



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

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

Отчет по практической работе №6
по дисциплине: «Управление информационной безопасностью»
на тему: «Настройка параметров системы обнаружения атак»

Группа:
ББМО-02-22
Выполнил:
Щелкушкин Е.Р.

Проверил:
Пимонов Р.В.

Москва, 2023

Содержание

Введение	3
Вопрос 1. Установка и настройка параметров IDS Snort.....	3
Вопрос 2. Разработка правил для IDS Snort	14
Заключение	16

Введение

Цель работы: Настройка параметров системы обнаружения атак.

Задачи:

- Установка и настройка параметров IDS Snort.
- Разработка правил для IDS Snort.

Вопрос 1. Установка и настройка параметров IDS Snort

Для выполнения задания необходимо скачать архив с требуемым ПО по ссылке: <https://1drv.ms/u/s!AlN4iiJAxsjbgVMVo5Ha-52vbvT9?e=YbZNad>

Подготовительная часть для работы IDS Snort:

1. Установка npcap-1.78.exe.

Запускаем exe файл и устанавливаем npcар (рис. 1-2).

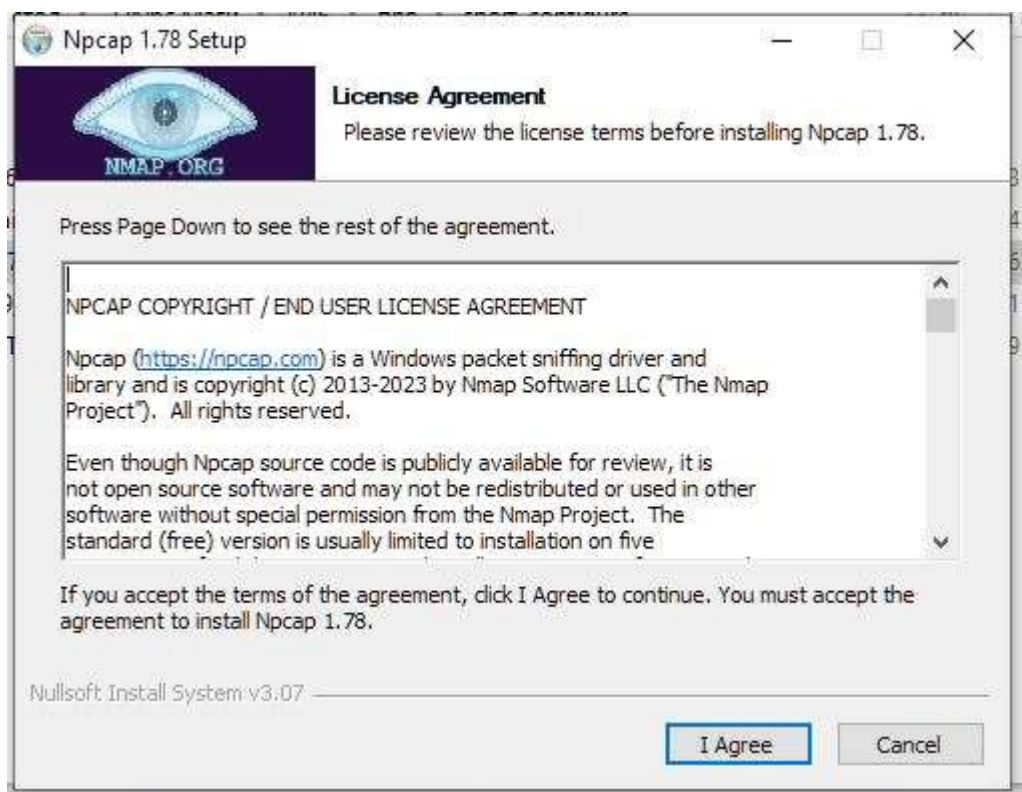


Рисунок 1 – Установка Npcap

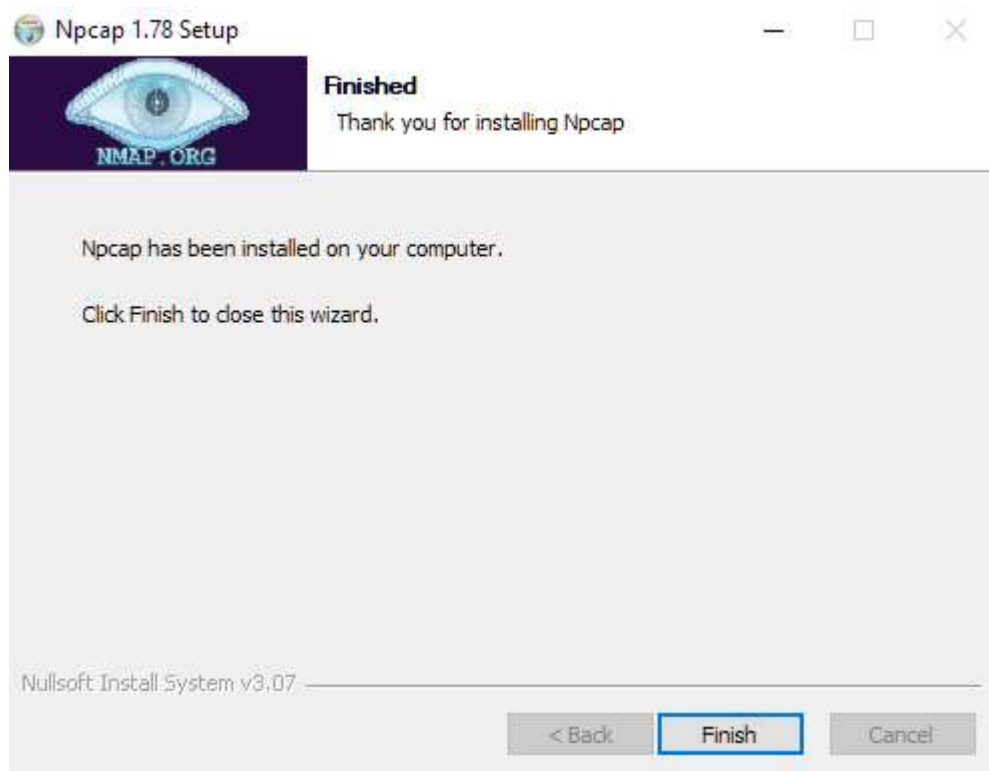


Рисунок 2 – Установка Npcap

2. Установка IDS Snort. Запускаем файл Snort_2_9_20_Installer.x64.exe и устанавливаем Snort (рис. 3).

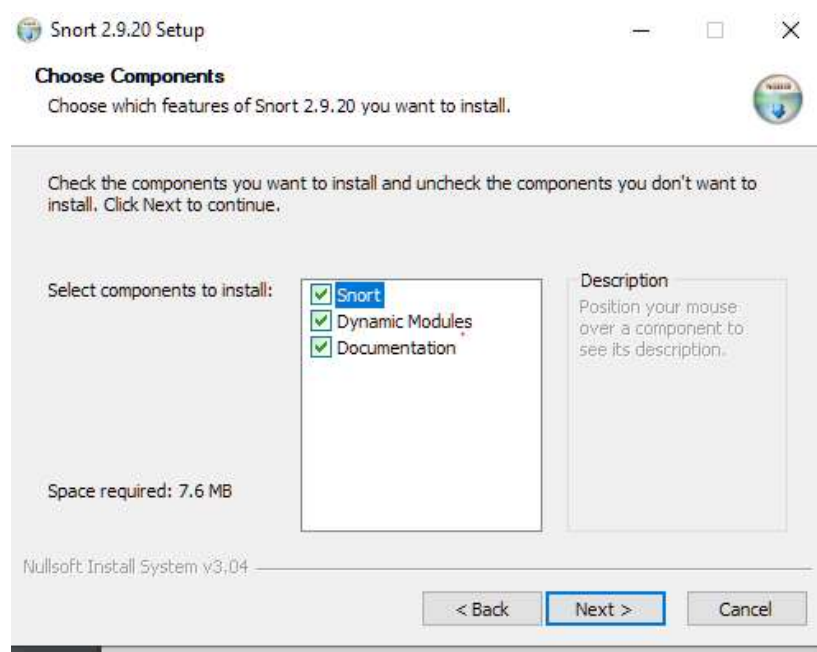
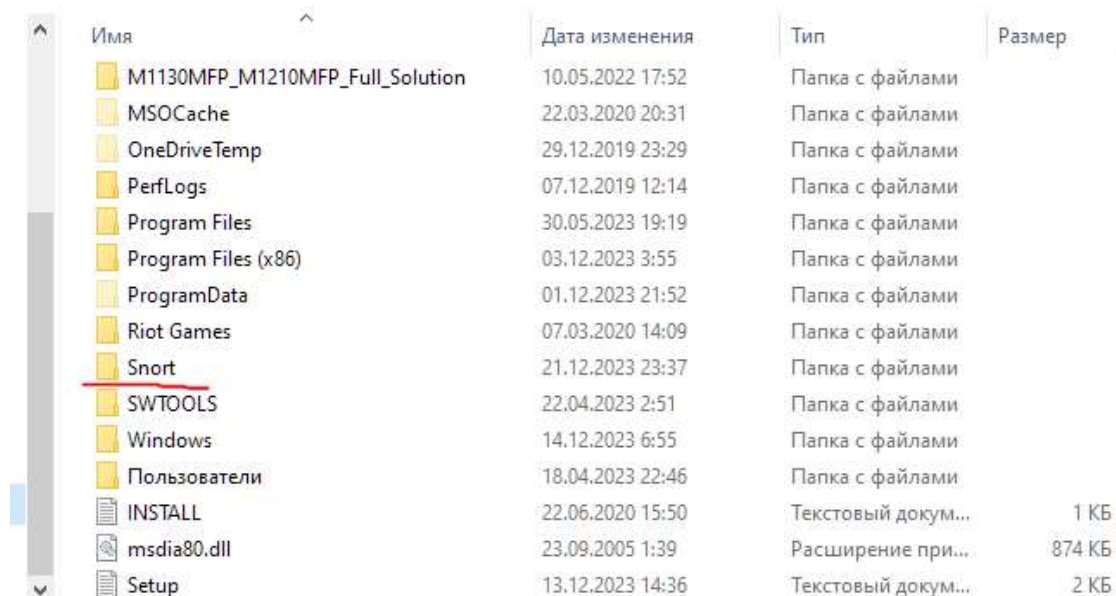


