Система защиты от DDoS атак на основе анализа логов

Цель:

- Обеспечение кибер-защиты от DDoS атак.

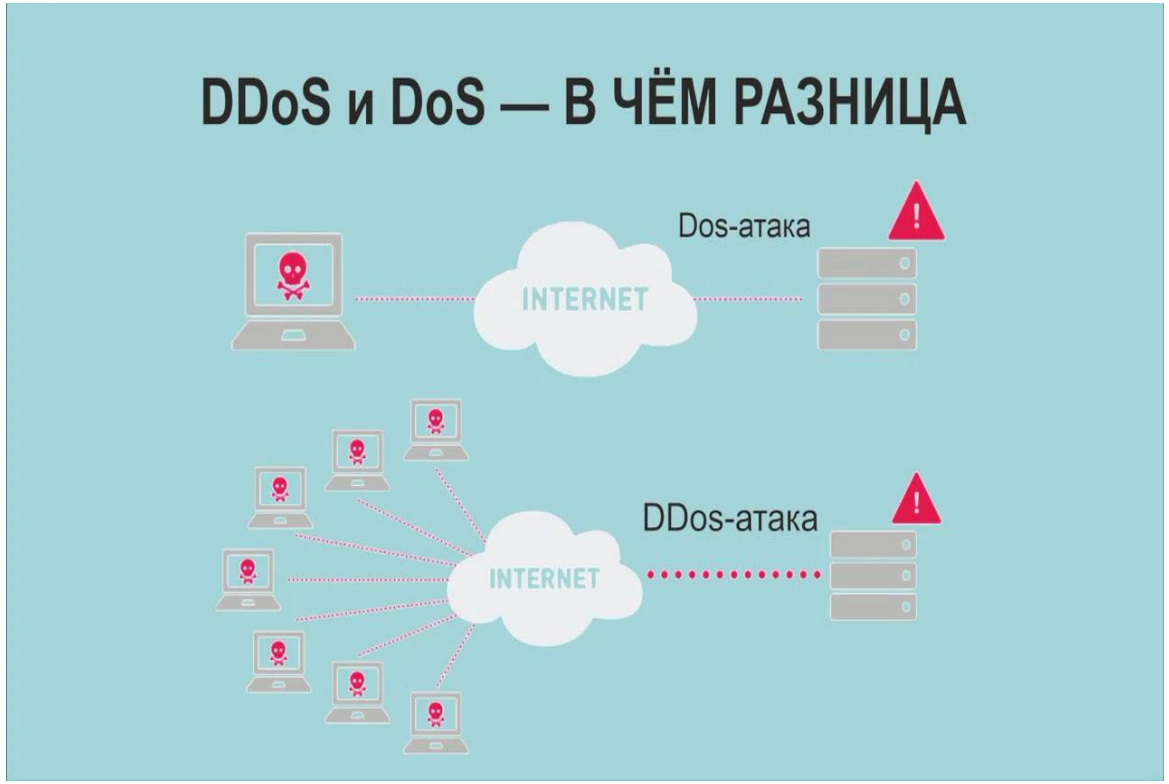
Задачи:

- Рассмотреть существующие средства анализа логов.
- Провести сравнительный анализ существующих программных решений и сделать выводы.
- Разработать ПО, способное к автономному функционированию, а также, на основе данных логов, способное определить нагрузочные атаки на сайт (DDoS) и провести контрмеры.

DoS и DDoS атаки

DoS атака (отказ в обслуживании) – это атака, приводящая к парализации работы сервера или ПК вследствие огромного количества запросов, с высокой скоростью поступающих на атакуемый ресурс.

DDoS атака (распределённый отказ в обслуживании) – это разновидность DoS атаки, которая организуется с помощью большого числа компьютеров, именуемых “зомби”, из-за чего атаке могут быть подвержены серверы даже с очень большой пропускной способностью каналов.



Зачем нужны DDoS атаки

Главная цель любой DDoS атаки – вывести атакуемый ресурс из строя. Тем самым осуществив простой ресурса или потерю репутации владельцев.

Осуществляются атаки с помощью таких запросов, как:

- флуд;
- пустые запросы;
- рандомные поисковые запросы, и т.д.

