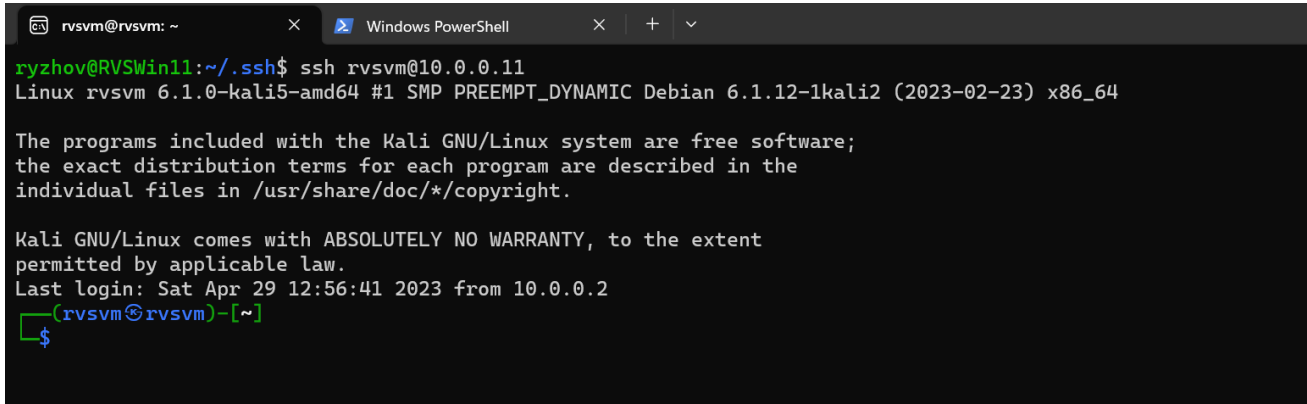


# Практическое задание: безопасность ОС Linux

**2/4 Практика с проверкой ментором**

Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля.



```
rvsvm@rvsvm: ~
Windows PowerShell
ryzhov@RCSWin11:~/ssh$ ssh rvsvm@10.0.0.11
Linux rvsvm 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23) 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: Sat Apr 29 12:56:41 2023 from 10.0.0.2
[rvsvm@rvsvm]~$
```

Установлено соединение по ssh с помощью ключа между хостом **Ryzhov@RCSWin11** ( приложение Linux Ubuntu (WSL) под Win11) и **rvsvm@rvsvm** (Kali Linux) – виртуальная машина

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

```
rvsvm@rvsvm: /home
ryzhov@RVSWin11:~/ssh$ ssh rvsvm@10.0.0.11
Linux rvsvm 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23) 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: Sat Apr 29 12:56:41 2023 from 10.0.0.2
(rvsvm@rvsvm)~$ sudo useradd -m rvs2vm
[sudo] пароль для rvsvm:
(rvsvm@rvsvm)~$ cd /
(rvsvm@rvsvm) [/]$ ls
bin  dev  home  initrd.img.old  lib32  libx32  media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib  lib64  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
(rvsvm@rvsvm) [/]$ cd /home
(rvsvm@rvsvm) [/home]$ ls
rvs2vm  rvsvm
(rvsvm@rvsvm) [/home]$
```

Создание нового пользователя:  
***sudo useradd -m rvs2***

У нового пользователя ***rvs2***  
сформирована своя домашняя  
директория

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

```
rvsvm@rvsvm: /home
$ sudo usermod -aG sudo rvs2vm

rvsvm@rvsvm: /home
$ sudo visudo -f /etc/sudoers.d/rvs2vm

rvsvm@rvsvm: /home
$
```

Предоставление прав на запуск утилит без пароля за счет добавления **rvs2vm** в группу «sudoers»:  
***sudo usermod -aG sudo rvs2***

```
GNU nano 7.2 /etc/sudoers.d/rvs2vm.tmp *
rvs2vm ALL=(ALL) NOPASSWD: /sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3
rvs2vm ALL=(ALL) NOPASSWD: /usr/bin/systemctl
rvs2vm ALL=(ALL) NOPASSWD: /sbin/ifup, /sbin/ifdown
```

Создание файла с именем **rvs2vm** в директории **/etc/sudoers.d/** с правами на запуск заданных утилит без пароля  
***sudo visudo -f /etc/sudoers.d/rvs2vm***

```
(rvsvm@rvsvm)~$ sudo su
(root@rvsvm)~$ # passwd rvs2vm
Новый пароль:
Повторите ввод нового пароля:
passwd: пароль успешно обновлён

(root@rvsvm)~$ #
```

