



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 на тему: Настройка параметров системы
обнаружения атак
по дисциплине: «Управление информационной безопасностью»**

Выполнил:
Студент группы ББМО-01-22
ФИО: Загороднов Е.А.

Проверил:

Р.В. Пимонов

Москва 2023

Содержание

ВВЕДЕНИЕ	3
1. Установка и настройка параметров IDS Snort.....	3
2. Разработка правил для IDS Snort	13
Вывод	15

ВВЕДЕНИЕ

Задача данного практической работы заключается в установке и настройке параметров IDS Snort, а также в создании эффективного правила для обнаружения сетевых атак. В ходе выполнения работы планируется осуществить установку необходимого программного обеспечения, провести настройку системы обнаружения вторжений Snort, и разработать качественное правило для обеспечения надежной защиты сети от потенциальных угроз. В конечном итоге, освоение данных навыков и практических нюансов в области IDS Snort позволит улучшить уровень безопасности информационной инфраструктуры.

1. Установка и настройка параметров IDS Snort

Для осуществления текущей практической работы необходимо провести установку указанного программного обеспечения. В данном контексте предлагается перейти по предоставленной ссылке и приступить к процессу установки. Подробности установки программного обеспечения наглядно продемонстрированы на рисунке 1.

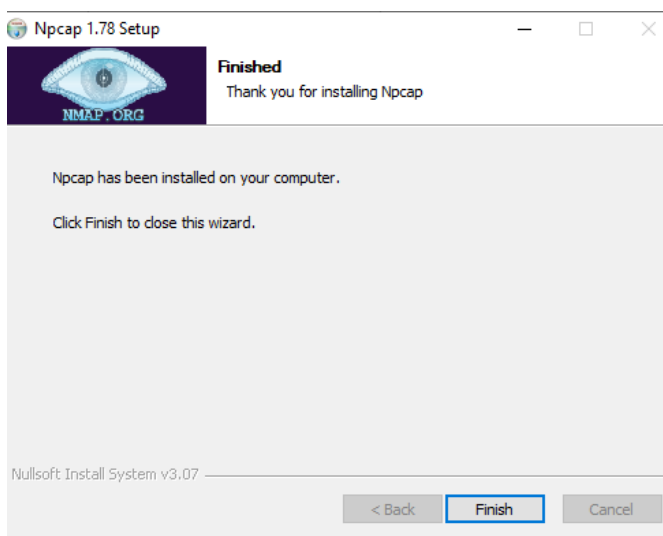


Рисунок 1 – Установка IDS Snort

Далее переходим в директорию **C:/Snort**, где в первую очередь необходимо настроить файл конфигурации для его успешной работы. Для настройки этого файла необходимо перейти в директорию **C:/Snort/etc** и откроем файл **snort.conf**. Процесс открытия файла показан на рисунке 2.

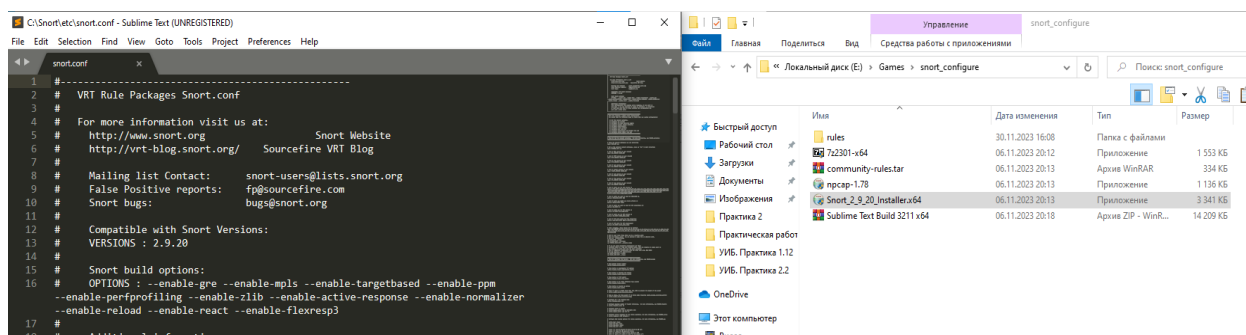


Рисунок 2 – Открытие файла Snort.conf

Теперь переходим в файле **snort.conf** к строкам 104-106 и вместо **...** прописываем **c:\snort**. Процесс показан на рисунке 3

