Практическая работа. Настройка безопасности в ОС Linux

Разверните виртуальную машину на любом дистрибутиве, основанном на Debian.

Выполните настройку по чек-листу:

1. Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля.
2. Создать нового пользователя с домашней директорией и выдать ему возможность запускать следующие утилиты без требования пароля:
    - */sbin/route*, */sbin/iptables*, */usr/bin/nmap*, */usr/sbin/hping3*
    - *usr/bin/systemctl*
    - *sbin/ifup*, */sbin/ifdown*
3. Установить минимальную длину пароля для пользователя в 8 символов.
4. Установить на сервер пакеты Java.
5. Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.
6. Настроить файервол на блокирование всего входящего и выходящего трафика.

Условия реализации:

По каждому пункту нужно предоставить:

- Команду / набор команд / текст, которыми вы пользовались для выполнения задания.
- Скриншот результата работы / получившегося файла.

Дополнительная информация:

- По пункту 1 предоставьте всё содержимое конфигурационного файла sshd и содержимое файла authorized_keys.
- По пункту 2 предоставьте вывод команды ls в директории home, вывод файла passwd, содержимое файла sudoers.
- По пункту 3 самостоятельно найдите информацию по установке минимального пароля. В качестве ответа предоставьте содержимое файла common-passwords.
- По пункту 4 предоставьте результат успешной установки Java (последняя доступная версия JRE).
- По пункту 5 предоставьте тексты задач cron, содержимое файла crontab (скрипт Bash — пожеланию)
- По пункту 6 предоставьте вывод всех цепочек и правил iptables.

Выполнение задания

1. Настройка ssh и подключение по ключу

Вывод конфигурационного файла sshd

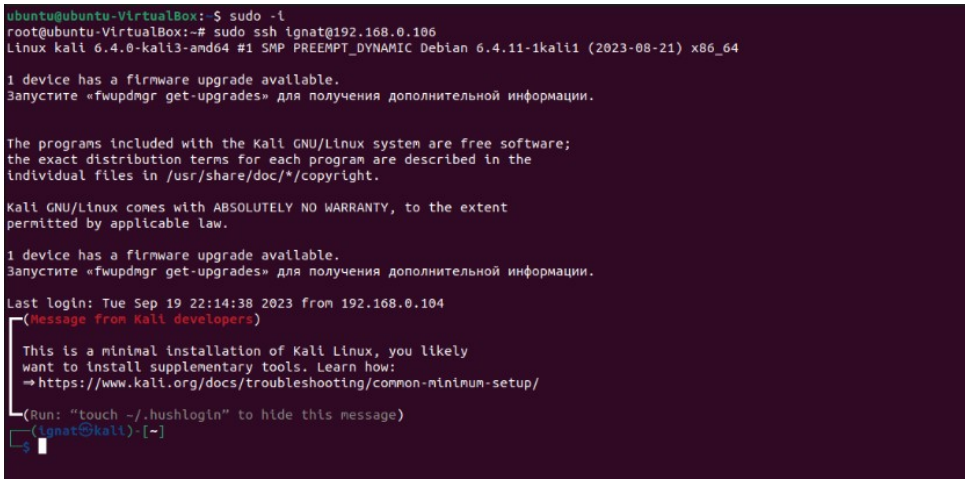
```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.
Include /etc/ssh/sshd_config.d/*.conf
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
# Ciphers and keying
#RekeyLimit default none
# Logging
#SyslogFacility AUTH
#LogLevel INFO
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
PubkeyAuthentication yes
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no
# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
```

```
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM yes
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none
# no default banner path
#Banner none
# Allow client to pass locale environment variables
AcceptEnv LANG LC_*
# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
```

