



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
**«МИРЭА – Российский технологический университет»**  
**РТУ МИРЭА**

---

Институт кибербезопасности и цифровых технологий  
Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

---

## **Отчёт по практической работе № 2.2**

По дисциплине

«Управление информационной безопасностью»

Тема: «Обнаружение и предупреждение компьютерных атак»

Задание: «Настройка параметров системы обнаружения атак»

Студент Кузькин Павел Александрович  
Группа ББМО-01-22

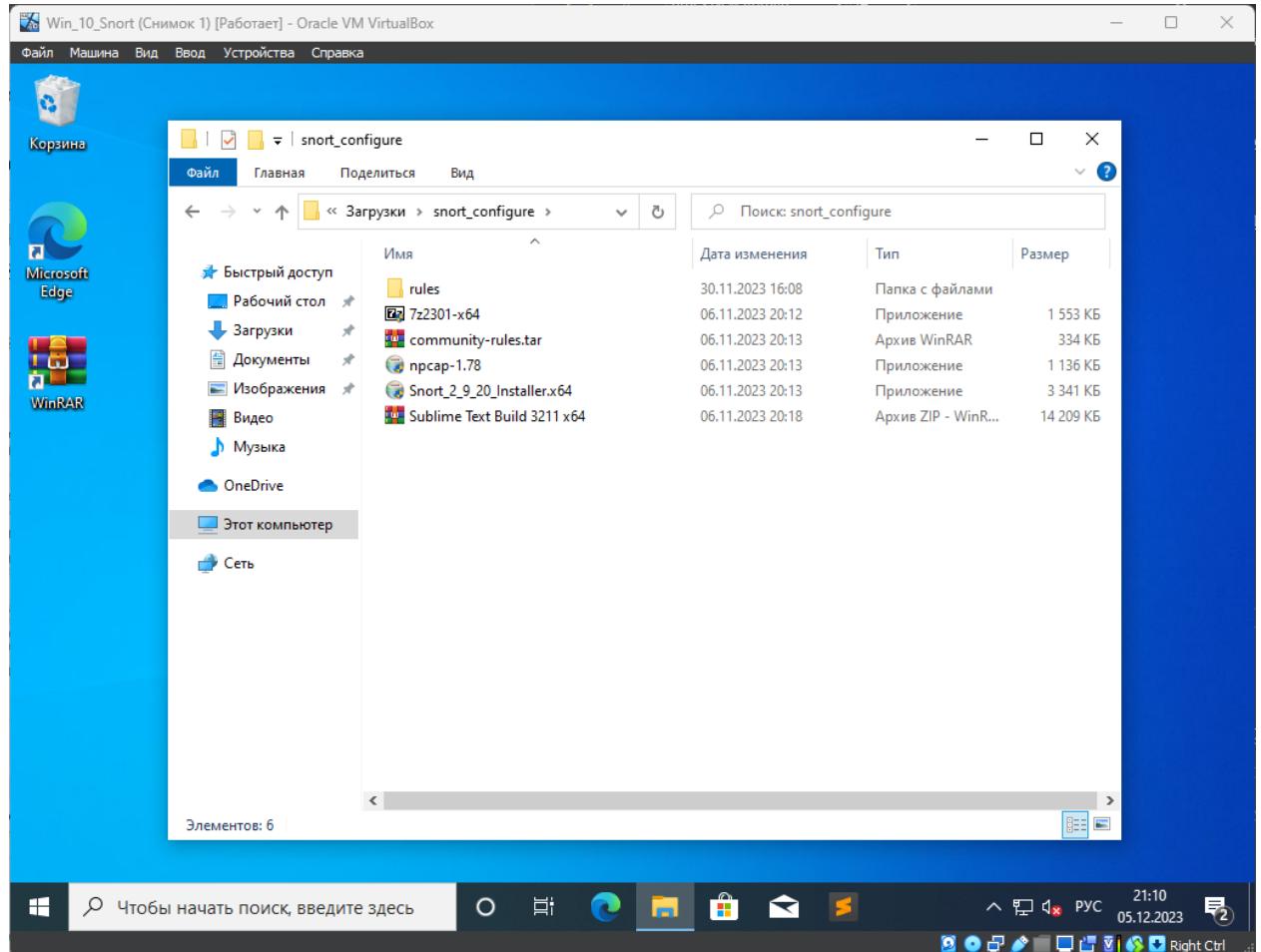
Работу проверил  
Пимонов Р.В.

Москва, 2023

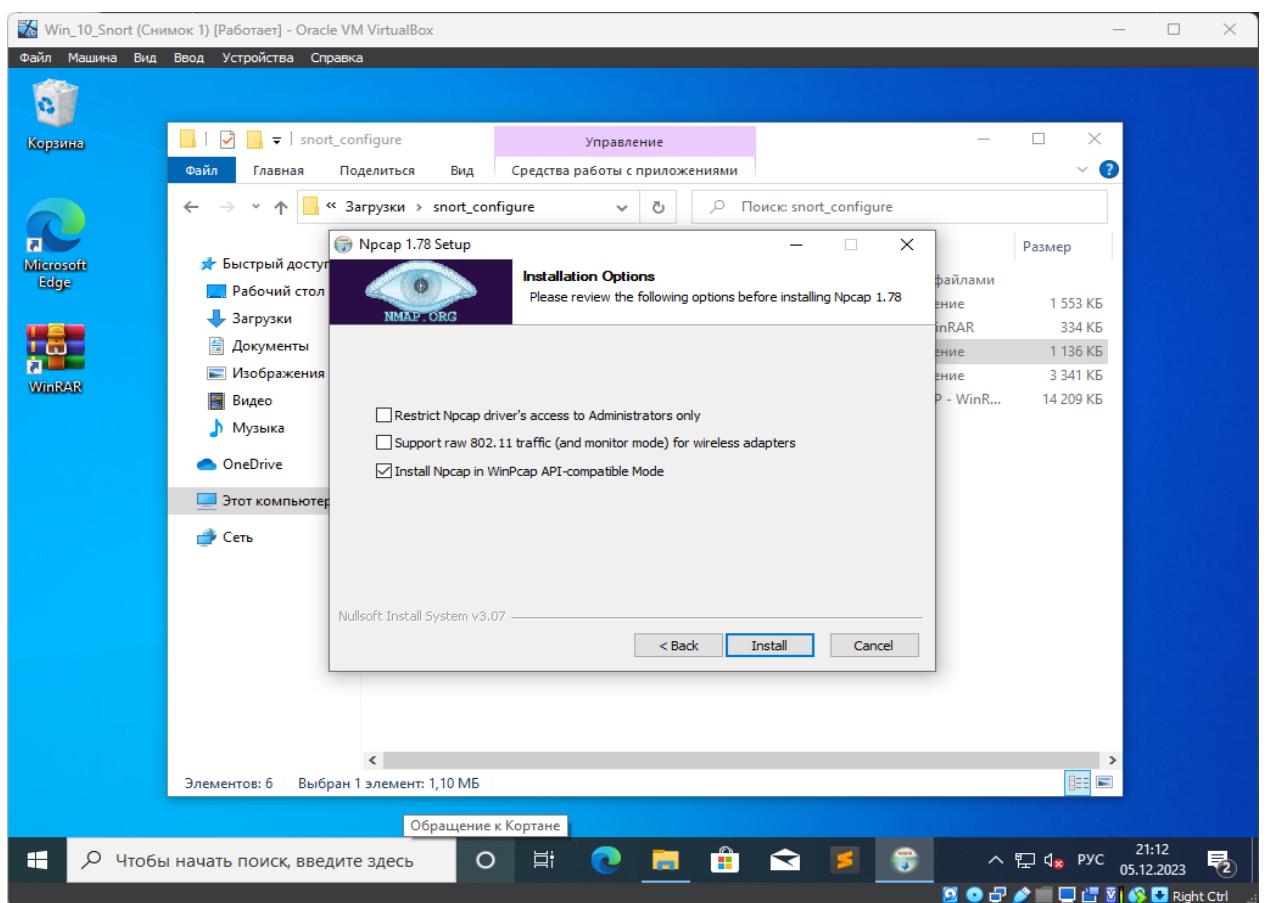
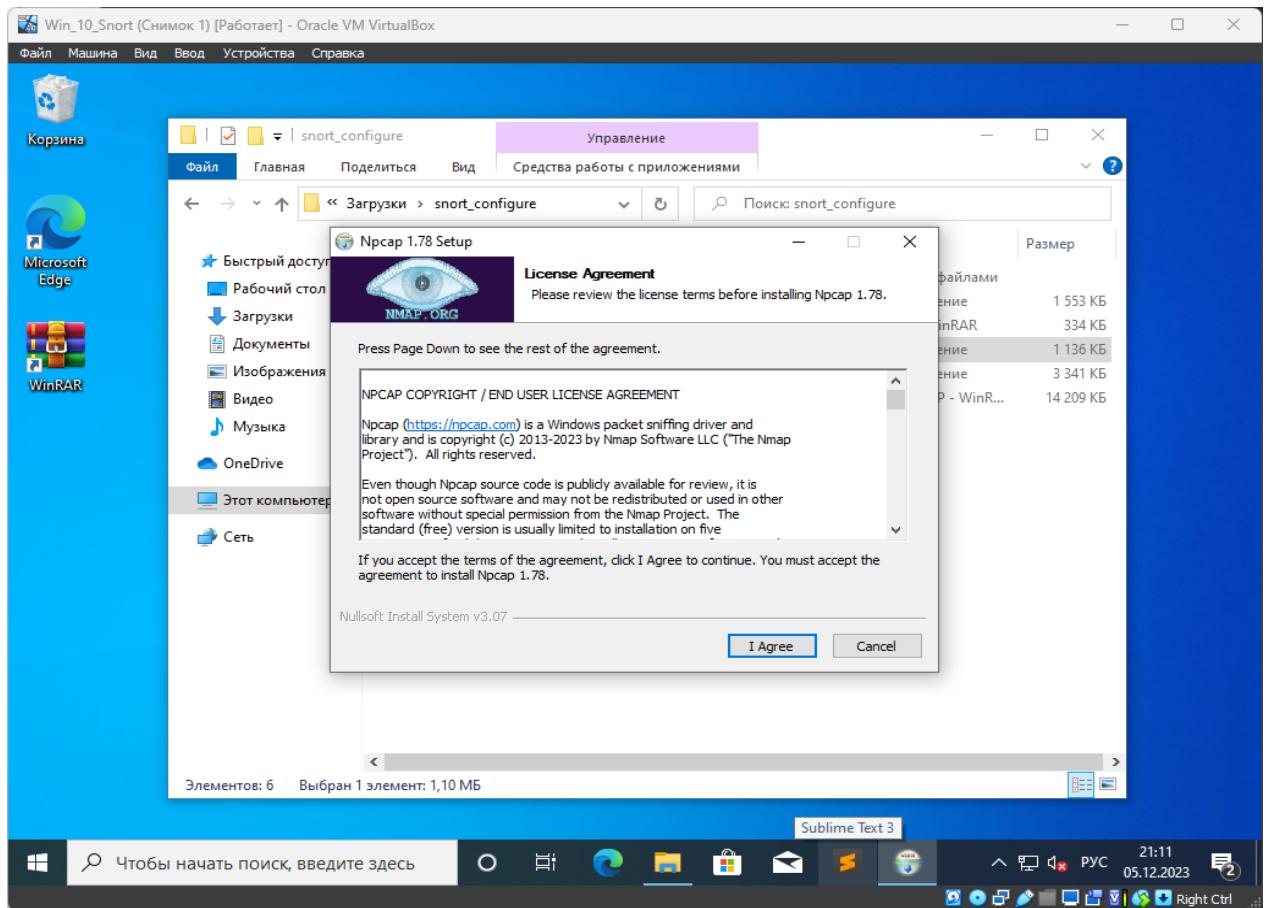
## Вопрос 1. Установка и настройка параметров IDS Snort