Рисунок 3 – Установка Snort

После установки в диске C:/ появится папка с файлами программы (рис. 4).

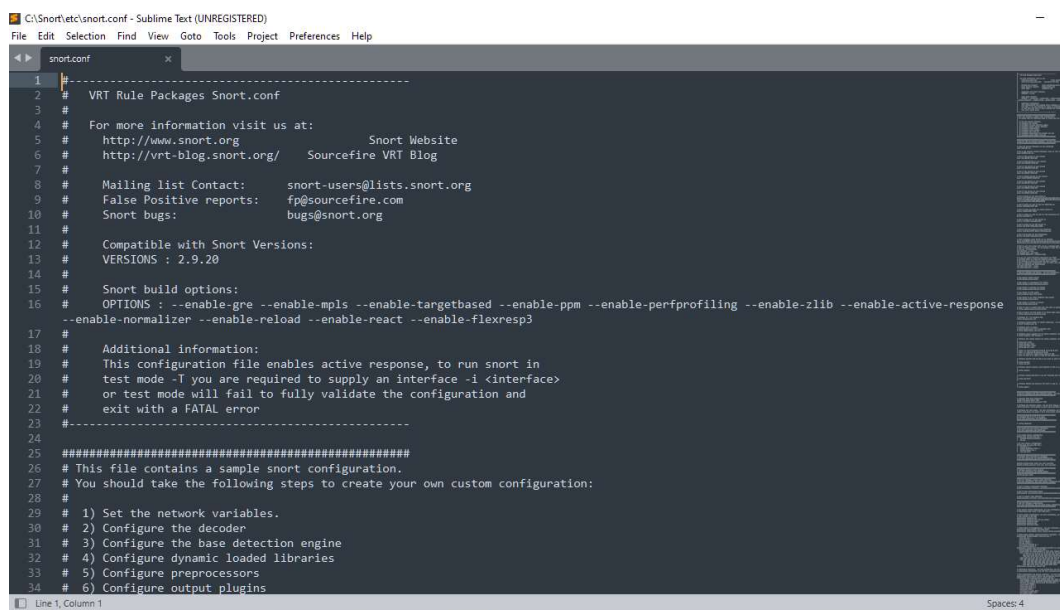


Имя	Дата изменения	Тип	Размер
M1130MFP_M1210MFP_Full_Solution	10.05.2022 17:52	Папка с файлами	
MSOCache	22.03.2020 20:31	Папка с файлами	
OneDriveTemp	29.12.2019 23:29	Папка с файлами	
PerfLogs	07.12.2019 12:14	Папка с файлами	
Program Files	30.05.2023 19:19	Папка с файлами	
Program Files (x86)	03.12.2023 3:55	Папка с файлами	
ProgramData	01.12.2023 21:52	Папка с файлами	
Riot Games	07.03.2020 14:09	Папка с файлами	
Snort	21.12.2023 23:37	Папка с файлами	
SWTOOLS	22.04.2023 2:51	Папка с файлами	
Windows	14.12.2023 6:55	Папка с файлами	
Пользователи	18.04.2023 22:46	Папка с файлами	
INSTALL	22.06.2020 15:50	Текстовый докум...	1 КБ
msdia80.dll	23.09.2005 1:39	Расширение при...	874 КБ
Setup	13.12.2023 14:36	Текстовый докум...	2 КБ

Рисунок 4 – директория Snort

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 (рис. 5).



```
snort.conf
1
2 # VRT Rule Packages Snort.conf
3 #
4 # For more information visit us at:
5 # http://www.snort.org           Snort Website
6 # http://vrt-blog.snort.org/     Sourcefire VRT Blog
7 #
8 # Mailing list Contact:  snort-users@lists.snort.org
9 # False Positive reports: fp@sourcefire.com
10 # Snort bugs:           bugs@snort.org
11 #
12 # Compatible with Snort Versions:
13 # VERSIONS : 2.9.20
14 #
15 # Snort build options:
16 # OPTIONS : --enable-gre --enable-mpis --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --enable-active-response
17 #           --enable-normalizer --enable-reload --enable-react --enable-flexresp3
18 #
19 # Additional information:
20 # This configuration file enables active response, to run snort in
21 # test mode -i 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
```

Рисунок 5 – Конфигурационный файл Snort (1)