Вывод файла authorized_keys

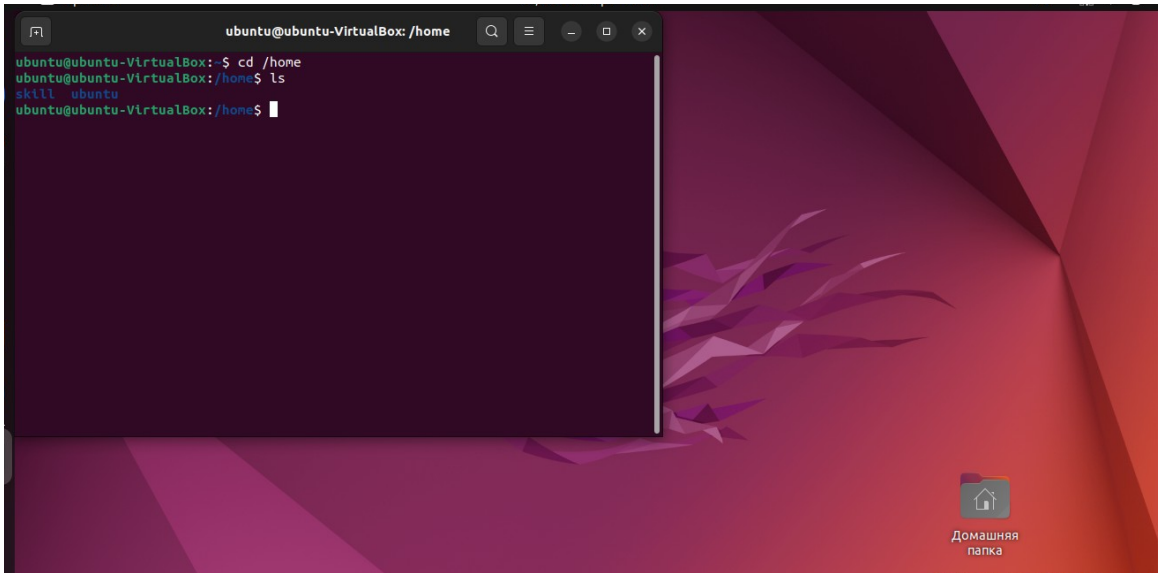
```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCnZaMdaA8CoqF9CtP50wJhFvBsNzpBBY/WtwJN53TOMm
G72UMJYysImVu+FcUTQWY4vbbHWrjEkvjRiJmRzkRPSRiL7PW3eQMZRTmNCEomiL2YL/
HCDPrV5cbMluCYse3UX/Uq6rmlxmLqvVsIQebu/
gq6GyIsf1Xl532Cv5nTJdhaZGR1B28fgLlSX5fQ1fDHfWzXVlCz3LXKYCsg35QfPP3w+IgfgEIJ1pgU+Zphg
XxTe3+5AYJMhycYC8pJb8Jp/C5POXl4TnEsFD/
diVnsH3geKoOpSaJBGQ09BrK7DItdMFxlAJNp6eoffJlpPRsV+ES46I5qU+ZUvcmZKGxv0HGp2Xrta6+vLt6
xJOHwpNUFswZ/e4EXZGEXOqz/
u4XVcDJHqostiXrz0uzkhdipPFYSYwwjg0zyMKrix2gIVSXZi3VB5Ejd3chyO3VR6L+woOfCEctmv5O7hAP
4zOdlgRPznxcFubrwoMAYeiOJhOh6yKEqBOCl2i/as4HgMmM= root@ubuntu-VirtualBox
```

Вывод результата подключения к машине через ssh по ключу

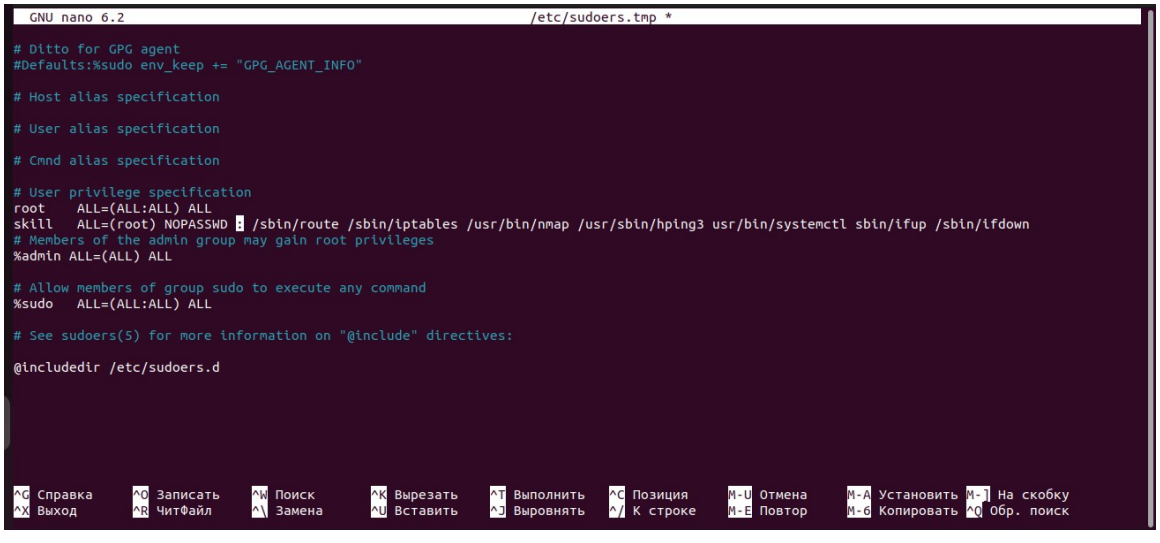


2. Создать нового пользователя с домашней директорией и выдать ему возможность запускать следующие утилиты без требования пароля.

