Программно-аппаратный комплекс анализа сетевого трафика

Автор: Зырянов Павел Григорьевич
Научный руководитель: доцент каф. ИВТиИБ АлтГТУ, к. т. н.,
Шарлаев Евгений Владимирович

Барнаул 2020

Актуальность работы

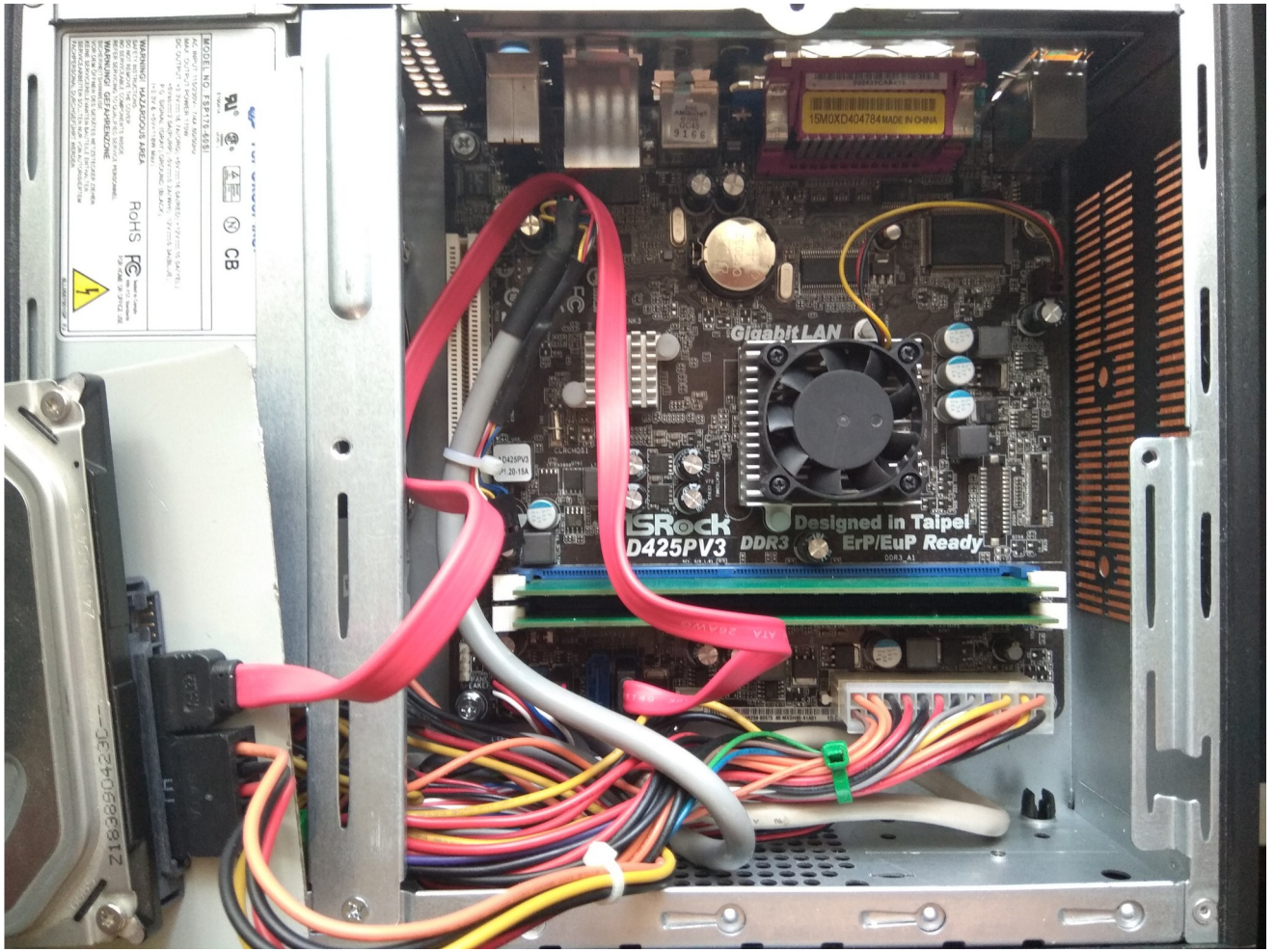
Отсутствие готовых систем со схожим функционалом в открытом доступе.

