



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

Институт кибербезопасности и цифровых технологий
Практическая работа № 2.2
по дисциплине
«Управление информационной безопасностью»

Выполнил:

ББМО–01–22

Чадов В. Т.

Проверил:

Пимонов Р. В.

«Зачтено»

«__»_____2023 г. _____

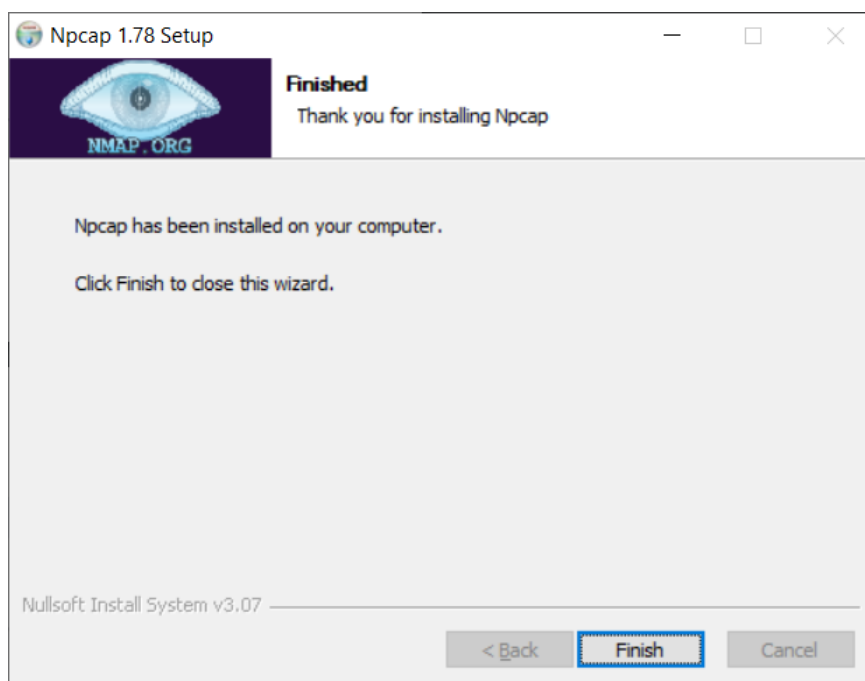
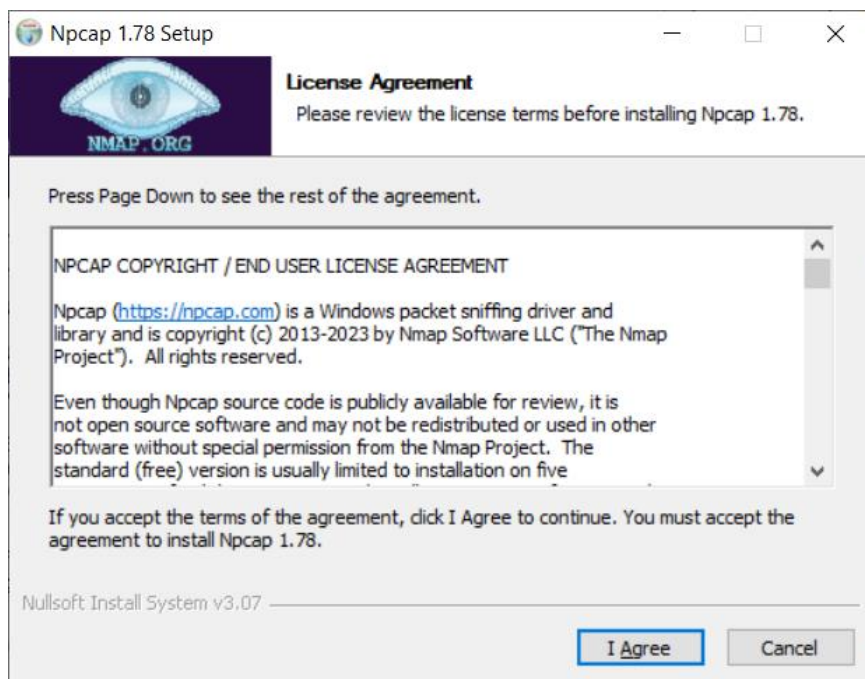
Москва 2023

