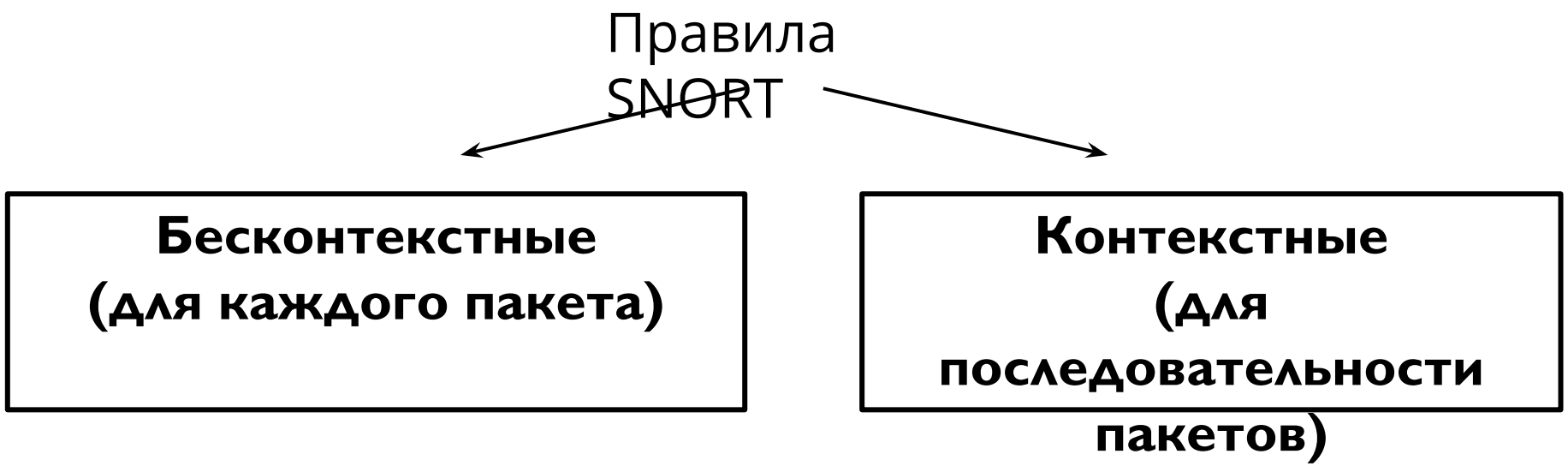
РАЗРАБОТКА СОБСТВЕННЫХ ПРАВИЛ ДЛЯ SNORT

ПОРЯДОК ДЕЙСТВИЙ

1. Изучить типы правил Snort
2. Изучить синтаксис правил Snort
3. Изучить принцип подключения к Snort файлов с дополнительными правилами
4. На основе примеров с сайта c-sec.ru написать примеры собственных правил
5. Проверить работоспособность написанных правил

ПРАВИЛА SNORT*



* http://c-sec.ru

ПРАВИЛА SNORT*

- Формат правила SNORT:

Заголовок правила («Rule Header») + Опции правила (Rule Options)

Правила пишутся в одну строку или с использованием в конце строки символа «\» для обозначения переноса

* http://c-sec.ru

ПРАВИЛА SNORT*

- Формат заголовка правила:

<Действие>

<Протокол>

<IP-адреса отправителей>

<Порты отправителей>

<Оператор направления>

<IP-адреса получателей>

<Порты получателей>

* http://c-sec.ru

ПРАВИЛА SNORT*

- Действия правила:

alert – правило выводит сообщение в выбранном режиме и заносит пакет в журнал

log – заносит пакет в журнал

pass – игнорирует пакет

activate – выводит сообщение и активирует правило с действием dynamic

dynamic – остается неактивным до активации правилом с действием activate

* http://c-sec.ru

ПРАВИЛА SNORT*

- Действия правила:

drop – блокирует и заносит пакет в журнал

reject – блокирует и заносит пакет в журнал, а затем обрывает TCP соединение или сообщает, что порт недоступен

sdrop – блокирует пакет, но не заносит его в журнал

* http://c-sec.ru

ПРАВИЛА SNORT*

- Протокол правила:

TCP

ICMP

UDP

IP

* http://c-sec.ru

ПРАВИЛА SNORT*

- Операторы направления:

«->» - от отправителя получателю

«<>» - в обе стороны

«<-» - такое значение не является допустимым

* http://c-sec.ru

ПРАВИЛА SNORT*

- Опции правил – категории опций
  - **general** – содержат сведения о правиле
  - **payload** – относятся к поиску информации в пользовательских данных пакетов
  - **non-payload** – относятся к поиску информации в служебных данных (заголовках) пакетов
  - **post-detection** – данные опции активируются после того, как правило сработало

* http://c-sec.ru

ПРАВИЛА SNORT*

- Опции категории «General»
  - **msg** – задает выводимое в случае срабатывания правила сообщение. msg:"<message text>"
  - **reference** – задает ссылки на внешние системы идентификации атак. reference:<id system>, <id>
  - **gid** – задает generator id (ключевое слово), позволяющее идентифицировать часть Snort, сгенерировавшую событие. gid:<generator id>
  - sid – задает уникальный идентификатор правила. Рекомендуется использовать sid > 999 9999. sid:<snort rules id>

* http://c-sec.ru

ПРАВИЛА SNORT*

- Опции категории «General»
  - **rev** – задает значение версии правила. rev:<revision integer>
  - **classtype** – задает класс атаки, к которому относится правило на основе файла classification.conf . classtype:<class name>
  - **priority** – задает уровень важности правила. priority:<priority integer>
  - **metadata** – позволяет указать дополнительную информацию о правиле. metadata:key1 value1, key2 value2;

* http://c-sec.ru

ПРАВИЛА SNORT*

- Основные опции категории «Payload»
  - **content** – задает строку для поиска в пользовательских данных. content:[!]"<content string>"
  - **protected_content** – задает значение хэш-функции строки для поиска в пользовательских данных. protected_content:[!]"<content hash>",, hash:[md5|sha256|sha512];
  - Прочие опции позволяют настроить поиск с опциями content или protected_content.

* http://c-sec.ru

ПРАВИЛА SNORT*

- Основные опции категории «Non-payload»
  - **ttl** – задает значение параметра time-to-live в TCP-пакетах. ttl:[<, >, =, <=, >=]<number>; ttl:[<number>]-[<number>];
  - **id** – задает значение параметра id в IP-пакетах id:<number>;
  - flags – задает значение флагов в TCP-пакетах. flags:[!|*|+]<FSRPAUCE0>[,<FSRPAUCE>];

* http://c-sec.ru

ПРАВИЛА SNORT*

- Основные опции категории «Non-payload»
  - **itype** – задает значение параметра type в ICMP-пакетах. itype:[<|>]<number>;
  - **icode** – задает значение параметра code в ICMP-пакетах icode:[<|>]<number>;
  - flags – задает значение флагов в TCP-пакетах. flags:[!|*|+]<FSRPAUCE0>[,<FSRPAUCE>];

* http://c-sec.ru

ПРАВИЛА SNORT*

- Требующиеся примеры правил:
  - Обнаружение пакетов ICMP Echo Request
  - Обнаружение обмена пакетами при обработке запроса «ping»
  - Обнаружение fin-сканирования
  - Обнаружение доступа к 3 различным сайтам
  - Обнаружение входящего запроса TCP-соединения
  - Обнаружение попытки доступа к web-серверу

* http://c-sec.ru