Переход в режим root с правами суперпользователя ***sudo su*** для создания пароля для rvs2vm из 8 знаков  
***passwd rvs2vm***

***Прим: Пароль сам задал из 8 знаков ... Я не нашел варианта как задать командой пароль из требуемого числа знаков без установки доп. утилит. Буду рад Вашей мне подсказке!***

## Установить на сервер пакеты Java

```
(rvsvm@rvsvm)~[/home]
$ su rvs2vm
Пароль:
$
$ pwd
/home
$ ls
rvs2vm  rvsvm
$ sudo apt install java -y
[sudo] пароль для rvs2vm: |
```

Смена пользователя с **rvsvm** на **rvs2vm** и установка пакетов Java  
***sudo apt install java -y***

```
в автоматическом режиме
update-alternatives: используется /usr/lib/jvm/java-17-openjdk-amd64/bin/jhsdb для предоставления /usr/bin/jhsdb (jhsdb) в автоматическом режиме
Обрабатываются триггеры для ca-certificates-java (20230103) ...
done.
Настраивается пакет openjdk-17-jdk:amd64 (17.0.6+10-1) ...
update-alternatives: используется /usr/lib/jvm/java-17-openjdk-amd64/bin/jconsole для предоставления /usr/bin/jconsole (jconsole) в автоматическом режиме
Настраивается пакет default-jdk-headless (2:1.17-74) ...
Настраивается пакет default-jdk (2:1.17-74) ...
$ java --version
openjdk 17.0.6 2023-01-17
OpenJDK Runtime Environment (build 17.0.6+10-Debian-1)
OpenJDK 64-Bit Server VM (build 17.0.6+10-Debian-1, mixed mode, sharing)
$ |
```

Пакеты были установлены

Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.

Установка и обновление антивирусного пакета **Clamav** :  
***sudo apt install clamav clamav-daemon clamav-freshclam***

```
rvsvm@rvsvm: /home
$ sudo apt install clamav clamav-daemon clamav-freshclam
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Уже установлен пакет clamav самой новой версии (1.0.1+dfsg-2).
Уже установлен пакет clamav-freshclam самой новой версии (1.0.1+dfsg-2).
clamav-freshclam помечен как установленный вручную.
Будут установлены следующие дополнительные пакеты:
  clamdscan
Предлагаемые пакеты:
  libclamunrar clamav-docs daemon
Следующие НОВЫЕ пакеты будут установлены:
  clamav-daemon clamdscan
Обновлено 0 пакетов, установлено 2 новых пакетов, для удаления отмечено 0 пакетов, и 492 пакетов не обновлено.
Необходимо скачать 267 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 1 253 kB.
Хотите продолжить? [Д/н] у
0% [Обработка]
```

```
ERROR: Initialization error:
$ sudo systemctl start clamav-freshclam
$ clamscan /home/rvsvm/.ssh
Loading:   34s, ETA:   0s [=====>]      8.66M/8.66M sigs
Compiling: 4s, ETA:   0s [=====>]      41/41 tasks

/home/rvsvm/.ssh: Permission denied
WARNING: /home/rvsvm/.ssh: Can't access file

----- SCAN SUMMARY -----
Known viruses: 8664268
Engine version: 1.0.1
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 39.745 sec (0 m 39 s)
Start Date: 2023:04:29 13:53:06
End Date:   2023:04:29 13:53:46
$
```

сканирование директории: ***clamscan /home/rvsvm/.ssh***

Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.

```
rvsvm@rvsvm: /home
$ sudo apt install clamav clamav-daemon clamav-freshclam
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Уже установлен пакет clamav самой новой версии (1.0.1+dfsg-2).
Уже установлен пакет clamav-freshclam самой новой версии (1.0.1+dfsg-2).
clamav-freshclam помечен как установленный вручную.
Будут установлены следующие дополнительные пакеты:
  clamdscan
Предлагаемые пакеты:
  libclamunrar clamav-docs daemon
Следующие НОВЫЕ пакеты будут установлены:
  clamav-daemon clamdscan
Обновлено 0 пакетов, установлено 2 новых пакетов, для удаления отмечено 0 пакетов, и 492 пакетов не обновлено.
Необходимо скачать 267 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 1 253 kB.
Хотите продолжить? [Д/н] у
0% [Обработка]
```

```
ERROR: Initialization error:
$ sudo systemctl start clamav-freshclam
$ clamscan /home/rvsvm/.ssh
Loading: 34s, ETA: 0s [=====>] 8.66M/8.66M sigs
Compiling: 4s, ETA: 0s [=====>] 41/41 tasks

/home/rvsvm/.ssh: Permission denied
WARNING: /home/rvsvm/.ssh: Can't access file

----- SCAN SUMMARY -----
Known viruses: 8664268
Engine version: 1.0.1
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 39.745 sec (0 m 39 s)
Start Date: 2023:04:29 13:53:06
End Date: 2023:04:29 13:53:46
$
```

