# ЗАПУСК SNORT В КАЧЕСТВЕ IDS

# ПОРЯДОК ДЕЙСТВИЙ

- Предварительная настройка:
  - Создание необходимых каталогов
  - Копирование необходимых файлов
  - Настройка прав доступа
- Настройка файла конфигурации
- Выбор режимов оповещения
- Запуск Snort
- Тестирование на примере обнаружения отправки ping-пакетов

# ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

- Создание необходимых каталогов*

# Создаём необходимые для Snort каталоги:

sudo mkdir /etc/snort

sudo mkdir /etc/snort/rules

sudo mkdir /etc/snort/rules/iplists

sudo mkdir /etc/snort/preproc_rules

sudo mkdir /usr/local/lib/snort_dynamicrules

sudo mkdir /etc/snort/so_rules

* http://c-sec.ru

# ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

- # Создаём файлы, в которых будут храниться правила и списки IP:
- sudo touch /etc/snort/rules/iplists/black_list.rules
- sudo touch /etc/snort/rules/iplists/white_list.rules
- sudo touch /etc/snort/rules/local.rules
- sudo touch /etc/snort/sid-msg.map

* http://c-sec.ru

# ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

- # Создаём каталоги, где будут храниться лог-файлы:
- sudo mkdir /var/log/snort
- sudo mkdir /var/log/snort/archived_logs

* http://c-sec.ru

# ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

- # Изменяем права доступа:
- sudo chmod -R 5775 /etc/snort
- sudo chmod -R 5775 /var/log/snort
- sudo chmod -R 5775 /var/log/snort/archived_logs
- sudo chmod -R 5775 /etc/snort/so_rules
- sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules

* http://c-sec.ru

# ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

- Копирование необходимых файлов*

```
cd ~/snort_src/snort-2.9.9.0/etc/

sudo cp *.conf* /etc/snort

sudo cp *.map /etc/snort

sudo cp *.dtd /etc/snort


cd ~/snort_src/snort-2.9.9.0/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/

sudo cp * /usr/local/lib/snort_dynamicpreprocessor/
```

* http://c-sec.ru

# ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

- Копирование необходимых файлов*

**classification.config** описывает типы категории атак, которые предустановленны в Snort.

**file_magic.conf** описываем файловые сигнатуры («магические числа») для определения типа файла.

**reference.config** содержит ссылки на системы идентификации атак.

**snort.conf** конфигурационный файл Snort, в котором хранятся переменные с настройками и путями к различными ресурсам.

**threshold.conf** позволяет настроить количество событий, необходимых для генерации оповещений (алертов), что может быть полезно в случае «шумных» правил.

**attribute_table.dtd** позволяет Snort использовать внешнюю информацию для определения протоколов и политик.

**gen-msg.map** указывает Snort какой препроцессор используется каким правилом.

**unicode.map** предоставляет соответствие между кодировками.

* http://c-sec.ru

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

1. Установка сетевых значений и переменных (Set the network variables)
2. Конфигурация декодеров (Configure the decoder)
3. Конфигурация базового (основного) механизма обнаружения (вторжений) (Configure the base detection engine)
4. Конфигурация динамически загружаемых библиотек (Configure dynamic loaded libraries)
5. Конфигурация препроцессоров (Configure preprocessors)
6. Конфигурация плагинов (Configure output plugins)
7. Настройка набора правил (Customize your rule set)
8. Настройка наборов правил препроцессора и декодера (Customize preprocessor and decoder rule set)
9. Customize shared object rule set

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

# Step #1: Set the network variables. For more information, see README.variables

Задание внутренней сети

ipvar HOME_NET

Задание внешней сети

ipvar EXTERNAL_NET

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

# Step #1: Set the network variables. For more information, see README.variables

Настройка путей к каталогам*

104 var RULE_PATH ../rules

105 var SO_RULE_PATH ../so_rules

106 var PREPROC_RULE_PATH ../preproc_rules

113 var WHITE_LIST_PATH ../rules

114 var BLACK_LIST_PATH ../rules

* http://c-sec.ru

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

# Step #1: Set the network variables. For more information, see README.variables

Настройка путей к каталогам*

104 var RULE_PATH /etc/snort/rules

105 var SO_RULE_PATH /etc/snort/so_rules

106 var PREPROC_RULE_PATH /etc/snort/preproc_rules

113 var WHITE_LIST_PATH /etc/snort/rules/iplists

114 var BLACK_LIST_PATH /etc/snort/rules/iplists

* http://c-sec.ru

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

# Step #2: Configure the decoder. For more information, see README.decode

Содержит конфигурационные дерективы, относящиеся к работе декодера

Формат директивы:

config <directive> [: <value>]

