УДК 004.05

Проектирование и разработка программного модуля «Защита от DDOS атак web-сервера» для ОАО «Дальморнефтегеофизика»

Тришкин Михаил Михаилович
Сахалинский государственный университет
студент

Агаширинова Валентина Юрьевна
Сахалинский государственный университет
Старший преподаватель кафедры информатики

Аннотация
В статье представлен обзор различных методов по организации защиты от распределенных атак на веб-сервисы. Рассмотрена и реализована система защиты от распределенных атак на веб-сервер как программный модуль с алгоритмом обнаружения DDoS-атак.
Ключевые слова: веб-приложения, хостинг, веб-сервер, программный модуль.

Design and development of the program module «Protection against DDOS attacks of the web server» for JSC «Dalmorneftegeofizika»

Trishkin Mikhail Mikhailovich
Sakhalin State University
Student

Agashirinova Valentina Yuryevna
Sakhalin State University
Senior Lecturer of the Department of Informatics

Abstract
The article provides an overview of various methods for organizing protection against distributed attacks on Web-services. The system of protection from distributed attacks on the Web-server as a software module with the algorithm for detecting DDoS attacks.
Keywords: web applications, hosting, web-server, software module.

К сожалению, в последнее время все большее распространение получил целый класс атак (DoS/DDoS), направленных на отказ в обслуживании. Успешная реализация таких атак позволяет блокировать доступ пользователей информационных систем к ресурсам различных серверов, что может вывести из рабочего состояния всю систему.

В настоящее время подобные проблемы крайне редко возникают из-за

технических неполадок - хостинг-провайдеры заранее предупреждают о плановых работах, а резервирование важнейших аппаратных блоков позволяет вести работу практически 24×7, без перебоя. Внезапное прекращение обслуживания зачастую связанно именно с термином «DDoS атака».

Противодействие серьезным DoS-атакам, на самом деле, панацеи, какой-то не существует. Серьезная атака всегда очень сложна в отражении, и при желании атакующий, владеющий серьезными ресурсами для атаки, практически гарантированно может положить любой сайт. Конечно все это стоит существенных затрат, тем не менее если есть такой интерес, то это возможно. Противодействие атакам, на самом деле должно начинаться на этапе проектирования системы, на этапе проектирования и разработки сайтов. Этот вопрос должен учитываться при выборе хостинг- провайдера, либо дата центра, в котором будет стоять оборудование, конфигурация оборудования, подключения каналов провайдеров доступа в интернет. Выбор конфигурации сетевого оборудования, защитного оборудования, файерволов и систем противодействия обычным взломам. Потому, что они так же могут являться узким местом в этой системе при DoS- атаках. Для крупных ресурсов для дата центров, существенной частью работ противодействию атак является, постоянное тесное сотрудничество с техническим персоналом, непосредственно провайдеров, предоставляющих доступ в интернет. Узкими местами всегда является, в первую очередь вычислительная мощность оборудования, на котором расположен атакуемый ресурс, внутренняя архитектура, имеющая свои ограничения, по количеству обрабатываемых запросов, а также система противодействия взлому, в силу того, что она анализирует весь входящий трафик и соответственно требует больших вычислительных мощностей на обработку. Иногда атаки бывают направлены непосредственно на файервол, для того, чтобы он начал блокировать все запросы к сайту. Опять же не справляясь с потоком запросов. Зачастую бывают просто объемные атаки, то есть генерирующие просто большой, бездумный и не интеллектуальный трафик. Направленный на то, чтобы забить канал связи дата центра, либо какого-то сервера. И превысить ограничения на передачу объема данных.

В каждом из этих мест необходимо продумать, свою защиту, необходимо это, учитывать заранее. И если вы сталкиваетесь с DoS-атаками, на системе, которая не учитывает возможность их проведения, то скорей всего эффективно противодействовать вы им не сможете. Существенной частью противодействия опять же является наличие регламента действий в случае DoS-атак, для сотрудников компании, позволяющий оперативно начать противодействие тем самым снизив время поражения.

