DOI 10.58351/2949-2041.2024.10.5.017
УДК 004.622

Выжигин Александр Юрьевич,
кандидат технических наук, доцент, заведующий кафедрой,
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации; кандидат технических наук,
доцент, Российский технологический университет МИРЭА, г.Москва
Vyzhigin Alexander Yurievich, Candidate of Technical Sciences, Associate Professor,
Head of Department Russian Academy of National Economy and Public Administration
under the President of the Russian Federation; candidate of technical sciences,
associate professor Russian Technological University MIREA, Moscow
SPIN-code:5086-0171; ResearcherID:T-9882-2018

Москалев Илья Сергеевич, студент,
МИРЭА – Российский технологический университет, г.Москва
Moskalev Ilyia Sergeevich, student,
MIREA – Russian Technological University, Moscow

Селин Андрей Александрович, кандидат технических наук,
МИРЭА – Российский технологический университет, г. Москва
Selin Andrei Aleksandrovich, Candidate of Technical Sciences,
MIREA – Russian Technological University, Moscow

Трубиенко Олег Владимирович,
кандидат технических наук, доцент, заведующий кафедрой,
МИРЭА – Российский технологический университет, г. Москва
Trubienko Oleg Vladimirovich, Candidate of Technical Sciences,
Associate Professor, Head of the Department,
MIREA – Russian Technological University, Moscow

АНАЛИТИКА ДАННЫХ КАК ИНСТРУМЕНТ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
DATA ANALYTICS AS A TOOL FOR SOLVING INFORMATION SECURITY PROBLEMS

Аннотация: Анализ данных важен во всех сферах жизни, в том числе в сфере информационной безопасности (ИБ). Задачи ИБ решаются с помощью сканеров безопасности или информационно-аналитических систем безопасности (ИАСБ). Сканеры (nmap, masscan, lynis, nikto и т.д.) решают задачи, связанные с обеспечением безопасности персональных компьютеров (ПК) и периферийных устройств (ПУ). Но все это не дает нам качественного результата. Вариант решения задачи через ИАСБ дает результат, необходимый для полной функциональной работы аналитика кибербезопасности.

ИАСБ предназначена для решения задач расследования киберинцидентов. Ее функционал – сбор и анализ информации, а также вывод аналитической отчетности, удобной пользователю для принятия решений о создании этапов борьбы с найденными угрозами и уязвимостями ПК иперифериных устройств (ПУ).

Научная новизна исследования заключается в следующем:

1. расширены возможности средств администрирования ПК и ПУ за счет применения методов вычислительной математики;

2. разработан улучшенный метод сканирования ПК и ПУ за счет интеграции нескольких программных комплексов;

3. разработан метод извлечения информации посредством применения технологии абстрактного синтаксического дерева;

4. разработана интеграция технологии получения информации из открытых источников для создания рекомендательного модуля в ИАСБ.

Цель работы – повышение эффективности работы средств администрирования безопасности персональных компьютеров и периферийных устройств за счет создании композиции из интеграции ряда программных комплексов, а также применения предиктивной аналитики для обозначения порядка решения задач в устранении угроз и уязвимостей ПК и ПУ.

Метод или методология проведения работы: в статье использовались такие методы как: OSINT (поиск информации из открытых источников, метод деловой разведки, суть которого заключается в получении конкретного ответа на конкретный вопрос); предиктивная аналитика (процесс прогнозирования информации на основе полученных данных); системное администрирование (процесс поддержки программных обеспечений в ПК).

Результаты: разработан функционал информационно-аналитической системы безопасности, использующий утилиты безопасности персональных компьютеров и периферийных устройств, алгоритмы предиктивной аналитики и практики методов деловой разведки.

Область применения результатов: полученные результаты могут использоваться работниками органов исполнительной власти нашей страны, а также обычными пользователями данной ИАСБ для оперативного получения информации, необходимой для обеспечения безопасности своих ПК и ПУ.

Abstract. Data analysis is important in all areas of life, including information security **(**IS). IS tasks are solved with the help of security scanners or information analytic security systems **(**IASS). Scanners **(**nmap, masscan, lynis, nikto, etc.) solve problems related to the security of personal computers **(**PC) and peripheral devices **(**PD). But all this does not give us a qualitative result. The variant of solving the problem through IASB gives the result required for a fully functional cybersecurity analyst. IASB is designed to solve cyber incident investigation tasks. Its functionality is to collect and analyze information, as well as the output of analytical reporting, convenient for the user to make decisions on the creation of steps to combat the found threats and vulnerabilities of PCs and peripheral devices **(**PD).

