



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт комплексной безопасности и специального приборостроения
КБ-4 «Интеллектуальные системы информационной безопасности»

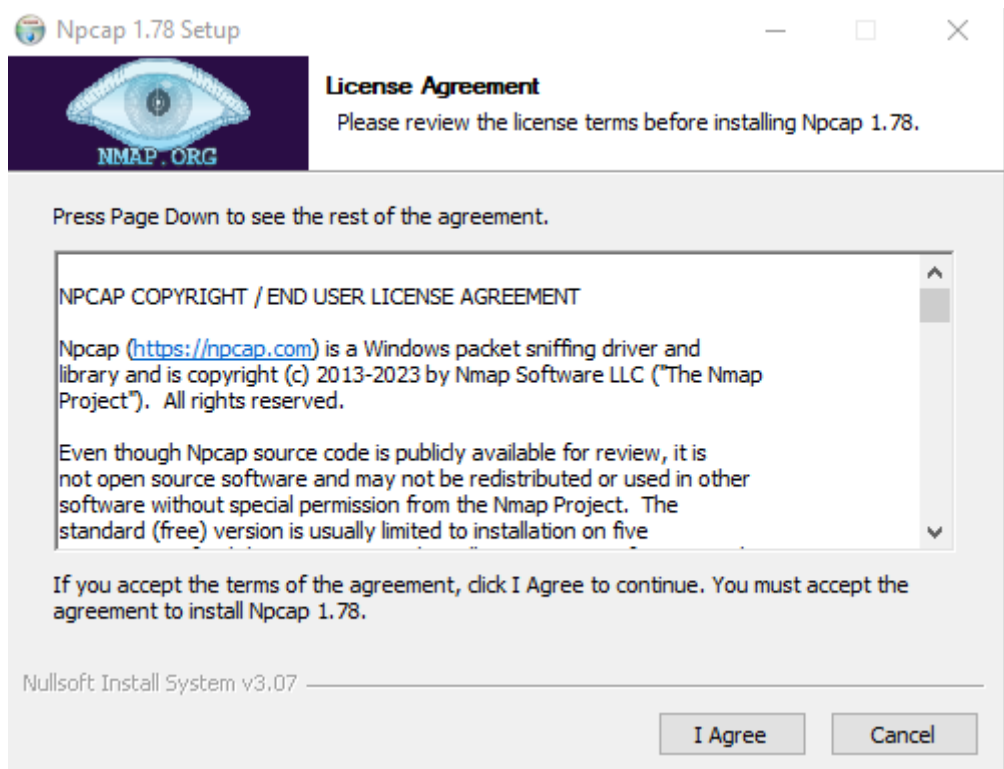
Отчёт
по практической работе
по дисциплине «Управление информационной
безопасностью»
на тему: «2.2 Snort IDS»

Выполнил студент:
Группы: ББМО-02-22
Исаев А.М.

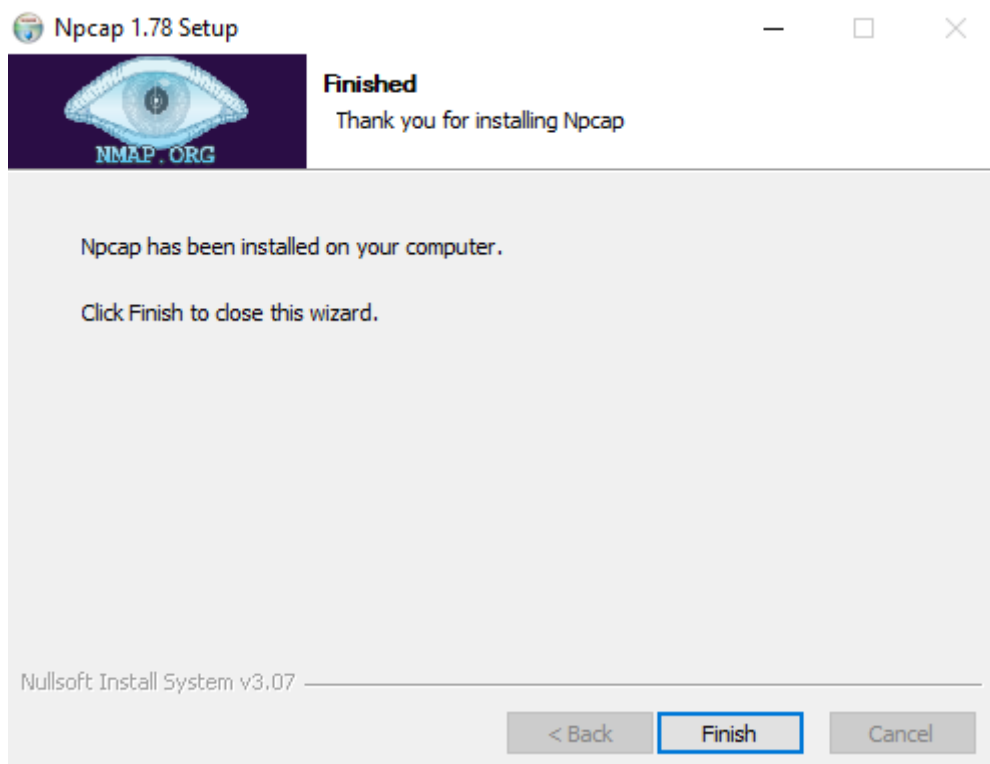
Проверил: Пимонов Р.В.