Широкие возможности для применения: для охраны сетевого периметра, вспомогательный инструмент компьютерного криминалиста, инструмент для участников CTF-соревнований.

Аппаратная платформа

Аппаратная платформа

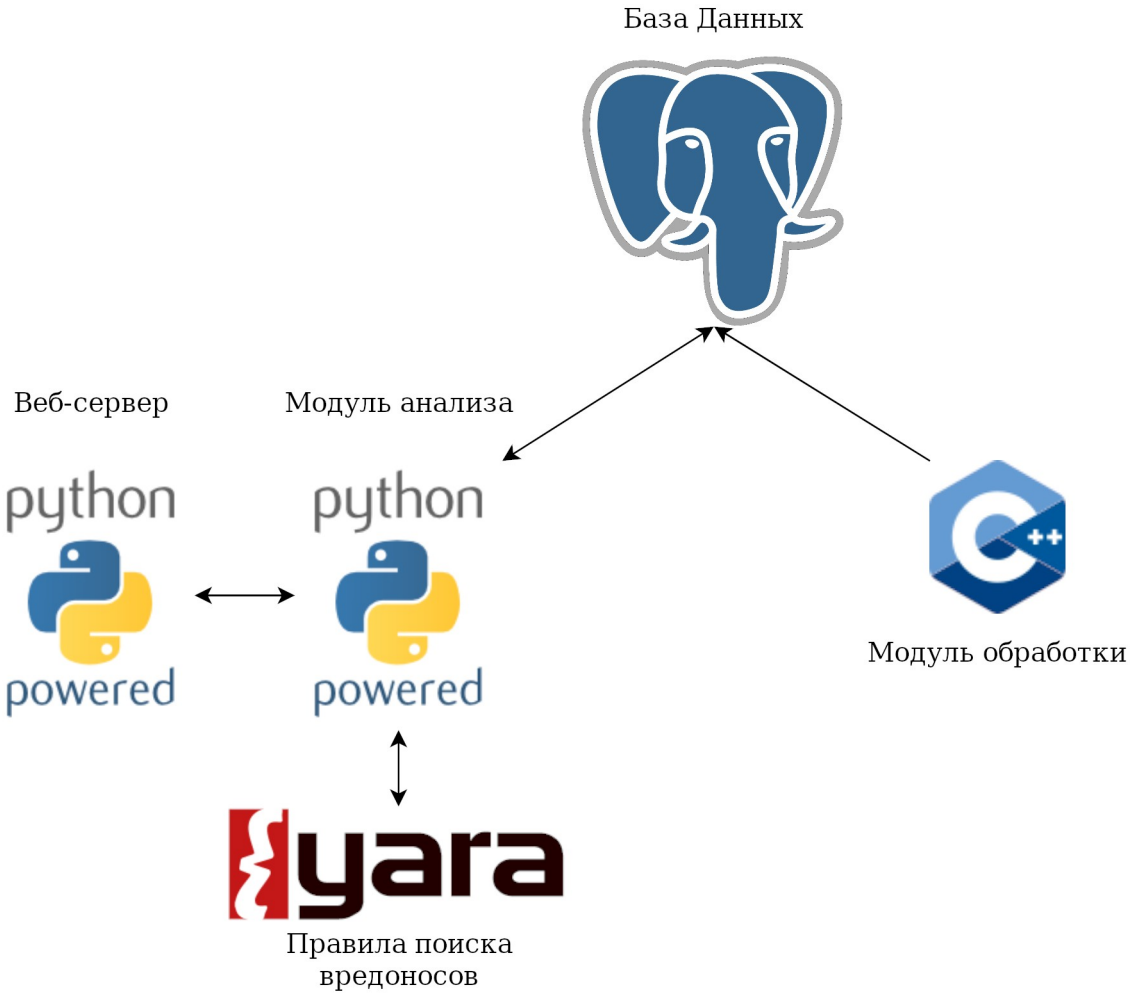
В аппаратной платформе не было использовано специфических и дорогостоящих компонентов за счёт программной оптимизации обработки данных



Характеристики аппаратной платформы

- форм-фактор корпуса – Mini-ITX;
- энергонезависимая паять – 160 ГБ HDD;
- оперативная память – 2 ГБ;
- тактовая частота процессора – 1,8 ГГц;
- количество ядер (потоков) процессора – 2;
- наличие сетевой карты с пропускной способностью 1 Гбит/с.

