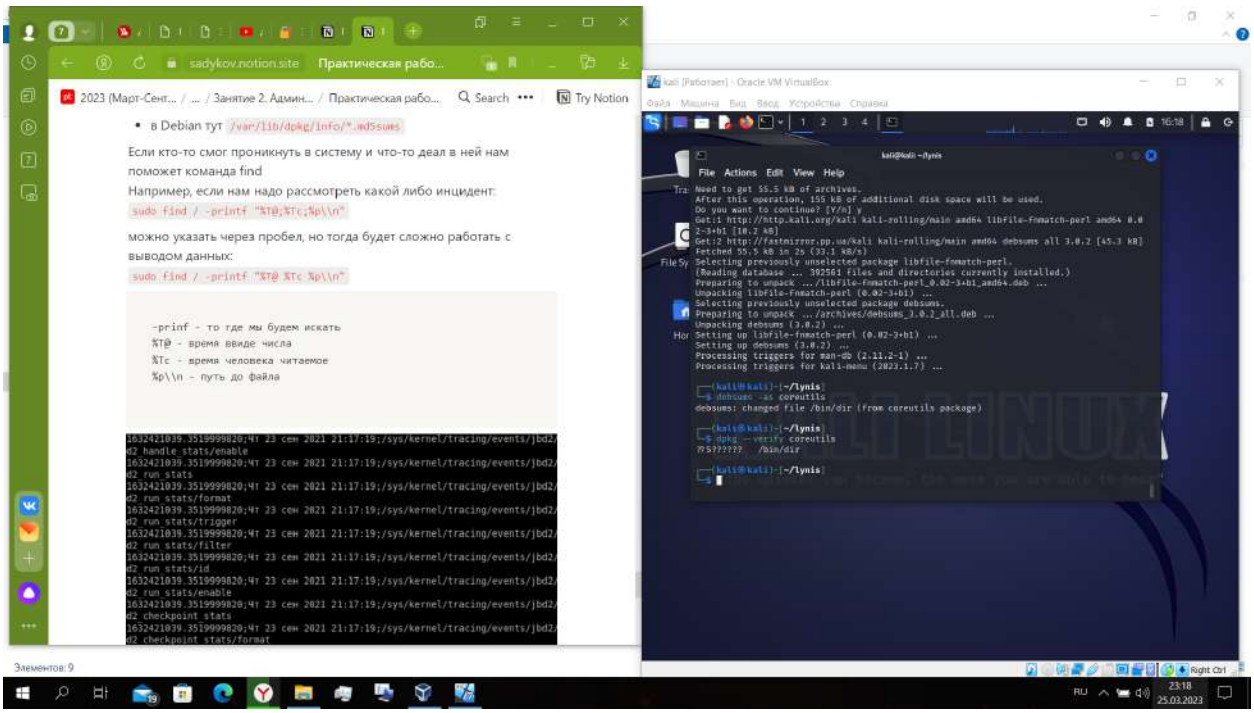
вводим команду sudo cp /bin/false /bin/dir

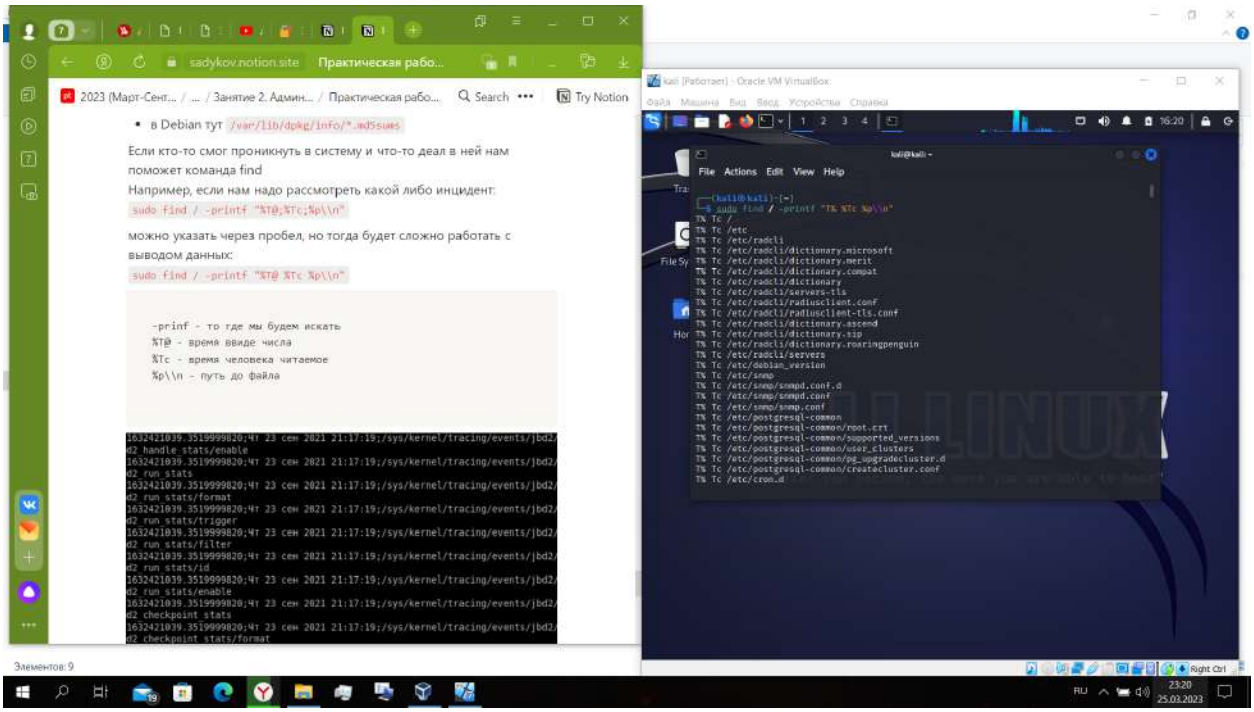
```
kali@kali: $ sudo cp /bin/false /bin/dir
kali@kali: $
```