Москва 2023

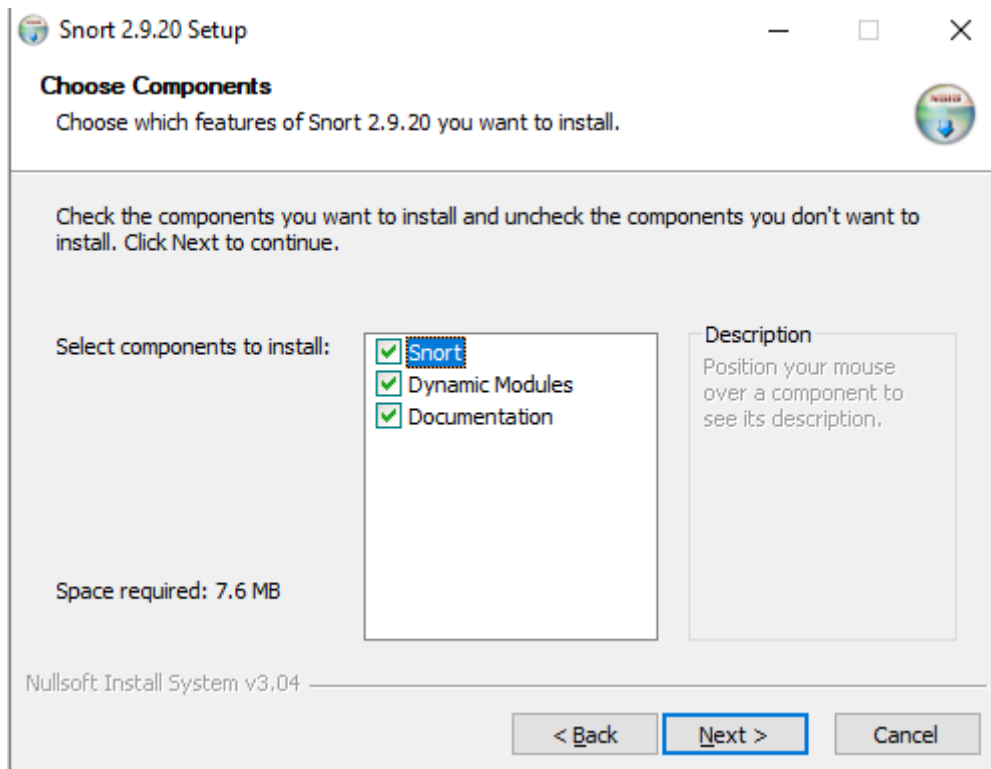
Для начала – установим прсар



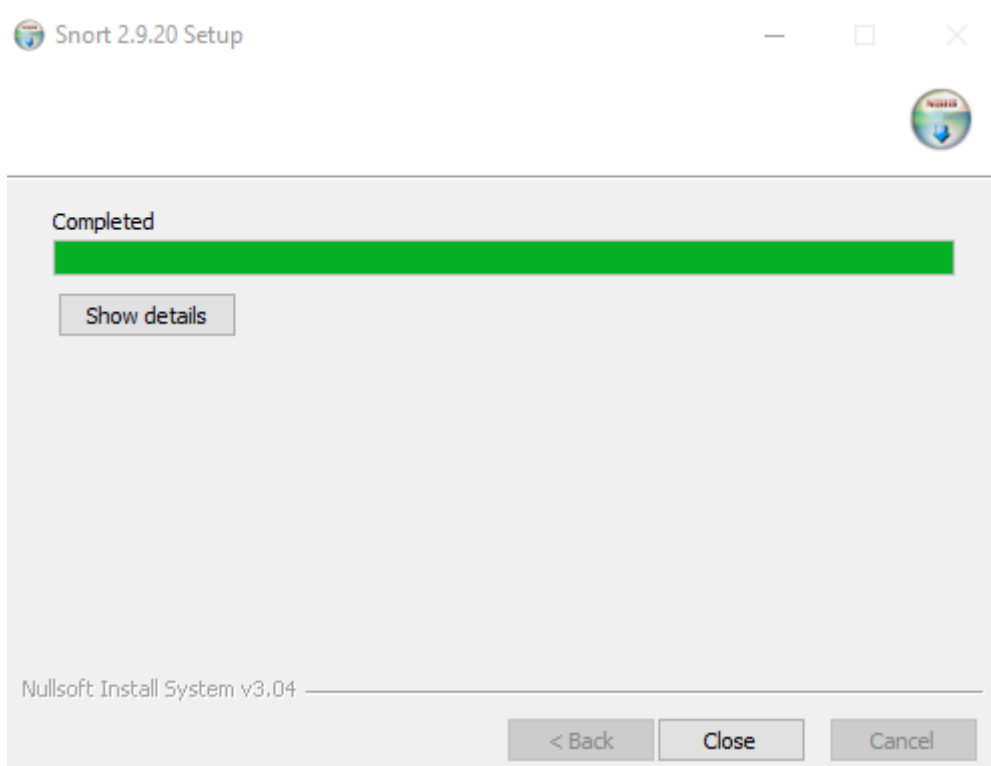
