МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №9
«Обеспечение безопасности в среде операционной системы GNU/Linux»

Практическая работа
по дисциплине «Системное программное обеспечение»
студента 3 курса группы ИВТ-б-о-222(2)
Чудопалова Богдана Андреевича

09.03.01 «Информатика и вычислительная техника»

Симферополь, 2025

Ход работы

1. Определить для обычного пользователя возможность для запуска команды tcpdump через команду sudo — для начала создал пользователя

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bogdan@bogdan-virtualbox:~$ sudo useradd -m example
[sudo] пароль для bogdan:
bogdan@bogdan-virtualbox:~$ sudo passwd example
Новый пароль:
Повторите ввод нового пароля:
passwd: пароль успешно обновлён
bogdan@bogdan-virtualbox:~$
```

Попробовал от его лица запустить tcpdump

```
bogdan@bogdan-virtualbox:~$ sudo su example
$ whoami
example
$ sudo tcpdump
[sudo] пароль для example:
example отсутствует в файле sudoers.
$
```

Отредактировал sudoers с помощью команды sudo visudo

```
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

example ALL=(ALL) /usr/bin/tcpdump
```

Результат

```
$ whoami
example
$ sudo tcpdump
[sudo] пароль для example:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

2. Установить пароль на загрузчик операционной системы — сгенерировал хеш-пароля

```
bogdan@bogdan-virtualbox:~$ grub-mkpasswd-pbkdf2
Введите пароль:
Повторно введите пароль:
Хэш PBKDF2 вашего пароля: grub.pbkdf2.sha512.10000.65D101E239D7C4A206E2FBD91ACAAF23BAB56FA19C4
D229655E46EF5A42CB0F60DDFBC091EFD7BEE854E96A24FC119C0903408F159FB.6273252A47CE482C632C3238A812
C2B08CAC73EBBEEC68C5ED880F97B8B0A59F80E5A6B67C50ED6021F3C69409D79E40B1A557ADC315
bogdan@bogdan-virtualbox:~$
```

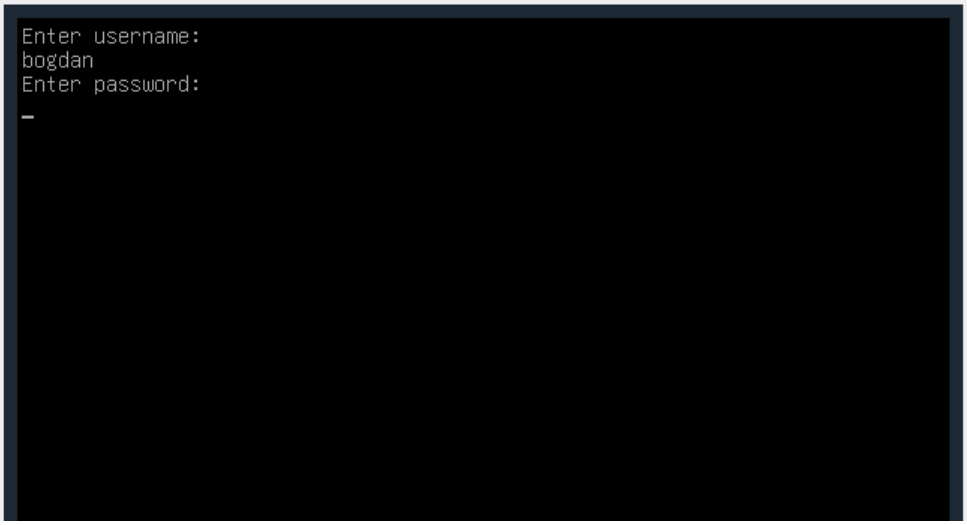
Далее отредактировал файл /etc/grub.d/00_header

```
cat << EOF
set superuser="bogdan"
password_pbkdf2 bogdan grub.pbkdf2.sha512.10000.65D101E239D7C4A206E2FBD91ACAAF23BAB56FA19C494F
9655E46EF5A42CB0F60DDFBC091EFD7BEE854E96A24FC119C0903408F159FB.6273252A47CE482C632C3238A812DAE
08CAC73EBBEEC68C5ED880F97B8B0A59F80E5A6B67C50ED6021F3C69409D79E40B1A557ADC315
EOF
-- РЕЖИМ ВСТАВКИ --
```