Переходим к строкам 104-106 и вместо `..\` прописываем `c:\snort\`.

Тоже самое делаем в строках 113-114 (рис. 6).

```
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.
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 #####
117 # Step #2: Configure the decoder. For more information, see README.decode
118 #####
119
120 # Stop generic decode events:
121 config disable_decode_alerts
122
123 # Stop Alerts on experimental TCP options
124 config disable_tcpopt_experimental_alerts
```

Рисунок 6 – Конфигурационный файл Snort (2)

Теперь необходимо указать путь для папки Log-файлов, куда Snort будет записывать все логи, доступные для просмотра и изучения. Редактируем пути к лог-файлам.

В папке `C:/snort` уже есть папка `log`, для этого предназначенная, поэтому прописываем путь `C:\snort\log`.

На строчке 186 прописываем в `config logdir: c:\snort\log`. Также необходимо удалить символ `" # "`, который выбрасывает строки из исполняемого файла, превращая их в комментарий. Результат (рис. 7):

```
182 #
183
184 # Configure default log directory for snort to log t
185 #
186 config logdir: c:\snort\log
187
188
189 #####
190 # Step #3: Configure the base detection engine. For
191 #####
192
```

Рисунок 7 – Конфигурационный файл Snort (3)

Строки 246-253 необходимо прописать так, как показано на изображении ниже (рис. 8):

```
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 #####
```

Рисунок 8 – Конфигурационный файл Snort (4)

Продолжаем редактирование. Теперь комментируем, добавляя знаки комментария " # " к строкам 259-265. В отредактированном варианте это выглядит так (рис. 9):

```
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 #####
259
260 # GTP Control Channle 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: label any from 65536
```

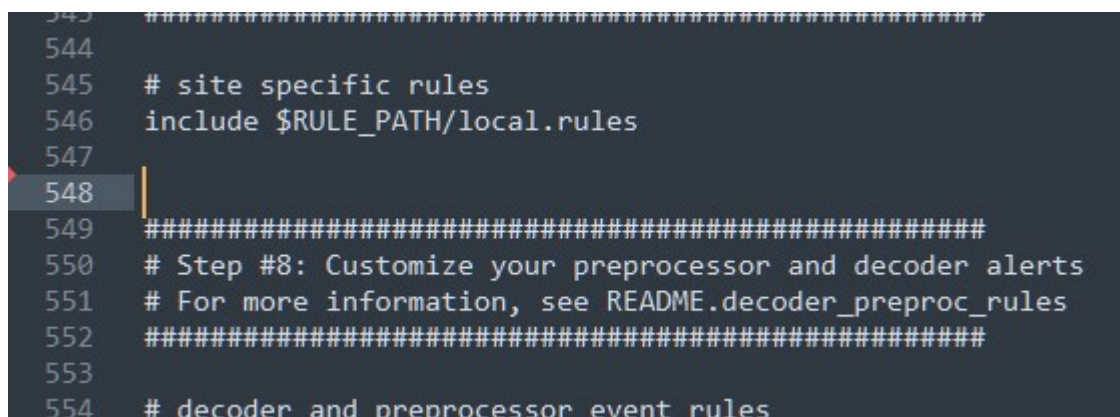
Рисунок 9 – Конфигурационный файл Snort (5)

