

## Настройка политики безопасности Linux

### 1 Настройка общей памяти

По умолчанию весь объем общей памяти /run/shm доступен для чтения и записи с возможностью выполнения программ. Это считается брешью в безопасности и многие эксплойты используют /run/shm для атак на запущенные сервисы. Для большинства настольных, а особенно серверных устройств рекомендуется монтировать этот файл в режиме только для чтения.

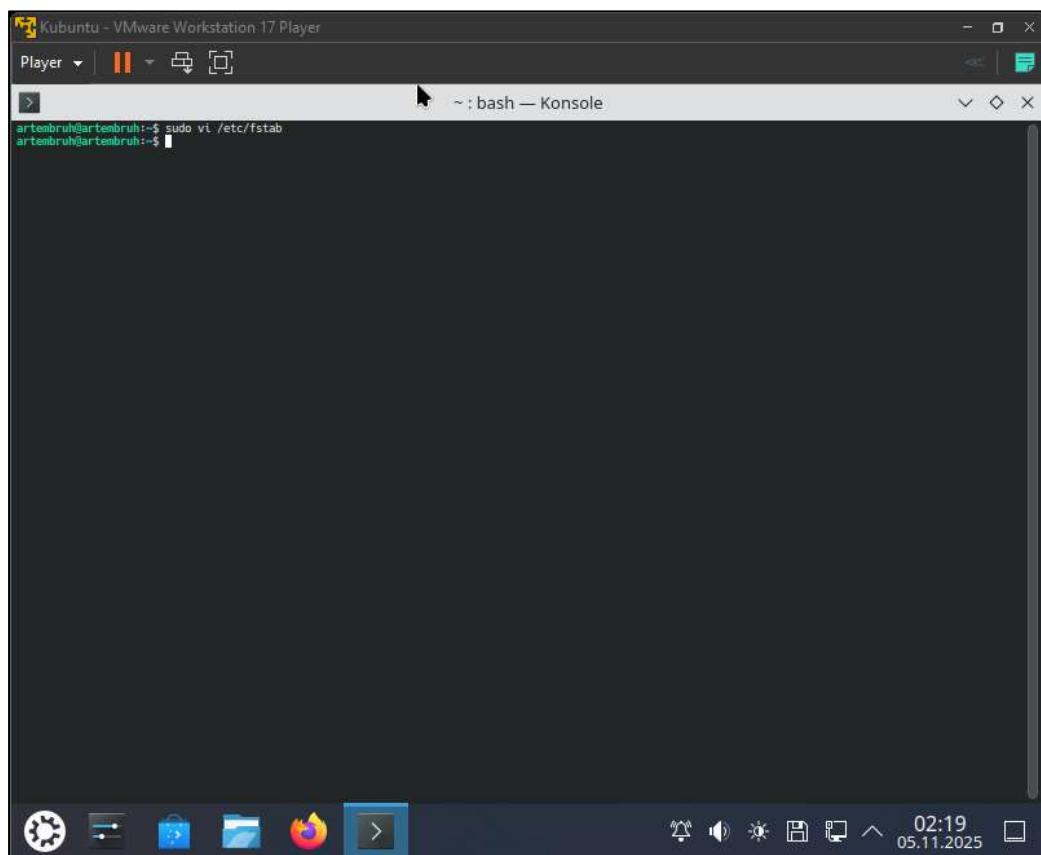
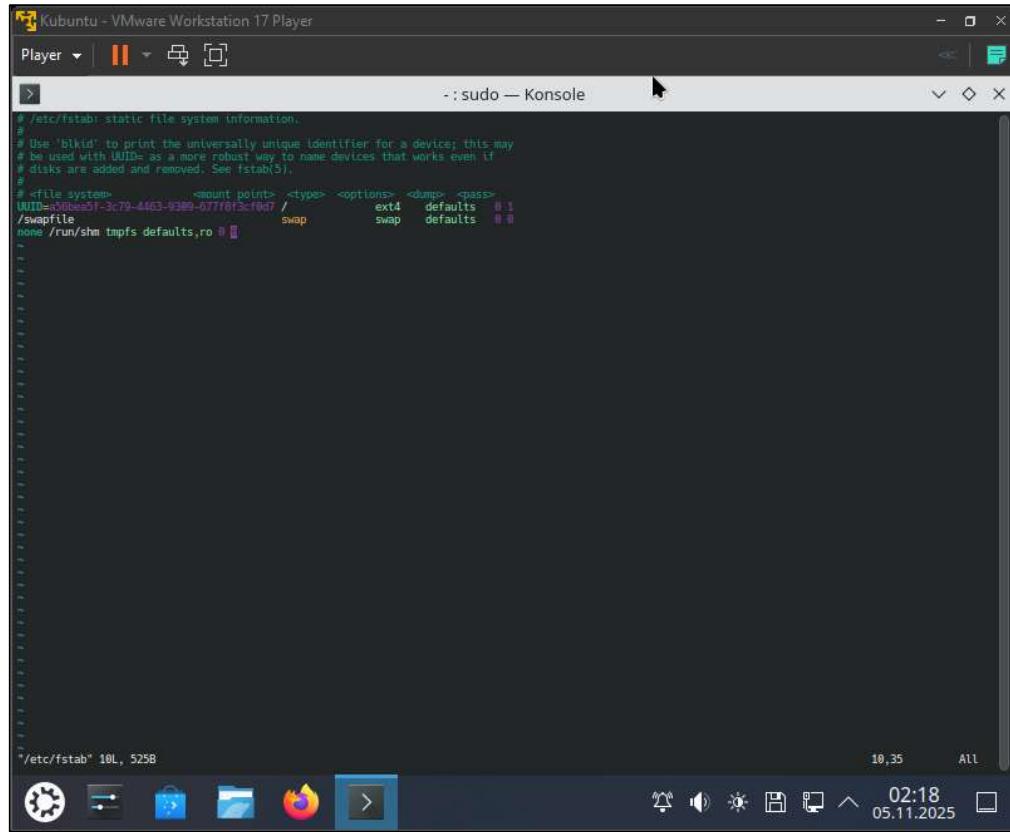


