Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Практика построения центров мониторинга и управления инцидентами ИБ

Отчет по лабораторной работе №1

Snort

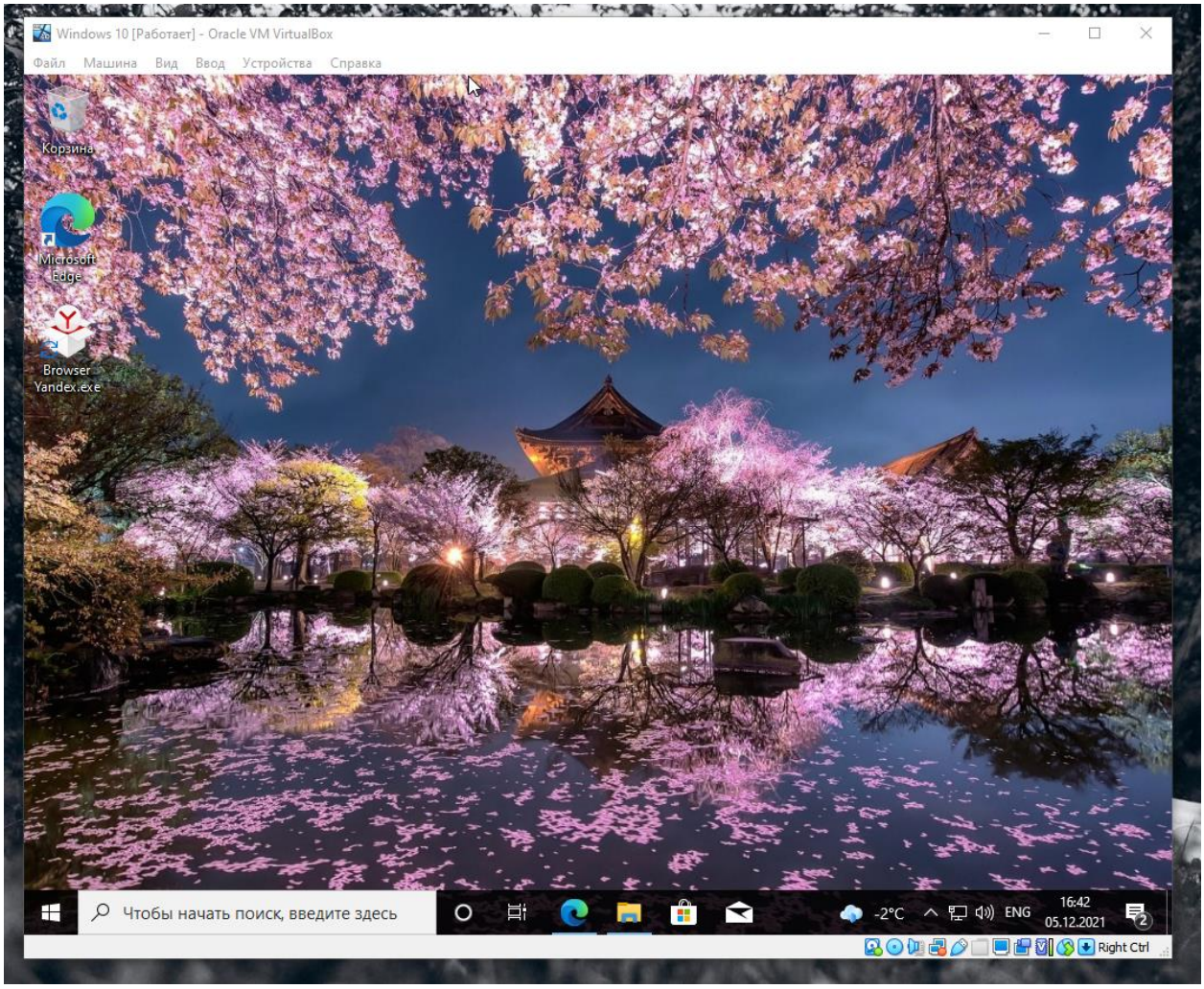
Выполнила студентка 5 курса группы 171-341

Решетникова Дарья

Москва 2021 г.

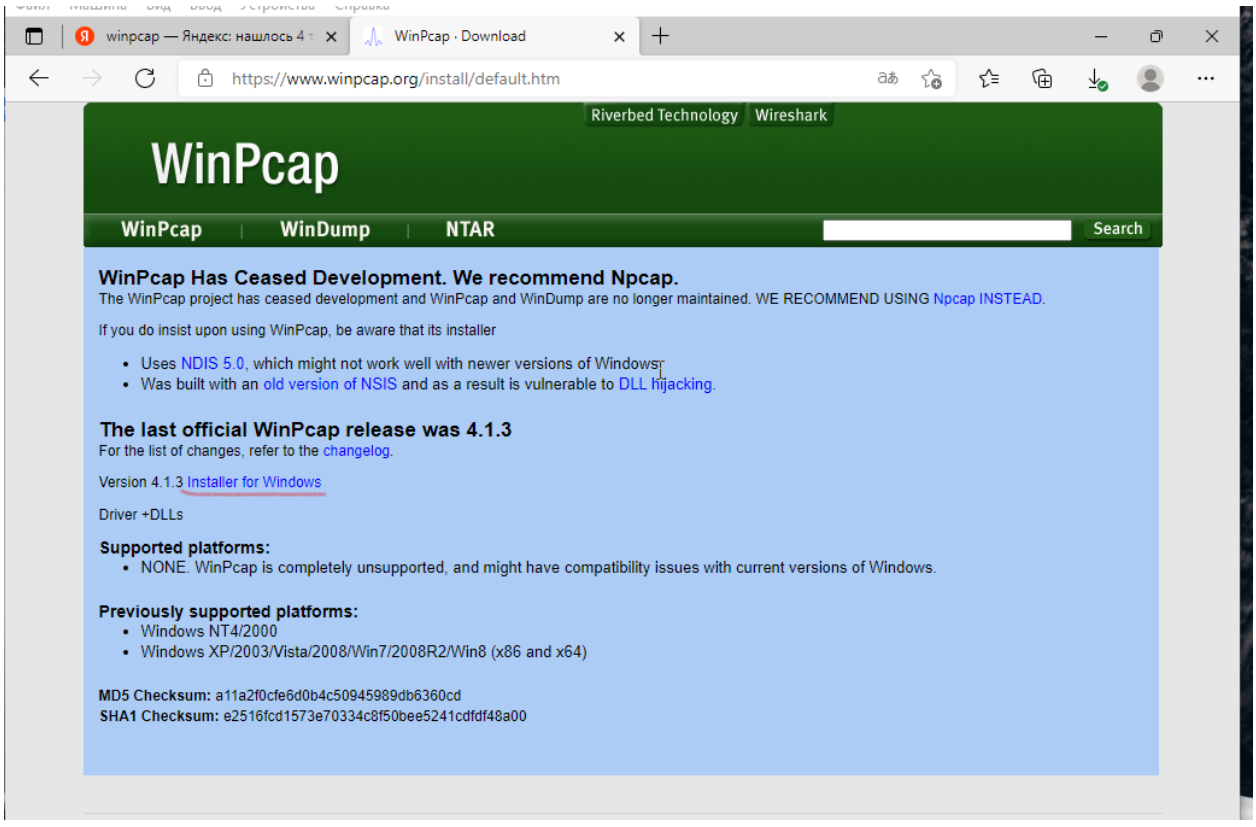
1. Установить и развернуть snort.

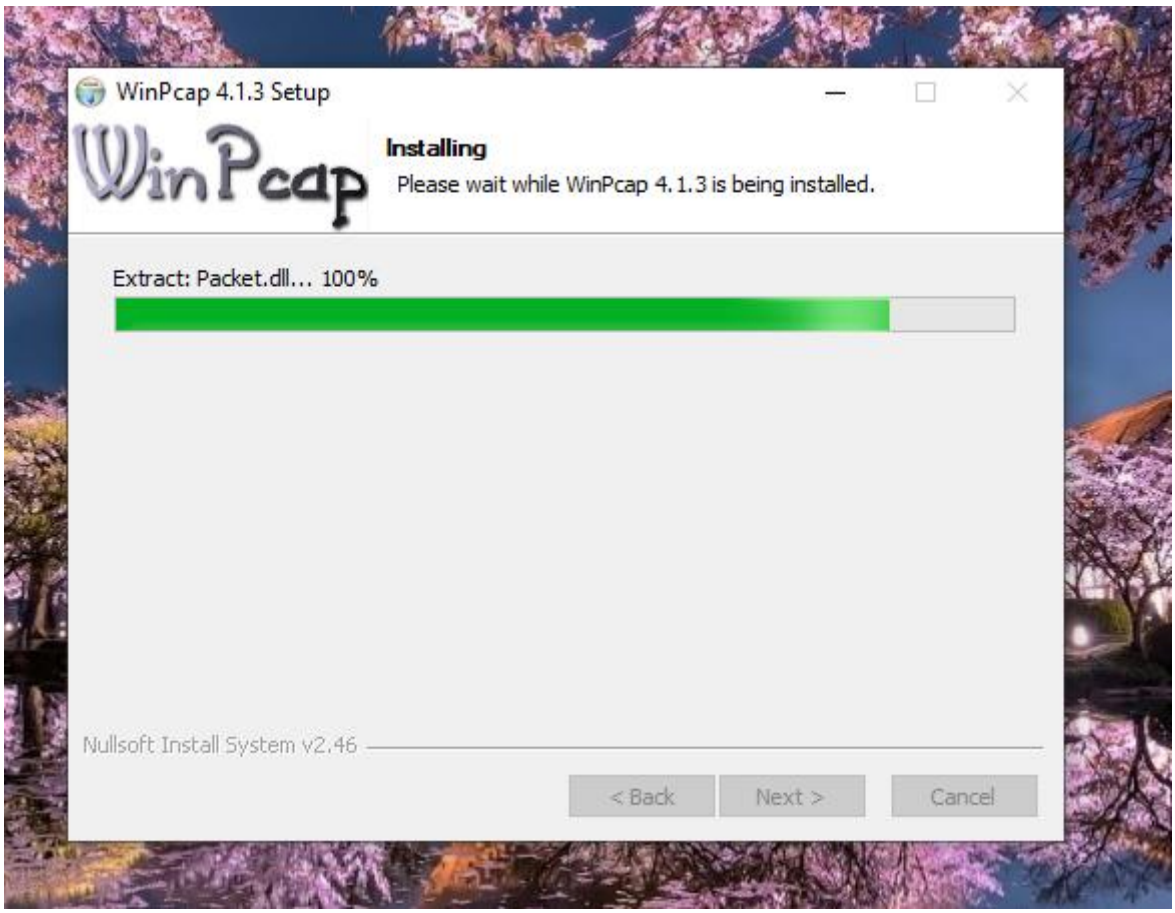
Установка и развертывание будет происходить на виртуальной машине Windows 10.



Установим утилиту WinPcap:

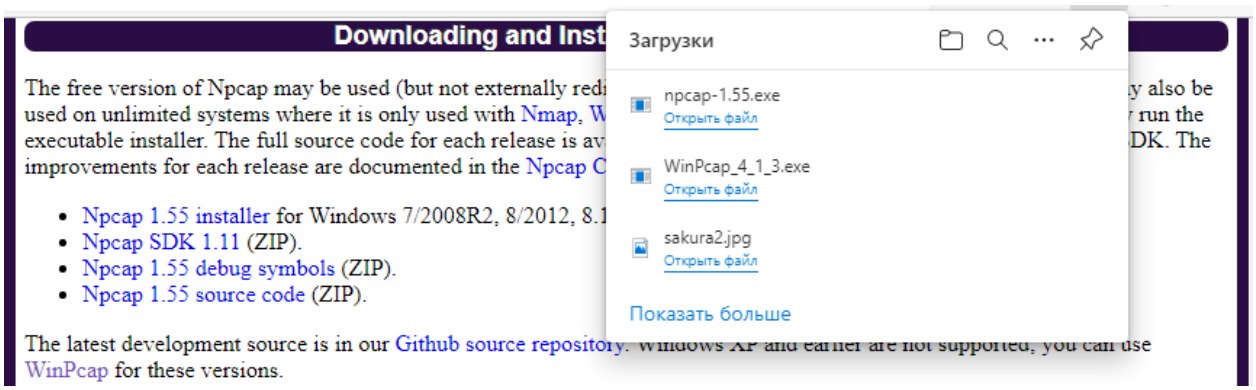

Windows 10 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
winpcap — Яндекс: нашлось 4
WinPcap - Home
https://www.winpcap.org
Riverbed Technology Wireshark
WinPcap
The industry-standard windows packet capture library
WinPcap | WinDump | NTAR
Search
Download
Get WinPcap
Documentation
Support
News and Releases
15 September 2018
WinPcap, though still available for download (v4.1.3), has not seen an upgrade in many years and there are no road map/future plans to update the technology. While community support may persist, technical oversight by Riverbed staff, responses to questions posed by Riverbed resources, and bug reporting are no longer available.
Gordon Lyon, Nmap project founder, has created Npcap, a packet capture library for Windows, that includes WinPcap compatibility and may be a suitable replacement for WinPcap and WinPcap Pro. Information can be found at https://nmap.org/npcap/.
More...
Introduction to WinPcap
For many years, WinPcap has been recognized as the industry-standard tool for link-layer network access in Windows environments, allowing applications to capture and transmit network packets bypassing the protocol stack, and including kernel-level packet filtering, a network statistics engine and support for remote packet capture.
WinPcap consists of a driver that extends the operating system to provide low-level network access and a library that is used to easily access low-level network layers. This library also contains the Windows version of the well-known libpcap Unix API.
Thanks to its set of features, WinPcap has been the packet capture and filtering engine for many open source and commercial network tools, including protocol analyzers, network monitors, network intrusion detection systems, sniffers, traffic generators and network testers. Some of these networking tools, like Wireshark, Nmap, Snort, and ntop are known and used throughout the networking community.
Чтобы начать поиск, введите здесь
-2°C
ENG
16:43
05.12.2021
Right Ctrl

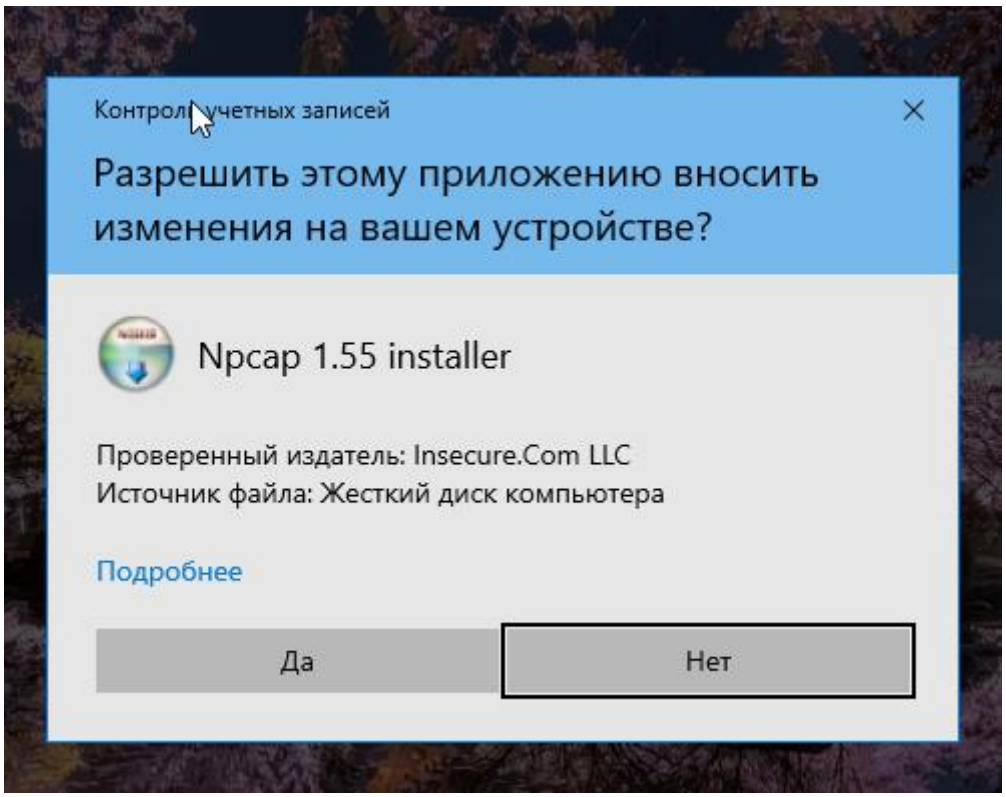

winpcap — Яндекс: нашлось 4
WinPcap - Download
https://www.winpcap.org/install/default.htm
Riverbed Technology Wireshark
WinPcap
WinPcap | WinDump | NTAR
Search
WinPcap Has Ceased Development. We recommend Npcap.
The WinPcap project has ceased development and WinPcap and WinDump are no longer maintained. WE RECOMMEND USING Npcap INSTEAD.
If you do insist upon using WinPcap, be aware that its installer
Uses NDIS 5.0, which might not work well with newer versions of Windows.
Was built with an old version of NSIS and as a result is vulnerable to DLL hijacking.
The last official WinPcap release was 4.1.3
For the list of changes, refer to the changelog.
Version 4.1.3 Installer for Windows
Driver +DLLs
Supported platforms:
NONE. WinPcap is completely unsupported, and might have compatibility issues with current versions of Windows.
Previously supported platforms:
Windows NT4/2000
Windows XP/2003/Vista/2008/Win7/2008R2/Win8 (x86 and x64)
MD5 Checksum: a11a2f0cfe6d0b4c50945989db6360cd
SHA1 Checksum: e2516fcd1573e70334c8f50bee5241cdfdf48a00

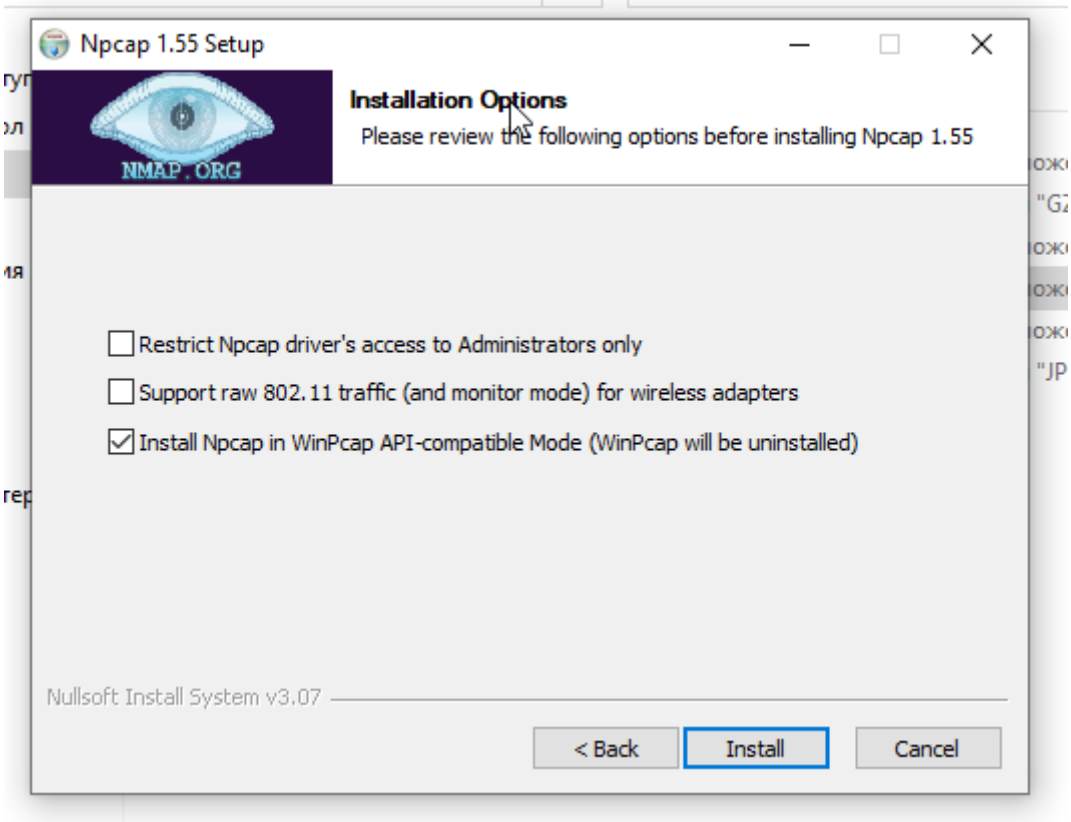


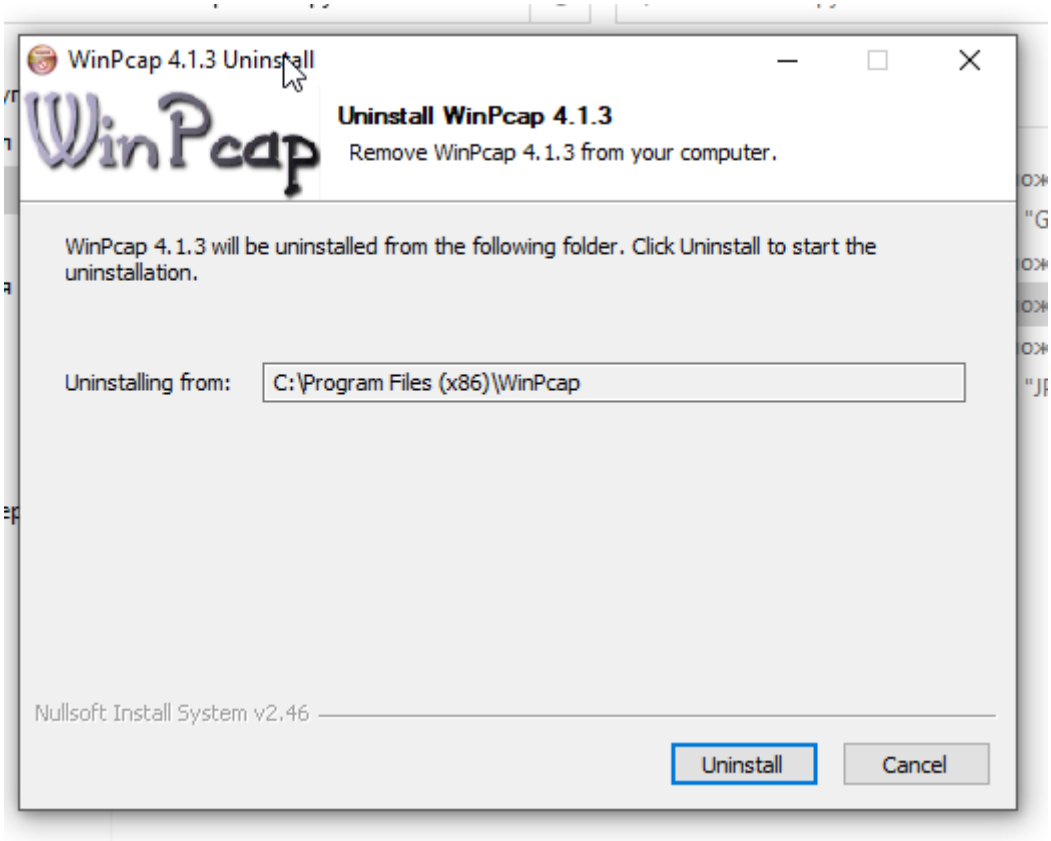
Также установим Npcap – библиотеку, предназначенную для сниффинга (и отправки) пакетов:

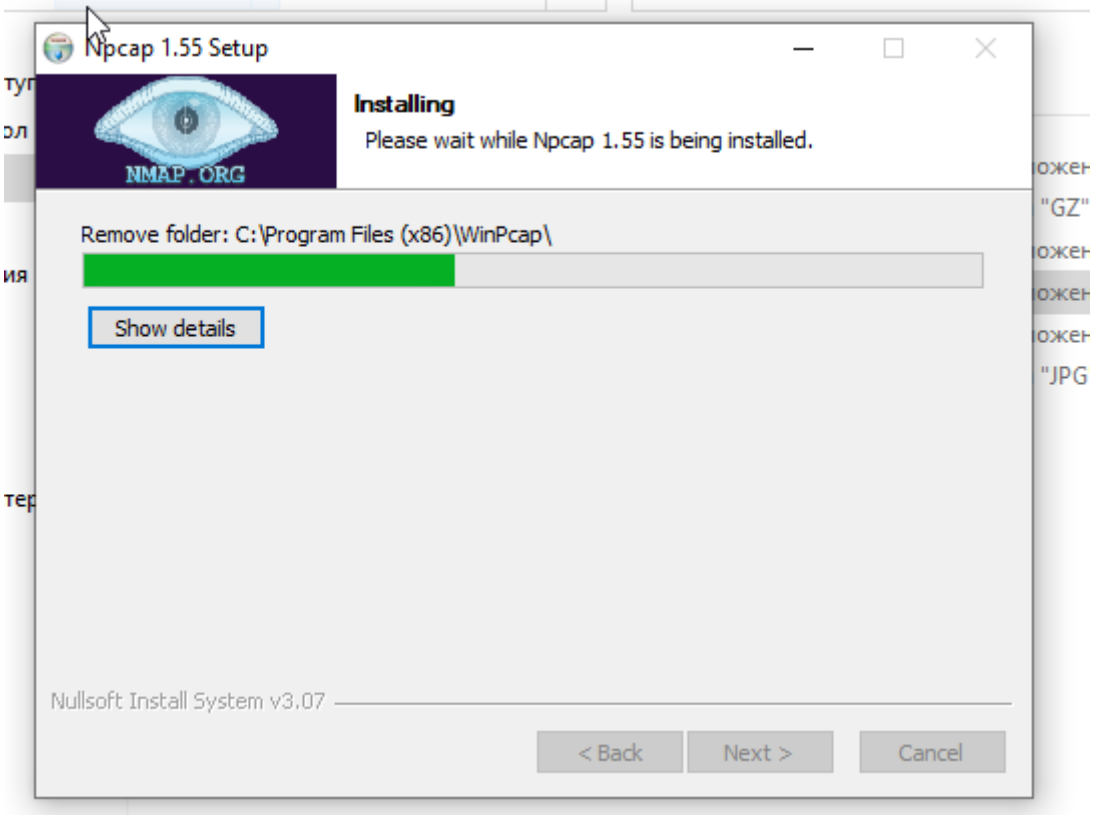

Windows 10 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Npcap: Windows Packet Capture
WinPcap - Download
https://nmap.org/npcap/
NMAP.ORG
Nmap Security Scanner
Intro
Ref Guide
Install Guide
Download
Changelog
Book
Docs
Security Lists
Nmap Announce
Nmap Dev
Bugtraq
Full Disclosure
Pen Test
Basics
More
Security Tools
Password audit
CorelCAD
CorelCAD 2021 Sale
DOWNLOAD
Npcap
Packet capture library for Windows
Npcap is the Nmap Project's packet capture (and sending) library for Microsoft Windows. It implements the open Pcap API using a custom Windows kernel driver alongside our Windows build of the excellent libpcap library. This allows Windows software to capture raw network traffic (including wireless networks, wired ethernet, localhost traffic, and many VPNs) using a simple, portable API. Npcap allows for sending raw packets as well. Mac and Linux systems already include the Pcap API, so Npcap allows popular software such as Nmap and Wireshark to run on all these platforms (and more) with a single codebase. Npcap began in 2013 as some improvements to the (now discontinued) WinPcap library, but has been largely rewritten since then with hundreds of releases improving Npcap's speed, portability, security, and efficiency. In particular, Npcap now offers:

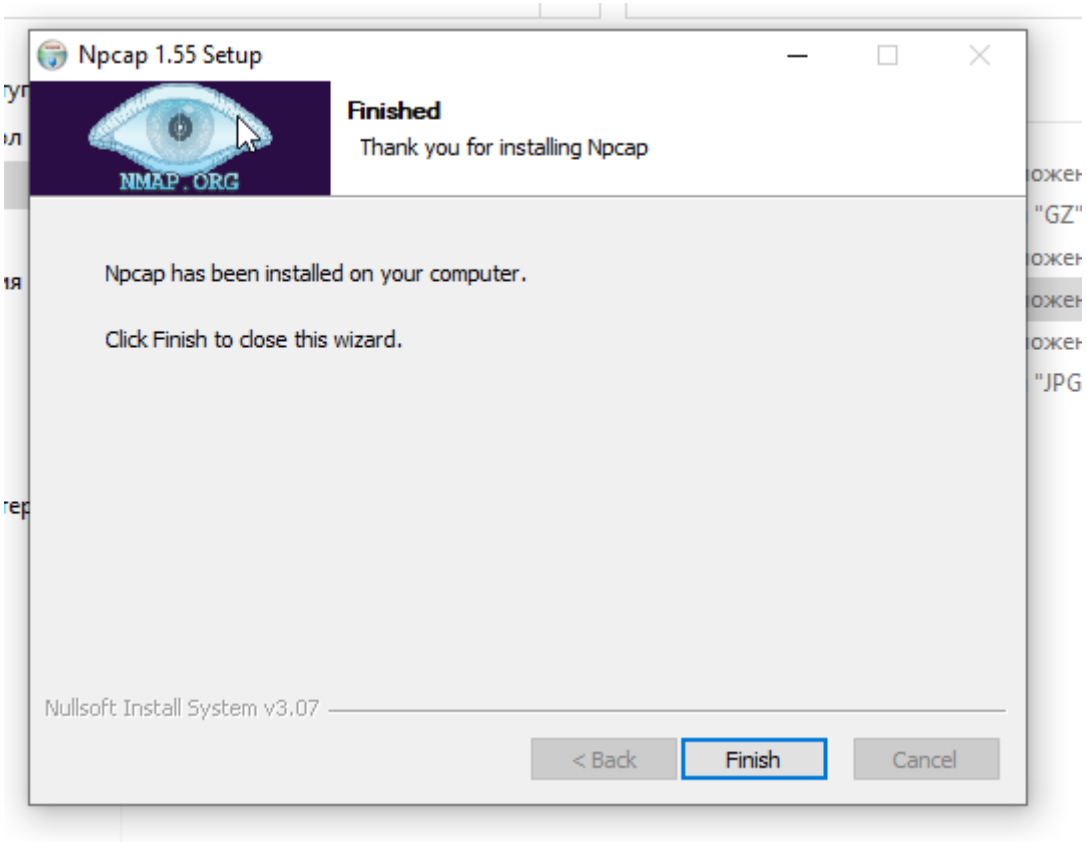

Downloading and Inst
The free version of Npcap may be used (but not externally redi
used on unlimited systems where it is only used with Nmap, W
executable installer. The full source code for each release is av
improvements for each release are documented in the Npcap C
Npcap 1.55 installer for Windows 7/2008R2, 8/2012, 8.1
Npcap SDK 1.11 (ZIP).
Npcap 1.55 debug symbols (ZIP).
Npcap 1.55 source code (ZIP).
The latest development source is in our Github source repository.
WinPcap for these versions.
Загрузки
npcap-1.55.exe
Открыть файл
WinPcap_4_1_3.exe
Открыть файл
sakura2.jpg
Открыть файл
Показать больше