Содержание

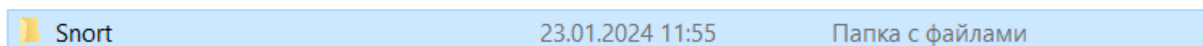
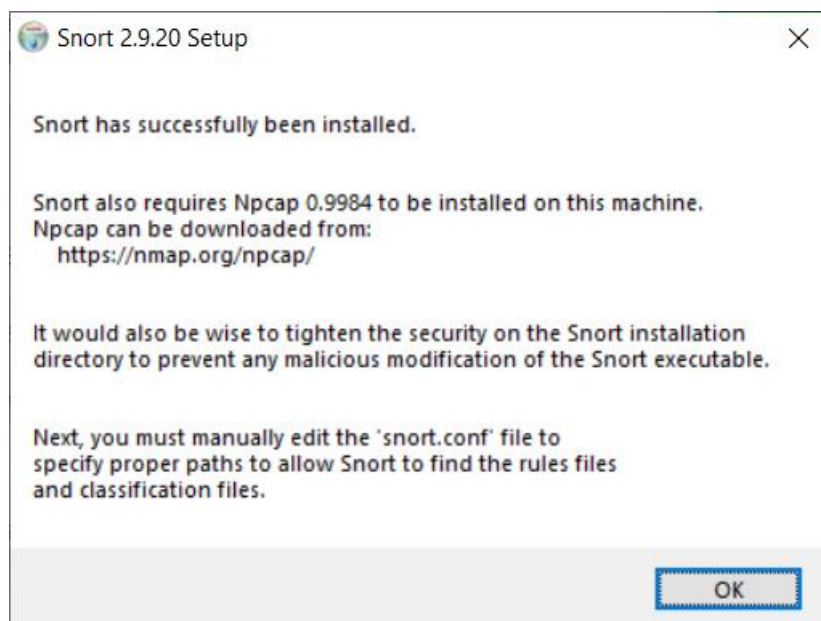
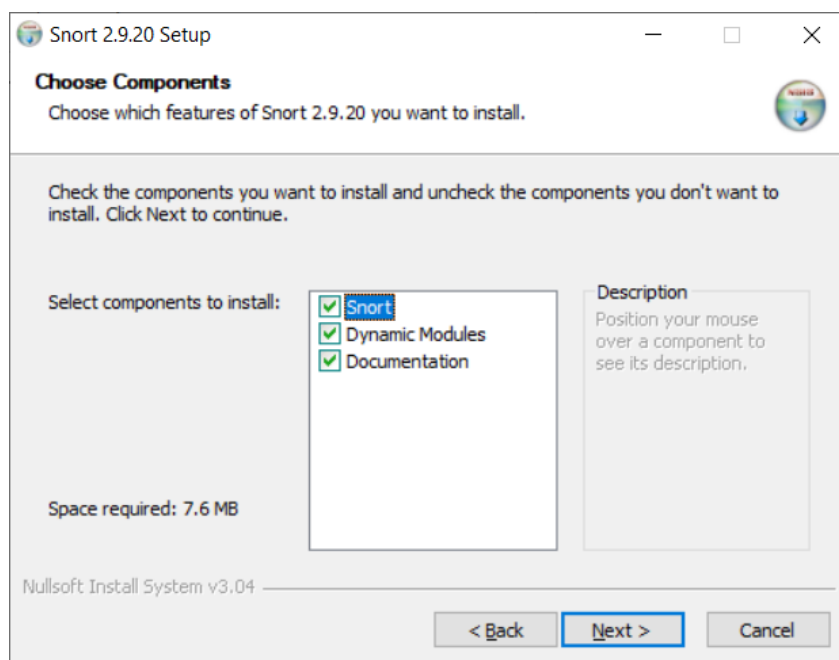
Установка и настройка параметров IDS Snort	3
Написание своего правила	10

Установка и настройка параметров IDS Snort

Установим прсар.



Установим snort.