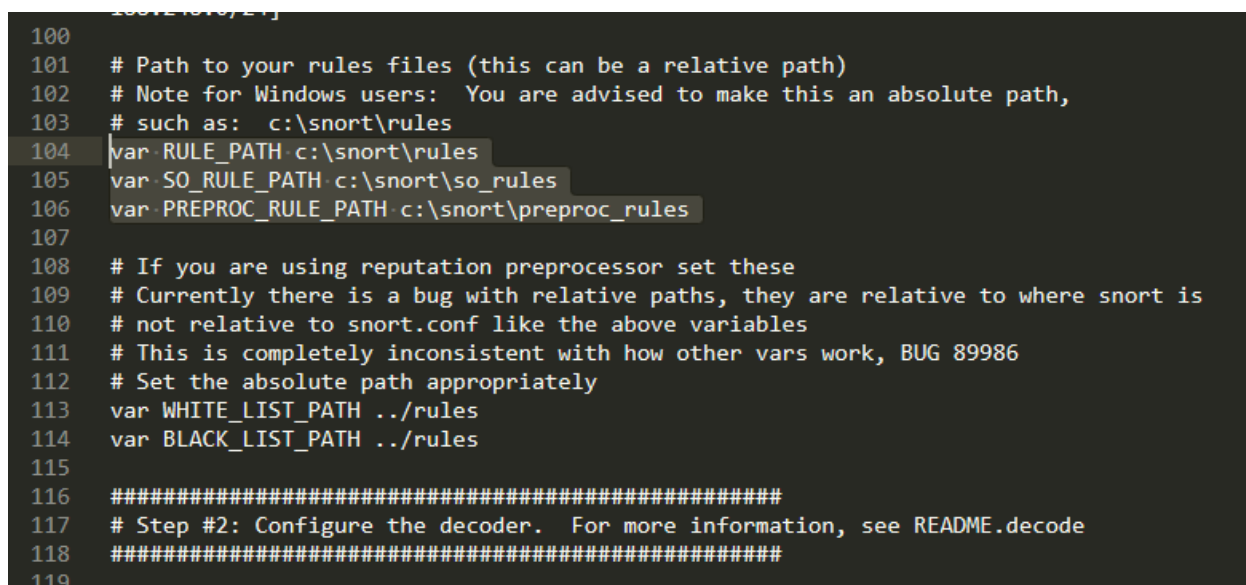


Рисунок 3 – Редактирование строк в файле snort.conf

Далее переходим к строкам 113-114 и делаем те же действия, что и делали в строках 104-106. Процесс показан на рисунке 4.

```

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
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

```

Рисунок 4 – Редактирование строк в файле snort.conf

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. Процесс указания пути для папки Log-файлов показан на рисунке 5.

```

175 #
176 # config snaplen:
177 #
178
179 # Configure default bpf_file to use for filtering what traffic reaches snort. For more
180 # information see snort -h command line options (-F)
181 #
182 # config bpf_file:
183 #
184 # Configure default log directory for snort to log to. For more information see snort -h
185 # command line options (-l)
186 # config logdir: c:\snort\log
187
188
189 #####
190 # Step #3: Configure the base detection engine. For more information, see README.decode
191 #####

```

Рисунок 5 – Написание команды config logdir: c:\snort\log

Далее переходим к строкам 246-253 и прописываем нужны команды для изменения файла конфигурации. Процесс показан на рисунке 6.

```
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\sfe_engine.dll
251
252 # path to dynamic rules libraries
253 dynamicrules_directory c:\Snort\lib\snort_dynamicrules
```

Рисунок 6 – Конфигурирование файла

Далее переходим к строкам 259-265 и добавляем знаки комментария "#". Процесс показан на рисунке 7.

```
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
```

Рисунок 7 – Добавление знака комментария "#"

Также необходимо раскомментировать строки 534-535, убрав знак "#". Процесс показан на рисунке 8.

```
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 classification.config
535 include reference.config
536
537 #####
538
539 # Step #7: Customize your rule set
540 # For more information, see Snort Manual, Writing Snort Rules
541 #
```

Рисунок 8 – Раскомментирование строк 534-535

Также отредактируем пункт, касающийся подключения правил для IDS Snort.