Контроль учетных записей
Разрешить этому приложению вносить изменения на вашем устройстве?
Npcap 1.55 installer
Проверенный издатель: Insecure.Com LLC
Источник файла: Жесткий диск компьютера
Подробнее
Да
Нет

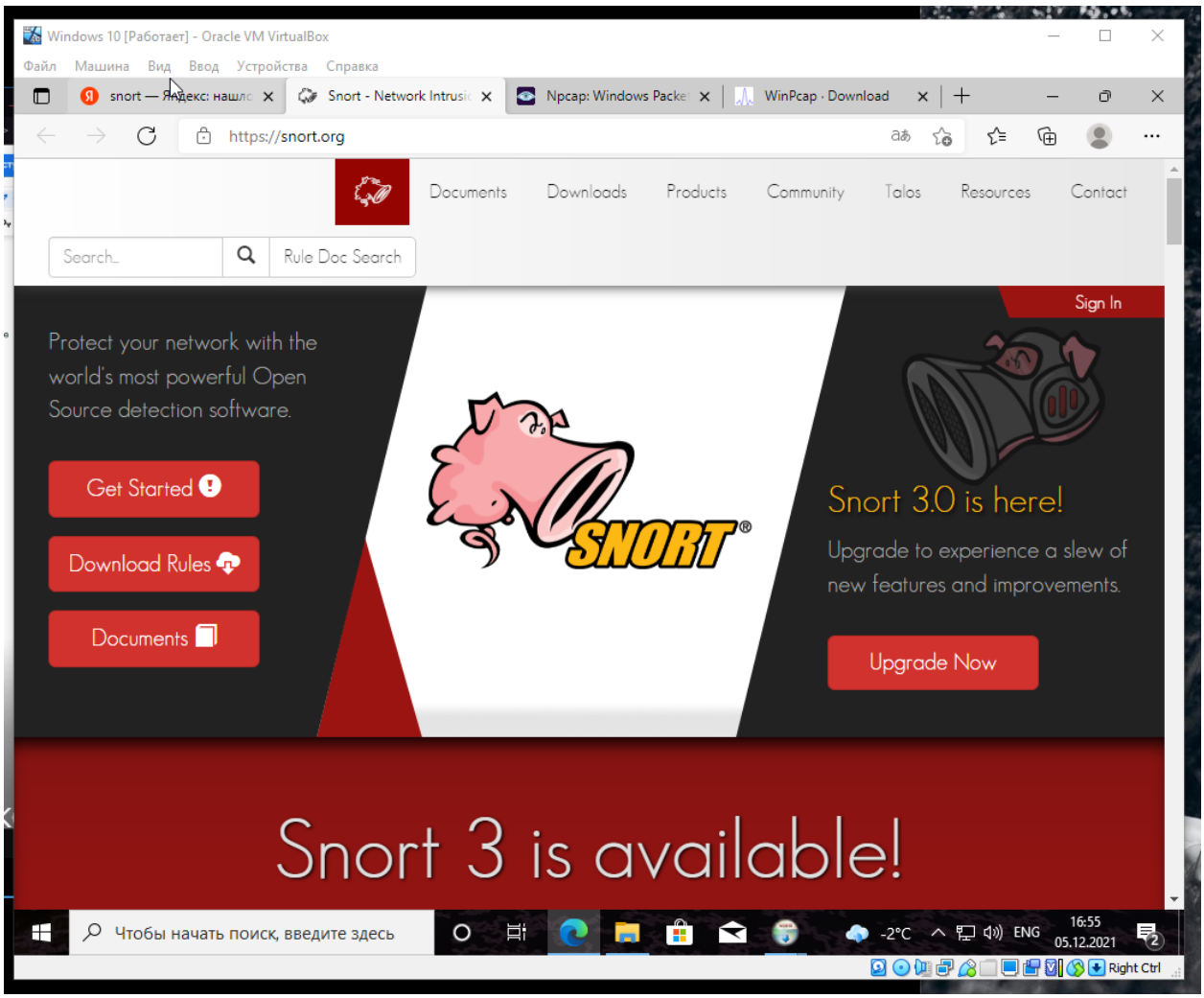

Npcap 1.55 Setup
NMAP.ORG
Installation Options
Please review the following options before installing Npcap 1.55
Restrict Npcap driver's access to Administrators only
Support raw 802.11 traffic (and monitor mode) for wireless adapters
Install Npcap in WinPcap API-compatible Mode (WinPcap will be uninstalled)
Nullsoft Install System v3.07
< Back
Install
Cancel


WinPcap 4.1.3 Uninstall
WinPcap
Uninstall WinPcap 4.1.3
Remove WinPcap 4.1.3 from your computer.
WinPcap 4.1.3 will be uninstalled from the following folder. Click Uninstall to start the uninstallation.
Uninstalling from:
C:\Program Files (x86)\WinPcap
Nullsoft Install System v2.46
Uninstall
Cancel

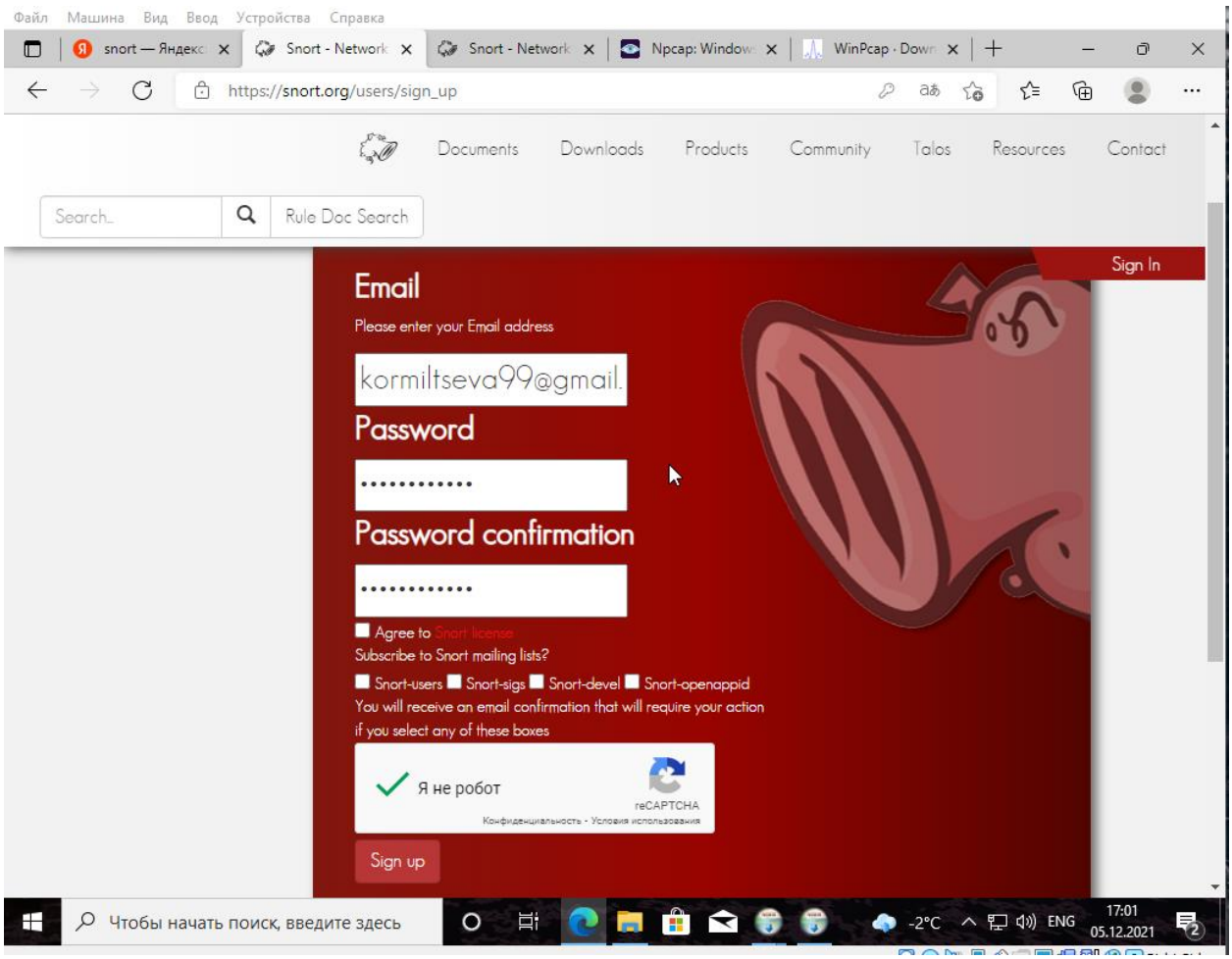

Npcap 1.55 Setup
NMAP.ORG
Installing
Please wait while Npcap 1.55 is being installed.
Remove folder: C:\Program Files (x86)\WinPcap\
Show details
Nullsoft Install System v3.07
< Back
Next >
Cancel

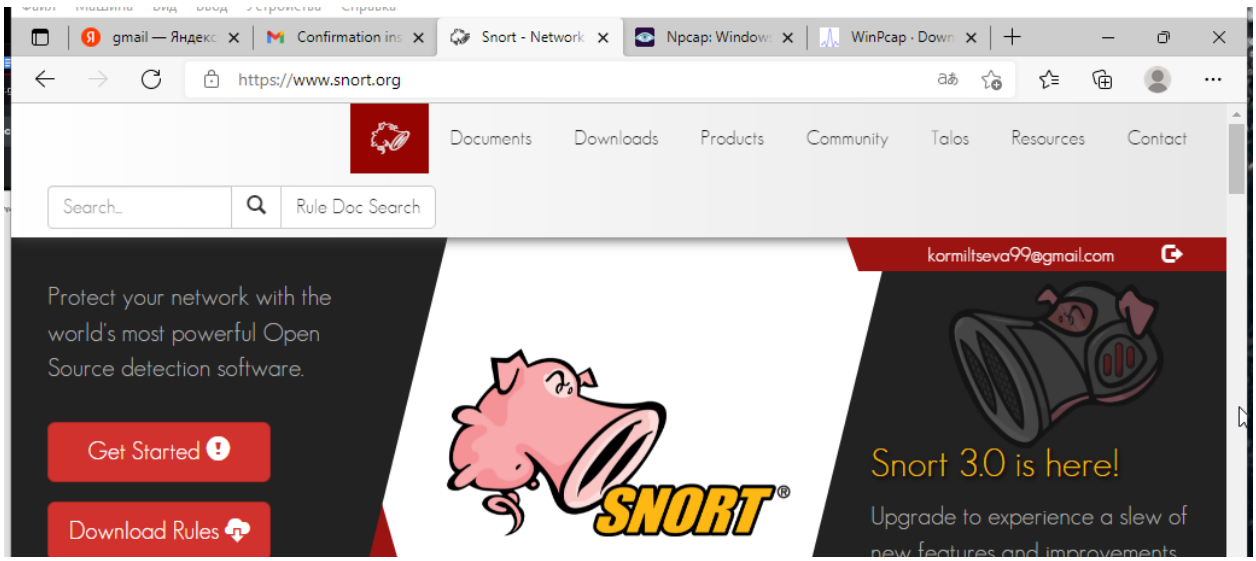


После перейдем на сайт Snort:

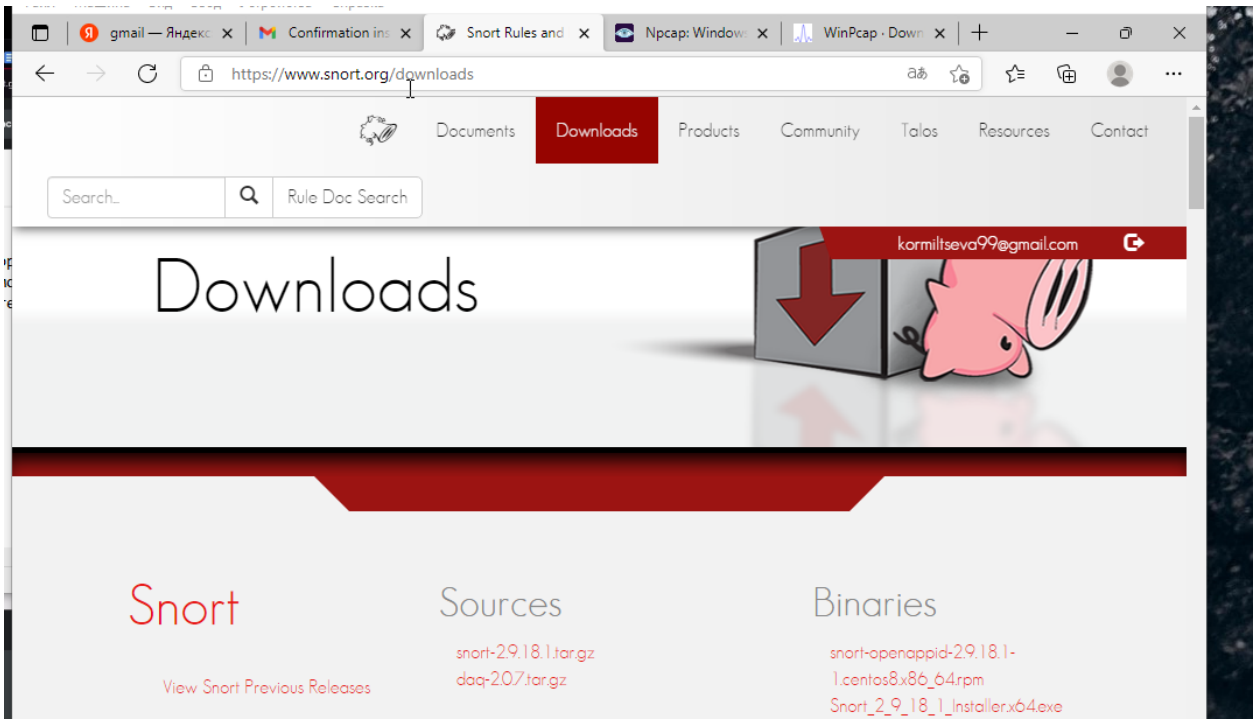


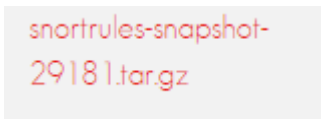
Зарегистрируемся на сайте для получения подписки:



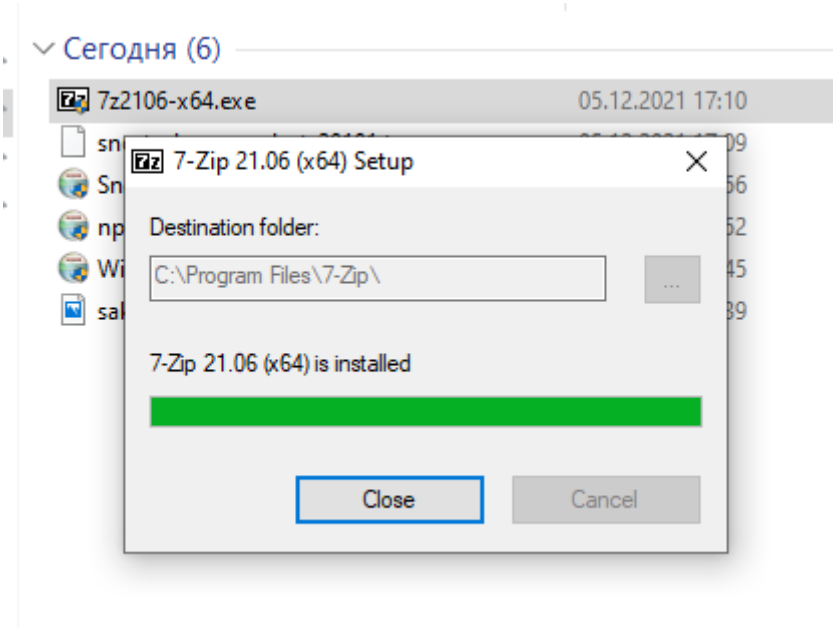


Далее загружаем правила, по которым Snort будет работать:

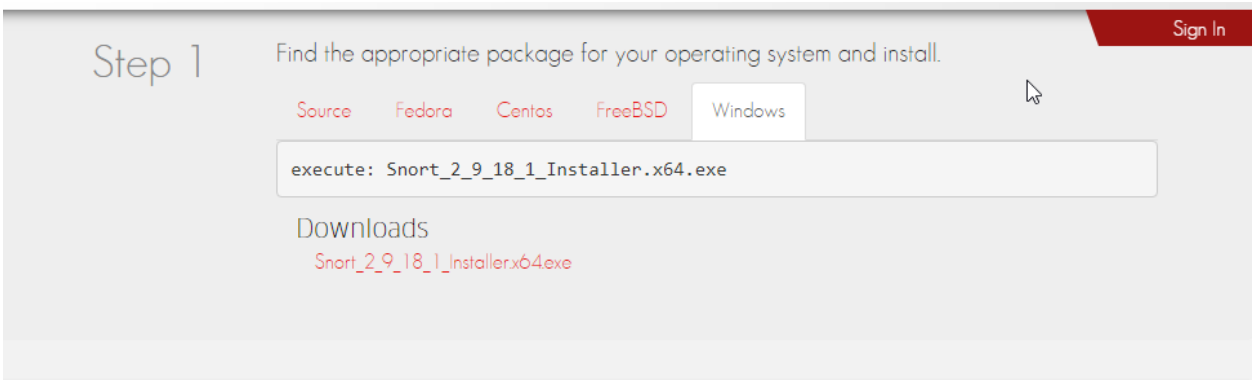


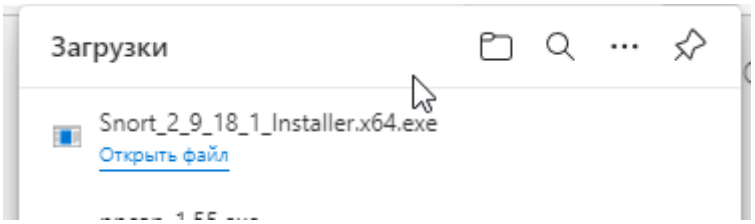


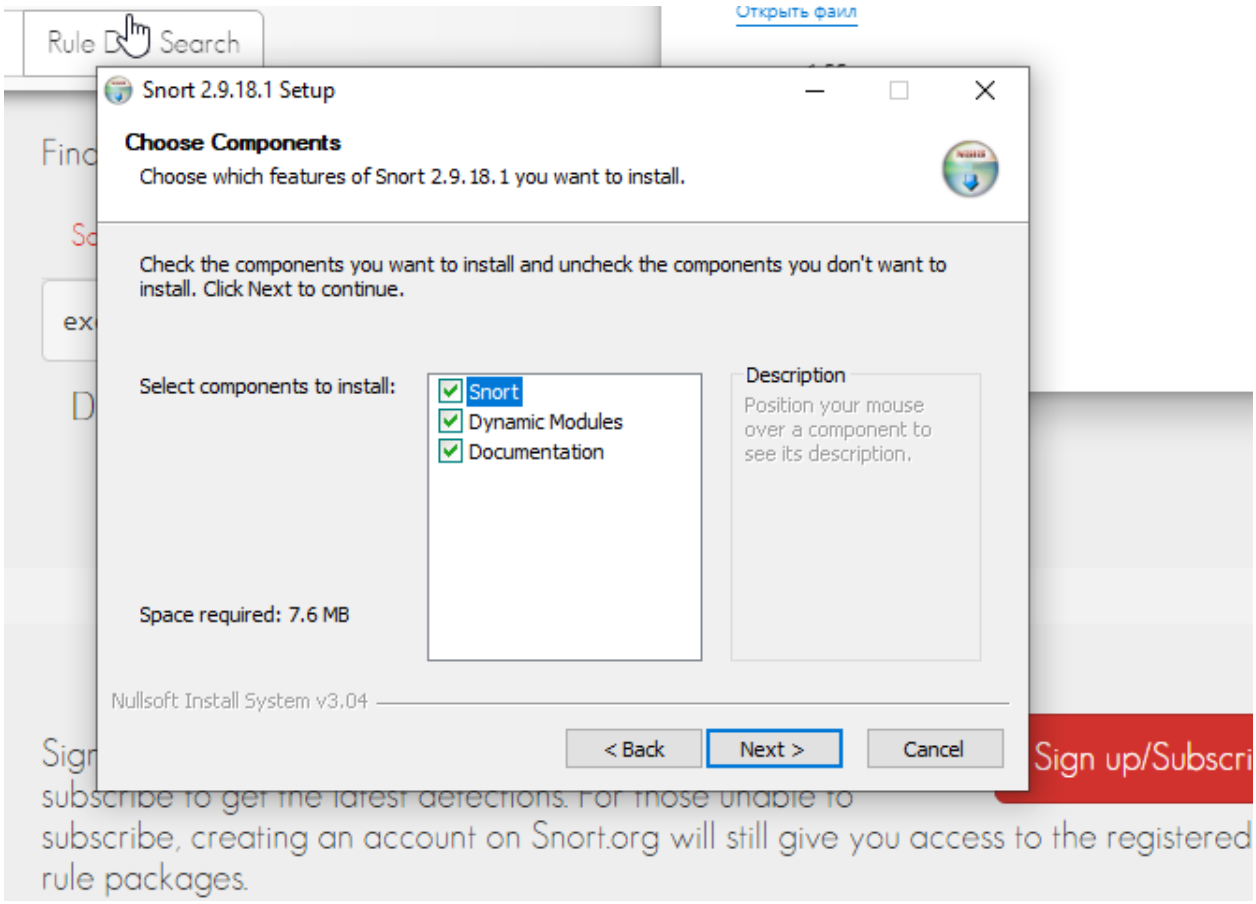
И установим архиватор для разархивирования скачанного файла:

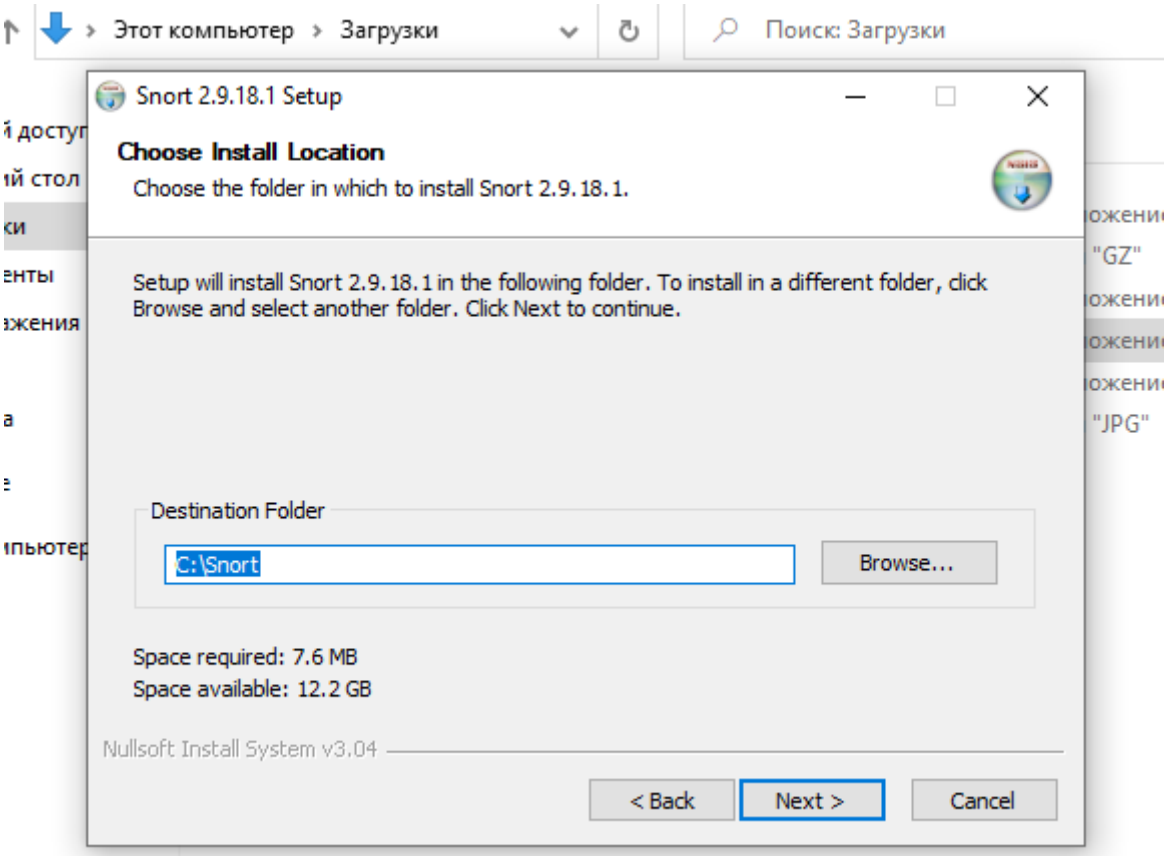


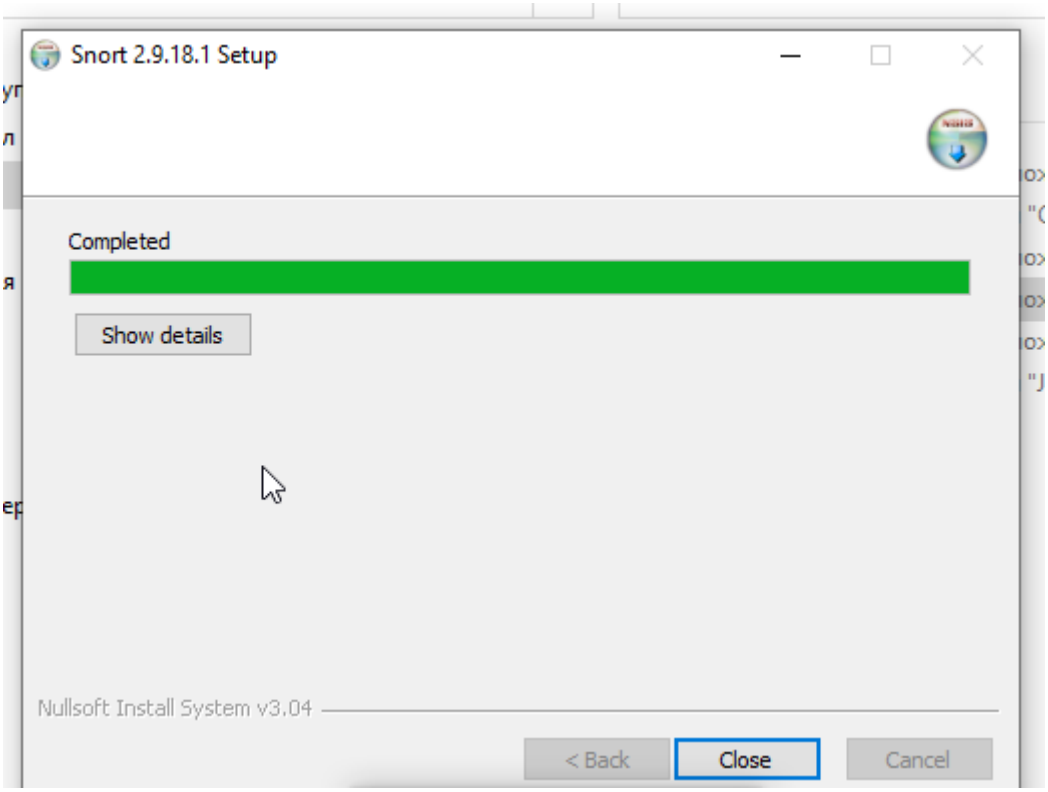
После скачаем файл Snort:

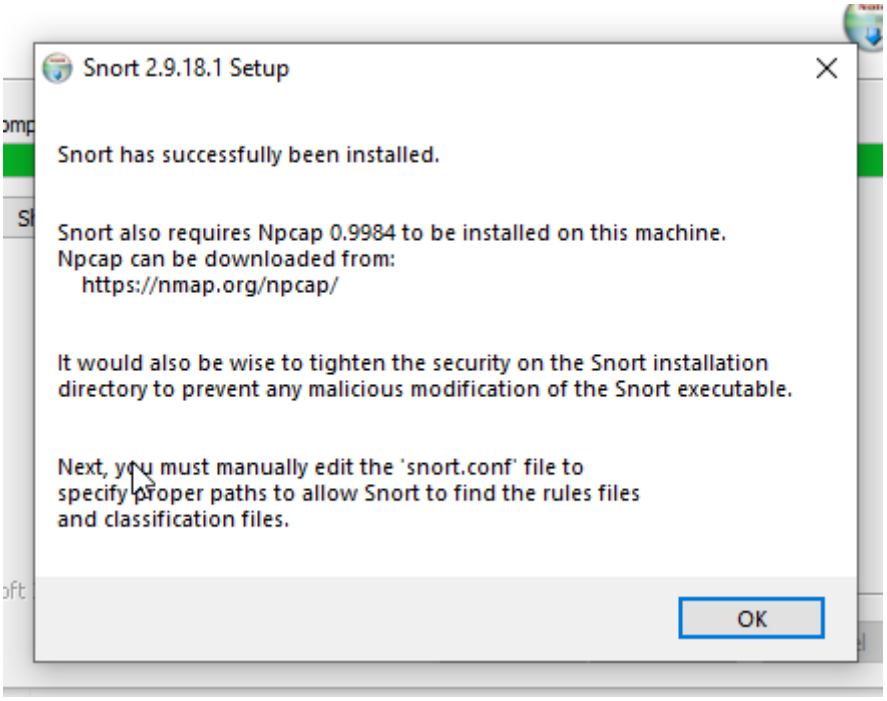




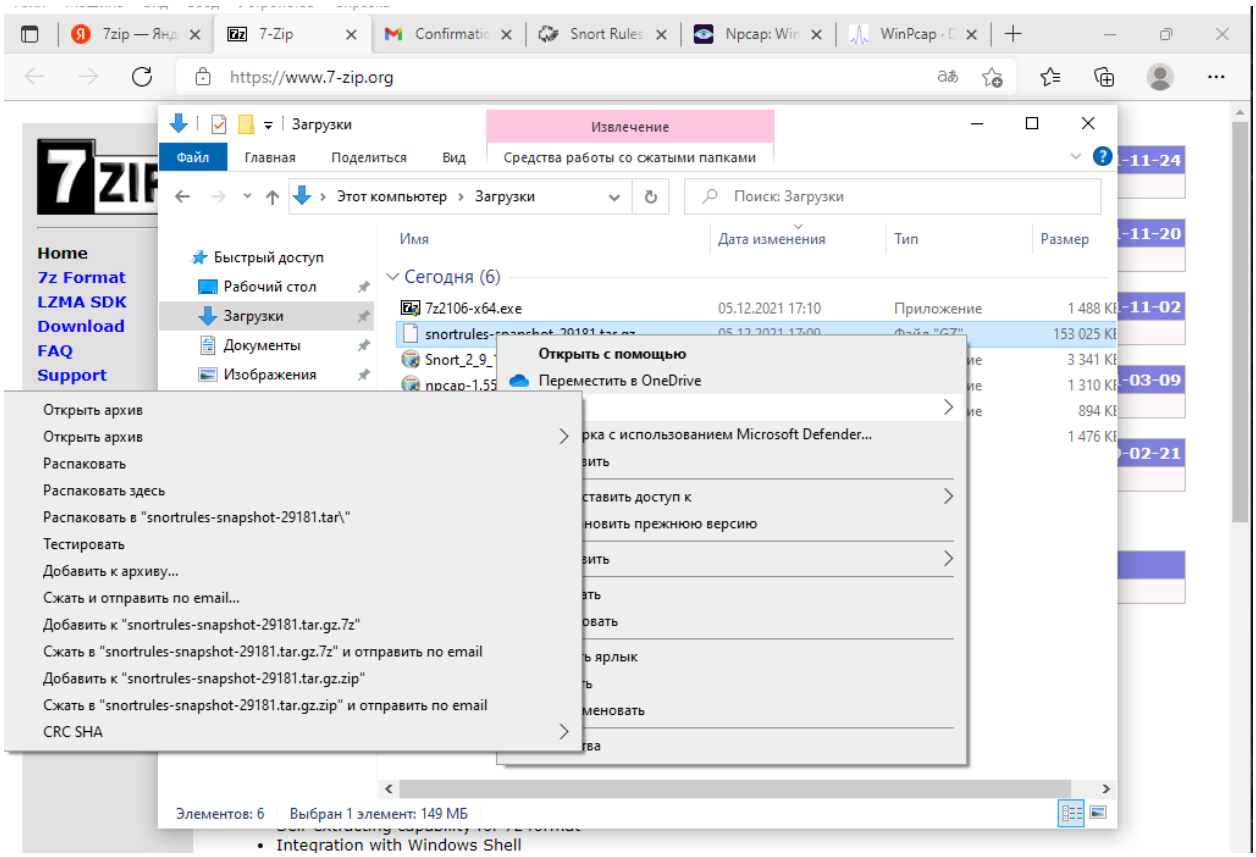

Rule Search
Открыть файл
Snort 2.9.18.1 Setup
Choose Components
Choose which features of Snort 2.9.18.1 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
Snort
Dynamic Modules
Documentation
Description
Position your mouse over a component to see its description.
Space required: 7.6 MB
Nullsoft Install System v3.04
< Back
Next >
Cancel
Sign up/Subscri
subscribe, creating an account on Snort.org will still give you access to the registered rule packages.