Рисунок 1 – Открываем папку fstab через терминал



The screenshot shows a terminal window titled "Kubuntu - VMware Workstation 17 Player". The window title bar includes icons for minimize, maximize, and close, along with a "Player" dropdown menu and a "Konsole" tab indicator. The terminal itself displays the contents of the "/etc/fstab" file, which contains static file system information. The file includes comments about blkid and UUID, and lists entries for the root file system (ext4), swap space, and tmpfs. The bottom status bar shows the file path as "/etc/fstab" and its size as 10L, 525B. The system tray at the bottom right shows the date and time as 05.11.2025 02:18.

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a device; this may
# be used with UUID= as a more robust way to name devices that works even if
# disks are added and removed. See fstab(5).
#
#       <mount point>   <type>  <options> <dump> <pass>
UUID=c0be51-3c79-4463-9389-077f8f3cf0d7 /          ext4    defaults  0 1
/swapfile           swap      swap    defaults  0 0
none   /run/shm   tmpfs   defaults,ro 0 0
```

Рисунок 2 – Папка fstab через терминал

## 2 Настройка Брандмауэра

По умолчанию UFW в Ubuntu может быть отключен. Чтобы включить его, выполните следующие команды в терминале. Включаем брандмауэр Uncomplicated Firewall, и проверяем статус. Разрешаем доступ через порт 80 с протоколом tcp. Запрещаем доступ через порт 22.

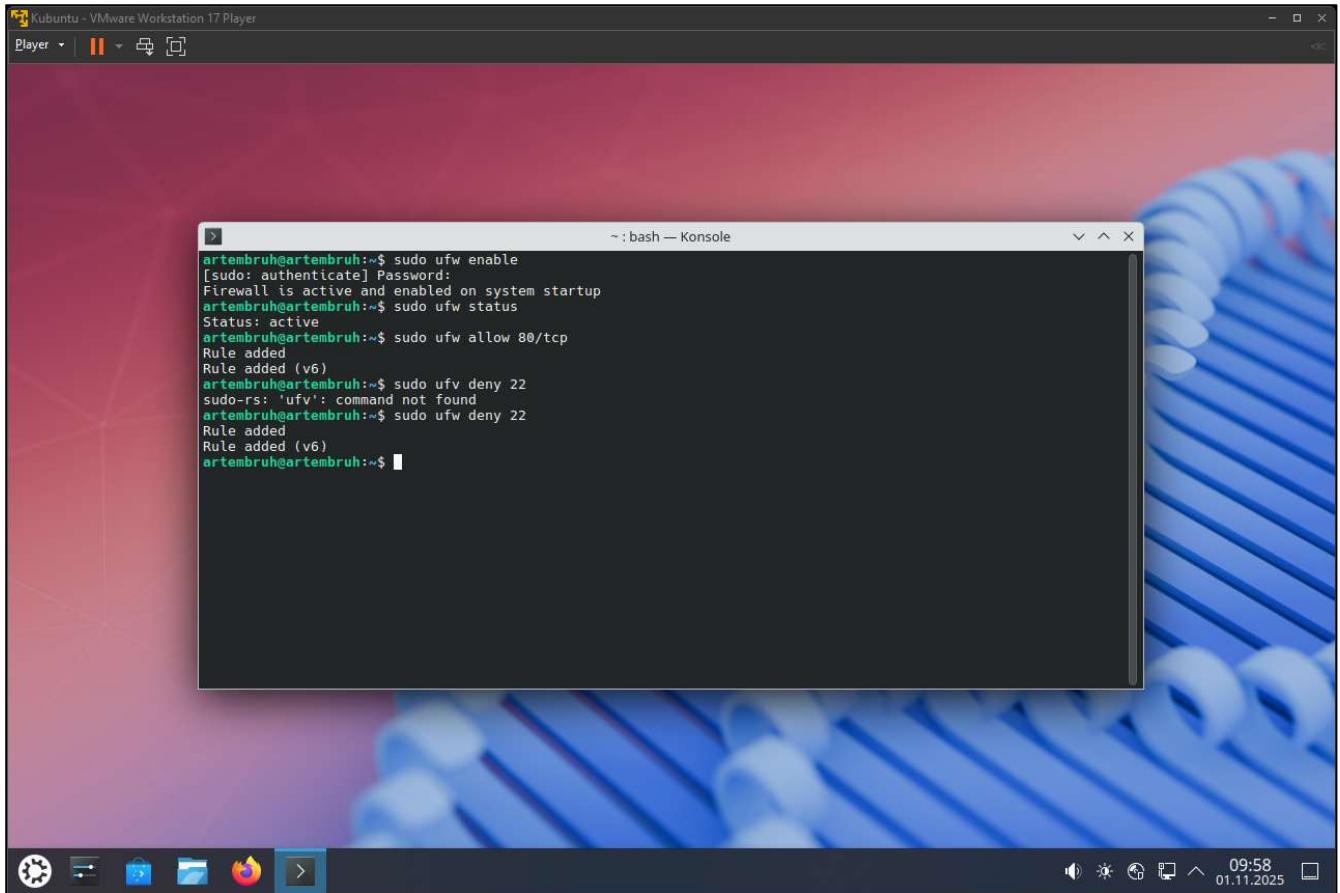


Рисунок 3 – Включаем Брандмауэр

### 3 Настройка доступа к общему каталогу

Ваш домашний каталог по умолчанию будет доступен каждому пользователю в системе. Так что если у вас есть гостевая учетная запись, то гость сможет получить полный доступ ко всем вашим личным файлам и документам. Но вы можете сделать его доступным только вам.

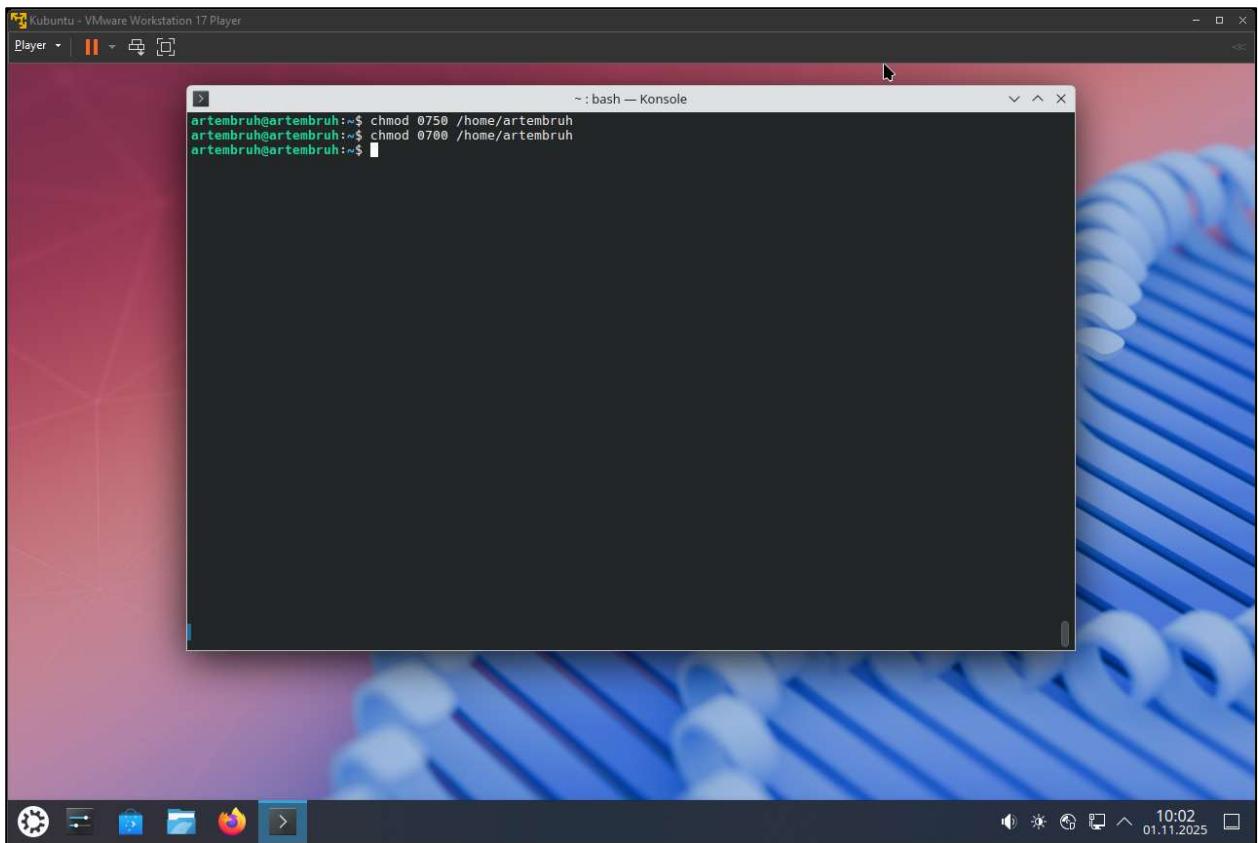


Рисунок 4 – Ограничеваем доступ к домашнему каталогу

#### 4 Проверка на наличие руткитов и вредоносного ПО

Устанавливаем rkhunter для проверки на наличие руткитов и вредоносного ПО.

