

# 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 фаервол на блокирование всего входящего и исходящего 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
AAAAB3NzaC1yc2EAAAADAQABAAQBGQCnZaMdaA8CoqF9CtP50wJhFvBsNzpBBY/WtwJN53TOMm
G72UMJYysImVu+FcUTQWY4vbbHWrjEkvjRiJmRzkRPSRiL7PW3eQMZRTmNCEomiL2YL/
HCDPrV5cbMluCYse3UX/Uq6rmlxmLqvVsIQebu/
ggq6GyIsf1Xl532Cv5nTJdhaZGR1B28fgLISX5fQ1fDHfWzXVlCz3LXKYCsg35QfPP3w+IgfgEIJ1pgU+Zphg
XxTe3+5AYJMhycYC8pJb8Jp/C5POXl4TnEsFD/
diVnsH3geKoOpSaJBGQ09BrK7DltdMFxlAJNp6eoffJlpPRsV+ES46I5qU+ZUvcmZKGxv0HGp2Xrta6+vLt6
xJOHwpNUFswZ/e4EXZGEXOqz/
u4XVcDJHqostiXrz0uzkhdipPFYSYwwjg0zyMKrix2gIVSXZi3VB5Ejd3chyO3VR6L+woOfCEctmv5O7hAP
4zOdlgRPznxcFubrwoMAYeioJhOh6yKEqBOCl2i/as4HgMmM= root@ubuntu-VirtualBox

```

## Вывод результата подключения к машине через ssh по ключу

```
ubuntu@ubuntu-VirtualBox:~$ sudo -l
root@ubuntu-VirtualBox:~# sudo ssh ignat@192.168.0.106
Linux kali 6.4.0-kali3-and64 #1 SMP PREEMPT_DYNAMIC Debian 6.4.11-1kali1 (2023-08-21) x86_64

1 device has a firmware upgrade available.
Запустите «fwupdmgtr get-upgrades» для получения дополнительной информации.

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.

1 device has a firmware upgrade available.
Запустите «fwupdmgtr get-upgrades» для получения дополнительной информации.

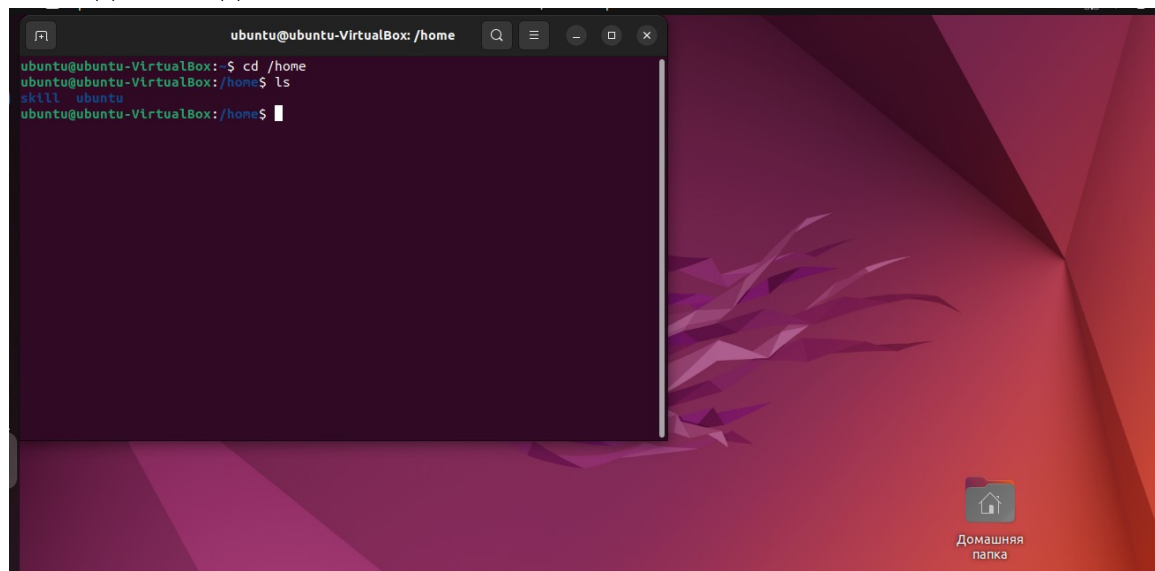
Last login: Tue Sep 19 22:14:38 2023 from 192.168.0.104
(Message from Kali developers)