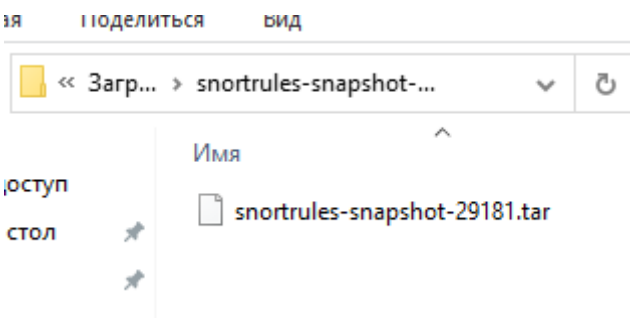

Этот компьютер › Загрузки
Поиск: Загрузки
Snort 2.9.18.1 Setup
Choose Install Location
Choose the folder in which to install Snort 2.9.18.1.
Setup will install Snort 2.9.18.1 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Snort
Browse...
Space required: 7.6 MB
Space available: 12.2 GB
Nullsoft Install System v3.04
< Back
Next >
Cancel

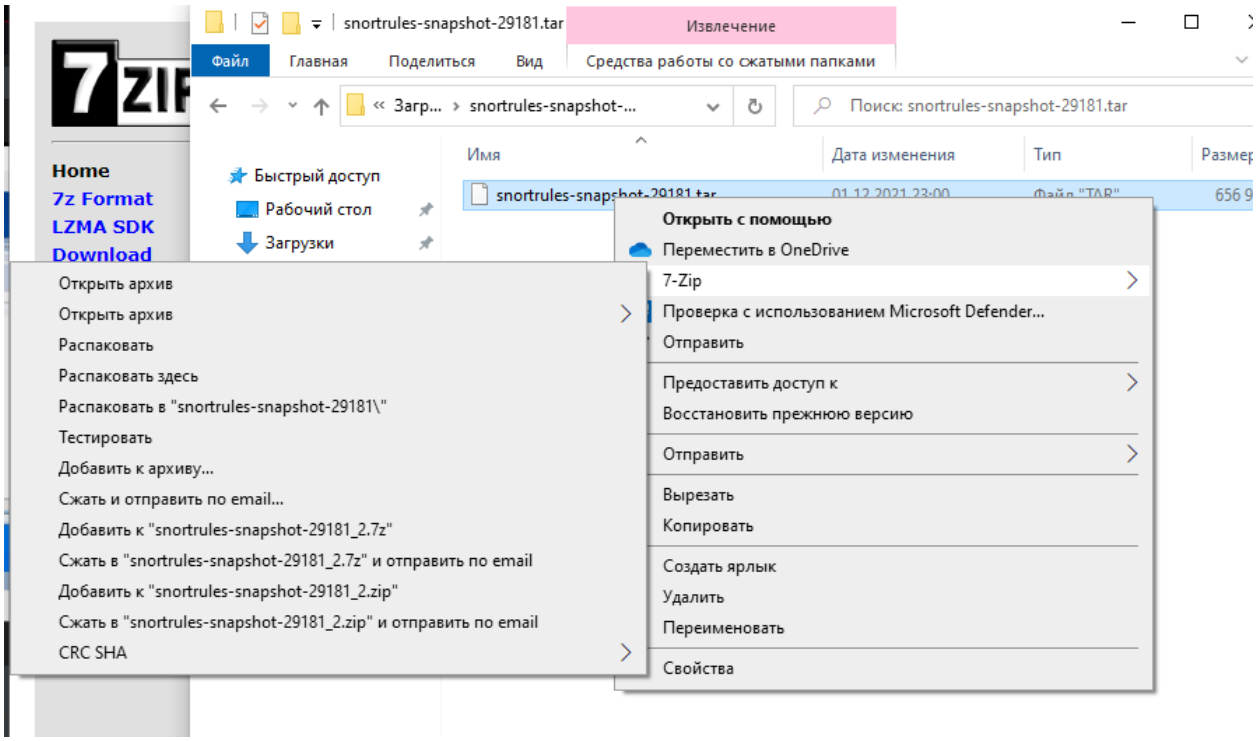


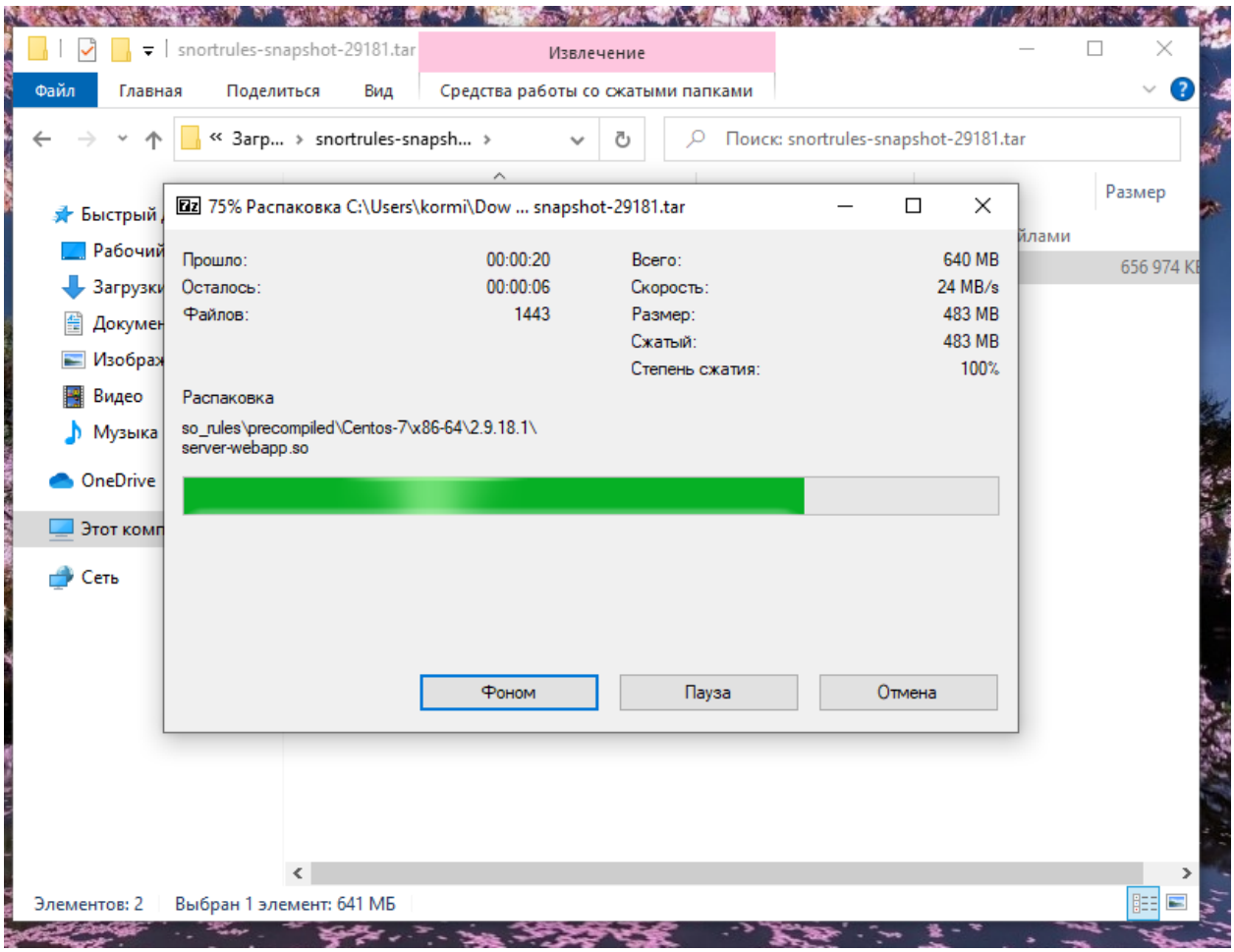


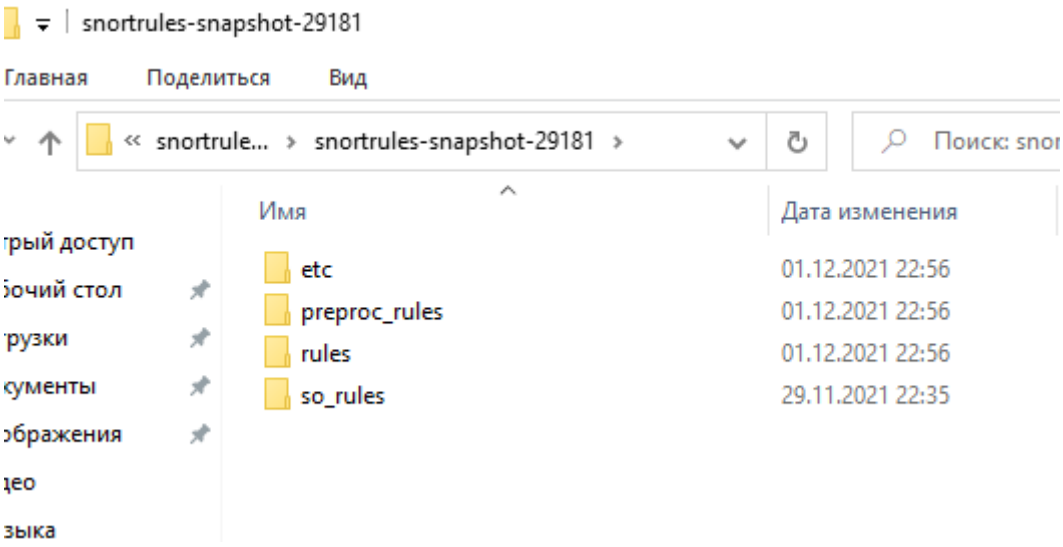
Распакуем файл с правилами:


7zip — Янд
7-Zip
Confirmatic
Snort Rules
Npcap: Win
WinPcap
https://www.7-zip.org
Загрузки
Извлечение
Файл
Главная
Поделиться
Вид
Средства работы со сжатыми папками
Этот компьютер › Загрузки
Поиск: Загрузки
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Имя
Дата изменения
Тип
Размер
Сегодня (6)
7z2106-x64.exe
05.12.2021 17:10
Приложение
1 488 КБ
153 025 КБ
3 341 КБ
1 310 КБ
894 КБ
1 476 КБ
Открыть с помощью
Переместить в OneDrive
Проверка с использованием Microsoft Defender...
Открыть архив
Открыть архив
Распаковать
Распаковать здесь
Распаковать в "snortrules-snapshot-29181.tar\"
Тестировать
Добавить к архиву...
Сжать и отправить по email...
Добавить к "snortrules-snapshot-29181.tar.gz.7z"
Сжать в "snortrules-snapshot-29181.tar.gz.7z" и отправить по email
Добавить к "snortrules-snapshot-29181.tar.gz.zip"
Сжать в "snortrules-snapshot-29181.tar.gz.zip" и отправить по email
CRC SHA
Элементов: 6
Выбран 1 элемент: 149 МБ
Home
7z Format
LZMA SDK
Download
FAQ
Support
Integration with Windows Shell

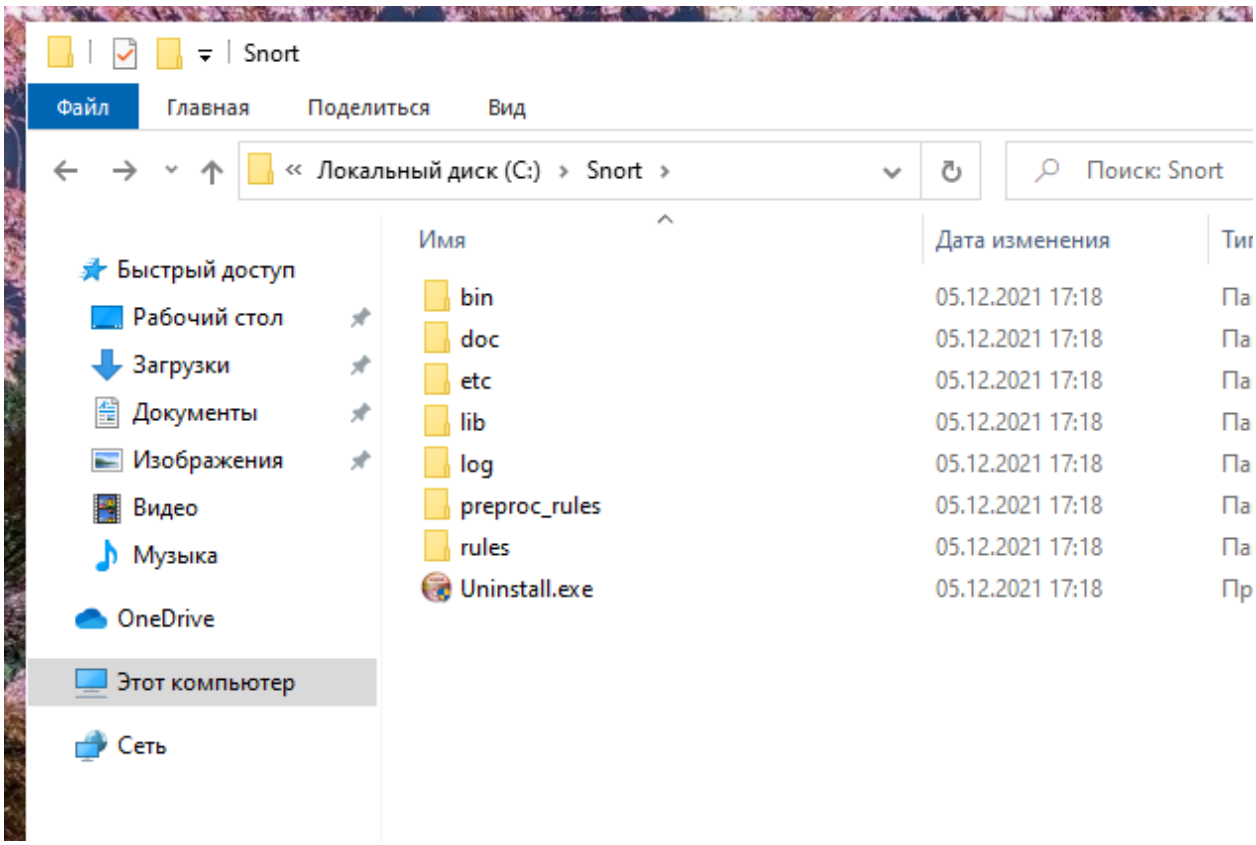

Поделиться
Вид
Загр... › snortrules-snapshot-...
Имя
snortrules-snapshot-29181.tar


snortrules-snapshot-29181.tar
Извлечение
Файл
Главная
Поделиться
Вид
Средства работы со сжатыми папками
Загр... › snortrules-snapshot-...
Поиск: snortrules-snapshot-29181.tar
Быстрый доступ
Рабочий стол
Загрузки
Имя
Дата изменения
Тип
Открыть с помощью
Переместить в OneDrive
7-Zip
Проверка с использованием Microsoft Defender...
Отправить
Предоставить доступ к
Восстановить прежнюю версию
Отправить
Вырезать
Копировать
Создать ярлык
Удалить
Переименовать
Свойства
Открыть архив
Открыть архив
Распаковать
Распаковать здесь
Распаковать в "snortrules-snapshot-29181\"
Тестировать
Добавить к архиву...
Сжать и отправить по email...
Добавить к "snortrules-snapshot-29181_2.7z"
Сжать в "snortrules-snapshot-29181_2.7z" и отправить по email
Добавить к "snortrules-snapshot-29181_2.zip"
Сжать в "snortrules-snapshot-29181_2.zip" и отправить по email
CRC SHA
Home
7z Format
LZMA SDK
Download

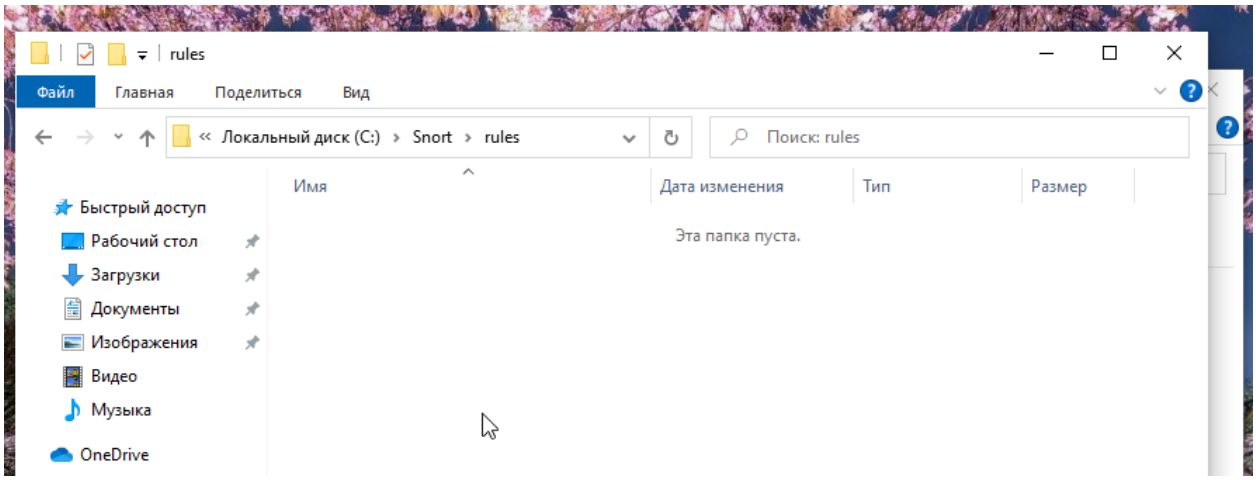




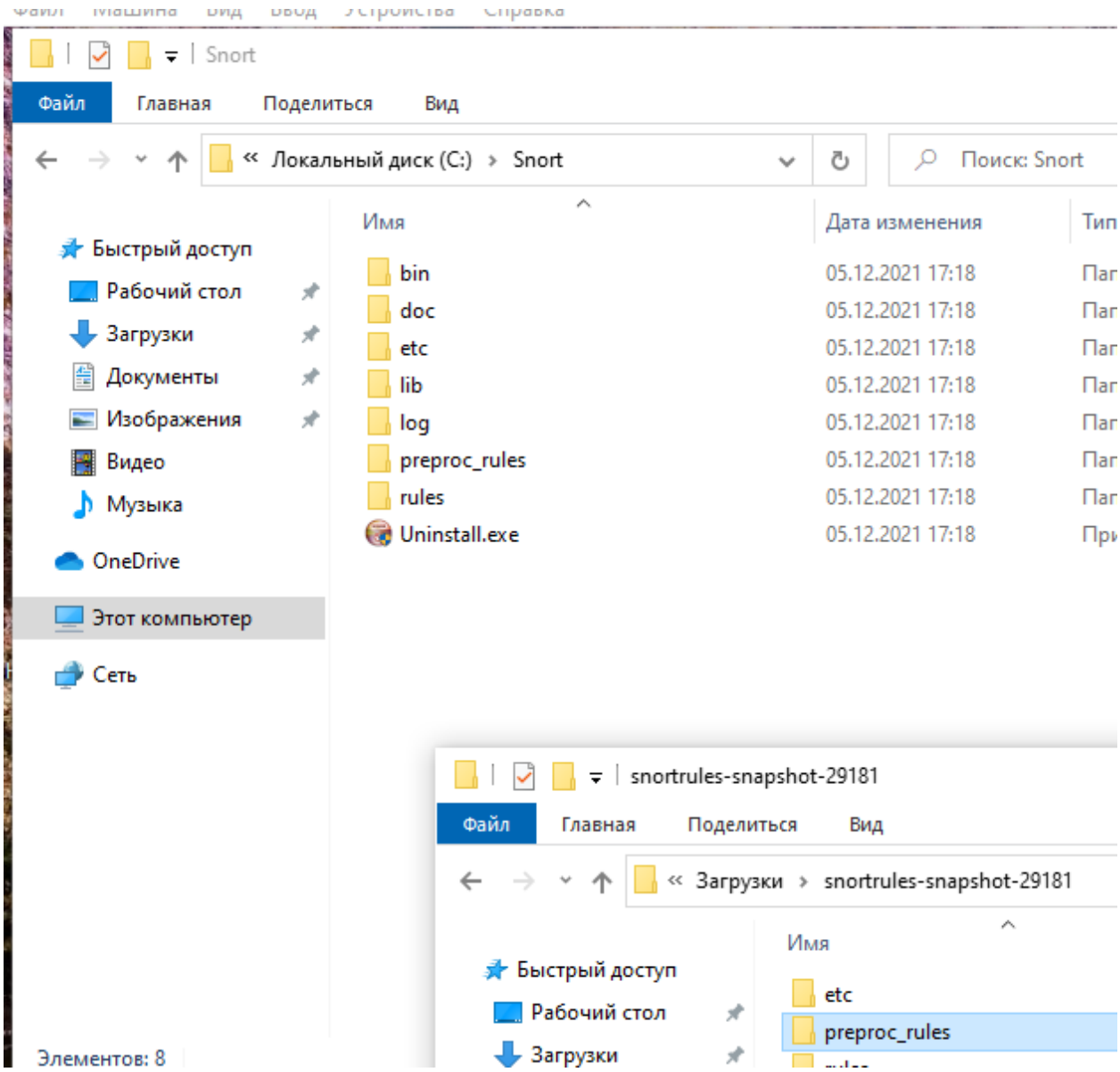
Перейдем к папке установленной утилиты Snort на диске C:

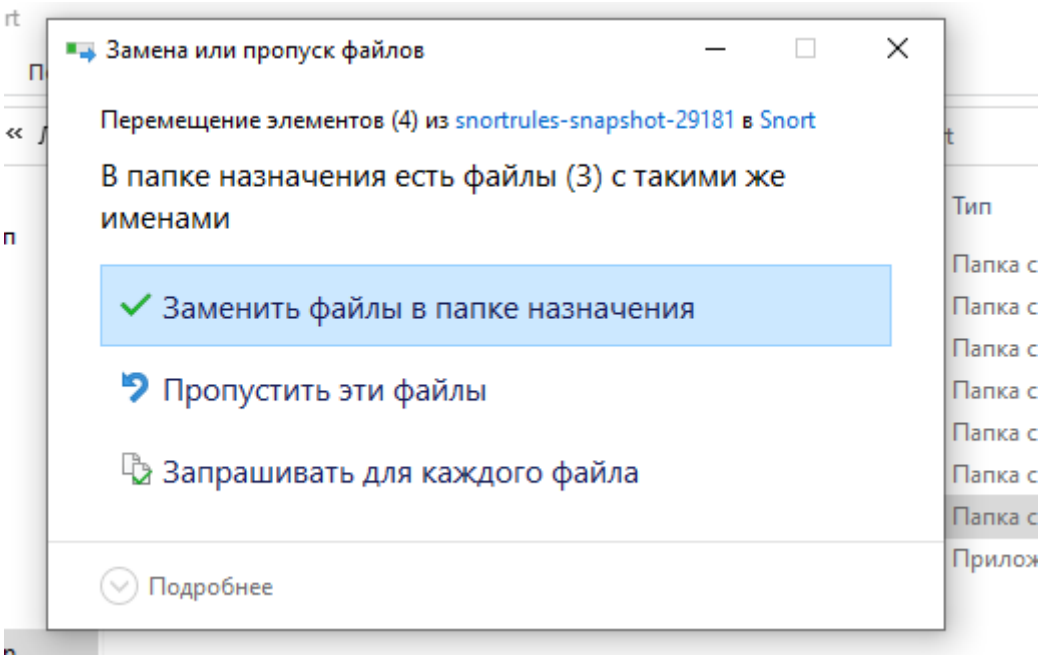


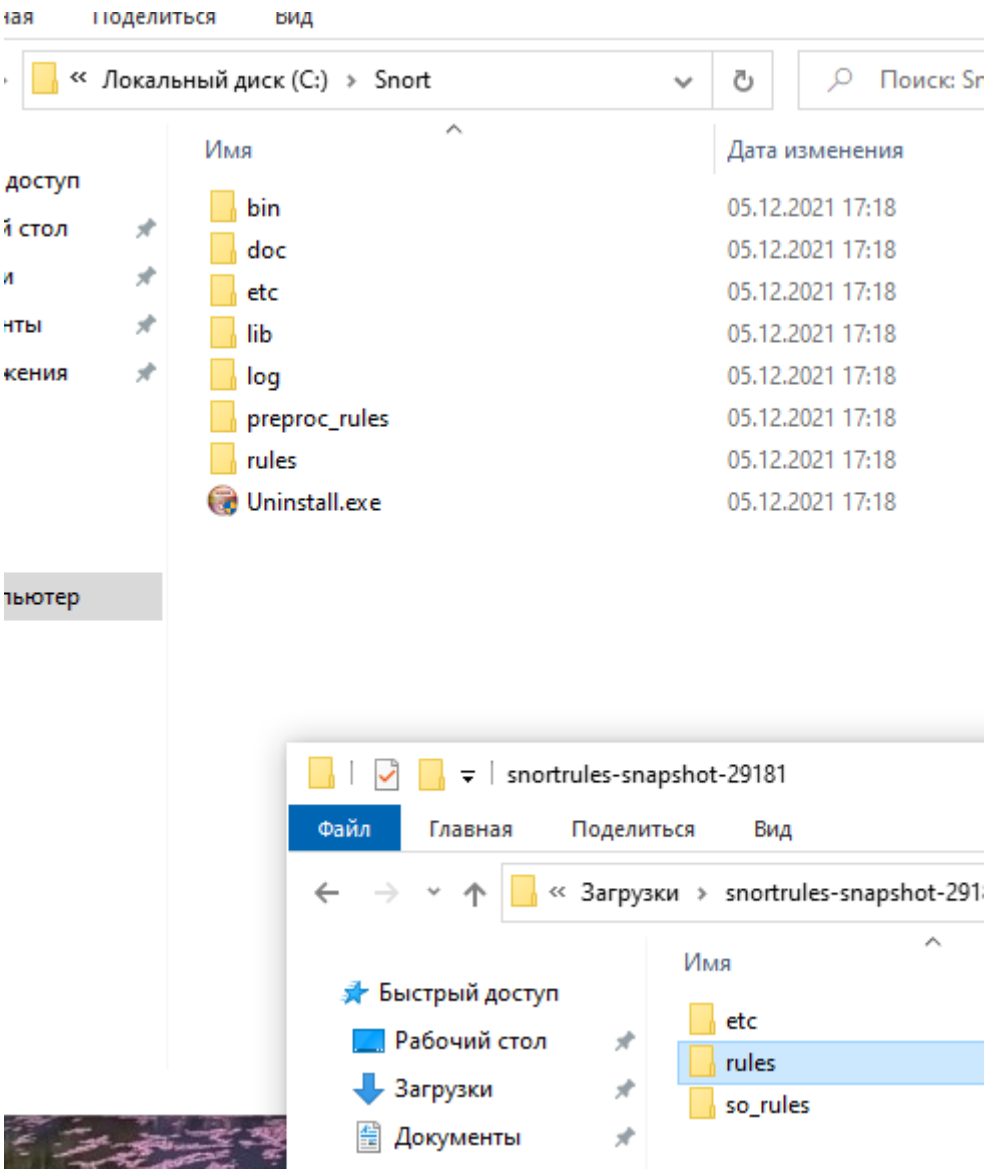
Папка rules пуста:

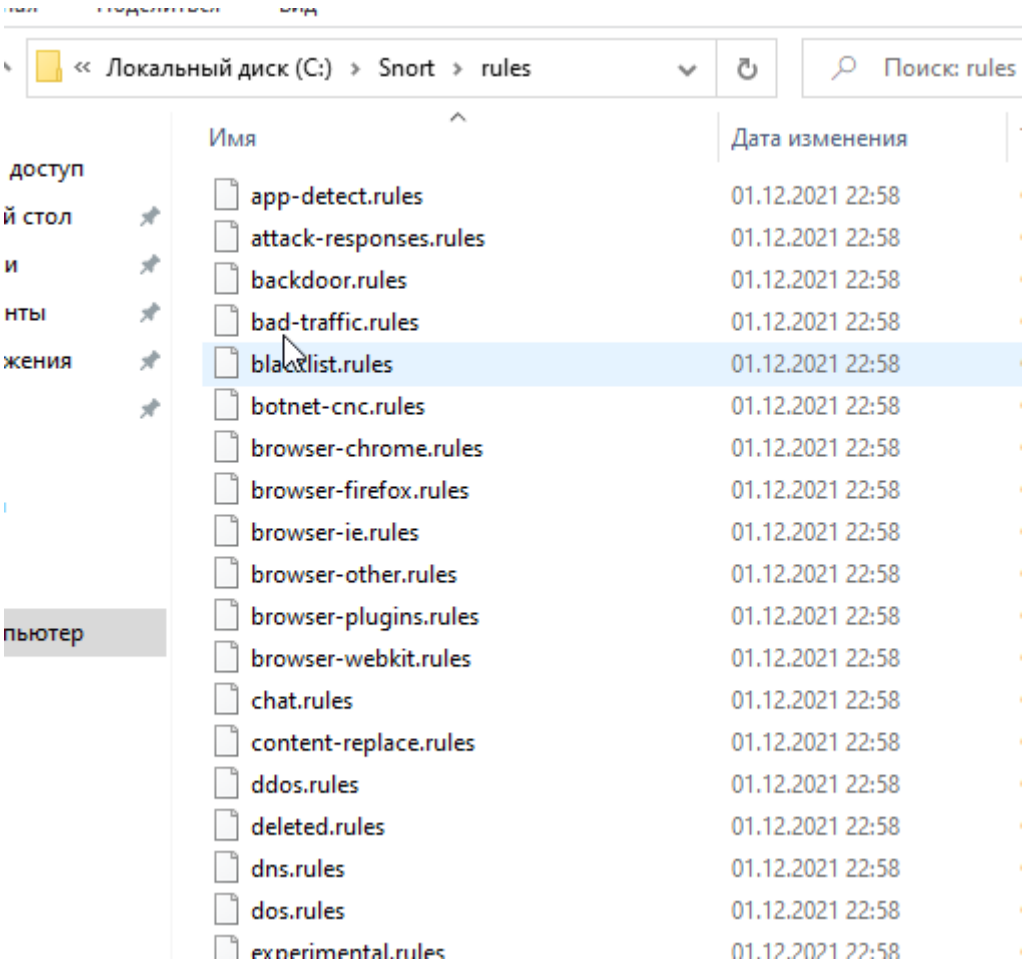


Заменим некоторые папки теми, что были скачаны с архивом с правилами:

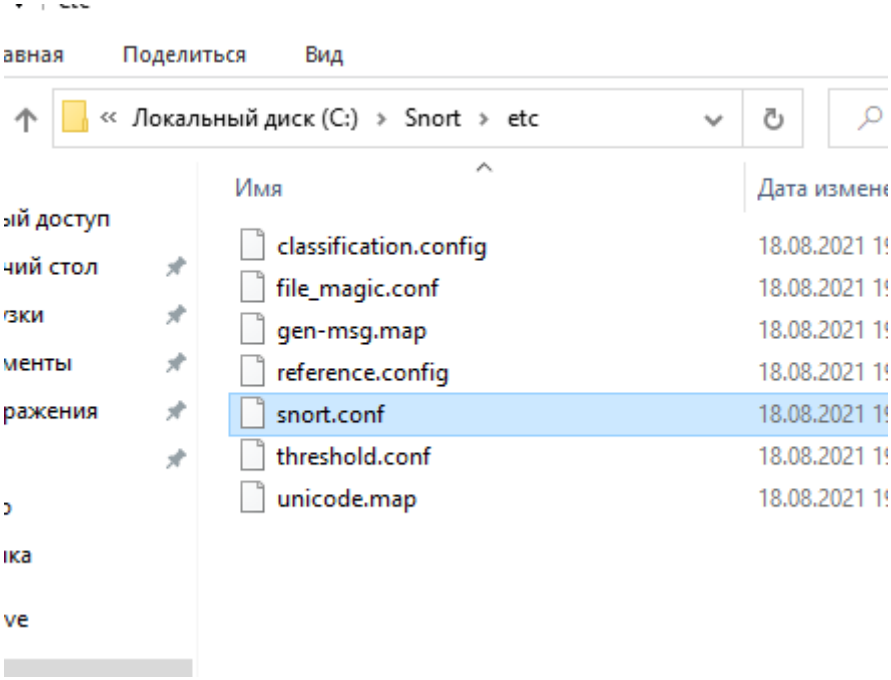

Snort
Файл
Главная
Поделиться
Вид
Локальный диск (C:) › Snort
Поиск: Snort
Имя
Дата изменения
Тип
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Видео
Музыка
OneDrive
Этот компьютер
Сеть
bin
doc
etc
lib
log
preproc_rules
rules
Uninstall.exe
05.12.2021 17:18
Элементов: 8
snortrules-snapshot-29181
Файл
Главная
Поделиться
Вид
Загрузки › snortrules-snapshot-29181
Имя
Быстрый доступ
Рабочий стол
Загрузки
etc
preproc_rules


Замена или пропуск файлов
Перемещение элементов (4) из snortrules-snapshot-29181 в Snort
В папке назначения есть файлы (3) с такими же именами
Заменить файлы в папке назначения
Пропустить эти файлы
Запрашивать для каждого файла
Подробнее
Тип
Папка с


Поделиться
Вид
Локальный диск (C:) › Snort
Поиск: Sn
доступ
й стол
нты
кения
ьютер
Имя
Дата изменения
bin 05.12.2021 17:18
doc 05.12.2021 17:18
etc 05.12.2021 17:18
lib 05.12.2021 17:18
log 05.12.2021 17:18
preproc_rules 05.12.2021 17:18
rules 05.12.2021 17:18
Uninstall.exe 05.12.2021 17:18
snortrules-snapshot-29181
Файл
Главная
Поделиться
Вид
Загрузки › snortrules-snapshot-291
Быстрый доступ
Рабочий стол
Загрузки
Документы
Имя
etc
rules
so_rules



Приступим к редакции правил. Редактировать файл с правилами будем в Notepad++:



```
C:\Users\kormi>ipconfig

Настройка протокола IP для Windows


Адаптер Ethernet Ethernet:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::f839:514c:af4c:dab0%6
   IPv4-адрес. . . . . . . . . . . . : 10.0.2.15
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . . : 10.0.2.2

C:\Users\kormi>
```

Изменениям подлежат следующие строки:

```
44  # Setup the network addresses you are protecting
45  ipvar HOME_NET 10.0.2.0/24

46
47  # Set up the external network addresses. Leave as "any" in most situations
48  ipvar EXTERNAL_NET !$HOME_NET
49
```

```
103 # such as:  c:\snort\rules
104 var RULE_PATH C:\Snort\rules
105 # var SO_RULE_PATH ../so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

```
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH C:\Snort\rules
114 var BLACK_LIST_PATH C:\Snort\rules
```

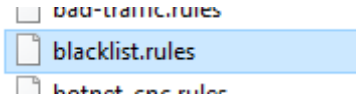
```
183
184 # Configure default log directo
185 #
186 config logdir: C:\Snort\log
```

```
246 # path to dynamic preprocessor libraries
247 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
248
249 # path to base preprocessor engine
250 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
251
252 # path to dynamic rules libraries
253 # dynamicdetection directory /usr/local/lib/snort_dynamicrules
254
```

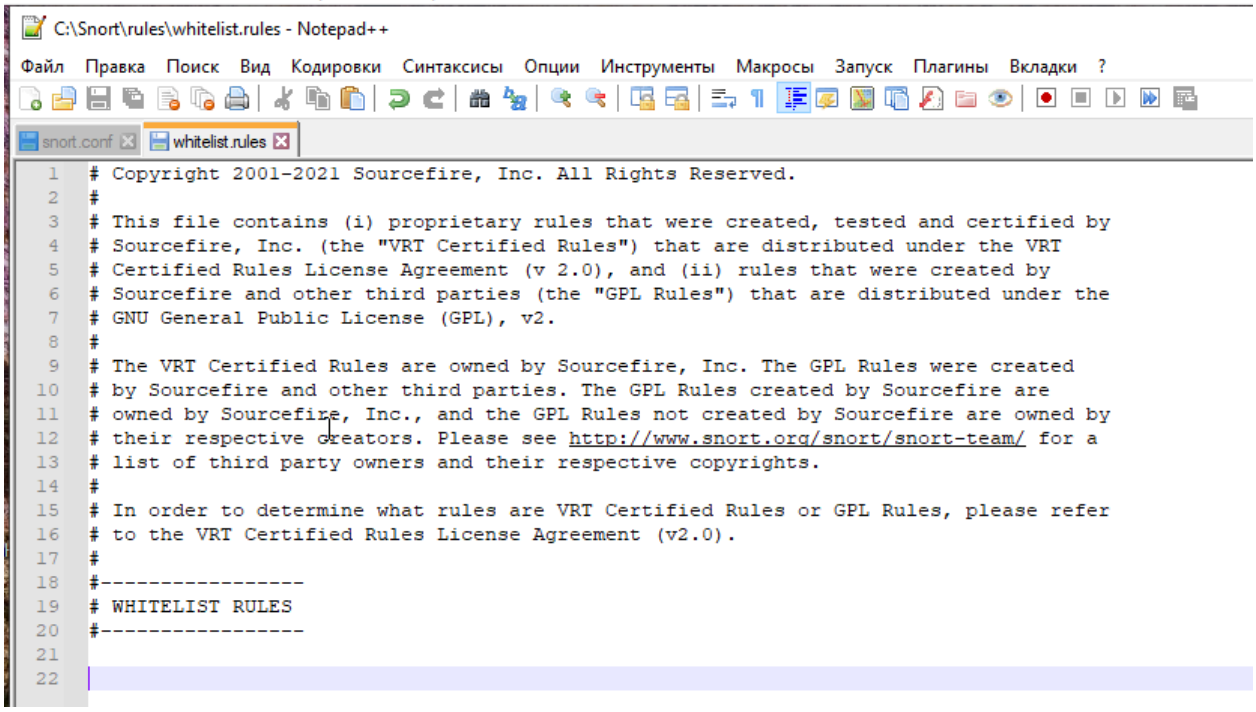
```
263  # Inline packet normalization. For more information, see README.normalize
264  # Does nothing in IDS mode
265  # preprocessor normalize_ip4
266  # preprocessor normalize_tcp: ips ecn stream
267  # preprocessor normalize_icmp4
268  # preprocessor normalize_ip6
269  # preprocessor normalize_icmp6
270
```

```
333
334  # Back Orifice detection.
335  # preprocessor bo
336
337  # FTP / Telnet normalization and ar
```

```
416
417  # Portscan detection.  For more information, see README.sfportscan
418  preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }
419
```



В папке rules присутствует только , поэтому создаем также whitelist.rules:

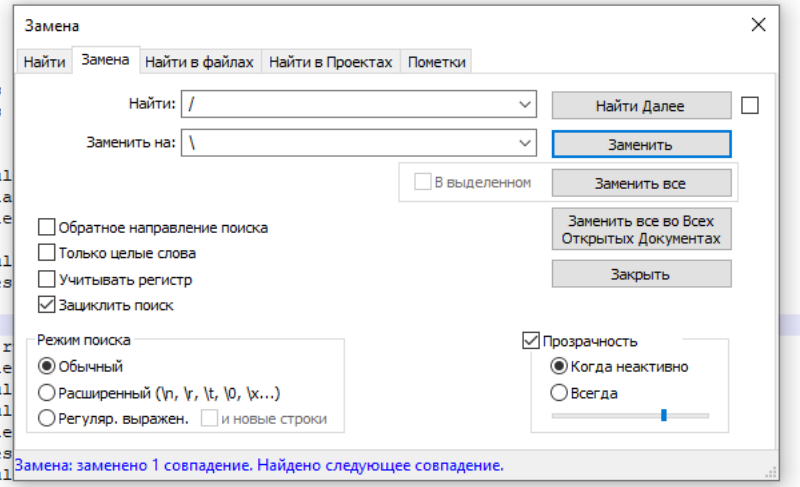



```
505
506  # Reputation preprocessor. For more information see README.reputation
507  preprocessor reputation: \
508     memcap 500, \
509     priority whitelist, \
510     nested_ip inner, \
511     whitelist $WHITE_LIST_PATH\whitelist.rules, \
512     blacklist $BLACK_LIST_PATH\blacklist.rules
513
```

Изменения с 546 по 651 строку с / на \:

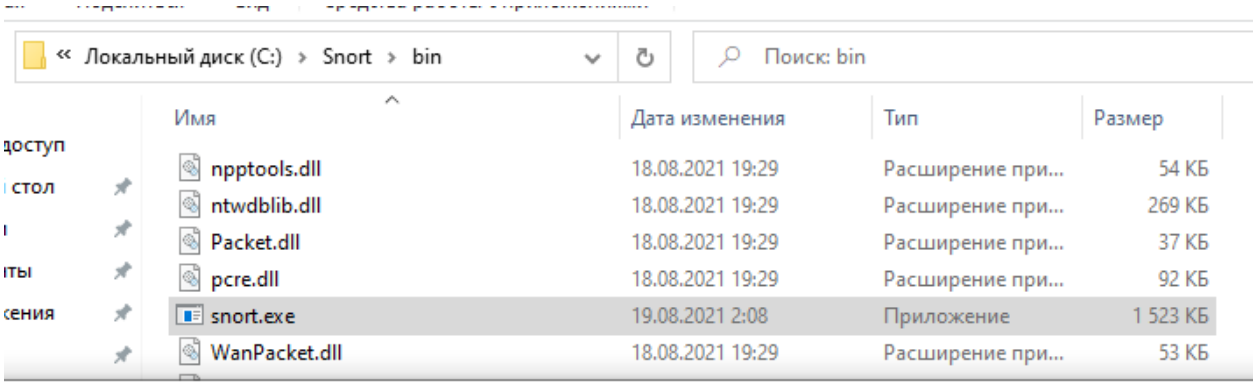
```
545  # site specific rules
546  include $RULE_PATH\local.rules
547
548  include $RULE_PATH\app-detect.rules
549  include $RULE_PATH\attack-responses.rules
550  include $RULE_PATH\backdoor.rules
551  include $RULE_PATH\bad-traffic.rules
552  include $RULE_PATH\blacklist.rules
553  include $RULE_PATH\botnet-cnc.rules
554  include $RULE_PATH\browser-chrome.rules
555  include $RULE_PATH\browser-firefox.rules
556  include $RULE_PATH\browser-ie.rules
557  include $RULE_PATH\browser-other.rules
558  include $RULE_PATH\browser-plugins.rules
559  include $RULE_PATH\browser-webkit.rules
```

```
590  include $RULE_PATH\multimedia.rules
591  include $RULE_PATH\mysql.rules
592  include $RULE_PATH\netbios.rules
593  include $RULE_PATH\nntp.rules
594  include $RULE_PATH\oracle.rules
595  include $RULE_PATH\os-linux.rules
596  include $RULE_PATH\os-other.rules
597  include $RULE_PATH\os-solaris.rules
598  include $RULE_PATH\os-windows.rules
599  include $RULE_PATH\other-ids.rules
600  include $RULE_PATH\p2p.rules
601  include $RULE_PATH\phishing-spam.rul
602  include $RULE_PATH\policy-multimedia
603  include $RULE_PATH\policy-other.rule
604  include $RULE_PATH\policy.rules
605  include $RULE_PATH\policy-social.rul
606  include $RULE_PATH\policy-spam.rules
607  include $RULE_PATH\pop2.rules
608  include $RULE_PATH/pop3.rules
609  include $RULE_PATH/protocol-finger.r
610  include $RULE_PATH/protocol-ftp.rule
611  include $RULE_PATH/protocol-icmp.rul
612  include $RULE_PATH/protocol-imap.rul
613  include $RULE_PATH/protocol-pop.rule
614  include $RULE_PATH/protocol-services
615  include $RULE_PATH/protocol-voip.rul
616  include $RULE_PATH/pua-adware.rules
617  include $RULE_PATH/pua-other.rules
```

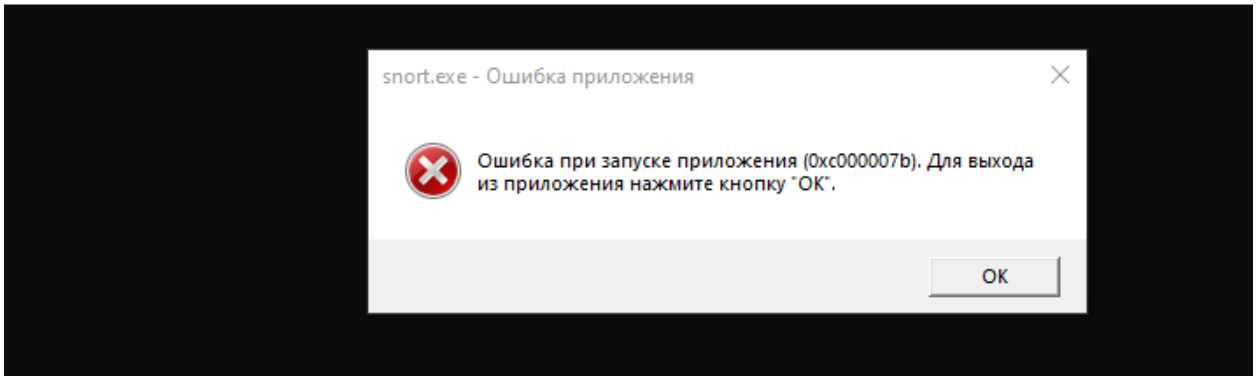


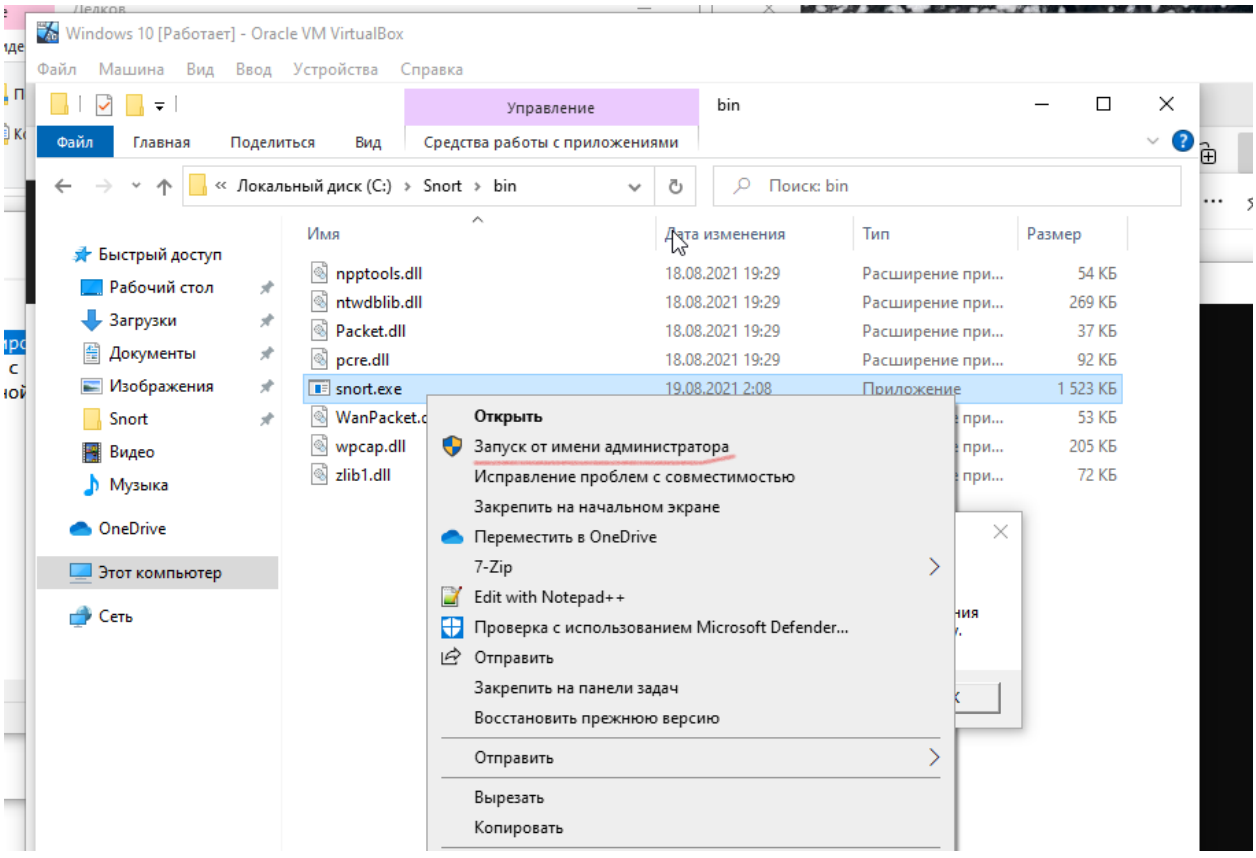

```
658  # decoder and preprocessor event rules
659  include $PREPROC_RULE_PATH/preprocessor.rules
660  include $PREPROC_RULE_PATH/decoder.rules
661  include $PREPROC_RULE_PATH/sensitive-data.rules
662
```

Сохраняем файл и запускаем Snort:

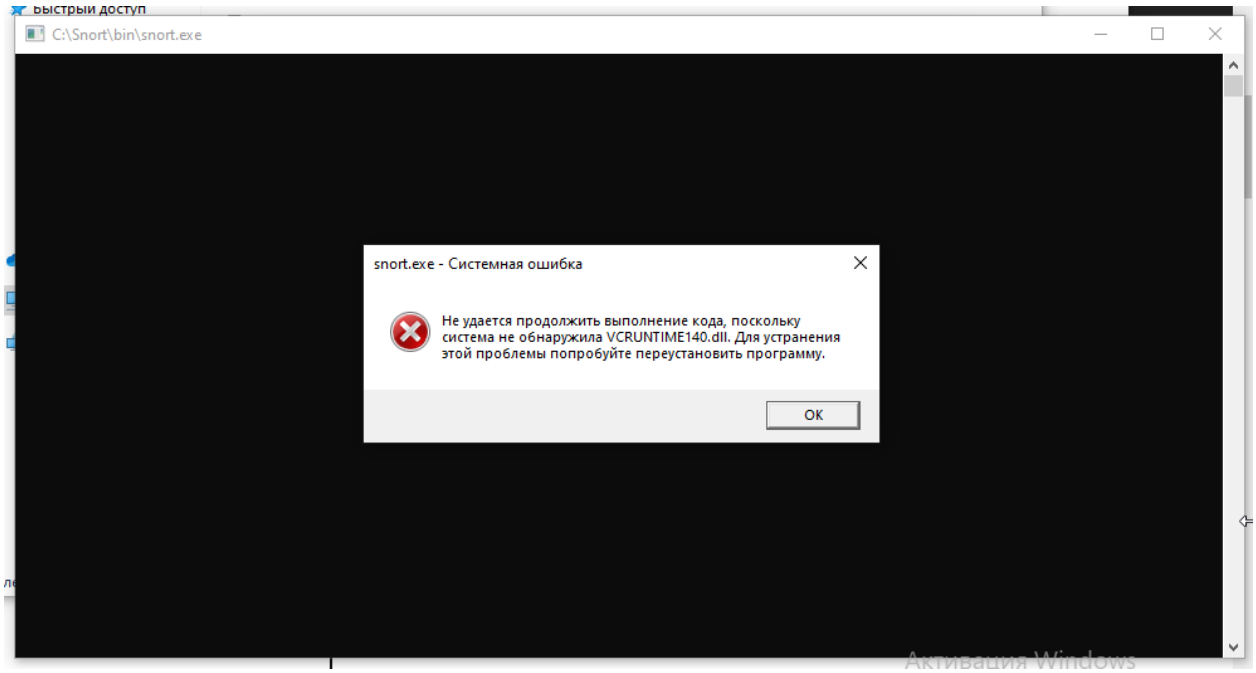


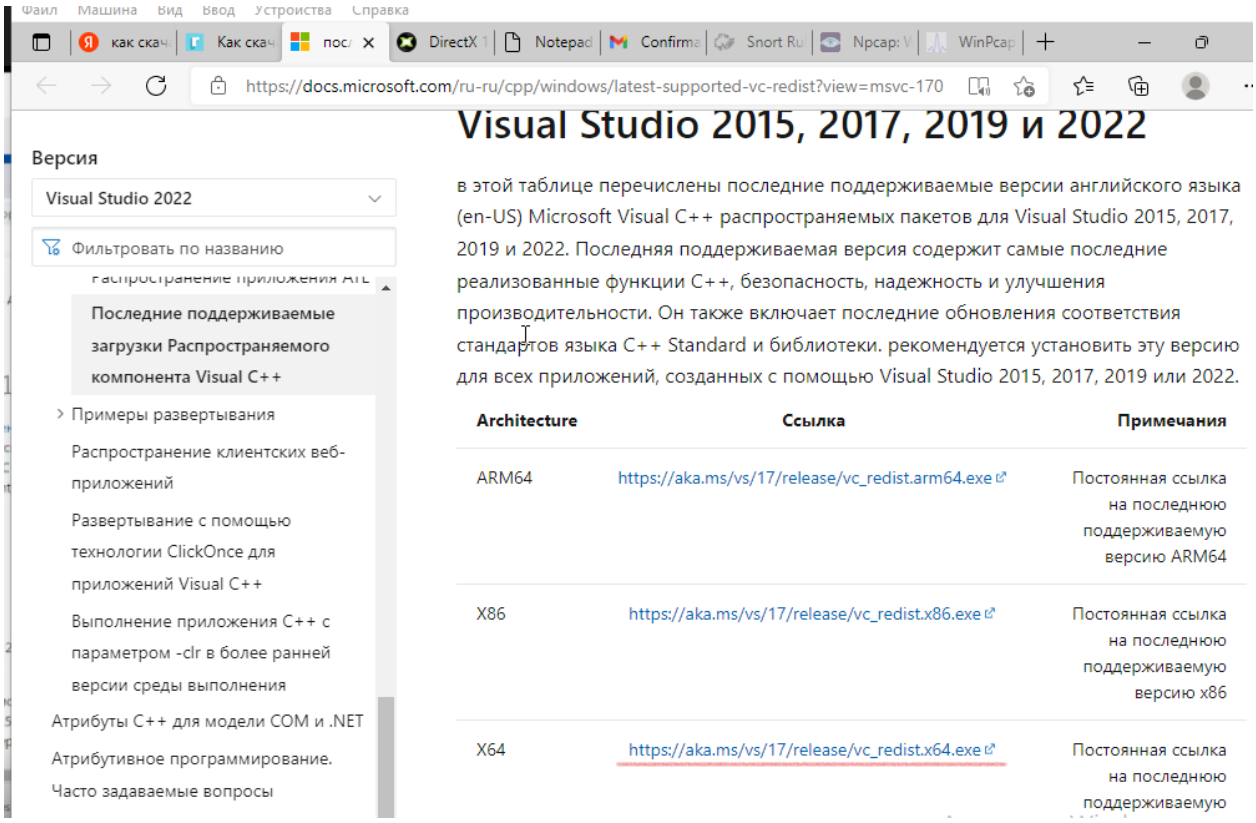
t\bin\snort.exe

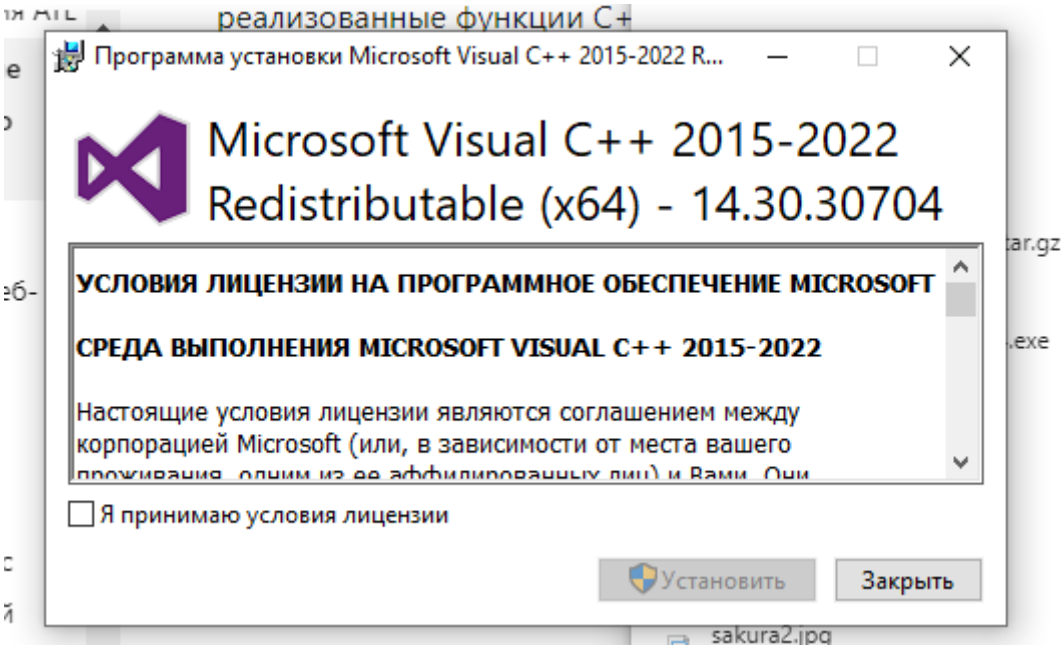




Встречаем ошибку. После попытки исправления встречаем другую ошибку:

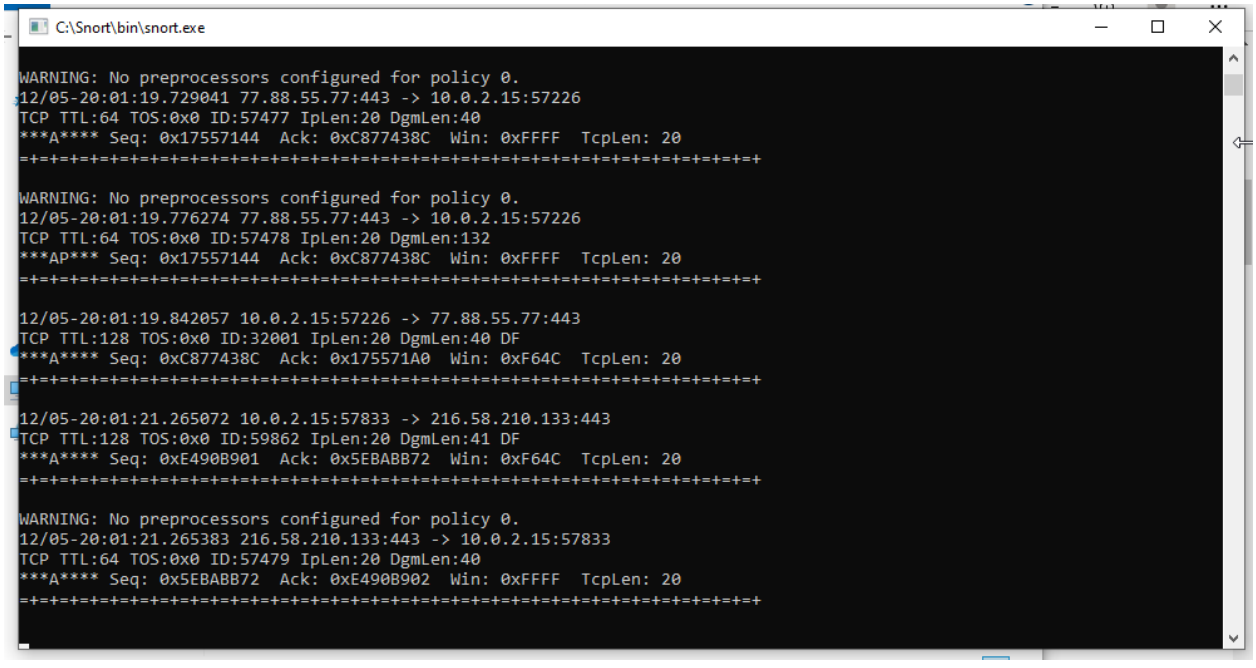

C:\Snort\bin\snort.exe
snort.exe - Системная ошибка
Не удается продолжить выполнение кода, поскольку система не обнаружила VCRUNTIME140.dll. Для устранения этой проблемы попробуйте переустановить программу.
OK


https://docs.microsoft.com/ru-ru/cpp/windows/latest-supported-vc-redist?view=msvc-170
Версия
Visual Studio 2022
Фильтровать по названию
Последние поддерживаемые загрузки Распространяемого компонента Visual C++
Примеры развертывания
Распространение клиентских веб-приложений
Развертывание с помощью технологии ClickOnce для приложений Visual C++
Выполнение приложения C++ с параметром -clr в более ранней версии среды выполнения
Атрибуты C++ для модели COM и .NET
Атрибутивное программирование.
Часто задаваемые вопросы
Visual Studio 2015, 2017, 2019 и 2022
в этой таблице перечислены последние поддерживаемые версии английского языка (en-US) Microsoft Visual C++ распространяемых пакетов для Visual Studio 2015, 2017, 2019 и 2022. Последняя поддерживаемая версия содержит самые последние реализованные функции C++, безопасность, надежность и улучшения производительности. Он также включает последние обновления соответствия стандартов языка C++ Standard и библиотеки. рекомендуется установить эту версию для всех приложений, созданных с помощью Visual Studio 2015, 2017, 2019 или 2022.
Architecture
Ссылка
Примечания
ARM64
https://aka.ms/vs/17/release/vc_redist.arm64.exe
Постоянная ссылка на последнюю поддерживаемую версию ARM64
X86
https://aka.ms/vs/17/release/vc_redist.x86.exe
Постоянная ссылка на последнюю поддерживаемую версию x86
X64
https://aka.ms/vs/17/release/vc_redist.x64.exe
Постоянная ссылка на последнюю



Запускаем программу вновь:

```
c:\Snort\bin>snort -u
snort: invalid option -- u

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18.1-WIN64 GRE (Build 1005)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

USAGE: snort [-options] <filter options>
       snort /SERVICE /INSTALL [-options] <filter options>
       snort /SERVICE /UNINSTALL
       snort /SERVICE /SHOW
Options:
        -A         Set alert mode: fast, full, console, test or none  (alert file alerts only)
        -b         Log packets in tcpdump format (much faster!)
        -B <mask>  Obfuscated IP addresses in alerts and packet dumps using CIDR mask
        -c <rules> Use Rules File <rules>
```



Посмотрим поддерживаемые интерфейсы:

```
c:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18.1-WIN64 GRE (Build 1005)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   08:00:27:B3:E2:01       0000:0000:fe80:0000:0000:0000:f839:514c \Device\NPF_{FCDA65A1-F1B2-47F7-922C-29EBEFF8BAD
5}      Intel(R) PRO/1000 MT Desktop Adapter
    2   00:00:00:00:00:00       disabled        \Device\NPF_Loopback    Adapter for loopback traffic capture

c:\Snort\bin>
```

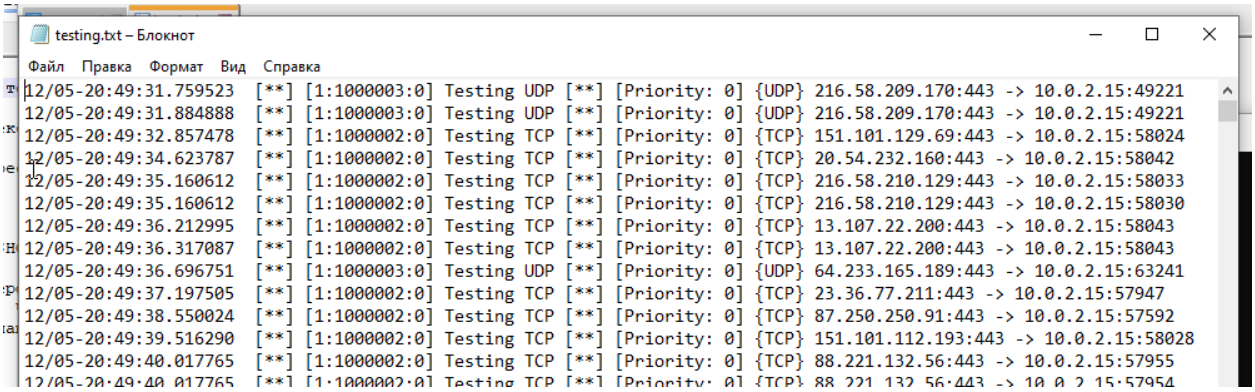
Программа запустилась без ошибок.

Проверим могут ли выводиться логи о событиях:

snort.conf | local.rules

