



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

Download
Dump

⌂
+ None : 3771 " x
None : 4343 " x
None : 52724 " x
None : 35783 " x
None : 61092 " x
123 : 40000 " x

Logged as: KXhbl [⌵](#)

RegExp

[A-Z0-9_]{31}= x SAAR%7B[0-9A-Za-z_\-]{32}%7D x +

15 +

Streams (0:)

2020-02-23 14:35:52	40000	2 packets
2020-02-23 14:35:52	40000	6 packets
2020-02-23 14:35:51	40000	2 packets
2020-02-23 14:35:50	40000	2 packets
2020-02-23 14:35:49	40000	2 packets
2020-02-23 14:35:49	40000	2 packets
2020-02-23 14:35:49	40000	5 packets
2020-02-23 14:35:49	40000	2 packets
2020-02-23 14:35:48	40000	2 packets
2020-02-23 14:35:48	40000	2 packets
2020-02-23 14:35:48	40000	2 packets
2020-02-23 14:35:48	40000	2 packets
2020-02-23 14:35:48	40000	2 packets
2020-02-23 14:35:47	40000	2 packets

Generate exploit
⌵

```
GET /static../storage/storage.db HTTP/1.1
Host: 6.6.11.2:40000
User-Agent: python-requests/2.23.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

```
HTTP/1.1 303 See Other
Server: nginx/1.10.2
Date: Sun, 23 Feb 2020 14:35:52 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 33
Connection: keep-alive
Location: /login
Set-Cookie: upid=1; Domain=6.6.11.2; Path=/
<a href="/login">See Other</a>
```