Виды DDoS атак

Атаки разделяются на три основных вида, по принципу воздействия:

- **Переполнение канала** — это ICMP-флуд, UDP-флуд, DNS-амплификация.
- **Использование незащищенности стека сетевых протоколов** — «пинг смерти», ACK/PUSH ACK-флуд, SYN-флуд, TCP null/IP null атака.
- **Атака на уровне приложений** — HTTP-флуд, медленные сессии, фрагментированные HTTP-пакеты.

Как защищаться от DDoS атак?

Основной способ защиты – фильтрация трафика на основе его содержимого, IP-адресов и других параметров. Реализовать его можно двумя путями:

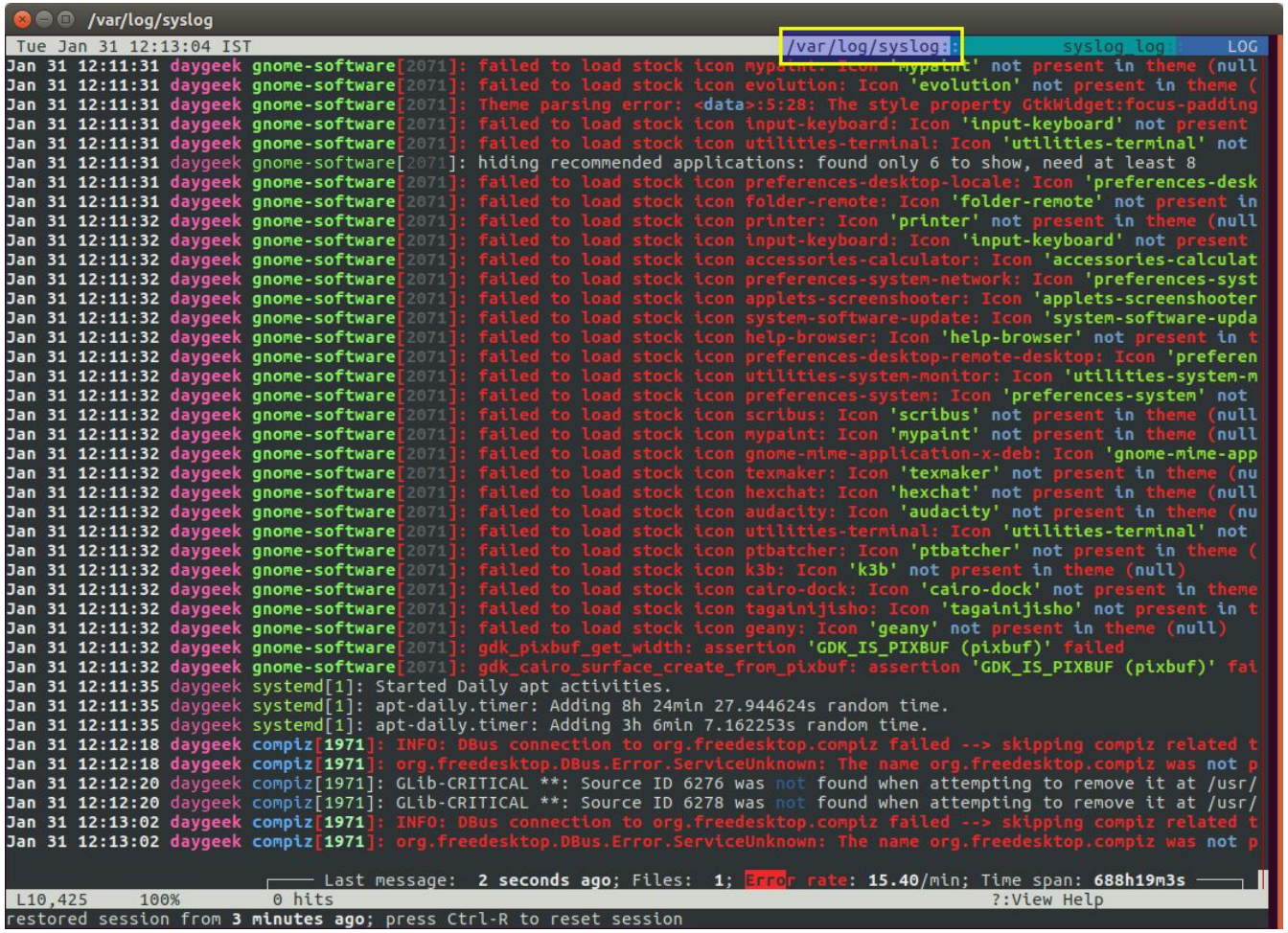
- Установить собственный сервер и программное обеспечение. Такой подход позволяет не зависеть от третьих лиц и позволяет полностью контролировать свою инфраструктуру, настраивая все под собственные нужды.
- Приобрести защиту от DDoS в виде услуги у сторонней компании. Этот путь дает возможность снизить издержки на обслуживание своего оборудования, снимает необходимость в найме профильных специалистов безопасности внутри компании.