Сконфигурируем snort.conf.

```
Welcome  snort.conf X
C: > Snort > etc > 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 --
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 #-----
```

```
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Lea
Welcome  snort.conf X
C: > Snort > etc > snort.conf
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
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
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG 8
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH c:\snort\rules
114 var BLACK_LIST_PATH c:\snort\rules
115
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
```

```

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 dynamicdetection directory c:\Snort\lib\snort_dynamicrules
254

```

```

263 # Inline packet normalization. For more informati
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

```

```

533 # metadata reference data. do not modify these lines
534 include c:\snort\etc\classification.config
535 include c:\snort\etc\reference.config
536

```

```

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 #####

```

Протестируем snort.conf и запустим snort.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3930]
(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>
```

Добавим сразу все файлы с правилами.




Этот компьютер > Локальный диск (C:) > Snort > rules					
Имя	Дата изменения	Тип	Размер		
black_list	23.09.2010 20:04	Файл "RULES"	40 КБ		
community	02.11.2023 16:12	Файл "RULES"	1 773 КБ		
local	23.01.2024 12:20	Файл "RULES"	0 КБ		
white_list	23.09.2010 20:04	Файл "RULES"	40 КБ		

Получили ошибку о отсутствии snort_dynamicrules

```
C:\Windows\System32\cmd.exe
C:\Snort\bin>snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 4
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 7144:7145 7510
7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444
41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7
144:7145 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>
```

ИМЯ	Дата изменения	тип	Размер
 snort_dynamicengine	23.01.2024 12:37	Папка с файлами	
 snort_dynamicpreprocessor	23.01.2024 12:37	Папка с файлами	
 snort_dynamicrules	23.01.2024 12:40	Папка с файлами	

```

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:-1635896672
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>

```

Добавим путь для community.rules

```

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

```

```

C:\Windows\System32\cmd.exe - snort -A console -c c:\snort\etc\snort.conf -i c:\snort\log -i 4
Acquiring network traffic from "\Device\NPF_{A693E237-256D-4B5E-B9F9-6F7F0806671C}".
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=560)

```


Напишем правило для теста которое будет реагировать на любое tcp соединение с sid 1000003

```
Welcome  snort.conf  local.rules X
C: > Snort > rules > local.rules
1  alert tcp any any -> any any (msg:"Testing TCP alert"; sid:1000003;)
2
```

```
C:\Windows\System32\cmd.exe - snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 4
01/23-13:06:31.756358 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 107.178.240.159:443 -> 192.168.1.72:3420
01/23-13:06:31.756358 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 107.178.240.159:443 -> 192.168.1.72:3420
01/23-13:06:31.774522 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 107.178.240.159:443 -> 192.168.1.72:3420
01/23-13:06:32.195783 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.195783 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.195783 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.612407 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 188.114.98.224:443 -> 192.168.1.72:3326
01/23-13:06:32.637307 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.637307 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.637307 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.637307 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.637307 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.637307 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.637307 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.637307 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.637529 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.637529 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.639275 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.649455 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.649455 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.649875 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.649875 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.651383 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.651383 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.653447 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.653447 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.654686 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:32.676096 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 142.250.74.5:443 -> 192.168.1.72:3417
01/23-13:06:34.720801 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 208.123.73.83:443 -> 192.168.1.72:2679
01/23-13:06:34.894553 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 208.123.73.83:443 -> 192.168.1.72:2679
01/23-13:06:34.897756 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 208.123.73.83:443 -> 192.168.1.72:2679
01/23-13:06:34.897756 *** [1:1000003:0] Testing TCP alert *** [Priority: 0] {TCP} 208.123.73.83:443 -> 192.168.1.72:2679
```

Написание своего правила

Выполним задание по варианту, напомним правило.

$$N = n \bmod m + 1 = 9 \bmod 10 + 1 = 10$$

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

Мой ip

```
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : beeline
Локальный IPv6-адрес канала . . . : fe80::19a9:851f:fe7c:3a0%15
IPv4-адрес. . . . . : 192.168.1.72
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : 192.168.1.1
```

Добавим собственный ip (основной шлюз) и поменяем сообщение, вместо tcp поставим ip чтобы поймать все пакеты

