

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

Факультет физики и информационных технологий

Кафедра общей физики

Основы безопасности операционных систем

Отчет по лабораторной работе №8

Исполнитель
студент группы КИ-22:

Д.В.Скрежендевский

Проверил
ст. преподаватель:

В.В.Грищенко

Гомель 2025

Цель работы: изучить основные принципы обеспечения безопасности в операционных системах Windows и Linux.

1 Ознакомиться и изучить на практике команды и утилиты, предназначенные для работы с пользователями, группами пользователей и правами доступа в операционных системах Linux и Windows

2 Вывести информацию о пользователях, существующих в операционных системах Linux и Windows

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-LocalUser

Name           Enabled Description
-----
Administrator  True    Built-in account for administering the computer/domain
DefaultAccount False   A user account managed by the system.
dmskrzh        True    user
Guest          False   Built-in account for guest access to the computer/domain

PS C:\Windows\system32>
```

Рисунок 2.1 - Пользователи в Windows

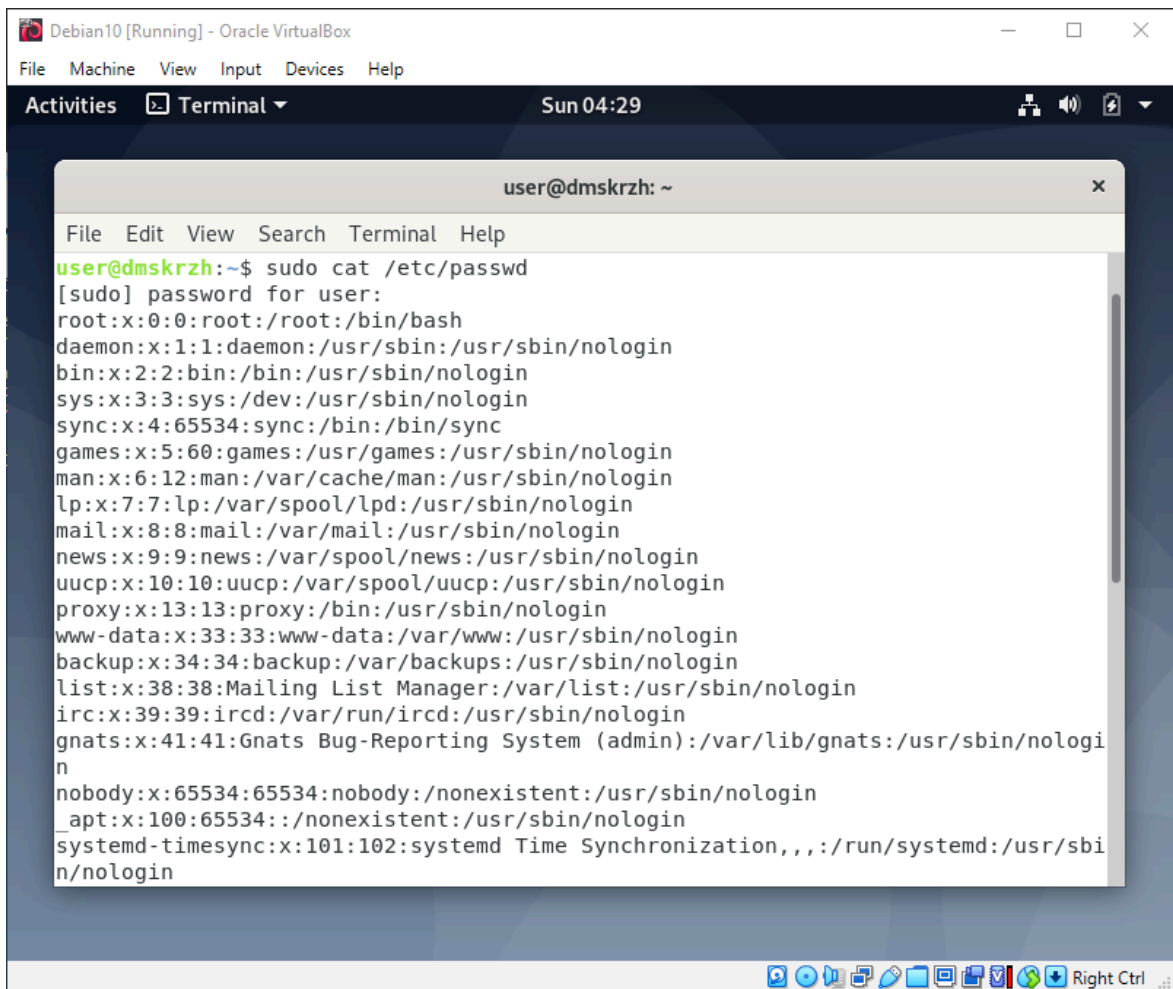


