

Настройка ClamAV (PC-R*)

1) Устанавливаем ClamAV с помощью apt (необходимо включить NAT):

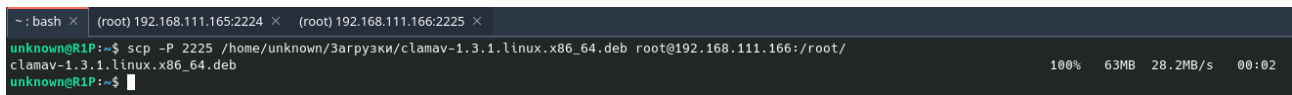
```
# apt install -y clamav
```

2) Скачиваем ClamAV с офф.сайта (или же с моего Google Disk):

https://drive.google.com/file/d/1MzMRP1B80-sCmfT9vx71Q_zefK03oCwf/view?usp=drive_link

3) Клонировем пакет clamav-1.3.1.linux.x86_64.deb с локальной машины на VM:

```
# scp -P 2225 /ноть/к/clamav-1.3.1.linux.x86_64.deb root@192.168.111.166:/root/
```

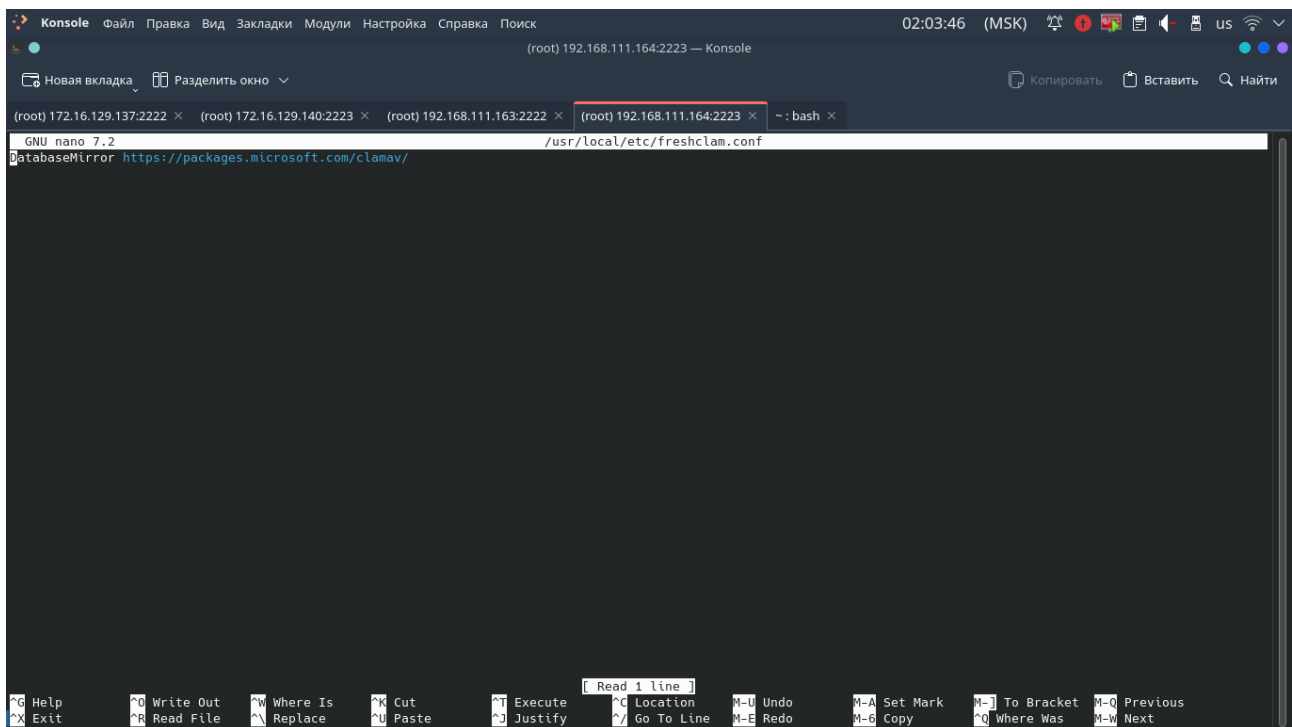
A terminal window showing the execution of the scp command. The command is: scp -P 2225 /home/unknown/Загрузки/clamav-1.3.1.linux.x86_64.deb root@192.168.111.166:/root/. The output shows the file being transferred at 100% speed, 63MB, 28.2MB/s, and it took 00:02. The prompt is unknown@RIP:~\$.

```
unknown@RIP:~$ scp -P 2225 /home/unknown/Загрузки/clamav-1.3.1.linux.x86_64.deb root@192.168.111.166:/root/
clamav-1.3.1.linux.x86_64.deb
unknown@RIP:~$
```