Все было успешно установлено!



Далее, установим сам Snort

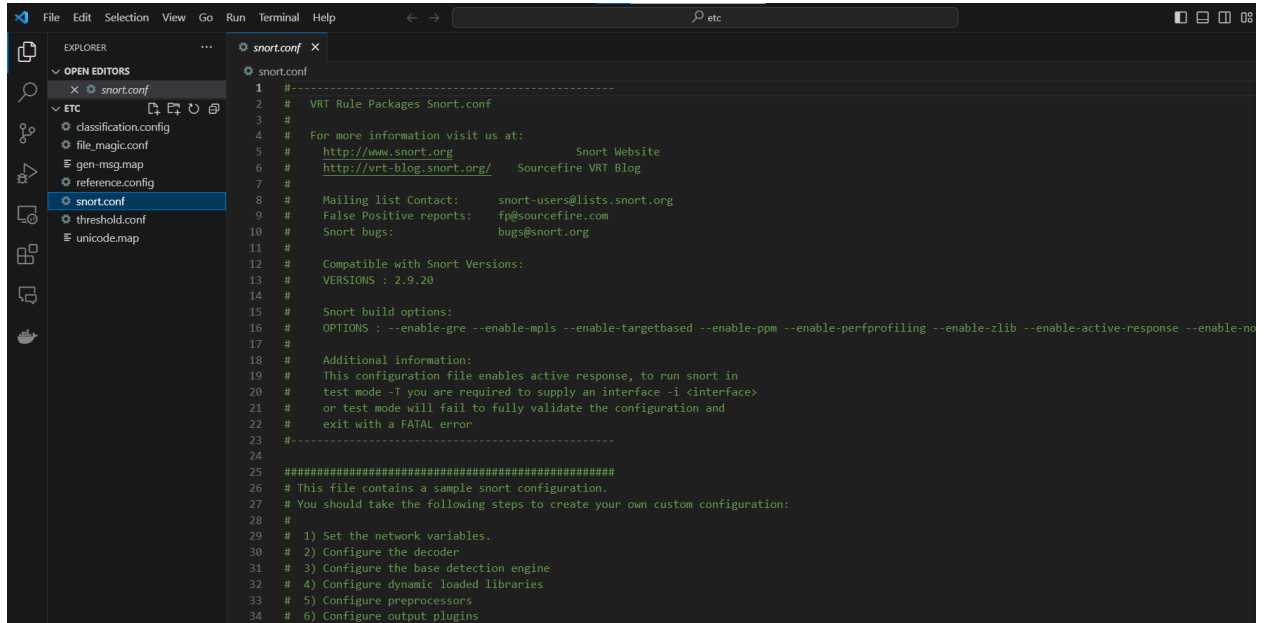


Все было успешно сделано.