Рисунок 2.2 - Пользователи в Linux

3 Вывести подробную информацию о текущем пользователе и его домашнем каталоге в операционных системах Linux и Windows

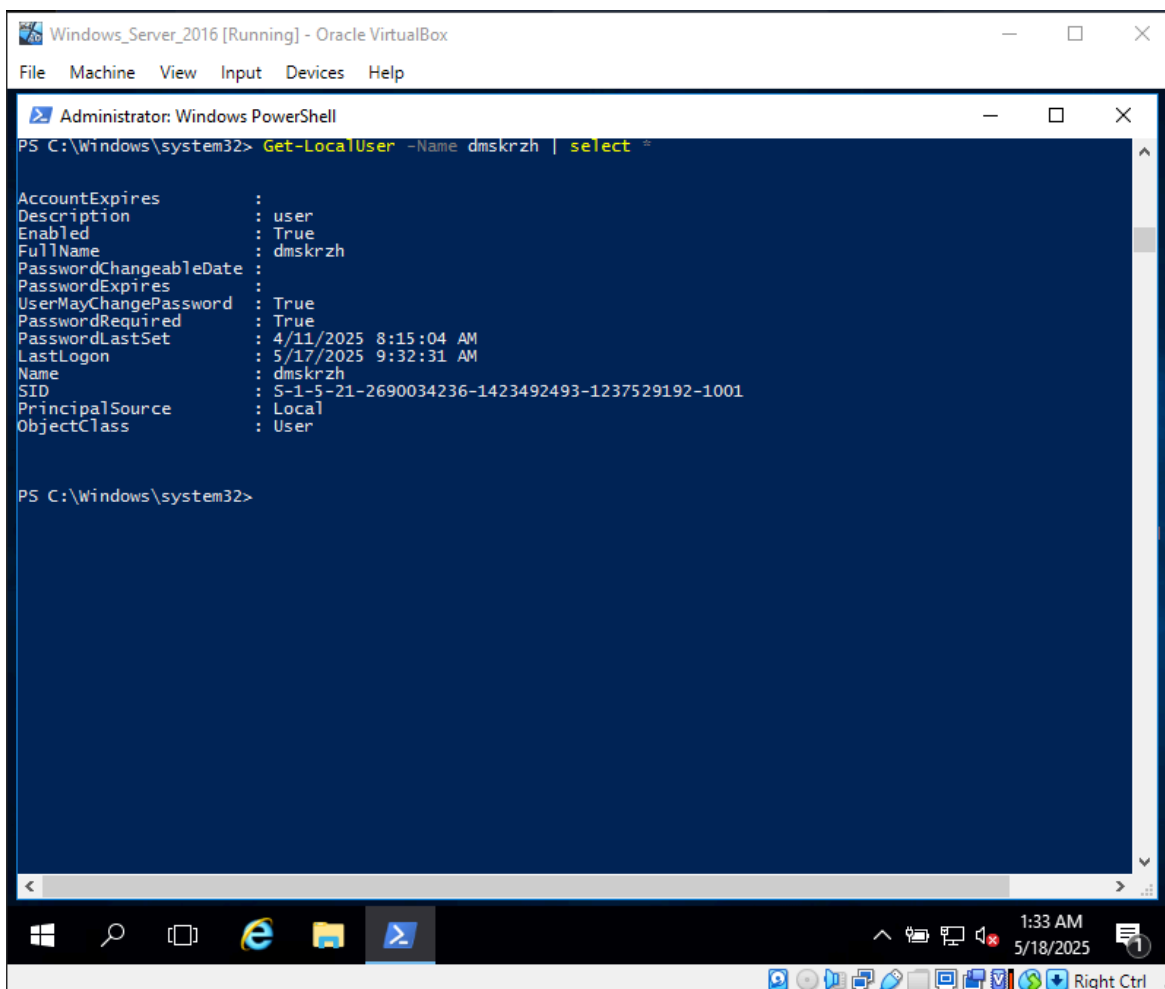


Рисунок 3.1 - Подробная информация в Windows

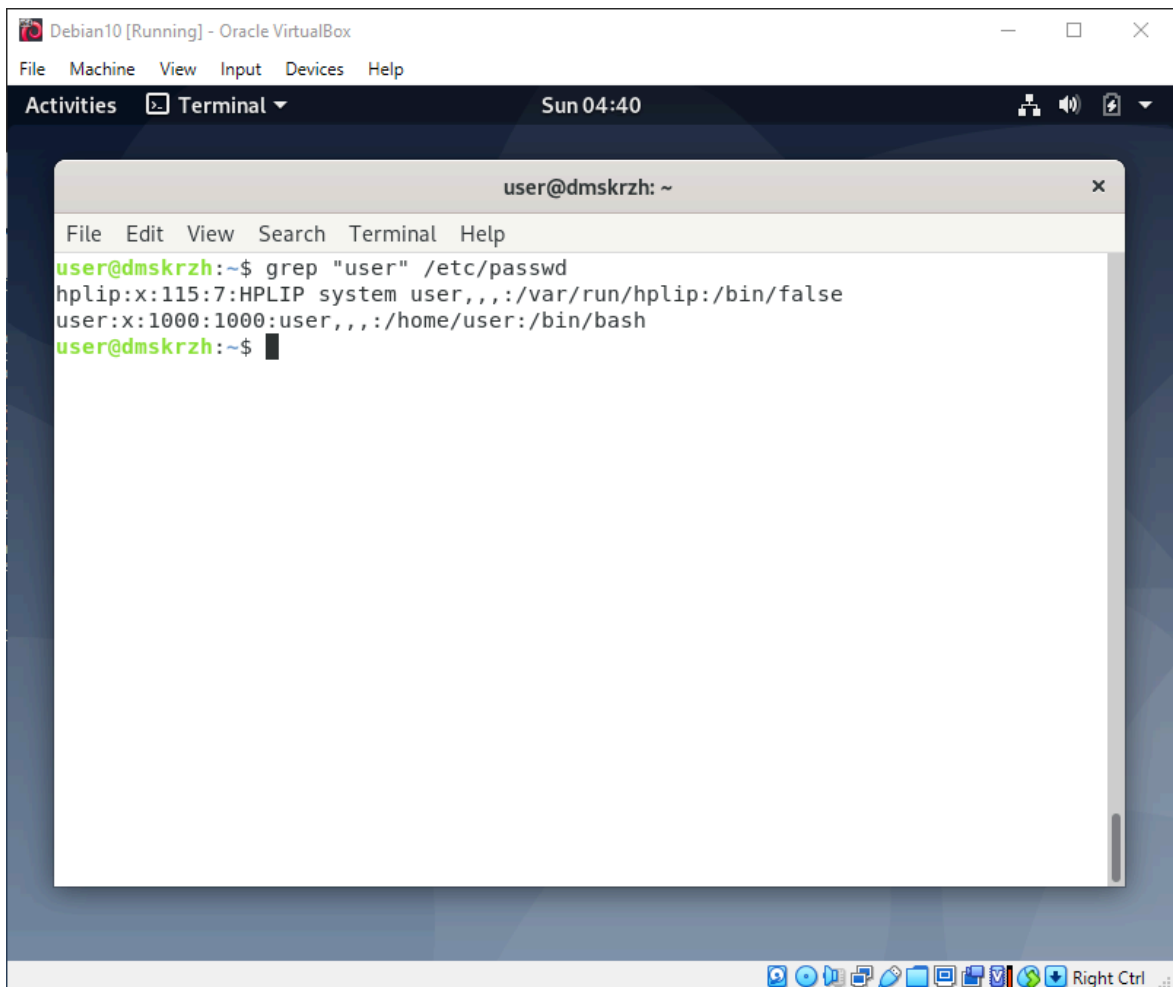


Рисунок 3.2 - Подробная информация в Linux

4 Создать пользователя student и вывести подробную информацию о нем и его домашнем каталоге в операционных системах Linux и Windows

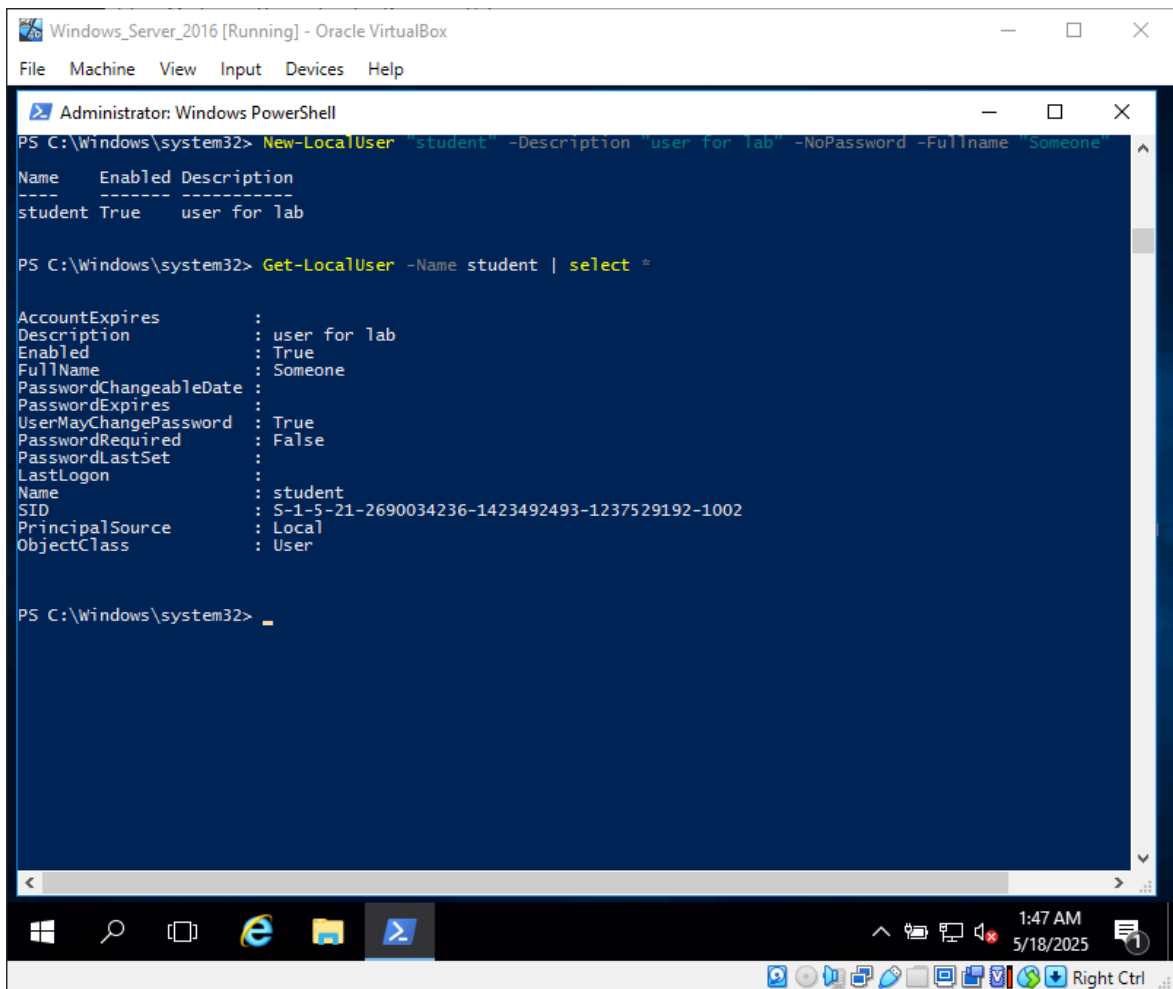


Рисунок 4.1 - Создание пользователя и просмотр подробной информации в Windows

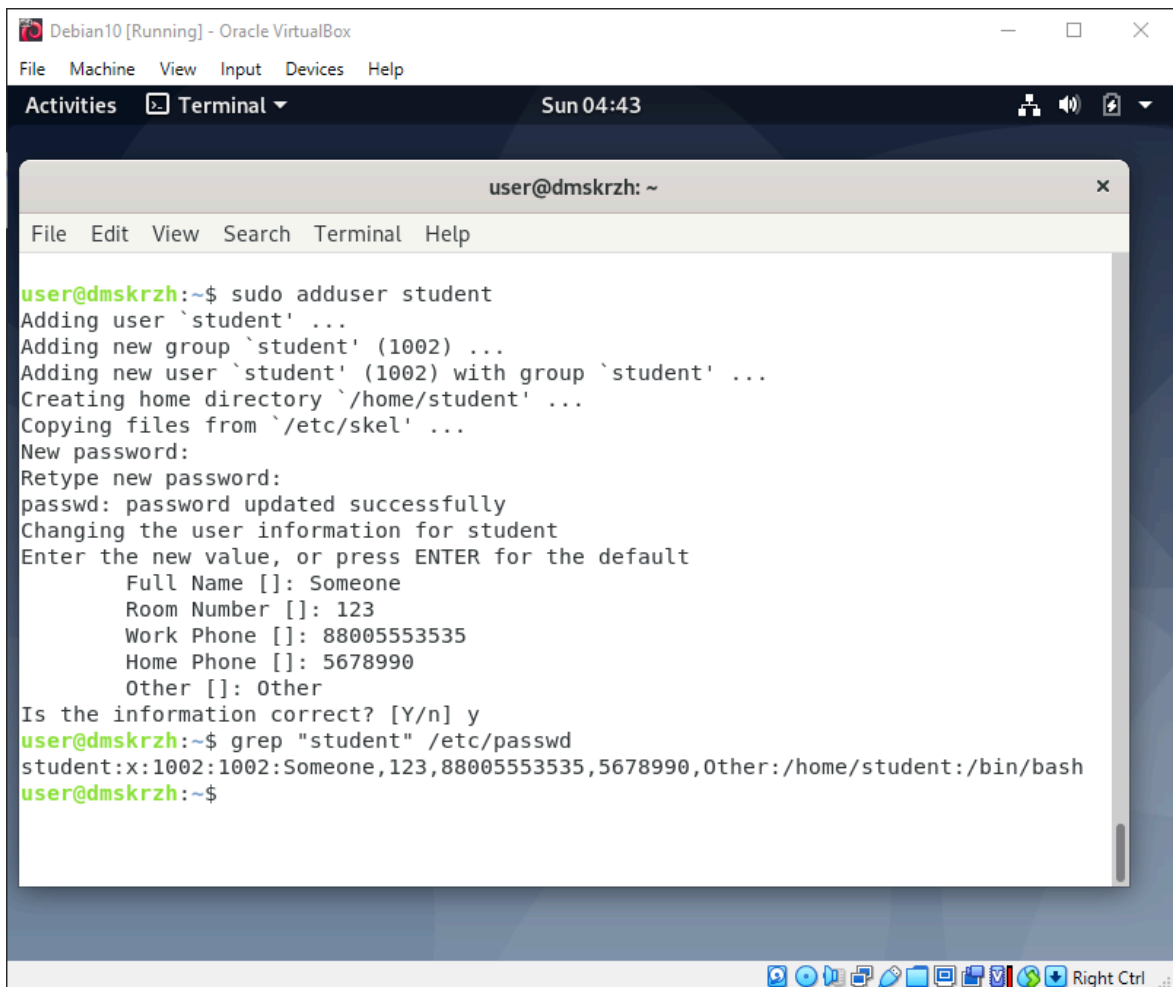


Рисунок 4.2 - Создание пользователя и просмотр подробной информации в Linux

5 Создать файл student.txt в домашнем каталоге пользователя student и вывести подробную информацию о нем и его домашнем каталоге в операционных системах Linux и Windows

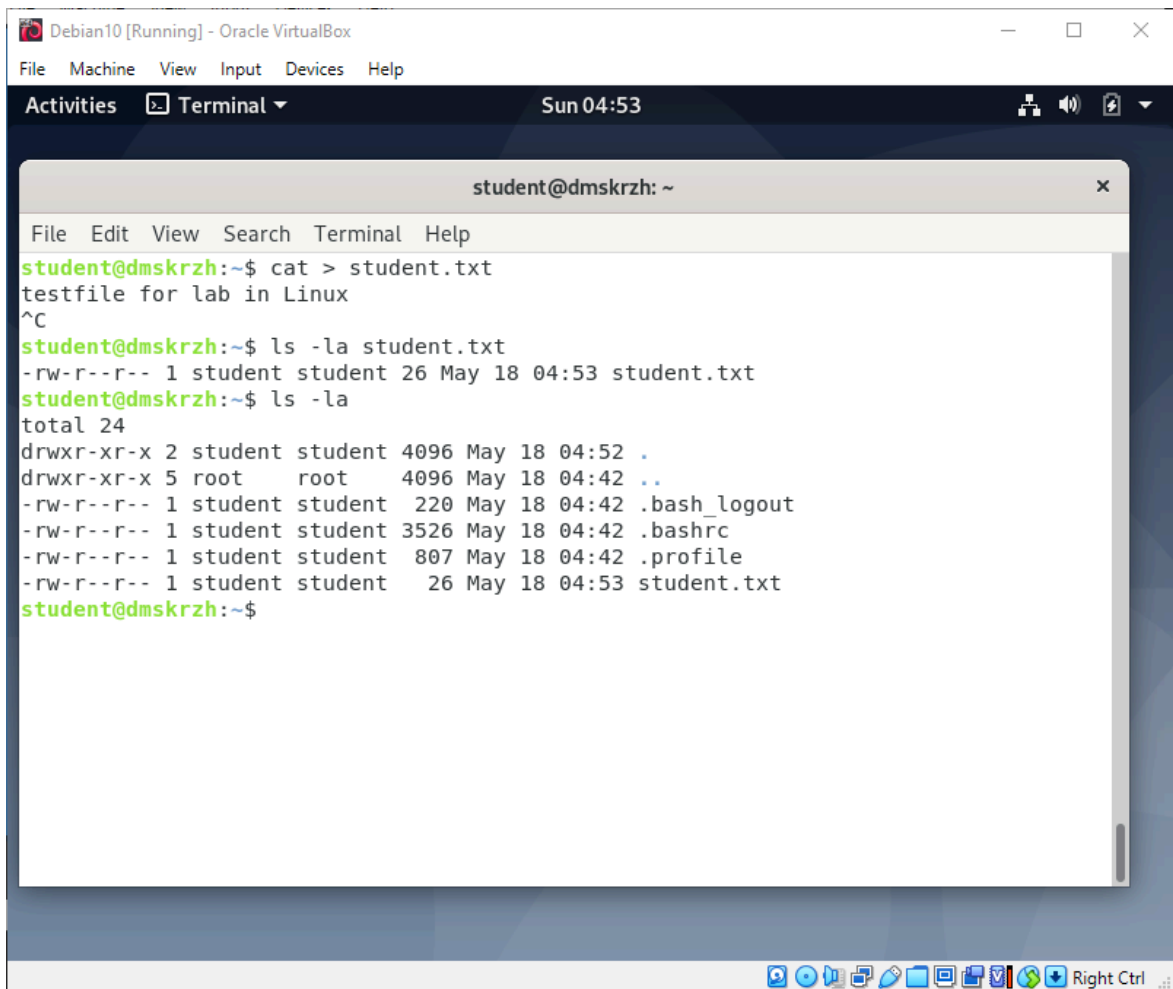


Рисунок 5.1 - Создание файла и вывод подробной информации о нем и домашнем каталоге в Linux

The screenshot shows a Windows PowerShell window titled "Windows_Server_2016 [Running] - Oracle VirtualBox". The window contains the following commands and output:

```
PS C:\Users\student.WIN-3G1QCSNBBDV> echo > student.txt
cmdlet Write-Output at command pipeline position 1
Supply values for the following parameters:
InputObject[0]: Testfile for lab in windows
InputObject[1]: net localgroup Users student /add
InputObject[2]:
PS C:\Users\student.WIN-3G1QCSNBBDV> dir student.txt

Directory: C:\Users\student.WIN-3G1QCSNBBDV

Mode                LastWriteTime         Length Name
----                -
-a-----         5/18/2025   2:05 AM             0 student.txt

PS C:\Users\student.WIN-3G1QCSNBBDV> dir

Directory: C:\Users\student.WIN-3G1QCSNBBDV

Mode                LastWriteTime         Length Name
----                -
d-r-----         5/18/2025   2:03 AM             Contacts
d-r-----         5/18/2025   2:03 AM             Desktop
d-r-----         5/18/2025   2:03 AM             Documents
d-r-----         5/18/2025   2:03 AM             Downloads
d-r-----         5/18/2025   2:03 AM             Favorites
d-r-----         5/18/2025   2:03 AM             Links
d-r-----         5/18/2025   2:03 AM             Music
d-r-----         5/18/2025   2:03 AM             Pictures
d-r-----         5/18/2025   2:03 AM             Saved Games
d-r-----         5/18/2025   2:03 AM             Searches
d-r-----         5/18/2025   2:03 AM             Videos
-a-----         5/18/2025   2:05 AM             0 student.txt

PS C:\Users\student.WIN-3G1QCSNBBDV>
```

The taskbar at the bottom shows the Windows Start button, search icon, task view icon, and several application icons. The system clock in the bottom right corner displays "2:06 AM 5/18/2025".

Рисунок 5.2 - Создание файла и вывод подробной информации о нем и домашнем каталоге в Windows

6 Сменить собственника файла student.txt и вывести подробную информацию о нем и его домашнем каталоге в операционных системах Linux и Windows

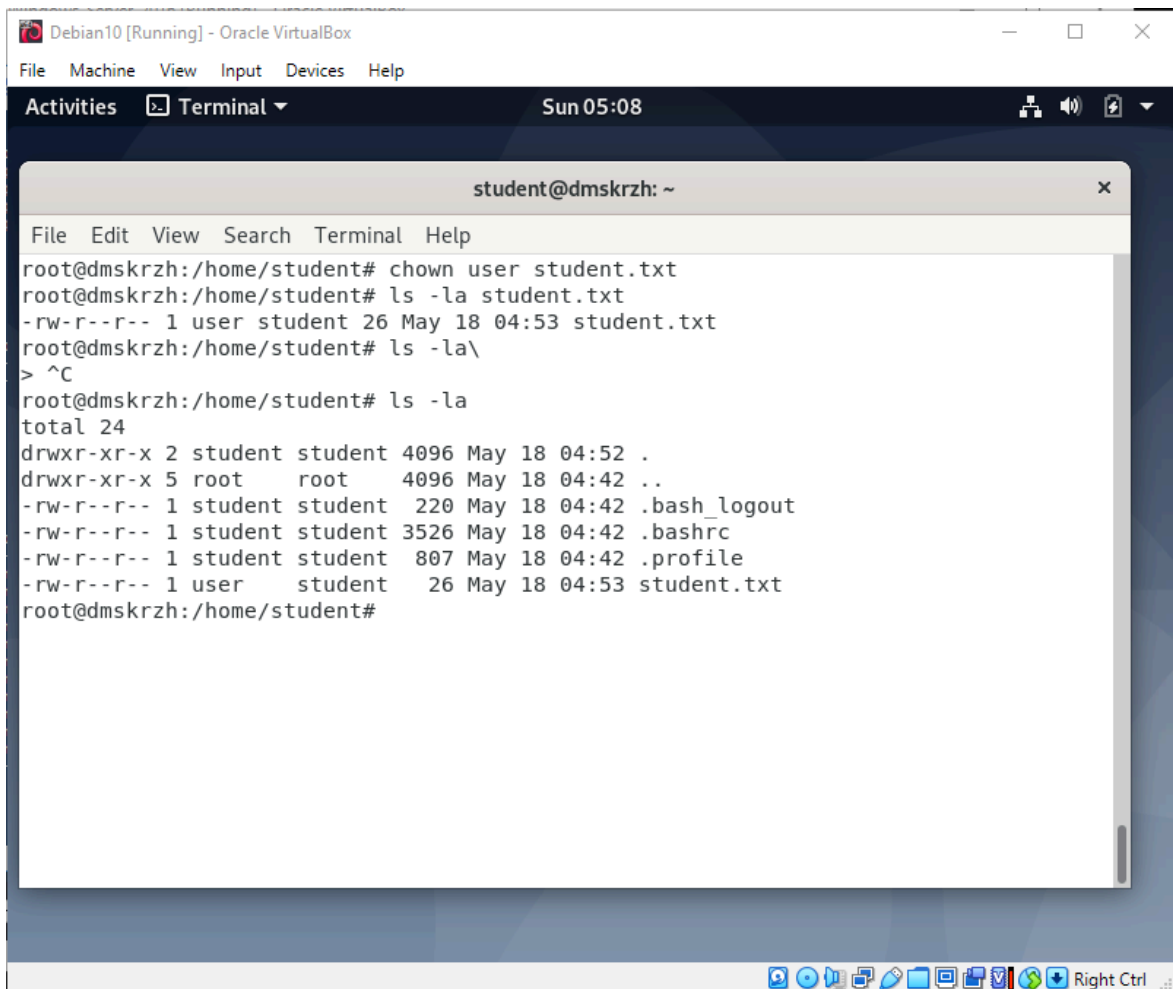


Рисунок 6.1 - Изменение собственника файла и вывод подробной информации о нем и домашнем каталоге в Linux

```
PS C:\Windows\system32> takeown /F C:\Users\student.WIN-3G1QCSNBBDV\student.txt
SUCCESS: The file (or folder): "C:\Users\student.WIN-3G1QCSNBBDV\student.txt" now owned by user "WIN-3G1QCSNBBDV\student".
PS C:\Windows\system32> dir C:\Users\student\student.txt
dir : Cannot find path 'C:\Users\student\student.txt' because it does not exist.
At line:1 char:1
+ dir C:\Users\student\student.txt
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\student\student.txt:String) [Get-ChildItem], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand

PS C:\Windows\system32> dir C:\Users\student.WIN-3G1QCSNBBDV\student.txt

Directory: C:\Users\student.WIN-3G1QCSNBBDV

Mode                LastWriteTime         Length Name
----                -
-a-----         5/18/2025   2:05 AM             0 student.txt

PS C:\Windows\system32> Get-ACL C:\Users\student.WIN-3G1QCSNBBDV\student.txt

Directory: C:\Users\student.WIN-3G1QCSNBBDV

Path      Owner                Access
----      -
student.txt WIN-3G1QCSNBBDV\Administrator NT AUTHORITY\SYSTEM Allow FullControl...

PS C:\Windows\system32> Get-ACL C:\Users\student.WIN-3G1QCSNBBDV

Directory: C:\Users

Path      Owner                Access
----      -
student.WIN-3G1QCSNBBDV BUILTIN\Administrators NT AUTHORITY\SYSTEM Allow FullControl...
```

Рисунок 6.2 - Изменение собственника файла и вывод подробной информации о нем и домашнем каталоге в Windows

7 На виртуальной машине с Linux проверить наличие установленного пакета с openssh-server и убедиться что служба запущена (при отсутствии выполнить установку и запуска данной службы)

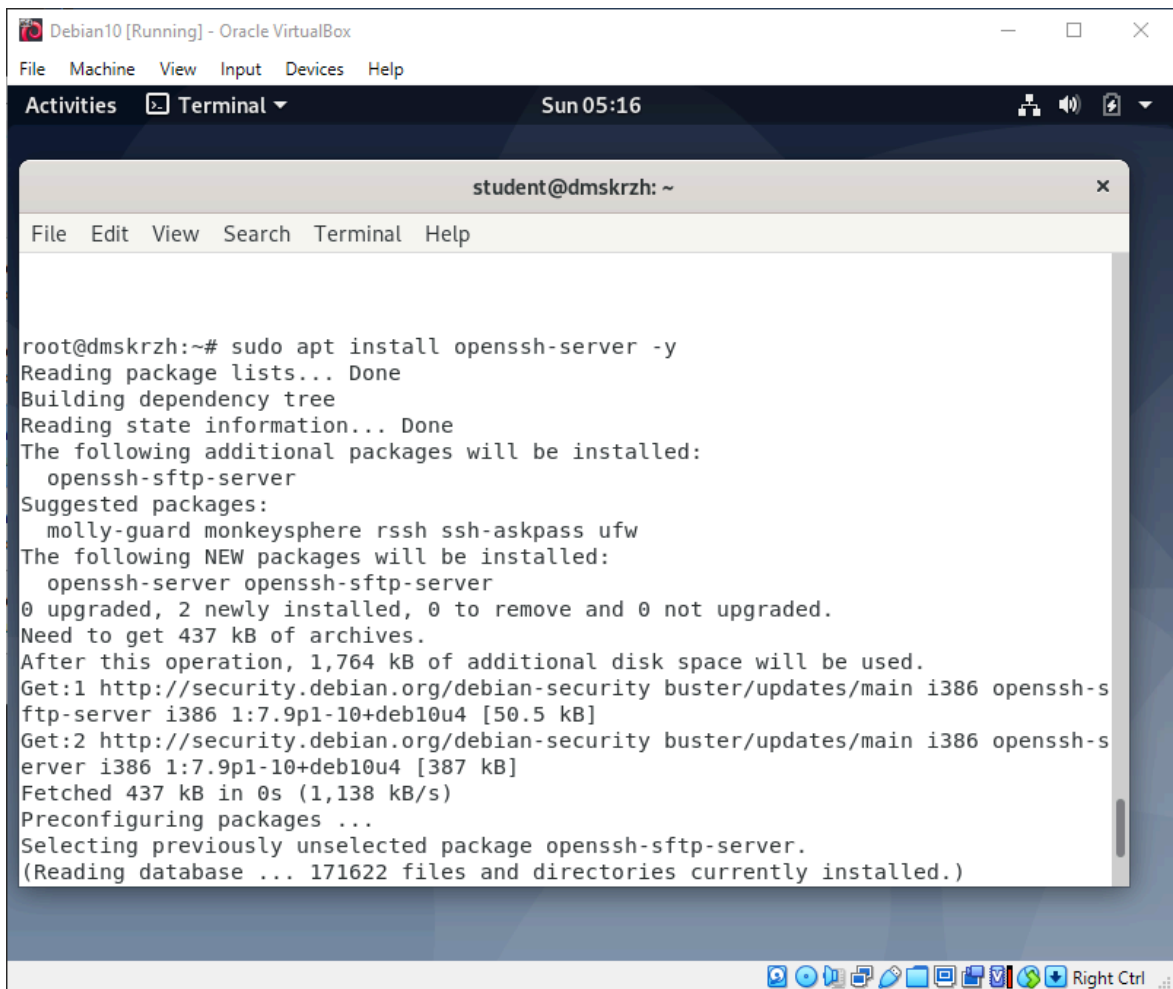
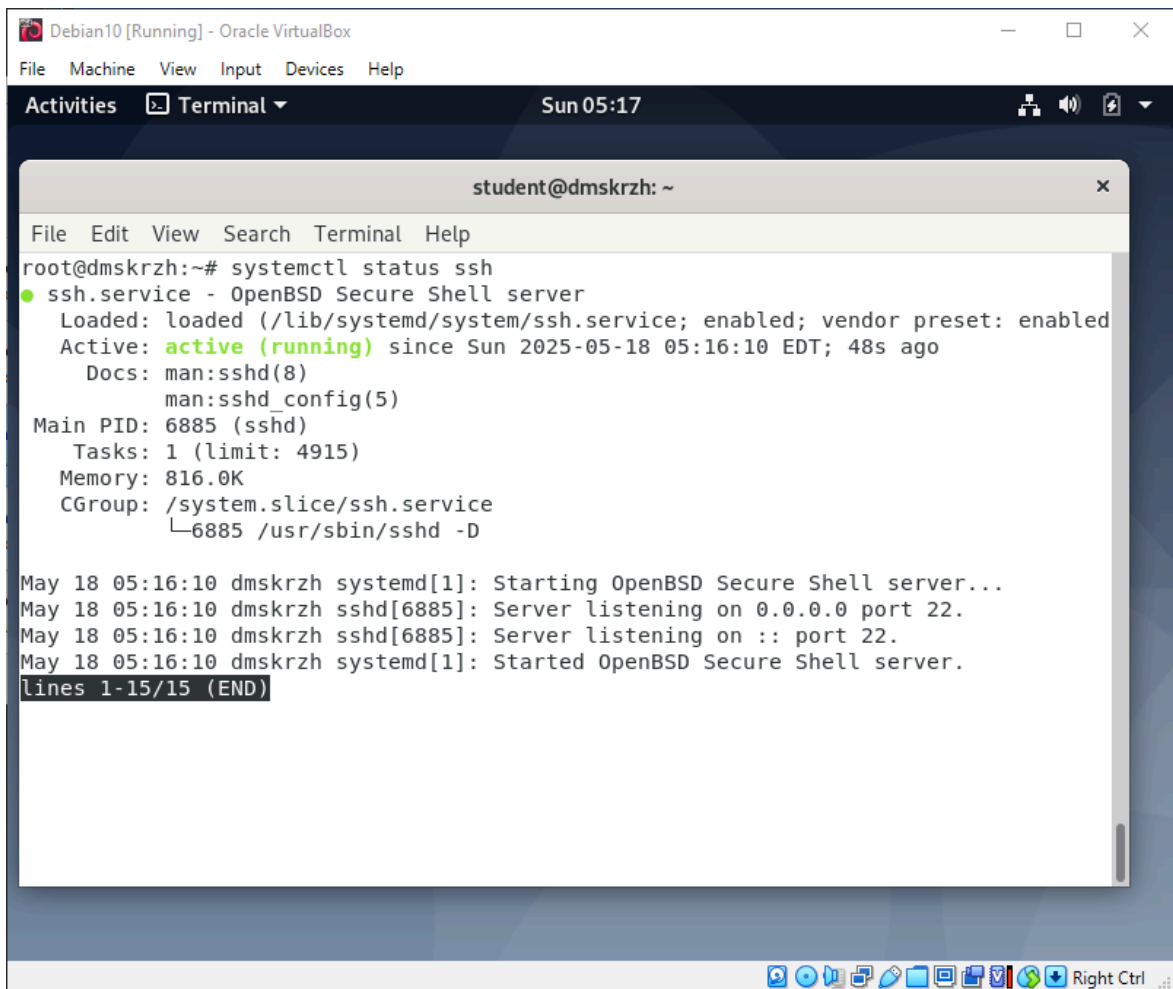


Рисунок 7.1 - Установка openssh



The image shows a terminal window titled "student@dmskrzh: ~" within an Oracle VM VirtualBox environment. The terminal displays the output of the command `systemctl status ssh`. The output indicates that the `ssh.service` is an OpenBSD Secure Shell server, loaded, enabled, and active (running) since Sun 2025-05-18 05:16:10 EDT. It shows the main PID as 6885 (sshd) and lists tasks, memory usage, and the CGroup. Below this, there are three log messages: "Starting OpenBSD Secure Shell server...", "Server listening on 0.0.0.0 port 22.", and "Started OpenBSD Secure Shell server." The terminal window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The top of the VirtualBox window shows "Debian10 [Running] - Oracle VirtualBox" and a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The bottom of the VirtualBox window shows a taskbar with various icons and a "Right Ctrl" button.