Заказать **защиту от DDoS атак**

Анализ логов

Логи (log) – это специальные текстовые файлы, в которых в хронологическом порядке фиксируется информация обо всех действиях программы или пользователей. Проще говоря, это **журнал регистрации** всех событий происходивших в системе:

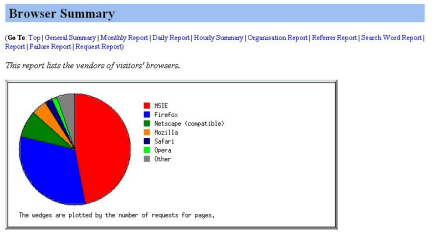
- **ошибки сервера** (сбои), возникающие при обращении к некоторым функциям сайта или задачам;
- **данные о доступе** – запись о подключении (или попытке входа) каждого пользователя, откуда и как он попал на сайт;
- **прочие**, записывающие информацию о работе компонентов сервера.

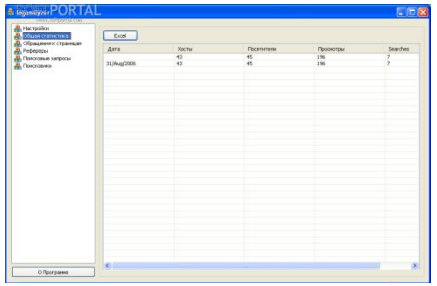


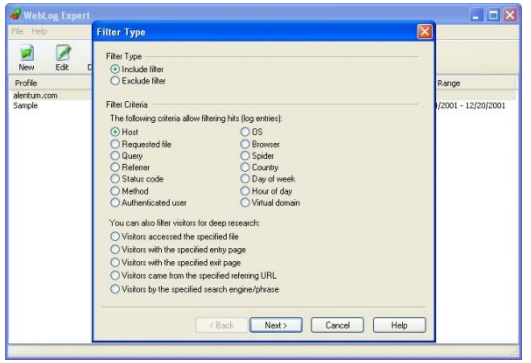
Программы анализа

Инструменты анализа логов:

- Analog 6.0
- Apache Log Analyzer 1.0
- Sawmill Enterprise 8.6.2
- WebSpy Vantage Ultimate 2.2.0.84
- WebLog Expert Lite 8.1
- OSSEC
- Prelude Semi







Сравнение инструментов анализа

Название	**Уровень доступа**	**ОС**	**Тип инструмента**	**Автономность**	**Определение угроз**	**Конфигурирование**	**Интерфейс**	**Тип интерфейса**
Analog 6.0	open-source	Cross platform	Анализатор	+	-	+	+	Console + html отчёт
Apache Log Analyzer 1.0	open-source	Windows	Анализатор	-	-	-	+	Windows+ xls
Sawmill Enterprise 8.6.2	Shareware	Cross platform	Анализатор	+	-	-	+	WEB
WebSpy Vantage Ultimate	Shareware	Windows	Анализатор	+	-	-	+	WEB
WebLog Expert Lite 8.1	Shareware	Windows	Анализатор	-	-	-	+	WEB
OSSEC	open-source	Cross platform	Система Обнаружения Вторжений	+	+	+	-	WEB-конфигурирование
Prelude Semi	open-source	Cross platform	Система Обнаружения Вторжений	+	+	+	-	От сторонних продуктов

Принцип работы программы