```
1  # Copyright 2001-2021 Sourcefire, Inc. All Rights Reserved.
2  #
3  # This file contains (i) proprietary rules that were created, tested and certified by
4  # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
5  # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
6  # Sourcefire and other third parties (the "GPL Rules") that are distributed under the
7  # GNU General Public License (GPL), v2.
8  #
9  # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
10 # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
11 # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
12 # their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
13 # list of third party owners and their respective copyrights.
14 #
15 # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16 # to the VRT Certified Rules License Agreement (v2.0).
17 #
18 #-------------
19 # LOCAL RULES
20 #-------------
21 alert icmp any any -> any any (msg:"Testing ICMP"; sid:1000001; )
22 alert tcp any any -> any any (msg:"Testing TCP"; sid:1000002; )
23 alert udp any any -> any any (msg:"Testing UDP"; sid:1000003; )
24
```

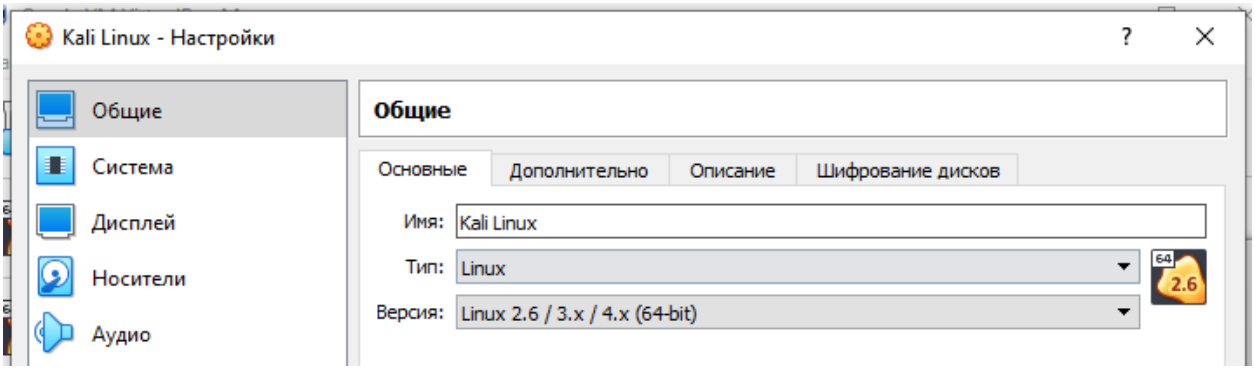
```
c:\Snort\bin>snort -i 1 -c c:\Snort\etc\snort.conf -A console > c:\Snort\log\testing.txt
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
```

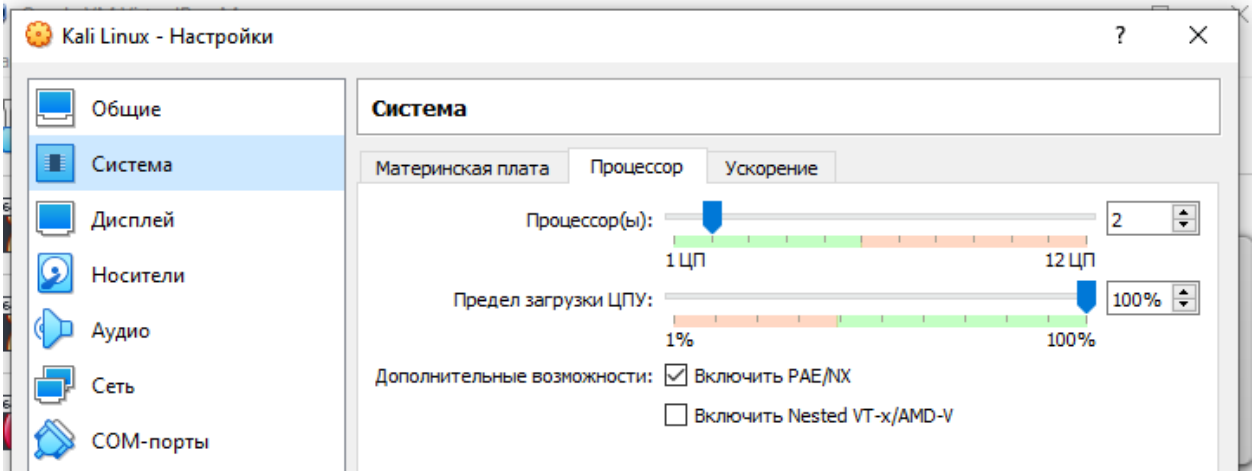


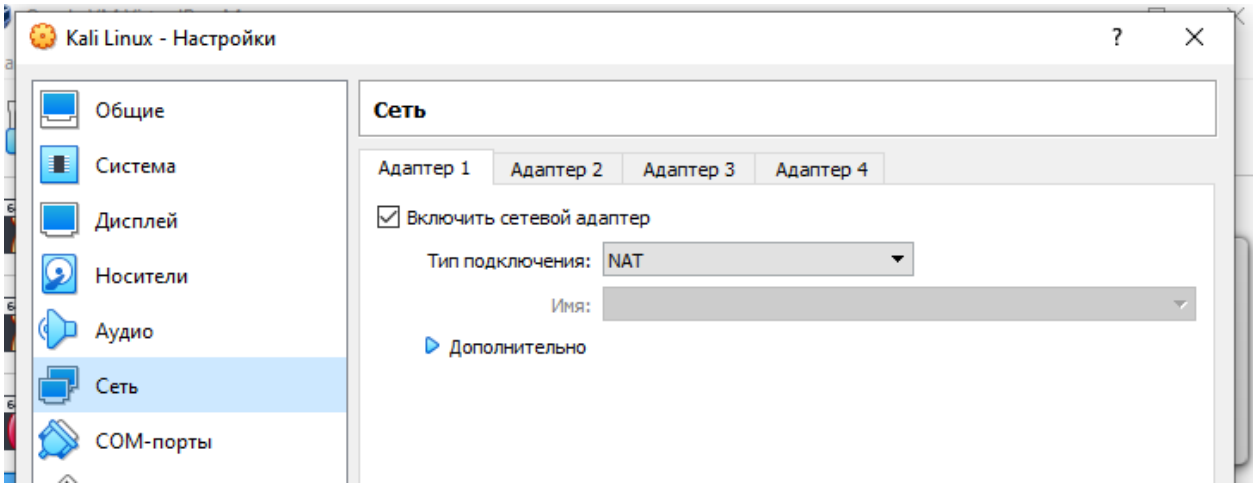
Проверка прошла успешно.

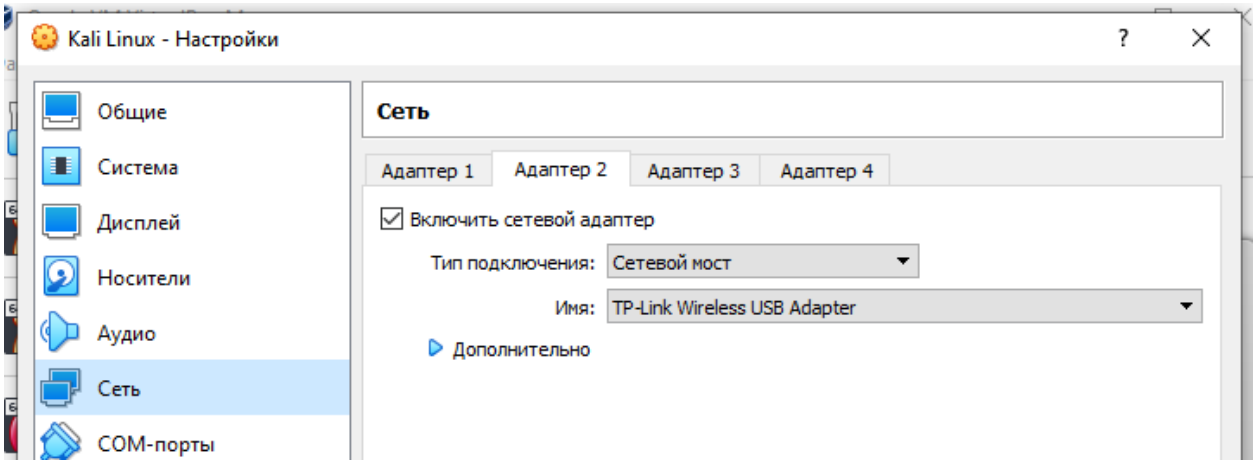
2. Установить виртуальную машину с Kali Linux

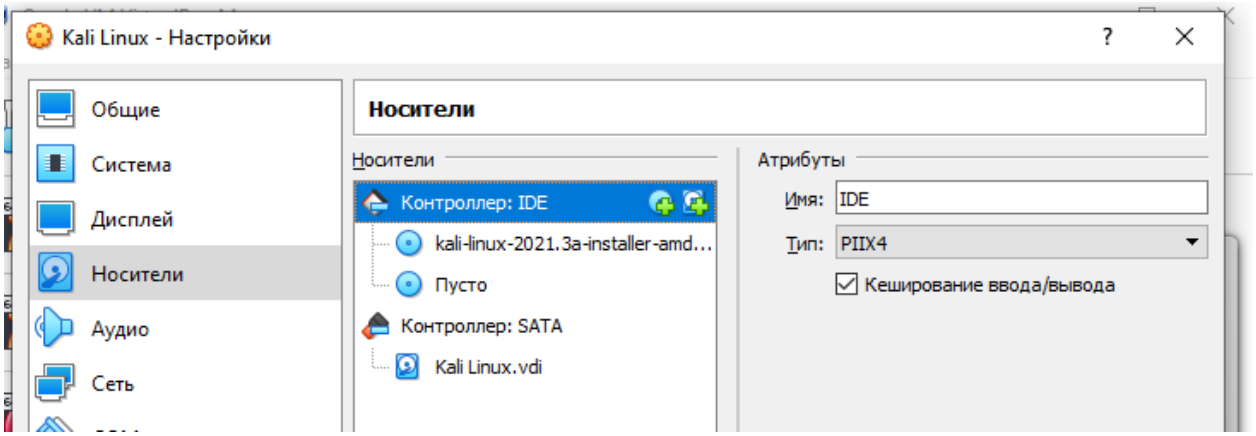
Создаем виртуальную машину со следующими настройками:

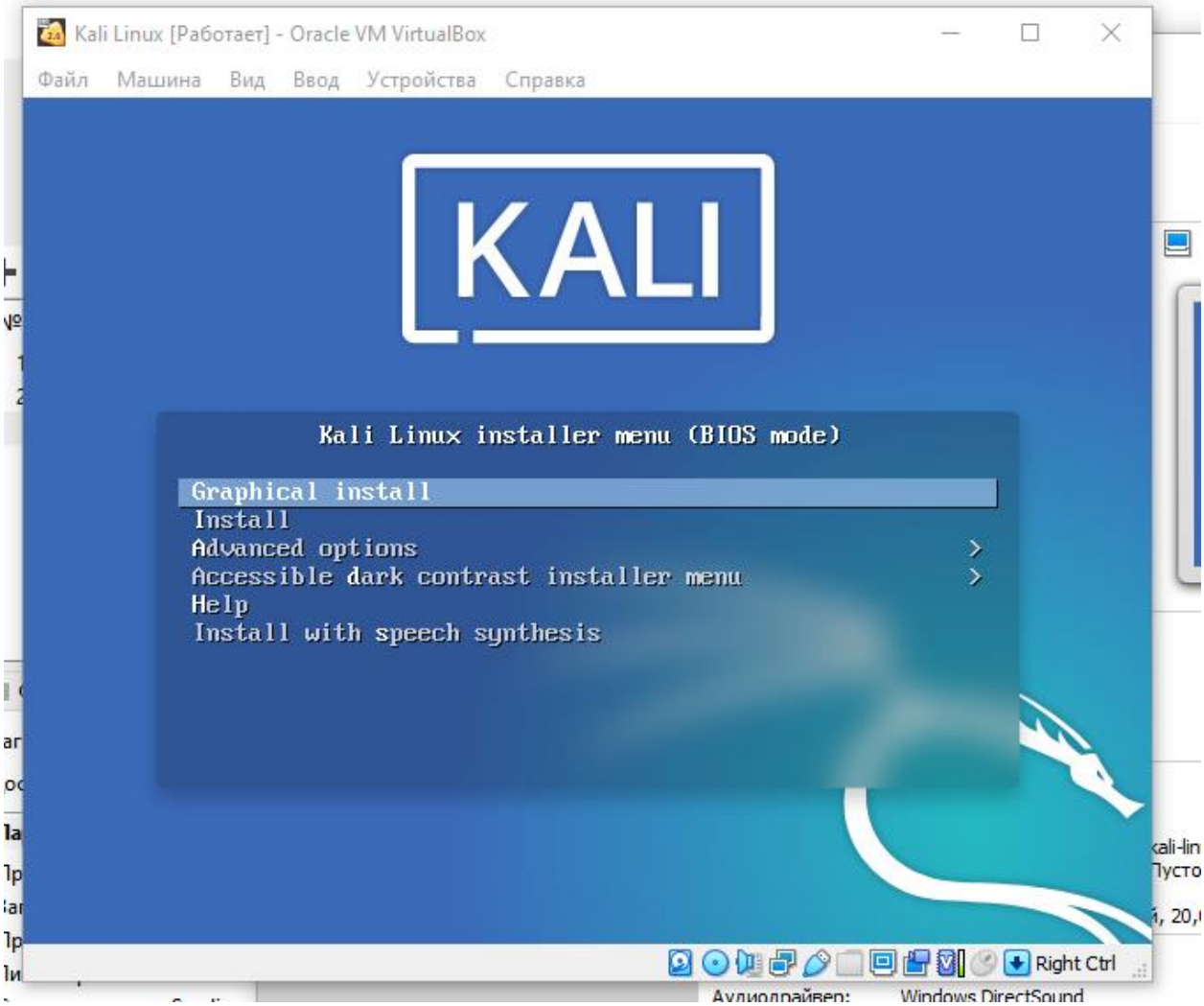


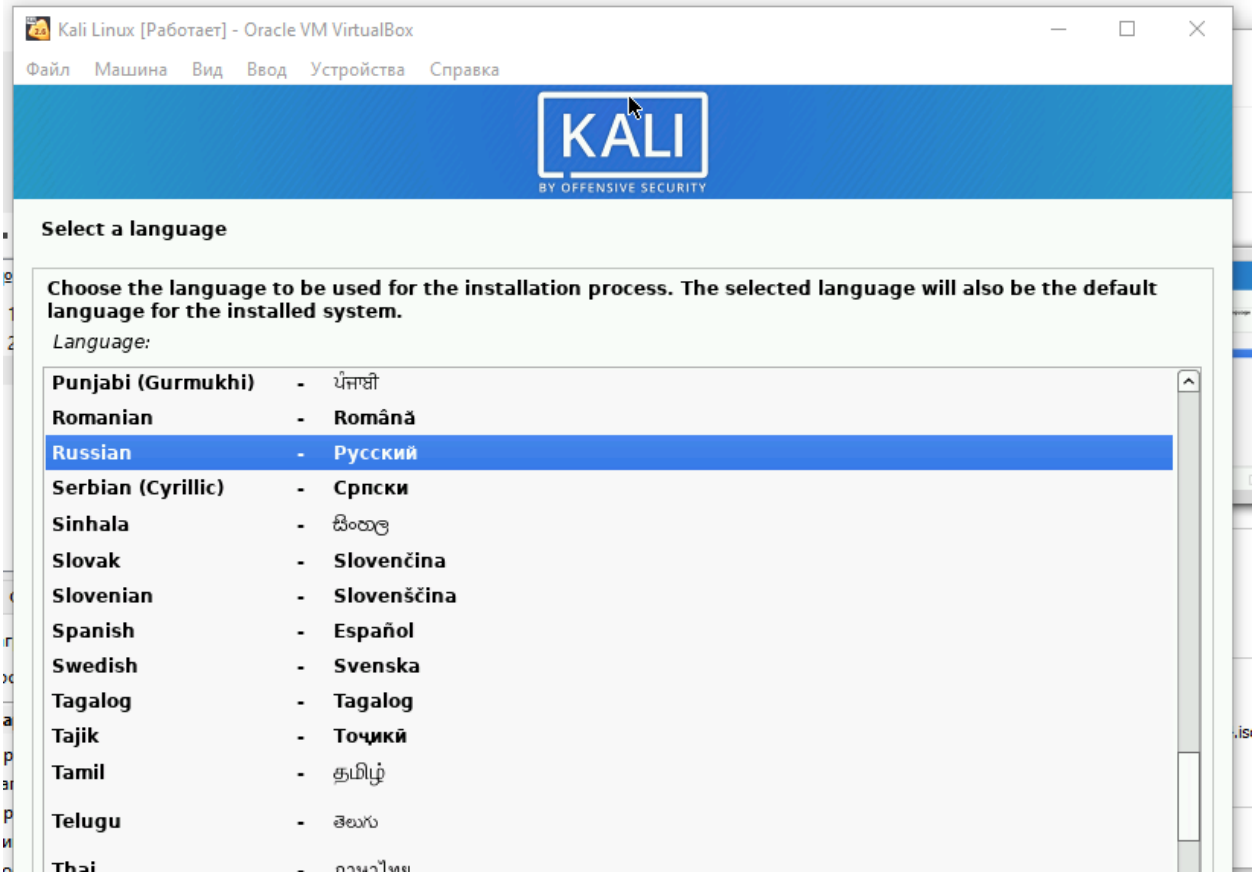


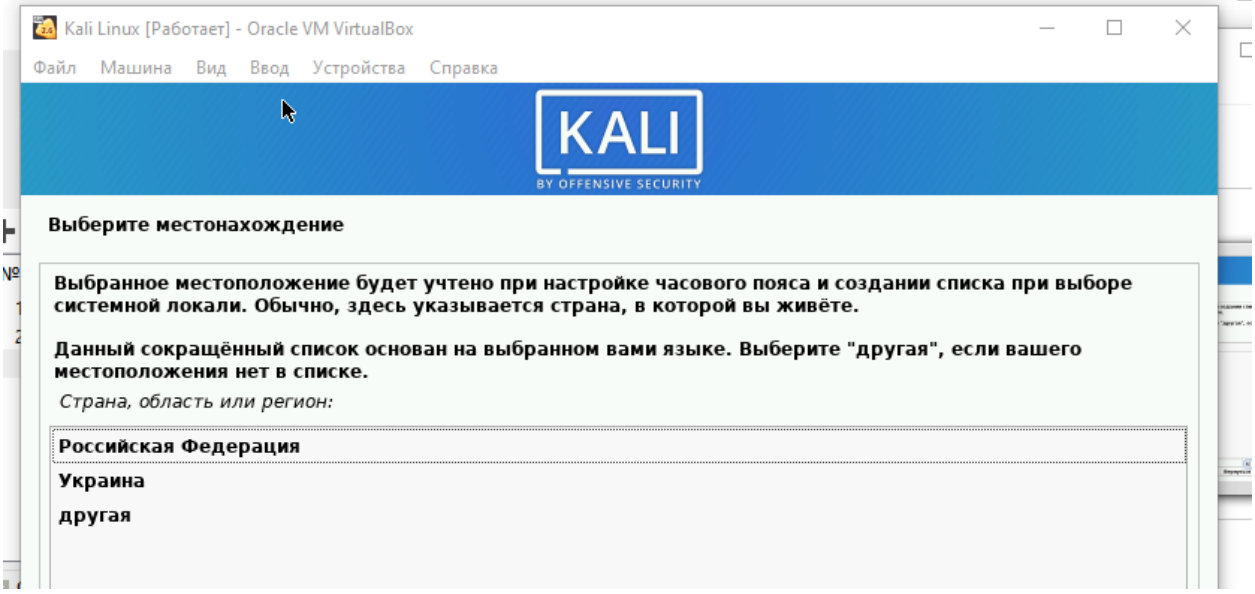

Kali Linux - Настройки
Общие
Система
Дисплей
Носители
Аудио
Сеть
COM-порты
Сеть
Адаптер 1
Адаптер 2
Адаптер 3
Адаптер 4
Включить сетевой адаптер
Тип подключения:
NAT
Имя:
Дополнительно

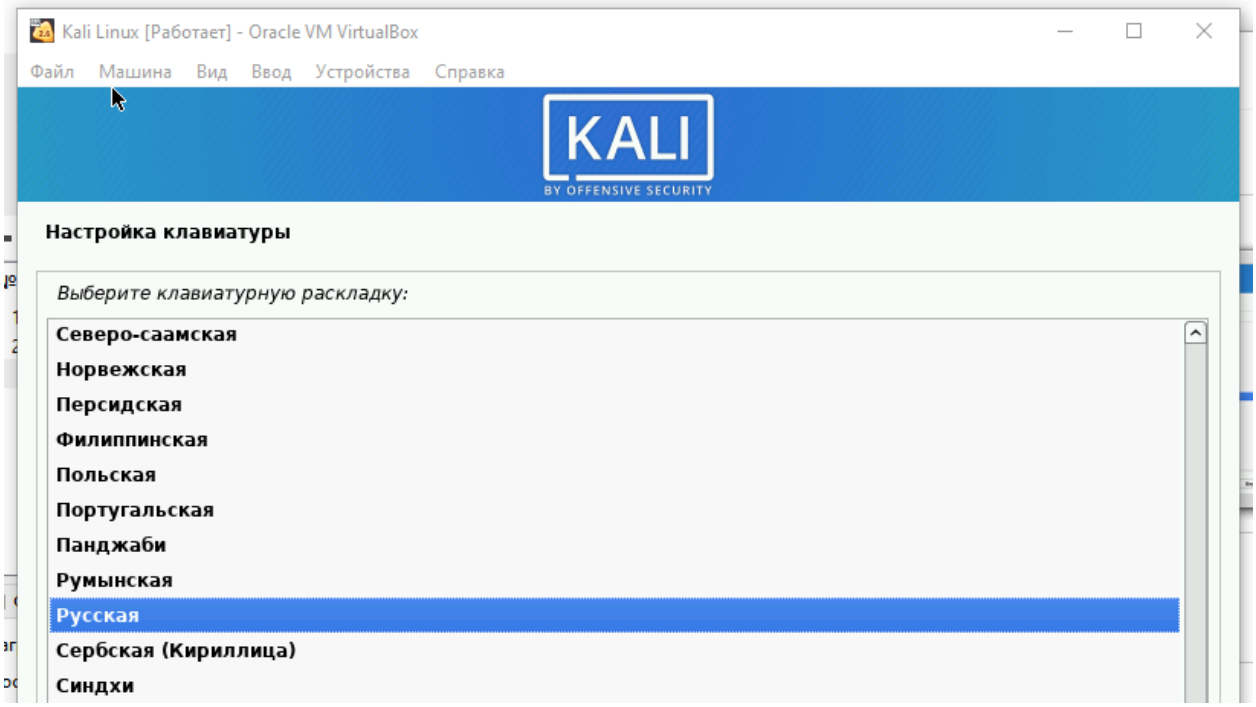

Kali Linux - Настройки
Общие
Система
Дисплей
Носители
Аудио
Сеть
COM-порты
Сеть
Адаптер 1
Адаптер 2
Адаптер 3
Адаптер 4
Включить сетевой адаптер
Тип подключения:
Сетевой мост
Имя:
TP-Link Wireless USB Adapter
Дополнительно

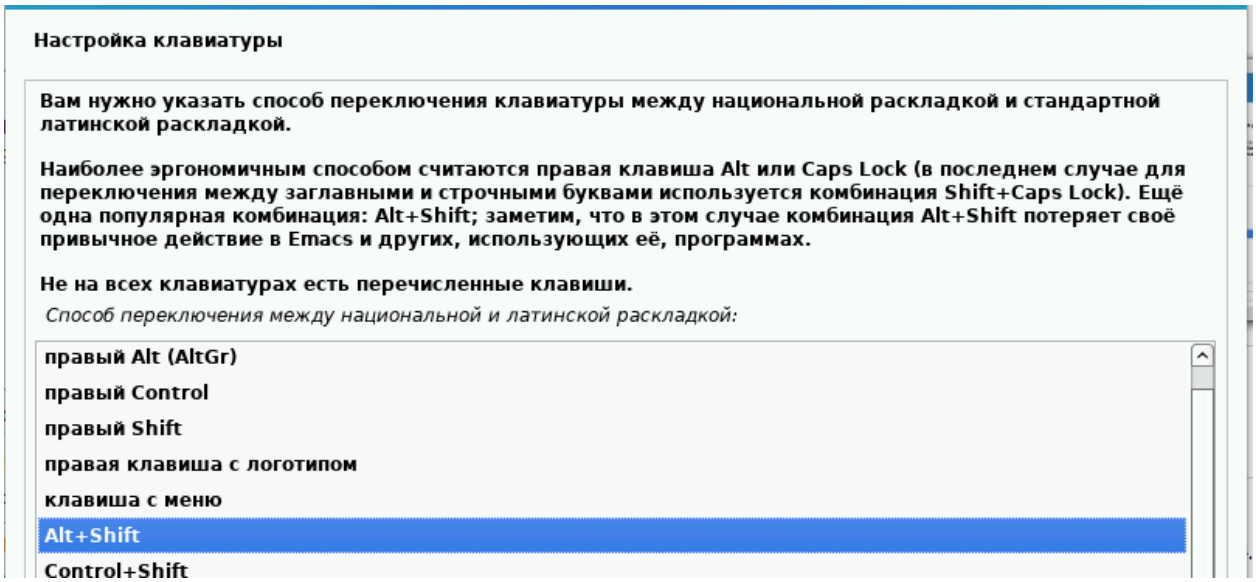

Kali Linux - Настройки
Общие
Система
Дисплей
Носители
Аудио
Сеть
Носители
Носители
Контроллер: IDE
kali-linux-2021.3a-installer-amd...
Пусто
Контроллер: SATA
Kali Linux.vdi
Атрибуты
Имя:
IDE
Тип:
PIIX4
Кеширование ввода/вывода

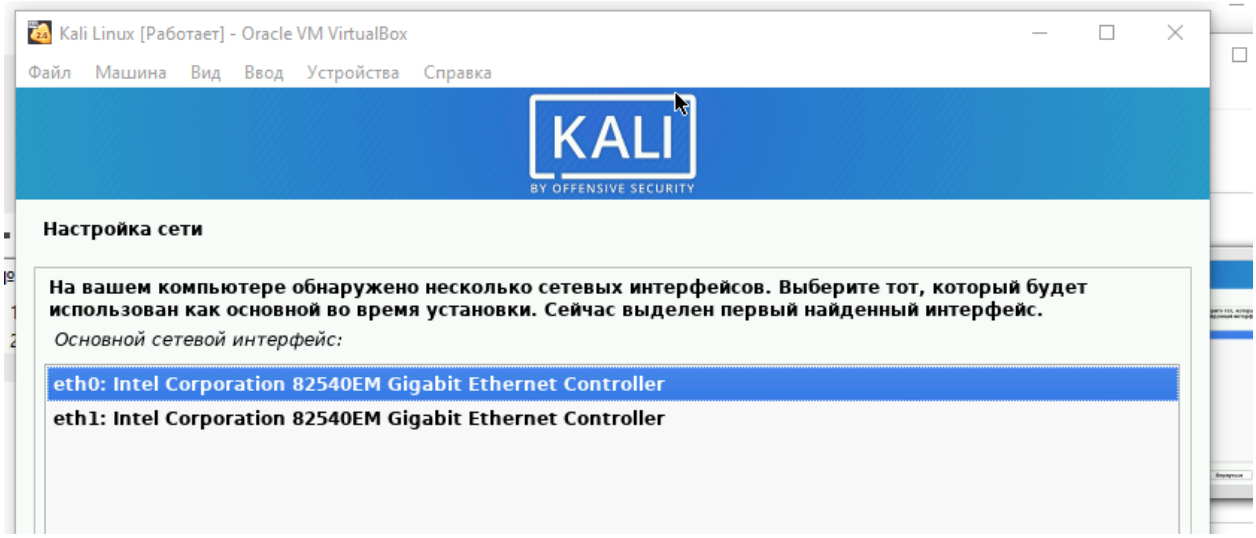

Kali Linux [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
KALI
Kali Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options
Accessible dark contrast installer menu
Help
Install with speech synthesis
Right Ctrl

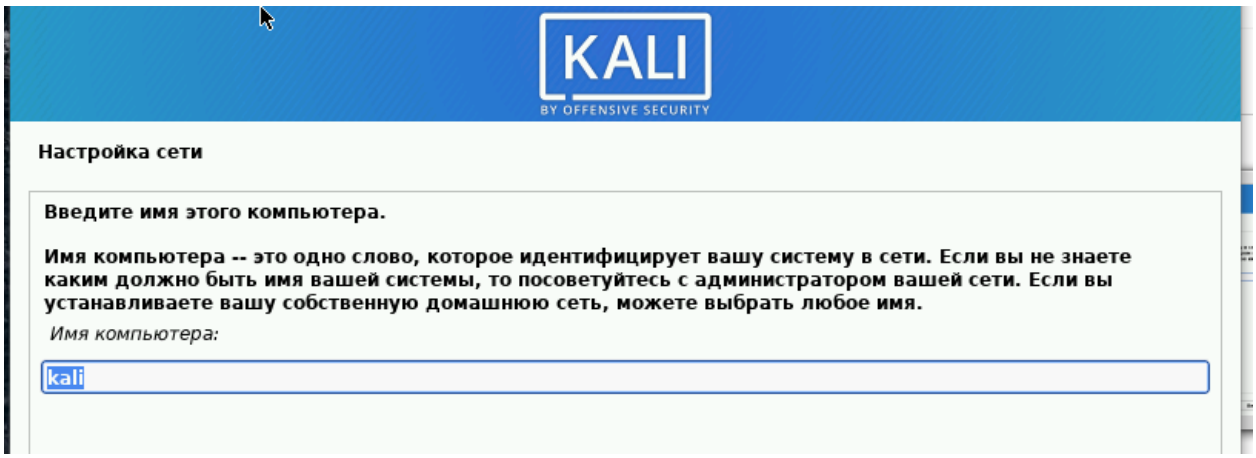

Kali Linux [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
KALI
BY OFFENSIVE SECURITY
Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
Punjabi (Gurmukhi) - ਪੰਜਾਬੀ
Romanian - Română
Russian - Русский
Serbian (Cyrillic) - Српски
Sinhala - සිංහල
Slovak - Slovenčina
Slovenian - Slovenščina
Spanish - Español
Swedish - Svenska
Tagalog - Tagalog
Tajik - Тоҷикӣ
Tamil - தமிழ்
Telugu - తెలుగు
Thai

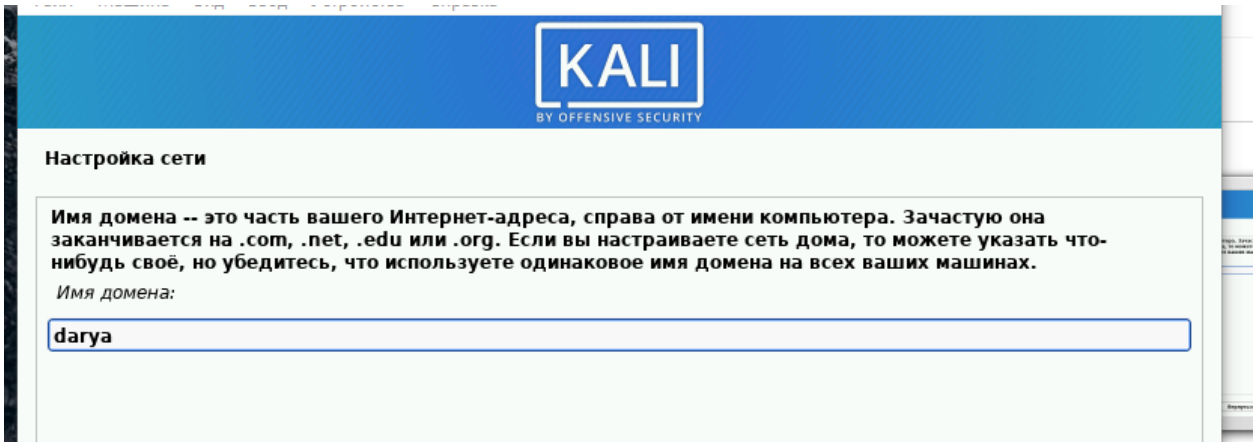

Kali Linux [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
KALI
BY OFFENSIVE SECURITY
Выберите местонахождение
Выбранное местоположение будет учтено при настройке часового пояса и создании списка при выборе системной локали. Обычно, здесь указывается страна, в которой вы живёте.
Данный сокращённый список основан на выбранном вами языке. Выберите "другая", если вашего местоположения нет в списке.
Страна, область или регион:
Российская Федерация
Украина
другая

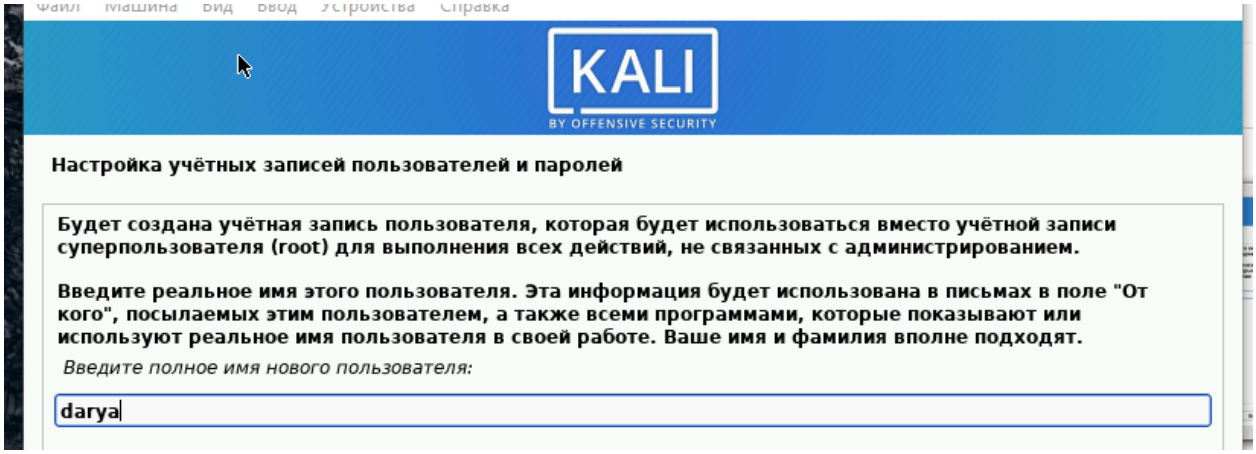

Kali Linux [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
KALI
BY OFFENSIVE SECURITY
Настройка клавиатуры
Выберите клавиатурную раскладку:
Северо-саамская
Норвежская
Персидская
Филиппинская
Польская
Португальская
Панджаби
Румынская
Русская
Сербская (Кириллица)
Синдхи

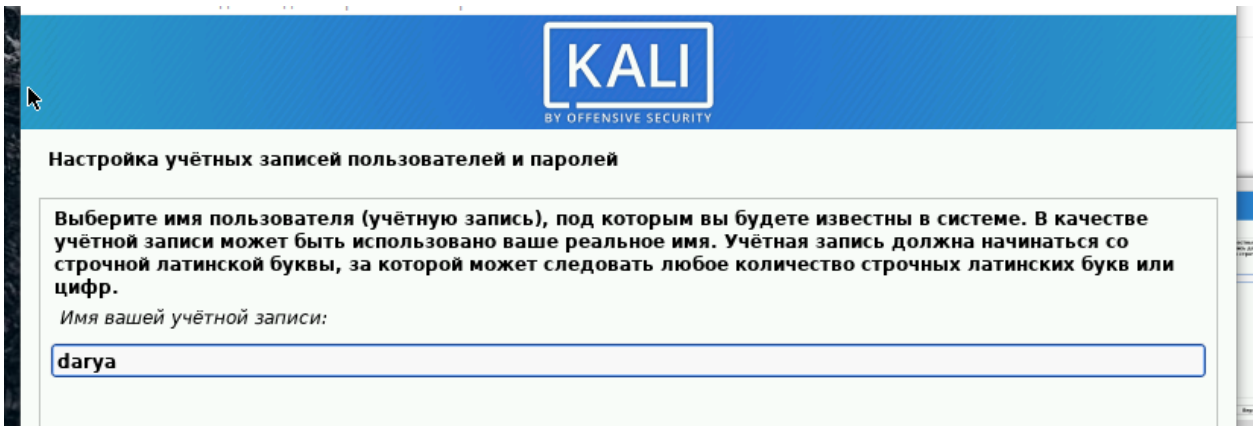

Настройка клавиатуры
Вам нужно указать способ переключения клавиатуры между национальной раскладкой и стандартной латинской раскладкой.
Наиболее эргономичным способом считаются правая клавиша Alt или Caps Lock (в последнем случае для переключения между заглавными и строчными буквами используется комбинация Shift+Caps Lock). Ещё одна популярная комбинация: Alt+Shift; заметим, что в этом случае комбинация Alt+Shift потеряет своё привычное действие в Emacs и других, использующих её, программах.
Не на всех клавиатурах есть перечисленные клавиши.
Способ переключения между национальной и латинской раскладкой:
правый Alt (AltGr)
правый Control
правый Shift
правая клавиша с логотипом
клавиша с меню
Alt+Shift
Control+Shift

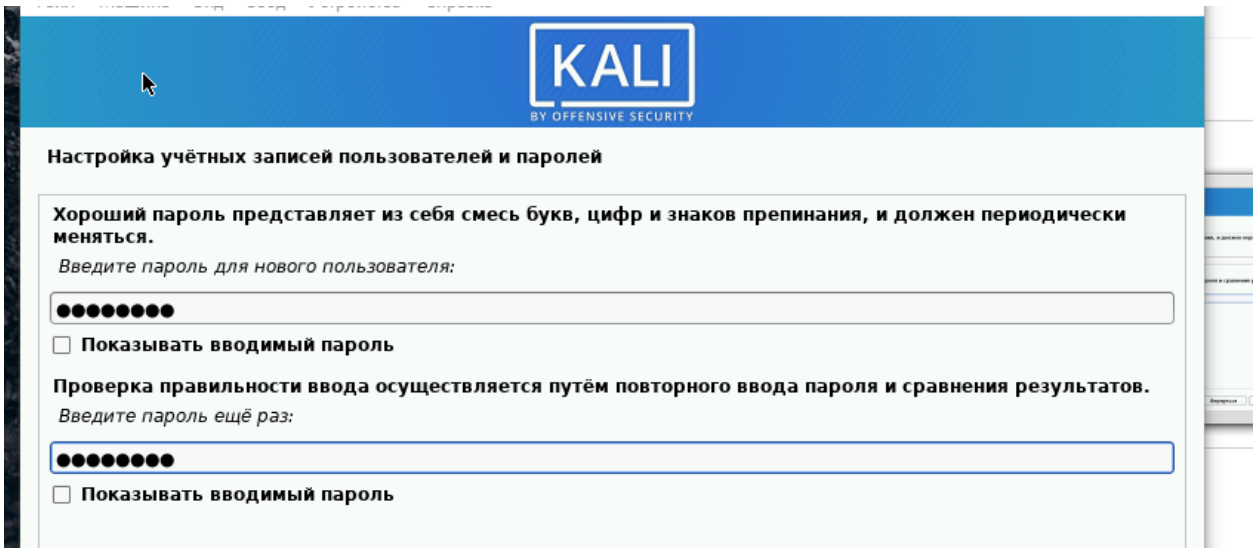

Kali Linux [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
KALI
BY OFFENSIVE SECURITY
Настройка сети
На вашем компьютере обнаружено несколько сетевых интерфейсов. Выберите тот, который будет использован как основной во время установки. Сейчас выделен первый найденный интерфейс.
Основной сетевой интерфейс:
eth0: Intel Corporation 82540EM Gigabit Ethernet Controller
eth1: Intel Corporation 82540EM Gigabit Ethernet Controller

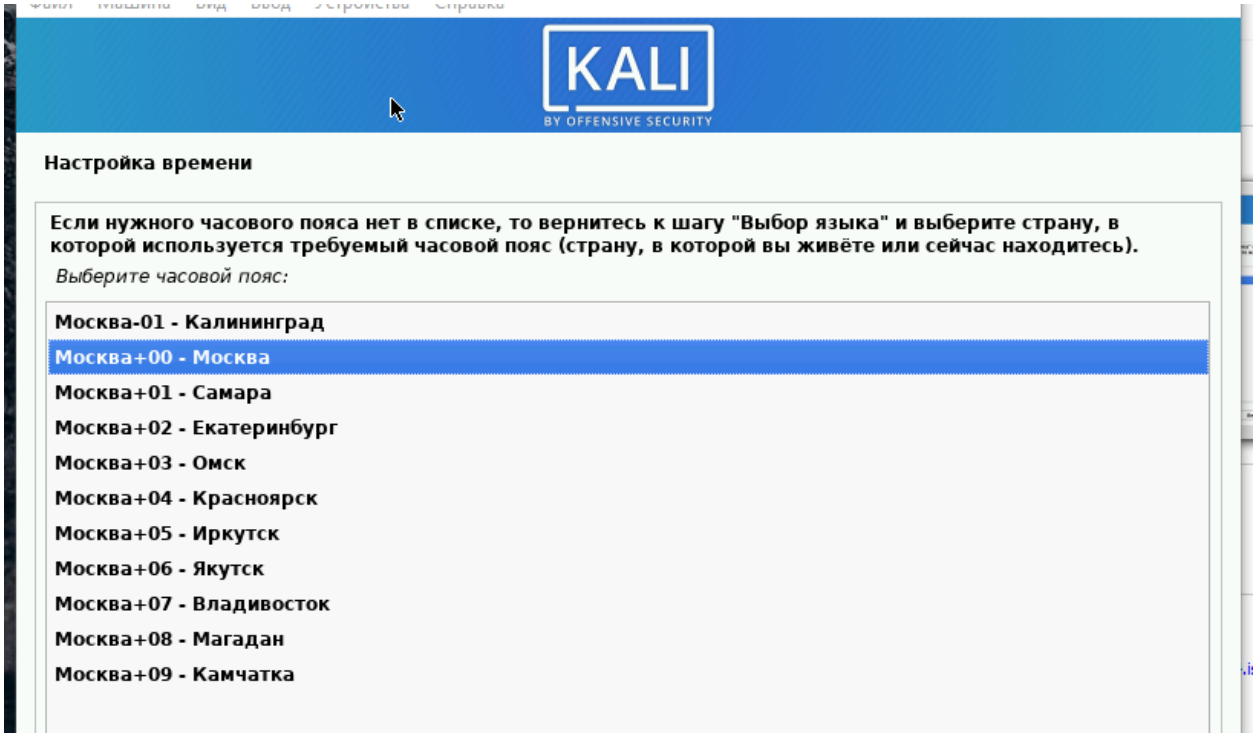

KALI
BY OFFENSIVE SECURITY
Настройка сети
Введите имя этого компьютера.
Имя компьютера -- это одно слово, которое идентифицирует вашу систему в сети. Если вы не знаете каким должно быть имя вашей системы, то посоветуйтесь с администратором вашей сети. Если вы устанавливаете вашу собственную домашнюю сеть, можете выбрать любое имя.
Имя компьютера:
kali

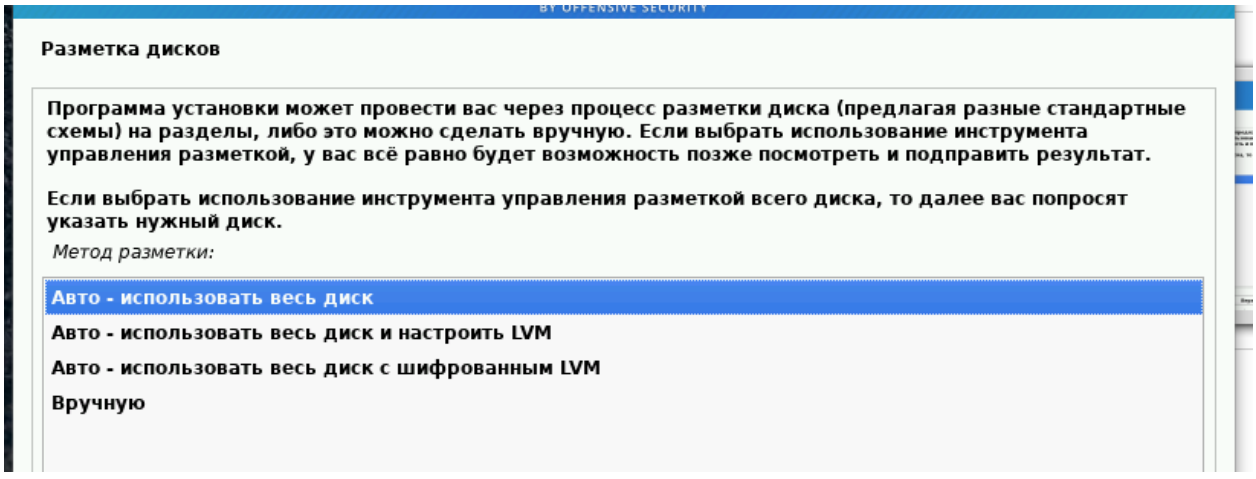

KALI
BY OFFENSIVE SECURITY
Настройка сети
Имя домена -- это часть вашего Интернет-адреса, справа от имени компьютера. Зачастую она заканчивается на .com, .net, .edu или .org. Если вы настраиваете сеть дома, то можете указать что-нибудь своё, но убедитесь, что используете одинаковое имя домена на всех ваших машинах.
Имя домена:
darya

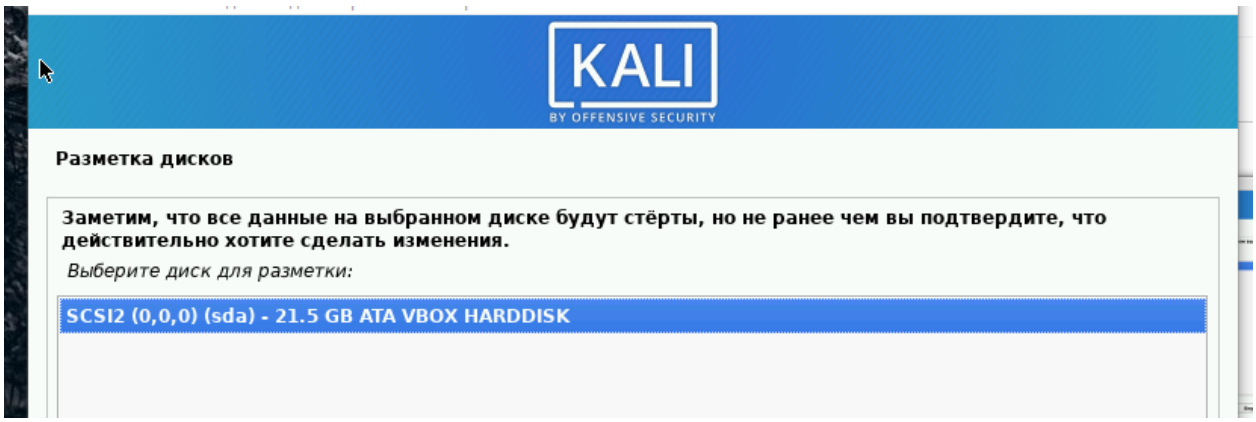

KALI
BY OFFENSIVE SECURITY
Настройка учётных записей пользователей и паролей
Будет создана учётная запись пользователя, которая будет использоваться вместо учётной записи суперпользователя (root) для выполнения всех действий, не связанных с администрированием.
Введите реальное имя этого пользователя. Эта информация будет использована в письмах в поле "От кого", посылаемых этим пользователем, а также всеми программами, которые показывают или используют реальное имя пользователя в своей работе. Ваше имя и фамилия вполне подходят.
Введите полное имя нового пользователя:
darya

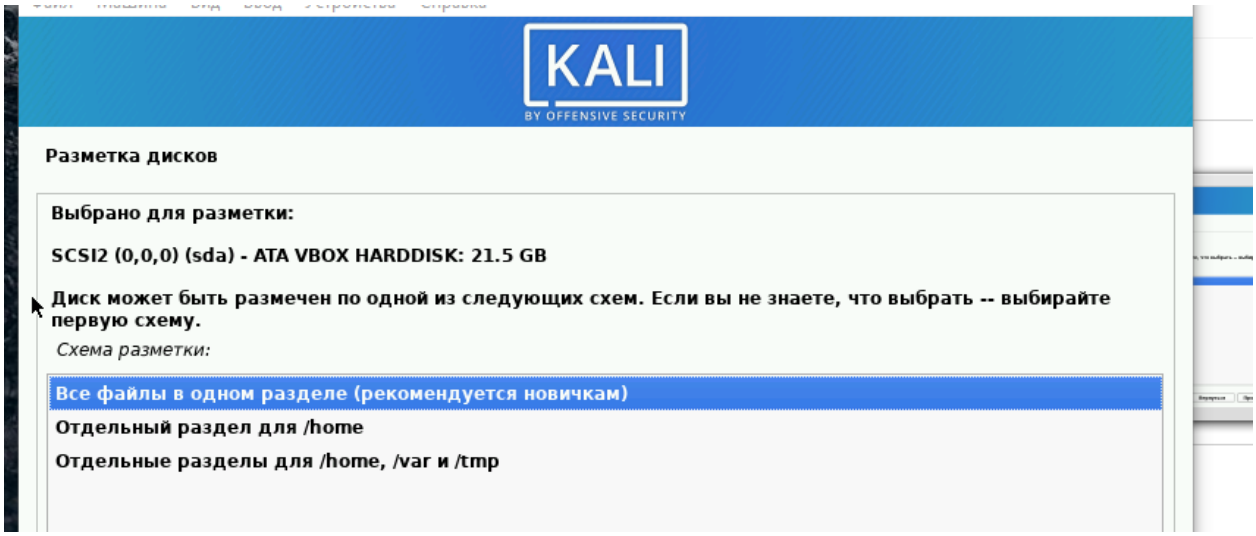

KALI
BY OFFENSIVE SECURITY
Настройка учётных записей пользователей и паролей
Выберите имя пользователя (учётную запись), под которым вы будете известны в системе. В качестве учётной записи может быть использовано ваше реальное имя. Учётная запись должна начинаться со строчной латинской буквы, за которой может следовать любое количество строчных латинских букв или цифр.
Имя вашей учётной записи:
darya

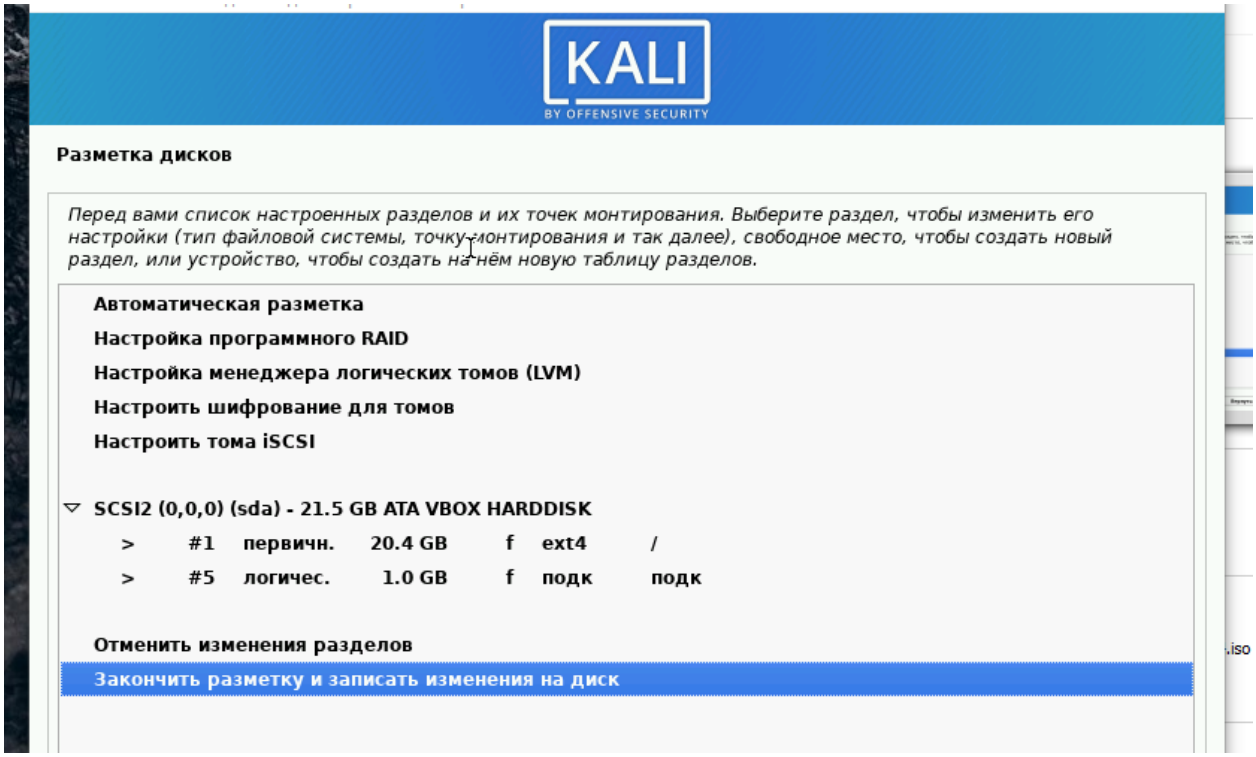

KALI
BY OFFENSIVE SECURITY
Настройка учётных записей пользователей и паролей
Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.