Компоненты программной части

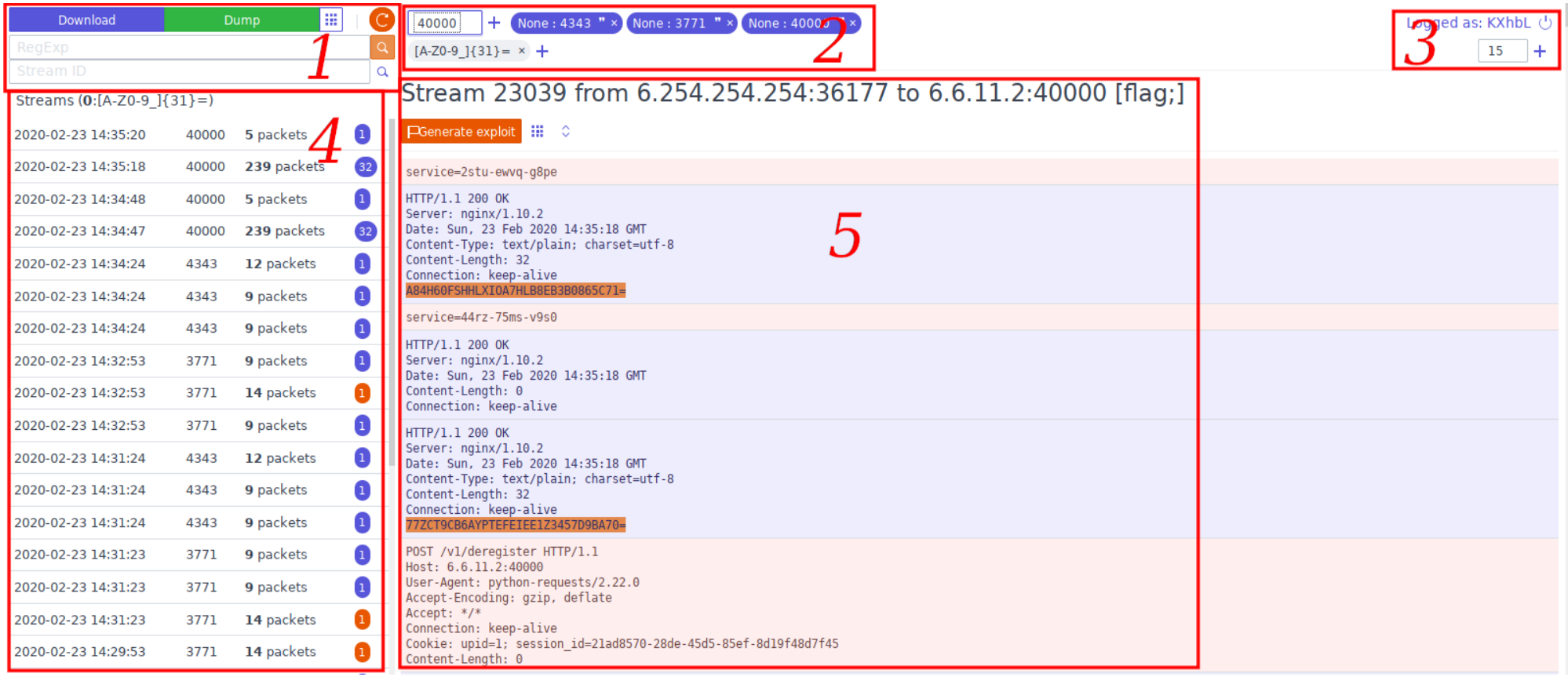


Хранение данных

→В качестве базы данных была выбрана PostgreSQL

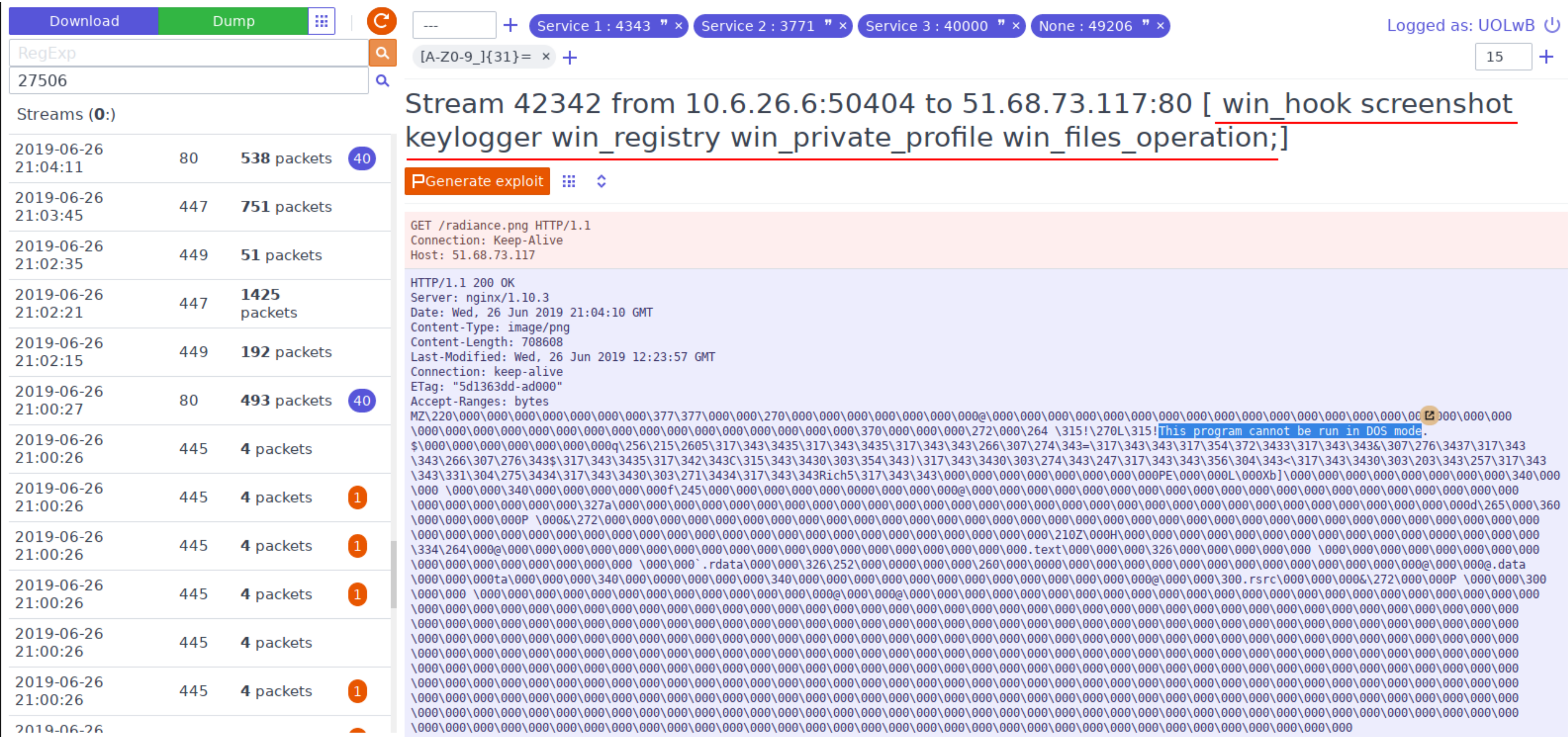
Сетевые соединения (потоки)	Сетевые пакеты
- Время установления соединения - Количество пакетов - Данные об отправителе - Данные о получателе - Результат анализа на Вредоносный код	- Время отправки пакета - Сторона, отправившая пакет - Полезная нагрузка