```
root@dmskrzh:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2025-05-18 05:16:10 EDT; 48s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 6885 (sshd)
    Tasks: 1 (limit: 4915)
   Memory: 816.0K
    CGroup: /system.slice/ssh.service
            └─6885 /usr/sbin/sshd -D

May 18 05:16:10 dmskrzh systemd[1]: Starting OpenBSD Secure Shell server...
May 18 05:16:10 dmskrzh sshd[6885]: Server listening on 0.0.0.0 port 22.
May 18 05:16:10 dmskrzh sshd[6885]: Server listening on :: port 22.
May 18 05:16:10 dmskrzh systemd[1]: Started OpenBSD Secure Shell server.
lines 1-15/15 (END)
```

Рисунок 7.2 - Служба ssh запущена

8 На виртуальной машине с Windows, включить и настроить удаленный доступ по RDP (Remote Desktop Protocol).

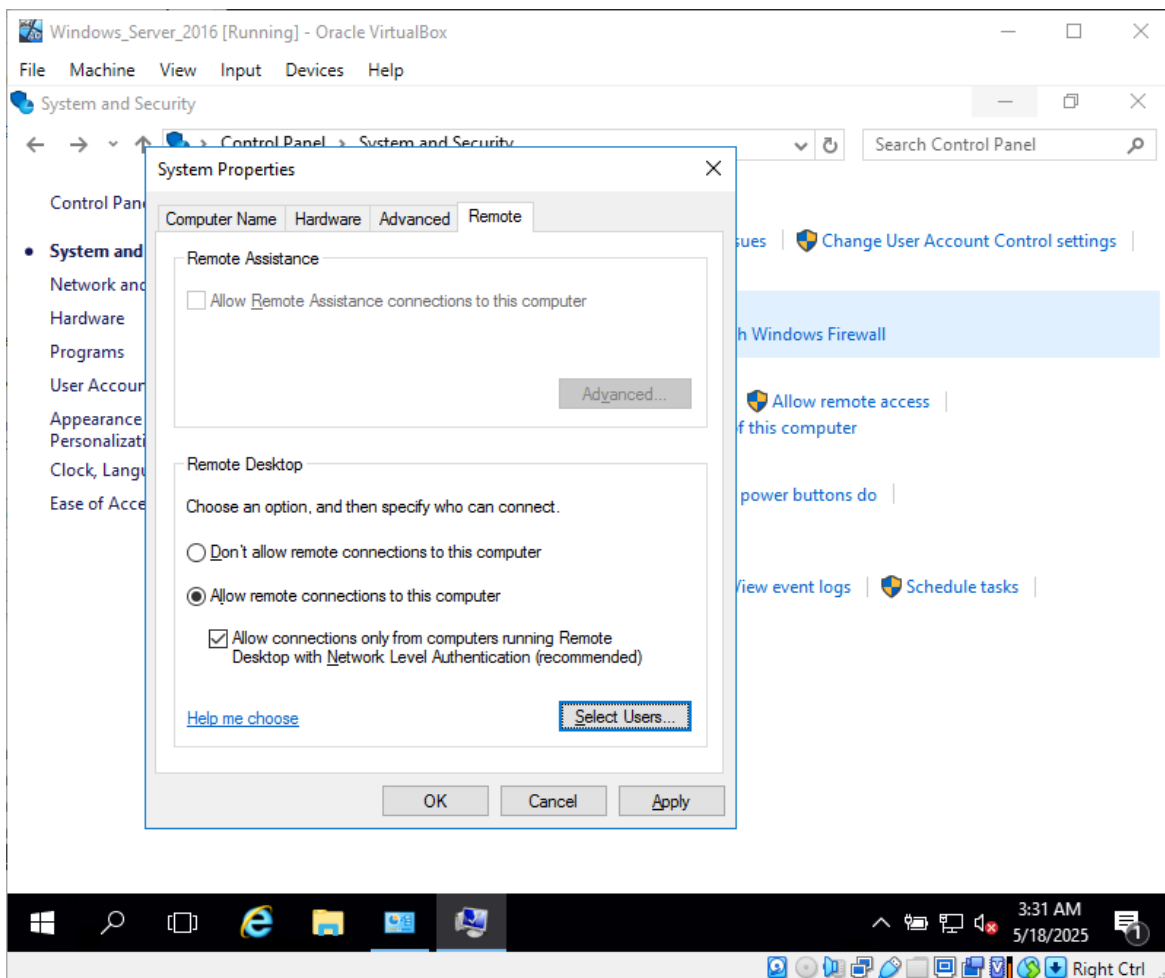


Рисунок 8.1 - Включение удаленного доступа

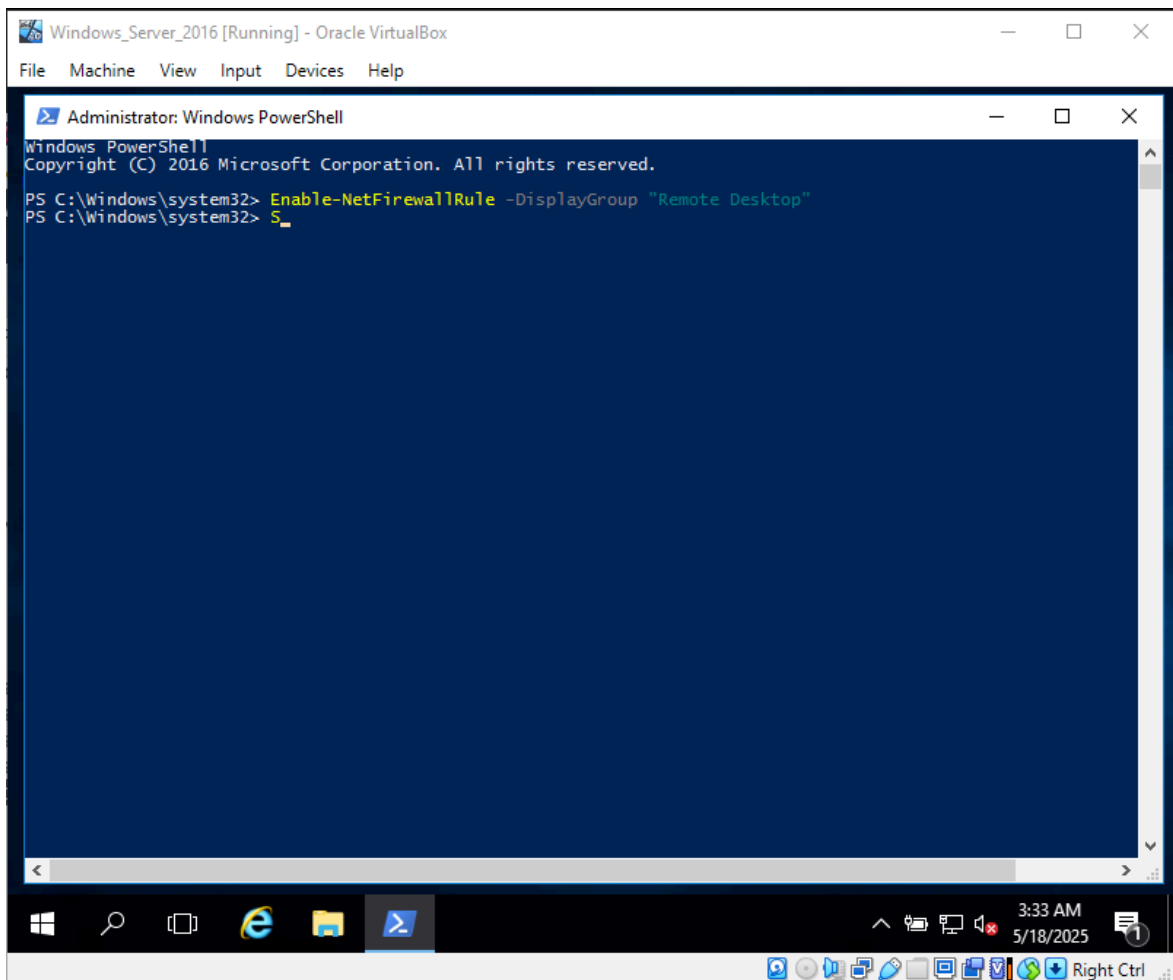


Рисунок 8.2 - Включение RDP через брандмауэр