Удалим строки 548-651. Процесс показан на рисунке на рисунках 9 и 10.

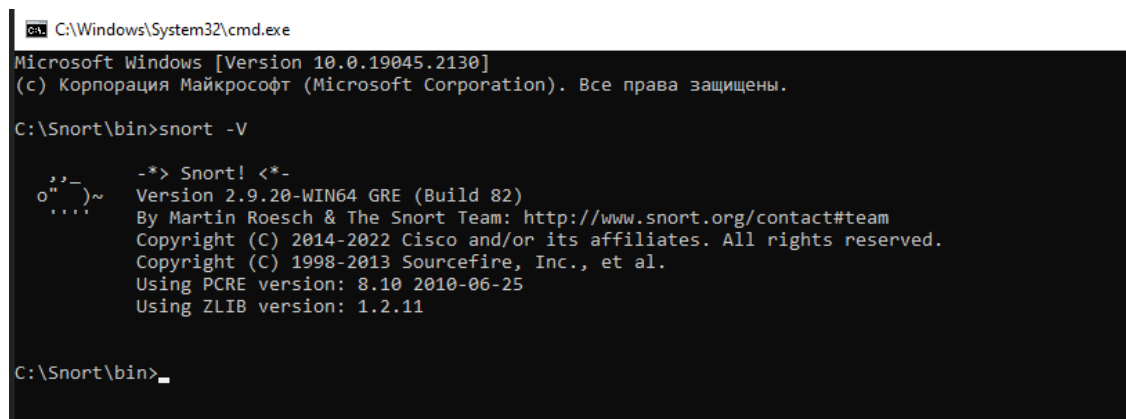
```
538 #####
539 # Step #7: Customize your rule set
540 # For more information, see Snort Manual, Writing Snort Rules
541 #
542 # NOTE: All categories are enabled in this conf file
543 #####
544
545 # site specific rules
546 include $RULE_PATH/local.rules
547
548 include $RULE_PATH/app-detect.rules
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
560 include $RULE_PATH/chat.rules
561 include $RULE_PATH/content-replace.rules
562 include $RULE_PATH/ddos.rules
563 include $RULE_PATH/dns.rules
564 include $RULE_PATH/dos.rules
565 include $RULE_PATH/experimental.rules
566 include $RULE_PATH/exploit-kit.rules
567 include $RULE_PATH/exploit.rules
568 include $RULE_PATH/file-executable.rules
569 include $RULE_PATH/file-flash.rules
```

Рисунок 9 – Строки 548-569 до удаления

```
546 include $RULE_PATH/local.rules
547
548
549
550 #####
551 # Step #8: Customize your preprocessor and decoder alerts
552 # For more information, see README.decoder_preproc_rules
553 #####
554
555 # decoder and preprocessor event rules
556 # include $PREPROC_RULE_PATH/preprocessor.rules
557 # include $PREPROC_RULE_PATH/decoder.rules
558 # include $PREPROC_RULE_PATH/sensitive-data.rules
559
560 #####
561 # Step #9: Customize your Shared Object Snort Rules
562 # For more information, see
563 # http://vrt-blog.snort.org/2009/01/using-vrt-certified-shared-object-rules.html
564 #####
565
566 # dynamic library rules
567 # include $SO_RULE_PATH/bad-traffic.rules
568 # include $SO_RULE_PATH/chat.rules
569 # include $SO_RULE_PATH/dos.rules
570 # include $SO_RULE_PATH/exploit.rules
```