Введите пароль для нового пользователя:
Показывать вводимый пароль
Проверка правильности ввода осуществляется путём повторного ввода пароля и сравнения результатов.
Введите пароль ещё раз:
Показывать вводимый пароль

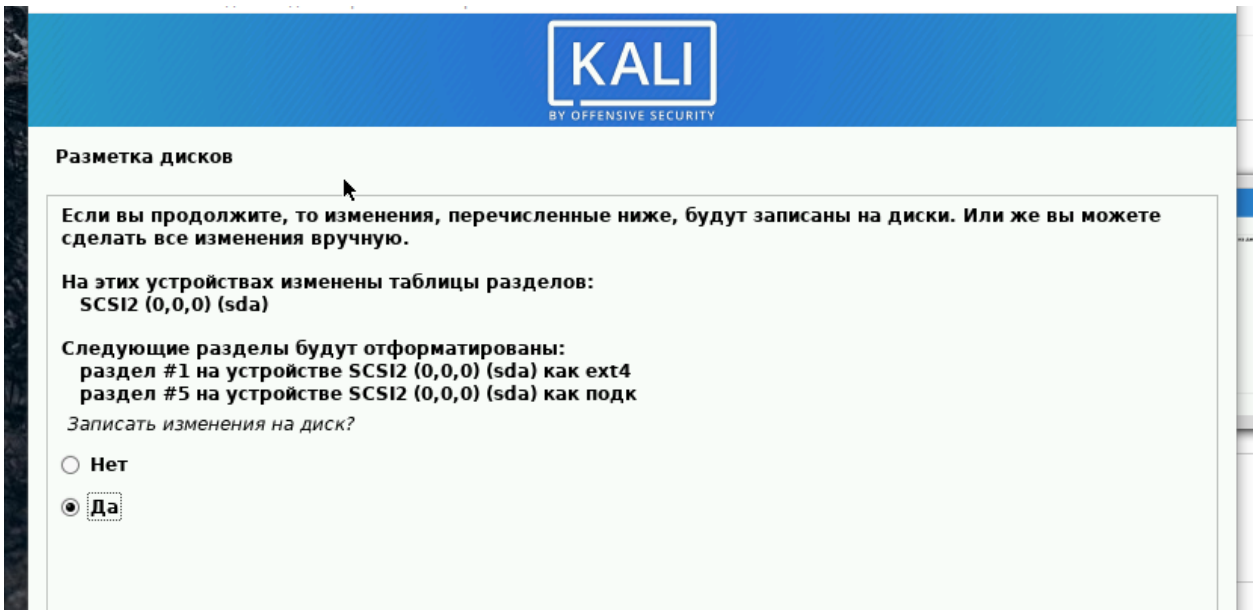

KALI
BY OFFENSIVE SECURITY
Настройка времени
Если нужного часового пояса нет в списке, то вернитесь к шагу "Выбор языка" и выберите страну, в которой используется требуемый часовой пояс (страну, в которой вы живёте или сейчас находитесь).
Выберите часовой пояс:
Москва-01 - Калининград
Москва+00 - Москва
Москва+01 - Самара
Москва+02 - Екатеринбург
Москва+03 - Омск
Москва+04 - Красноярск
Москва+05 - Иркутск
Москва+06 - Якутск
Москва+07 - Владивосток
Москва+08 - Магадан
Москва+09 - Камчатка

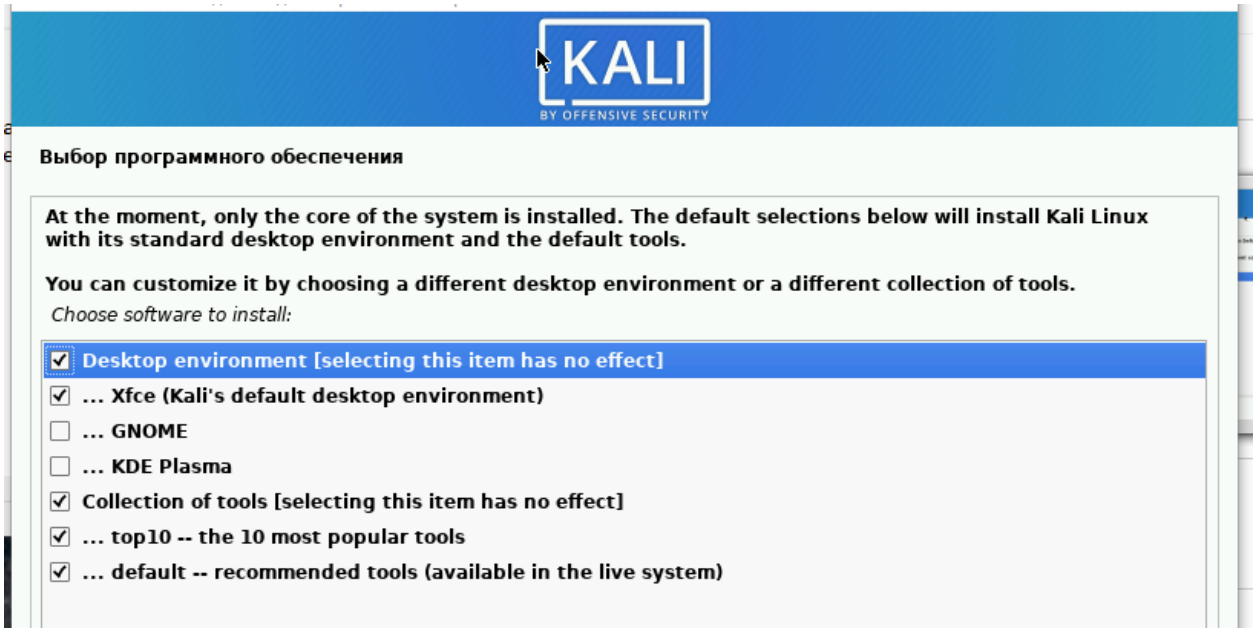

BY OFFENSIVE SECURITY
Разметка дисков
Программа установки может провести вас через процесс разметки диска (предлагая разные стандартные схемы) на разделы, либо это можно сделать вручную. Если выбрать использование инструмента управления разметкой, у вас всё равно будет возможность позже посмотреть и подправить результат.
Если выбрать использование инструмента управления разметкой всего диска, то далее вас попросят указать нужный диск.
Метод разметки:
Авто - использовать весь диск
Авто - использовать весь диск и настроить LVM
Авто - использовать весь диск с шифрованным LVM
Вручную

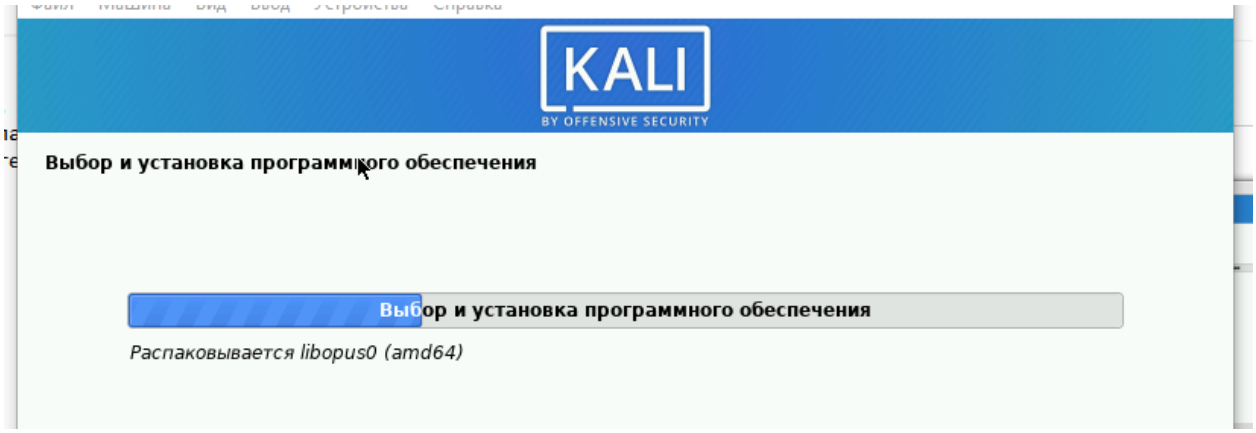

KALI
BY OFFENSIVE SECURITY
Разметка дисков
Заметим, что все данные на выбранном диске будут стёрты, но не ранее чем вы подтвердите, что действительно хотите сделать изменения.
Выберите диск для разметки:
SCSI2 (0,0,0) (sda) - 21.5 GB ATA VBOX HARDDISK

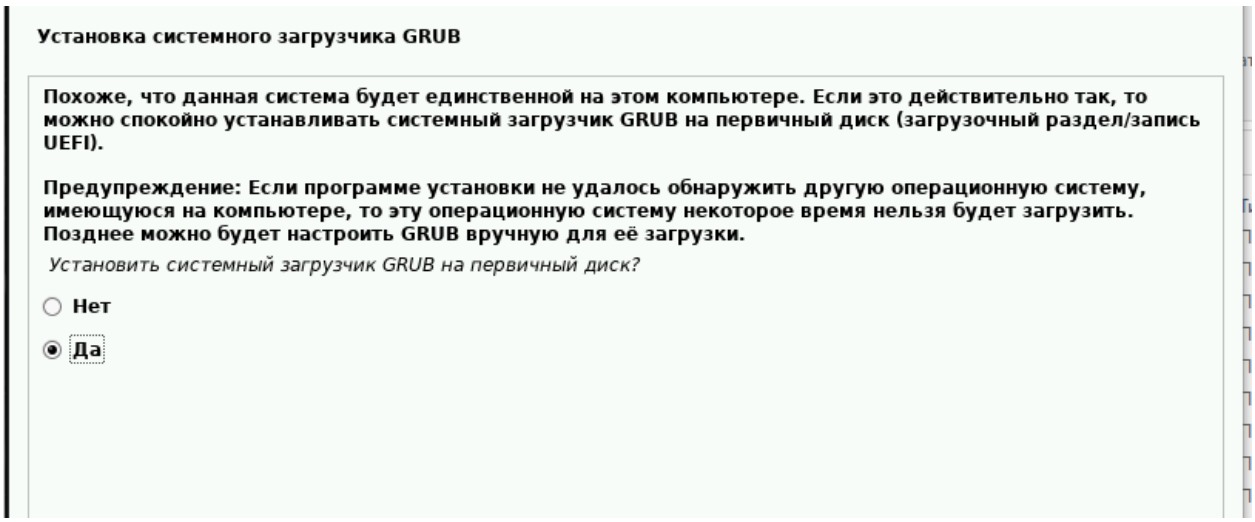

KALI
BY OFFENSIVE SECURITY
Разметка дисков
Выбрано для разметки:
SCSI2 (0,0,0) (sda) - ATA VBOX HARDDISK: 21.5 GB
Диск может быть размечен по одной из следующих схем. Если вы не знаете, что выбрать -- выбирайте первую схему.
Схема разметки:
Все файлы в одном разделе (рекомендуется новичкам)
Отдельный раздел для /home
Отдельные разделы для /home, /var и /tmp

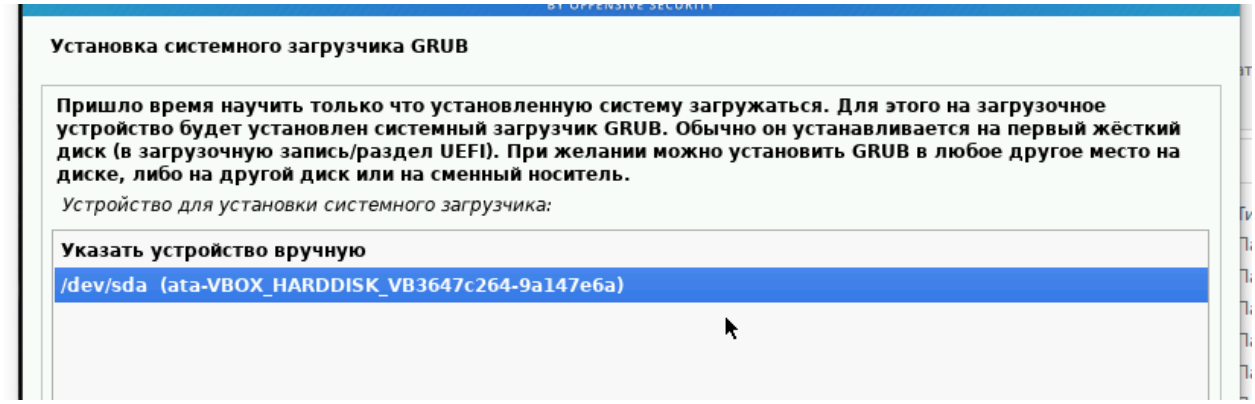

KALI
BY OFFENSIVE SECURITY
Разметка дисков
Перед вами список настроенных разделов и их точек монтирования. Выберите раздел, чтобы изменить его настройки (тип файловой системы, точку монтирования и так далее), свободное место, чтобы создать новый раздел, или устройство, чтобы создать на нём новую таблицу разделов.
Автоматическая разметка
Настройка программного RAID
Настройка менеджера логических томов (LVM)
Настроить шифрование для томов
Настроить тома iSCSI
SCSI2 (0,0,0) (sda) - 21.5 GB ATA VBOX HARDDISK
> #1 первичн. 20.4 GB f ext4 /
> #5 логичес. 1.0 GB f подк подк
Отменить изменения разделов
Закончить разметку и записать изменения на диск

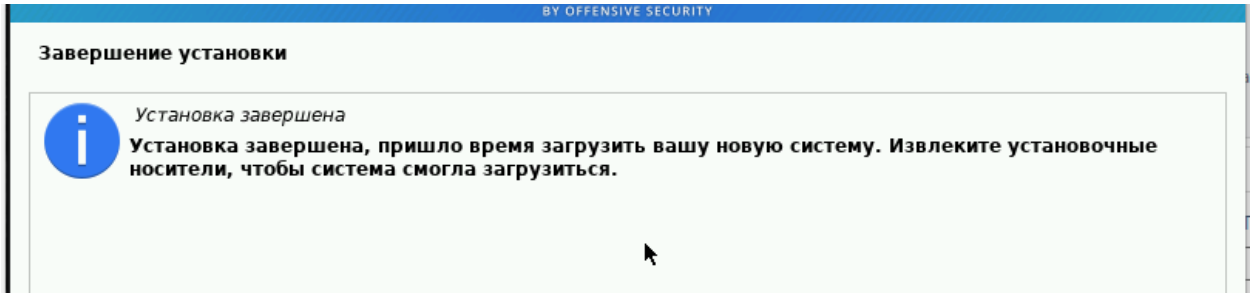

KALI
BY OFFENSIVE SECURITY
Разметка дисков
Если вы продолжите, то изменения, перечисленные ниже, будут записаны на диски. Или же вы можете сделать все изменения вручную.
На этих устройствах изменены таблицы разделов:
SCSI2 (0,0,0) (sda)
Следующие разделы будут отформатированы:
раздел #1 на устройстве SCSI2 (0,0,0) (sda) как ext4
раздел #5 на устройстве SCSI2 (0,0,0) (sda) как подк
Записать изменения на диск?
Нет
Да

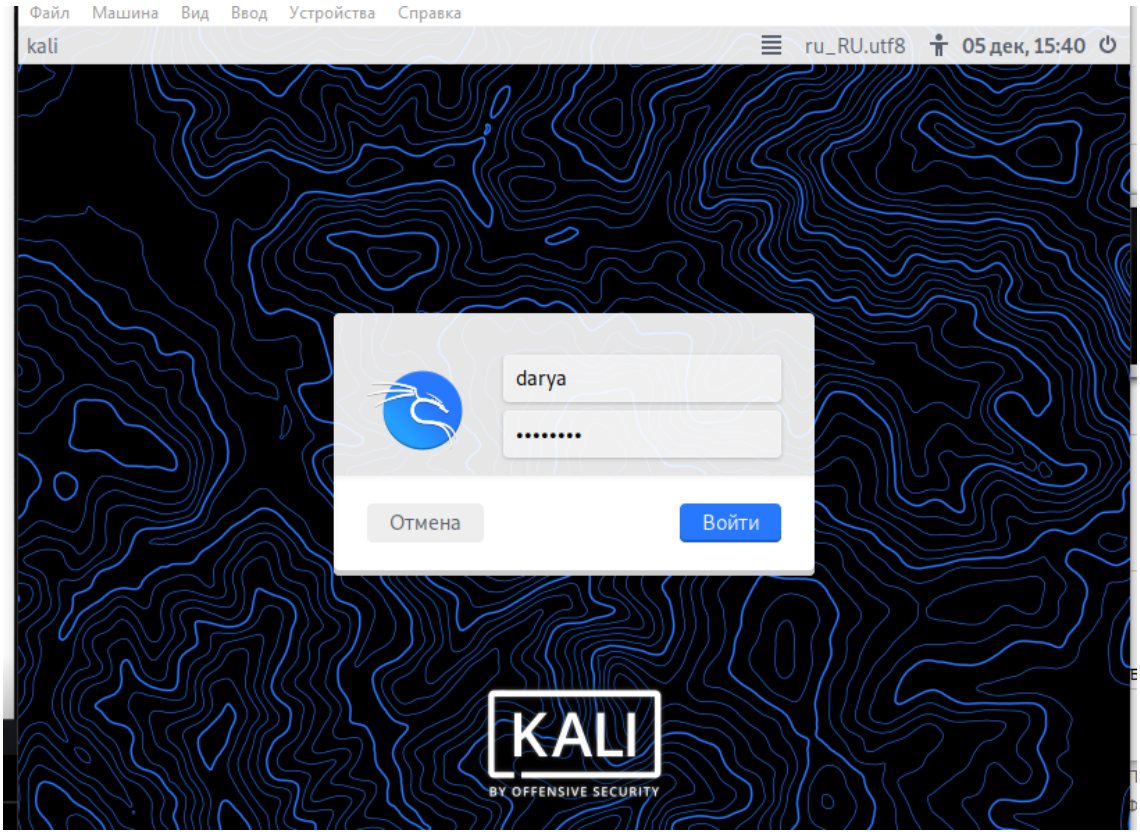

KALI
BY OFFENSIVE SECURITY
Выбор программного обеспечения
At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.
You can customize it by choosing a different desktop environment or a different collection of tools.
Choose software to install:
Desktop environment [selecting this item has no effect]
... Xfce (Kali's default desktop environment)
... GNOME
... KDE Plasma
Collection of tools [selecting this item has no effect]
... top10 -- the 10 most popular tools
... default -- recommended tools (available in the live system)

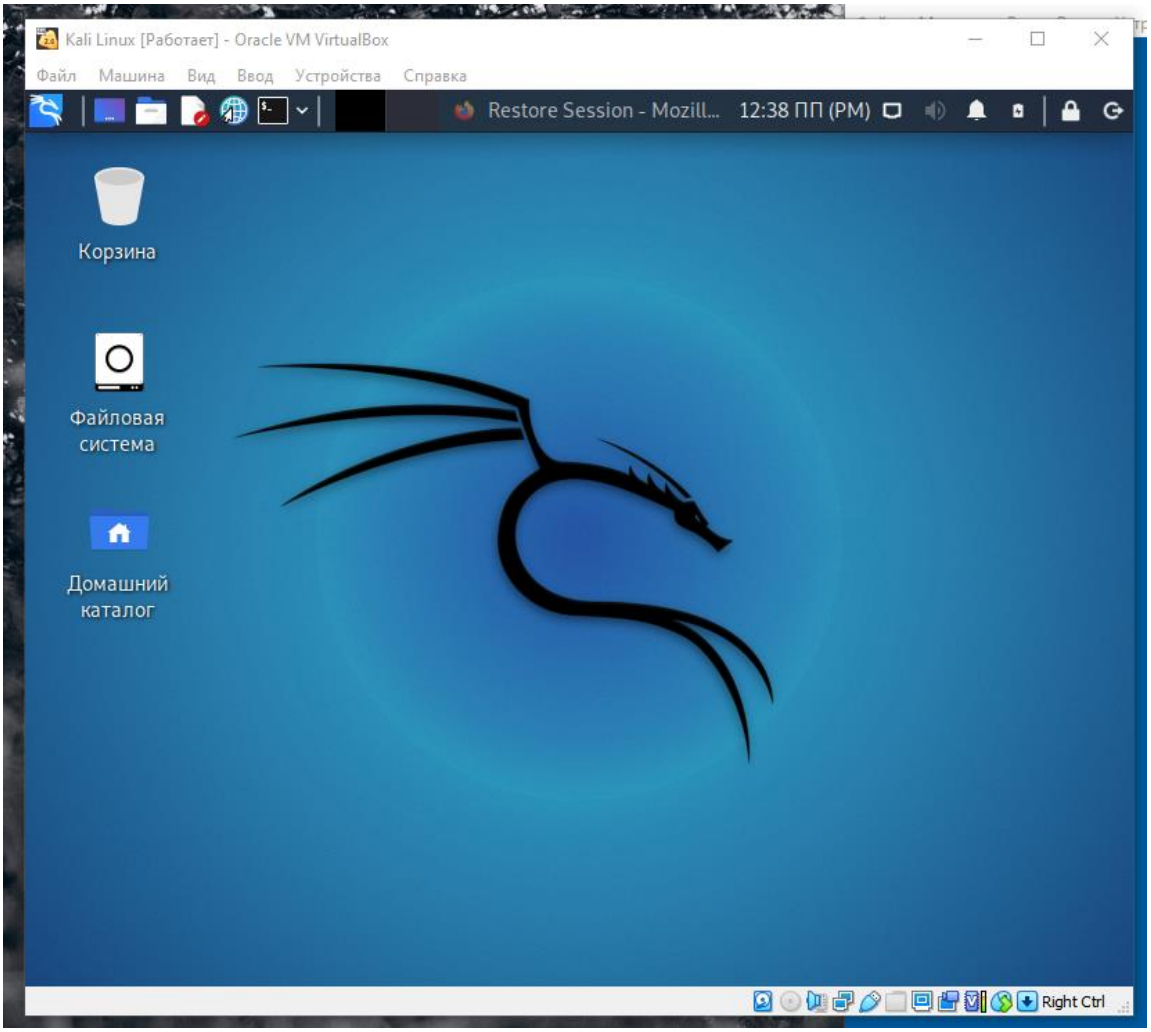

KALI
BY OFFENSIVE SECURITY
Выбор и установка программного обеспечения
Выбор и установка программного обеспечения
Распаковывается libopus0 (amd64)


Установка системного загрузчика GRUB
Похоже, что данная система будет единственной на этом компьютере. Если это действительно так, то можно спокойно устанавливать системный загрузчик GRUB на первичный диск (загрузочный раздел/запись UEFI).
Предупреждение: Если программе установки не удалось обнаружить другую операционную систему, имеющуюся на компьютере, то эту операционную систему некоторое время нельзя будет загрузить. Позднее можно будет настроить GRUB вручную для её загрузки.
Установить системный загрузчик GRUB на первичный диск?
Нет
Да


Установка системного загрузчика GRUB
Пришло время научить только что установленную систему загружаться. Для этого на загрузочное устройство будет установлен системный загрузчик GRUB. Обычно он устанавливается на первый жёсткий диск (в загрузочную запись/раздел UEFI). При желании можно установить GRUB в любое другое место на диске, либо на другой диск или на сменный носитель.
Устройство для установки системного загрузчика:
Указать устройство вручную
/dev/sda (ata-VBOX_HARDDISK_VB3647c264-9a147e6a)


BY OFFENSIVE SECURITY
Завершение установки
Установка завершена
Установка завершена, пришло время загрузить вашу новую систему. Извлеките установочные носители, чтобы система смогла загрузиться.

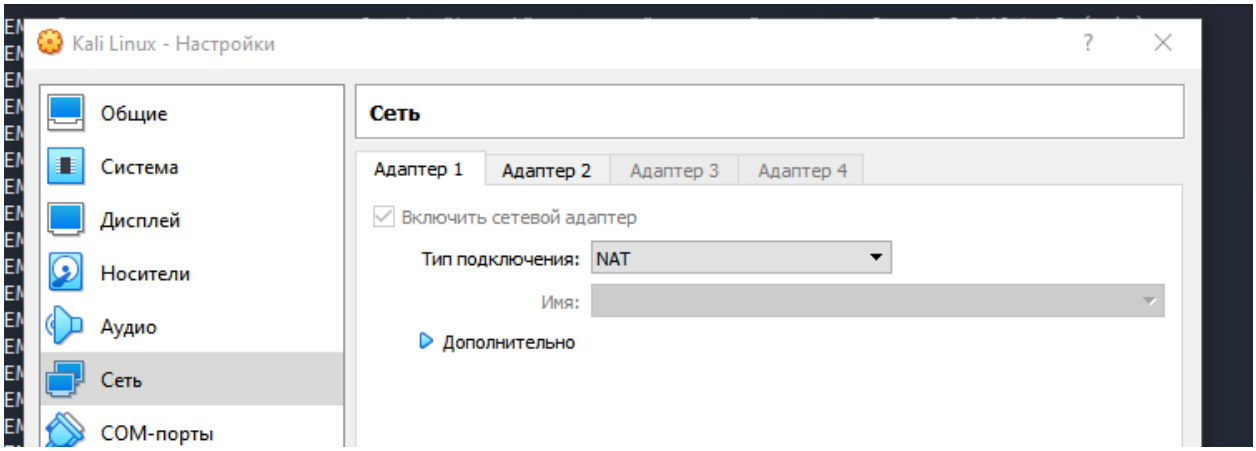

Файл Машина Вид Ввод Устройства Справка
kali
ru_RU.utf8
05 дек, 15:40
darya
Отмена
Войти
KALI
BY OFFENSIVE SECURITY

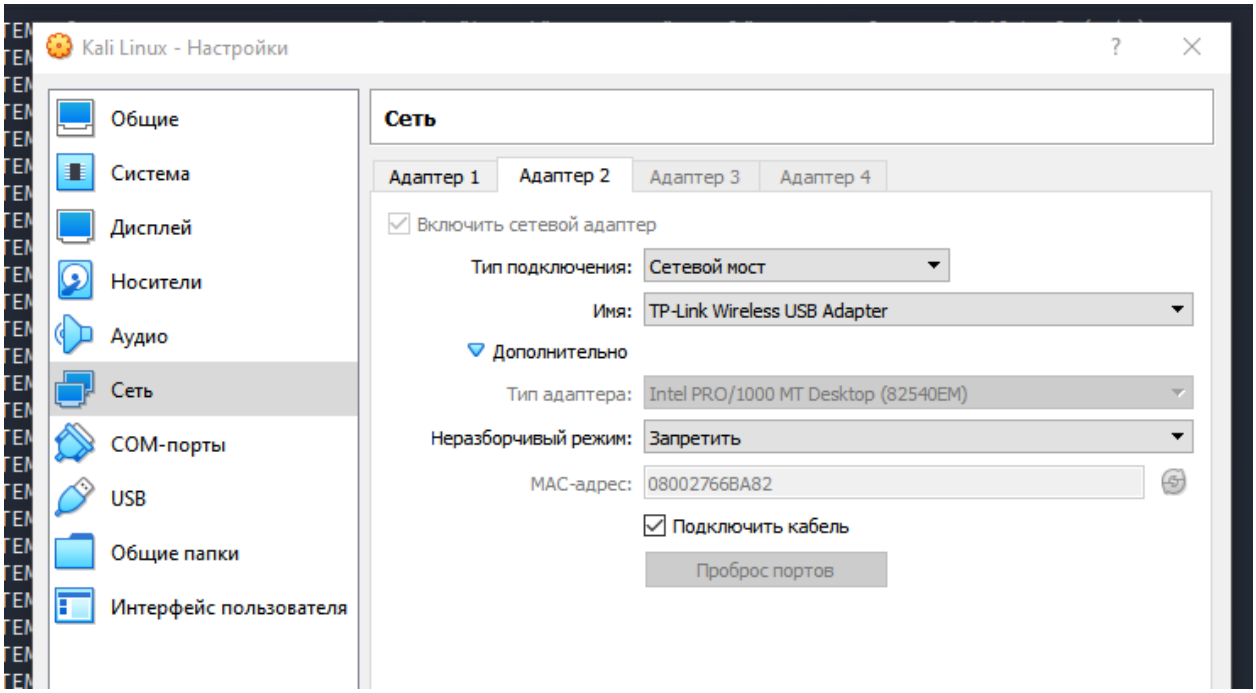

Kali Linux [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Restore Session - Mozill...
12:38 ПП (PM)
Корзина
Файловая система
Домашний каталог
Right Ctrl

3. Провести: **а) атаку** или б) несанкционированное сканирование.

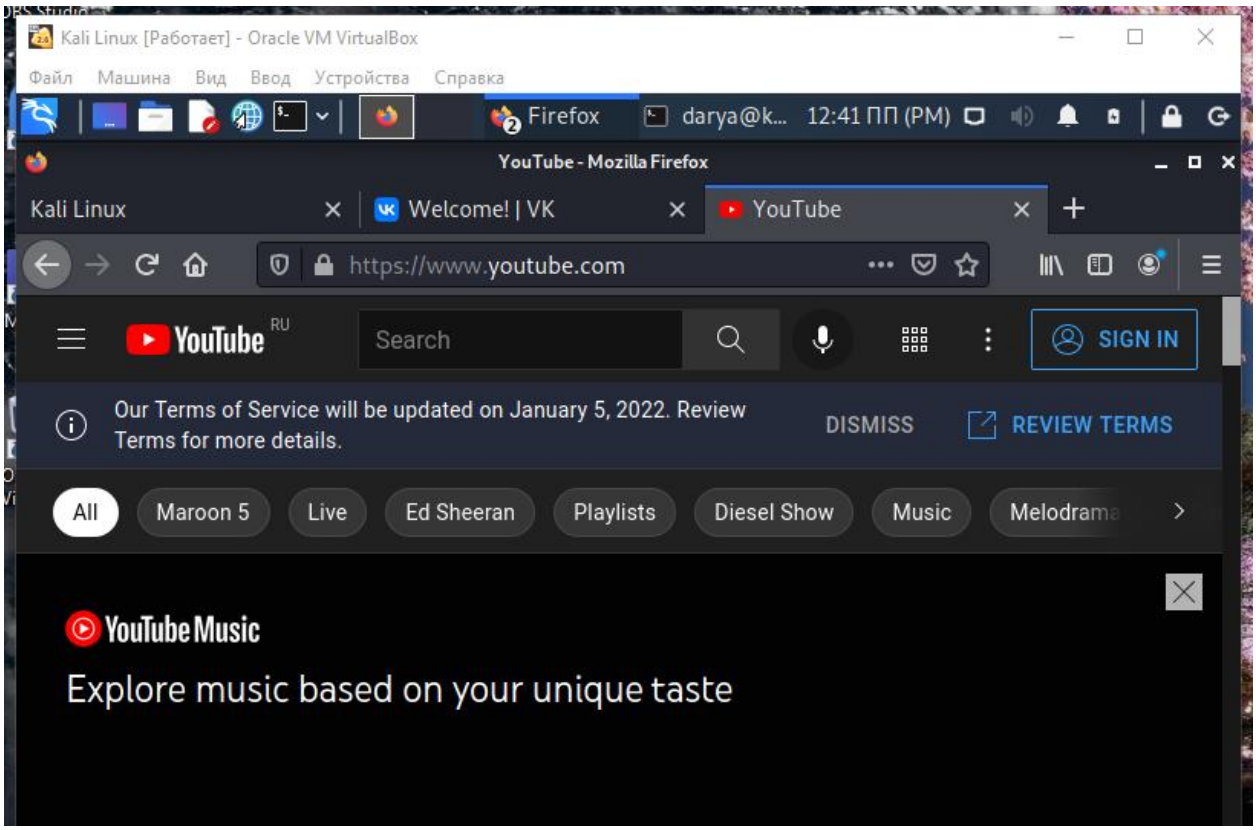
Для начала проверим связь виртуальных машин и их доступ в Интернет. При этом сеть на машинах настроена следующим образом.

Kali Linux:

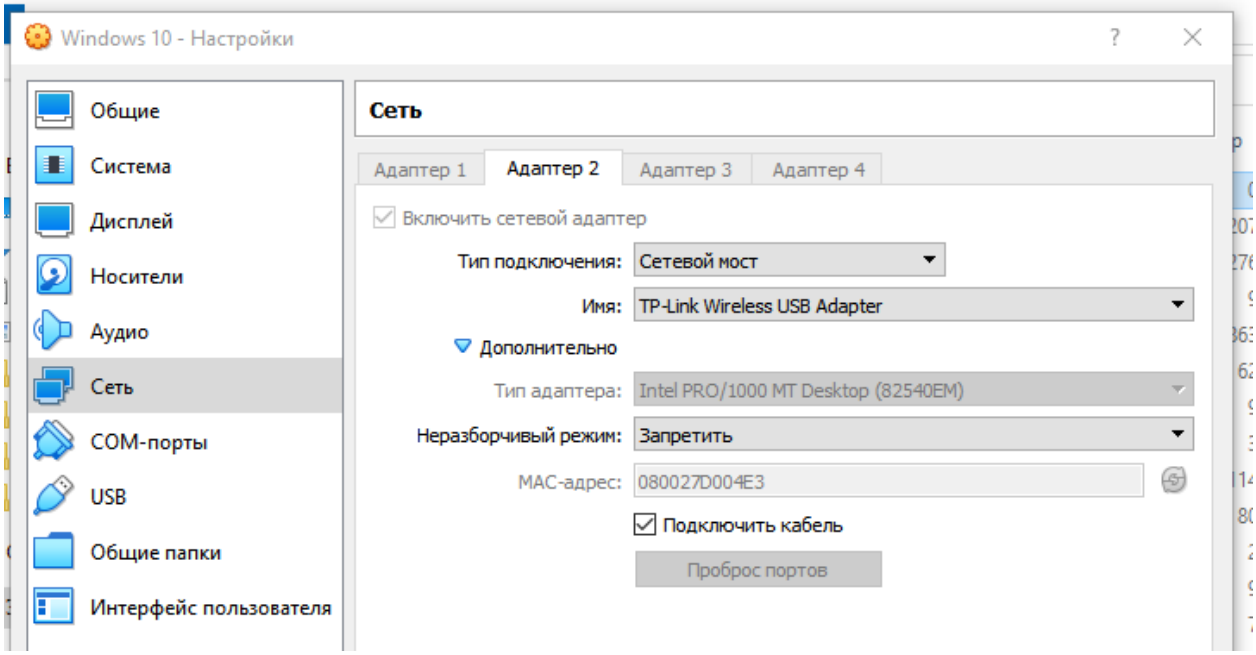




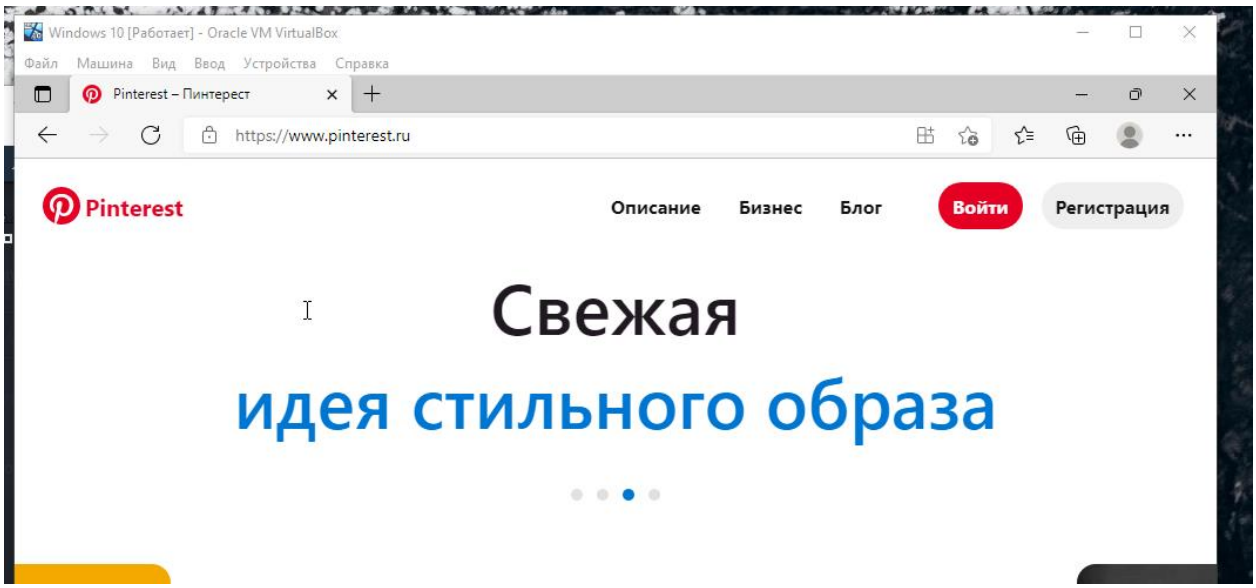
Доступ в Интернет:



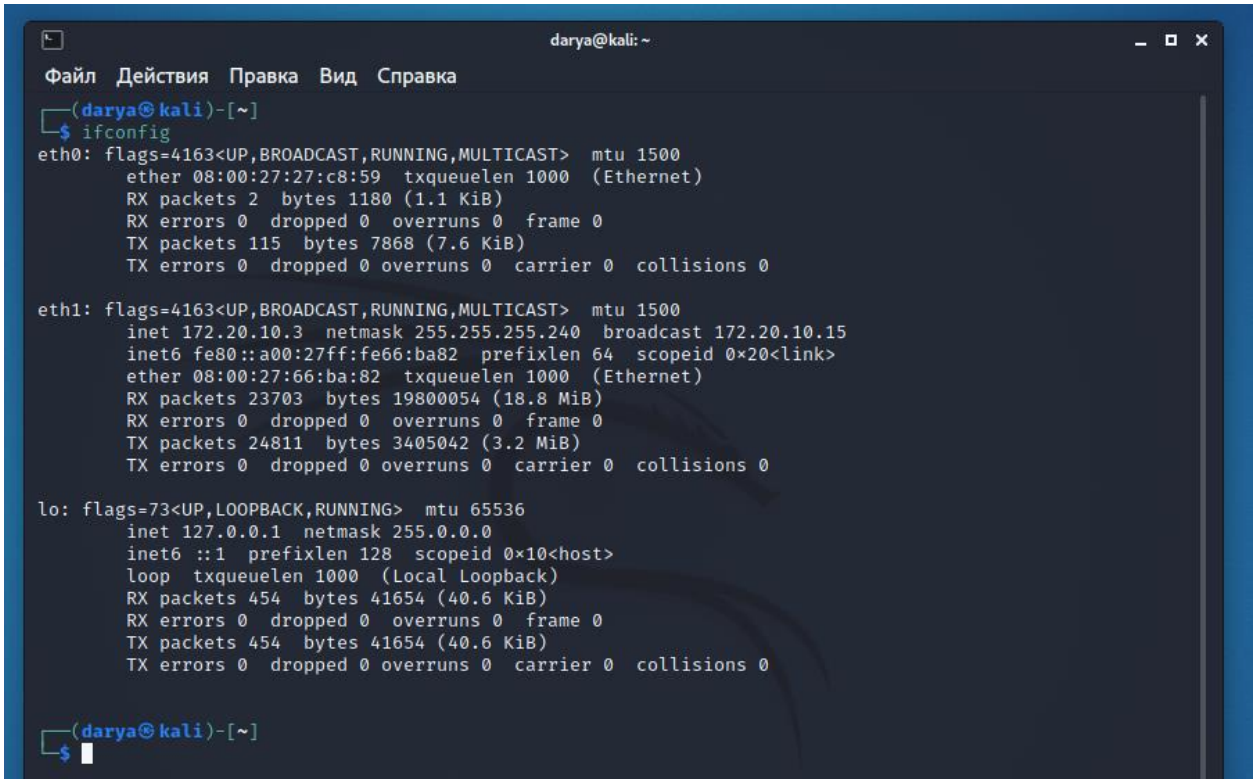
Windows:

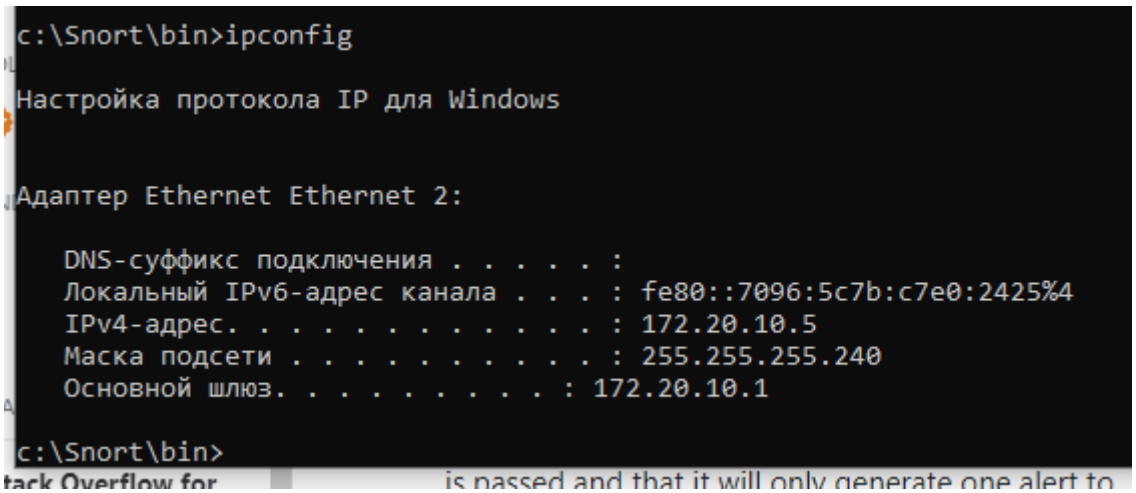


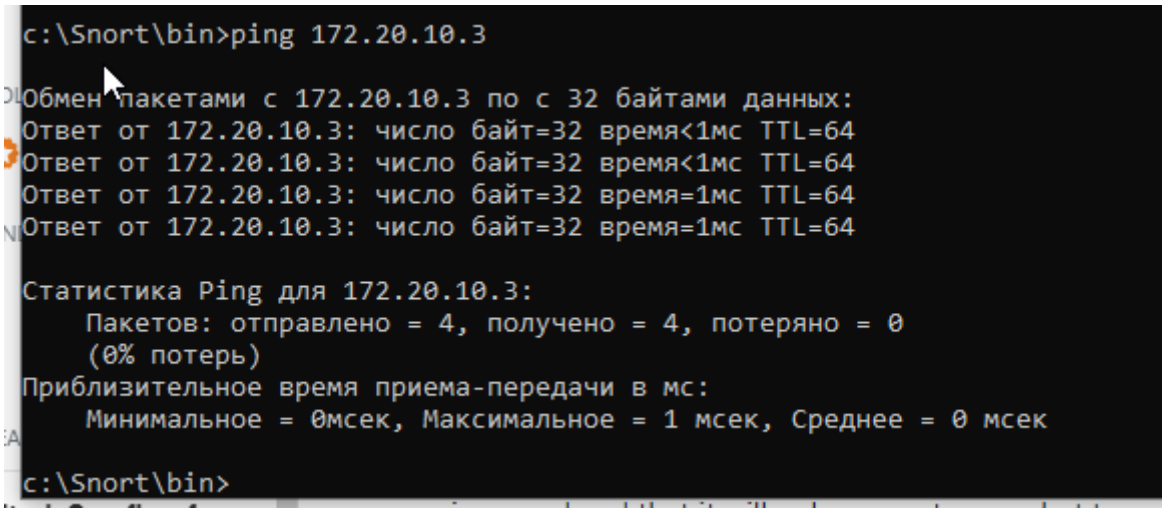
Доступ в Интернет:

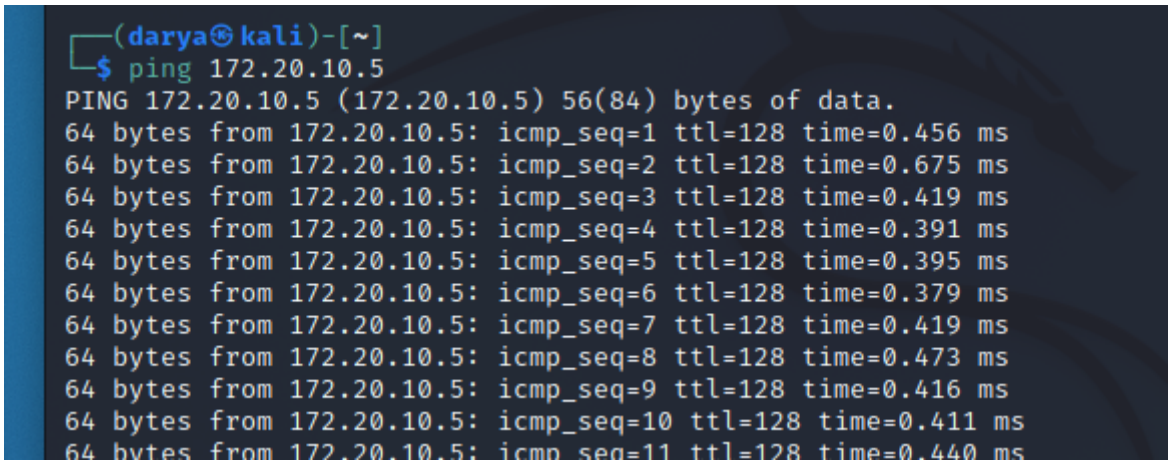


Теперь проверим могут ли машины видеть друг друга в локальной сети:

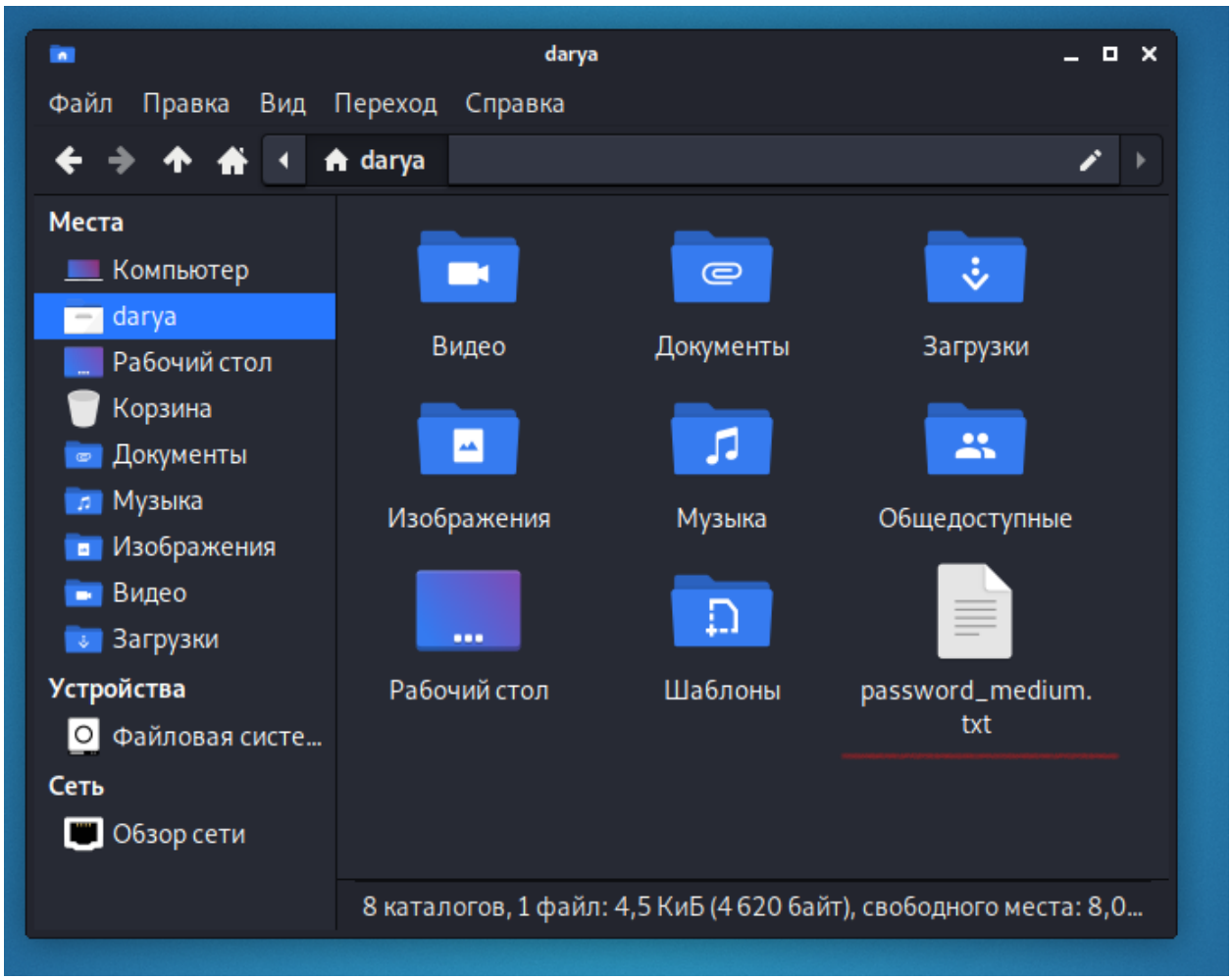


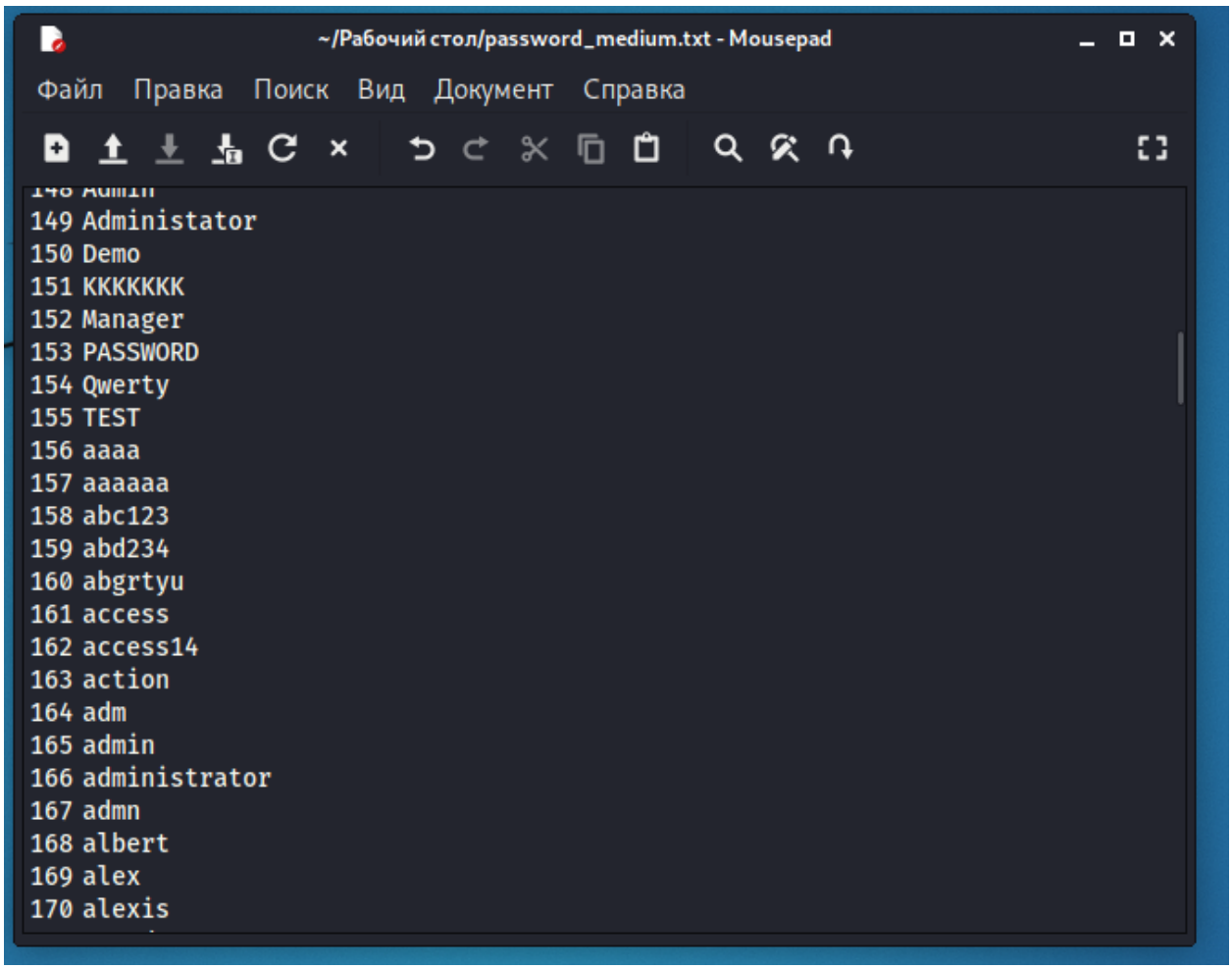




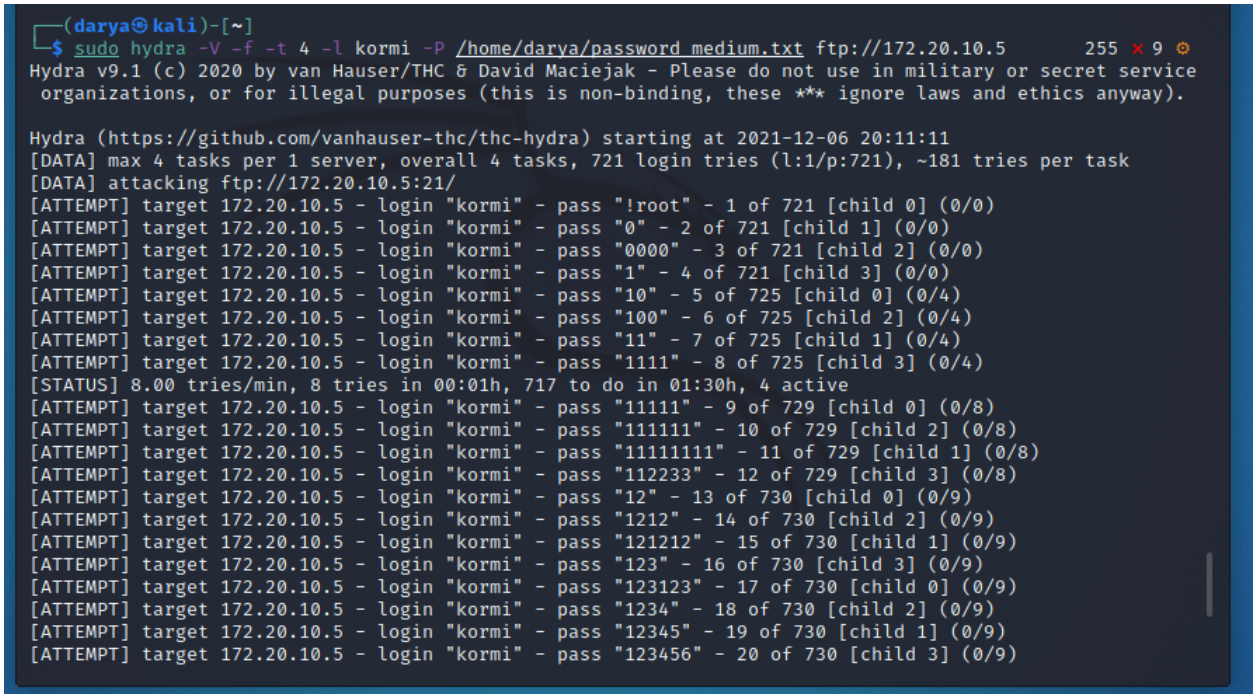


Когда внутренняя сеть между машинами создана и отлажена, приступим к проведению атаки. Выбор пал на атаку Brute-force SSH. Попробуем подобрать пароль пользователя kormi по SSH. Осуществим атаку с помощью Hydra. Для этого скачаем файл с подборкой несложных паролей:


darya
Файл Правка Вид Переход Справка
darya
Места
Компьютер
darya
Рабочий стол
Корзина
Документы
Музыка
Изображения
Видео
Загрузки
Устройства
Файловая систе...
Сеть
Обзор сети
Видео
Документы
Загрузки
Изображения
Музыка
Общедоступные
Рабочий стол
Шаблоны
password_medium.txt
8 каталогов, 1 файл: 4,5 КиБ (4 620 байт), свободного места: 8,0...



А после дадим команду на взлом:



Атака не увенчалась успехом. Пароль не был подобран.

4. Написать правила в Snort, поместить их в папку с правилами и продемонстрировать результат работы IDS.

Немного изменим файл snort.conf, а именно 45 строку:

```
43
44  # Setup the network addresses you are protecting
45  ipvar HOME_NET 172.20.10.1/28
46
47  # Set up the external network addresses. Leave as "any" in most
48  ipvar EXTERNAL_NET !$HOME_NET
49
50  # List of DNS servers on your network
51  ipvar DNS_SERVERS $HOME_NET
52
53  # List of SMTP servers on your network
54  ipvar SMTP_SERVERS $HOME_NET
```

Пишем правило в local.rules:

snort.conf | local.rules

```
4   # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
5   # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
6   # Sourcefire and other third parties (the "GPL Rules") that are distributed under the
7   # GNU General Public License (GPL), v2.
8   #
9   # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
10  # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
11  # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
12  # their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
13  # list of third party owners and their respective copyrights.
14  #
15  # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16  # to the VRT Certified Rules License Agreement (v2.0).
17  #
18  #-------------
19  # LOCAL RULES
20  #-------------
21  # alert icmp any any -> any any (msg:"Testing ICMP"; sid:1000001; )
22  # alert tcp any any -> any any (msg:"Testing TCP"; sid:1000002; )
23  # alert udp any any -> any any (msg:"Testing UDP"; sid:1000003; )
24  alert tcp any any -> $HOME_NET 21 (msg:"Possible FTP brute forcing!"; flags: S+; sid:10000001; rev: 1;)
25
```

Смотрим интерфейсы и выбираем 4:

```
c:\Snort\bin>snort -W

          -*> Snort! <*-
  o"  )~  Version 2.9.18.1-WIN64 GRE (Build 1005)
   ''''   By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
          Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using PCRE version: 8.10 2010-06-25
          Using ZLIB version: 1.2.11

Index   Physical Address       IP Address      Device Name     Description
-----   ----------------       ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{BDDB929F-0D13-4A89-AAD3-C7F6051E8BA6}      WAN Miniport (Ne
twork Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{D2B87321-9A91-4521-AF8E-374EAE1EE9AA}      WAN Miniport (IP
v6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{B9C3EA29-AB44-4ED6-AB53-545B8E4258FC}      WAN Miniport (IP
)
    4   08:00:27:D0:04:E3       0000:0000:fe80:0000:0000:0000:7096:5c7b \Device\NPF_{338C02C9-EBC7-471C-8698-822B61BF5BD
9}      Intel(R) PRO/1000 MT Desktop Adapter #2
    5   00:00:00:00:00:00       disabled        \Device\NPF_Loopback    Adapter for loopback traffic capture

c:\Snort\bin>
```

Stack Overflow for ... is passed and that it will only generate one alert to ... Intel Corporation Moscow, Russia

Запускаем Snort, логи должны будут записываться в файл brute_force.txt:

```
c:\Snort\bin>snort -i 4 -c c:\Snort\etc\snort.conf -A console > c:\Snort\log\brute_force.txt
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 37
```

Тем временем на Kali Linux пароль подбирается:

```
darya@kali: ~
Файл  Действия  Правка  Вид  Справка
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "50" - 81 of 730 [child 3] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "51" - 82 of 730 [child 1] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "5150" - 83 of 730 [child 0] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "52" - 84 of 730 [child 2] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "53" - 85 of 730 [child 3] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "54" - 86 of 730 [child 1] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "55" - 87 of 730 [child 0] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "5555" - 88 of 730 [child 2] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "56" - 89 of 730 [child 3] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "57" - 90 of 730 [child 1] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "58" - 91 of 730 [child 0] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "59" - 92 of 730 [child 2] (0/9)
[STATUS] 7.67 tries/min, 92 tries in 00:12h, 638 to do in 01:24h, 4 active
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "6" - 93 of 730 [child 3] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "60" - 94 of 730 [child 1] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "61" - 95 of 730 [child 0] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "62" - 96 of 730 [child 2] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "63" - 97 of 730 [child 3] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "64" - 98 of 730 [child 1] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "65" - 99 of 730 [child 0] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "654321" - 100 of 730 [child 2] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "66" - 101 of 730 [child 3] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "6666" - 102 of 730 [child 1] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "666666" - 103 of 730 [child 0] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "67" - 104 of 730 [child 2] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "68" - 105 of 730 [child 3] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "69" - 106 of 730 [child 1] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "6969" - 107 of 730 [child 0] (0/9)
[ATTEMPT] target 172.20.10.5 - login "kormi" - pass "696969" - 108 of 730 [child 2] (0/9)
```

Открываем файл brute_force.txt:

```
brute_force.txt – Блокнот
Файл  Правка  Формат  Вид  Справка
12/06-22:56:42.710001  [**] [1:10000001:1] Possible FTP brute forcing! [**] [Priority: 0] {TCP} 172.20.10.3:48998 -> 172.20.1
12/06-22:56:42.710001  [**] [1:10000001:1] Possible FTP brute forcing! [**] [Priority: 0] {TCP} 172.20.10.3:48992 -> 172.20.1
12/06-22:56:42.710001  [**] [1:10000001:1] Possible FTP brute forcing! [**] [Priority: 0] {TCP} 172.20.10.3:48996 -> 172.20.1
12/06-22:56:43.358844  [**] [1:10000001:1] Possible FTP brute forcing! [**] [Priority: 0] {TCP} 172.20.10.3:49000 -> 172.20.1
12/06-22:56:43.480873  [**] [1:10000001:1] Possible FTP brute forcing! [**] [Priority: 0] {TCP} 172.20.10.3:48994 -> 172.20.1
12/06-22:56:44.234086  [**] [1:10000001:1] Possible FTP brute forcing! [**] [Priority: 0] {TCP} 172.20.10.3:49002 -> 172.20.1
12/06-22:56:44.375796  [**] [1:10000001:1] Possible FTP brute forcing! [**] [Priority: 0] {TCP} 172.20.10.3:49000 -> 172.20.1
```

```
0] {TCP} 172.20.10.3:48998 -> 172.20.10.5:21
0] {TCP} 172.20.10.3:48992 -> 172.20.10.5:21
0] {TCP} 172.20.10.3:48996 -> 172.20.10.5:21
0] {TCP} 172.20.10.3:49000 -> 172.20.10.5:21
0] {TCP} 172.20.10.3:48994 -> 172.20.10.5:21
0] {TCP} 172.20.10.3:49002 -> 172.20.10.5:21
0] {TCP} 172.20.10.3:49000 -> 172.20.10.5:21
```

Сообщения записываются в файл. Правило работает корректно.