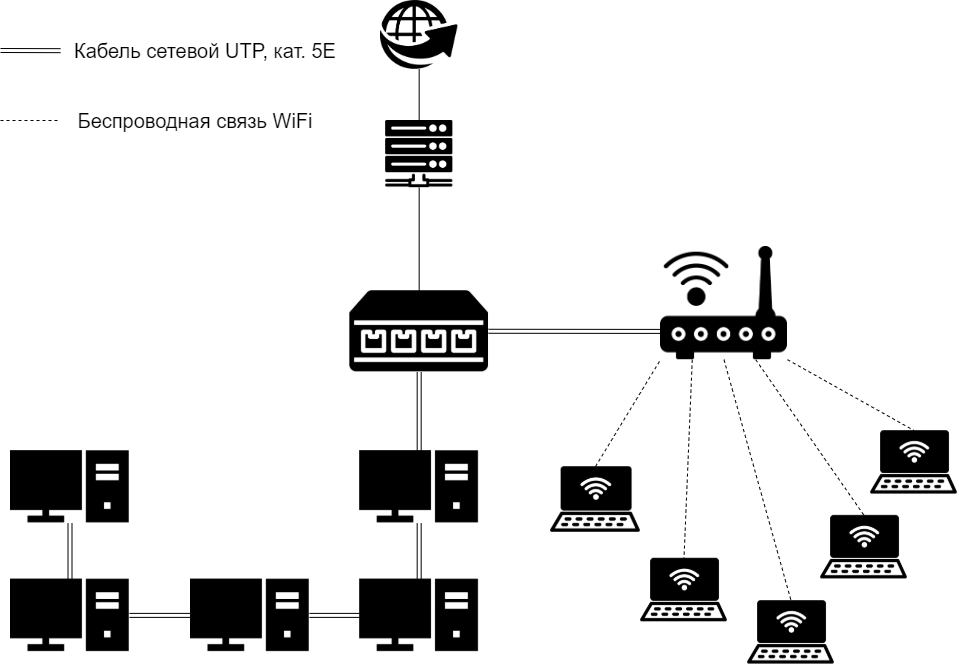
## Лабораторная работа № 9. Системы обнаружения вторжений.

1. Спроектировать физическую сеть для заданного расположения узлов

Сеть в аудитории с компьютерами в университете



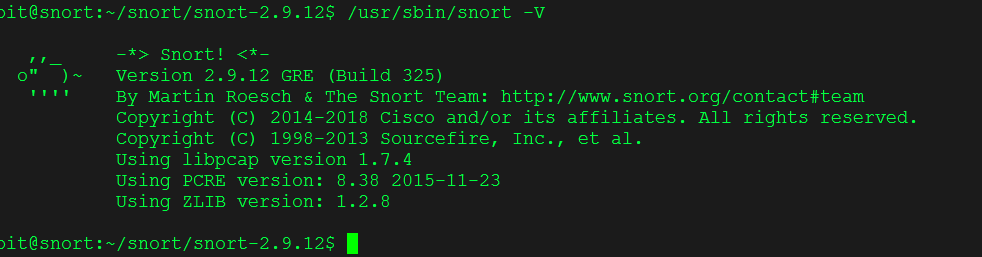
1. Установка и настройка системы IDS (системы обнаружения вторжений) Snort

Установка командой rpm:

rpm –i snort-1.9.1-1snort.i386.rpm

После этого все необходимые файлы будут скопированы в систему.

Проверка установки



Настройка системы:

Далее создаём ряд файлов и каталогов, необходимых для работы Snort, и устанавливаем права доступа для этих файлов:  
# 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

# 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

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

# 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

После чего копируем конфигурационные файлы из извлечённого архива Snort в каталог /etc/snort

Конфигурационный файл Snort /etc/snort/snort.conf содержит все настройки, которые использует Snort в режиме NIDS. Файл для удобства разделён на следующие части:

* Установка сетевых значений и переменных (Set the network variables)
* Конфигурация декодеров (Configure the decoder)
* Конфигурация базового (основного) механизма обнаружения (вторжений) (Configure the base detection engine)
* Конфигурация динамически загружаемых библиотек (Configure dynamic loaded libraries)
* Конфигурация препроцессоров (Configure preprocessors)
* Конфигурация плагинов (Configure output plugins)
* Настройка набора правил (Customize your rule set)
* Настройка препроцессоров и декодеров набора правил (Customize preprocessor and decoder rule set)
* Customize shared object rule set

Открываем файл (например, sudo gedit /etc/snort/snort.conf) и настраиваем следующие параметры:

1. Настраиваем Set the network variables

Задание внутренней сети

Опция ipvar HOME\_NET any задаёт диапазон внутренних IP-адресов (хост или список хостов) для домашний сети, которые мы собираемся защищать и трафик которых Snort будет анализировать. Значение переменной $HOME\_NET соответствует стандарту RFC 1918 (адресное пространство). Имеется возможность указания сетевого интерфейса: $<ИМЯ\_СЕТЕВОГО\_ИНТЕРФЕЙСА>\_ADDRESS (например, ipvar HOME\_NET $eth0\_ADDRESS). Значение переменной будет равно IP адресу. Чаще всего этот параметр используется на компьютерах, которые получают IP адрес динамически. Можно задать маску и указать несколько IP-адресов через запятую (пробелы не допускаются): ipvar HOME\_NET [10.1.1.0/24,192.168.1.0/24]. По умолчанию установлено значение any, что может привести к большому количеству ошибок первого рода (false positives alerts). В нашем случае установим IP-адрес машины, на которой установлен Snort:

ipvar HOME\_NET 192.168.0.104

Задание внешней сети

Опция ipvar EXTERNAL\_NET any задаёт диапазон внешних IP-адресов сетей, из которых исходит угроза. Можно использовать логическое отрицание с помощью символа “!”, например ipvar EXTERNAL\_NET !$HOME\_NET исключает из переменной $EXTERNAL\_NET сеть $HOME\_NET. Данное значение оставим по умолчанию any, чтобы все адреса, отличные от $HOME\_NET, воспринимались внешними.

ipvar EXTERNAL\_NET any

Настраиваем пути к каталогам, которые создали ранее.

var RULE\_PATH /etc/snort/rules  
var SO\_RULE\_PATH /etc/snort/so\_rules  
var PREPROC\_RULE\_PATH /etc/snort/preproc\_rules  
var WHITE\_LIST\_PATH /etc/snort/rules/iplists  
var BLACK\_LIST\_PATH /etc/snort/rules/iplists

Настраиваем Customize your rule set

В данном файле содержится список включаемых файлов вида include $RULE\_PATH/НАЗВАНИЕ\_НАБОРА\_ПРАВИЛ.rules, которые Snort использует по умолчанию для импорта правил. Все эти строки, за исключением одной - include $RULE\_PATH/local.rules, указывающую путь к файлу, где будут храниться наши правила, необходимо закомментировать, так как мы будем использовать менеджер правил для Snort - PulledPork, которых хранит все правила в одном файле.

Если не использовать PulledPork для управления набором правил, то необходимо вручную скачать набор правил с сайта Snort и разархивировать их в каталог /etc/snort/rules, откуда Snort их будет загружать при запуске.

После внесения изменений в настройки конфигурационного файла, необходимо выполнить следующую команду для проверки корректности конфигурационного файла:

sudo snort -T -c /etc/snort/snort.conf -i eth0

где опция -T указывает, что нужно протестировать текущую конфигурацию Snort, -c задаёт путь к конфигурационному файлу, а -i задаёт сетевой интерфейс, который Snort будет слушать.