Общий алгоритм работы программы следующий:

- Пользователь отправляет запрос на сайт;
- Прокси-сервер ищет данный IP-адрес в черном списке. Если находит, то запрос не обрабатывается;

- Запрос обрабатывается прокси-сервером и отправляется на проксируемый сервер. Далее прокси-сервер ищет по таблице адресов IP-адрес. Если находит IP-адрес, далее он проверяет дату последнего запроса с текущей датой, если они равны, то он проверяет сколько запросов было отправлено за данный период времени. Если количество запросов превышает установленный порог запросов в конкретный период времени, то IP-адрес пользователя блокируется на определенное время, установленное в настройках;
- Запрос обрабатывается на проксируемом сервере;
- Запрос отправляется на прокси-сервер;
- Запрос отправляется пользователю.

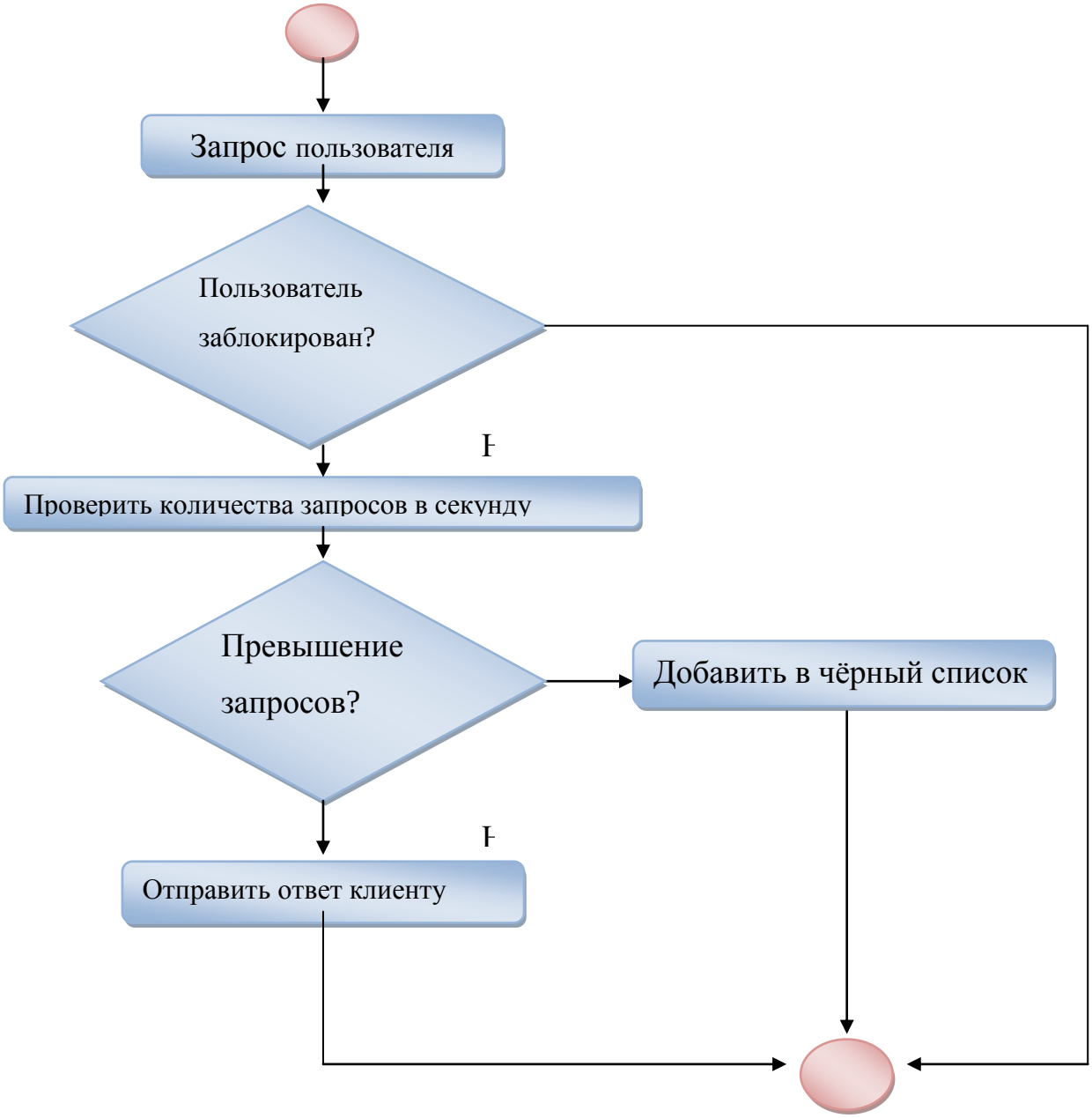


Рисунок 1 – Алгоритм работы программы

Для работы и проверки программы потребовалось три вычислительные машины с разными, IP-адресами.

