Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Кафедра:
Защищенных Сетей Связи (ЗСС)

Разработка программного модуля Threat Intelligence на базе Logstash

Автор:
Миколаени М. С.
Руководитель:
Скорых М. А., ассист. каф. ЗСС

Санкт-Петербург
2022

СПб ГУТ)))

Цель:

- Разработать модуль TI на базе Logstash

Задачи:

- Рассмотреть основные термины и определения TI;
- Рассмотреть принципы работы с различными базами репутации;
- Разработать программный модуль TI.

Базы репутации

Репутация - показатель, позволяющий определить, является ли рассматриваемый IP-адрес источником вредоносного трафика.
Примеры баз:

- Spamhaus XBL;
- Alienvault;
- Virustotal;
- AbuseIPDB;
- Teamcymru.




Взаимодействие с базами репутации

Рис. 1 - Алгоритм взаимодействия с базой репутации Alienvault

Взаимодействие с базами репутации

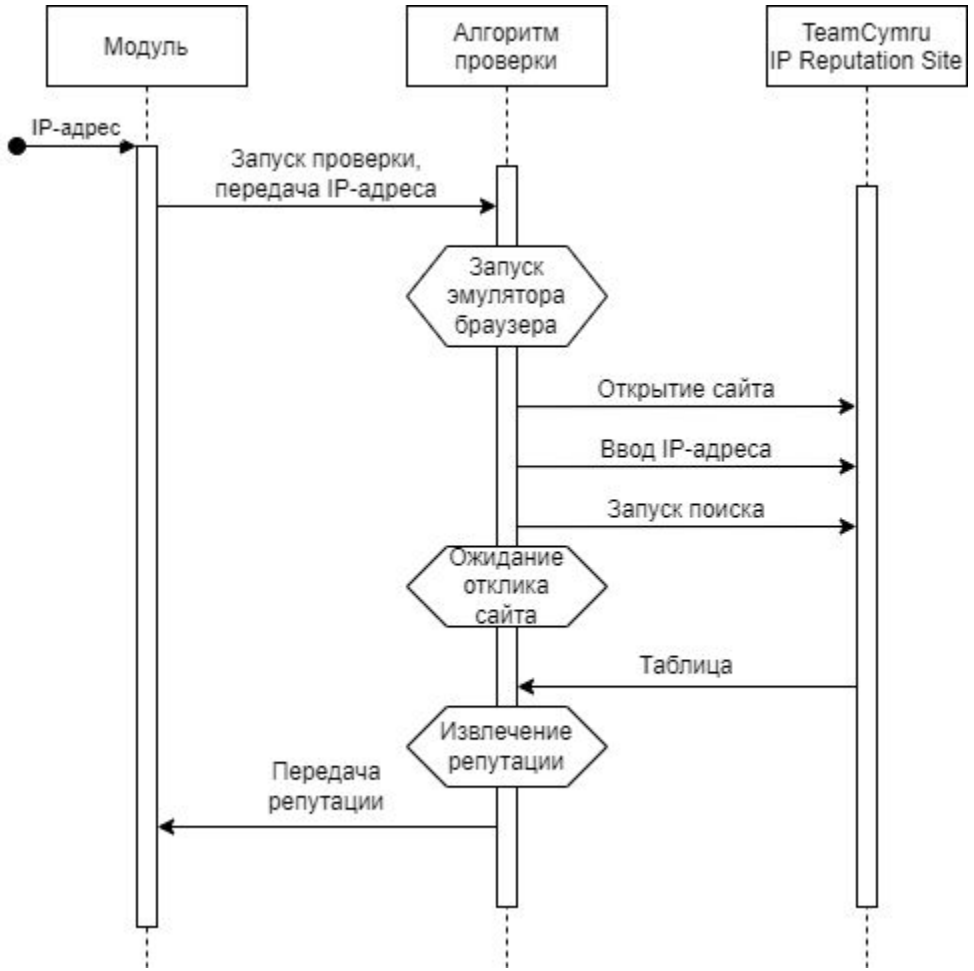

Рис. 2 - Алгоритм взаимодействия с базой репутации Teamcymru

Logstash

Logstash - это ПО для сборки, обработки и последующего перенаправления в конечное хранилище данных.