9 Проверить возможность подключения к ВМ с Linux используя протокол SSH и Password Authentication (Для проверки необходимо установить Git Bash на локальный компьютер)

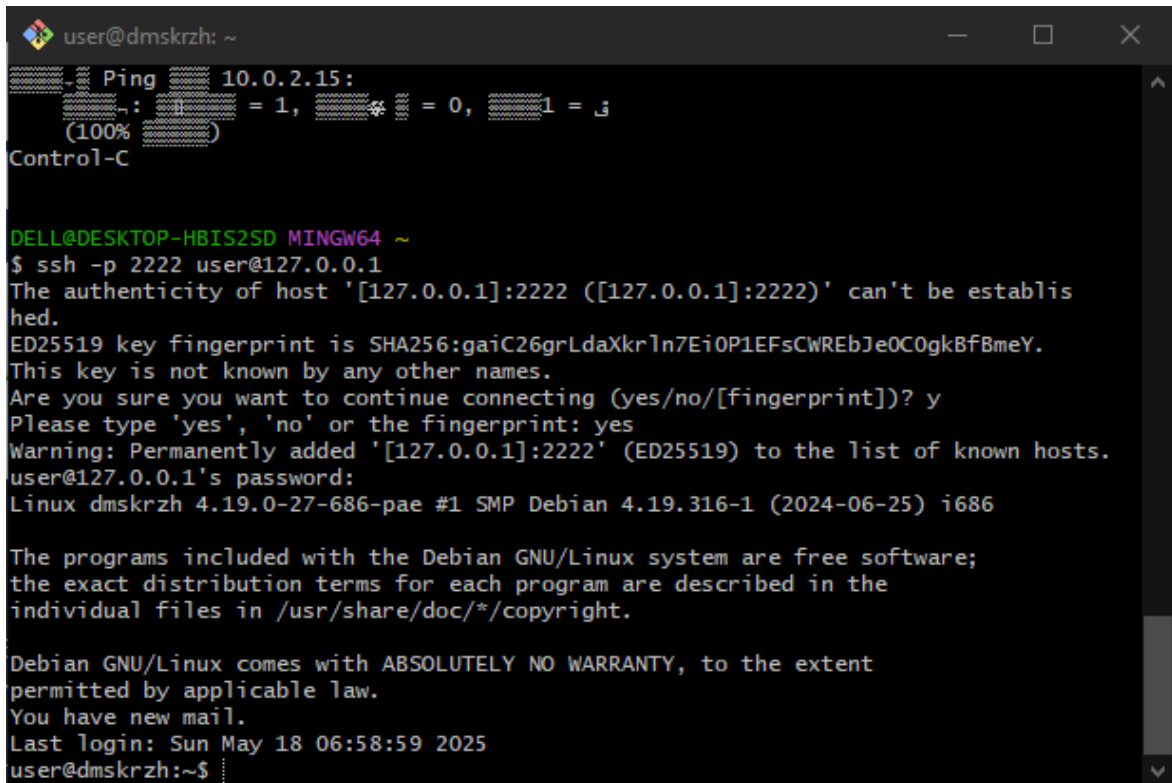
A screenshot of a terminal window titled 'user@dmskrzh: ~'. The window shows a ping command being executed: 'ping 10.0.2.15:'. The output shows a successful connection with a 100% success rate. Below this, the user presses 'Control-C'. Then, the user runs the command '\$ ssh -p 2222 user@127.0.0.1'. The terminal shows the SSH connection process, including a warning about the authenticity of the host and a confirmation to add the host to the list of known hosts. The user then enters their password, and the terminal shows the login prompt for the user 'user' on the Linux VM 'dmskrzh'. The VM is running Debian 4.19.316-1 (2024-06-25) i686. The terminal also displays the Debian GNU/Linux system's free software license and warranty information, and the last login time: 'Sun May 18 06:58:59 2025'. The prompt returns to 'user@dmskrzh:~\$'.