Таблица 1 –IP-адреса

	IP-адрес
Проксируемый сервер	192.168.0.105
Прокси-сервер с программным модулем	192.168.0.107
Клиент	192.168.0.101

Клиент с адресом 192.168.0.101 отправляет запросы с помощью утилиты Apache Benchmark. С параметрами – с 100 – n 1000 на адрес 192.168.0.107/tisiz/index.php/.

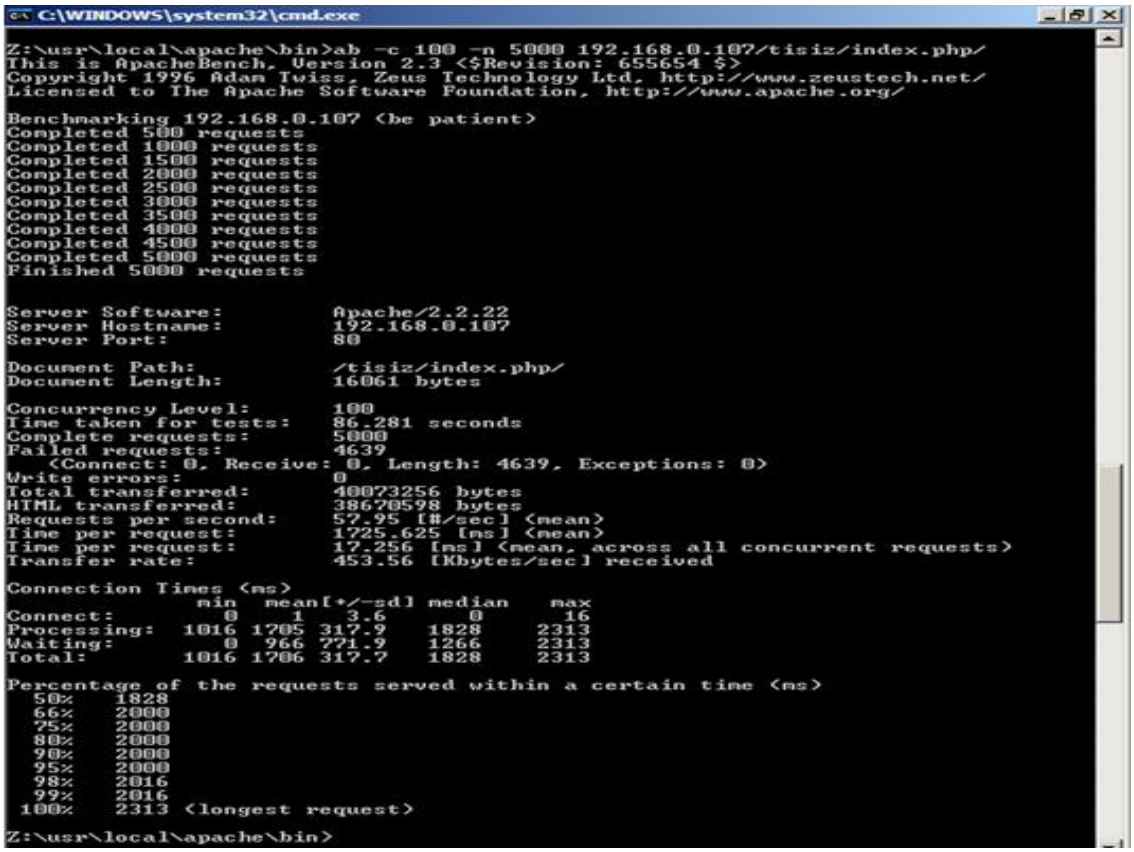


Рисунок 2 – работа утилиты Apache Benchmark

Через некоторое время сервер обрушился, так как не справился с количеством запросов.