Графический интерфейс системы



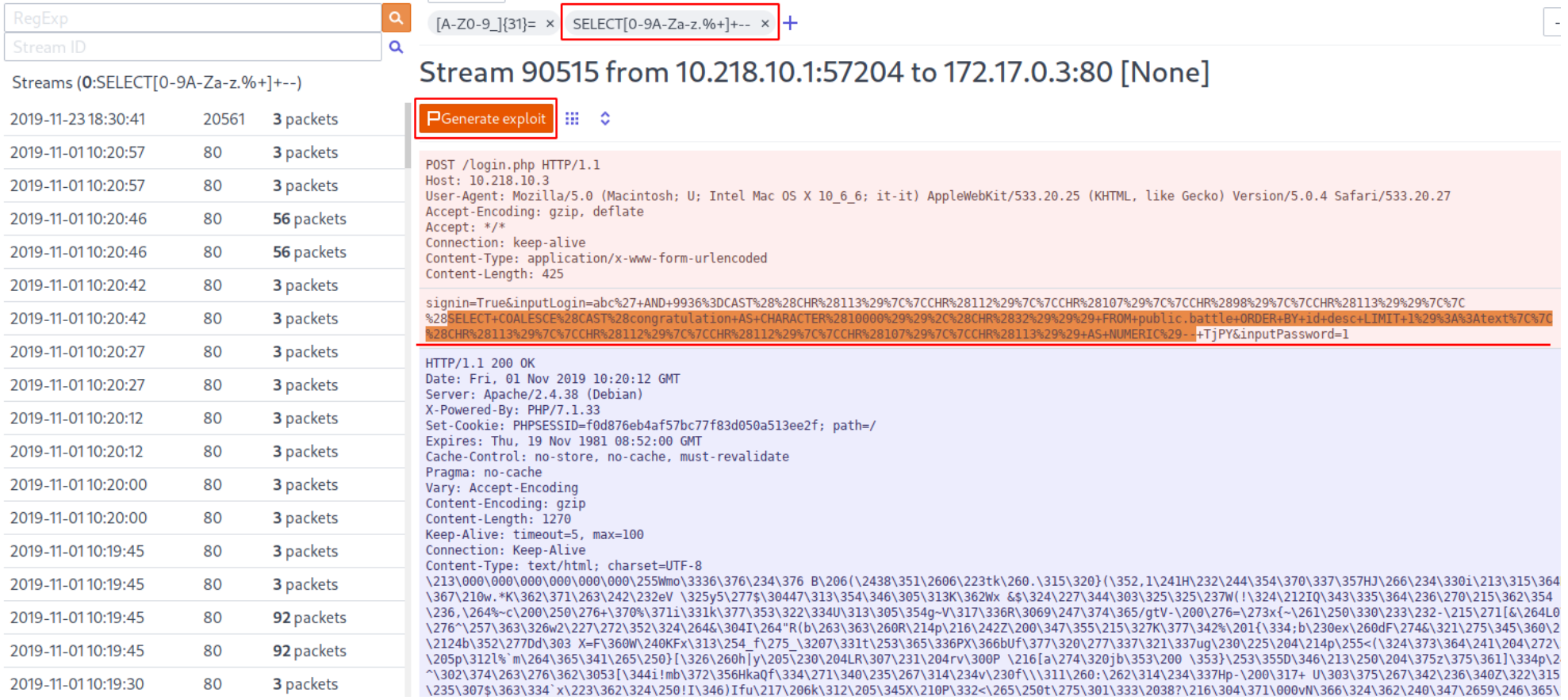
1 – основное управление системой
2 – фильтры соединений по номеру порта и содержимому
3 – фильтр по времени в минутах и кнопка выхода из сессии
4 – список соединений
5 – детальная информация о соединении и переданные пакеты