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

| | |
|---|---|
| config disable_decode_alerts | Выключает оповещения, созданные на этапе работы декодера Snort. |
| config disable_tcpopt_experimental_alerts | Выключает оповещения, созданные экспериментальными опциями TCP |
| config disable_tcpopt_obsolete_alerts | Выключает оповещения, созданные устаревшими опциями TCP |
| config checksum_mode: all | Типы пакетов, для которых должна считаться контрольная сумма: все |

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

# Step #3: Configure the base detection engine.  For more information, see README.decode

Содержит конфигурационные дерективы, относящиеся к основному механизму обнаружения атак

Формат директивы:

config <directive> [: <value>]

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

| | |
|---|---|
| config pcre_match_limit: 3500 | Ограничивает количество откатов для заданной опции регулярных выражений |
| config detection: search-method ac-split search-optimize max-pattern-len 20 | Определяет тип используемого быстрого метода проверки сигнатур |
| config event_queue: max_queue 8 log 5 order_events content_length | Определяет условия очереди событий Snort |

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

Step #4: Configure dynamic loaded libraries.

Содержит пути к динамическим загружаемым библиотекам:

- Динамическим библиотекам препроцессора
- Основному механизму препроцессора
- Динамическим библиотекам правил

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

Step #5: Configure preprocessors

Содержит указания на использование препроцессоров в формате

preprocessor <Имя препроцессора>

preprocessor <Имя препроцессора>: возможные опции

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

Step #6: Configure output plugins

Содержит указания на подключение различных модулей вывода

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

Step #7: Customize your rule set

Содержит указания на подключение различных наборов правил в формате:

include $RULE_PATH/НАЗВАНИЕ_НАБОРА_ПРАВИЛ.rules

При работе с менеджером правил PulledPork следует закомментировать все строки кроме

include $RULE_PATH/local.rules

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

Step #7: Customize your rule set

Создание первого тестового правила для Snort*

В файл local.rules следует записать правило:

alert icmp any any -> $HOME_NET any (msg:"<текст сообщения>"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)

* http://c-sec.ru

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

Step #7: Customize your rule set

alert icmp any any -> $HOME_NET any (msg:"<текст сообщения>"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)

Данное правило означает: для любых ICMP-пакетов из любой сети в нашу домашнюю сеть HOME_NET генерируется предупреждение <текст сообщения>

* http://c-sec.ru

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

Step #7: Customize your rule set

После создания файла следует запустить проверку корректности конфигурационного файла Snort

sudo snort -T -c /etc/snort/snort.conf -i etho

* http://c-sec.ru

Step #7: Customize your rule set

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

В случае успешного тестирования должен наблюдаться следующий вывод:

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
1 Snort rules read
    1 detection rules
    0 decoder rules
    0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
0 Dynamic rules
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

* http://c-sec.ru

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

Step #8: Customize your preprocessor and decoder alerts

Содержит указания на подключение различных наборов правил препроцессора и декодера в формате:

include $PREPROC_RULE_PATH/НАЗВАНИЕ_НАБОРА_ПРАВИЛ.rules

# НАСТРОЙКА ФАЙЛА КОНФИГУРАЦИИ

Step #9: Customize your Shared Object Snort Rules

Содержит указания на подключение различных наборов правил для общих объектов:

include $SO_RULE_PATH/НАЗВАНИЕ_НАБОРА_ПРАВИЛ.rules

# ВЫБОР РЕЖИМОВ ОПОВЕЩЕНИЯ

При запуске Snort следует выбрать возможные режимы создания оповещений

| Опции | Описание |
|---|---|
| -A fast | Режим быстрых оповещений |
| -A full | Режим полных оповещений |
| -A unsock | Режим оповещений через сокет |
| -A none | Режим отключения оповещений |
| -A console | Режим вывода оповещений на консоль (экран) |
| -A cmg | Режим оповещений в стиле cmg |

# ЗАПУСК SNORT И ТЕСТИРОВАНИЕ ПРАВИЛА

Запуск Snort

```
sudo snort -A console -q -c /etc/snort/snort.conf -i etho
```

Затем следует отправить ICMP-пакеты с другого хоста и убедиться в срабатывании правила, созданного для Snort

* http://c-sec.ru