Обновил grub

```
bogdan@bogdan-virtualbox:~$ sudo vim /etc/grub.d/00_header
bogdan@bogdan-virtualbox:~$ sudo update-grub
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/lubuntu-grub-theme.cfg'
Generating grub configuration file ...
Found theme: /usr/share/grub/themes/lubuntu-grub-theme/theme.txt
Found linux image: /boot/vmlinuz-6.11.0-17-generic
Found initrd image: /boot/initrd.img-6.11.0-17-generic
Found memtest86+x64 image: /boot/memtest86+x64.bin
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
bogdan@bogdan-virtualbox:~$
```

После перезагрузки



3. Отредактировать существующую политику для SELinux с сервисом Samba таким образом, чтобы можно было настроить работу с разделяемым ресурсом, находящимся в произвольном месте файловой системы — для начала включил permissive режим, чтобы избежать блокировок действий и обойтись только занесением в логи

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
# enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
# disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
# default - equivalent to the old strict and targeted policies
# mls     - Multi-Level Security (for military and educational use)
# src     - Custom policy built from source
SELINUXTYPE=default

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
~
~
```

Активировал selinux

```
bogdan@bogdan-virtualbox:~$ sudo vim /etc/selinux/config
bogdan@bogdan-virtualbox:~$ sudo selinux-activate
Activating SE Linux
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/lubuntu-grub-theme.cfg'
Generating grub configuration file ...
Found theme: /usr/share/grub/themes/lubuntu-grub-theme/theme.txt
Found linux image: /boot/vmlinuz-6.11.0-17-generic
Found initrd image: /boot/initrd.img-6.11.0-17-generic
Found memtest86+x64 image: /boot/memtest86+x64.bin
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
SE Linux is activated.  You may need to reboot now.
bogdan@bogdan-virtualbox:~$
```

Создал в /mnt директорию разделяемого ресурса

```
bogdan@bogdan-virtualbox:~$ sudo mkdir /mnt/task
```

Создал профиль конфигурации для данной директории

```
[guestshare]
   path = /mnt/task
   read only = no
   browseable = yes
   valid users =
   guest ok = yes
```

Перезапустил сервисы

```
bogdan@bogdan-virtualbox:~$ service smbd restart
bogdan@bogdan-virtualbox:~$ service nmbd restart
bogdan@bogdan-virtualbox:~$
```

Просмотр логов selinux, дал понять, что есть ошибки с samba

```
bogdan@bogdan-virtualbox: ~
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1746910692.813:65): avc:  denied  { getattr } for  pid=707 comm="pool-switcheroo" path="/usr/sh
are/locale-langpack/ru/LC_MESSAGES/libc.mo" dev="sda1" ino=1211269 scontext=system_u:system_r:switcheroo_t:s0 tcon
text=system_u:object_r:usr_t:s0 tclass=file permissive=1

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.
```

Для их устранения изменил тип контекста безопасности директории

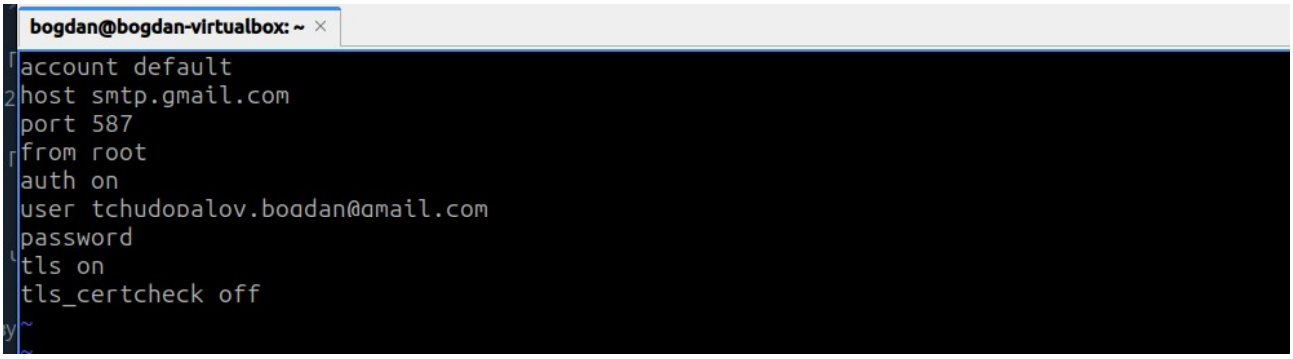
```
bogdan@bogdan-virtualbox:~$ sudo semanage fcontext -a -t samba_share_t "/mnt/task(/.*)?"
bogdan@bogdan-virtualbox:~$
```