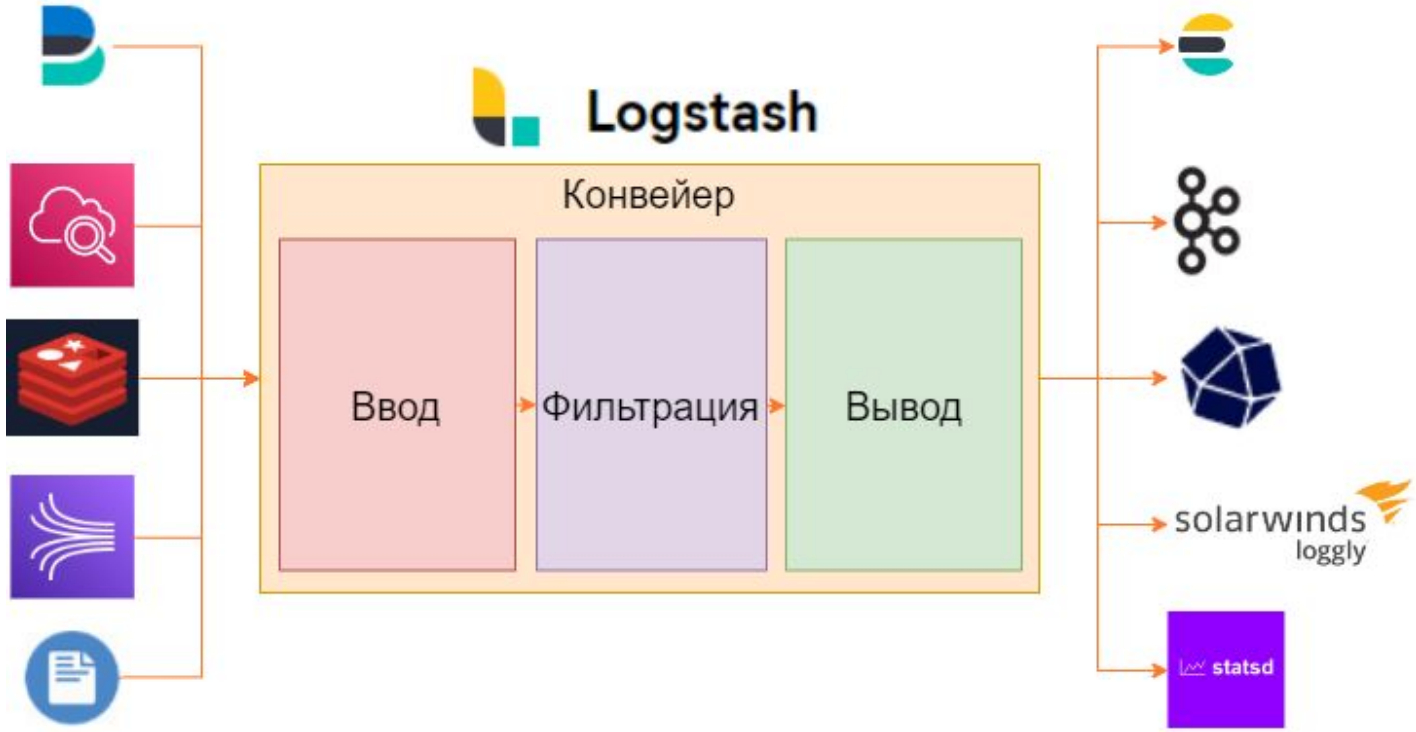

Рис. 3 - Алгоритм работы Logstash

Принцип работы

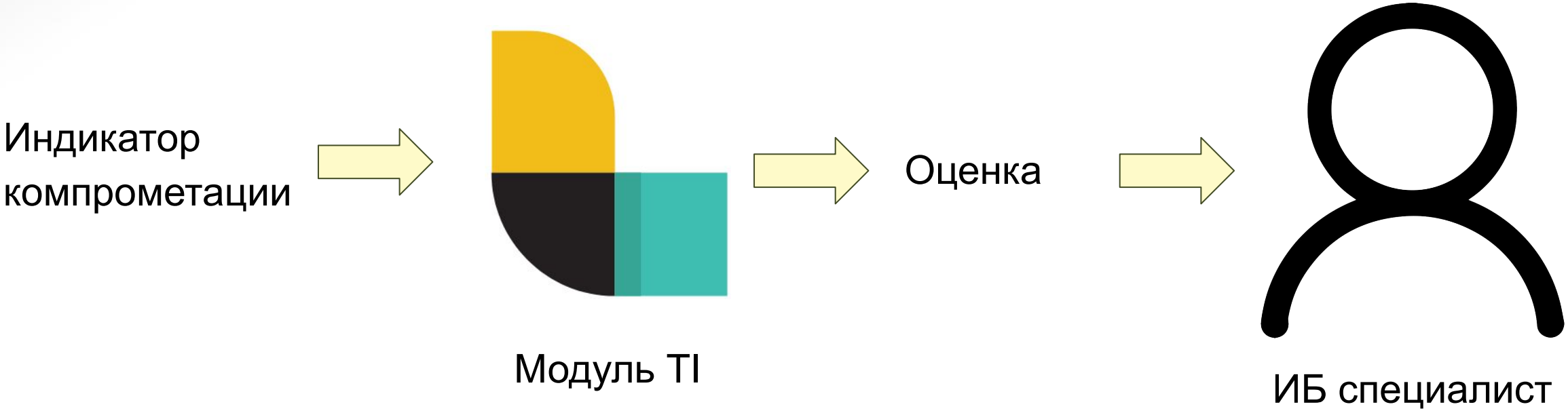

Рис. 4 - Принцип работы разработанного программного модуля

Алгоритм работы модуля

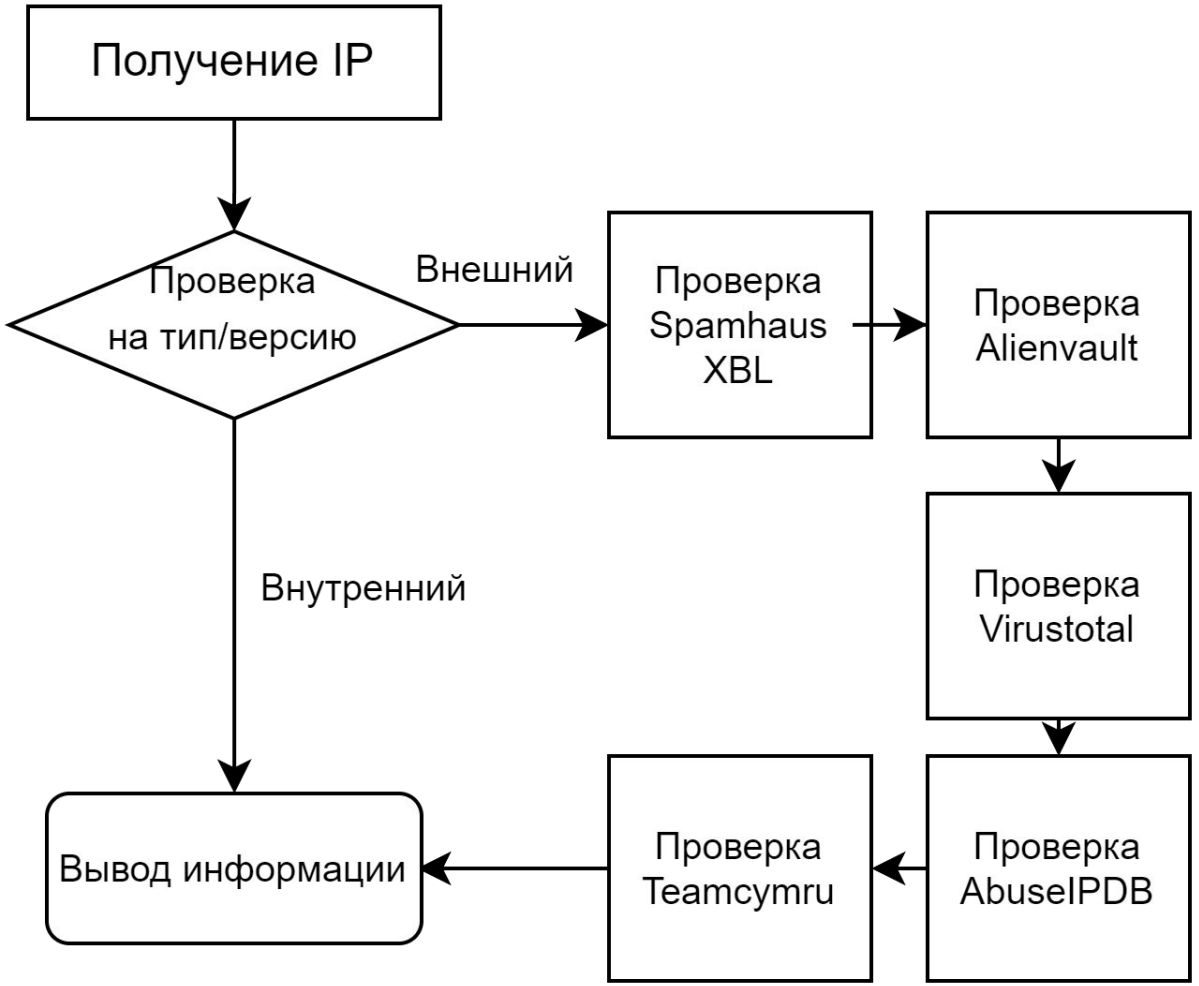

Рис. 5 - Внутренняя структура программного модуля

Тестирование

91.238.229.134 - СПбГУТ

```
{
   "alienvault_score" => 0,
   "abuseipdb_score" => 100,
   "teamcymru_score" => 38,
   "virustotal_score" => 0,
   "spamhaus_score" => 0,
   "Total match" => 2
}
```

IP Abuse Reports for **91.238.229.134**:

This IP address has been reported a total of **141** times from 72 distinct sources. 91.238.229.134 was first reported on February 23rd 2021, and the most recent report was **1 hour ago**.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	Date	Comment	Categories
derLoosi	1 hour ago	Hit on CMS login honeypot	Web App Attack
GeekOnTheHill	12 hours ago	GET /admin.php?f=/bmLUxZLeaiRIek7s/umvUsXN4HV g3BzRf.txt HTTP/1.1	Hacking, Web App Attack
FlyerOne	05 Jun 2022	IP blocked	Bad Web Bot, Web App Attack