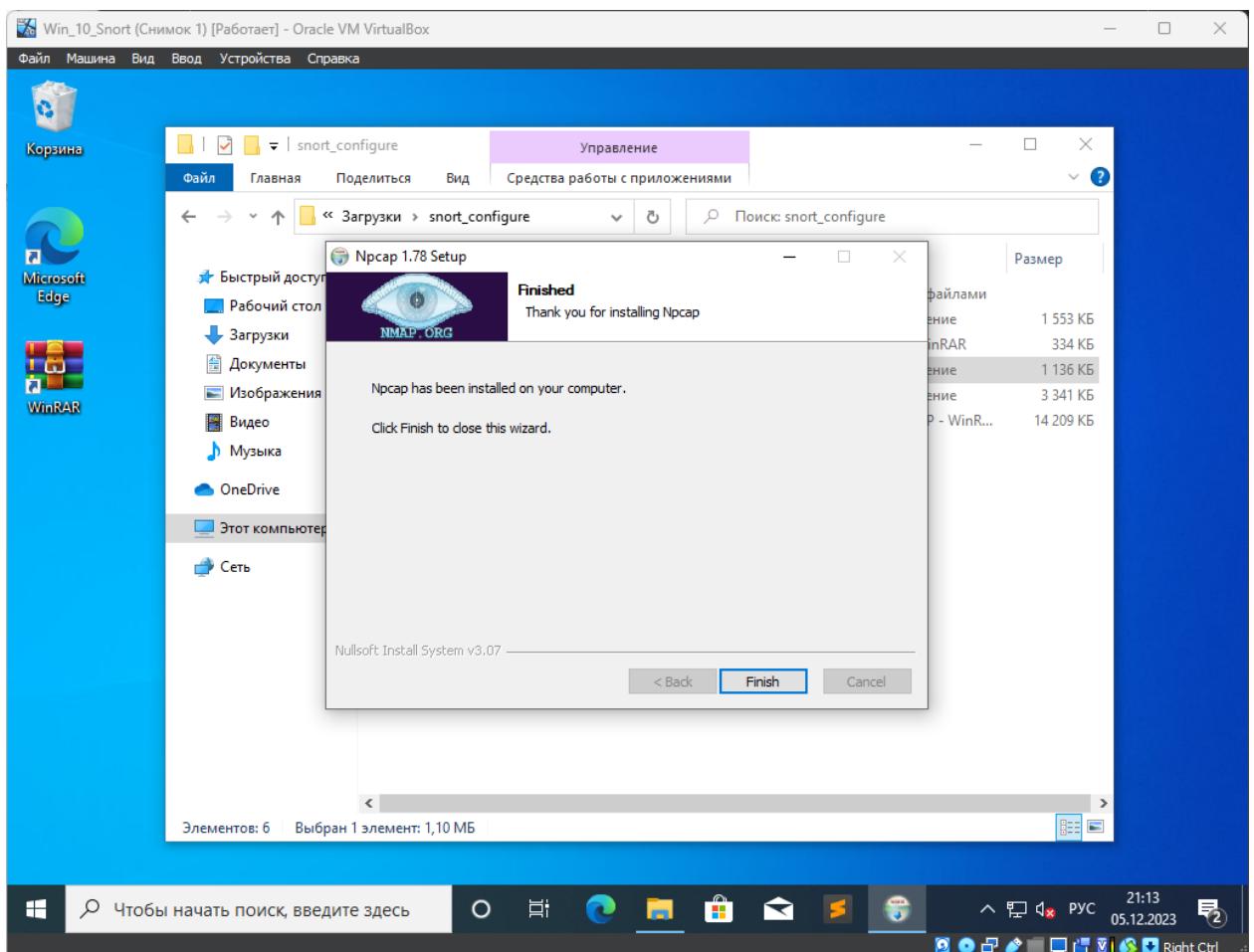
Перед выполнением задания скачаем архив с требующимся ПО по ссылке: <https://1drv.ms/u/s!AlN4iiJAxsjbgVMVo5Ha-52vbvT9?e=YbZNad>.

Разархивируем его и посмотрим его содержимое:

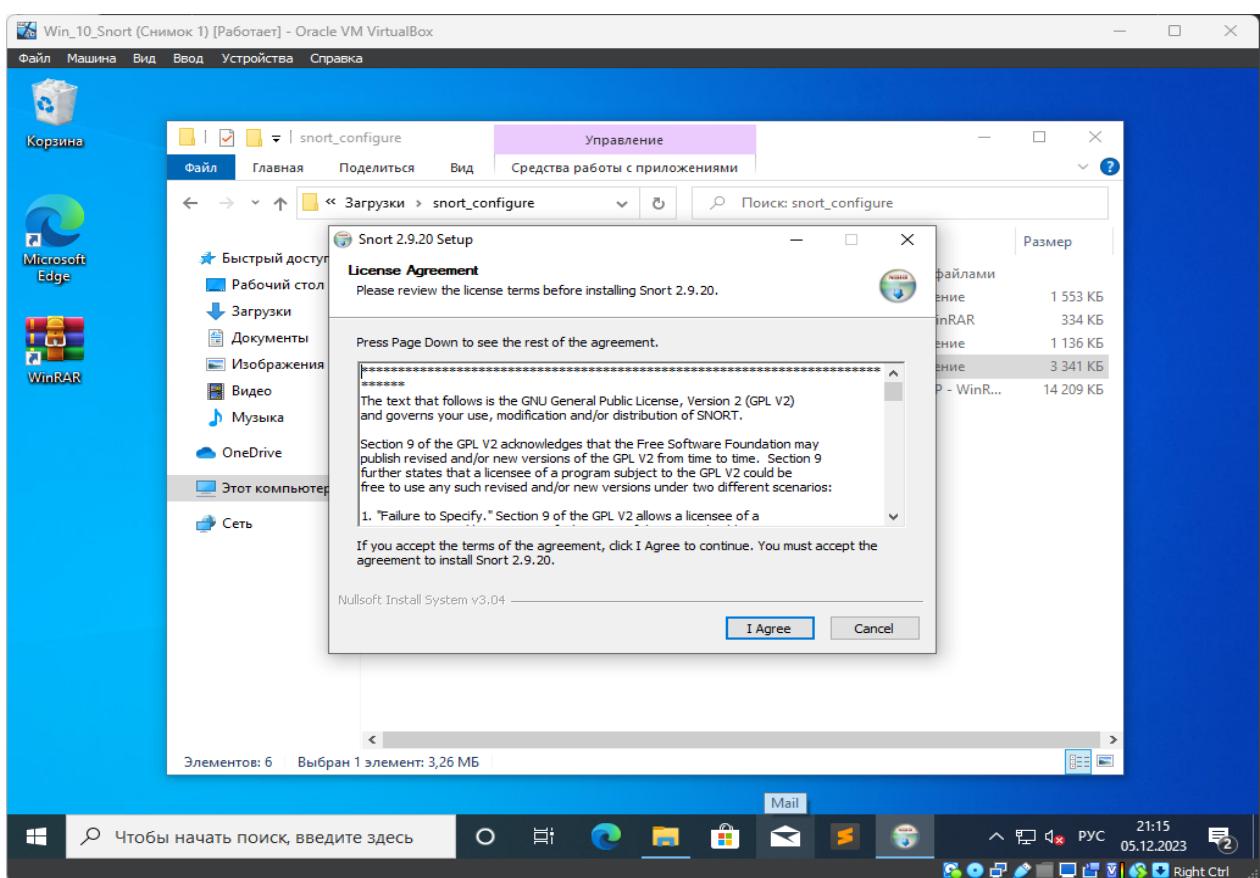


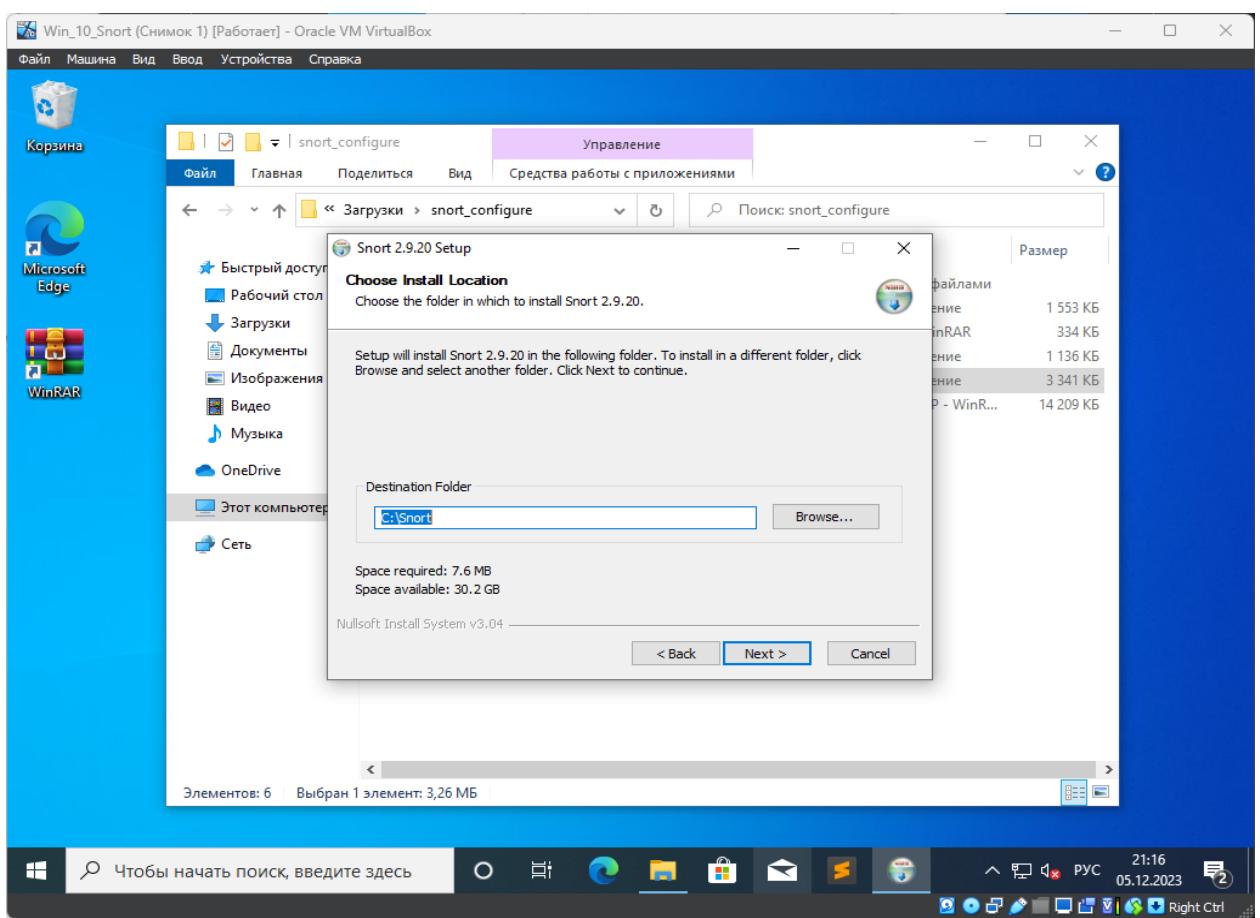
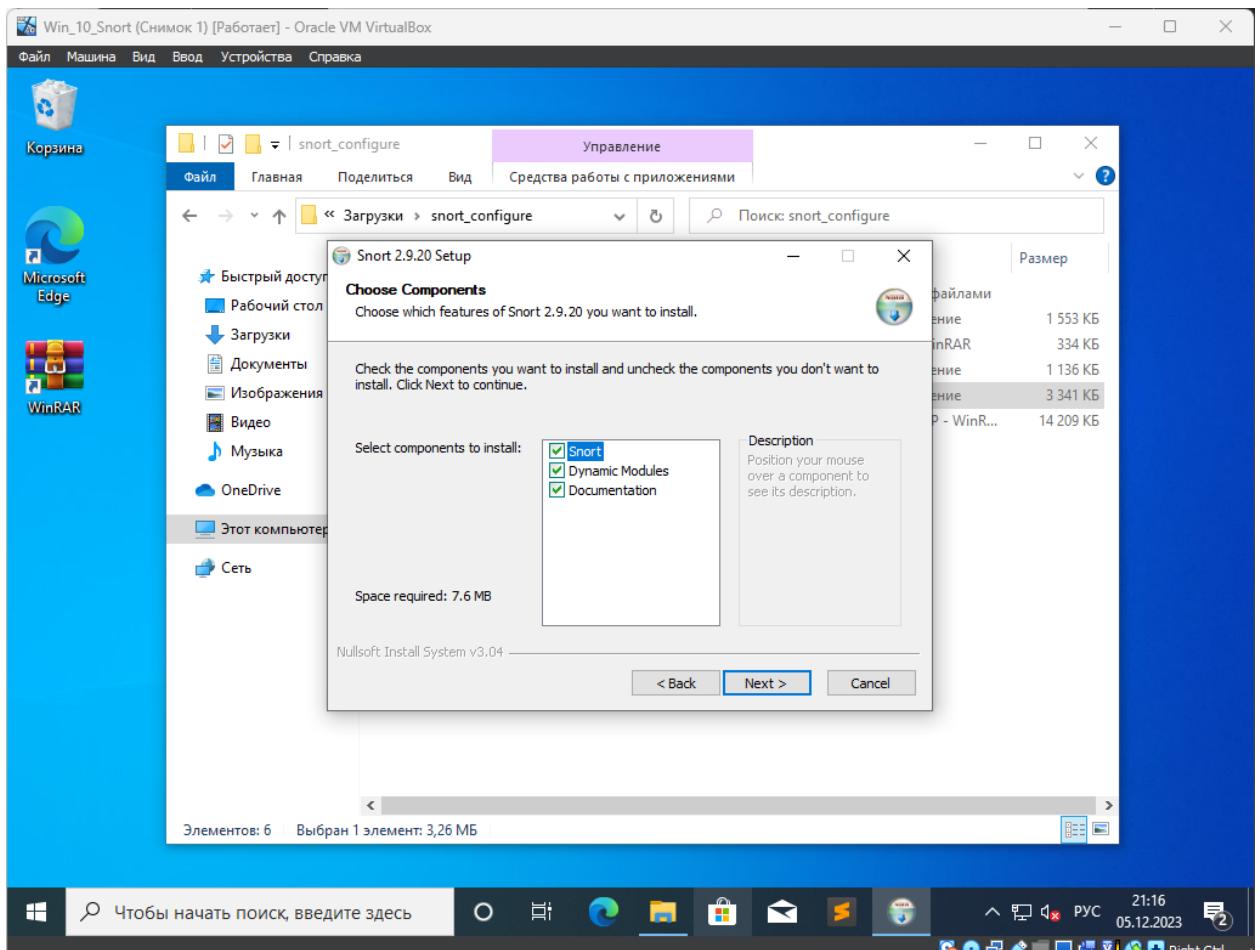
## Выполним установку нрсар:

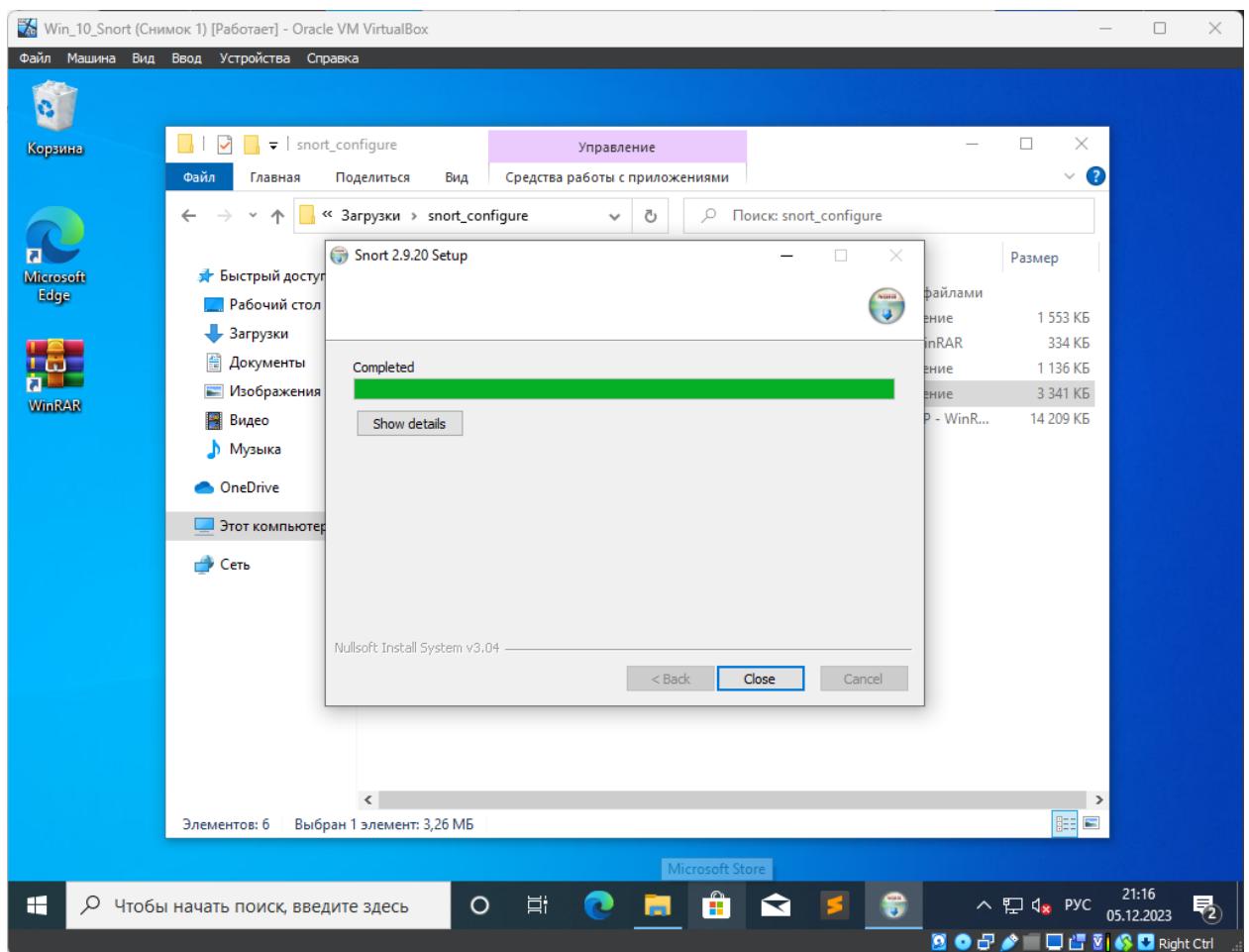




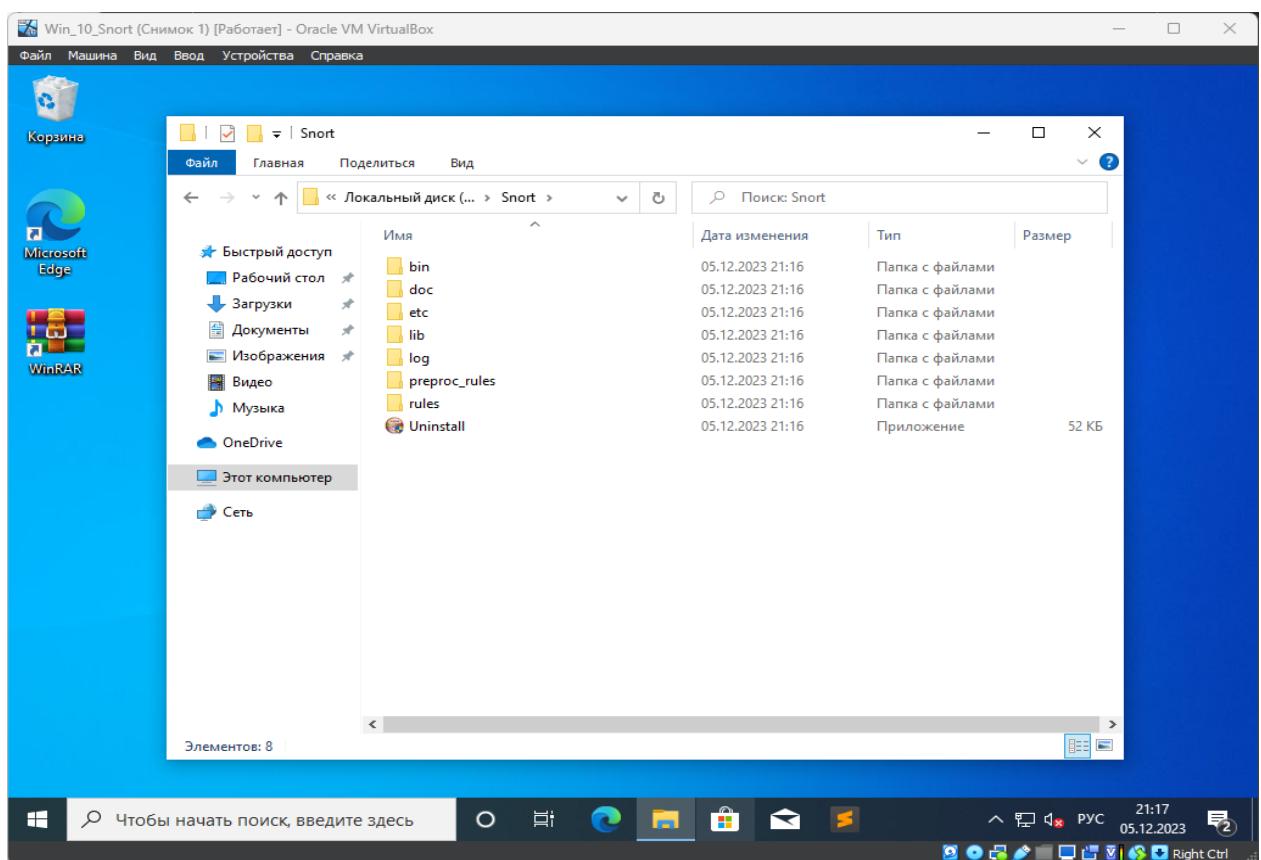
Выполним установку IDS Snort:





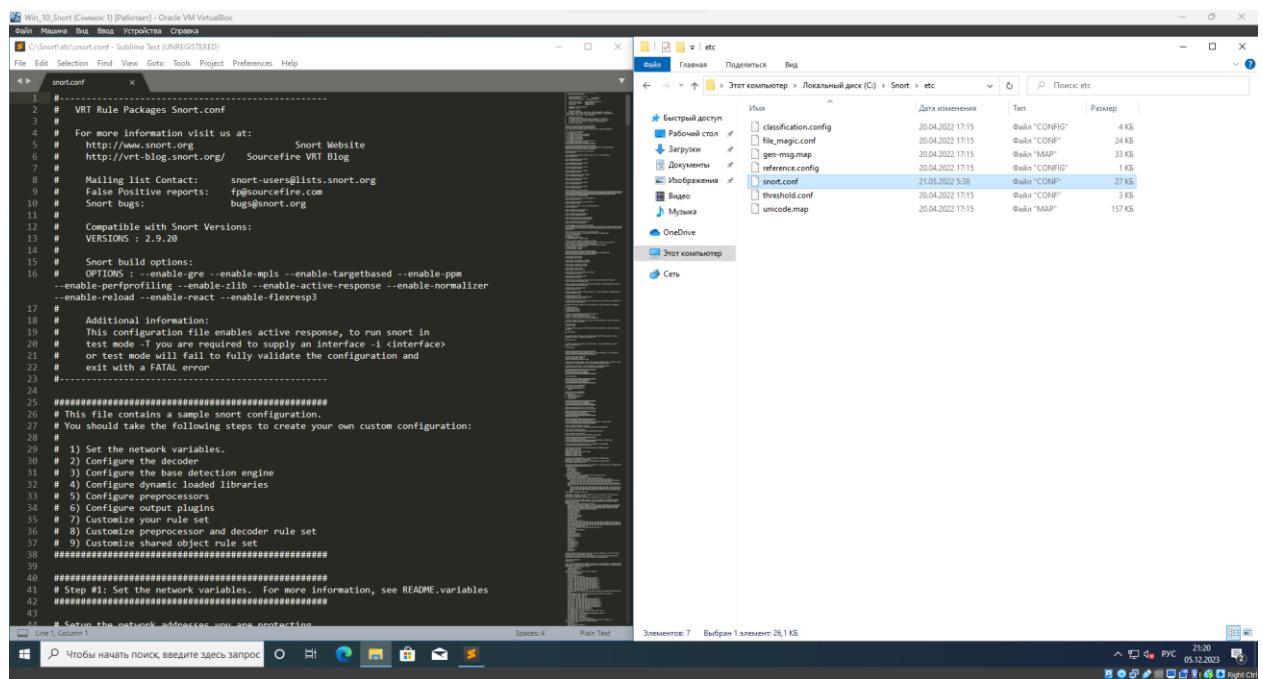


После установки в диске C:/ появится папка с файлами программы:



После перехода в директорию C:/Snort в первую очередь необходимо настроить файл конфигурации для его успешной работы.