4) Удаляем все файлы в директории clamav: **rm /var/lib/clamav/***

Добавляем в файлы "/etc/freshclam.conf" и "/usr/local/etc/freshclam.conf" следующее:

DatabaseMirror <https://packages.microsoft.com/clamav/>

A terminal window showing the nano editor editing the file /usr/local/etc/freshclam.conf. The editor is GNU nano 7.2. The content of the file is DatabaseMirror https://packages.microsoft.com/clamav/. The terminal window has a dark background and a light-colored text area. The top bar shows the time 02:03:46 (MSK) and various system icons. The bottom bar shows various keyboard shortcuts like Help, Exit, Write Out, Read File, etc.

```
GNU nano 7.2 /usr/local/etc/freshclam.conf
DatabaseMirror https://packages.microsoft.com/clamav/
```

Примечание:

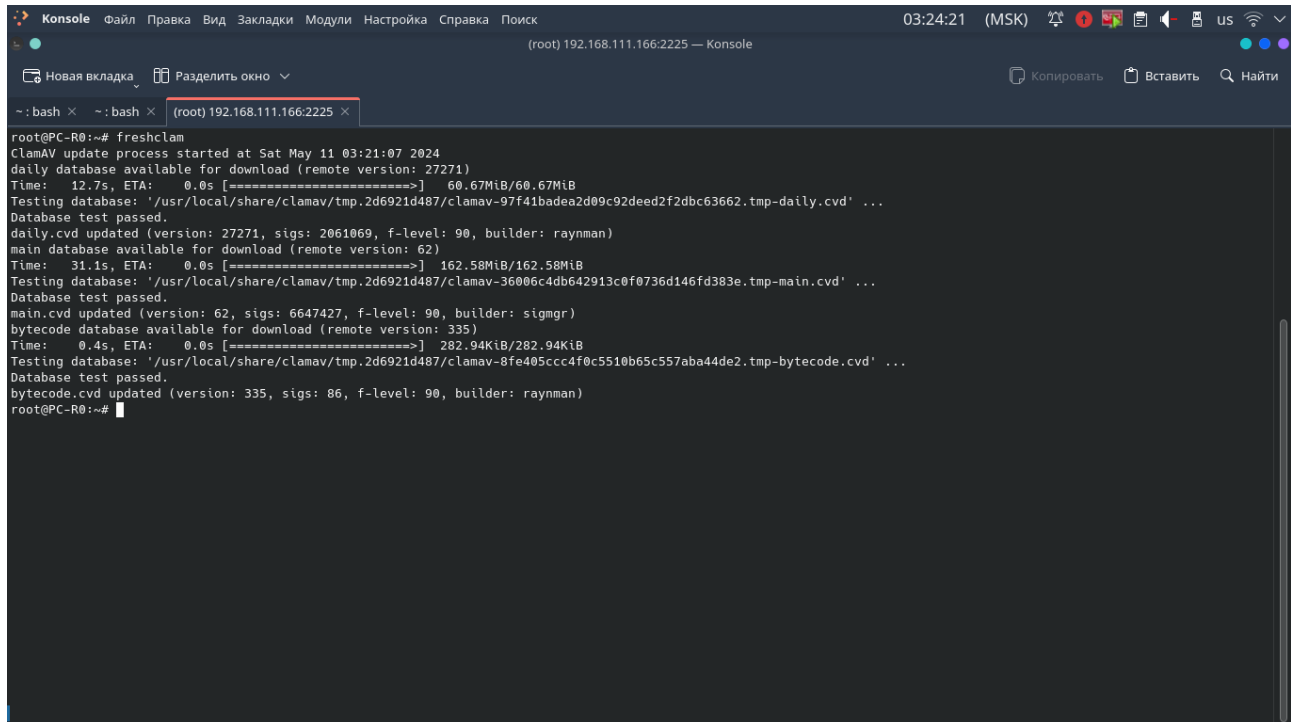
Все эти манипуляции производятся из-за санкций компании CISCO.