Рисунок 9.1 - Подключение по SSH

10 Изучить лучшие практики по настройке SSH с целью обеспечения максимально безопасного его использования

11 Внести изменения в конфигурацию SSH сервера на ВМ с Linux используя ранее изученные рекомендации

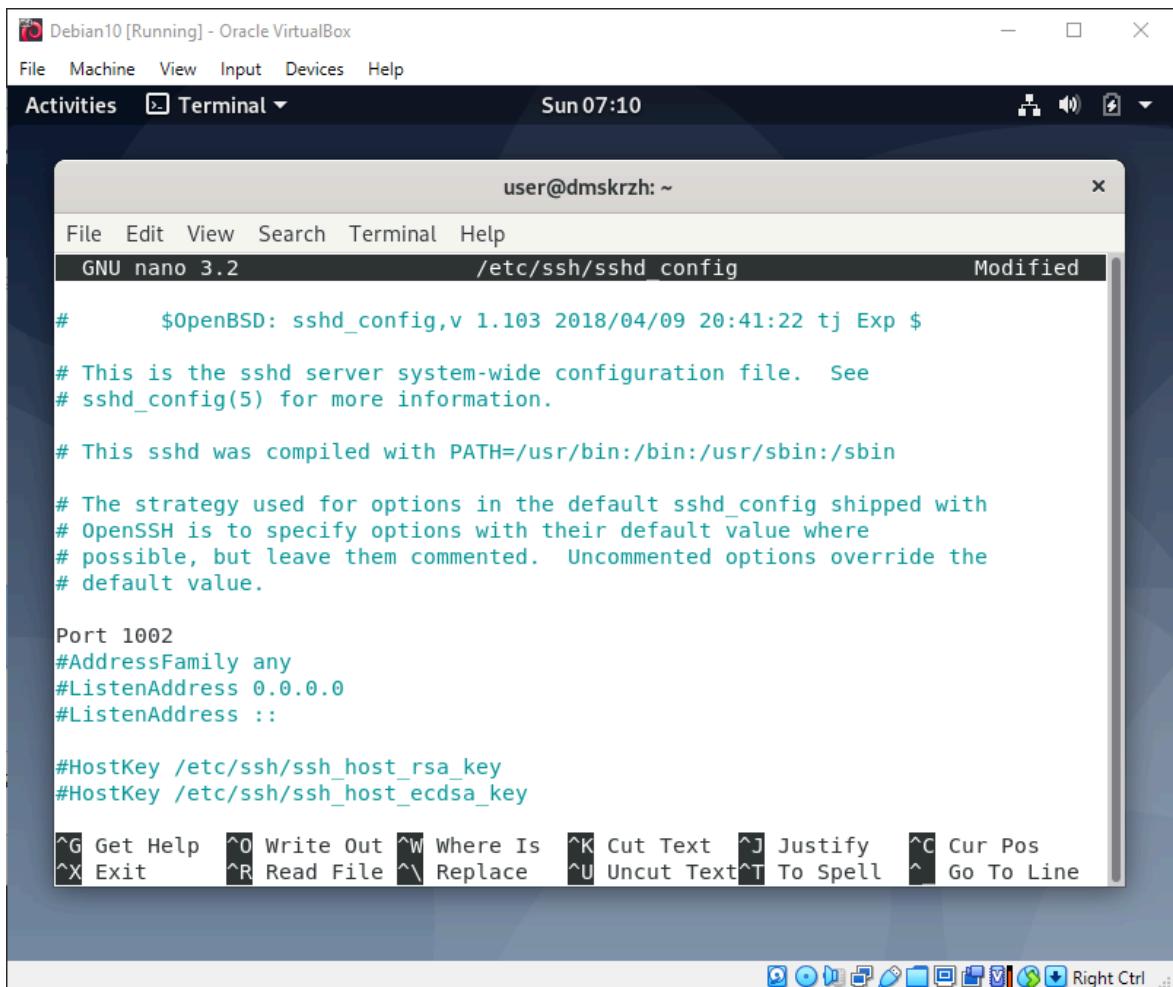


Рисунок 11.1 - Изменение порта

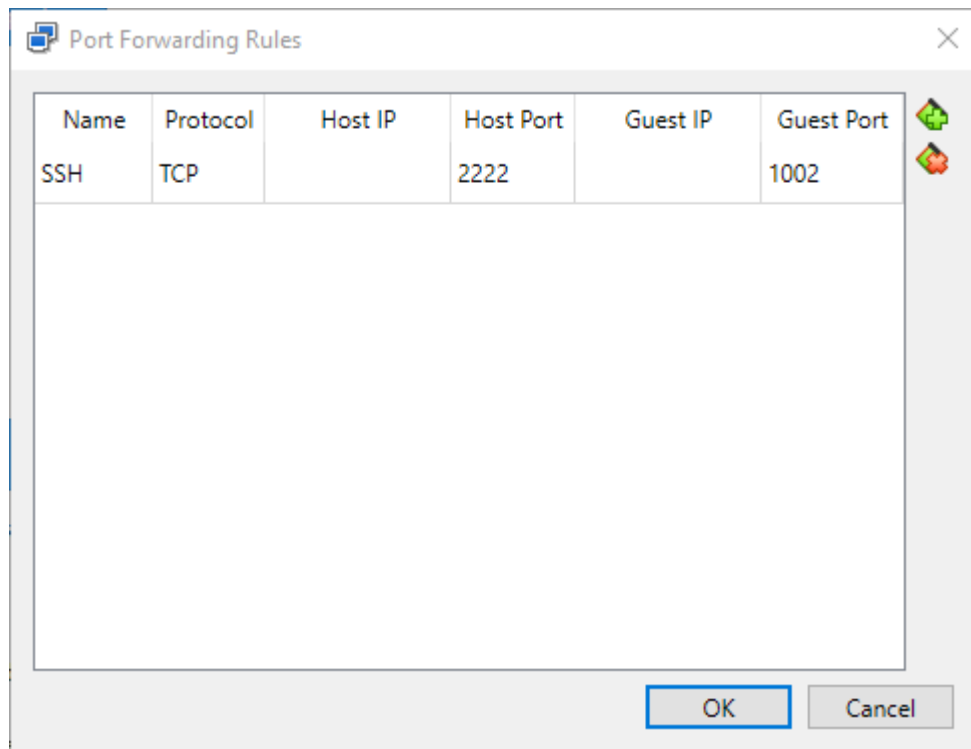


Рисунок 11.2 - Изменение порта в настройках сети VirtualBox

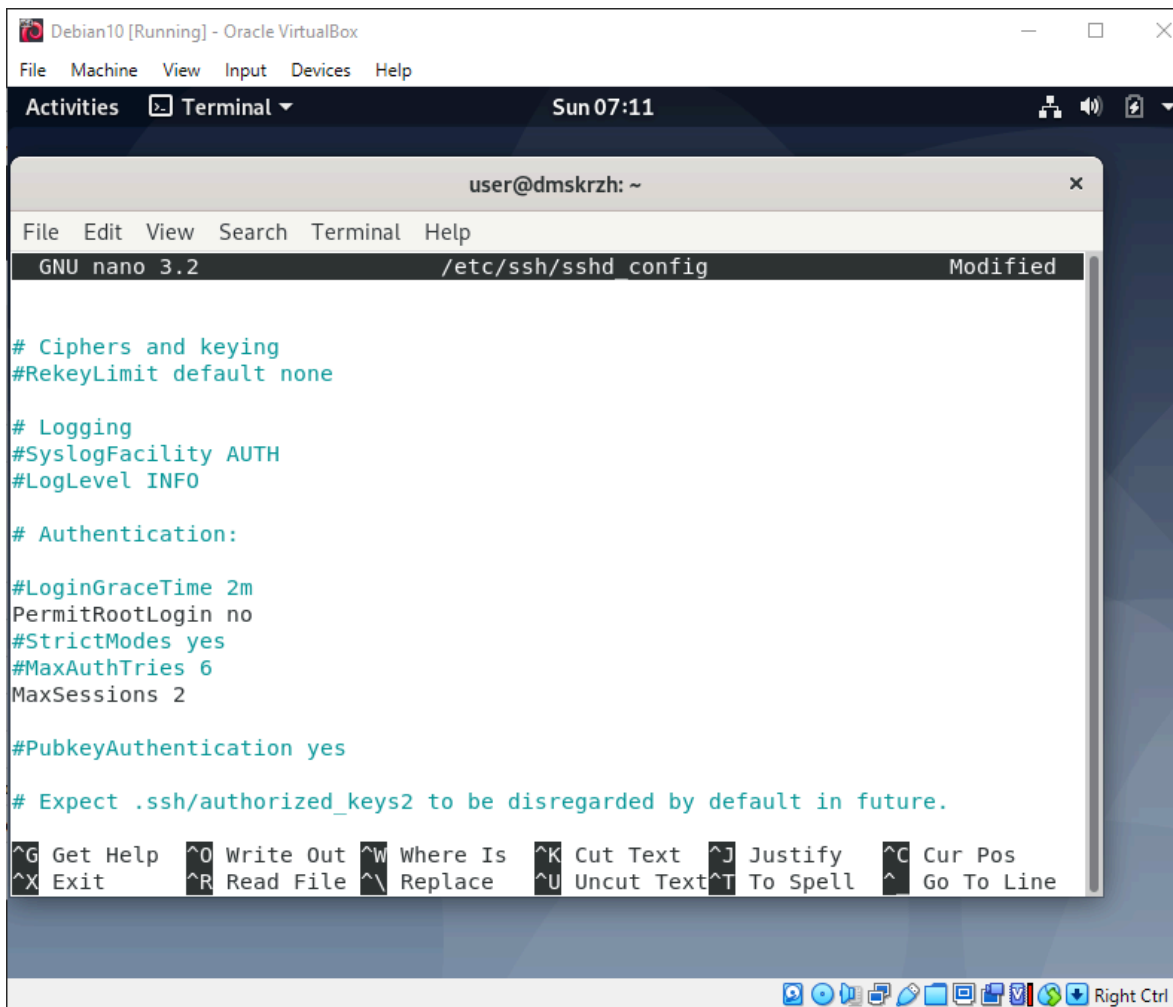


Рисунок 11.3 - Отключение возможности подключения под root и уменьшение максимального количества сессий

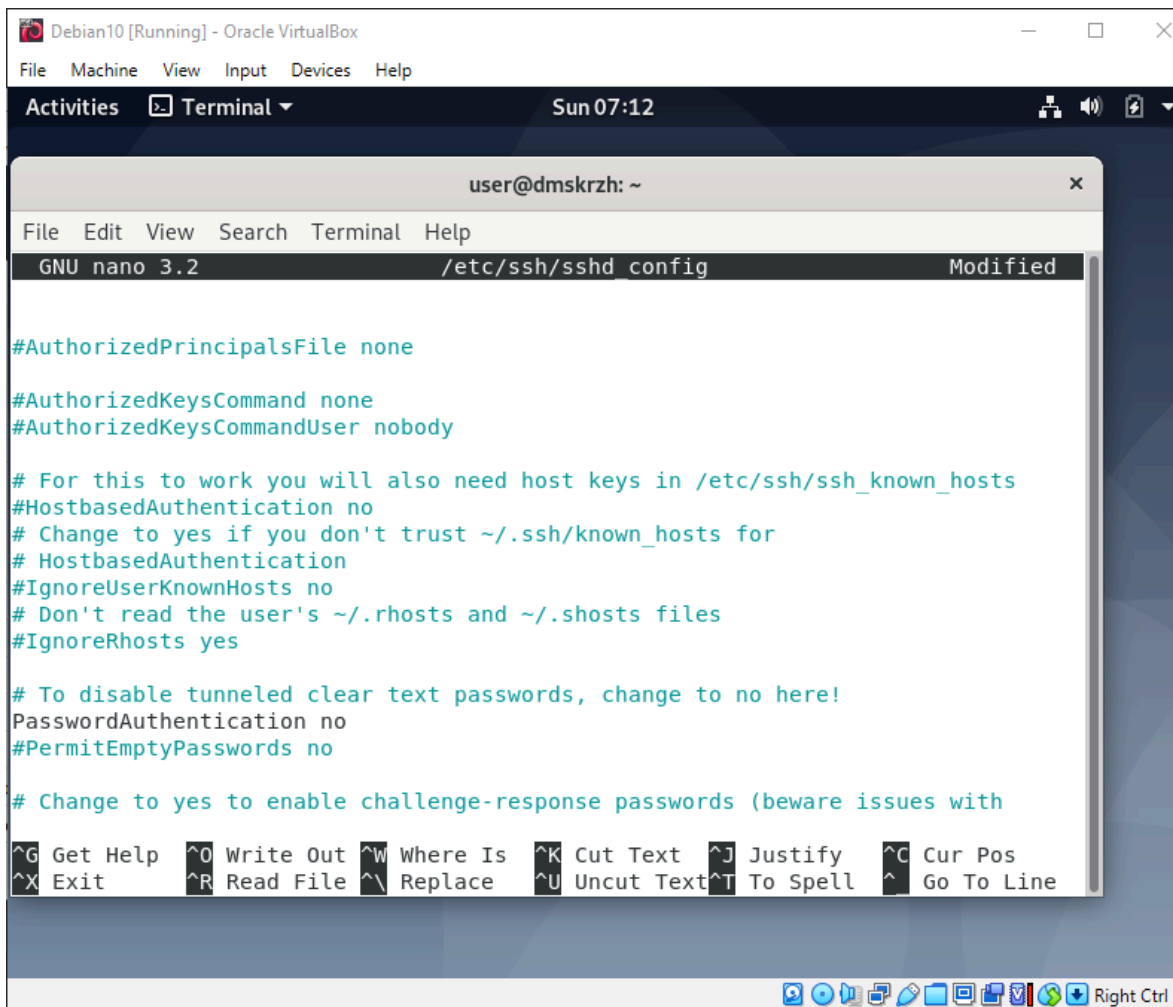


Рисунок 11.4 - Отключение подключения по паролю

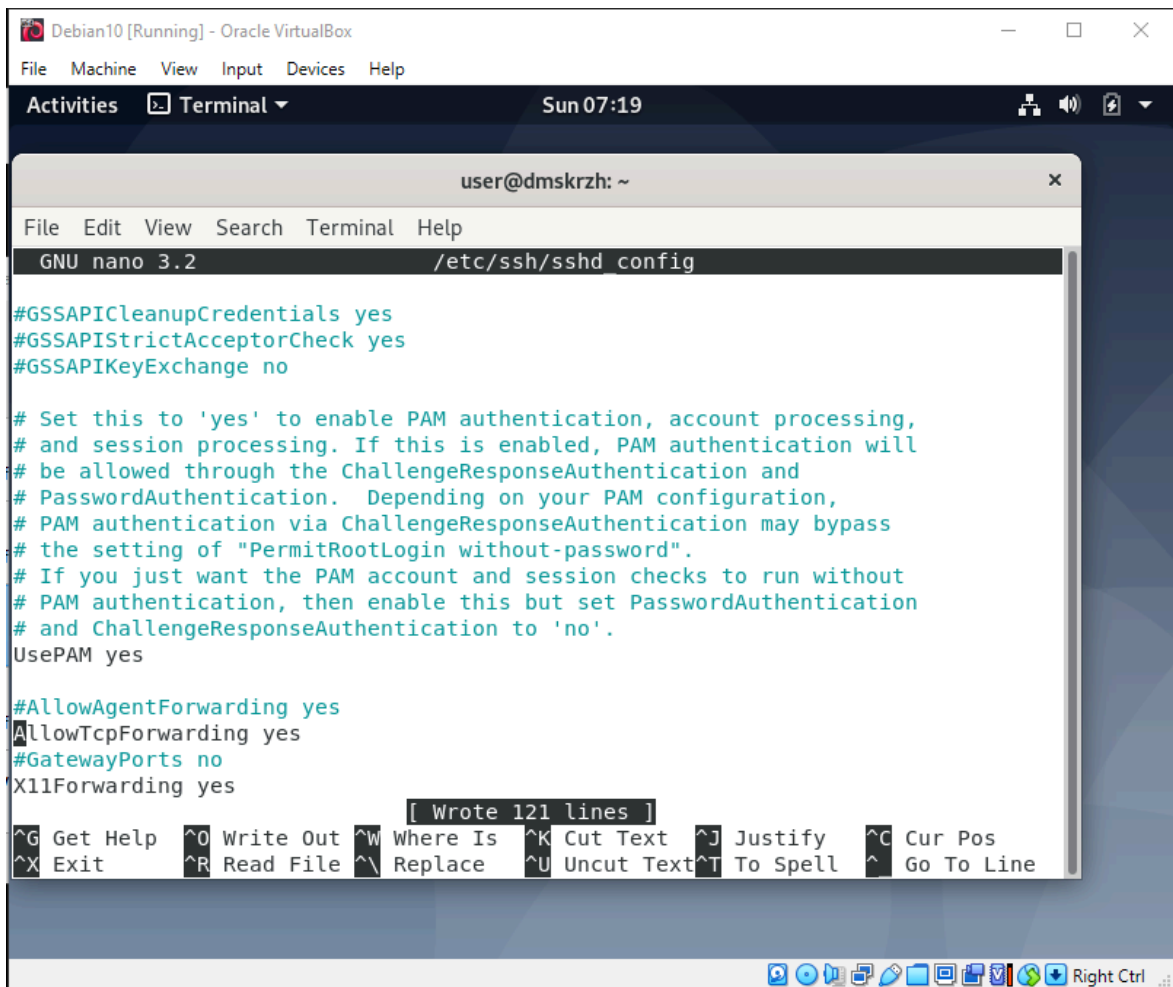
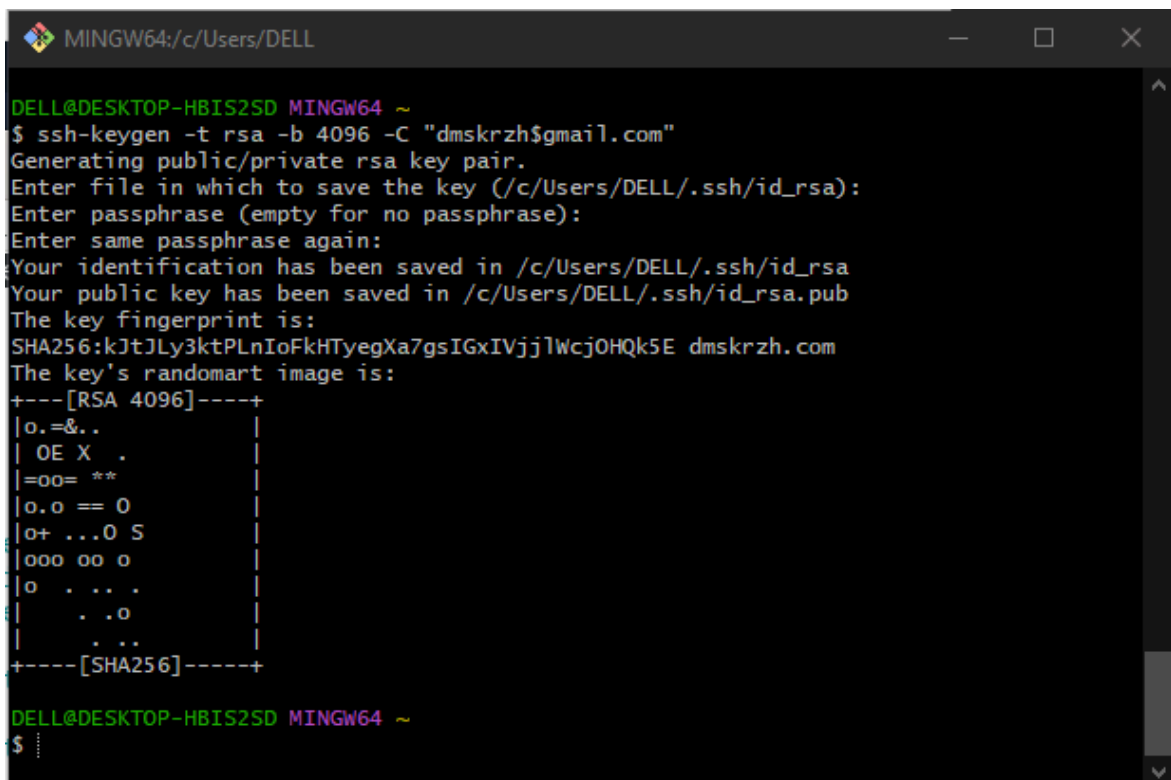


Рисунок 11.5 - Включение TCP

12 На локальном устройстве сгенерировать SSH key pair и загрузить публичный ключ на ВМ с Linux

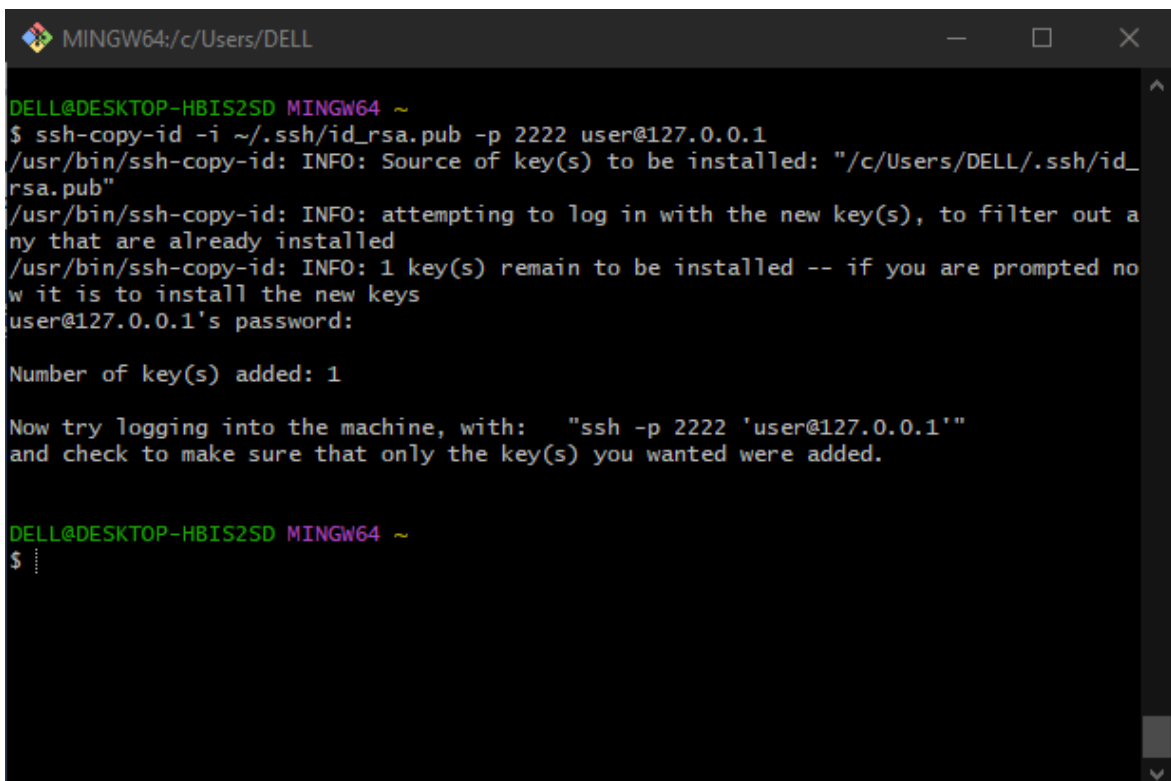