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/

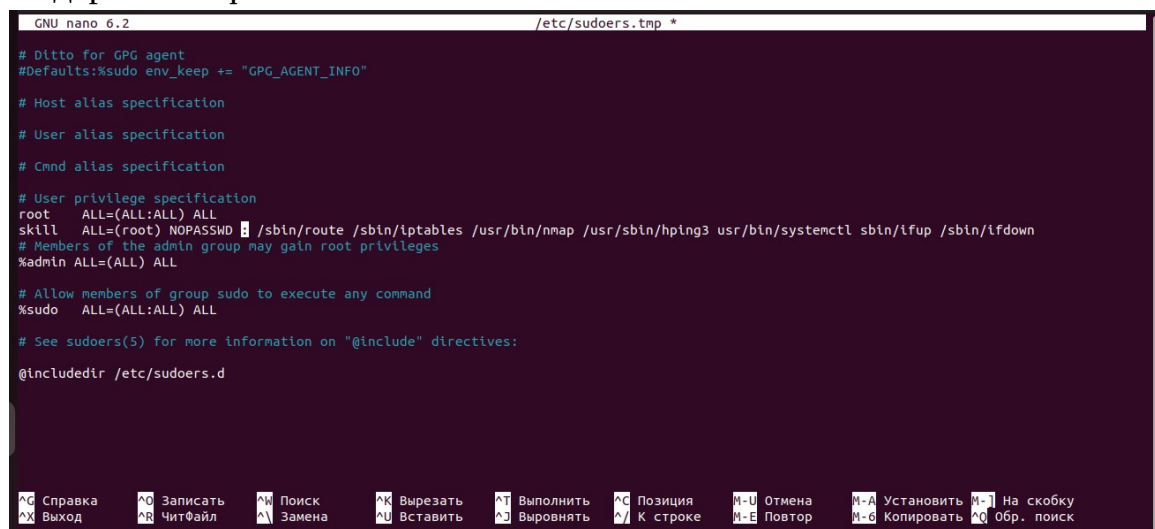
(Run: "touch ~/.hushlogin" to hide this message)
(ignat@kali) ~$
```

## 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”

GNU nano 6.2/etc/passwd

```
#root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailng List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105:/:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111:/:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin
tss:x:106:113:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:116:/:/run/uidd:/usr/sbin/nologin
systemd-oom:x:108:117:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:109:118:/:/nonexistent:/usr/sbin/nologin
```

СправкаЗаписатьПоискВырезатьВыполнитьПозицияОтменаУстановитьНа скобкуВыходЧитФайлЗаменаВставитьВыводитьК строкеПовторКопироватьОбр. поиск

GNU nano 6.2/etc/passwd

```
uidd:x:107:116:/:/run/uidd:/usr/sbin/nologin
systemd-oom:x:108:117:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:109:118:/:/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/mtsc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
rktl:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124:/:/nonexistent:/bin/false
sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
fwupd-refresh:x:120:126:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
nm-openvpn:x:121:127:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
saned:x:122:129:/:/var/lib/saned:/usr/sbin/nologin
colord:x:123:130:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:124:131:/:/var/lib/geoclue:/usr/sbin/nologin
pulse:x:125:132:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:126:65534:/:/run/gnome-initial-setup:/bin/false
hplip:x:127:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:128:134:Gnome Display Manager:/var/lib/gdm3:/bin/false
ubuntu:x:1000:1000:ubuntu,,,:/home/ubuntu:/bin/bash
vboxadd:x:999:1:/:/var/run/vboxadd:/bin/false
skill:x:1001:1001:/:/home/skill:/bin/sh
clamav:x:129:137:/:/var/lib/clamav:/bin/false
sshd:x:130:65534:/:/run/ssh:/usr/sbin/nologin
```

СправкаЗаписатьПоискВырезатьВыполнитьПозицияОтменаУстановитьНа скобкуВыходЧитФайлЗаменаВставитьВыводитьК строкеПовторКопироватьОбр. поиск

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

### Содержимое файла “/etc/pam.d/common-password”

GNU nano 6.2/etc/pam.d/common-password