5) Устанавливаем ClamAV с помощью скопированного пакета с локальной системы:

```
# chmod +x clamav-1.3.1.linux.x86_64.deb && dpkg -i clamav-1.3.1.linux.x86_64.deb
```

6) Перезагружаем систему: **reboot**

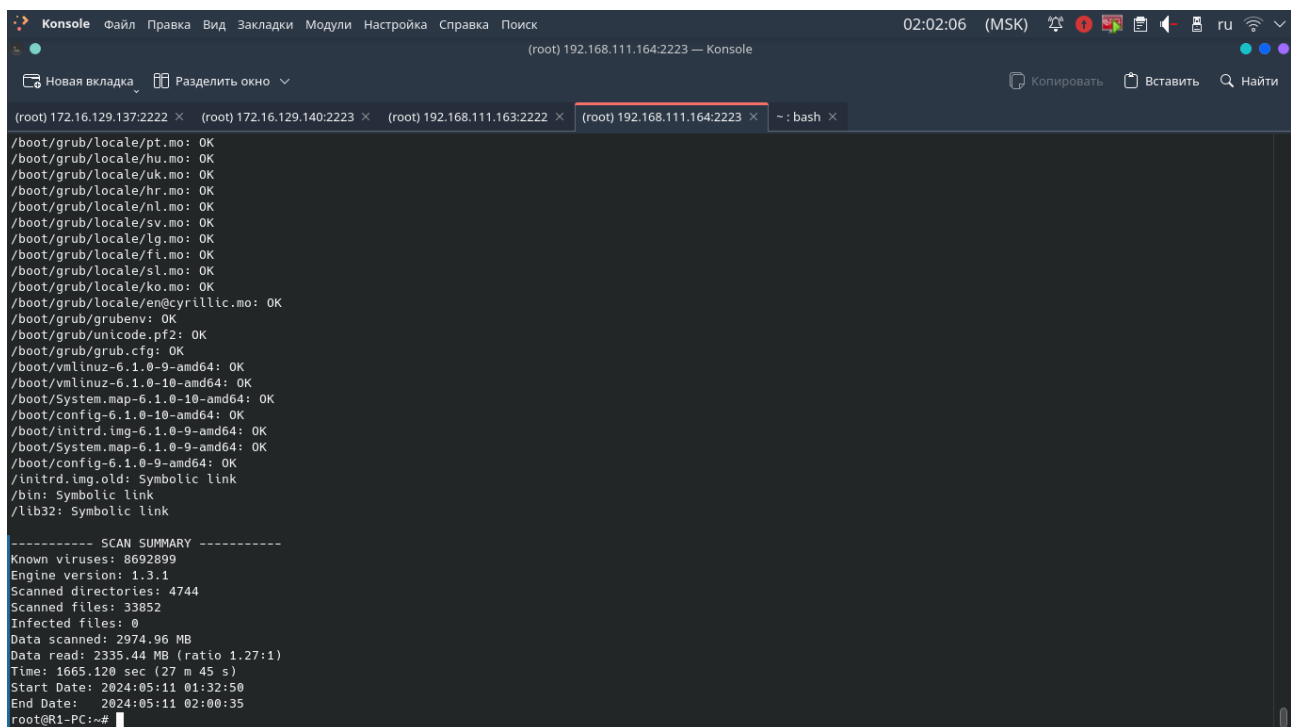
7) Скачиваем необходимые БД для сканирования: **freshclam**



```
root@PC-R0:~# freshclam
ClamAV update process started at Sat May 11 03:21:07 2024
daily database available for download (remote version: 27271)
Time: 12.7s, ETA: 0.0s [=====] 60.67MiB/60.67MiB
Testing database: '/usr/local/share/clamav/tmp.2d6921d487/clamav-97f41badea2d09c92deed2f2dbc63662.tmp-daily.cvd' ...
Database test passed.
daily.cvd updated (version: 27271, sigs: 2061069, f-level: 90, builder: raynman)
main database available for download (remote version: 62)
Time: 31.1s, ETA: 0.0s [=====] 162.58MiB/162.58MiB
Testing database: '/usr/local/share/clamav/tmp.2d6921d487/clamav-36006c4db642913c0f0736d146fd383e.tmp-main.cvd' ...
Database test passed.
main.cvd updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
bytecode database available for download (remote version: 335)
Time: 0.4s, ETA: 0.0s [=====] 282.94KiB/282.94KiB
Testing database: '/usr/local/share/clamav/tmp.2d6921d487/clamav-8fe405ccc4f0c5510b65c557aba44de2.tmp-bytecode.cvd' ...
Database test passed.
bytecode.cvd updated (version: 335, sigs: 86, f-level: 90, builder: raynman)
root@PC-R0:~#
```