```
GET /login HTTP/1.1
Host: 6.6.11.2:40000
User-Agent: python-requests/2.23.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: upid=1
```

Отсутствие готовых систем со схожим функционалом в открытом доступе.

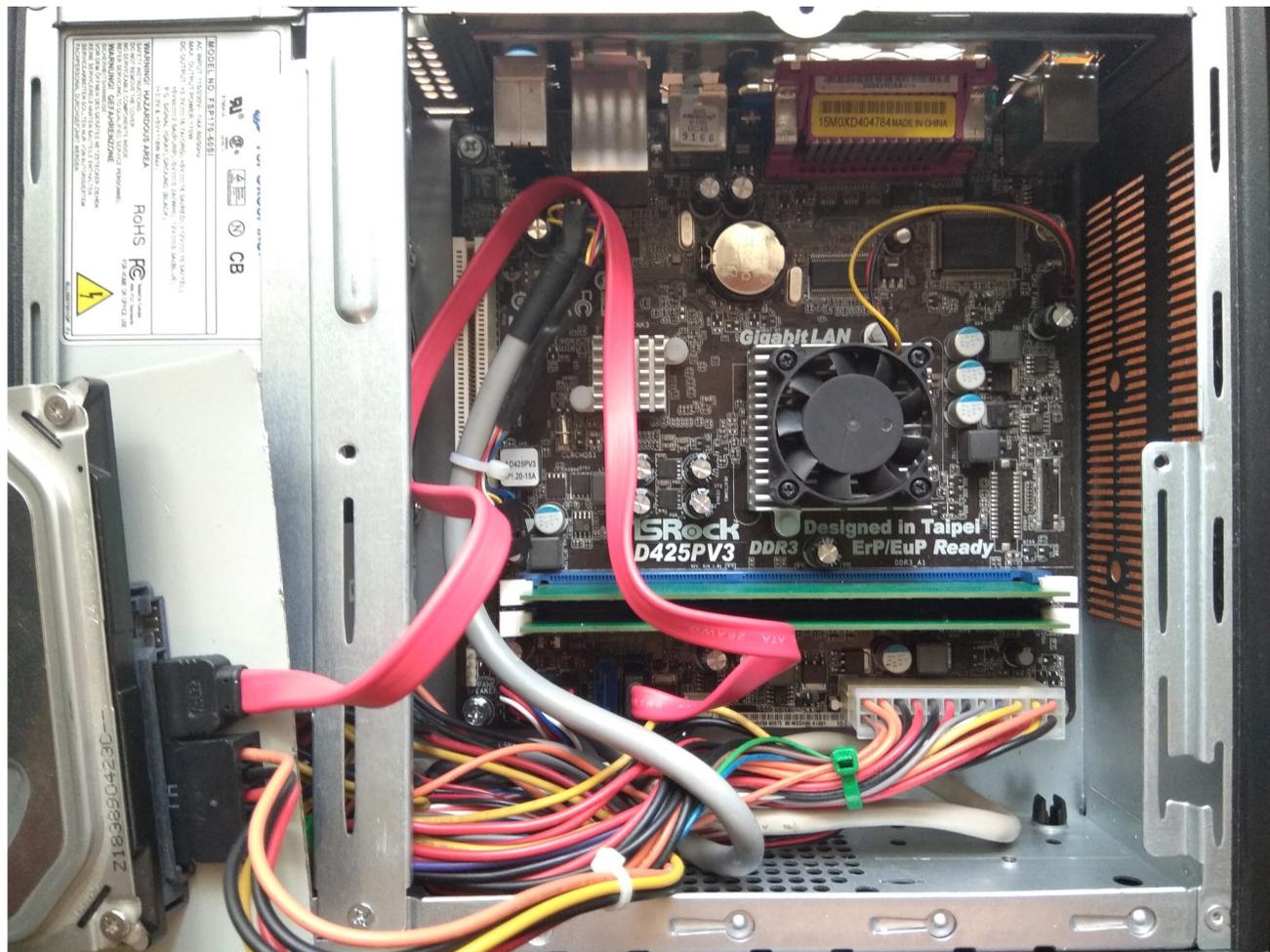
Широкие возможности для применения: для охраны сетевого периметра, вспомогательный инструмент компьютерного криминалиста, инструмент для участников CTF-соревнований.

Аппаратная платформа



Аппаратная платформа

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



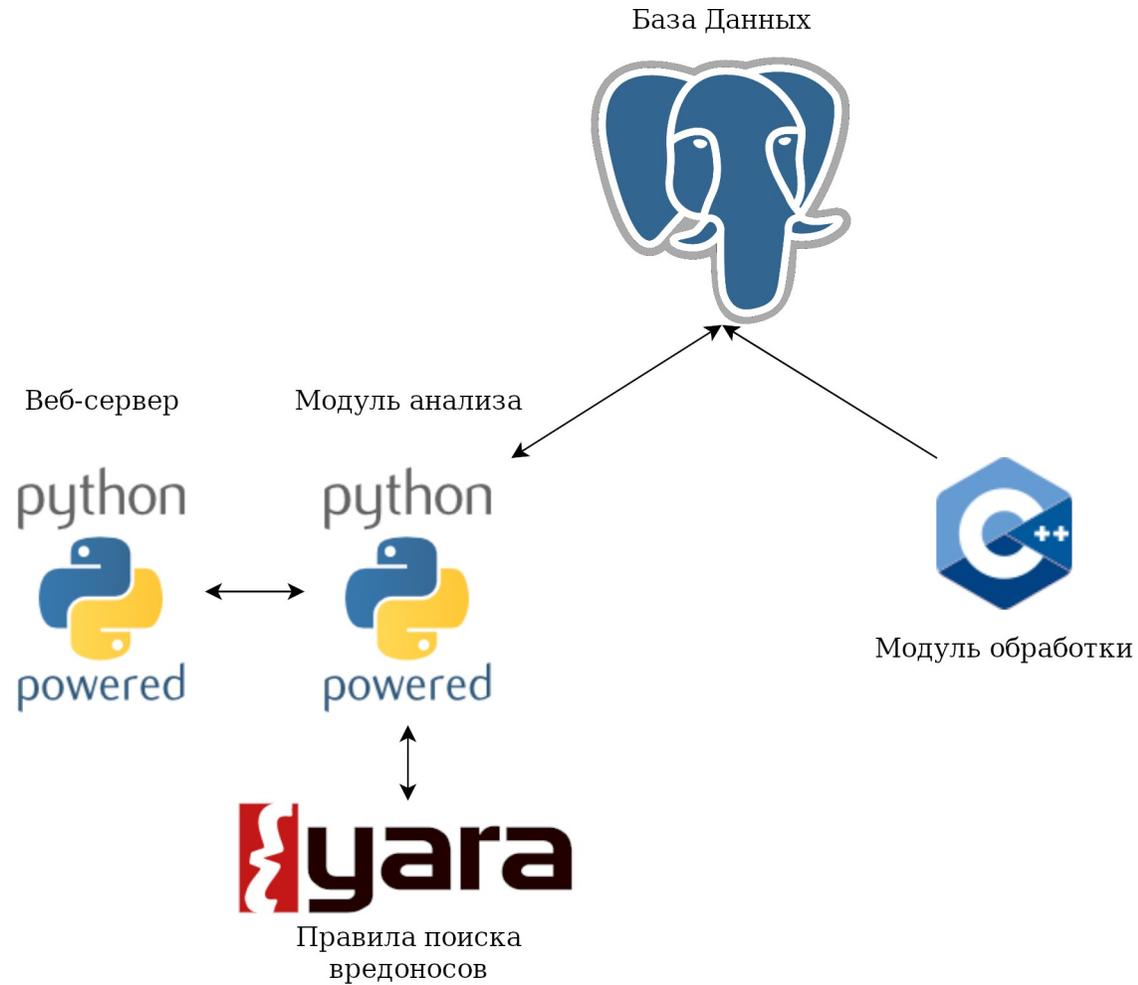
Характеристики аппаратной платформы

5

- форм-фактор корпуса – Mini-ITX;
- энергонезависимая память – 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

6



Хранение данных

7

→ В качестве базы данных была выбрана PostgreSQL

Сетевые соединения (потоки)

- Время установления соединения
- Количество пакетов
- Данные об отправителе
- Данные о получателе
- Результат анализа на вредоносный код

Сетевые пакеты

- Время отправки пакета
- Сторона, отправившая пакет
- Полезная нагрузка

Графический интерфейс системы

The screenshot shows a network analysis tool interface with several key components highlighted by red boxes and numbered 1 through 5:

- 1**: The top navigation bar containing 'Download' and 'Dump' buttons.
- 2**: The search bar containing a filter expression: `[A-Z0-9_]{31}=`.
- 3**: The top right corner showing the user is logged in as 'KXhbl' and a session timer at '15' minutes.
- 4**: A table listing network streams with columns for timestamp, IP address, and packet count.
- 5**: A detailed view of a selected stream (Stream 23039) showing HTTP request and response details, including headers and body content.

Streams (0:[A-Z0-9_]{31}=)
2020-02-23 14:35:20 40000 5 packets
2020-02-23 14:35:18 40000 239 packets
2020-02-23 14:34:48 40000 5 packets
2020-02-23 14:34:47 40000 239 packets
2020-02-23 14:34:24 4343 12 packets
2020-02-23 14:34:24 4343 9 packets
2020-02-23 14:34:24 4343 9 packets
2020-02-23 14:32:53 3771 9 packets
2020-02-23 14:32:53 3771 14 packets
2020-02-23 14:32:53 3771 9 packets
2020-02-23 14:31:24 4343 12 packets
2020-02-23 14:31:24 4343 9 packets
2020-02-23 14:31:24 4343 9 packets
2020-02-23 14:31:23 3771 9 packets
2020-02-23 14:31:23 3771 9 packets
2020-02-23 14:31:23 3771 14 packets
2020-02-23 14:29:53 3771 14 packets