Результат анализа вредоносного трафика



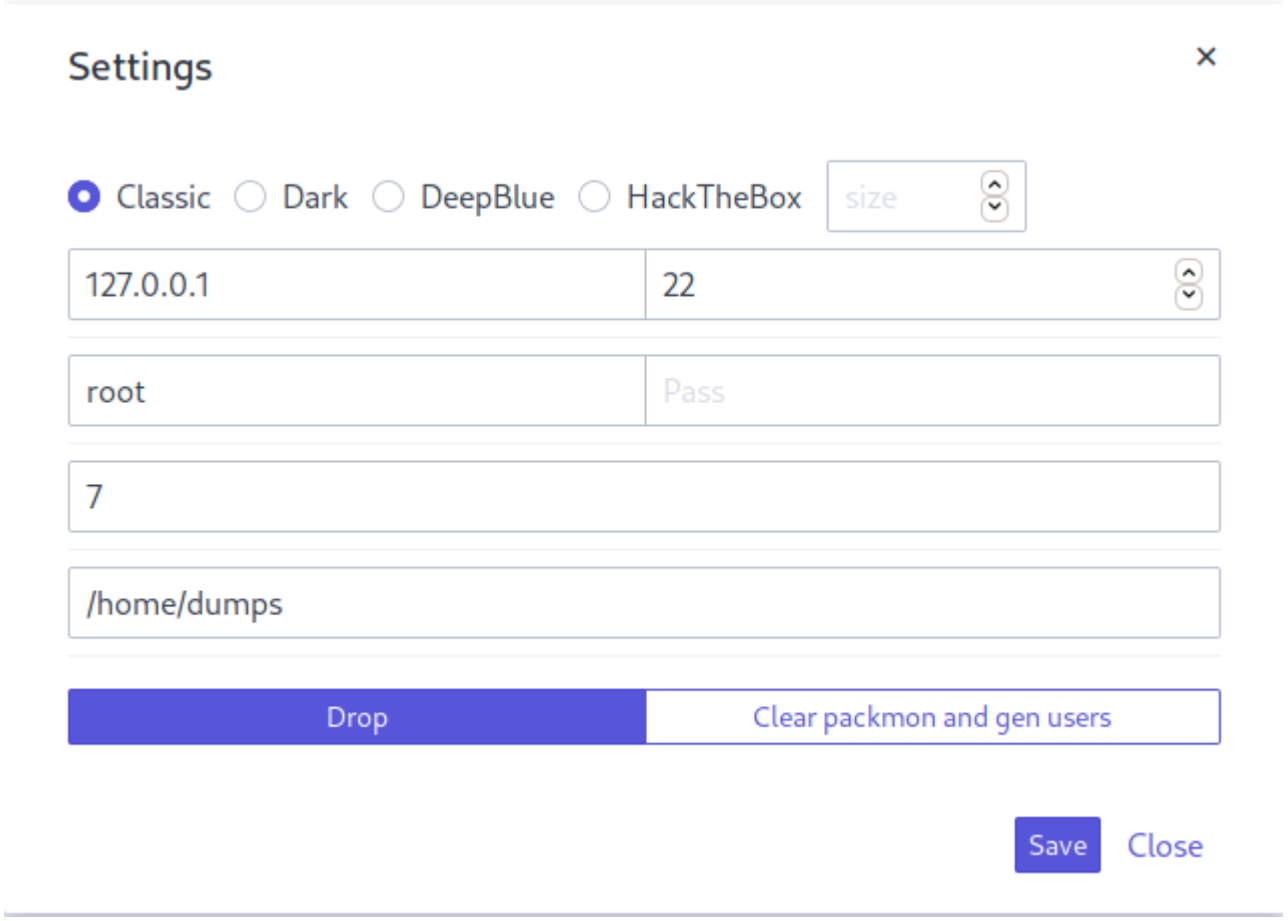
В трафике был найден исполняемый файл с вредоносными и подозрительными функциями