Также необходимо раскомментировать строки 534-535, убрав знак # (рис. 10).

```
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
```

Рисунок 10 – Конфигурационный файл Snort (6)

Также отредактируем пункт, касающийся подключения правил для IDS Snort. Удалим строки 548-651 (рис. 11).



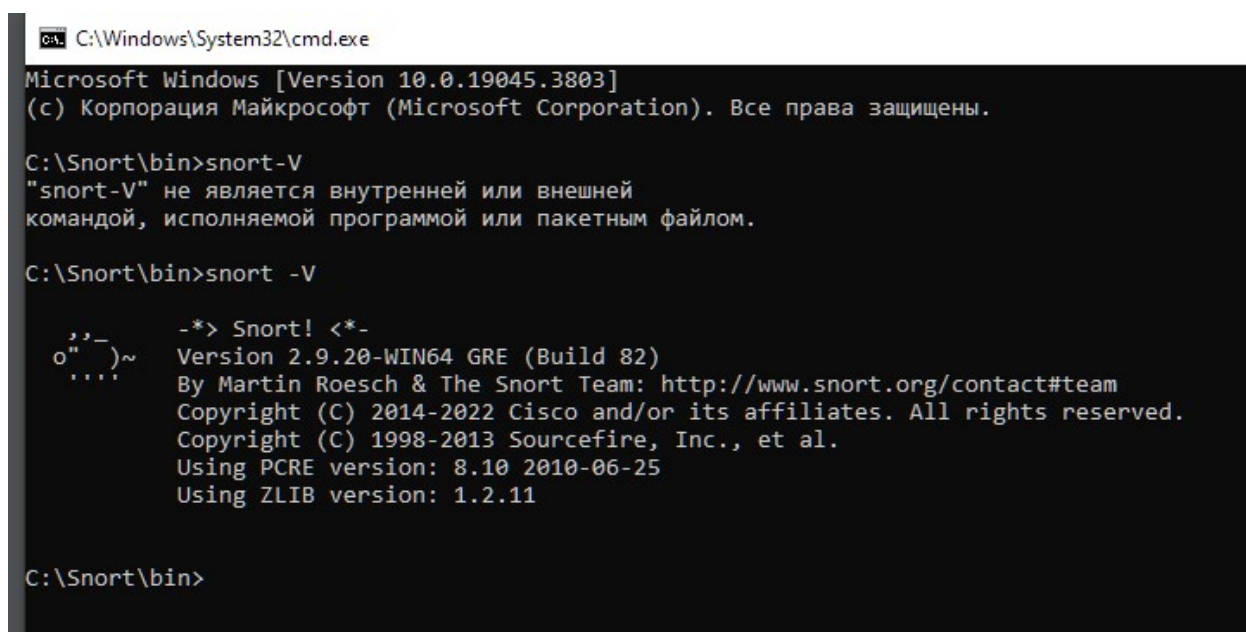
```
544
545 # site specific rules
546 include $RULE_PATH/local.rules
547
548
549 #####
550 # Step #8: Customize your preprocessor and decoder alerts
551 # For more information, see README.decoder_preproc_rules
552 #####
553
554 # decoder and preprocessor event rules
```

Рисунок 11 – Конфигурационный файл Snort (7)

Конфигурирование файла закончено. Теперь необходимо проверить правильность написанной конфигурации. Для этого переходим в папку C:/Snort/bin.

Открываем эту папку в командной строке Windows (сделать это можно нажав на панель, отображающую текущую директорию, ввести в ней cmd и нажать Enter, командная строка откроется сразу в данной папке).

Введем команду snort -V, отображающую текущую версию IDS Snort (рис. 12).



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3803]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Snort\bin>snort-V
"snort-V" не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

C:\Snort\bin>snort -V

  _ _ _
  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

C:\Snort\bin>
```

Рисунок 12 – Версия Snort

Просмотрим командой `snort -W` доступные интерфейсы, в данном случае наиболее подходящим для тестирования является интерфейс сетевой карты (номер 5 на изображении ниже) (рис. 13).