Scientific novelty of the research consists in the following:

1) the possibilities of PC and PU administration tools are extended by applying the methods of computational mathematics;

2) an improved method of PC and PU scanning is developed due to the integration of several program complexes;

3) a method of information retrieval through application ofAbstract syntax tree technology was developed;

4) integration of open source information retrieval technology to create a recommendation module in IASB is developed.

Work purpose

increasing the efficiency of security administration tools for personal computers and peripheral devices by creating a composition of integration of a number of program complexes, as well as the use of predictive analytics to indicate the order of problem solving in eliminating threats and vulnerabilities of PCs and PUs.

Methodology

in the article were used such methods as: OSINT (search for information from open sources, a method of business intelligence, the essence of which is to obtain a specific answer to a specific question); predictive analytics (the process of predicting information based on the obtained data); system administration (the process of supporting software in PCs).

Results: developed the functionality of an information-analytical security system using security utilities for personal computers and peripheral devices, algorithms of predictive analytics and the practice of business intelligence methods.

Practical implications

the obtained results can be used by the employees of the executive authorities of our country, as well as by ordinary users of this IASB to promptly obtain the information necessary to ensure the security of their PCs and PIs.

Ключевые слова: информационно-аналитическая система, предиктивная аналитика, АСД, информационная безопасность, деловая разведка, язык запросов Googledorks, язык программирования Python, интерполяция функции, datascience, вычислительная математика.

Keywords: Information analytics, predictive analytics, ASD, information security, business intelligence, Googledorks query language, Python programming language, function interpolation, data science, computational mathematics. не проверял еще.

Введение

В современном мире из-за увеличения хакерских группировок, а также повышения уровня их подготовки, существует проблема обеспечения безопасности данных на персональных компьютерах и периферийных устройствах. Вопрос обеспечения безопасности информации стоит остро как никогда. В эпоху передовых информационных технологий формируется мнение, что использование хвалёного качественного инструмента для обеспечения информационной безопасности ПК и ПУ обеспечит долгосрочную защиту от утечек информации, повреждений системы ПК, запрет на перехват трафика ПК и ПУ и т.д. Но это далеко не так. Не смотря на наличие средств защиты информации от крупных ИБ гигантов, как КОД БЕЗОПАСНОСТИ, по сей день ведутся научные разработки в сфере обеспечения информационной безопасности.

Для решения поставленной проблемы было проведено исследование, цель которого – повышение эффективности работы средств администрирования безопасности ПК и ПУ за счет создания композиции из интеграции ряда программных комплексов, а также применения предиктивной аналитики для обозначения порядка решения задач в устранении угроз и уязвимостей ПК и ПУ.

Для достижения поставленной цели были решены следующие задачи:

- проведен обзор и анализ существующих информационно-аналитических систем безопасности;
- проведено описание предлагаемой ИАСБ;
- описана интеграция сканеров безопасности в информационно-аналитическую систему;
- описан метод извлечения информации с помощью технологии обработки данных с помощью абстрактного синтаксического дерева;
- описана математическая модель машинного обучения;
- проведено описание работы информационно-аналитической системы безопасности для решения профессиональных задач;
- проведено тестирование работоспособности ИАСБ;

Анализ существующих информационно-аналитических систем безопасности

Для разработки улучшенной ИАС требуется провести обзор и анализ уже существующих систем. Рассмотрим некоторые из них (табл. 1).

Таблица 1

Сравнение ИАС

	Anomali	EclecticIQ	ThreatConnect	Threat Intelligence Platform
Интеграция существующих отчетов в систему	+	+	+	-
Количество встроенных средств сбора и анализа информации	100+	20-100	100+	20-100
Форматы представления данных	csv, json, http	csv, json, http	csv, json, http	csv, json, http
Поиск совпадений в SIEM-системах	+	+	+	+
Интеграция со сторонними системами ИБ	+	+	+	+
Интеграция по REAT API	+	+	+	+
Отображение информации в виде графов	+	+	+	-

Anomali. Является системой анализа угроз возникновения киберинцидентов. Устанавливается на виртуальной машине, интегрируется с SIEM-системами, анализирует разведывательные отчеты, имеет множество встроенных инструментов для поиска и анализа информации о состоянии защищенности системы ПК. Поддерживает форматы данных: csv, json, http.

EclecticIQ. Система «EclecticIQ» анализирует уже собранные аналитиками данные по инцидентам кибербезопасности. В работе использует протокол передачи данных TLP. Он нужен для пересылки конфиденциальной информации специалистам, с соответствующим уровнем доступа.

ThreatConnect. ThreatConnect автоматизирует сбор и анализ полученной информации с помощью агрегации данных. Интегрируется с SIEM-системами. Предоставляет информацию в расширенном виде.

ThreatIntelligencePlatform.Обеспечивает поиск и анализ информации с дальнейшим ее нормированием, передачу обработанных данных на внутренние средства защиты.

По результатам сравнения лучшими являются системы Anomali и ThreatConnect, так как они предоставляют максимально полный спектр своих услуг.

Описание функциональности предложенного решения

Для устранения проблем при решении задач поиска и анализа информации критических информационных инфраструктур была разработана собственная информационно-аналитическая система безопасности (ИАСБ) (рис. 1).

Рис. 1 Описание функционалов разработанной ИАСБ в нотации IDEF0

На рисунке 1 изображена диаграмма IDEF0, где отображены все функционалы ИАСБ.

Ввод IP-адреса – начальный этап работы ИАС безопасности. Он нужен для определения объекта поиска и анализа информации. Под IP-адресом могут подразумеваться совершенно разные объекты, в том числе персональные компьютеры и периферийные устройства.

Сбор информации с помощью АПК (аппаратно-программных комплексов). Информация собирается с помощью сканеров, которые интегрируются в систему для отображения состояния защищенности критической информационной инфраструктуры.

Анализ информации. Полученные данные предобработаны с целью отображения максимально качественной информации для решения профильных задач специалистами по кибербезопасности, а также для контроля безопасности ресурсов домашними пользователями. Нормализация данных в таблице дает более четкое и качественное понимание текущей отображаемой ситуации объекта критической информационной инфраструктуры.

Рекомендательная информация. Здесь было интегрировано 2 вида анализа данных: методы деловой разведки и текстовая аналитика. Первый вид предназначен для сбора информации по конкретно введенному вопросу: «угрозы и уязвимости порта *номер_порта*». Система выведет рекомендации для устранения угроз и уязвимостей введенного порта из найденных в списке. Текстовая аналитика выполняет одну из главных ролей в поиске рекомендаций: извлечение основной информации с выбранной системой сайта.

Для улучшения качества работы системы создана обертка в виде docker-контейнера. С помощью системы контейнеризации, разработанная ИАСБ работает качественнее и быстрее, благодаря асинхронному выполнению задач при работе системы.

Интеграция аппаратно-программных комплексов в ИАСБ

Важным этапом получения и анализа информации об объекте безопасности является использование сканеров безопасности. Сканер безопасности – это программное решение для диагностики инфокоммуникационной сети. Именно за счет них происходит поиск и анализ информации по IP-адресу. Так как разработанная ИАСБ проектировалась на базе операционного семейства Linux, сделать интеграцию не сложно. В языке разработки Python есть библиотека subprocess. В ней метод call () выполняет задачи с использованием стороннего языка программирования (рис. 2).

```
# Masscan сканирование и сохранение в JSON
masscan_cmd = f'masscan {ip} -p80,443,8000-8100,0-200 --rate=20 -oJ masscan_output.json'
subprocess.run(masscan_cmd, shell=True)
```

Рис. 2 Интеграция скрипта сканера masscan в ИАСБ

Технология АСД (абстрактное синтаксическое дерево)

Конвертация данных из форматов JSON и XML не всегда проста, как это может показаться на первый взгляд. Например, в разработанной информационно-аналитической системы при попытке получения информации по ключу выдавалась лишь буква самого значения. И здесь как раз обнаружилась погрешность обработки данных сканеров. Для решения этой проблемы была внедрена технология абстрактного синтаксического дерева (АСД). АСД – это синтаксическая модель описания работы программы. Работу данной технологии отображена в блок-схеме (рис. 3).

Рис. 3 Блок-схема описания работы АСД в ИАСБ

Отдельно стоит остановиться на функции литерального считывании данных. Она распознает код в комментариях и выполняет его. Анализ выражения с помощью такого метода может быть затруднительным, но с точки зрения безопасной разработки приложений этот вариант является наиболее пригодным для использования.

Предиктивный анализ данных объекта критической информационной инфраструктуры

Одной из составляющих в работе ИАС безопасности является выявление действительного затрачиваемого времени на обработку данных по найденным портам. Для этого процесса вычисления будут извлекаться из таблицы ниже (рис. 4).

	port	ttl	timestamp
14	443	63	1.01808e+22
12	8080	63	4.81092e+16
11	80	63	4.76329e+14
9	25	63	1.48853e+14
13	22	63	1.3099e+14
10	21	63	1.25036e+14

Рис. 4 Пример таблицы после проведения предиктивного анализа данных для вычисления времени на обработку данных по портам

Для подсчета времени необходимо:

1. Составить уравнения по столбцам («port», «ttl»);
2. Найти их корни (также извлечь действительную часть корней, если корни комплексные);
3. Объединить в вектор значений;
4. Перемножить корни, чтобы получить константу для подстановки в уравнение для расчета столбца «timestamp» (timestamp = abs (port*c + ttl), где c – посчитанная константа)

С точки зрения истинности, результаты, посчитанные таким путем, совпадают с их реальными значениями в области сетевых технологий.

Например:

1. порт 443 – поддержка протокола SSL;
2. порт 8080 – альтернативный порт протокола HTTP;
3. порт 80 – порт протокола HTTP;
4. порт 25 – порт для пересылки сообщений по электронной почте (протокол SMTP);
5. порт 22 – Secure Shell (SSH) порт для шифрования сетевых служб;
6. порт 21 – (FTPS) порт для безопасной передачи файлов;

В данном примере отражено совпадение математических расчетов с действительностью.

Исследование работоспособности информационно-аналитической системы СканБез

Для исследования работоспособности ИАСБ СканБез выполним один из запросов (рис. 5).

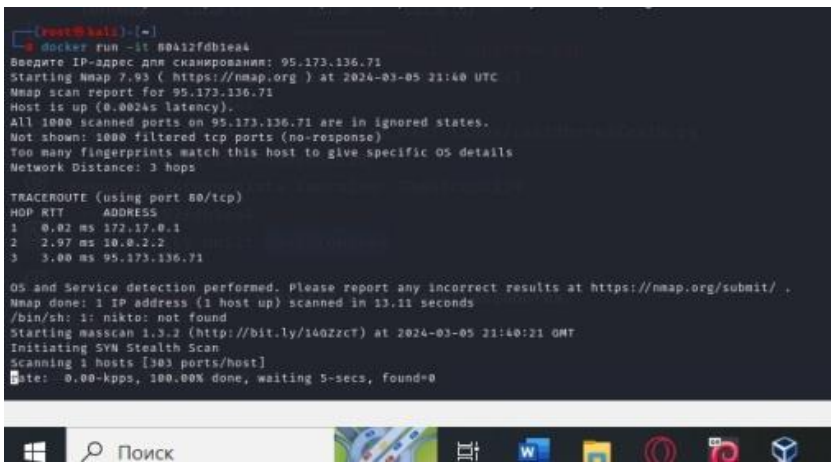

Рис. 5 Ввод данных в ИАСБ

Алгоритм работы ИАС безопасности:

1. При запуске системы ввести IP-адрес для проверки инфраструктуры.

2. Подождать немного времени и получить результаты, необходимые для анализа и дальнейших действий

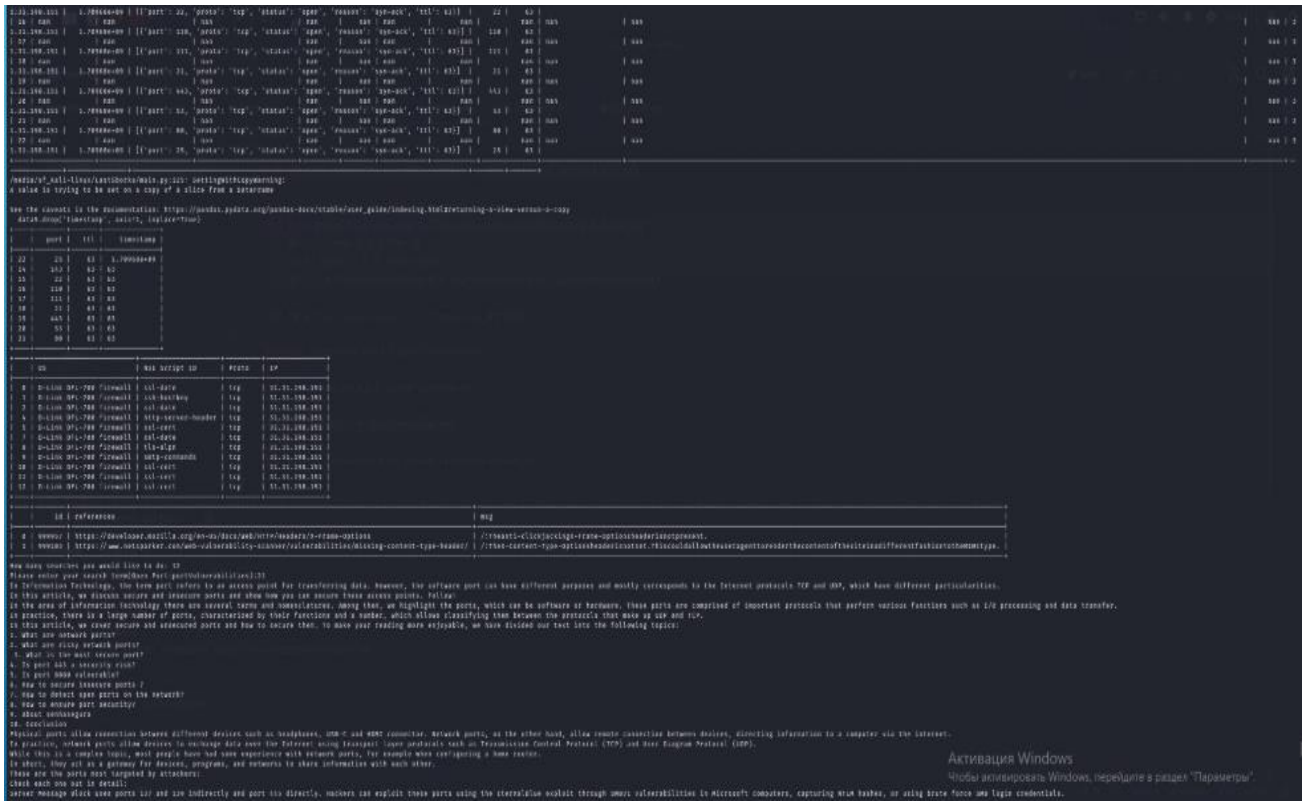

Рис. 6 Пример обработки данных в ИАСБ

Изучив данные рисунки, можно с уверенностью сказать, что разработанная информационно-аналитическая система безопасности работает качественно в соответствии со своим функционалом.

Заключение

Проведенные эксперименты доказали эффективность совместного использования средств администрирования безопасности персональных компьютеров, периферийных устройств и предиктивной аналитики. Цель работы была достигнута. Расширены возможности средств администрирования ПК и ПУ за счет применения методов вычислительной математики. Разработан улучшенный метод сканирования ПК и ПУ за счет интеграции нескольких программных комплексов. Разработан метод извлечения информации посредством применения технологии абстрактного синтаксического дерева. Разработана интеграция технологии получения информации из открытых источников для создания рекомендательного модуля в ИАСБ, функционал которой позволяет решать производственные задачи в масштабах предприятия.

Список литературы:

1. Галыгина Л. В., Галыгина И. В. Социальные аспекты информационной безопасности. Лабораторный практикум. М.: Лань. 2021. 64 с.

2. Гришина Н. В. Основы информационной безопасности предприятия. Учебное пособие. М.: Инфра-М. 2021. 216 с.

3. Христинич И.В. Информационная безопасность в сети Интернет // Законность. 2022. N 4. С. 20 – 23.

4. Новикова Е. Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи. М.: Academia. 2018. 192 с.

5. Белов А. С. Модернизация системы информационной безопасности = Modernizationofthe Information Security System: The ApproachtoDeterminingthe Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. – 2022. – № 4. – С. 76-80.

6. Васильков, А.В. Безопасность и управление доступом в информационных системах. Учебное пособие / А.В. Васильков. – М.: Форум, 2021. – 463 с.

7. Девянин, П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. – М.: Радио и связь, 2018. – 176 с.

8. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. – М.: Форум, Инфра-М, 2021. – 416 с.

References:

1. Galygina L. V., Galygina I. V. Social Aspects of Information Security. Laboratory practice. Moscow: Lan. 2021. 64 c.

2. Grishina N. V. Fundamentals of information security of the enterprise. Study guide. Moscow: Infra-M. 2021. 216 c.

3. Khristinich I.V. Information security in the Internet // Legality. 2022. N 4. C. 20 – 23.

4. Novikova E. L. Provision of information security of info-communication networks and communication systems. Moscow: Academia. 2018. 192 c.

5. Belov, A. S. Modernization of the Information Security System = Modernization of the Information Security System: The Approach to Determining the Frequency / A. S. Belov, M. M. Dobryshin, D. E. Shugurov // Information Protection. Insight. – 2022. – № 4. – C. 76-80.

6. Vasilkov, A.V. Security and access control in information systems. Study guide / A.V. Vasilkov. – Moscow: Forum, 2021. – 463 c.

7. Devyanin, P.N. Security analysis of access control and information flows in computer systems / P.N. Devyanin. – Moscow: Radio and Communications, 2018. – 176 c.

8. Shangin, V.F. Information security of computer systems and networks / V.F. Shangin. – Moscow: Forum, Infra-M, 2021. – 416 c.