```
Stream 23039 from 6.254.254.254:36177 to 6.6.11.2:40000 [flag;]
Generate exploit
service=2stu-ewvq-g8pe
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 23 Feb 2020 14:35:18 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 32
Connection: keep-alive
A84H60FSHXLXIOA7HLB8EB3B0865C71=
service=44rz-75ms-v9s0
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 23 Feb 2020 14:35:18 GMT
Content-Length: 0
Connection: keep-alive
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 23 Feb 2020 14:35:18 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 32
Connection: keep-alive
77ZCT9CB6AYPTEFEIEE1Z3457D9BA70=
POST /v1/deregister HTTP/1.1
Host: 6.6.11.2:40000
User-Agent: python-requests/2.22.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: upid=1; session_id=21ad8570-28de-45d5-85ef-8d19f48d7f45
Content-Length: 0
```

- 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

Автоматическое скачивание дампов сетевого трафика

Settings ×

Classic Dark DeepBlue HackTheBox ↑
↓

<input type="text" value="127.0.0.1"/>	<input type="text" value="22"/> ↑ ↓
<input type="text" value="root"/>	<input type="text" value="Pass"/>
<input type="text" value="7"/>	
<input type="text" value="/home/dumps"/>	

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

Темы

The screenshot shows the UOLWB interface with a list of network streams on the left and a detailed view of a selected stream on the right. The stream is identified as 'Stream 91986 from 10.80.97.1:51560 to 10.60.97.2:8080 [None]'. The detailed view shows a POST request to 'register HTTP/1.1' with various headers and a large body of data. The body contains a complex JSON payload with fields like 'name', 'color', 'message', 'password', and 'token'.

This screenshot is identical to the one on the left, showing the same network stream list and detailed view of a POST request. It demonstrates the consistency of the data across different views or instances of the application.

This screenshot is identical to the previous ones, showing the same network stream list and detailed view of a POST request. It further illustrates the application's ability to handle and display network traffic data.

This screenshot is identical to the previous ones, showing the same network stream list and detailed view of a POST request. It highlights the application's user interface and data processing capabilities.

Для удобства пользователей было разработано тем оформления

Тестирование

Разработанный комплекс был успешно протестирован на следующих соревнованиях CTF:



ENOWARS 2019



RuCTFE
2019