```

C:\Snort\bin> snort -W

-*> 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

Index  Physical Address      IP Address      Device Name      Description
-----
1      00:00:00:00:00:00      disabled       \Device\NPF_{22F3887F-66CC-43C1-A33A-3EA251CAD37D}  WAN Miniport
(Network Monitor)
2      00:00:00:00:00:00      disabled       \Device\NPF_{C12D36A6-679D-487B-BC8C-4AC6368142D6}  WAN Miniport
(IPv6)
3      00:00:00:00:00:00      disabled       \Device\NPF_{D43EEE7B-2184-459C-90E5-3A86DDB36FE2}  WAN Miniport
(IP)
4      00:50:56:C0:00:08      192.168.31.1   \Device\NPF_{704671BD-48DD-41B0-AD5D-BAB53C51FD8E}  VMware Virtual
Ethernet Adapter for VMnet8
5      00:00:00:00:00:00      disabled       \Device\NPF_{56A41210C-5630-4181-80F5-4A34087330F5}  WAN Miniport

```

Рисунок 13 – Доступные интерфейсы

Тестируем конфигурацию Snort, вводим команду:

```
snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 5
```

ключ `-T` указывает, что нужно протестировать текущую конфигурацию Snort;

ключ `-c` означает, что включен 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`. Исправим ее.

Добавим файл `local.rules` в папку `C:/Snort/rules` (рис. 14):

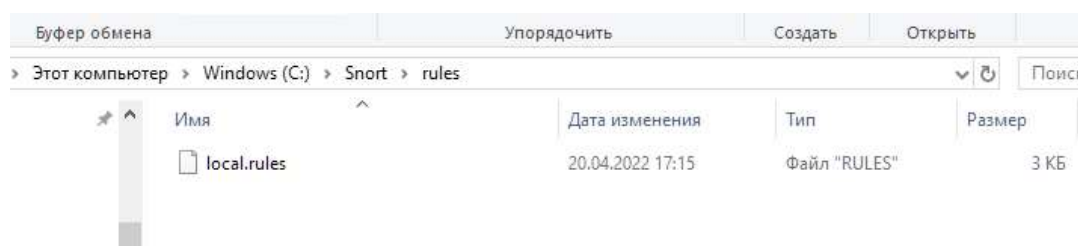
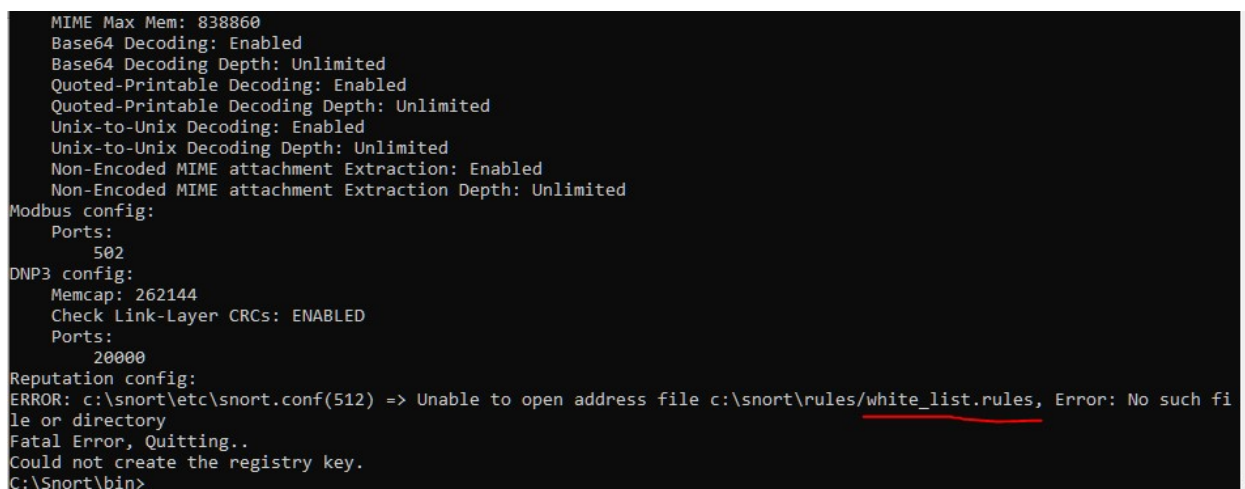


Рисунок 14 – Добавление файла

Снова тестируем конфигурацию Snort, вводим команду:

```
snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 5
```

Тестирование завершено ошибкой, которая указывает на отсутствие файла `white_list.rules`. Исправим ее. Сразу же добавим и файл `black_list.rules`. Эти файлы нет необходимости создавать вручную, их достаточно скопировать из папки для занятия `rules`. Если эти два файла также открыть в тестовом редакторе, то можно увидеть уже написанные правила, которые можно найти и скачать на официальном сайте Snort (рис. 15-16).