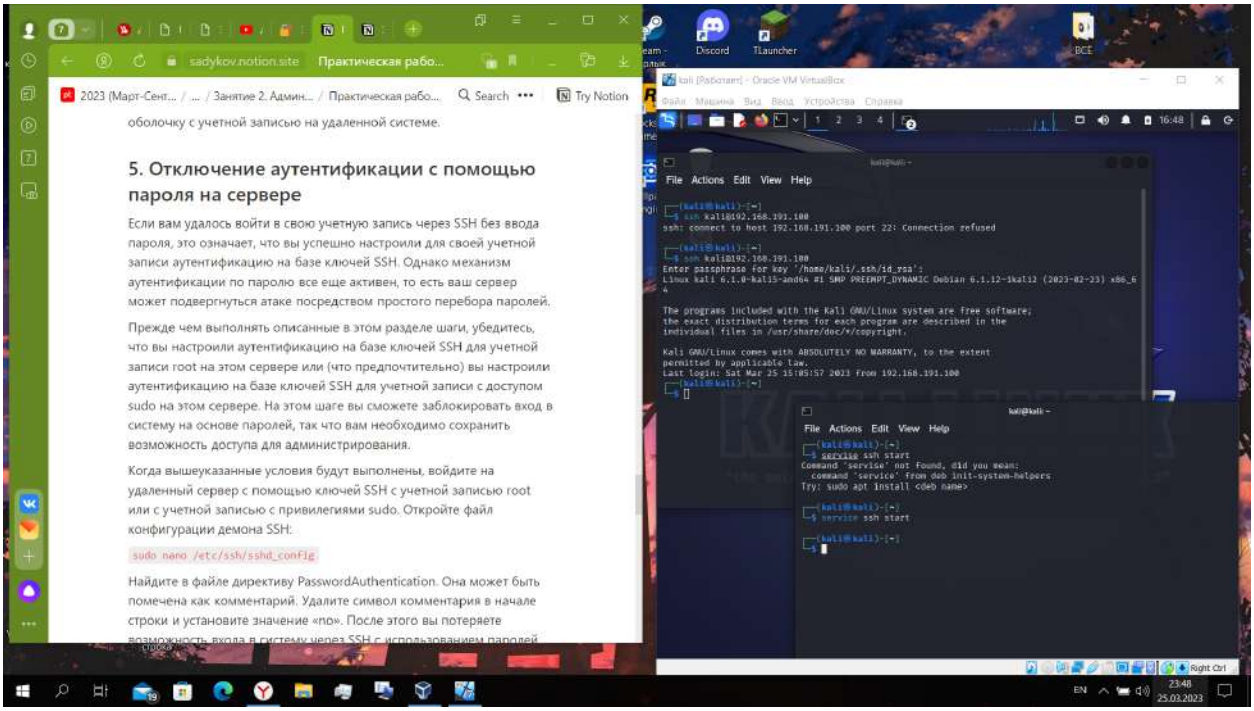

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
вводим команду sudo cp /bin/false /bin/dir
kali@kali: $ sudo cp /bin/false /bin/dir
kali@kali: $
теперь при запуске dir мы можем увидеть, что ничего не будет происходить, кроме как если посмотреть логическую ложь, то будет ошибка
echo $?
kali@kali: $ dir
kali@kali: $ echo $?
1
kali@kali: $
соответственно, чтобы нам быстро проверить этот пакет, мы можем выполнить команду
debsums
и если она не установленна, то необходимо её установить через команду
Элементов: 9
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
Exit status:
0 if OK,
1 if minor problems (e.g., cannot access subdirectory),
2 if serious trouble (e.g., cannot access command-line argument).
GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/dir>
or available locally via: info '(coreutils) dir invocation'
(kali@kali)-[~/lynis]
$ sudo mv /bin/dir /bin/dir.bak
(kali@kali)-[~/lynis]
$ sudo cp /bin/false /bin/dir
(kali@kali)-[~/lynis]
$ dir
(kali@kali)-[~/lynis]
$ echo $
$
(kali@kali)-[~/lynis]
$ echo $?
0
(kali@kali)-[~/lynis]
Right Ctrl
RU
23:16
25.03.2023