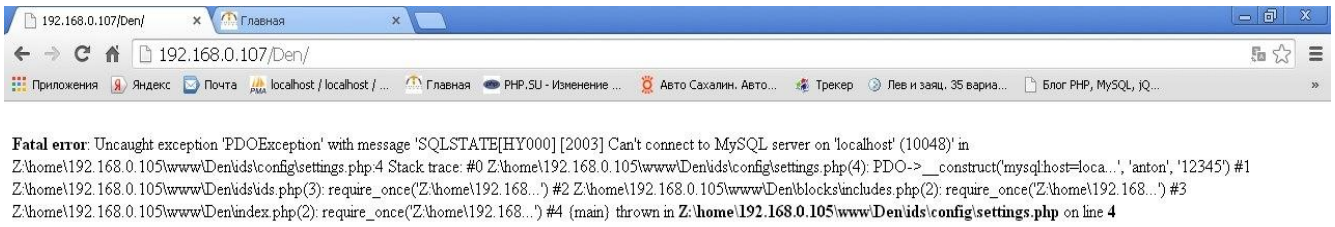


Рисунок 3. – Алгоритм работы программы

Прокси-сервер прослушивает 80 порт, и проксирует сервер

находящийся по адресу 192.168.0.105:81. В настройках пользователь указывает количество запросов в секунду при котором будет блокироваться IP-адрес злоумышленника, и время блокировки.

Пример настроек программы для реализации защиты от DDoSатак

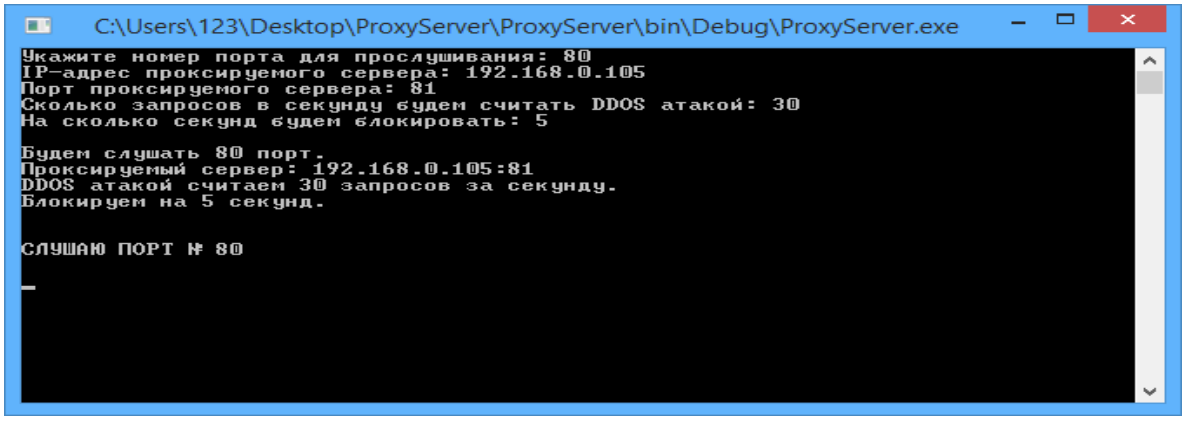


Рисунок 4. - Пример работы программы

- прослушиваемый сервер находится на 80 порту;
- адрес проксируемого сервера находится по адресу 192.168.0.105;
- порт проксируемого сервера 81;
- количество запросов в секунду будут считаться атакой 30 запросов;
- время, на которое будет блокироваться нарушитель 5 сек;

При обнаружении атаки, прокси-сервер журналирует происходящую атаку и блокирует доступ нарушителю на определенное время, заданное в настройках при запуск прокси-сервера.