Для настройки этого файла необходимо перейти в директорию C:/Snort/etc и открыть файл snort.conf, сделать это можно, например в текстовом редакторе Sublime Text или VS Code. Дальнейшие операции по редактированию конфигурационных файлов будут производится с помощью Sublime Text. Откроем файл C:/Snort/etc/snort.conf:



```
# Win_10_Snort [Snort] - Oracle VM VirtualBox
Файл Меню Вид Внешк Устройства Справка
C:\Snort\etc\snort.conf - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
+ snort.conf A
1 #
2 #-----#
3 # VRT Rule Packages Snort.conf
4 #
5 # For more information visit us at:
6 # http://www.snort.org Snort Website
7 # http://vrt-blog.snort.org/ Sourcefire VRT Blog
8 #
9 # Mailing list Contact: snort-users@lists.snort.org
10 # False Positive reports: fp@sourcefire.com
11 # Snort bugs: bugs@snort.org
12 #
13 # Compatible with Snort Versions:
14 # VERSIONS : 2.9.20
15 #
16 # Snort build options:
17 # OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm
--enable-perfprofiling --enable-libs --enable-active-response --enable-normalizer
--enable-reload --enable-react --enable-flexresp
18 #
19 # Additional information:
20 # This configuration file enables active response, to run snort in
21 # test mode -T you are required to supply an interface -i <interface>
22 # or test mode will fail to fully validate the configuration and
23 # exit with a FATAL error
24 #
25 #####
26 # This file contains a sample snort configuration.
27 # You should take the following steps to create your own custom configuration:
28 #
29 # 1) Set the network variables.
30 # 2) Configure the decoder
31 # 3) Configure the base detection engine
32 # 4) Configure dynamic loaded libraries
33 # 5) Configure preprocessors
34 # 6) Configure output plugins
35 # 7) Customize your rule set
36 # 8) Configure shared object rule set
37 # 9) Customize shared object rule set
38 #####
39 #
40 # Step #1: Set the network variables. For more information, see README.variables
41 #
42 #####
43 #
44 # Setup the network addresses you are protecting
```

Слева: Текстовый редактор Sublime Text с открытым файлом C:/Snort/etc/snort.conf. Правее: Стартовое меню Windows с доступом к интернету, почте и т.д. Внизу: Панель задач с часами и датой (21:20, 05.12.2023).

Зададим корректный путь в строках 104-106, 113-114:

```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
C:\Snort\etc\snort.conf • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
snort.conf
86 # List of ports you run ftp servers on
87 portvar FTP_PORTS [21,2100,3535]
88
89 # List of ports you run SIP servers on
90 portvar SIP_PORTS [5060,5061,5600]
91
92 # List of file data ports for file inspection
93 portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
94
95 # List of GTP ports for GTP preprocessor
96 portvar GTP_PORTS [2123,2152,3386]
97
98 # other variables, these should not be modified
99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179.0/24,205.188.248.0/24]
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users: You are advised to make this an absolute path,
103 # such as: c:\snort\rules
104 var RULE_PATH c:\snort\rules
105 var SO_RULE_PATH c:\snort\so_rules
106 var PREPROC_RULE_PATH c:\snort\preproc_rules
107
108 # If you are using reputation preprocessor set these
109 # Currently there is a bug with relative paths, they are relative to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG 89986
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH c:\snort\rules
114 var BLACK_LIST_PATH c:\snort\rules
115
116 #####
```

Line 88, Column 1      Spaces: 4      Plain Text

21:27      РУС      05.12.2023      2

Теперь необходимо указать путь для папки Log-файлов, куда Snort будет записывать все логи, доступные для просмотра и изучения. Отредактируем 186 строку:

The screenshot shows a Windows 10 desktop environment within an Oracle VM VirtualBox window. A Sublime Text editor is open, displaying the 'snort.conf' configuration file. The file contains various directives for Snort, such as traffic types, log directories, and detection engines. A specific line, 'config logdir: c:\snort\log', is highlighted with a yellow selection bar. The status bar at the bottom of the Sublime Text window indicates 'Line 186, Column 28'. The system tray shows the date and time as 05.12.2023 21:30.

```
163 #
164 # <type> ::= pcap | afgang | dump | nfq | ipq | ipfw
165 # <mode> ::= read-file | passive | inline
166 # <var> ::= arbitrary <name>=<value passed to DAQ
167 # <dir> ::= path as to where to look for DAQ module so's
168
169 # Configure specific UID and GID to run snort as after dropping privs. For more information see snort
# -h command line options
170 #
171 # config set_gid:
172 # config set_uid:
173
174 # Configure default snaplen. Snort defaults to MTU of in use interface. For more information see
README
175 #
176 # config snaplen:
177 #
178
179 # Configure default bpf_file to use for filtering what traffic reaches snort. For more information
see snort -h command line options (-F)
180 #
181 # config bpf_file:
182 #
183
184 # Configure default log directory for snort to log to. For more information see snort -h command
line options (-l)
185 #
186 config logdir: c:\snort\log
187
188
189 #####
190 # Step #3: Configure the base detection engine. For more information, see README.decode
```

Далее отредактируем строки 247, 250, 253:

The screenshot continues from the previous one, showing the same Windows 10 desktop and Sublime Text editor. The 'snort.conf' file is still open, and the user has moved to the next section of the configuration. Lines 247 through 262 are visible, which define dynamic preprocessors and detection engines. The line 'dynamicpreprocessor directory c:\Snort\lib\snort\_dynamicpreprocessor' is highlighted with a yellow selection bar. The status bar at the bottom of the Sublime Text window indicates '8 lines, 300 characters selected'. The system tray shows the date and time as 05.12.2023 21:35.

```
231
232 #config profile_rules: print all, sort avg_ticks
233 #config profile_procs: print all, sort avg_ticks
234
235 #####
236 # Configure protocol aware flushing
237 # For more information see README.stream5
238 #####
239 config paf_max: 16000
240
241 #####
242 # Step #4: Configure dynamic loaded libraries.
243 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
244 #####
245
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 c:\Snort\lib\snort_dynamicrules
254
255 #####
256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 #####
259
260 # GTP Control Channel Preprocessor. For more information, see README.GTP
261 # processor gtp: ports { 2123 3386 2152 }
```

Закомментируем строки 265-269:

```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
C:\Snort\etc\snort.conf • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
snort.conf
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 c:\Snort\lib\snort_dynamicrules
254
255 ######
256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 #####
259
260 # GTP Control Channel Preprocessor. For more information, see README.GTP
261 # preprocessor gtp: ports { 2123 3386 2152 }
262
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
271 # Target-based IP defragmentation. For more information, see README.frag3
272 preprocessor frag3_global: max_frgs 65536
273 preprocessor frag3_engine: policy windows detect_anomalies overlap_limit 10 min_fragment_length 100
timeout 180
274
275 # Target-Based stateful inspection/stream reassembly. For more information, see README.stream5
276 preprocessor stream5_global: track_tcp yes, \
277     track_udp yes, \
278     track_icmp no, \
279     max_tcp 262144, \

```

5 lines, 164 characters selected Microsoft Store Spaces: 4 Plain Text

Windows Start Search Microsoft Store Taskbar 21:36 05.12.2023 Right Ctrl

Отредактируем строки 534-535:

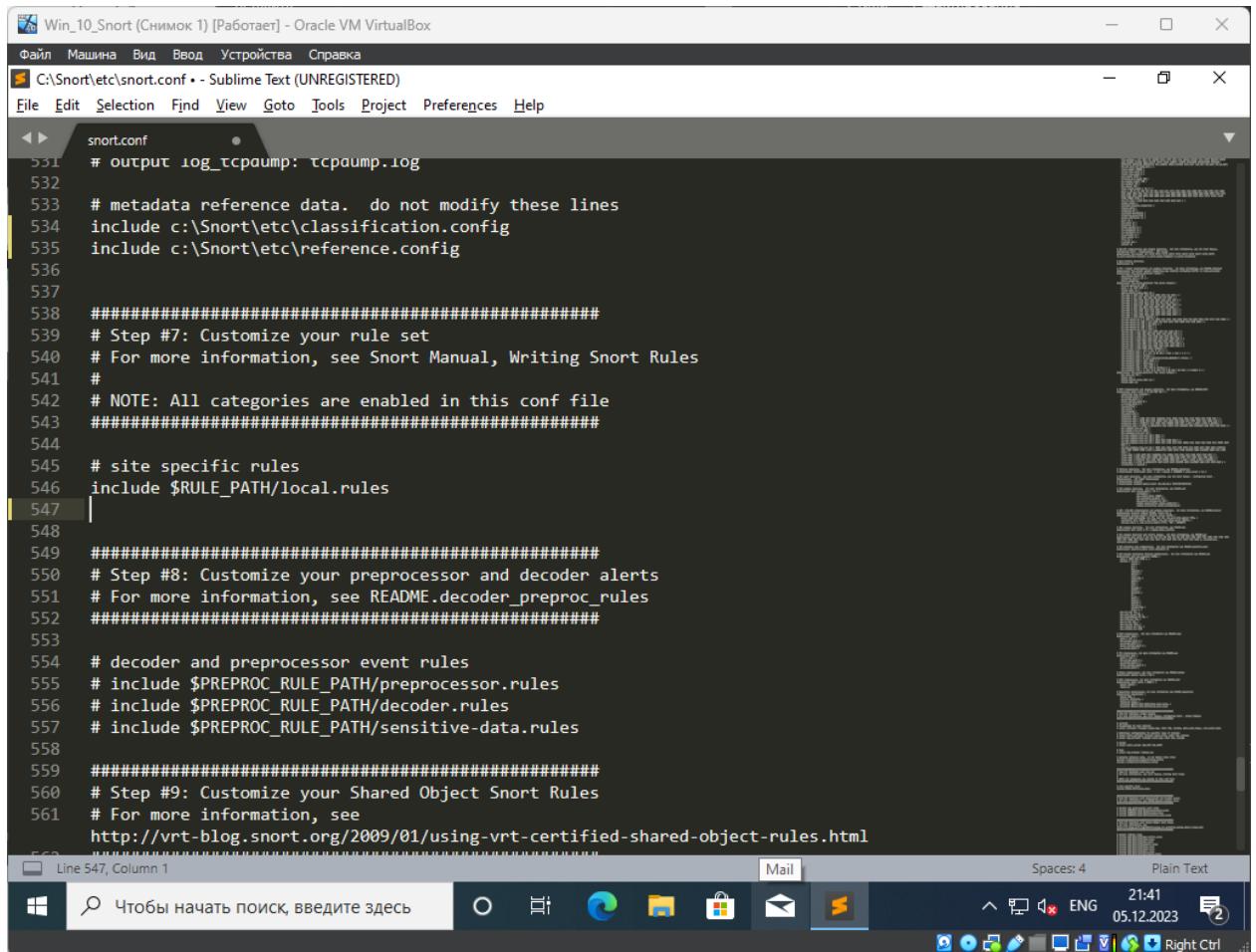
```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
C:\Snort\etc\snort.conf • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
snort.conf
512     blacklist $BLACK_LIST_PATH/black_list.rules
513
514 ######
515 # Step #6: Configure output plugins
516 # For more information, see Snort Manual, Configuring Snort - Output Modules
517 #####
518
519 # unified2
520 # Recommended for most installs
521 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types
522
523 # Additional configuration for specific types of installs
524 # output alert_unified2: filename snort.alert, limit 128, nostamp
525 # output log_unified2: filename snort.log, limit 128, nostamp
526
527 # syslog
528 # output alert_syslog: LOG_AUTH LOG_ALERT
529
530 # pcap
531 # output log_tcpdump: tcpdump.log
532
533 # metadata reference data. do not modify these lines
534 include c:\Snort\etc\classification.config
535 include c:\Snort\etc\reference.config
536
537
538 ######
539 # Step #7: Customize your rule set
540 # For more information, see Snort Manual, Writing Snort Rules
541 #
542 # NOTE: All categories are enabled in this conf file
543 #####

```

2 lines, 60 characters selected Microsoft Store Spaces: 4 Plain Text

Windows Start Search Microsoft Store Taskbar 21:38 05.12.2023 Right Ctrl

Также отредактируем пункт, касающийся подключения правил для IDS Snort. Удалим строки 548-651 и получим следующую картинку:

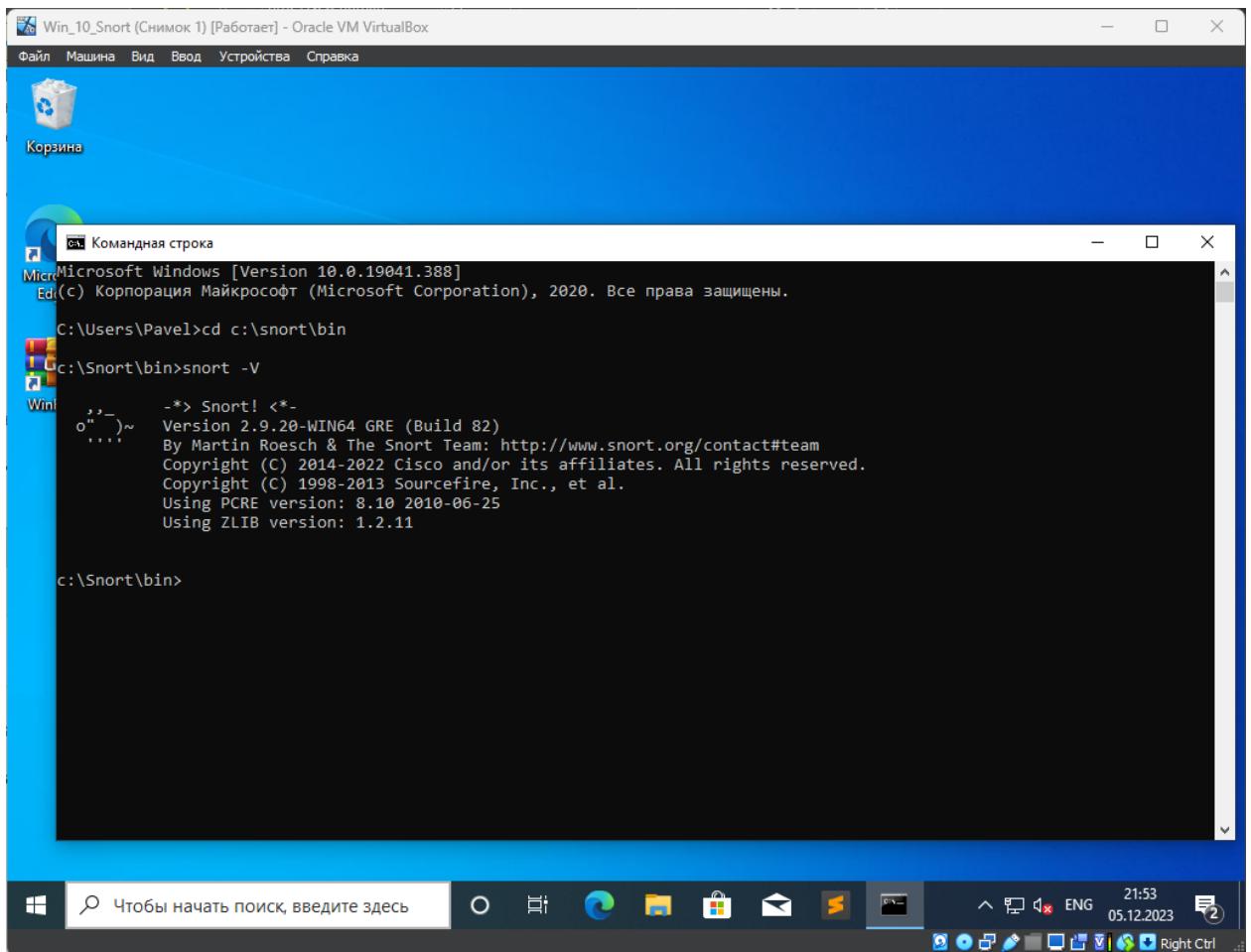


```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
C:\Snort\etc\snort.conf • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

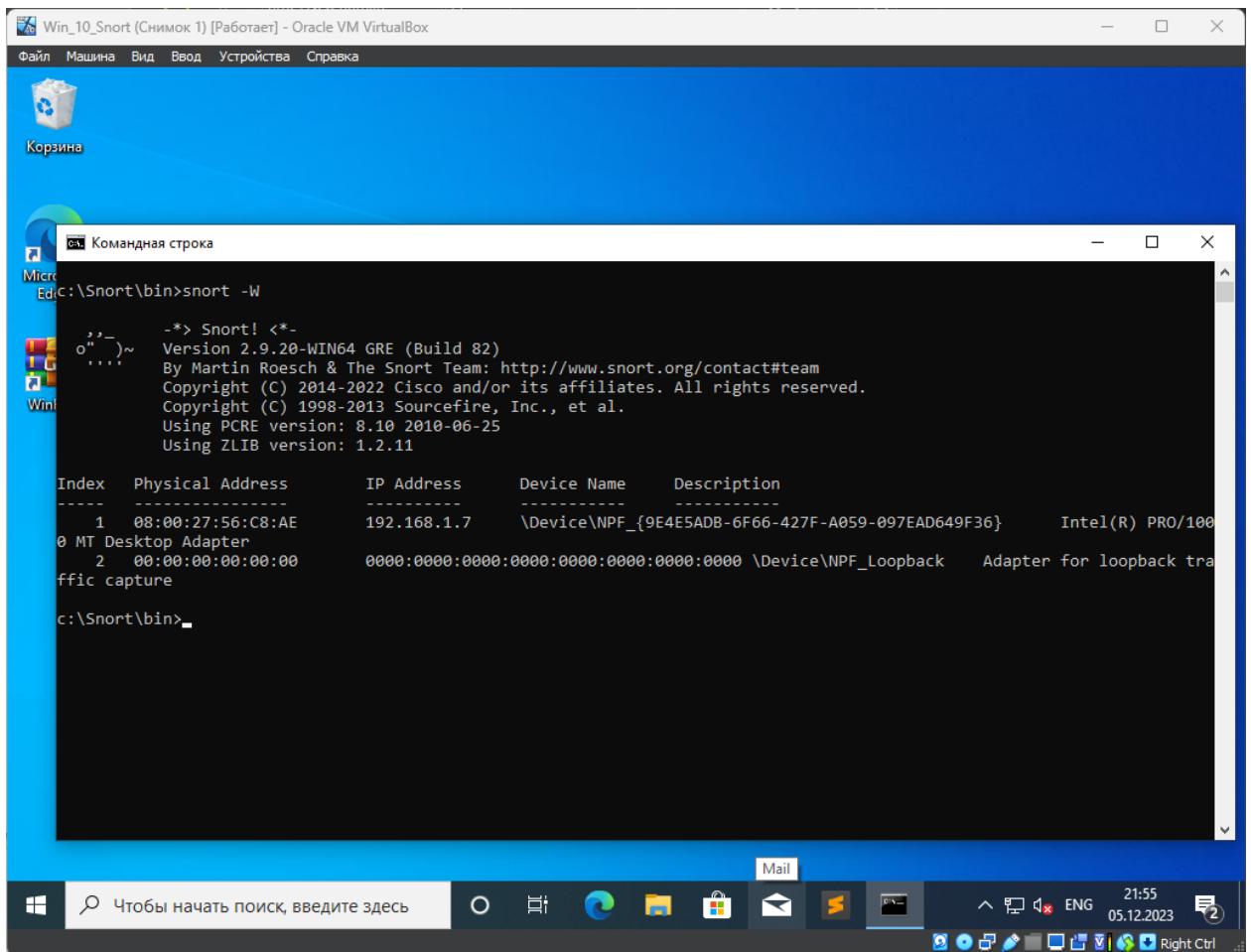
snort.conf
531 # output log_tcpdump: tcpdump.log
532
533 # metadata reference data. do not modify these lines
534 include c:\Snort\etc\classification.config
535 include c:\Snort\etc\reference.config
536
537
538 ##### Step #7: Customize your rule set #####
539 # For more information, see Snort Manual, Writing Snort Rules
540 #
541 #
542 # NOTE: All categories are enabled in this conf file
543 #####
544
545 # site specific rules
546 include $RULE_PATH/local.rules
547
548 #####
549 # Step #8: Customize your preprocessor and decoder alerts
550 # For more information, see README.decoder_preproc_rules
551 #####
552
553
554 # decoder and preprocessor event rules
555 # include $PREPROC_RULE_PATH/preprocessor.rules
556 # include $PREPROC_RULE_PATH/decoder.rules
557 # include $PREPROC_RULE_PATH/sensitive-data.rules
558
559 #####
560 # Step #9: Customize your Shared Object Snort Rules
561 # For more information, see
http://vrt-blog.snort.org/2009/01/using-vrt-certified-shared-object-rules.html

Line 547, Column 1
Spaces: 4 Plain Text
Windows Mail 21:41 05.12.2023 Right Ctrl
```

Конфигурирование файла закончено. Теперь необходимо проверить правильность написанной конфигурации. Для этого переходим в папку C:/Snort/bin используя командную строку и выводим версию IDS Snort:



Просмотрим доступные интерфейсы. В данном случае наиболее подходящим для тестирования является интерфейс сетевой карты (номер 1 на изображении ниже):