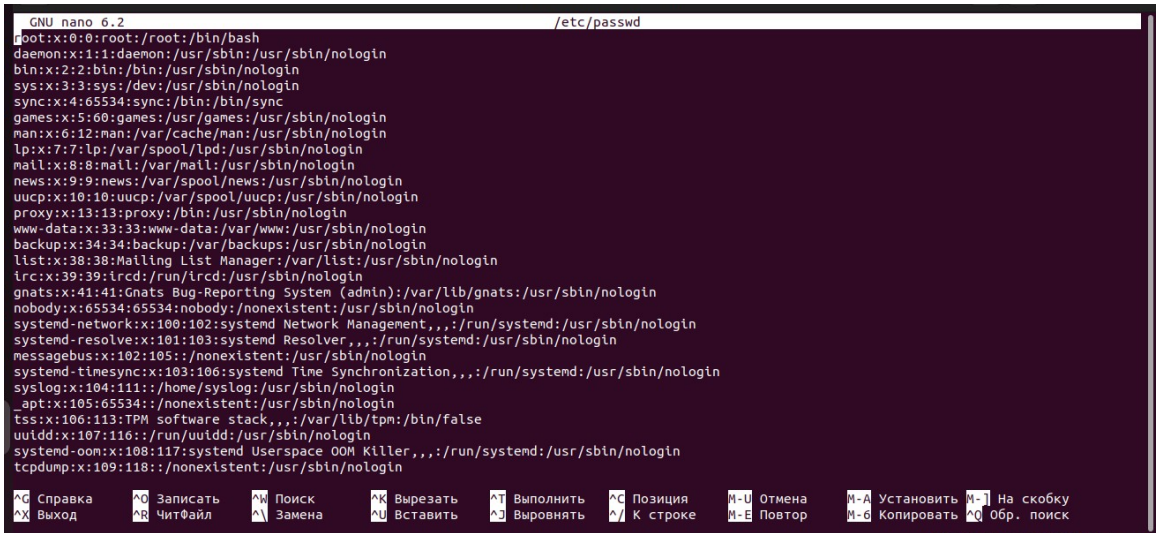
Вывод команды “ls”

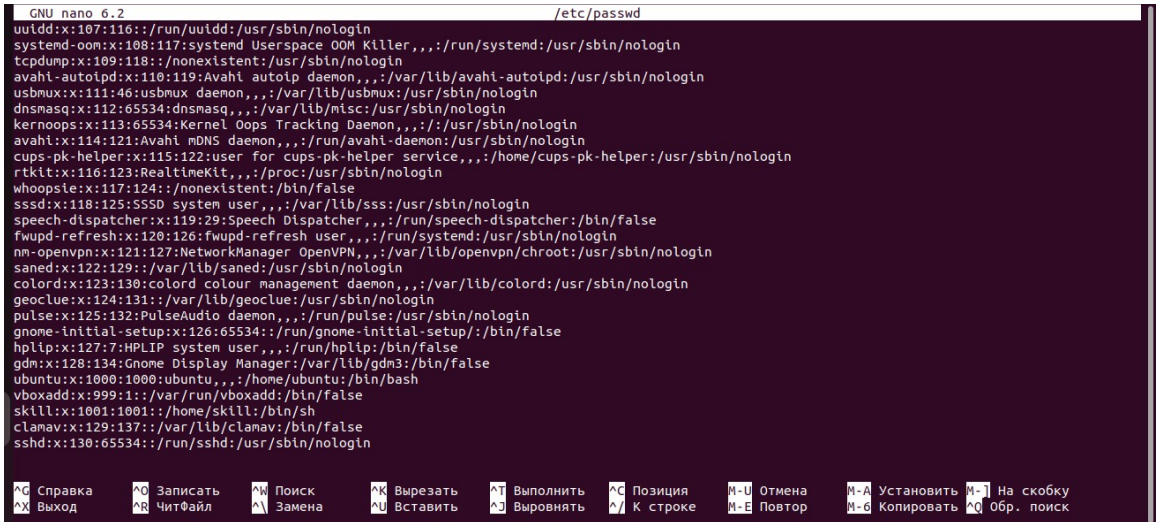


Содержимое файла “sudoers”