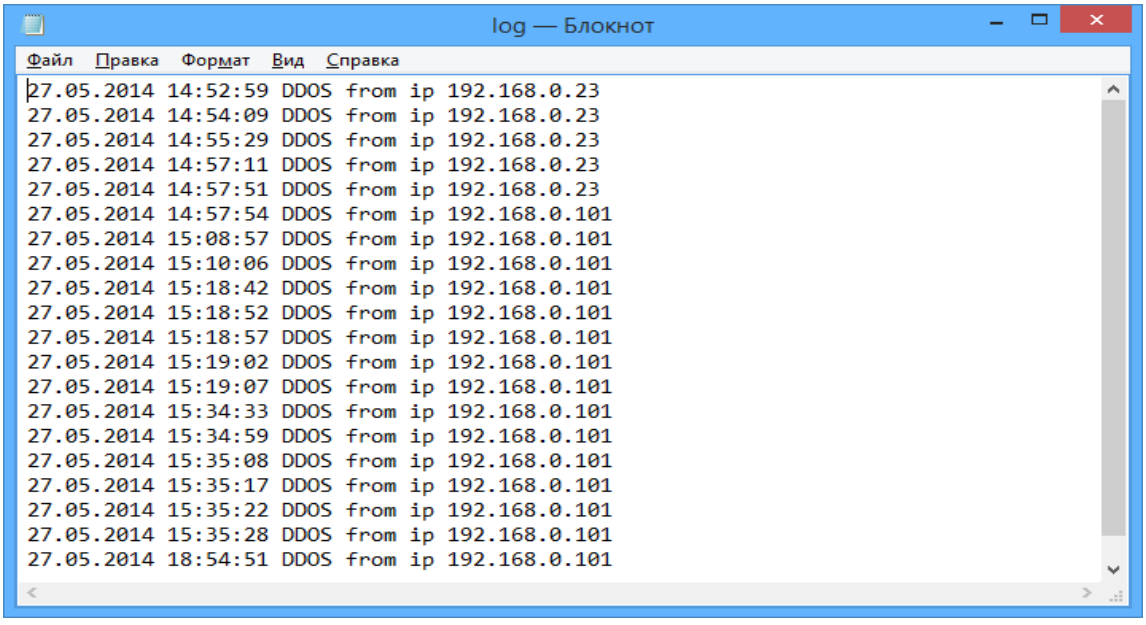
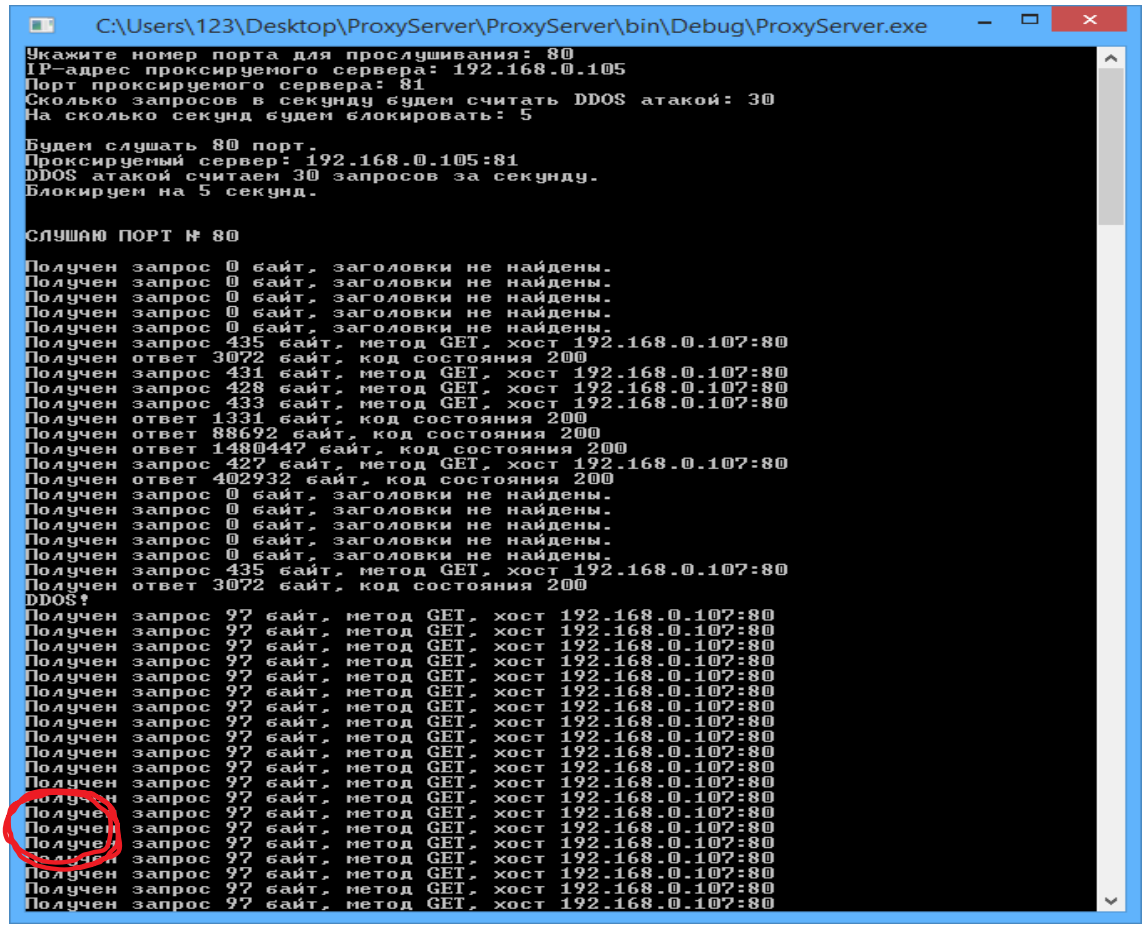