```
artembruh@artembruh:~$ sudo apt install rkhunter
Installing:
rkhunter

Installing dependencies:
binutils           libbinutils    libblockfile1 postfix      ruby-net-telnet   ruby-xmlrpc
binutils-common    libctf-nobfd0 liblinsl2   rake          ruby-ruby2-keywords   ruby3.3
binutils-x86-64-linux-gnu libctf0       libruby     ruby          ruby-rubygems   rubygems-integration
bsd-mailx          libbgprofng0 libruby0.3.3  ruby-csv     ruby-sdbm      unhide
fonts-lato         libblockfile-bin net-tools   ruby-did-you-mean   ruby-webrick   unhide.rb

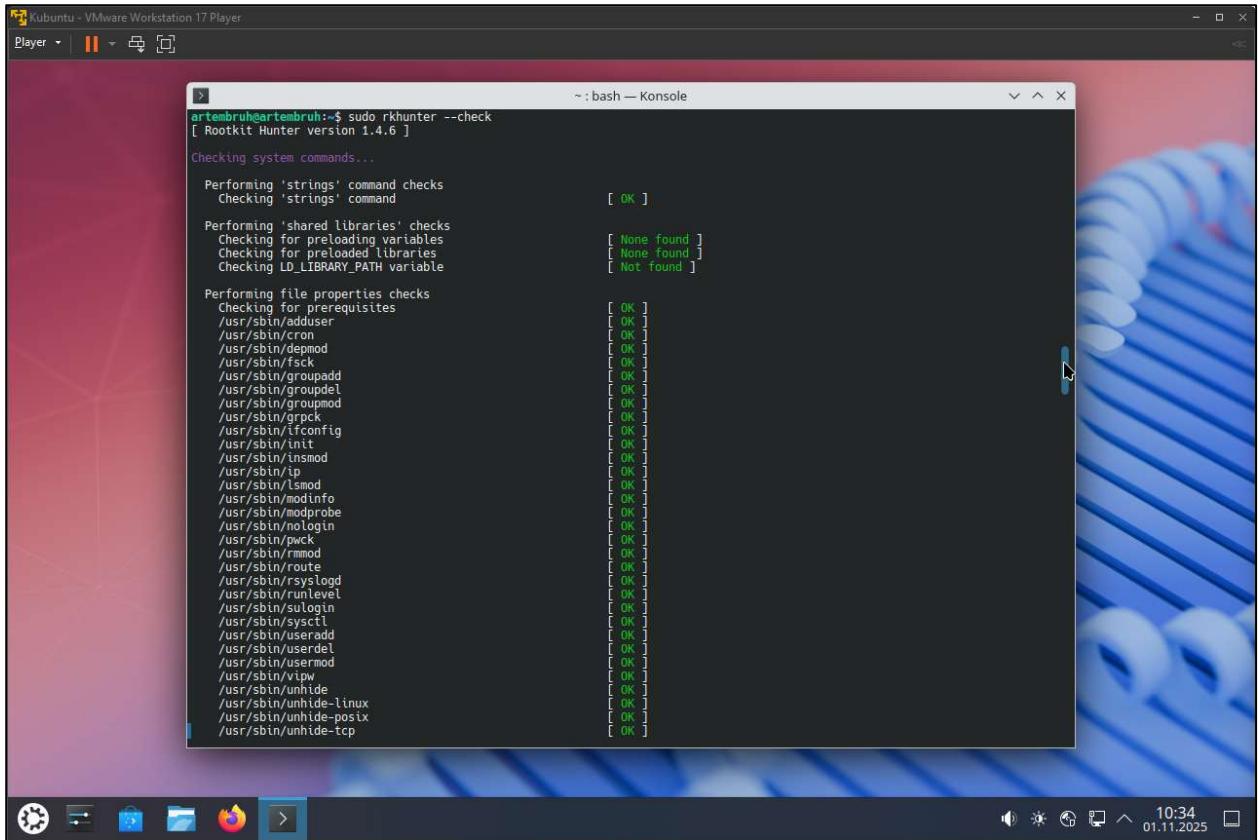
Suggested packages:
binutils-doc        postfix-cdb   postfix-lmdb  postfix-mysql  postfix-sqlite | dovecot-common bundler
gorofng-gui        postfix-doc   postfix-mta-sts-resolver  postfix-pcre  procmail   ri
binutils-gold       postfix-ldap  postfix-mongodb  postfix-pgsql  sasl2-bin   ruby-dev