Поиск артефактов в трафике



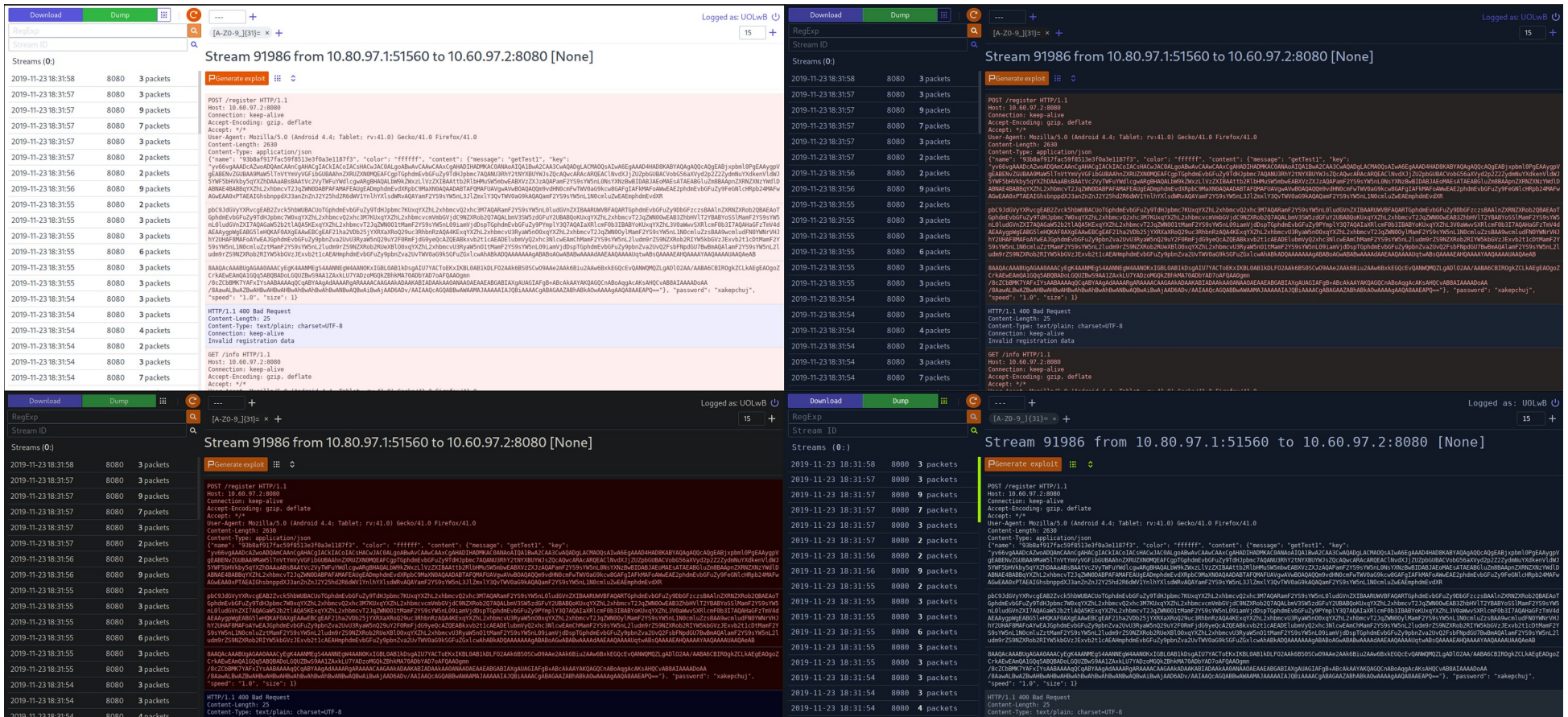
С помощью применения фильтра по содержимому были найдены подключения, в которых производились попытки SQL-инъекции.
По нажатию на кнопку «Generate exploit» можно сформировать скрипт на языке python для проверки эффективности защиты от этой атаки.

Автоматическое скачивание дампов сетевого трафика



В системе реализована возможность автоматического скачивания сетевого трафика с удалённого сервера по протоколу SSH. Параметры для этого задаются в диалоговом окне настроек.

Темы



Для удобства пользователя было разработано несколько тем оформления

Тестирование

Разработанный комплекс был успешно протестирован на следующих соревнованиях CTF:

ENOWARS 2019

RuCTFE
2019