```
bogdan@bogdan-virtualbox:~$ sudo restorecon -Rv /mnt/task/
Relabeled /mnt/task from system_u:object_r:mnt_t:s0 to system_u:object_r:samba_share_t:s0
bogdan@bogdan-virtualbox:~$ sudo ls -Zd /mnt/task/
system_u:object_r:samba_share_t:s0 /mnt/task/
bogdan@bogdan-virtualbox:~$
```

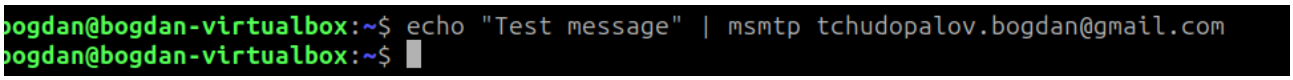
После этого просмотри логи

```
bogdan@bogdan-virtualbox:~$ sudo su root
root@bogdan-virtualbox:/home/bogdan# echo " " > /var/log/audit/audit.log
root@bogdan-virtualbox:/home/bogdan# service smbd restart
root@bogdan-virtualbox:/home/bogdan# service nmbd restart
root@bogdan-virtualbox:/home/bogdan# audit2why < /var/log/audit/audit.log
Nothing to do
root@bogdan-virtualbox:/home/bogdan#
```

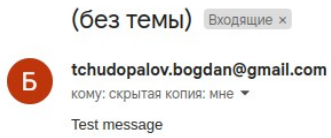
4. Настроить программу logwatch на отсылку оповещений по почте о неудачных попытках входа в систему — для начала настроил msmtp, для этого в домашней директории создал конфиг



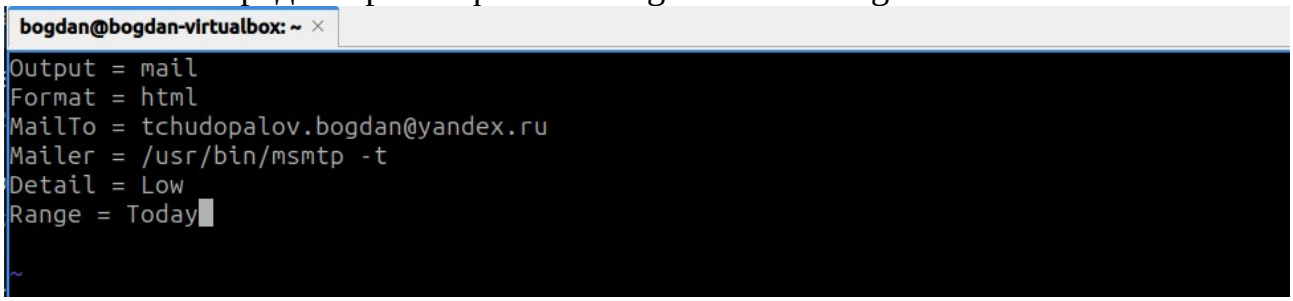
Далее протестировал сервер



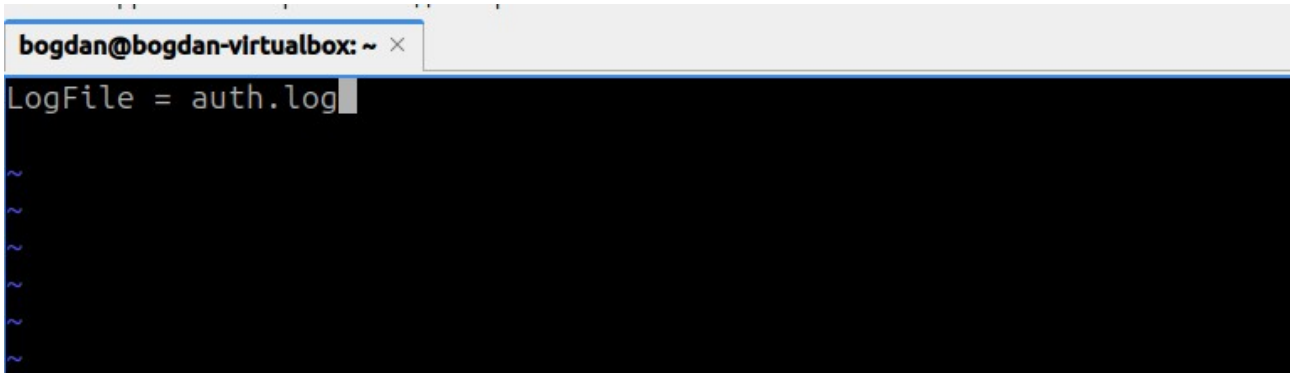
Результат



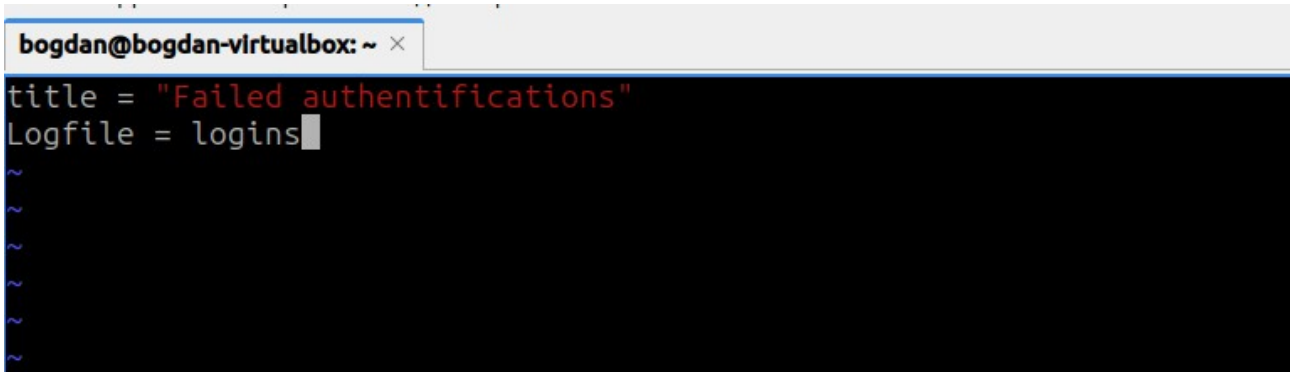
После этого отредактировал файл /etc/logwatch/conf/logwatch.conf



Далее добавил сервис, который будет анализировать информацию из файла /var/log/auth.log, назвал сервис logins

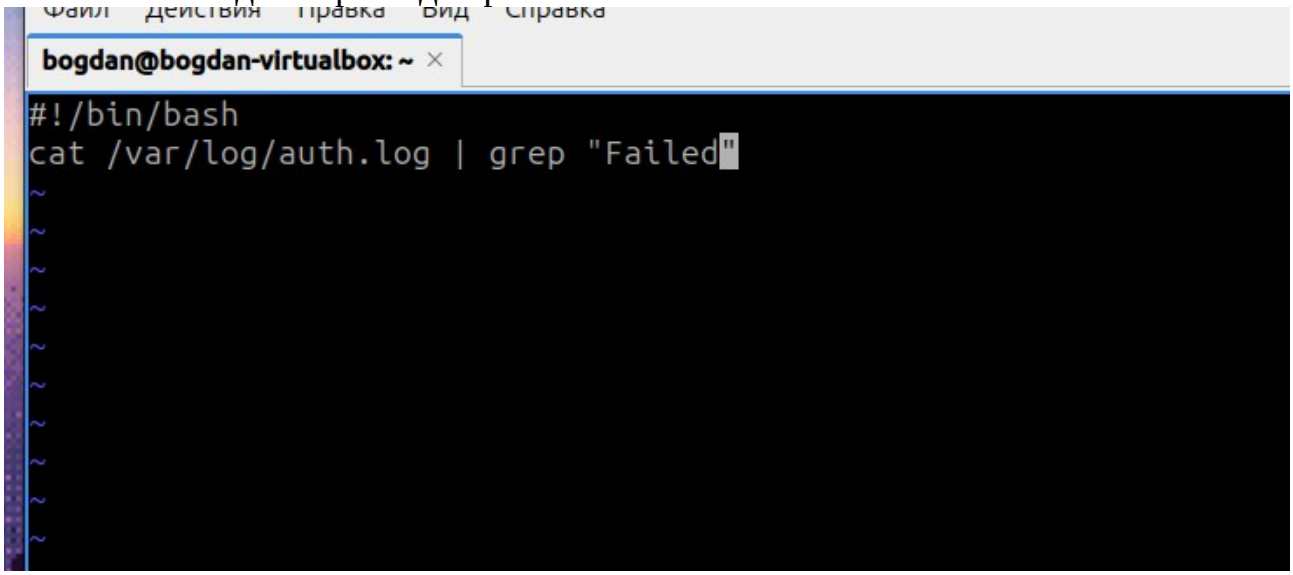


После этого указал заголовок секции отчета и название файла