Рис. 6 - Оценка IP-адреса 91.238.229.134 базой репутации AbuseIPDB

IP	Reputation Score	Days Observed	Category	Country Code
91.238.229.134	38	19	bot	

Рис. 7 - Оценка IP-адреса 91.238.229.134 базой репутации Teamcymru

Тестирование

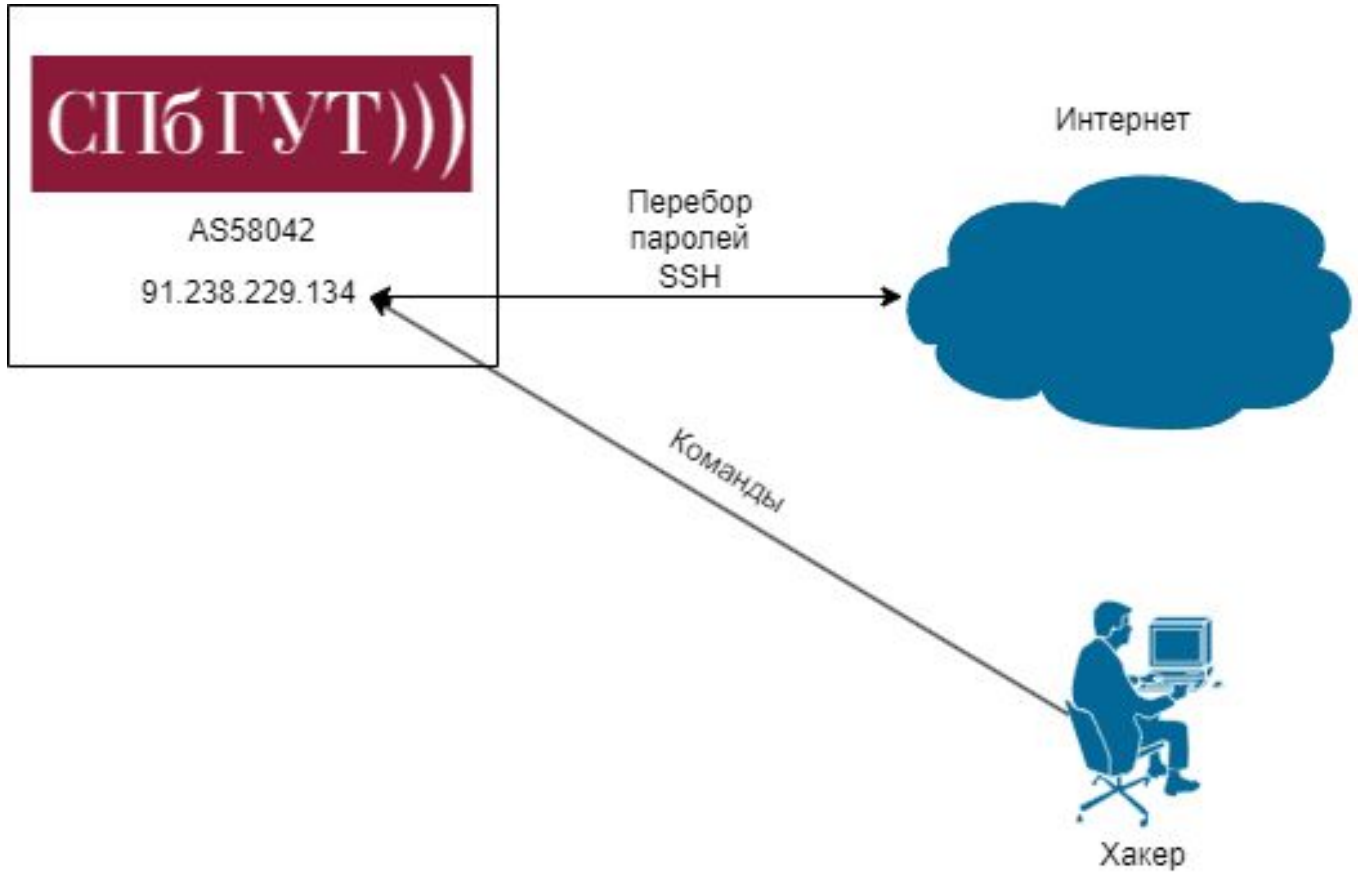

Рис. 8 - Предполагаемый метод компрометации СПбГУТ

Тестирование

203.248.175.71 - LG DACOM

```
{
   "virustotal_score" => -6,
   "spamhaus_score" => 0,
   "abuseipdb_score" => 100,
   "teamcymru_score" => 100,
   "alienvault_score" => 1
   "Total match" => 4
}
```

8.8.8.8 - Google DNS

```
{
   "Total match" => 0,
   "abuseipdb_score" => 0,
   "spamhaus_score" => 0,
   "alienvault_score" => 0,
   "virustotal_score" => 92,
   "teamcymru_score" => 1
}
```

2a02:6b8:a::a - yandex.ru

```
{
   "alienvault_score" => 0,
   "abuseipdb_score" => 0,
   "Total match" => 0
}
```

Заключение

- Поставленные в настоящем исследовании задачи выполнены, цель достигнута. В результате проделанной работы были рассмотрены основные понятия TI и разработан модуль для Logstash, анализирующий IP-адрес как один из популярных индикаторов компрометации.

Спасибо за внимание!