Установка и обновление антивирусного пакета **Clamav** :  
***sudo apt install clamav clamav-daemon clamav-freshclam***

***Прим: В процессе работы выявилась проблема – антивирус не обновлялся на виртуальной машине. Обновиться получилось только после того, как зашел с хост - компьютера на виртуальную машину через ssh***

сканирование директории: ***clamscan /home/rvsvm/.ssh***

Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.

```
rvs2vm@rvsvm: ~/STUD/stud_clam
GNU nano 7.2 /tmp/cron
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# 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 1 * * * /home/rvs2vm/STUD/stud_clam/update_clam.sh
0 4 * * 1 /home/rvs2vm/STUD/stud_clam/scan_clam.sh

#обновление в 01 час 1-го числа каждого месяца, сканирование 04 часа каждый понедельник
```

Были созданы два bash-скрипта:

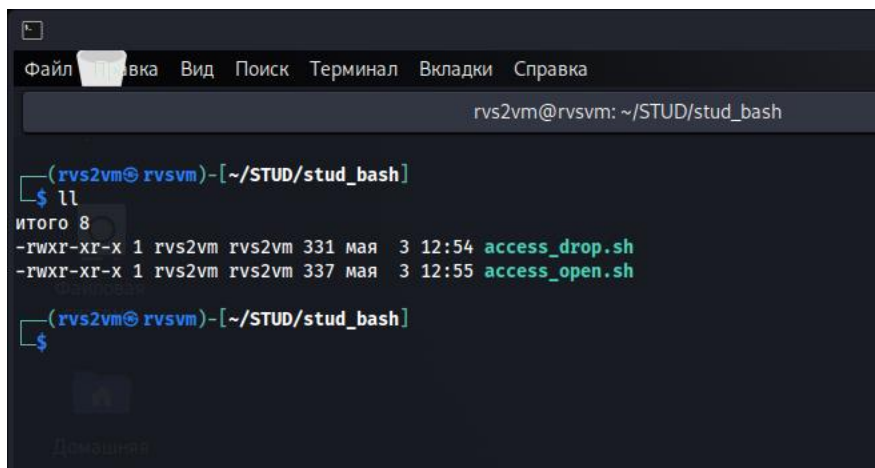
- ***update\_clam.sh*** (обновление антивируса)
- ***scan\_clam.sh*** (сканирование антивирусом)
- Все скрипты в целевой директории были сделаны исполняемыми: ***sudo ./chmod +x \*.sh***

Скрипты прилагаются в GitHub

Для создания периодических задач был отредактирован файл ***/etc/crontab*** командой: ***crontab -e***



Настроить фаервол на блокирование всего входящего и исходящего трафика.



```
rvs2vm@rvsvm: ~/STUD/stud_bash
(rvs2vm@ rvsvm)~[~/STUD/stud_bash]
$ ll
итого 8
-rwxr-xr-x 1 rvs2vm rvs2vm 331 мая  3 12:54 access_drop.sh
-rwxr-xr-x 1 rvs2vm rvs2vm 337 мая  3 12:55 access_open.sh
(rvs2vm@ rvsvm)~[~/STUD/stud_bash]
$
```

Были созданы два bash-скрипта:

- ***access\_drop.sh*** (блокирование всего трафика)
- ***access\_open.sh*** (восстановление всего трафика)
- Все скрипты в целевой директории были сделаны исполняемыми: ***sudo ./chmod +x \*.sh***