Summary:
Upgrading: 0, Installing: 31, Removing: 0, Not Upgrading: 0
Download size: 14,6 MB
Space needed: 67,1 MB / 39,3 GB available

Continue? [Y/n]
Get:1 http://archive.ubuntu.com/ubuntu questing/main amd64 fonts-lato all 2.015-1 [2 781 kB]
Get:2 http://archive.ubuntu.com/ubuntu questing/main amd64 liblinsl2 amd64 1.3.0-3build3 [41,4 kB]
Get:3 http://archive.ubuntu.com/ubuntu questing/main amd64 postfix amd64 3.10.2-2ubuntu2 [1 300 kB]
Get:4 http://archive.ubuntu.com/ubuntu questing/main amd64 binutils-common amd64 2.45-7ubuntu1 [22 kB]
Get:5 http://archive.ubuntu.com/ubuntu questing/main amd64 libbinutils amd64 2.45-7ubuntu1 [602 kB]
Get:6 http://archive.ubuntu.com/ubuntu questing/main amd64 libbgprofng0 amd64 2.45-7ubuntu1 [991 kB]
Get:7 http://archive.ubuntu.com/ubuntu questing/main amd64 libctf-nobfd0 amd64 2.45-7ubuntu1 [102 kB]
Get:8 http://archive.ubuntu.com/ubuntu questing/main amd64 libctf0 amd64 2.45-7ubuntu1 [99,8 kB]
Get:9 http://archive.ubuntu.com/ubuntu questing/main amd64 binutils-x86-64-linux-gnu amd64 2.45-7ubuntu1 [1 140 kB]
Get:10 http://archive.ubuntu.com/ubuntu questing/main amd64 binutils amd64 2.45-7ubuntu1 [208 kB]
Get:11 http://archive.ubuntu.com/ubuntu questing/main amd64 net-tools amd64 2.10-1.3ubuntu2 [208 kB]
Get:12 http://archive.ubuntu.com/ubuntu questing/universe amd64 rkhunter all 1.4.6-13 [219 kB]
Get:13 http://archive.ubuntu.com/ubuntu questing/main amd64 libblockfile-bin amd64 1.17-2build1 [11,5 kB]
Get:14 http://archive.ubuntu.com/ubuntu questing/main amd64 libblockfile1 amd64 1.17-2build1 [7 200 B]
Get:15 http://archive.ubuntu.com/ubuntu questing/main amd64 bsd-mailx amd64 8.1.2-0.20220412vcs-1.1 [65,8 kB]
Get:16 http://archive.ubuntu.com/ubuntu questing/main amd64 rubygems-integration all 1.19 [5 550 B]
Get:17 http://archive.ubuntu.com/ubuntu questing/main amd64 ruby3.3 amd64 3.3.8-2ubuntu2 [59,0 kB]
Get:18 http://archive.ubuntu.com/ubuntu questing/main amd64 ruby-rubygems all 3.6.7-7ubuntu1 [332 kB]
Get:19 http://archive.ubuntu.com/ubuntu questing/main amd64 ruby amd64 1:3.3 [3 666 B]
Get:20 http://archive.ubuntu.com/ubuntu questing/main amd64 rake all 13.2.1-1 [45,8 kB]
Get:21 http://archive.ubuntu.com/ubuntu questing/main amd64 ruby-csv all 3.3.4-1 [43,0 kB]
Get:22 http://archive.ubuntu.com/ubuntu questing/main amd64 ruby-did-you-mean all 1.6.3-2 [14,8 kB]
Get:23 http://archive.ubuntu.com/ubuntu questing/main amd64 ruby-net-telnet all 0.2.0-1 [13,3 kB]
Get:24 http://archive.ubuntu.com/ubuntu questing/main amd64 ruby-ruby2-keywords all 0.0.5-1 [4 280 B]
```

Рисунок 5 – Установка rkhunter

После установки выполните обновление баз данных и сканирование



Ubuntu - VMware Workstation 17 Player

Player | || | ☰

~ : bash — Konsole