```
MINGW64:/c/Users/DELL

DELL@DESKTOP-HBIS2SD MINGW64 ~
$ ssh-keygen -t rsa -b 4096 -C "dmskrzh@gmail.com"
Generating public/private rsa key pair.
Enter file in which to save the key (/c/Users/DELL/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /c/Users/DELL/.ssh/id_rsa
Your public key has been saved in /c/Users/DELL/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:kJtJLy3ktPLnIoFkHTyegXa7gsIGxIVjjlWcjOHQk5E dmskrzh.com
The key's randomart image is:
+---[RSA 4096]-----+
|o.=&..|
| OE X .|
|=00= **|
|o.o == 0|
|o+ ...0 5|
|ooo oo o|
|o ... .|
| . .o|
| . ..|
+-----[SHA256]-----+

DELL@DESKTOP-HBIS2SD MINGW64 ~
$
```

Рисунок 12.1 - Создание ключей



```
MINGW64:/c/Users/DELL

DELL@DESKTOP-HBIS2SD MINGW64 ~
$ ssh-copy-id -i ~/.ssh/id_rsa.pub -p 2222 user@127.0.0.1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/c/Users/DELL/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
user@127.0.0.1's password:

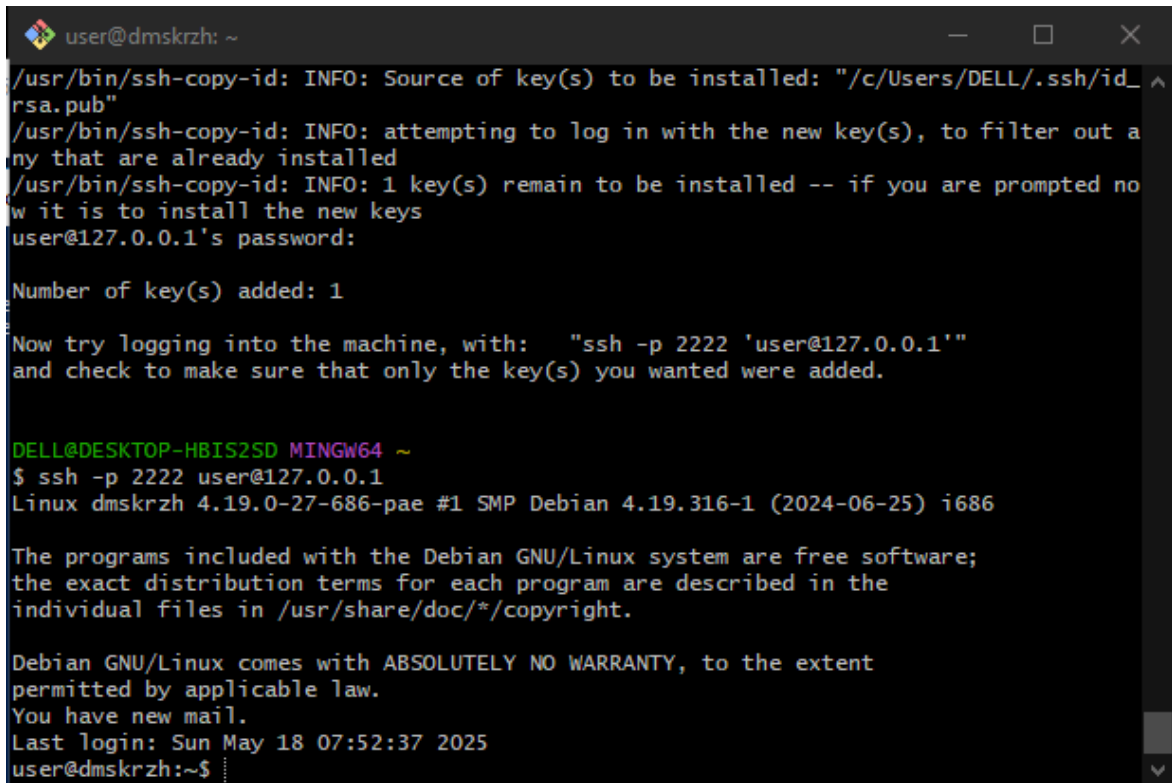
Number of key(s) added: 1

Now try logging into the machine, with: "ssh -p 2222 'user@127.0.0.1'"
and check to make sure that only the key(s) you wanted were added.

DELL@DESKTOP-HBIS2SD MINGW64 ~
$
```

Рисунок 12.2 - Пересылка ключа на линукс

13 Проверить возможность подключения по SSH используя Key Authentication



```
user@dmskrzh: ~  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/c/Users/DELL/.ssh/id_ ^  
rsa.pub"  
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out a  
ny that are already installed  
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted no  
w it is to install the new keys  
user@127.0.0.1's password:  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with:  "ssh -p 2222 'user@127.0.0.1'"  
and check to make sure that only the key(s) you wanted were added.  
  
DELL@DESKTOP-HBIS2SD MINGW64 ~  
$ ssh -p 2222 user@127.0.0.1  
Linux dmskrzh 4.19.0-27-686-pae #1 SMP Debian 4.19.316-1 (2024-06-25) i686  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
You have new mail.  
Last login: Sun May 18 07:52:37 2025  
user@dmskrzh:~$
```

Рисунок 13.1 - Успешное подключение с помощью ключа

14 Изучить особенности настройки и использования ВМ с Linux в качестве SSH Jump Host для организации подключения к ВМ с Windows по RDP

15 Проверить возможность получения удаленного доступа к ВМ с Window, используя для этого ВМ с Linux в качестве SSH Jump Host

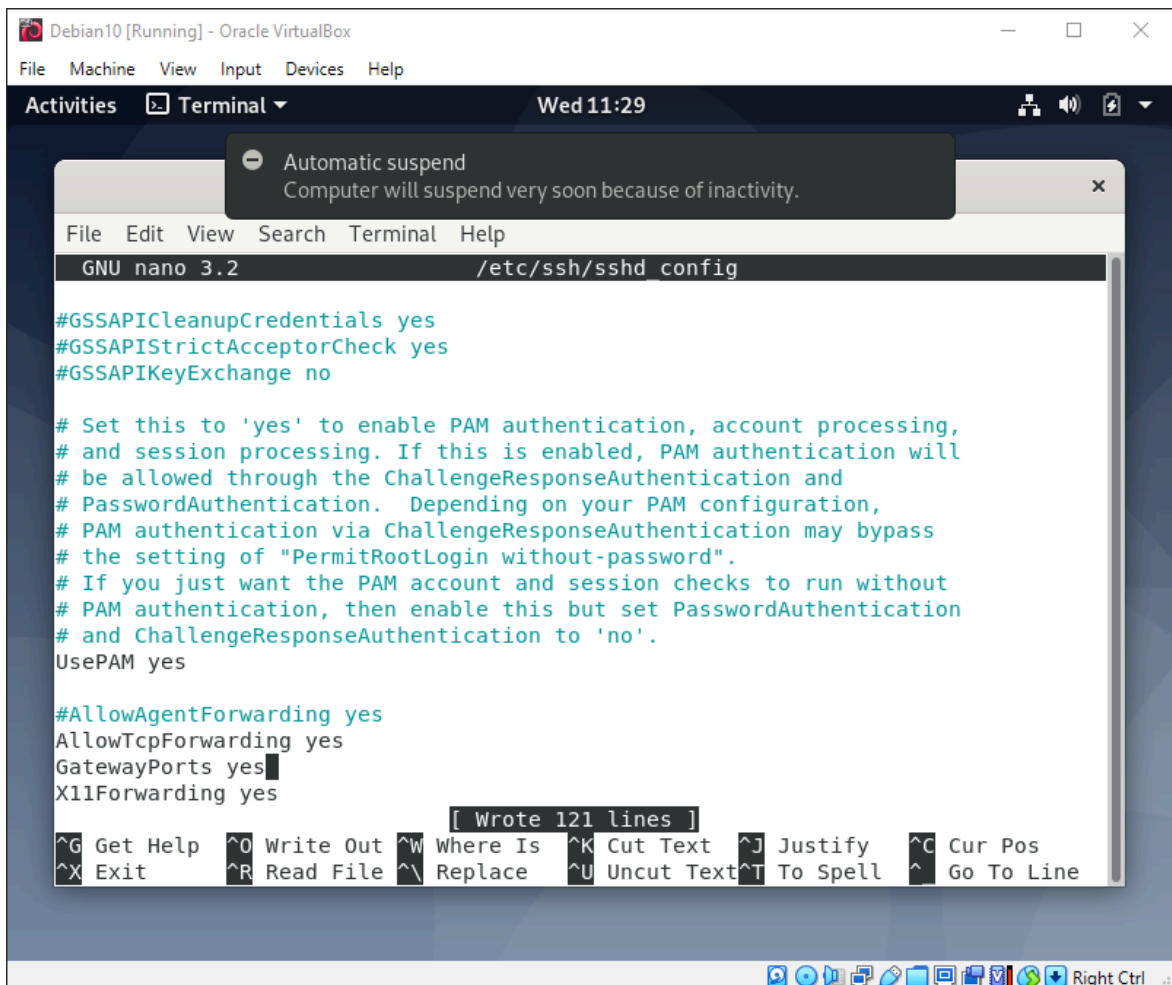


Рисунок 15.1 - Внесение изменений в конфигурацию SSH


```
user@dmskrzh: ~
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed May 21 11:09:59 2025 from 10.0.2.2
user@dmskrzh:~$ exit
logout
Connection to 127.0.0.1 closed.