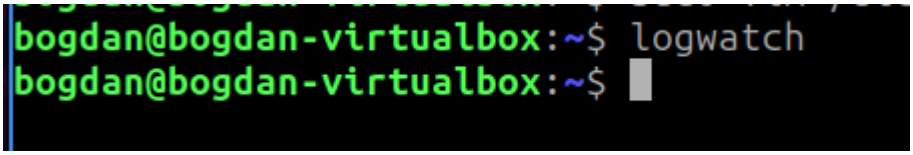


Список команд, которыми создавал и редактировал файлы

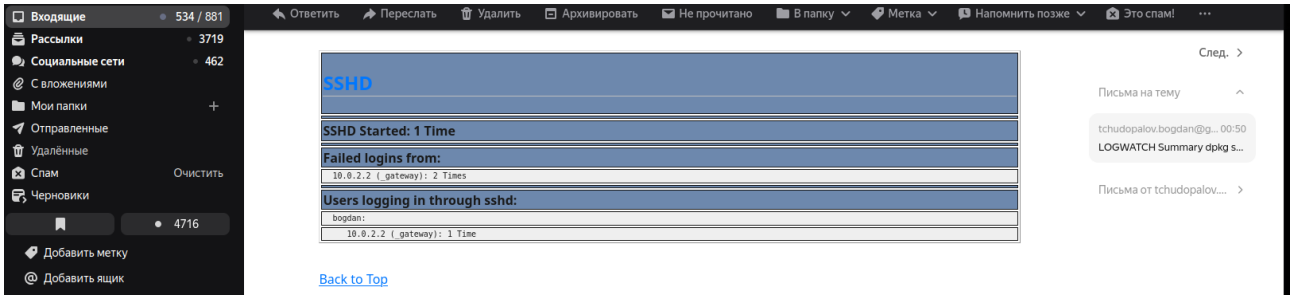
Также был создан скрипт для работы



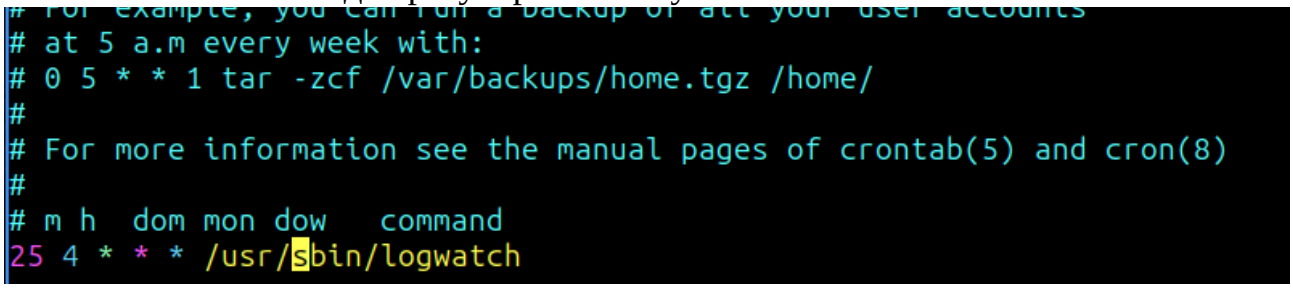
Вручную запустил logwatch



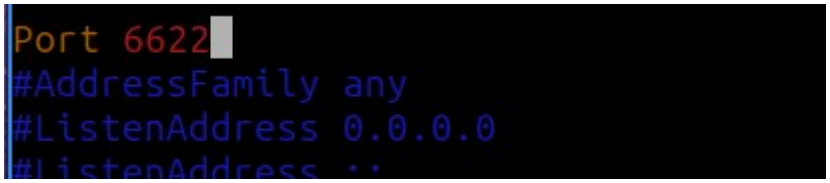
Результат:



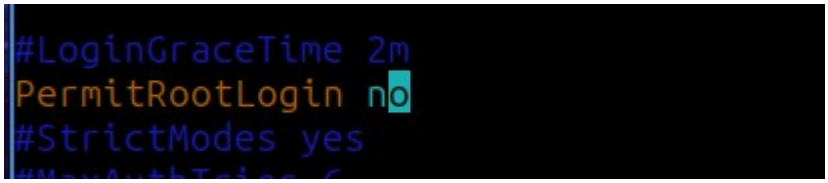
Воспользовался cron для регулярного получения писем



5. Настроить ограничения для работы программы ssh путем редактирования файла конфигурации. Запретить удаленный доступ к системе суперпользователю, изменить порт для подключения с 22 на иной (например 6622) — отредактировал следующие строки в конфиге, порт



Логин под root



Перезапустил ssh