Рисунок 10 – Строки 548-569 после удаления

Конфигурирование файла закончено. Теперь необходимо проверить правильность написанной конфигурации. Для этого переходим в папку **C:/Snort/bin**. Запускаем командную строку через ввод команды **cmd**. У нас запускается командная строка и вводим команду **snort -V**, которая отображает текущую версию IDS Snort. Процесс показан на рисунке 11.



```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

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 11 – Запуск Snort

Далее командой **snort -W** просмотрим доступные интерфейсы, в данном случае наиболее подходящим для тестирования является интерфейс сетевой карты. Процесс ввода команды показан на рисунке 12.

Index	Physical Address	IP Address	Device Name	Description
1	00:00:00:00:00:00	disabled	\Device\NPF_{6C1297FC-5197-4F3A-8864-00F0E9D5624D}	WAN Miniport (Network Monitor)
2	00:00:00:00:00:00	disabled	\Device\NPF_{8B29B738-7777-47F1-9E5F-E60324C82A7B}	WAN Miniport (IPv6)
3	00:00:00:00:00:00	disabled	\Device\NPF_{6342896D-6893-4A60-8B84-B990E6116EDA}	WAN Miniport (IP)
4	C0:4A:00:2A:B7:4F	192.168.0.118	\Device\NPF_{E44E7345-7A95-42F9-BC3D-427CC8433006}	802.11n USB Wireless LAN Card
5	00:50:56:C0:00:08	192.168.74.1	\Device\NPF_{CA450770-8510-4406-B1D5-8CFE82CDFE00}	VMware Virtual Ethernet Adapter for VMnet8
6	00:50:56:C0:00:01	192.168.41.1	\Device\NPF_{EFE2488E-83D0-4051-A460-308B5D64FA9E}	VMware Virtual Ethernet Adapter for VMnet1
7	1C:1B:0D:77:F2:A6	192.168.0.115	\Device\NPF_{D01052D3-ECE0-4DCA-B0B2-297B3F98E57A}	Realtek PCIe GbE Family Controller
8	C2:4A:00:2A:B7:4F	169.254.18.54	\Device\NPF_{028CE244-9FE2-421E-B886-2828F00038A3}	Microsoft Hosted Network Virtual Adapter
9	CA:4A:00:2A:B7:4F	169.254.171.226	\Device\NPF_{E700C789-6875-471F-8D76-D41803EEDCA0}	Microsoft Wi-Fi Direct Virtual Adapter #2
10	C6:4A:00:2A:B7:4F	169.254.171.83	\Device\NPF_{D04B02C4-10FA-4FD4-9483-1159C71CC140}	Microsoft Wi-Fi Direct Virtual Adapter
11	00:00:00:00:00:00	192.168.56.1	\Device\NPF_{23182061-19A0-4613-A972-5AD49FB569DC}	VirtualBox Host-Only Ethernet Adapter
12	00:00:00:00:00:00	0000:0000:0000:0000:0000:0000	\Device\NPF_{loopback}	Adapter for loopback traffic capture
13	00:FF:B6:DA:3E:AE	169.254.116.123	\Device\NPF_{B6DA3EAE-AE5A-4A9B-8209-4050E537F2EB}	TAP-Windows Adapter V9

Рисунок 12 – Доступные сетевые интерфейсы

Тестируем конфигурацию Snort, вводим команду: **snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2**. Процесс ввода показан на рисунке 13. Видим, что Тестирование завершено ошибкой, которая указывает на отсутствие файла **local.rules**.


```

C:\Windows\System32\cmd.exe
C:\Snort\bin>snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2
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 6988 7000:7001
45 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
1 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 4343 4848 5250
: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 90
443 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\c:\snort\rules\local.rules(0) Unable to open rules file "c:\snort\etc\c:\snort\rules\local.rules": Invalid argument.

```

Рисунок 13 – Тестирование конфигурации Snort

Для исправления ошибка добавим файл **local.rules** в папку C:/Snort/rules. Процесс добавления файла показан на рисунке 14.

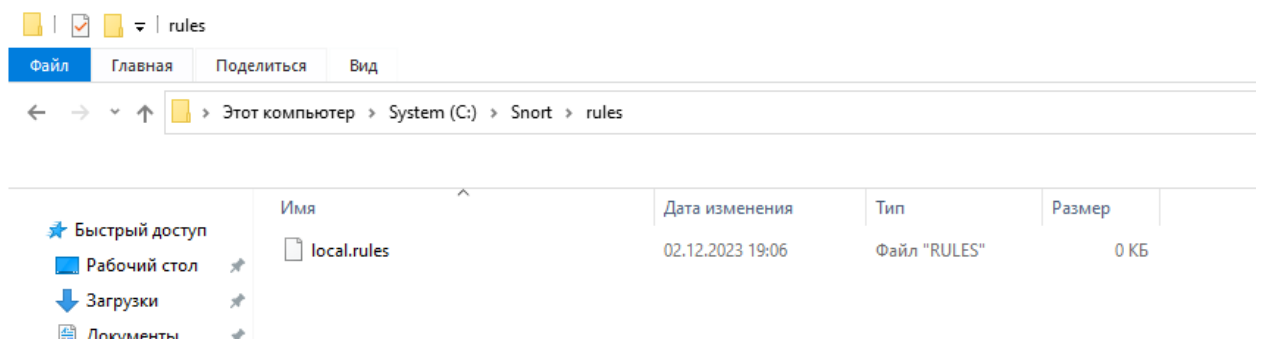


Рисунок 14 – Добавление файла local.rules в директорию

Снова тестируем конфигурацию Snort, вводим команду: **snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2**. Процесс тестирования показан на рисунке 15. Тестирование снова завершено с ошибкой. Ошибка заключается в том, что отсутствует файл **white_list.rules**.