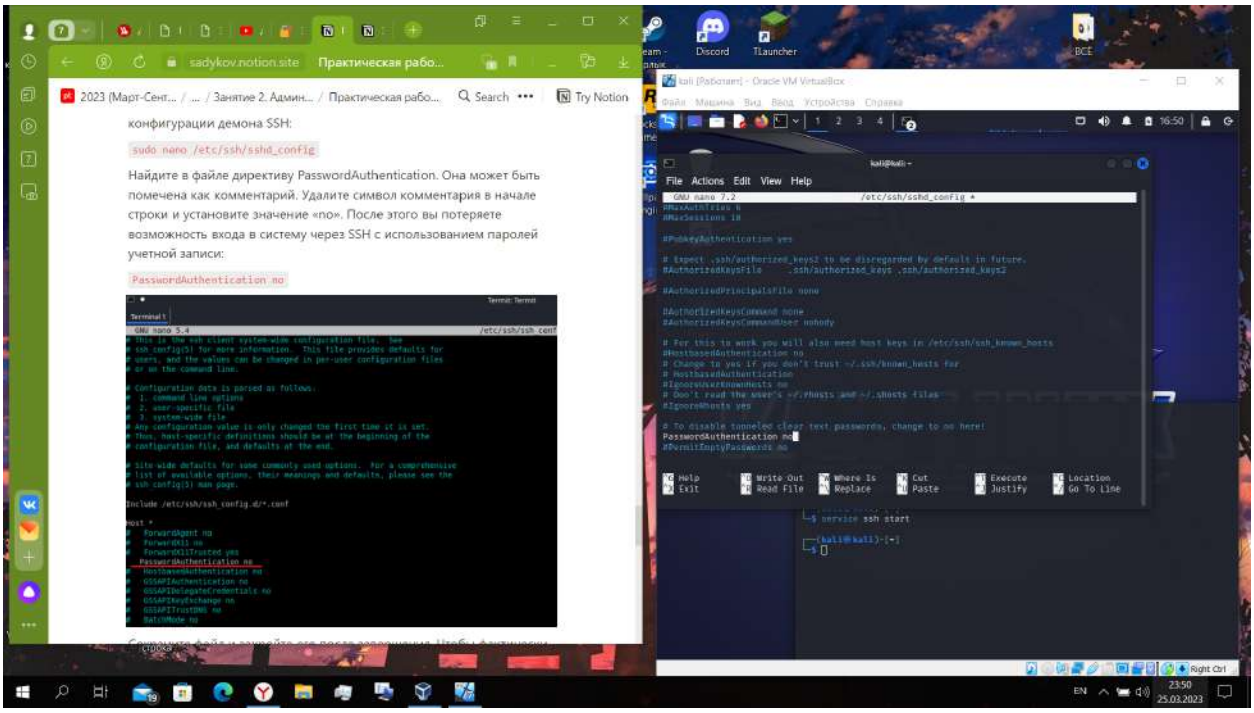

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
debsums служит, в первую очередь, для нахождения изменённых администратором файлов установленных в системе пакетов или повреждённых файлов из-за некачественного носителя и в какой-то мере используется в качестве инструмента обеспечения безопасности.
debsums -a - Проверяет все файлы (включая конфигурационные, которые обычно располагаются слева)
debsums -e - Проверяет только конфигурационные файлы пакетов
debsums -c - Выводит список измененных на stdout файлов
debsums -l - Отображает файлы, в которых отсутствует информация о md5sum
debsums -s - Выводит только ошибки; при их отсутствии не производит никаких действий
debsums <название программного пакета> - Отображает пакеты, которые необходимо проверить с помощью debsums
debsums -ac coreutils - запуск проверки
debsums -cs coreutils - запуск проверки
kali@kali: $ debsums -cs coreutils
/bin/dir
kali@kali: $ debsums -ac coreutils
/bin/dir
kali@kali: $ debsums -ac
Элементов: 9
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
(kali@kali)-[~/lynis]
$ debsums
Command 'debsums' not found, but can be installed with:
sudo apt install debsums
Do you want to install it? (N/y)y
sudo apt install debsums
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
libfile-fnmatch-perl
The following NEW packages will be installed:
debsums libfile-fnmatch-perl
0 upgraded, 2 newly installed, 0 to remove and 235 not upgraded.
Need to get 55.5 kB of archives.
After this operation, 155 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libfile-fnmatch-perl amd64 0.02-3+b1 [10.2 kB]
Get:2 http://fastmirror.pp.ua/kali kali-rolling/main amd64 debsums all 3.0.2 [45.3 kB]
Fetched 55.5 kB in 2s (33.1 kB/s)
Selecting previously unselected package libfile-fnmatch-perl.
(Reading database ... 392561 files and directories currently installed.)
Preparing to unpack .../libfile-fnmatch-perl_0.02-3+b1_amd64.deb ...
Unpacking libfile-fnmatch-perl (0.02-3+b1) ...
Selecting previously unselected package debsums.
Preparing to unpack .../archives/debsums_3.0.2_all.deb ...
Unpacking debsums (3.0.2) ...
Right Ctrl
RU
23:17
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
информация о md5sum
debsums -s - Выводит только ошибки; при их отсутствии не производит никаких действий
debsums <название программного пакета> - Отображает пакеты, которые необходимо проверить с помощью debsums
debsums -ac coreutils - запуск проверки
debsums -cs coreutils - запуск проверки
kali@kali:~$ debsums -cs coreutils
/bin/dir
kali@kali:~$ debsums -ac coreutils
/bin/dir
kali@kali:~$ debsums -ac
/bin/dir
можно также проверить утилитой
dpkg --verify coreutils
kali@kali: $ dpkg --verify coreutils
??5?????? /bin/dir
но он будет более загадачным
в RedHat используется немного подругому
Элементов: 9
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
libfile-fnmatch-perl
The following NEW packages will be installed:
debsums libfile-fnmatch-perl
0 upgraded, 2 newly installed, 0 to remove and 235 not upgraded.
Need to get 55.5 kB of archives.
After this operation, 155 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libfile-fnmatch-perl amd64 0.02-3+b1 [10.2 kB]
Get:2 http://fastmirror.pp.ua/kali kali-rolling/main amd64 debsums all 3.0.2 [45.3 kB]
Fetched 55.5 kB in 2s (33.1 kB/s)
Selecting previously unselected package libfile-fnmatch-perl.
(Reading database ... 392561 files and directories currently installed.)
Preparing to unpack .../libfile-fnmatch-perl_0.02-3+b1_amd64.deb ...
Unpacking libfile-fnmatch-perl (0.02-3+b1) ...
Selecting previously unselected package debsums.
Preparing to unpack .../archives/debsums_3.0.2_all.deb ...
Unpacking debsums (3.0.2) ...
Setting up libfile-fnmatch-perl (0.02-3+b1) ...
Setting up debsums (3.0.2) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for kali-menu (2023.1.7) ...
(kali㉿kali)-[~/lynis]
$ debsums -cs coreutils
debsums: changed file /bin/dir (from coreutils package)
(kali㉿kali)-[~/lynis]
Right Ctrl
RU
23:17
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
в Debian тут /var/lib/dpkg/info/*.md5sums
Если кто-то смог проникнуть в систему и что-то деал в ней нам поможет команда find