```
bogdan@bogdan-virtualbox:~$ sudo systemctl restart ssh
bogdan@bogdan-virtualbox:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
     Active: active (running) since Sun 2025-05-11 01:16:10 MSK; 4s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 2320 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 2322 (sshd)
      Tasks: 1 (limit: 10740)
     Memory: 1.2M (peak: 12.0M)
        CPU: 42ms
     CGroup: /system.slice/ssh.service
             └─2322 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

трa 11 01:16:10 bogdan-virtualbox systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
трa 11 01:16:10 bogdan-virtualbox sshd[2322]: Server listening on :: port 22.
трa 11 01:16:10 bogdan-virtualbox systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
bogdan@bogdan-virtualbox:~$
```

Попытка подключения

```
→  ~ ssh bogdan@localhost -p 6622
bogdan@localhost's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-17-generic x8

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro
Last login: Sun May 11 01:19:07 2025 from 10.0.2.2
bogdan@bogdan-virtualbox:~$ exit
выход
Connection to localhost closed.
→  ~ ssh bogdan@localhost -p 2222
ssh: connect to host localhost port 2222: Connection refused
→  ~
```

Попытка входа под root

```
→  ~ ssh root@localhost -p 6622
root@localhost's password:
Permission denied, please try again.
root@localhost's password:
Permission denied, please try again.
root@localhost's password:
```

6. Настроить аутентификацию программы SSH по ключевой паре вместо паролей — внес следующее изменение в конфиг на виртуальной машине

```
PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none
```

Генерация пары ключей

```
➜  ~ ssh-keygen -t rsa -b 4096 -C "tchudopalov.bogdan@gmail.com"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/bogdan/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/bogdan/.ssh/id_rsa
Your public key has been saved in /home/bogdan/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:GDXA/Ipv2mT60yO56gbazqGY7EV5i0ix9nxKXgsWHYA tchudopalov.bogdan@gmail.com
The key's randomart image is:
+---[RSA 4096]----+
|  .. o..o        |
| E  . o. .       |
| .   ...         |
|  o o .o.        |
| + + +..S        |
|o * = o          |
| +.X =oo         |
|++*.*=B o        |
|=+o==*++ .       |
+----[SHA256]-----+
```

Копирование ключей на гостевую ОС

```
➜  ~ ssh-copy-id -i ~/.ssh/id_rsa.pub -p 6622 bogdan@localhost

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/bogdan/.ssh/ic
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted
all the new keys
bogdan@localhost's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -p 6622 'bogdan@localhost'"
and check to make sure that only the key(s) you wanted were added.

➜  ~
➜  ~
```

Попытка подключения

```
→  ~ ssh -v -p 6622 bogdan@localhost
OpenSSH_9.6p1 Ubuntu-3ubuntu13.11, OpenSSL 3.0.13 30 Jan 2024
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: include /etc/ssh/ssh_config.d/*.conf matched n
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to localhost [127.0.0.1] port 6622.
debug1: Connection established.
debug1: identity file /home/bogdan/.ssh/id_rsa type 0
debug1: identity file /home/bogdan/.ssh/id_rsa-cert type -1
debug1: identity file /home/bogdan/.ssh/id_ecdsa type -1
debug1: identity file /home/bogdan/.ssh/id_ecdsa-cert type -1
debug1: identity file /home/bogdan/.ssh/id_ecdsa_sk type -1
debug1: identity file /home/bogdan/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /home/bogdan/.ssh/id_ed25519 type -1
debug1: identity file /home/bogdan/.ssh/id_ed25519-cert type -1
debug1: identity file /home/bogdan/.ssh/id_ed25519_sk type -1
```

Результат

```
debug1: client_input_hostkeys: host key found matching a different name/address, sk
ostsFile update
debug1: Remote: /home/bogdan/.ssh/authorized_keys:1: key options: agent-forwarding
ty user-rc x11-forwarding
debug1: Remote: /home/bogdan/.ssh/authorized_keys:1: key options: agent-forwarding
ty user-rc x11-forwarding
debug1: Sending environment.
debug1: channel 0: setting env LANG = "ru_RU.UTF-8"
debug1: pledge: fork
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-17-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro
Last login: Sun May 11 01:37:25 2025 from 10.0.2.2
bogdan@bogdan-virtualbox:~$
```