DELL@DESKTOP-HBIS2SD MINGW64 ~
$ ssh -L 11389:192.168.1.2:3389 -p 2222 user@127.0.0.1
Linux dmskrzh 4.19.0-27-686-pae #1 SMP Debian 4.19.316-1 (2024-06-25) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed May 21 11:23:50 2025 from 10.0.2.2
user@dmskrzh:~$
```

Рисунок 15.2 - Создание SSH туннеля

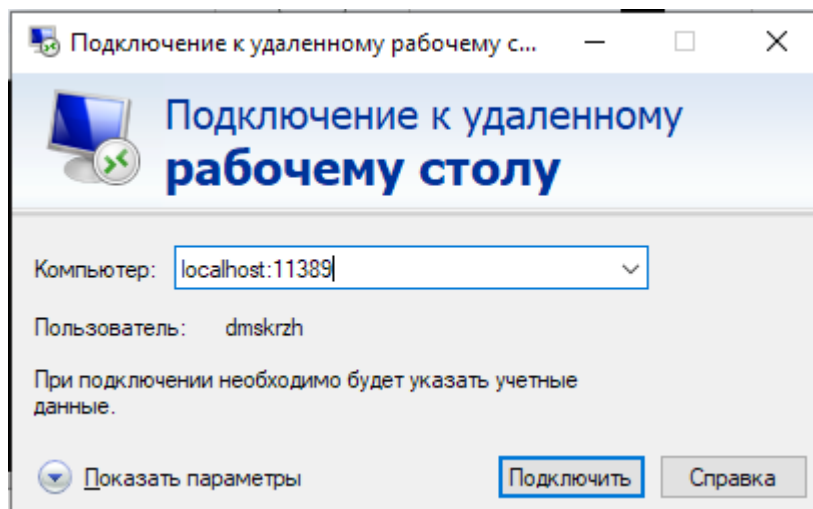


Рисунок 15.3 - Утилита подключения к ВМ на Windows

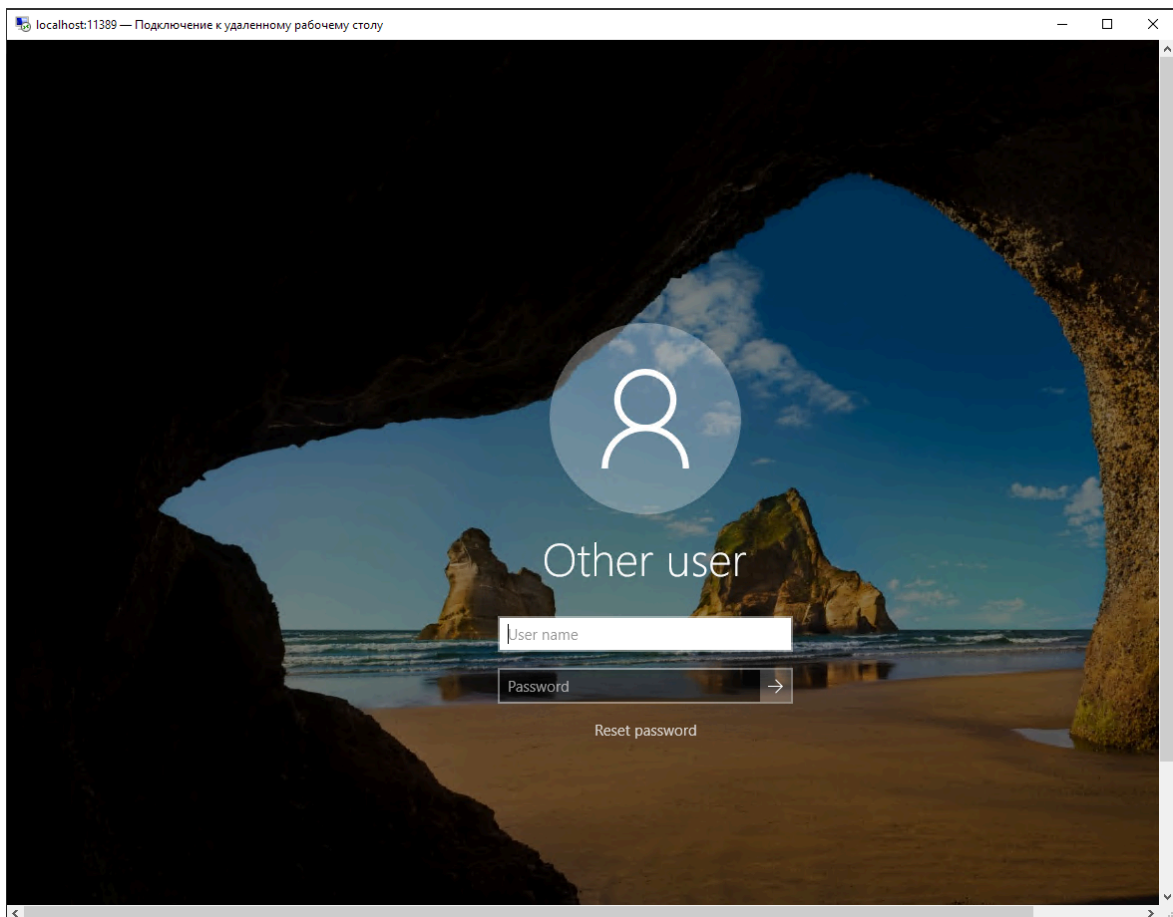


Рисунок 15.4 - Подключение к ВМ

Контрольные вопросы

1. Что такое учетная запись в операционной системе?

Учетная запись — это идентификатор пользователя в операционной системе, который определяет его права и доступ к ресурсам.

2. Где находятся сведения об учетных записях и группах в Linux?

Данные об учетных записях хранятся в файле `/etc/passwd`, а данные о группах в файле `/etc/group`

3. Расшифруйте запись об учетной записи Linux.

`rich:x:1003:100:Rich Blum:/home/rich:/bin/bash`

имя_пользователя:пароль:UID:GID:дополнительная_информация:домашний_каталог:используемая_оболочка

4. Где находятся сведения паролях пользователя в Linux?

Пароли хранятся в файле `/etc/shadow`.

5. Объясните запись об пароле в Linux.

rich:\$1\$E/moFkeTSUnTQ3KqZUoA4Fl2tPUoIc:16860:5:30:14:-1:-1:

имя_пользователя:зашифрованный_пароль:случайное_значение_для_усиления_защиты:дата_создания_пароля:дата_последнего_изменения_пароля:параметры_управления_сроками_действия_пароля

6. Какие утилиты Linux выводят сведения о пользователях?

whoami – выводит имя пользователя

who (w) – получение списка всех активных пользователей

id – выводит информацию об идентичности пользователя

7. Какие виды учетных записей существуют в Linux?

- Пользователь
- Суперпользователь
- Системный пользователь

8. Как следует работать с учетной записью суперпользователя?

При работе от имени суперпользователя следует быть очень внимательными, т.к. при ошибке могут потеряться системные данные, что потенциально способно нарушить загрузку системы.

9. Команды работы с учетной записью суперпользователя?

Команда su позволяет переключаться между пользователями внутри командной оболочки.

Команда sudo за один раз способна запускать только одну программу, указанную после ее имени.

10. Принципы создания сильного пароля

- Добавление цифр или знаков препинания
- Смешивание регистров
- Запись пароля в обратном порядке
- Увеличение длины пароля

11. Основные команды для работы с пользователями и группами.

- su – запускает командную оболочку от имени другого пользователя;
- sudo – выполняет команду от имени другого пользователя;
- useradd – для создания учетной записи;
- usermod – для изменения учетной записи;
- passwd – изменяет пароль пользователя;
- chage – может использоваться для установки даты истечения срока действия пользовательской учетной записи, установки

минимального и максимального срока действия пароля, даты истечения срока действия пароля, а также установки количества дней, в течение которых выводятся предупреждения об истечении срока действия пароля;

- userdel – для удаления учетной записи;
- groups – для ознакомления со списком групп;
- groupadd – добавление группы;
- groupmod – изменить имя группы пользователей;
- groupdel – удалить группу пользователей с помощью утилиты

12. Какие права существуют в Linux по отношению к файлам и каталогам?

Существуют права владения и доступа.

13. Что такое UID и GID?

UID (User ID) — уникальный идентификатор пользователя

GID (Group ID) — идентификатор группы

14. Объясните права доступа файла или каталога.

- rwx rw- r--

Флаг владелец группа остальные

x – Права на выполнение

r – Права на запись

w – Права на чтение

15. Основные команды и утилиты для работы с правами доступа.

chmod – изменяет режим доступа к файлу.

umask – определяет разрешения доступа к файлам по умолчанию.

chgrp – изменяет группу файла.

15. Что такое специальные права доступа?

SUID — выполнение программы с правами владельца

SGID — выполнение с правами группы

Sticky Bit — предотвращение удаления файлов не владельцем

16. Что такое SID?

SID (Security ID) – уникальный идентификатор объекта безопасности.

17. Какие виды групп пользователей существуют в Windows?

- Backup Operators
- Cryptographic Operators

- Debugger Users
- Distributed COM Users
- Event Log Readers
- Guests
- IIS_IUSRS
- Network Configuration Operators
- Performance Log Users
- Performance Monitor Users
- Power Users
- Remote Desktop Users
- Replicator
- Users

18. Основные командлеты для работы с пользователями и группами.

Add-LocalGroupMember – добавить пользователя в локальную группу;

Disable-LocalUser – отключить локальную учетную запись;

Enable-LocalUser – включить учетную запись (разблокировать);

Get-LocalGroup – получить информацию о локальной группе;

Get-LocalGroupMember – получить список пользователей в локальной группе;

Get-LocalUser – получить информацию о локальном пользователе;

New-LocalGroup – создать новую локальную группы;

New-LocalUser – создать пользователя;

Remove-LocalGroup – удалить группу;

Remove-LocalGroupMember – удалить члена из группы;

Remove-LocalUser – удалить локального пользователя;

Rename-LocalGroup – переименовать группу;

Rename-LocalUser – переименовать пользователя;

Set-LocalGroup – изменить группу;

Set-LocalUser – изменить пользователя.

19. Принципы настройки владения и прав доступа в Windows.

Для управления доступом к файлам и папкам в Windows на каждый объект файловой системы NTFS (каталог или файл) назначается специальный ACL (Access Control List, список контроля доступа). В ACL объекта задаются доступные операции (разрешения), которые может совершать с этим объектом пользователь и/или группы.

20. Базовые разрешения на доступ к каталогам.

- Full Control – Полный доступ (чтение, запись, изменение, удаление).

- Modify – Чтение, запись, удаление.
- List Folder Contents – Просмотр содержимого папки.
- Read & Execute – Чтение и выполнение.
- Write – Создание файлов и папок.
- Read – Чтение файлов и вложенных каталогов.

21. Базовые разрешения на доступ к файлам.

- Full Control – Полный доступ (чтение, запись, удаление).
- Modify – Чтение, запись, удаление.
- Read & Execute – Чтение и выполнение файлов.
- Write – Запись и удаление содержимого файла (без удаления самого файла).
- Read – Чтение файла.