Например, если нам надо рассмотреть какой либо инцидент:
sudo find / -printf "%T@;%Tc;%p\\n"
можно указать через пробел, но тогда будет сложно работать с выводом данных:
sudo find / -printf "%T@ %Tc %p\\n"
-prinf - то где мы будем искать
%T@ - время ввиде числа
%Tc - время человека читаемое
%p\\n - путь до файла
1632421039.3519999820;Чт 23 сен 2021 21:17:19;/sys/kernel/tracing/events/jbd2/jbd2_handle_stats/enable
1632421039.3519999820;Чт 23 сен 2021 21:17:19;/sys/kernel/tracing/events/jbd2/jbd2_run_stats
1632421039.3519999820;Чт 23 сен 2021 21:17:19;/sys/kernel/tracing/events/jbd2/jbd2_run_stats/format
1632421039.3519999820;Чт 23 сен 2021 21:17:19;/sys/kernel/tracing/events/jbd2/jbd2_run_stats/trigger
1632421039.3519999820;Чт 23 сен 2021 21:17:19;/sys/kernel/tracing/events/jbd2/jbd2_run_stats/filter
1632421039.3519999820;Чт 23 сен 2021 21:17:19;/sys/kernel/tracing/events/jbd2/jbd2_run_stats/id
1632421039.3519999820;Чт 23 сен 2021 21:17:19;/sys/kernel/tracing/events/jbd2/jbd2_run_stats/enable
1632421039.3519999820;Чт 23 сен 2021 21:17:19;/sys/kernel/tracing/events/jbd2/jbd2_checkpoint_stats
1632421039.3519999820;Чт 23 сен 2021 21:17:19;/sys/kernel/tracing/events/jbd2/jbd2_checkpoint_stats/format
Элементов: 9
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
Need to get 55.5 kB of archives.
After this operation, 155 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libfile-fnmatch-perl amd64 0.02-3+b1 [10.2 kB]
Get:2 http://fastmirror.pp.ua/kali kali-rolling/main amd64 debsums all 3.0.2 [45.3 kB]
Fetched 55.5 kB in 2s (33.1 kB/s)
Selecting previously unselected package libfile-fnmatch-perl.
(Reading database ... 392561 files and directories currently installed.)
Preparing to unpack .../libfile-fnmatch-perl_0.02-3+b1_amd64.deb ...
Unpacking libfile-fnmatch-perl (0.02-3+b1) ...
Selecting previously unselected package debsums.
Preparing to unpack .../archives/debsums_3.0.2_all.deb ...
Unpacking debsums (3.0.2) ...
Setting up libfile-fnmatch-perl (0.02-3+b1) ...
Setting up debsums (3.0.2) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for kali-menu (2023.1.7) ...
(kali㉿kali)-[~/lynis]
$ debsums -as coreutils
debsums: changed file /bin/dir (from coreutils package)
(kali㉿kali)-[~/lynis]
$ dpkg --verify coreutils
??5?????? /bin/dir
(kali㉿kali)-[~/lynis]
Right Ctrl
RU
23:18
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
в Debian тут /var/lib/dpkg/info/*.md5sums
Если кто-то смог проникнуть в систему и что-то деал в ней нам поможет команда find
Например, если нам надо рассмотреть какой либо инцидент:
sudo find / -printf "%T@;%Tc;%p\\n"
можно указать через пробел, но тогда будет сложно работать с выводом данных:
sudo find / -printf "%T@ %Tc %p\\n"
-prinf - то где мы будем искать
%T@ - время ввиде числа
%Tc - время человека читаемое
%p\\n - путь до файла
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
оболочку с учетной записью на удаленной системе.
5. Отключение аутентификации с помощью пароля на сервере
Если вам удалось войти в свою учетную запись через SSH без ввода пароля, это означает, что вы успешно настроили для своей учетной записи аутентификацию на базе ключей SSH. Однако механизм аутентификации по паролю все еще активен, то есть ваш сервер может подвергнуться атаке посредством простого перебора паролей.
Прежде чем выполнять описанные в этом разделе шаги, убедитесь, что вы настроили аутентификацию на базе ключей SSH для учетной записи root на этом сервере или (что предпочтительно) вы настроили аутентификацию на базе ключей SSH для учетной записи с доступом sudo на этом сервере. На этом шаге вы сможете заблокировать вход в систему на основе паролей, так что вам необходимо сохранить возможность доступа для администрирования.
Когда вышеуказанные условия будут выполнены, войдите на удаленный сервер с помощью ключей SSH с учетной записью root или с учетной записью с привилегиями sudo. Откройте файл конфигурации демона SSH:
sudo nano /etc/ssh/sshd_config
Найдите в файле директиву PasswordAuthentication. Она может быть помечена как комментарий. Удалите символ комментария в начале строки и установите значение «no». После этого вы потеряете
Discord
TLauncher
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help