Далее, настроим конфигурационный файл для успешной и правильной работы Snort

Откроем 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-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --enable-active-response --enable-no
17 #
18 # Additional information:
19 # This configuration file enables active response, to run snort in
20 # test mode -T you are required to supply an interface -i <interface>
21 # or test mode will fail to fully validate the configuration and
22 # exit with a FATAL error
23 #-----
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
```

Изменим 103-106 строки

```
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
```

Изменим 113-114 строки

```
113  var WHITE_LIST_PATH c:\snort\rules
114  var BLACK_LIST_PATH c:\snort\rules
```

И 186 строку

```
186  config logdir: c:\snort\log
187
```

Укажем пути к библиотекам и движку

```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor

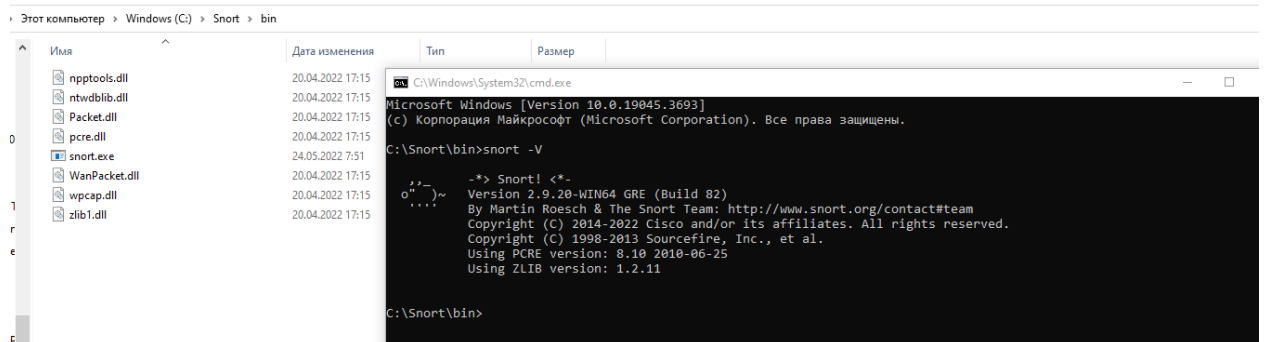
# path to base preprocessor engine
dynamicengine c:\Snort\lib\snort_dynamicengine\sfe_engine.dll

# path to dynamic rules libraries
dynamicdetection directory c:\Snort\lib\snort_dynamicrules
```

Укажем c:\snort для корректной работы

```
# metadata reference data. do not modify these lines
include c:\snort\etc\classification.config
include c:\snort\etc\reference.config
```

Необходимо добавить white_list.rules и black_list.rules



```
==== 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
10 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 81
444 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 31
7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085
1371 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 dyna
Fatal Error, Quitting..
Could not create the registry key.
C:\Snort\bin>
```

Введем команду, с помощью которой мы сможем протестировать конф.файл

snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 4

```

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <B
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
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 1
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:1837511328
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>

```

Все работает! Добавим community.rules и укажем путь на него

т компьютер > Windows (C:) > Snort > rules

Имя	Дата изменения	Тип	Размер
 black_list.rules	23.09.2010 20:04	Файл "RULES"	40 КБ
 community.rules	02.11.2023 16:12	Файл "RULES"	1 773 КБ
 local.rules	04.12.2023 13:18	Файл "RULES"	0 КБ
 white_list.rules	23.09.2010 20:04	Файл "RULES"	40 КБ

```

545 # site specific rules
546 include $RULE_PATH/local.rules
547
548 include $RULE_PATH/community.rules
549

```

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**

Ключ -A показывает, что все предупреждения (alerts) будут дублироваться выводом на консоль. Snort проверил файл конфигурации и начал свою работу в режиме IDS:

```

[ Number of patterns truncated to 20 bytes: 15 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\\Device\\NPF_{76E4A1B7-EB76-4029-9985-6753CAB1D1E5}".
Decoding Ethernet

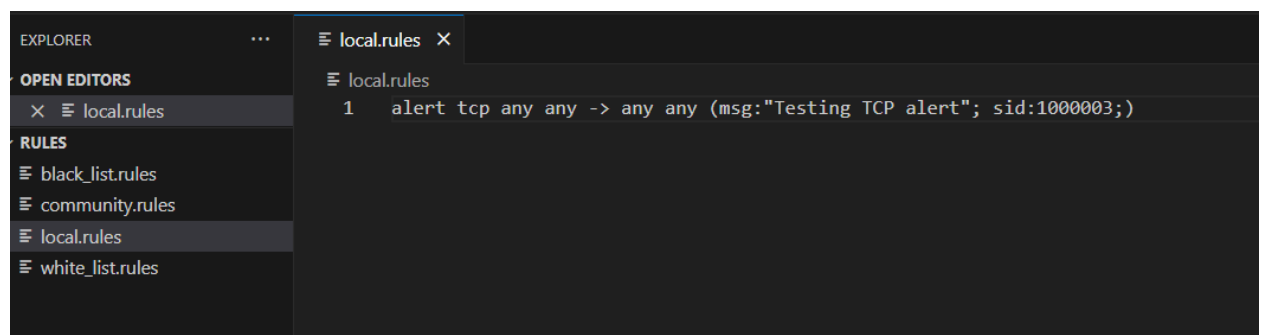
    === Initialization Complete ===

    -*> 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=8188)

```

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



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".

Введем команду и убедимся что алерты работают.

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

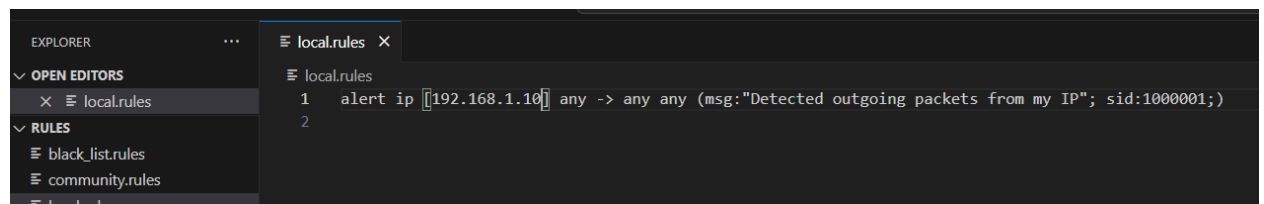
[illegible]

Вопрос 2. Разработка правил для IDS Snort 1. Определить номер выполняемого задания по формуле: $N = n \bmod m + 1$, где N – номер задания; m – количество заданий; n – номер строки с Фамилией в файле: https://docs.google.com/spreadsheets/d/1S_t5WzsKG52ednX4scHOn8WHzk7823kHENAm9C2ssnw/edit#gid=0

$N = 9 + 1 = 10$. – 10 номер задания

10. Создать правило для Snort, которое срабатывает при обнаружении всех исходящих ip-пакетов с Вашим ip-адресом с выводом соответствующего сообщения.

Создадим правило по аналогии: но вместо tcp укажем собственный ip-адрес



```
1 alert ip [192.168.1.10] any -> any any (msg:"Detected outgoing packets from my IP"; sid:1000001;)
2
```

Убедимся что все работает.

12/04-15:10:36.148419	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.150008	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.150876	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.152604	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.153429	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.154576	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.155815	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.157083	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.157912	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.160114	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.161146	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.164041	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.170543	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.650312	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.692651	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.708267	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:36.717541	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.087708	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{TCP}
12/04-15:10:37.455587	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.455704	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.455763	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.457660	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.457766	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.457815	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.496511	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.497550	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.506149	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.586957	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.587249	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.590969	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.597105	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.602409	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.608133	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.627785	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.641407	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.641529	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.672097	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.687727	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.898247	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.898516	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.905570	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.905746	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.905924	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.926632	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.926934	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.927053	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.927794	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}
12/04-15:10:37.945597	[**]	[1:1000001:0]	Detected outgoing packets from my IP	[**]	[Priority: 0]	{UDP}