```
artembruh@artembruh:~$ sudo rkhunter --check
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...
Performing 'strings' command checks
  Checking 'strings' command [ OK ]
Performing 'shared libraries' checks
  Checking for preloading variables [ None found ]
  Checking for preloaded libraries [ None found ]
  Checking LD_LIBRARY_PATH variable [ Not found ]
Performing file properties checks
  Checking for prerequisites
    /usr/sbin/adduser [ OK ]
    /usr/sbin/cron [ OK ]
    /usr/sbin/demod [ OK ]
    /usr/sbin/fsck [ OK ]
    /usr/sbin/groupadd [ OK ]
    /usr/sbin/groupdel [ OK ]
    /usr/sbin/groupmod [ OK ]
    /usr/sbin/plock [ OK ]
    /usr/sbin/tcconfig [ OK ]
    /usr/sbin/init [ OK ]
    /usr/sbin/insmod [ OK ]
    /usr/sbin/ip [ OK ]
    /usr/sbin/lsmod [ OK ]
    /usr/sbin/modinfo [ OK ]
    /usr/sbin/modprobe [ OK ]
    /usr/sbin/nologin [ OK ]
    /usr/sbin/pwck [ OK ]
    /usr/sbin/rmod [ OK ]
    /usr/sbin/route [ OK ]
    /usr/sbin/rsyslogd [ OK ]
    /usr/sbin/runlevel [ OK ]
    /usr/sbin/sulogin [ OK ]
    /usr/sbin/sysctl [ OK ]
    /usr/sbin/useradd [ OK ]
    /usr/sbin/userdel [ OK ]
    /usr/sbin/usermod [ OK ]
    /usr/sbin/vipw [ OK ]
    /usr/sbin/unhide [ OK ]
    /usr/sbin/unhide-linux [ OK ]
    /usr/sbin/unhide-posix [ OK ]
    /usr/sbin/unhide-tcp [ OK ]
```

10:34 01.11.2025

Рисунок 5 – Обновление баз данных и сканирование

The screenshot shows a Kubuntu desktop environment within a VMware Player window. A terminal window titled 'bash — Konsole' displays the output of a system scan. The output includes various checks such as malware detection, account and configuration file reviews, and filesystem integrity checks. A summary at the end indicates no rootkits were found, though one suspect file was identified. The desktop interface includes a dock with icons for Dash, Home, Applications, and the Dash search bar, along with a system tray showing the date and time.

```
Checking system startup files for malware [ None found ]
Performing group and account checks
  Checking for passwd file [ Found ]
  Checking for root equivalent (UID 0) accounts [ None found ]
  Checking for passwordless accounts [ None found ]
  Checking for passwd file changes [ None found ]
  Checking for group file changes [ None found ]
  Checking root account shell history files [ None found ]

Performing system configuration file checks
  Checking for an SSH configuration file [ Not found ]
  Checking for a running system logging daemon [ Found ]
  Checking for a system logging configuration file [ Found ]
  Checking if syslog remote logging is allowed [ Not allowed ]

Performing filesystem checks
  Checking /dev for suspicious file types [ None found ]
  Checking for hidden files and directories [ Warning ]

[Press <ENTER> to continue]

System checks summary
=====
File properties checks...
  Files checked: 190
  Suspect files: 1

Rootkit checks...
  Rootkits checked : 478
  Possible rootkits: 0

Applications checks...
  All checks skipped

The system checks took: 4 minutes and 0 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

artembru@artembru:~$
```

Рисунок 6 – Результат сканирования

## Вывод

Безопасность Kubuntu — это комплексный процесс, который требует регулярного внимания и действий. Настройка UFW позволяет эффективно защитить систему от несанкционированного сетевого доступа. Ограничение доступа к домашней папке позволит защитить файлы от посторонних пользователей.