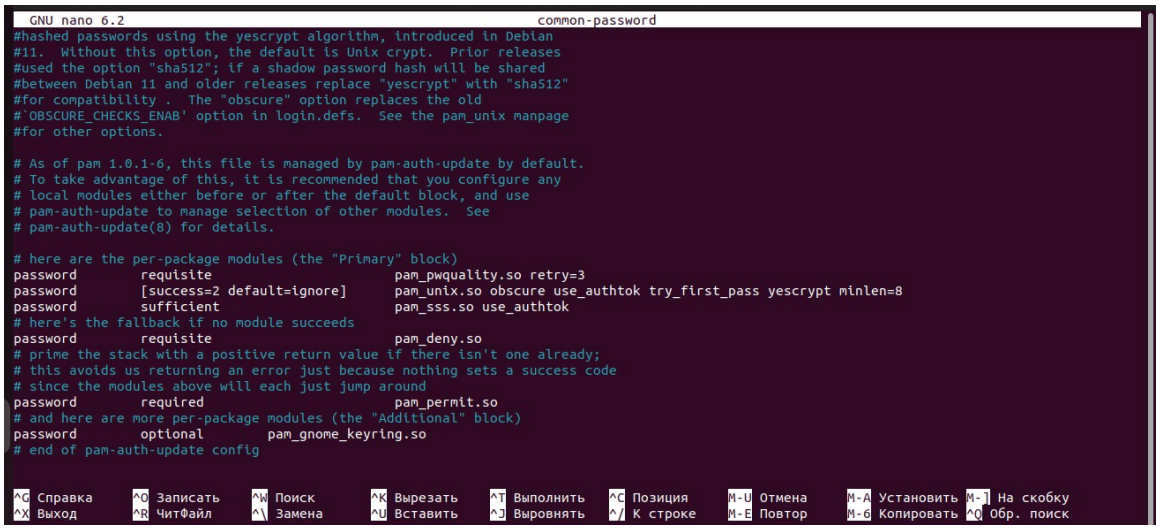
Содержимое файла “passwd”





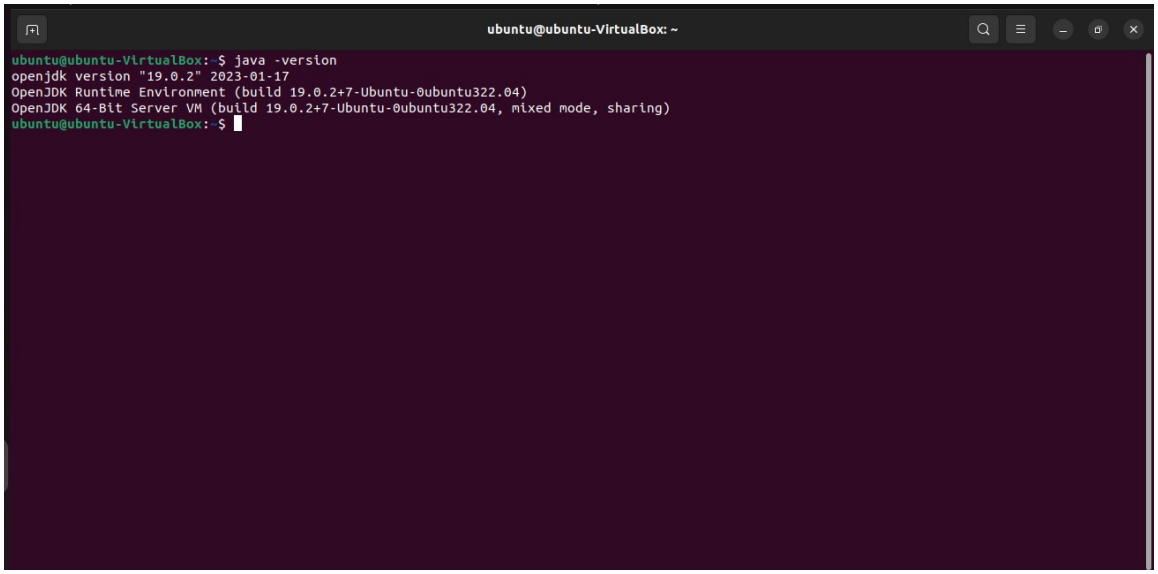
3. Настройка параметров для пароля. Установить минимальную длину пароля для пользователя в 8 символов.

Содержимое файла “pam.d/common-password”



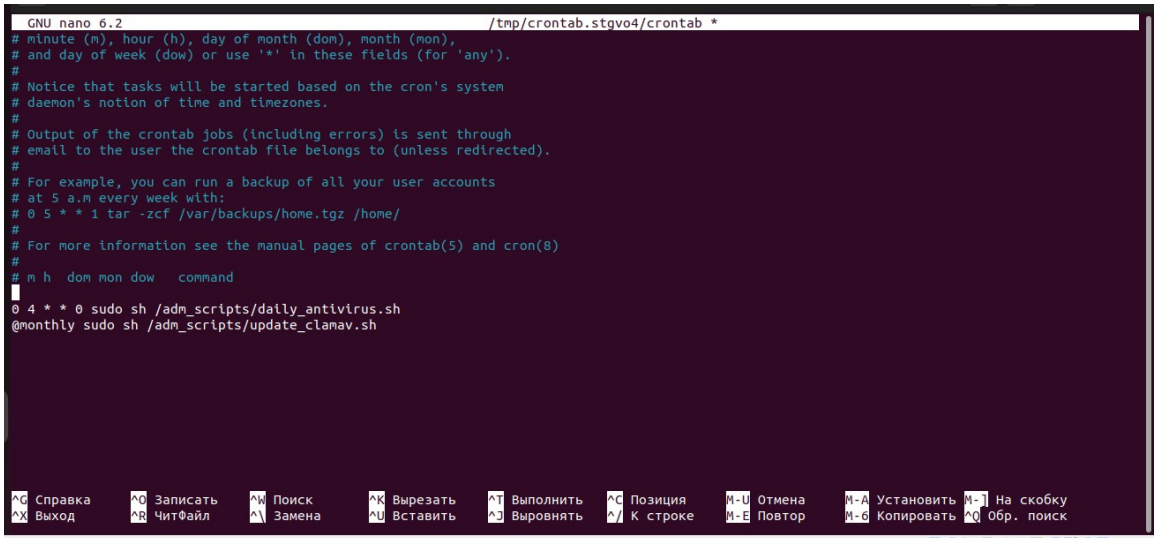
4.Установка JAVA

Версия “Java”

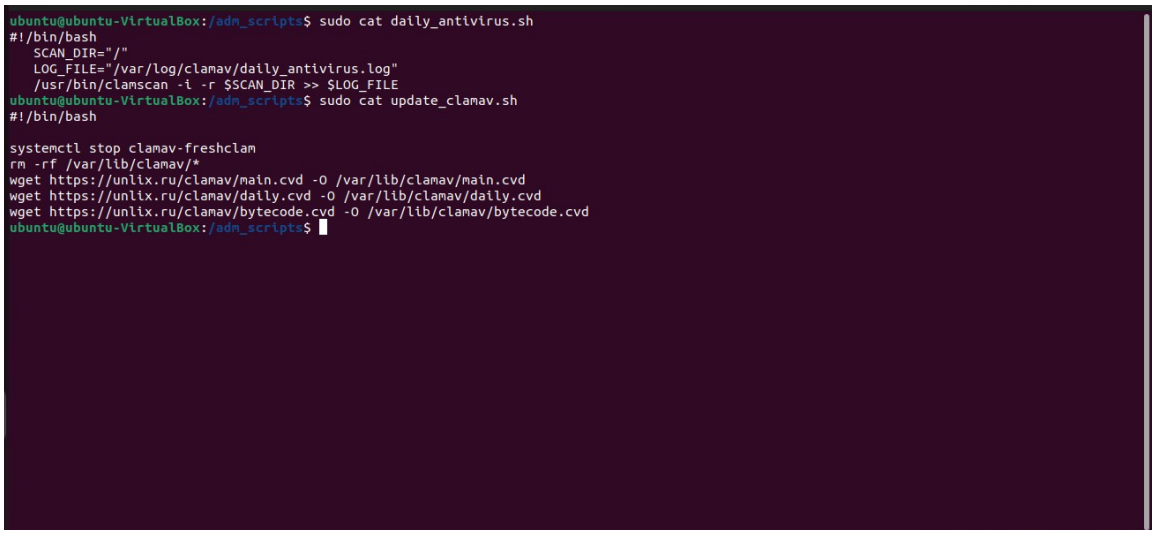


5. Автоматический запуск антивируса

Содержимое файла “crontab”



Скрипты на запуск антивируса и обновление



6. Настройка фаервола