```

POP Memcap: 838860
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 file or directory
Fatal Error, Quitting..
Could not create the registry key.
C:\Snort\bin>

```

Рисунок 15 – Тестирование конфигурации Snort

Добавим файлы **white_list.rules** и **black_list.rules** в папку с файлом **local.rules**. Процесс добавления файлов показан на рисунке 16.

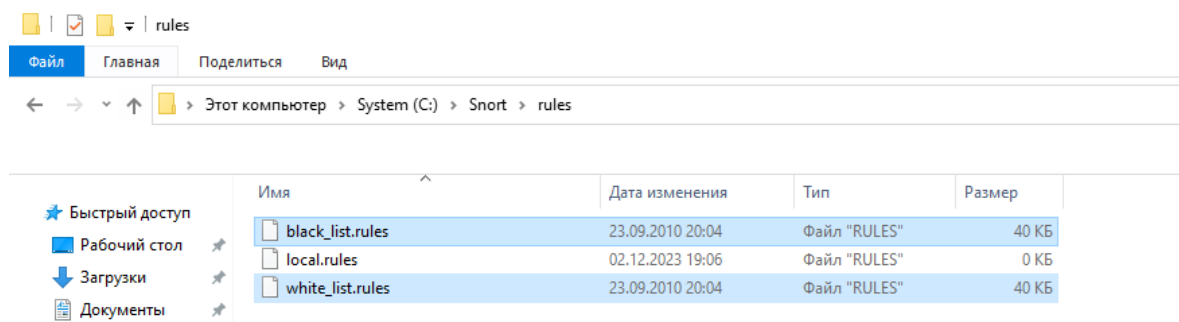


Рисунок 16 – Добавление файлов в директорию

После добавления данных файлов снова запускаем тестирование с помощью команды **snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2**. Процесс показан на рисунке 17. Видим, что тестирование завершено успешно.

```
-*> 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:-2037763424
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>
```

Рисунок 17 – Успешное завершение тестирования

Теперь добавим еще один файл с правилами, который можно скачать со официального сайта snort.org. Этот файл называется **community.rules**. Процесс добавление файла в папку rules показан на рисунке 18.

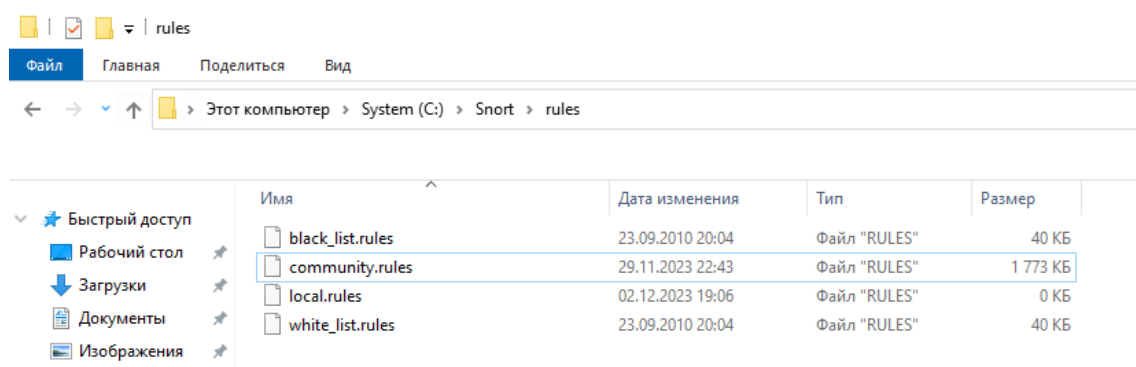


Рисунок 18 – Добавление файла community.rules

Открываем файл конфигурации и добавляем в него строку, которая добавляет еще один файл правил в конфигурацию IDS Snort. Процесс показан на рисунке 19.