Последние 2 скриншота - вход в ssh-сессию, изменение конфигурационного файла.

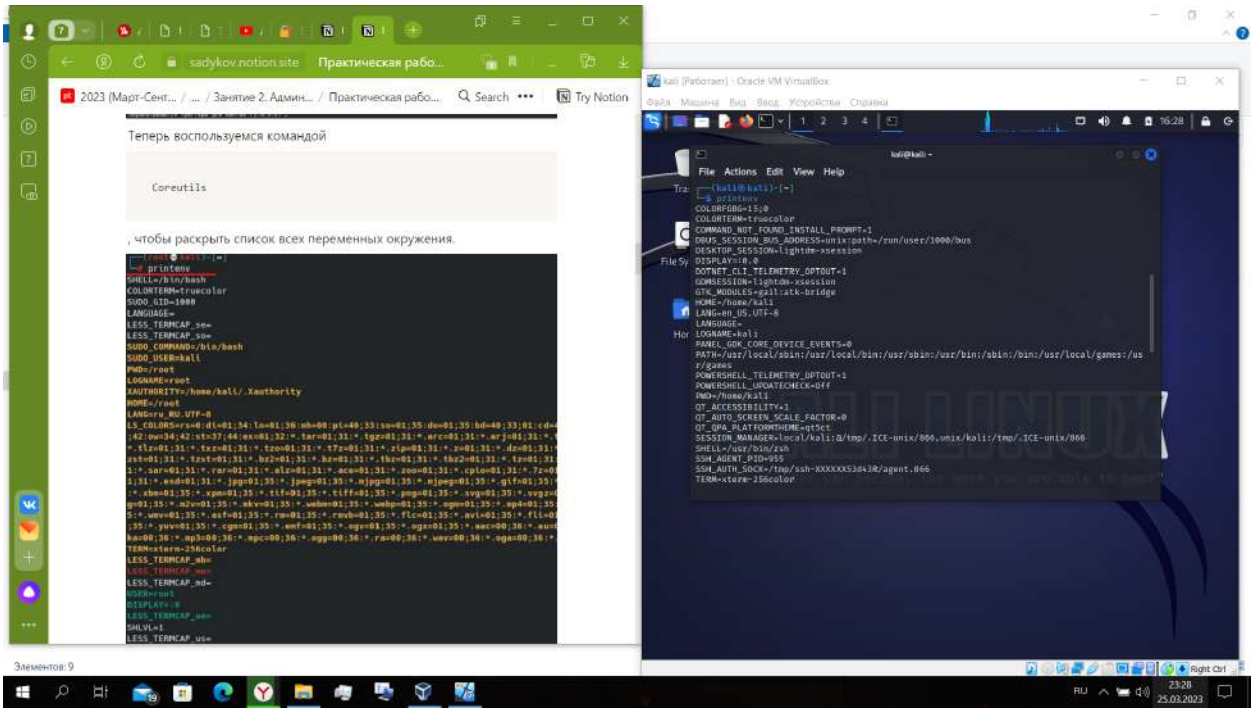
Практическая работа "Переменные окружения в Linux .bashrc, .bash_profile и .bash_login"

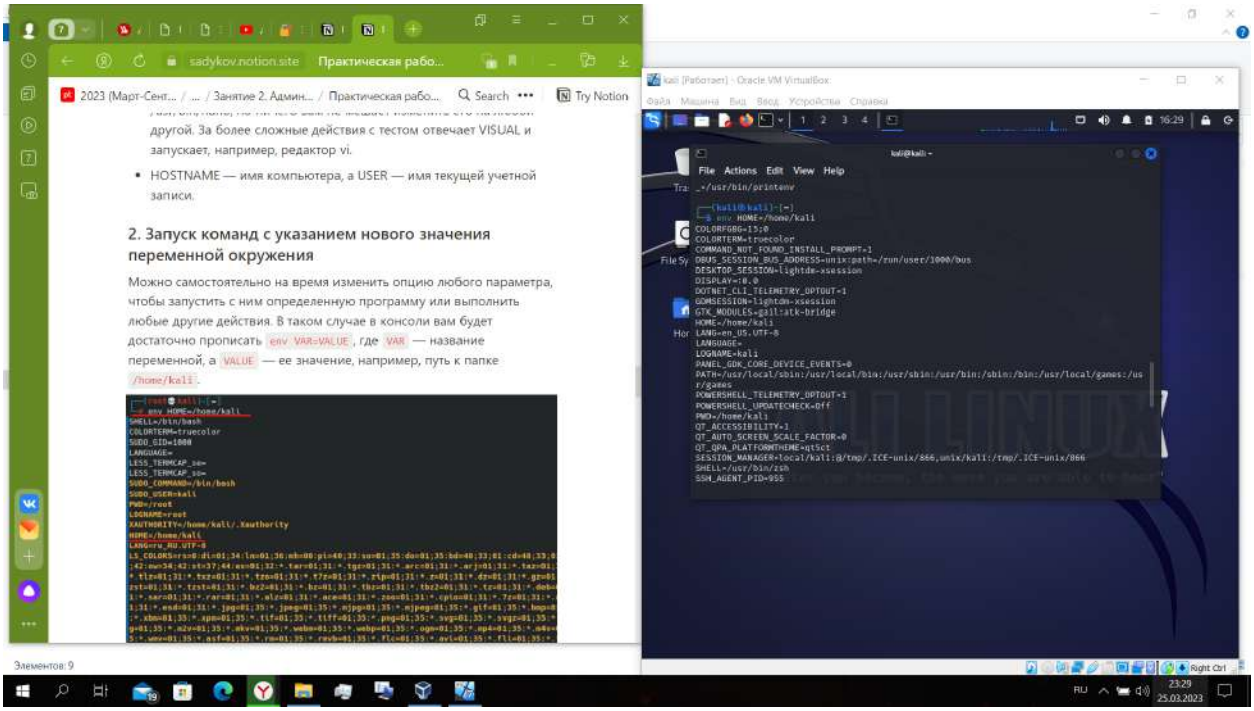
Цель работы:

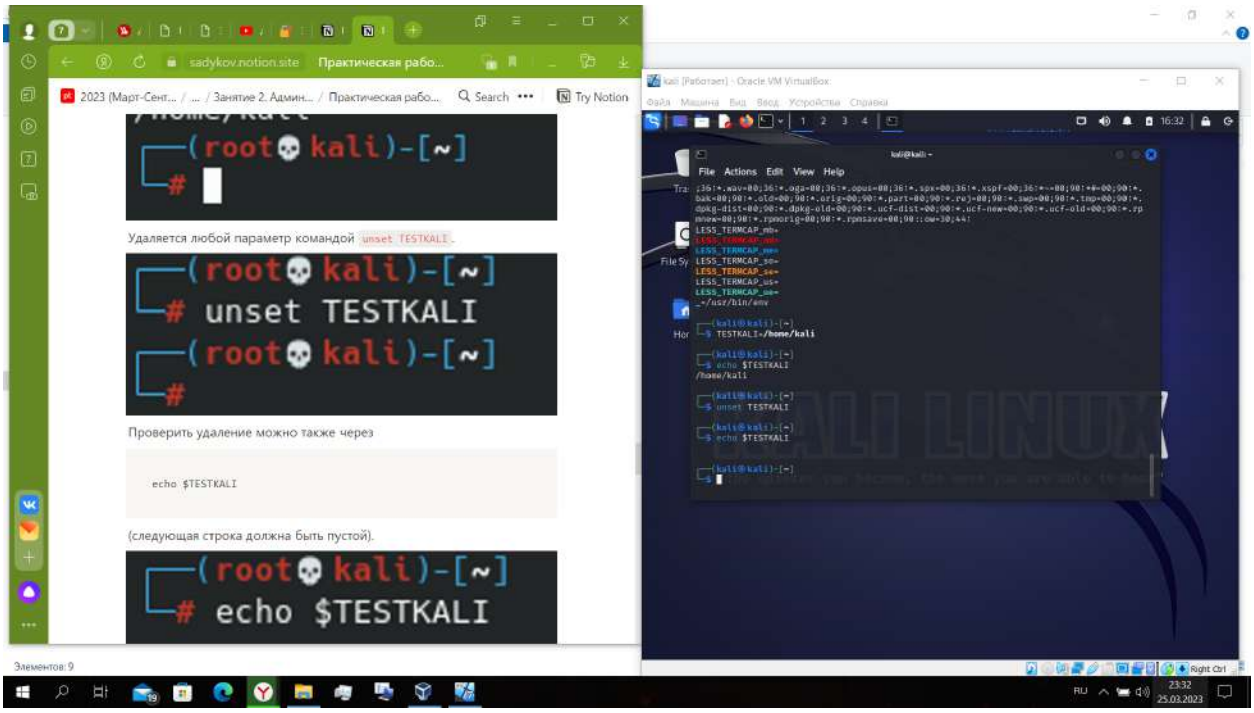
- Научиться работать с переменным окружением в linux.

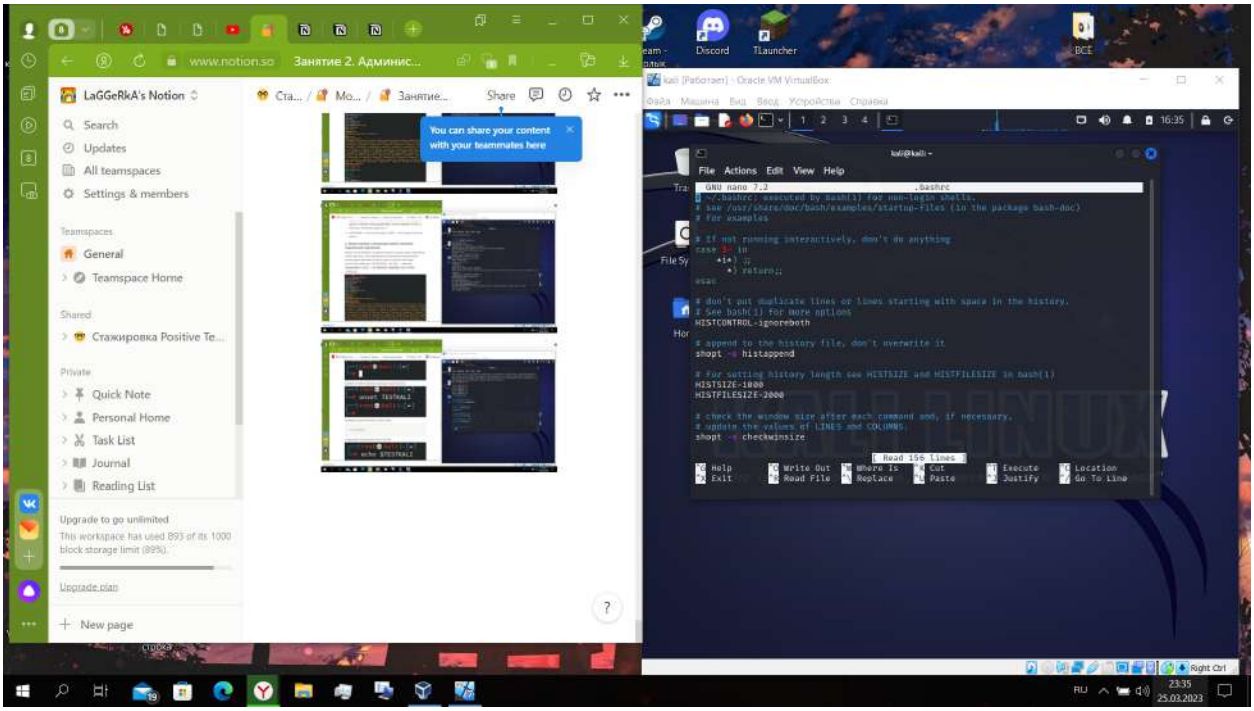
Задача:

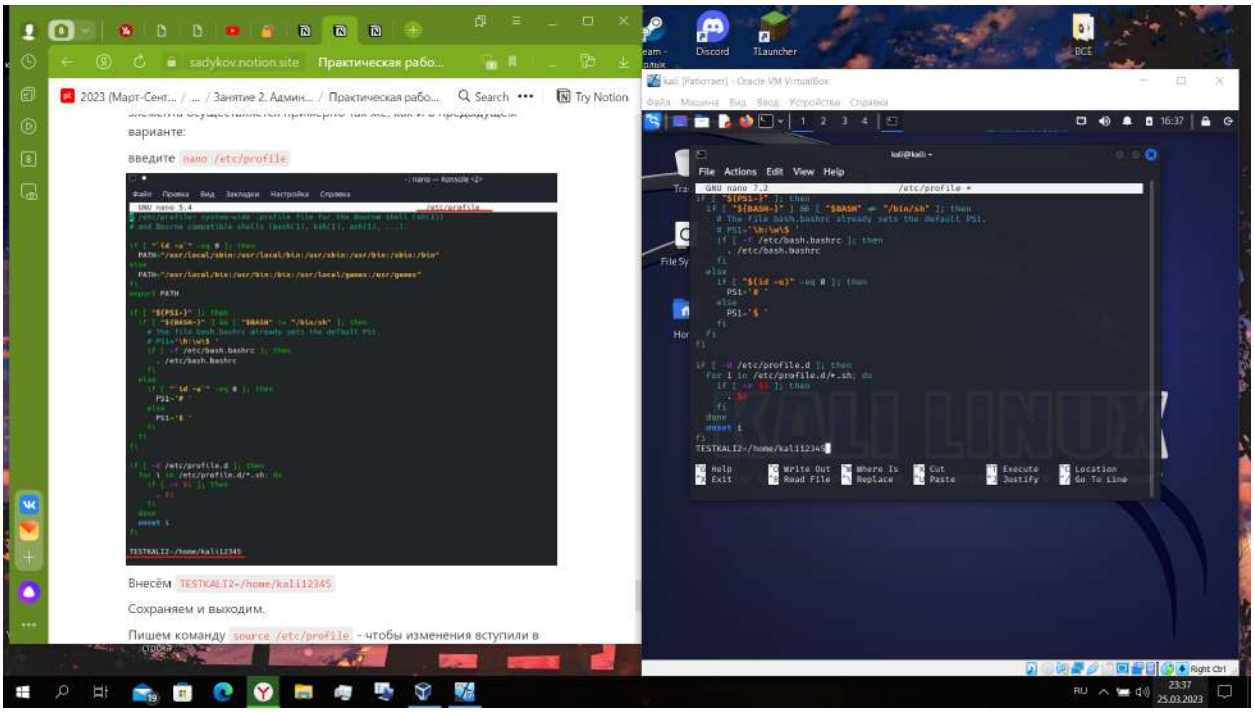
- Научиться работать с .bashrc, .bash_profile и .bash_login.

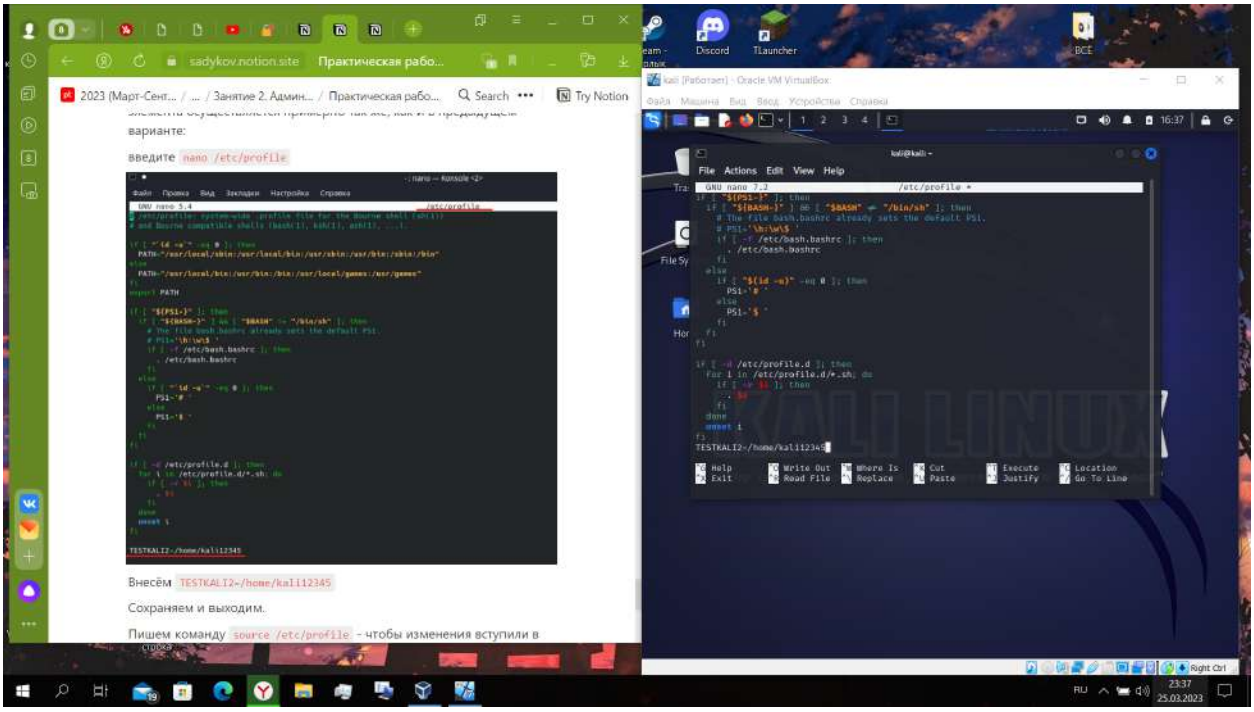

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
Теперь воспользуемся командой
Coreutils
, чтобы раскрыть список всех переменных окружения.
printenv
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
Элементов: 9
23:28
25.03.2023