Скрипты прилагаются в GitHub

# Настроить фаервол на блокирование всего входящего и исходящего трафика.

```
(rvs2vm@ rvs2vm)~[/STUD/stud_bash]
$ ping 10.0.0.138
PING 10.0.0.138 (10.0.0.138) 56(84) bytes of data.
64 bytes from 10.0.0.138: icmp_seq=1 ttl=255 time=15.1 ms
64 bytes from 10.0.0.138: icmp_seq=2 ttl=255 time=6.82 ms
64 bytes from 10.0.0.138: icmp_seq=3 ttl=255 time=5.65 ms
64 bytes from 10.0.0.138: icmp_seq=4 ttl=255 time=6.27 ms
64 bytes from 10.0.0.138: icmp_seq=5 ttl=255 time=7.18 ms
^C
--- 10.0.0.138 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 5.649/8.194/15.055/3.469 ms

(rvs2vm@ rvs2vm)~[/STUD/stud_bash]
$ nano access_drop.sh

(rvs2vm@ rvs2vm)~[/STUD/stud_bash]
$ sudo ./access_drop.sh
[sudo] пароль для rvs2vm:

(rvs2vm@ rvs2vm)~[/STUD/stud_bash]
$ ping 10.0.0.138
PING 10.0.0.138 (10.0.0.138) 56(84) bytes of data.
^C
--- 10.0.0.138 ping statistics ---
25 packets transmitted, 0 received, 100% packet loss, time 24557ms

(rvs2vm@ rvs2vm)~[/STUD/stud_bash]
$
```

Доступ закрыт для исходящего трафика

```
ryzhov@RVSWin11:~$ ping 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data.
64 bytes from 10.0.0.11: icmp_seq=1 ttl=63 time=1.44 ms
64 bytes from 10.0.0.11: icmp_seq=2 ttl=63 time=0.932 ms
64 bytes from 10.0.0.11: icmp_seq=3 ttl=63 time=0.931 ms
64 bytes from 10.0.0.11: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from 10.0.0.11: icmp_seq=5 ttl=63 time=1.03 ms
64 bytes from 10.0.0.11: icmp_seq=6 ttl=63 time=0.957 ms

--- 10.0.0.11 ping statistics ---
^C6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 0.931/1.095/1.435/0.195 ms
ryzhov@RVSWin11:~$ ping 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data.

--- 10.0.0.11 ping statistics ---
^C8 packets transmitted, 0 received, 100% packet loss, time 7278ms

ryzhov@RVSWin11:~$
```

Доступ закрыт для входящего трафика

# Возврат открыт доступ к входящего и исходящего трафика к виртуальной машине

```
(rvs2vm@ rvs2vm) [~/STUD/stud_bash]
$ ping 10.0.0.138
PING 10.0.0.138 (10.0.0.138) 56(84) bytes of data.
^C
--- 10.0.0.138 ping statistics ---
25 packets transmitted, 0 received, 100% packet loss, time 24557ms
```

```
(rvs2vm@ rvs2vm) [~/STUD/stud_bash]
$ nano access_open.sh
```

```
(rvs2vm@ rvs2vm) [~/STUD/stud_bash]
$ sudo ./access_open.sh
```

```
(rvs2vm@ rvs2vm) [~/STUD/stud_bash]
$ ping 10.0.0.138
PING 10.0.0.138 (10.0.0.138) 56(84) bytes of data.
64 bytes from 10.0.0.138: icmp_seq=1 ttl=255 time=6.40 ms
64 bytes from 10.0.0.138: icmp_seq=2 ttl=255 time=6.75 ms
64 bytes from 10.0.0.138: icmp_seq=3 ttl=255 time=6.57 ms
64 bytes from 10.0.0.138: icmp_seq=4 ttl=255 time=6.40 ms
64 bytes from 10.0.0.138: icmp_seq=5 ttl=255 time=5.96 ms
64 bytes from 10.0.0.138: icmp_seq=6 ttl=255 time=7.40 ms
^C
--- 10.0.0.138 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 5.961/6.579/7.403/0.438 ms
```

```
(rvs2vm@ rvs2vm) [~/STUD/stud_bash]
$
```

Доступ открыт для исходящего трафика

```
--- 10.0.0.11 ping statistics ---
^C6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 0.931/1.095/1.435/0.195 ms
ryzhov@RVSWin11:~$ ping 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data.

--- 10.0.0.11 ping statistics ---
^C8 packets transmitted, 0 received, 100% packet loss, time 7278ms

ryzhov@RVSWin11:~$ ping 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data.
64 bytes from 10.0.0.11: icmp_seq=1 ttl=63 time=1.37 ms
64 bytes from 10.0.0.11: icmp_seq=2 ttl=63 time=1.05 ms
64 bytes from 10.0.0.11: icmp_seq=3 ttl=63 time=1.38 ms
64 bytes from 10.0.0.11: icmp_seq=4 ttl=63 time=1.27 ms
64 bytes from 10.0.0.11: icmp_seq=5 ttl=63 time=1.40 ms
64 bytes from 10.0.0.11: icmp_seq=6 ttl=63 time=1.23 ms
^C
--- 10.0.0.11 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 1.052/1.281/1.399/0.119 ms
ryzhov@RVSWin11:~$
```

Доступ открыт для входящего трафика