Рисунок 2.6 – Журнал

После того как прокси-сервер обнаружил попытку DDoS-атаки прокси-сервер блокирует адрес атакующего на определенное время и в окне прокси-сервера появляется сообщение «DDOS!».



```
Укажите номер порта для прослушивания: 80
IP-адрес проксируемого сервера: 192.168.0.105
Порт проксируемого сервера: 81
Сколько запросов в секунду будем считать DDOS атакой: 30
На сколько секунд будем блокировать: 5

Будем слушать 80 порт.
Проксируемый сервер: 192.168.0.105:81
DDOS атакой считаем 30 запросов за секунду.
Блокируем на 5 секунд.


СЛУШАЮ ПОРТ № 80

Получен запрос 0 байт, заголовки не найдены.
Получен запрос 0 байт, заголовки не найдены.
Получен запрос 0 байт, заголовки не найдены.
Получен запрос 0 байт, заголовки не найдены.
Получен запрос 0 байт, заголовки не найдены.
Получен запрос 435 байт, метод GET, хост 192.168.0.107:80
Получен ответ 3072 байт, код состояния 200
Получен запрос 431 байт, метод GET, хост 192.168.0.107:80
Получен запрос 428 байт, метод GET, хост 192.168.0.107:80
Получен запрос 433 байт, метод GET, хост 192.168.0.107:80
Получен ответ 1331 байт, код состояния 200
Получен ответ 88692 байт, код состояния 200
Получен ответ 1480447 байт, код состояния 200
Получен запрос 427 байт, метод GET, хост 192.168.0.107:80
Получен ответ 402932 байт, код состояния 200
Получен запрос 0 байт, заголовки не найдены.
Получен запрос 0 байт, заголовки не найдены.
Получен запрос 0 байт, заголовки не найдены.
Получен запрос 0 байт, заголовки не найдены.
Получен запрос 0 байт, заголовки не найдены.
Получен запрос 435 байт, метод GET, хост 192.168.0.107:80
Получен ответ 3072 байт, код состояния 200
DDOS!
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
Получен запрос 97 байт, метод GET, хост 192.168.0.107:80
```

Рисунок 2.7 – Сообщение об обнаружение атаки

Библиографический список

1. Афанасьев А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. М.: Горячая линия-Телеком, 2012. 550 с.
2. Галатенко В. А. Основы информационной безопасности. М.: Интернет-Университет Информационных Технологий: Бином. Лаборатория знаний, 2008. 205 с.
3. Данжани Н. Средства сетевой безопасности. М.:Кудиц–Пресс, 2012. 368 с.
4. Жуков Ю. Основы веб–хакинга. Нападение и защита. Учебное пособие. Питер, 2012. 176 с.
5. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. М.: Новый Юрист, 2010. 256с.
6. Лукацкий А. Обнаружение атак. Учебное пособие. BHV– Санкт – Петербург, 2014. 608 с.