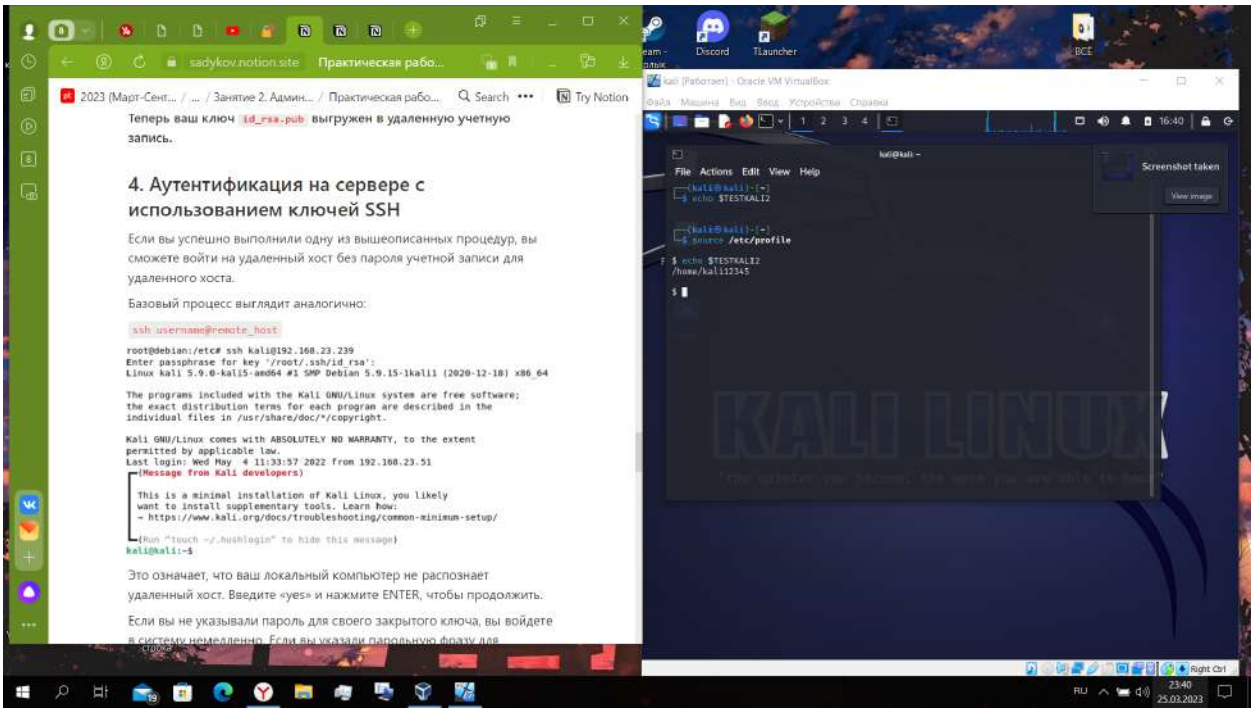

sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
другой. За более сложные действия с тестом отвечает VISUAL и запускает, например, редактор vi.
HOSTNAME — имя компьютера, а USER — имя текущей учетной записи.
2. Запуск команд с указанием нового значения переменной окружения
Можно самостоятельно на время изменить опцию любого параметра, чтобы запустить с ним определенную программу или выполнить любые другие действия. В таком случае в консоли вам будет достаточно прописать env VAR=VALUE, где VAR — название переменной, а VALUE — ее значение, например, путь к папке /home/kali.
env HOME=/home/kali
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
Элементов: 9
23:29
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
(root kali)-[~]
#
Удаляется любой параметр командой unset TESTKALI.
(root kali)-[~]
unset TESTKALI
(root kali)-[~]
#
Проверить удаление можно также через
echo $TESTKALI
(следующая строка должна быть пустой).
(root kali)-[~]
echo $TESTKALI
Элементов: 9
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
Right Ctrl
23:32
25.03.2023


www.notion.so
Занятие 2. Администр...
LaGGeRkA's Notion
Search
Updates
All teamspaces
Settings & members
Teamspaces
General
Teamspace Home
Shared
Стажировка Positive Te...
Private
Quick Note
Personal Home
Task List
Journal
Reading List
Upgrade to go unlimited
This workspace has used 893 of its 1000 block storage limit (89%).
Upgrade plan
New page
Share
You can share your content with your teammates here
Discord
TLauncher
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
GNU nano 7.2 .bashrc
Read 156 lines
Right Ctrl
23:35
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
варианте:
введите nano /etc/profile
Внесём TESTKALI2-/home/kali12345
Сохраняем и выходим.
Пишем команду source /etc/profile - чтобы изменения вступили в
Discord
TLauncher
File Actions Edit View Help
GNU nano 7.2 /etc/profile *
TESTKALI2-/home/kali12345
Help
Write Out
Where Is
Cut
Execute
Location
Exit
Read File
Replace
Paste
Justify
Go To Line
Right Ctrl
23:37
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
варианте:
введите nano /etc/profile
Внесём TESTKALI2-/home/kali12345
Сохраняем и выходим.
Пишем команду source /etc/profile - чтобы изменения вступили в
Discord
TLauncher
File Actions Edit View Help
GNU nano 7.2 /etc/profile *
TESTKALI2-/home/kali12345
Help
Write Out
Where Is
Cut
Execute
Location
Exit
Read File
Replace
Paste
Justify
Go To Line
Right Ctrl
23:37
25.03.2023


sadykov.notion.site
Практическая рабо...
2023 (Март-Сент... / ... / Занятие 2. Админ... / Практическая рабо...
Search
Try Notion
Теперь ваш ключ id_rsa.pub выгружен в удаленную учетную запись.
4. Аутентификация на сервере с использованием ключей SSH
Если вы успешно выполнили одну из вышеописанных процедур, вы сможете войти на удаленный хост без пароля учетной записи для удаленного хоста.
Базовый процесс выглядит аналогично:
ssh username@remote_host
root@debian:/etc# ssh kali@192.168.23.239
Enter passphrase for key '/root/.ssh/id_rsa':
Linux kali 5.9.0-kali5-amd64 #1 SMP Debian 5.9.15-1kali1 (2020-12-18) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 4 11:33:57 2022 from 192.168.23.51
(Message from Kali developers)
This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
- https://www.kali.org/docs/troubleshooting/common-minimum-setup/
(Run "touch ~/.hushlogin" to hide this message)
kali@kali:~$
Это означает, что ваш локальный компьютер не распознает удаленный хост. Введите «yes» и нажмите ENTER, чтобы продолжить.
Если вы не указывали пароль для своего закрытого ключа, вы войдете
Discord
TLauncher
kali [Работает] - Oracle VM VirtualBox
File Actions Edit View Help
Screenshot taken
View image
$ echo $TESTKALI2
/home/kali12345
Right Ctrl
23:40
25.03.2023