```
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 #####
544
545 # site specific rules
546 include $RULE_PATH/local.rules
547
548 include $RULE_PATH/community.rules
```

Рисунок 19 – Добавление строки 548

Далее 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**. Процесс запуска в режиме IDS показан на рисунке 20.

```
==== 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>
Commencing packet processing (pid=13404)
```

Рисунок 20 – Запуска в режиме IDS

2. Разработка правил для IDS Snort

Для начала определим номер выполняемого задания по формуле:

$$N = n \bmod m + 1,$$

где N – номер задания;

m – количество заданий;

n – номер строки с Фамилией в файле:

Расчитав формулу со своими значениями, получалось значение 9. Следовательно приступаем к заданию 9: **Создать правило для Snort, которое срабатывает при обнаружении строки "hack" в DNS-запросе с выводом соответствующего сообщения.**

Приступим к написанию правила для нашего правила для: **Создать правило для Snort, которое срабатывает при обнаружении строки "hack" в DNS-запросе с выводом соответствующего сообщения.** Переходим в файл local.rules и пишем правило: **alert udp any any -> any 53 (msg:" DNS query with the keyword 'hack'"; content:"|68 61 63 6B|"; nocase; dns; sid:1000001;).** Процесс добавления правила показан на рисунке 21.

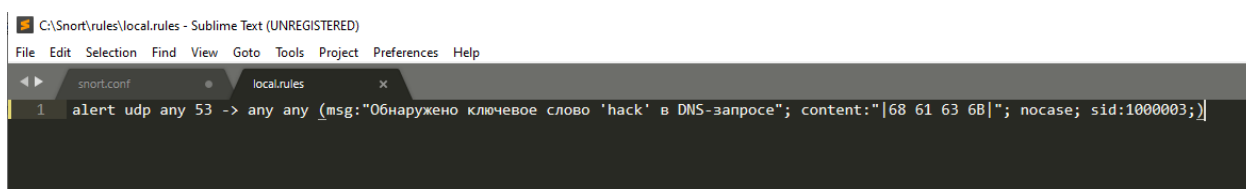


Рисунок 21 – Добавление правила для выполнения задания

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**. Процесс запуска Snort в режиме IDS показан на рисунке 22. Успешный запуск с правилом, которое мы добавили ранее показан на рисунке 23.

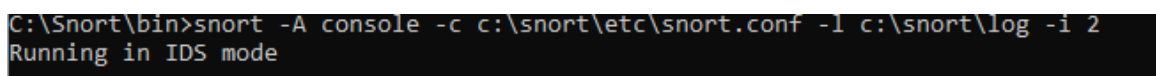


Рисунок 22 – Запуск Snort в режиме IDS

```

--== 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=3744)

```

Рисунок 23 – Успешный запуск с правилом для Snort, которое срабатывает при обнаружении строки "hack" в DNS-запросе с выводом соответствующего сообщения.

Вывод

В результате выполнения практической работы с Snort были приобретены ценные навыки по установке и настройке системы обнаружения вторжений. Создание собственных правил, например, для обнаружения конкретных строк в сетевом трафике, дает возможность персонализировать защиту и адаптировать ее к конкретным потребностям. Опыт работы с Snort подчеркнул важность баланса между точностью обнаружения и предотвращением ложных срабатываний, что является критическим аспектом при обеспечении безопасности в сетевой среде. Этот опыт предоставил понимание того, как эффективно использовать инструменты обнаружения вторжений для повышения уровня защиты в информационных системах.