```
MIME Max Mem: 838860
Base64 Decoding: Enabled
Base64 Decoding Depth: Unlimited
Quoted-Printable Decoding: Enabled
Quoted-Printable Decoding Depth: Unlimited
Unix-to-Unix Decoding: Enabled
Unix-to-Unix Decoding Depth: Unlimited
Non-Encoded MIME attachment Extraction: Enabled
Non-Encoded MIME attachment Extraction Depth: Unlimited
Modbus config:
  Ports:
    502
DNP3 config:
  Memcap: 262144
  Check Link-Layer CRCs: ENABLED
  Ports:
    20000
Reputation config:
ERROR: c:\snort\etc\snort.conf(512) => Unable to open address file c:\snort\rules\white_list.rules, Error: No such fi
le or directory
Fatal Error, Quitting..
Could not create the registry key.
C:\Snort\bin>
```

Рисунок 15 – Ошибка `white_list.rules`

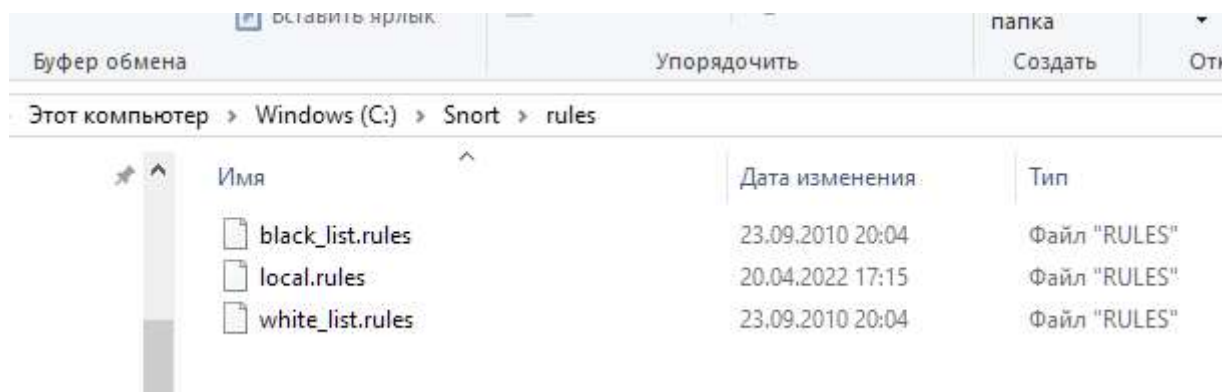


Рисунок 16 – добавление `white_list.rules` и `black_list.rules`

После исправления всех ошибок и повторном вводе команды

```
snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2
```

в командной строке появится сообщение об успешном окончании тестирования конфигурационного файла (рис. 17).

```
C:\Windows\System32\cmd.exe

-*)> 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:1857172128
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>
```

Рисунок 17 – Работа Snort без ошибок

Теперь добавим еще один файл с правилами, который можно скачать с официального сайта [snort.org](http://www.snort.org). Этот файл называется `community.rules`. При скачивании он изначально содержится в архиве с расширением `tar.gz` (рис. 18).





Этот компьютер > Windows (C:) > Snort > rules			
Имя	Дата изменения	Тип	
 <code>black_list.rules</code>	23.09.2010 20:04	Файл "RULES"	
 <code>community.rules</code>	21.12.2023 19:04	Файл "RULES"	
 <code>local.rules</code>	20.04.2022 17:15	Файл "RULES"	
 <code>white_list.rules</code>	23.09.2010 20:04	Файл "RULES"	

Рисунок 18 – добавление `community_rules`

Открываем файл конфигурации и добавляем в него строку, которая добавляет еще один файл правил в конфигурацию IDS Snort (рис. 19).

