Средство исследования и анализа вредоносного ПО

Цель работы – создание программного продукта, на основе комплекта Open Source ПО, обеспечивающего возможность из единого пользовательского интерфейса управлять задачами по:

1. исследованию и анализу вредоносного ПО;
2. контролю и анализу сетевого трафика;
3. контролю целостности кода ОС, ОПО, СПО.

Среда реализации Debian (актуальной версии), рабочий стол LXDE.

Результатом работы должны быть:

1. исходный код разработанного приложения;
2. инструкция по сборке, установке, проверке функций разработанного ПО, инструкция по администрированию, инструкция по эксплуатации;
3. пояснительная записка с описанием классов ВПО;
4. контрольный пример анализа и исследования ВПО, содержащий не менее 3х экземпляров актуального ВПО каждого класса;
5. база ВПО, которая может использоваться для выявления и анализа ВПО без подключения к сети Интернет.

Состав функций средства исследования и анализа ВПО и предложения по использованию Open Source ПО для реализации данных функций приведены в таблице ниже (см. **Таблица 1**):

**Таблица 1**

|  |  |  |
| --- | --- | --- |
| № п/п | Требование к функциям средства анализа ВПО | Предложения по выбору Open Source ПО |
| 1. | Исследование ВПО | Cuckoo Sandbox |
| 1.1. | Автоматизированное создание защищенной среды исполнения кода ВПО |
| 1.2. | Автоматическое выявление характеристик ВПО (в т.ч. процессы, файлы, ключи реестра, URL, IP-адреса, EMAIL-адреса, DNS-имена, признаки сетевого трафика, признаки программного кода, признаки обрабатываемых данных) |
| 2. | Анализ трафика ВПО, выявление аномалий сетевых взаимодействий | Suricata, Snort, Moloch + Elastic Search |
| 3. | Выявление ВПО, реагирование на инциденты |  |
| 3.1. | Автоматическая классификация ВПО на основе их характеристик | Yara |
| 3.2. | Реагирование на инциденты, обогащение данных по инцидентам | TheHive |
| 3.3. | Возможность применения облачных антивирусных технологий для выявления ВПО | Cortex |
| 3.4. | Ведение реестра ВПО | Интеграция с MISP |
| 4. | Анализ кода ВПО | IDA Pro, GDB |
| 4.1. | Дизассемблирование кода ВПО |
| 4.2. | Удаленная отладка кода ВПО на различных платформах. |
| 4.3. | Декомпилирование кода ВПО |
| 4.4. | Предоставление программного интерфейса для создания расширений (плагинов) специального анализа кода ВПО |
| 5. | Контроль целостности кода ОС, СПО, ОПО | OSSEC HIDS |