8) Проводим тестовое сканирование на выявление вирусов: **clamscan -r / --exclude-dir=/proc**

```
--exclude-dir=/sys --exclude-dir=/dev -l /var/log/clamav/scan.log
```



```
(root) 172.16.129.137:2222 x (root) 172.16.129.140:2223 x (root) 192.168.111.163:2222 x (root) 192.168.111.164:2223 x ~: bash x
/boot/grub/locale/pt.mo: OK
/boot/grub/locale/hu.mo: OK
/boot/grub/locale/uk.mo: OK
/boot/grub/locale/hr.mo: OK
/boot/grub/locale/nl.mo: OK
/boot/grub/locale/sv.mo: OK
/boot/grub/locale/lg.mo: OK
/boot/grub/locale/fi.mo: OK
/boot/grub/locale/sl.mo: OK
/boot/grub/locale/ko.mo: OK
/boot/grub/locale/en@cyrillic.mo: OK
/boot/grub/grubenv: OK
/boot/grub/unicode.pf2: OK
/boot/grub/grub.cfg: OK
/boot/vmlinuz-6.1.0-9-amd64: OK
/boot/vmlinuz-6.1.0-10-amd64: OK
/boot/System.map-6.1.0-10-amd64: OK
/boot/config-6.1.0-10-amd64: OK
/boot/initrd.img-6.1.0-9-amd64: OK
/boot/System.map-6.1.0-9-amd64: OK
/boot/config-6.1.0-9-amd64: OK
/initrd.img.old: Symbolic link
/bin: Symbolic link
/lib32: Symbolic link

----- SCAN SUMMARY -----
Known viruses: 8692899
Engine version: 1.3.1
Scanned directories: 4744
Scanned files: 33852
Infected files: 0
Data scanned: 2974.96 MB
Data read: 2335.44 MB (ratio 1.27:1)
Time: 1665.120 sec (27 m 45 s)
Start Date: 2024:05:11 01:32:50
End Date: 2024:05:11 02:00:35
root@R1-PC:~#
```