Тестируем конфигурацию Snort, вводим команду: snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 1, где ключ -T указывает, что нужно протестировать текущую конфигурацию Snort; ключ -с означает, что включён режим IDS (далее следует путь к конфигурационному файлу snort.conf); ключ -l включает режим записи на жесткий диск с указанием пути к файлу; ключ -i указывает на порядковый номер(index) интересующего нас интерфейса. Тестирование завершено ошибкой, которая указывает на отсутствие файла local.rules:

```
c:\Snort\bin>snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 1
Running in Test mode

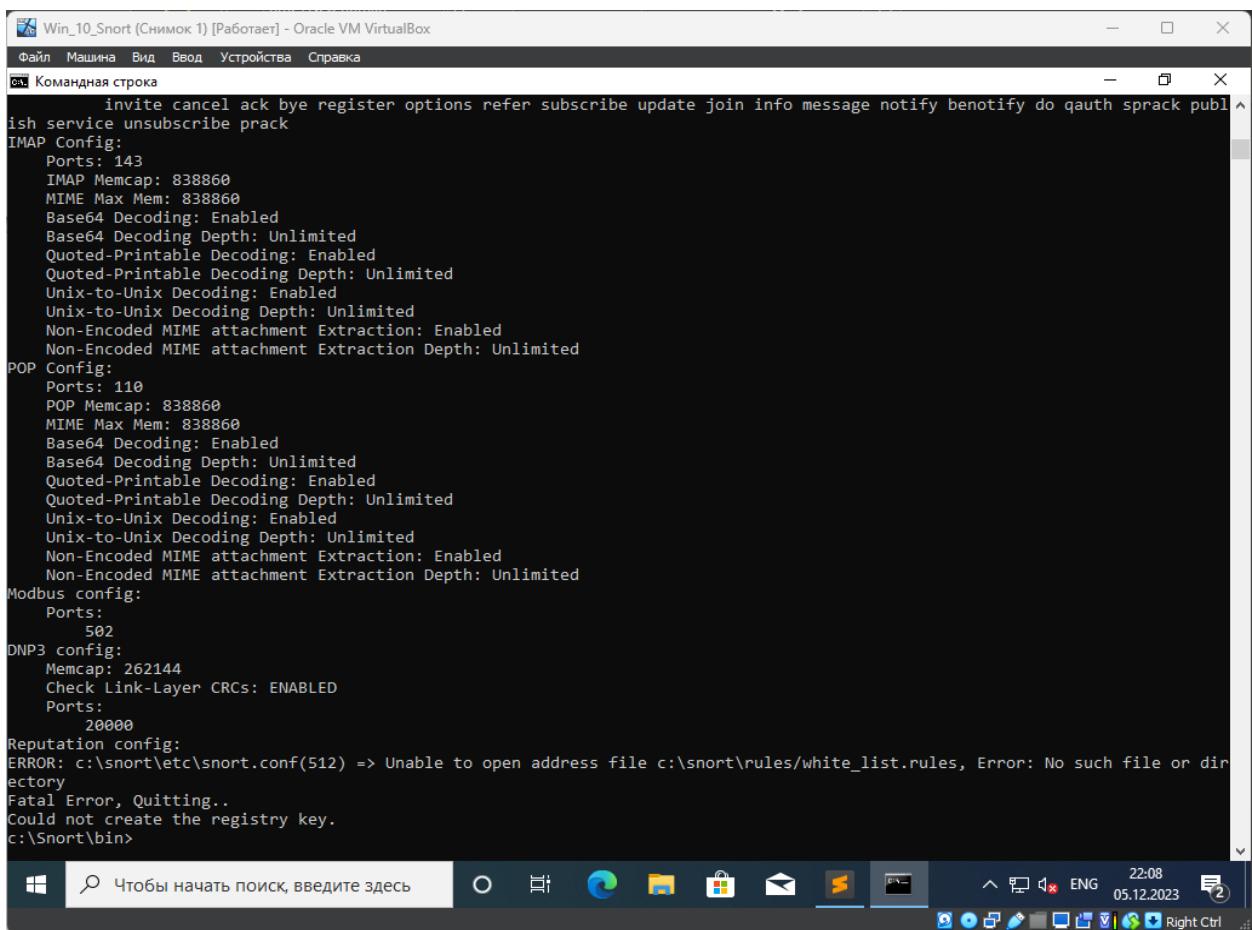
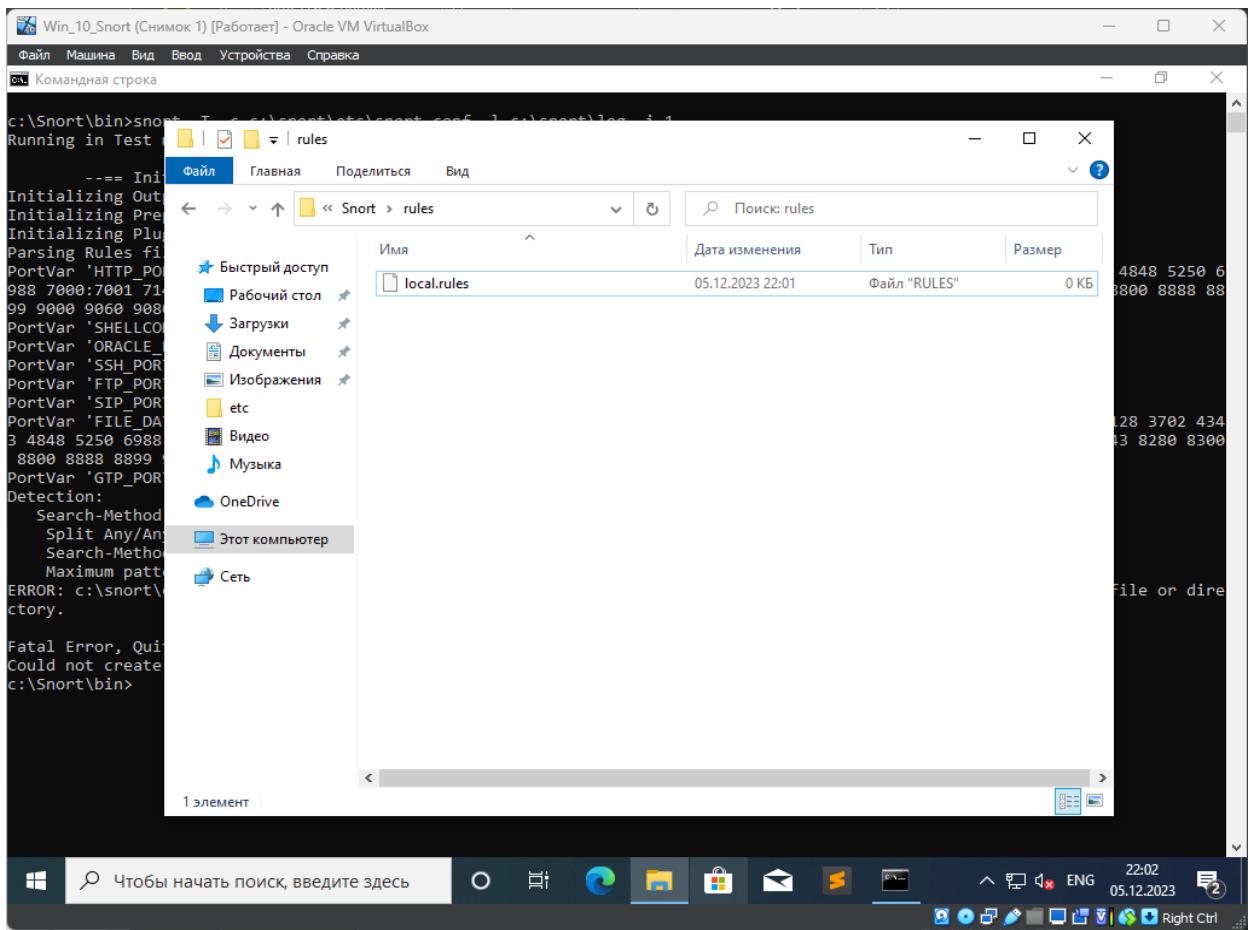
      === Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6
988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 88
99 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 3702 434
3 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 'GTP_PORTS' defined : [ 2123 2152 3386 ]

Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20

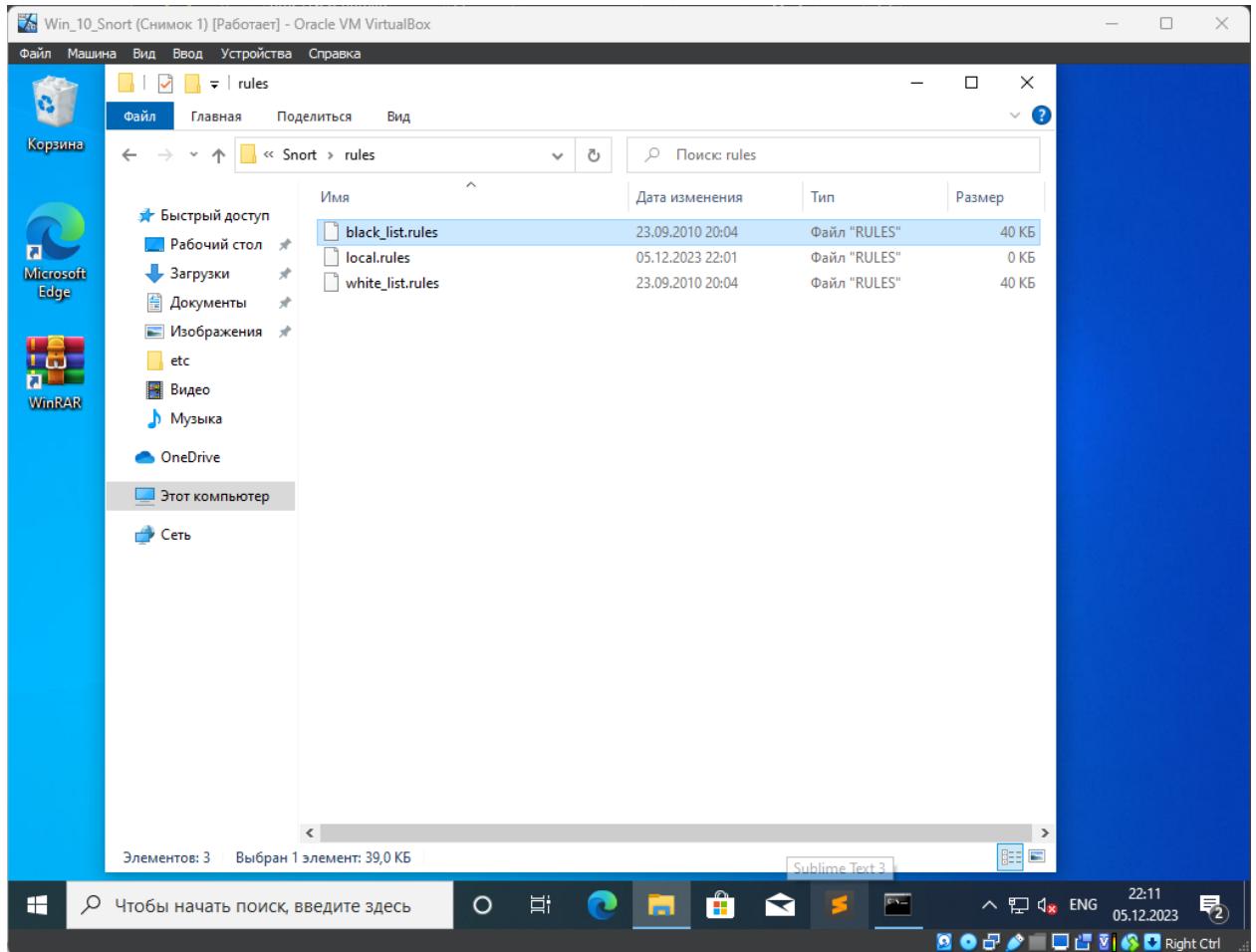
ERROR: c:\snort\etc\snort.conf(253) Could not stat dynamic module path "c:\Snort\lib\snort_dynamicrules": No such file or directory.

Fatal Error, Quitting..
Could not create the registry key.
c:\Snort\bin>
```

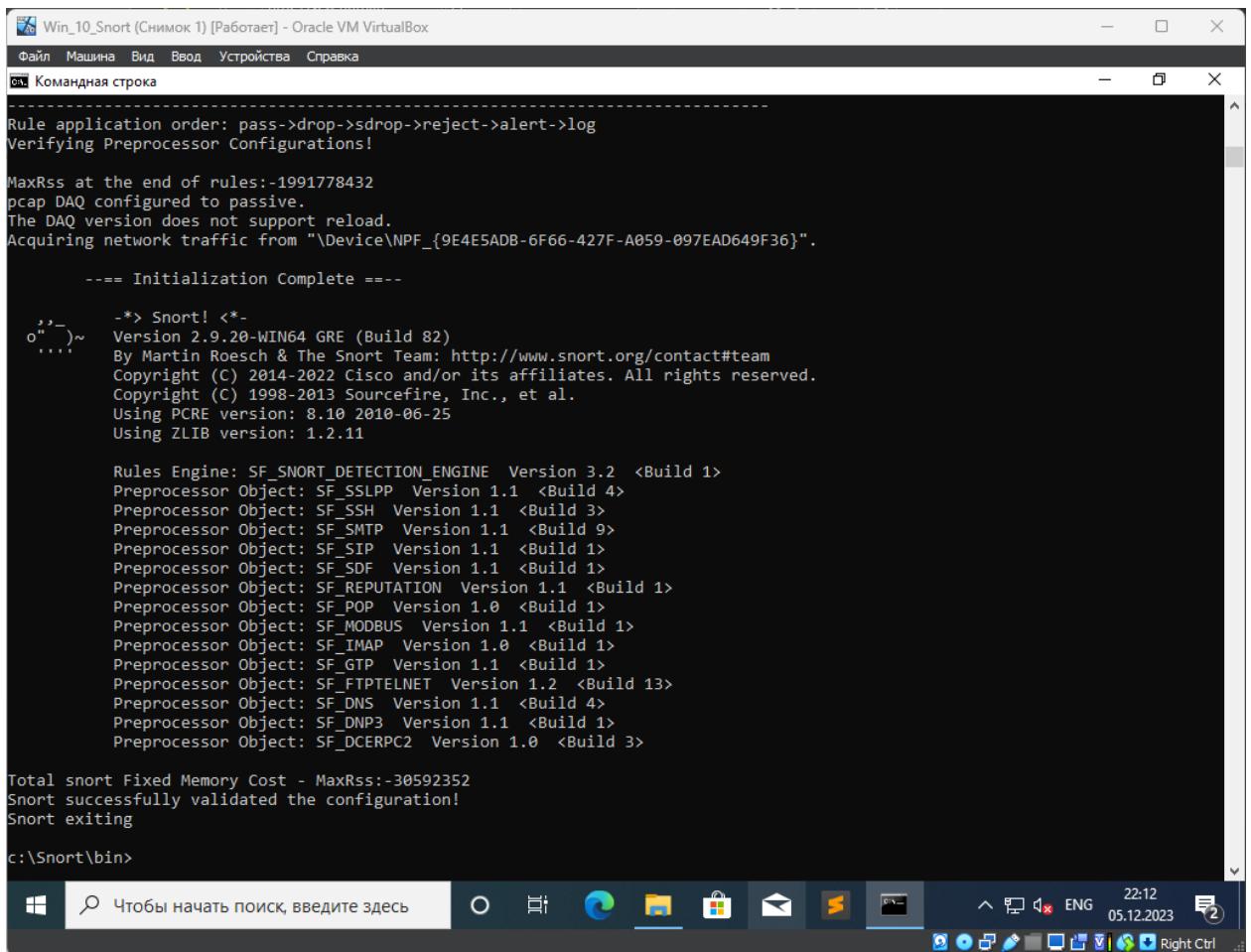
Исправим ошибку. Для этого добавим файл local.rules в папку C:\Snort\rules и снова запустим тестирование:



Увидим, что тестирование снова завершено ошибкой, которая указывает на отсутствие файла `white_list.rules`. Исправим её. Сразу же добавим и файл `black_list.rules`:



Снова запустим тест и убедимся, что ошибок нет:



```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
сн. Командная строка

-----
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!

MaxRss at the end of rules:-1991778432
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{9E4E5ADB-6F66-427F-A059-097EAD649F36}".

    === Initialization Complete ===

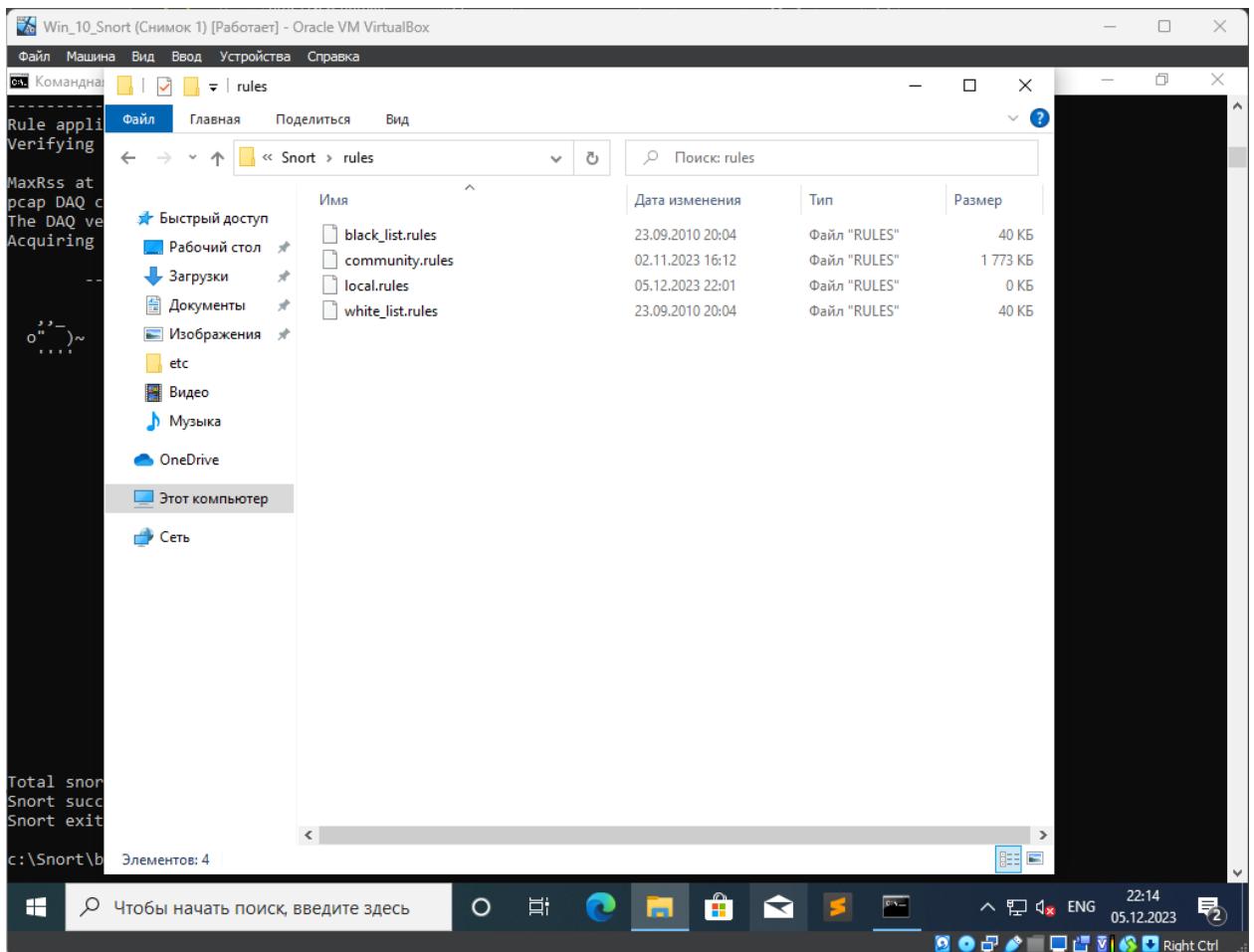
o'''~  -*> Snort! <*-
    Version 2.9.20-WIN64 GRE (Build 82)
    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using PCRE version: 8.10 2010-06-25
    Using ZLIB version: 1.2.11

    Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
    Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
    Preprocessor Object: SF_SSH Version 1.1 <Build 3>
    Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
    Preprocessor Object: SF_SIP Version 1.1 <Build 1>
    Preprocessor Object: SF_SDF Version 1.1 <Build 1>
    Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
    Preprocessor Object: SF_POP Version 1.0 <Build 1>
    Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
    Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
    Preprocessor Object: SF_GTP Version 1.1 <Build 1>
    Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
    Preprocessor Object: SF_DNS Version 1.1 <Build 4>
    Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
    Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>

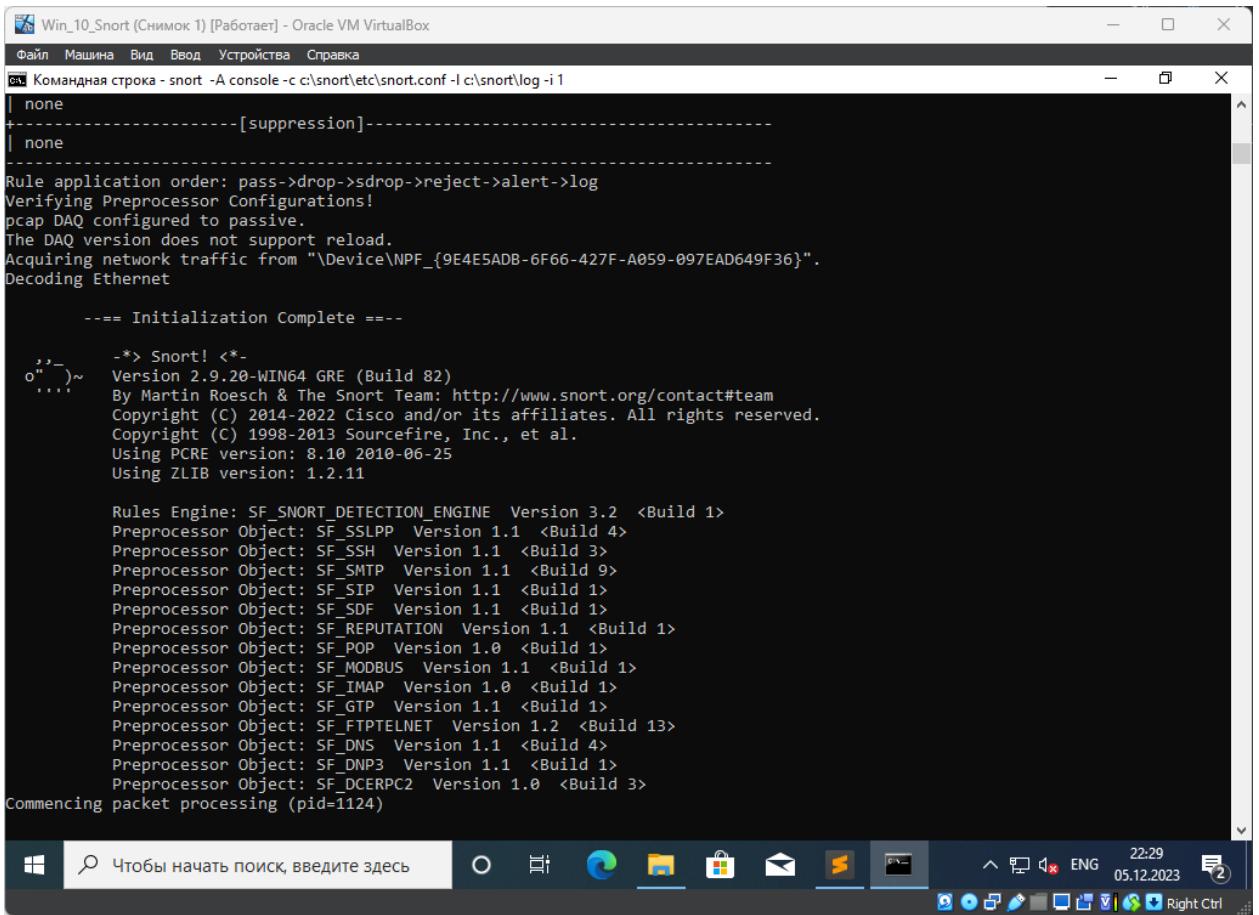
Total snort Fixed Memory Cost - MaxRss:-30592352
Snort successfully validated the configuration!
Snort exiting

c:\Snort\bin>
```

Теперь добавим ещё один файл с правилами community.rules:



Запускаем Snort в режиме IDS, введя данную команду в командной строке: `snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 1`. Новый ключ “-A” показывает, что все предупреждения (alerts) будут дублироваться выводом на консоль. Snort проверил файл конфигурации и начал свою работу в режиме IDS:



```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
snort: Командная строка - snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 1
| none
+-----[suppression]-----
| none

Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{9E4E5ADB-6F66-427F-A059-097EAD649F36}".
Decoding Ethernet

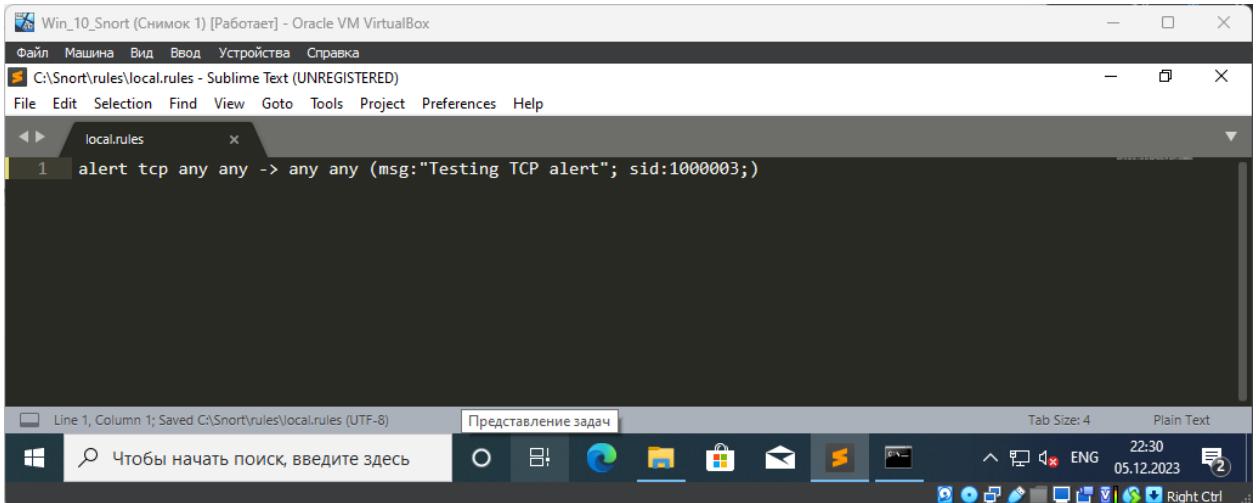
==== Initialization Complete ====

-*> Snort! <*-
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 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

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>

Commencing packet processing (pid=1124)
```

Теперь напишем правило (отредактируем файл local.rules), которое позволит генерировать предупреждение при обнаружении любых TCP пакетов от любого источника к любому назначению, с сообщением 'Testing TCP alert' и идентификатором сигнала 1000003:



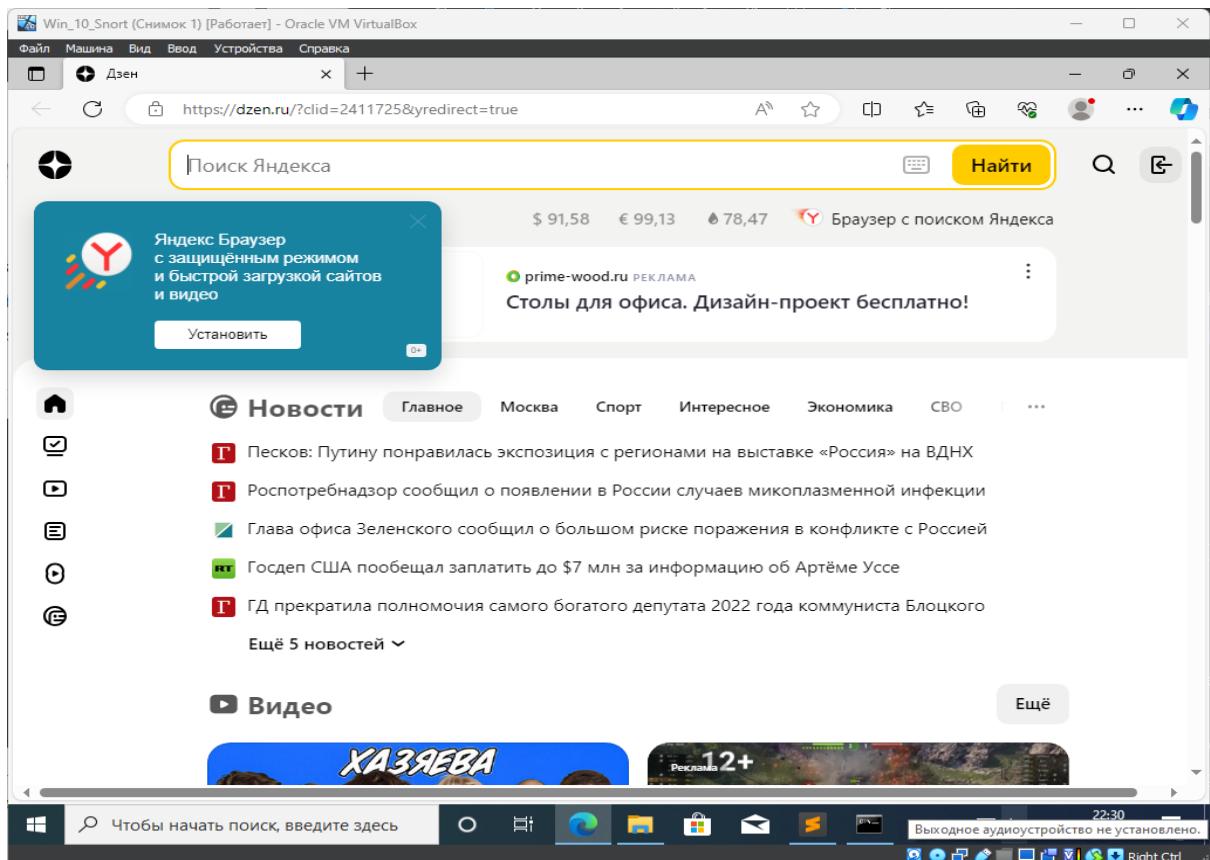
```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
C:\Snort\rules\local.rules - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
local.rules
1 alert tcp any any -> any any (msg:"Testing TCP alert"; sid:1000003;)

Line 1, Column 1; Saved C:\Snort\rules\local.rules (UTF-8) Представление задач Tab Size: 4 Plain Text
Windows 10_Snort 22:30 ENG 05.12.2023 Right Ctrl
```

Поясним записи:

- ❖ alert – это действие, которое предписывает системе генерировать предупреждение при срабатывании данного правила;
- ❖ tcp – это протокол, к которому применяется правило, в данном случае, это TCP (Transmission Control Protocol), один из основных протоколов передачи данных интернета;
- ❖ первая запись “any any” – эти части указывают исходный IP-адрес и порт отправителя (“any” означает “любой”, то есть правило применяется ко всем исходящим IP-адресам и портам);
- ❖ – эта часть разделяет данные об исходе (source) и данных о назначении (destination);
- ❖ вторая запись “any any” – эти части указывают на IP-адрес и порт назначения;
- ❖ (msg:"Testing TCP alert"; sid:1000003;) – это дополнительная информация к правилу. Здесь msg указывает на сообщение или описание правила, в данном случае, это "Testing TCP alert". Идентификатор сигнала sid представляет собой уникальный числовой идентификатор этого правила в рамках системы IDS/IPS.