```

543 #####
544
545 # site specific rules
546 include $RULE_PATH/local.rules
547
548 include $RULE_PATH/community.rules
549
550 #####
551 # Step #8: Customize your preprocessor and decoder ale
552 # For more information, see README.decoder_preproc_rul
553 #####
554
555 # decoder and preprocessor event rules

```

Рисунок 19 – Правим конфиг

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 5
```

Ключ -A показывает, что все предупреждения (alerts) будут дублироваться выводом на консоль.

Snort проверил файл конфигурации и начал свою работу в режиме IDS (рис. 20):

```

C:\Windows\System32\cmd.exe - snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 2
Acquiring network traffic from "\Device\NPF_{C12D36A6-679D-487B-BC8C-4AC6368142}
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=23004)

```

Рисунок 20 – Режим IDS

Теперь самостоятельно попробуем написать правило для IDS Snort. Открываем файл в текстовом редакторе и вводим строку, как показано на рисунке ниже.

Описание введенной строки по частям:

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.

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).

any any: Эти части указывают на IP-адрес и порт назначения. Аналогично "any" означает "любой", применение правила ко всем IP-адресам и портам назначения.

(msg:"Testing TCP alert"; sid:1000003;): Это дополнительная информация к правилу. msg указывает на сообщение или описание правила, в данном случае, это "Testing TCP alert". sid (идентификатор сигнала) представляет собой уникальный числовой идентификатор этого правила в рамках системы IDS/IPS.

Введенное правило в файле local.rules означает следующее: «Генерировать предупреждение при обнаружении любых TCP пакетов от любого источника к любому назначению, с сообщением 'Testing TCP alert' и идентификатором сигнала 1000003» (рис. 21).



Рисунок 21 – Тестовое правило

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 2
```

Для проверки работы данного правила достаточно выйти в сеть интернет и перейти по любому адресу, после этого в командной строке появится уведомление о срабатывании данного правила (рис. 22).

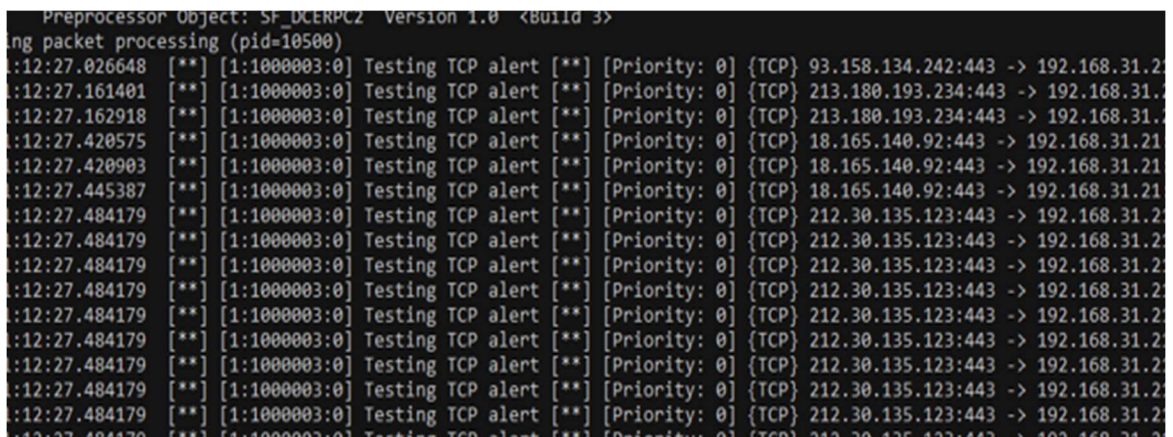


Рисунок 22 – Проверка правила

Вопрос 2. Разработка правил для IDS Snort

Вариант 7. (по списку я 46)

Задание 7. Создать правило для Snort, которое срабатывает при обнаружении HTTPS-трафика.

Необходимо обнаружить трафик HTTPS (порт 443).

Для того чтобы создать правило Snort, которое будет срабатывать при обнаружении HTTPS-трафика, откроем файл local.rules и добавим в него строки, представленные на рисунке 23.

Заключение

Системы обнаружения вторжений, такие как Snort, используются для мониторинга сетевого трафика с целью обнаружения атаки, осуществляемой злоумышленником, прежде чем она сможет причинить вред или повлиять на сеть.

Если злоумышленник выполняет сканирование портов в сети, атака может быть обнаружена, вместе с количеством предпринятых попыток, IP-адресом злоумышленника и другими деталями.

В данной практической работе мы установили и настроили параметры IDS Snort. Разработали правило для IDS Snort по своему варианту.