```
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11. Without this option, the default is Unix crypt. Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility. The "obscure" option replaces the old
# OBSCURE_CHECKS_ENAB option in login.defs. See the pam_unix manpage
# for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password requisite pam_pwquality.so retry=3
password [success=2 default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt minlen=8
password sufficient pam_sss.so use_authtok
# here's the fallback if no module succeeds
password requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password required pam_permit.so
# and here are more per-package modules (the "Additional" block)
password optional pam_gnome_keyring.so
# end of pam-auth-update config
```

СправкаЗаписатьПоискВырезатьВыполнитьПозицияОтменаУстановитьНа скобкуВыходЧитФайлЗаменаВставитьВыводитьК строкеПовторКопироватьОбр. поиск



## 4. Установка JAVA

### Версия “Java”

```
ubuntu@ubuntu-VirtualBox: ~  
$ java -version  
openjdk version "19.0.2" 2023-01-17  
OpenJDK Runtime Environment (build 19.0.2+7-Ubuntu-0ubuntu322.04)  
OpenJDK 64-Bit Server VM (build 19.0.2+7-Ubuntu-0ubuntu322.04, mixed mode, sharing)  
ubuntu@ubuntu-VirtualBox: ~
```

## 5. Автоматический запуск антивируса

### Содержимое файла “crontab”

```
GNU nano 6.2 /tmp/crontab.stgv04/crontab *  
# minute (m), hour (h), day of month (dom), month (mon),  
# and day of week (dow) or use '*' in these fields (for 'any').  
#  
# Notice that tasks will be started based on the cron's system  
# daemon's notion of time and timezones.  
#  
# Output of the crontab jobs (including errors) is sent through  
# email to the user the crontab file belongs to (unless redirected).  
#  
# For example, you can run a backup of all your user accounts  
# at 5 a.m every week with:  
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/  
#  
# For more information see the manual pages of crontab(5) and cron(8)  
#  
# m h dom mon dow   command  
0 4 * * 0 sudo sh /adm_scripts/daily_antivirus.sh  
@monthly sudo sh /adm_scripts/update_clamav.sh
```

## Скрипты на запуск антивируса и обновление

```
ubuntu@ubuntu-VirtualBox:/adm_script$ sudo cat daily_antivirus.sh  
#!/bin/bash  
SCAN_DIR="/"  
LOG_FILE="/var/log/clamav/daily_antivirus.log"  
/usr/bin/clamscan -i -r $SCAN_DIR >> $LOG_FILE  
ubuntu@ubuntu-VirtualBox:/adm_script$ sudo cat update_clamav.sh  
#!/bin/bash  
  
systemctl stop clamav-freshclam  
rm -rf /var/lib/clamav/*  
wget https://unix.ru/clamav/main.cvd -O /var/lib/clamav/main.cvd  
wget https://unix.ru/clamav/daily.cvd -O /var/lib/clamav/daily.cvd  
wget https://unix.ru/clamav/bytecode.cvd -O /var/lib/clamav/bytecode.cvd  
ubuntu@ubuntu-VirtualBox:/adm_script$
```

## 6. Настройка фаервола

```
ubuntu@ubuntu-VirtualBox: /  
ubuntu@ubuntu-VirtualBox:~$ sudo iptables -P INPUT DROP  
ubuntu@ubuntu-VirtualBox:~$ sudo iptables -P OUTPUT DROP  
ubuntu@ubuntu-VirtualBox:~$ sudo iptables -L  
Chain INPUT (policy DROP)  
target    prot opt source                destination  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy DROP)  
target    prot opt source                destination  
ubuntu@ubuntu-VirtualBox:~$
```