Снова запускаем Snort в режиме IDS, введя данную команду в командной строке: snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 1. Для проверки работы данного правила выйдем в сеть интернет и перейти по любому адресу, после этого в командной строке появится уведомление о срабатывании данного правила:



```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Дзен
https://dzen.ru/?clid=2411725&yredirect=true
Поиск Яндекса Найти
Яндекс Браузер с защищенным режимом и быстрой загрузкой сайтов и видео Установить
$ 91,58 € 99,13 ₽ 78,47 Браузер с поиском Яндекса
prime-wood.ru РЕКЛАМА Столы для офиса. Дизайн-проект бесплатно!
Новости Главное Москва Спорт Интересное Экономика СВО ...
Песков: Путину понравилась экспозиция с регионами на выставке «Россия» на ВДНХ
Роспотребнадзор сообщил о появлении в России случаев микоплазменной инфекции
Глава офиса Зеленского сообщил о большом риске поражения в конфликте с Россией
Госдеп США пообещал заплатить до $7 млн за информацию об Артёме Уссе
ГД прекратила полномочия самого богатого депутата 2022 года коммуниста Блоцкого
Ещё 5 новостей ▾
Видео Ещё
ХАЗЯЕВА
Чтобы начать поиск, введите здесь
О: Выходное аудиоустройство не установлено.
22:30
Right Ctrl
```

Win\_10\_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

cmd. Командная строка - snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 1

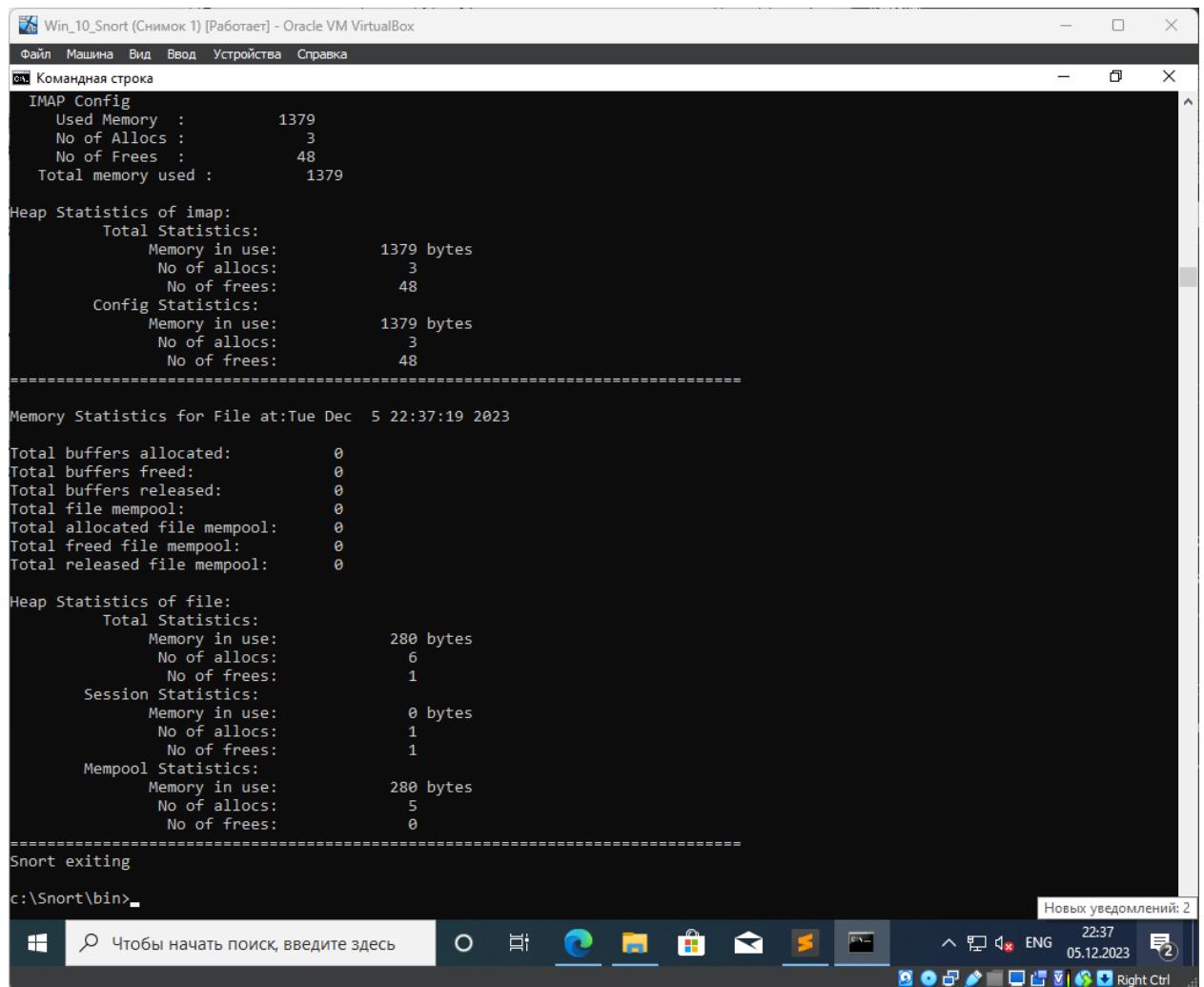
```
43 -> 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:49931
12/05-22:30:59.961639 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a00:1148:db00:0000:0000:0000:0000:0026:4
43 -> 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:49931
12/05-22:30:59.961675 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:4
9931 -> 2a00:1148:db00:0000:0000:0000:0000:0026:443
12/05-22:31:00.064338 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 87.250.254.106:443 -> 192.168.1.7:49880
12/05-22:31:00.159101 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 62.217.160.5:443 -> 192.168.1.7:49900
12/05-22:31:00.209261 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:4
9931 -> 2a02:06b8:0000:0000:0000:0000:0000:0090:443
12/05-22:31:00.222052 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a02:06b8:0000:0000:0000:0000:0000:0090:4
43 -> 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:49901
12/05-22:31:00.310567 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 62.217.160.5:443 -> 192.168.1.7:49907
12/05-22:31:00.318643 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:4
9908 -> 2a02:06b8:0020:0000:0000:0000:0000:0215:443
12/05-22:31:00.332220 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a02:06b8:0020:0000:0000:0000:0000:0215:4
43 -> 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:49908
12/05-22:31:00.368605 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 87.240.129.133:443 -> 192.168.1.7:49906
12/05-22:31:00.412325 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:4
9910 -> 2a02:06b8:0000:0000:0000:0000:0000:0000:443
12/05-22:31:00.419493 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a02:06b8:000a:0000:0000:0000:0000:000a:4
43 -> 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:49910
12/05-22:31:00.430290 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 87.240.129.135:443 -> 192.168.1.7:49909
12/05-22:31:00.615109 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:4
9915 -> 2620:01ec:0c11:0000:0000:0000:0200:443
12/05-22:31:00.644924 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2620:01ec:0c11:0000:0000:0000:0000:0200:4
43 -> 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:49915
12/05-22:31:00.651360 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 62.217.161.40:443 -> 192.168.1.7:49913
12/05-22:31:00.714030 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 62.217.161.39:443 -> 192.168.1.7:49922
12/05-22:31:00.715129 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 62.217.161.69:443 -> 192.168.1.7:49926
12/05-22:31:00.729883 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 62.217.161.71:443 -> 192.168.1.7:49927
12/05-22:31:00.742237 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 204.79.197.203:443 -> 192.168.1.7:49921
12/05-22:31:00.813299 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 68.219.88.97:443 -> 192.168.1.7:49914
12/05-22:31:00.845671 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 62.217.160.4:443 -> 192.168.1.7:49889
12/05-22:31:00.929835 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 23.38.98.53:443 -> 192.168.1.7:49917
12/05-22:31:01.090386 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.5:8009 -> 192.168.1.7:49929
12/05-22:31:01.881953 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:4
9931 -> 2a00:1148:db00:0000:0000:0000:0000:0026:443
12/05-22:31:01.882002 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:4
9931 -> 2a00:1148:db00:0000:0000:0000:0000:0026:443
12/05-22:31:01.888612 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a00:1148:db00:0000:0000:0000:0000:0026:4
43 -> 2a00:1370:8186:2f6f:9d57:5208:9ae4:bdfe:49931
12/05-22:31:01.895140 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 87.250.254.106:443 -> 192.168.1.7:49896
12/05-22:31:01.920964 [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 87.250.254.106:443 -> 192.168.1.7:49896
```

## Вопрос 2. Разработка правил для IDS Snort

Номер строки с фамилией в файле равен 4, если поделить 4 на 10 (количество заданий), то остаток будет равен 4. Прибавляем к 4 единицу и получаем номер варианта = 5.

Таким образом, необходимо создать правило для Snort, которое срабатывает при обнаружении всех входящих tcp-пакетов с конкретного сайта с выводом соответствующего сообщения.

Прервём работу IDS Snort комбинацией клавиш “Ctrl+c”:



```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машинка Вид Ввод Устройства Справка
сн Командная строка

IMAP Config
Used Memory : 1379
No of Allocs : 3
No of Frees : 48
Total memory used : 1379

Heap Statistics of imap:
Total Statistics:
Memory in use: 1379 bytes
No of allocs: 3
No of frees: 48
Config Statistics:
Memory in use: 1379 bytes
No of allocs: 3
No of frees: 48
=====
Memory Statistics for File at:Tue Dec 5 22:37:19 2023

Total buffers allocated: 0
Total buffers freed: 0
Total buffers released: 0
Total file mempool: 0
Total allocated file mempool: 0
Total freed file mempool: 0
Total released file mempool: 0

Heap Statistics of file:
Total Statistics:
Memory in use: 280 bytes
No of allocs: 6
No of frees: 1
Session Statistics:
Memory in use: 0 bytes
No of allocs: 1
No of frees: 1
Mempool Statistics:
Memory in use: 280 bytes
No of allocs: 5
No of frees: 0
=====
Snort exiting
c:\Snort\bin>
```

Предположим, мы хотим получать уведомления о входящих tcp-пакетах с сайта <https://tsvetology.ru>. Сперва узнаем какой ip-адреса разолвится (это можно сделать с помощью утилиты nslookup):

```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
C:\Snort\rules\local.rules - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
с: Командная строка
1
2 C:\Users\Pavel>nslookup tsvetology.ru
    Трасса: gpon.net
    Address: 192.168.1.1
    Не заслуживающий доверия ответ:
    Имя : tsvetology.ru
    Address: 2.59.41.155

C:\Users\Pavel>
```

Line 2, Column 18      Tab Size: 4      Plain Text

Теперь напишем правило (указан 443 порт, т.к. используется протокол https; 192.168.1.7 – это адрес, где установлен IDS Snort):

```
Win_10_Snort (Снимок 1) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
C:\Snort\rules\local.rules - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
local.rules
1 # alert tcp any any -> any any (msg:"Testing TCP alert"; sid:1000003;
2 alert tcp 2.59.41.155 443 -> 192.168.1.7 any (msg:"An incoming package from the website https://tsvetology.ru"; sid:1000004;)

Line 2, Column 97      Tab Size: 4      Plain Text
```

Снова запустим IDS Snort, перейдём на сайт <https://tsvetology.ru> и увидим оповещения:

