УДК 004.451

ХАРУК Р. В.

ОБРАБОТКА ДАННЫХ ИЗ ЖУРНАЛА АУДИТА В СИСТЕМАХ МОНИТОРИНГА СОБЫТИЙ БЕЗОПАСНОСТИ

В статье представлен метод и алгоритмы обработки данных о событиях безопасности в системе мониторинга событий безопасности, предлагается новый универсальный формат для представления событий аудита в системе. Новая структура позволит осуществить представление данных распространенных систем аудита в формализованном виде, удобном для дальнейшей обработки и автоматического анализа. Это способствует ускорению обработки данных событий. При обработке определяется принадлежность каждого события к классам событий. Данное решение позволяет выделять наиболее опасные (класс событий-тревог) из всех событий, что, в свою очередь, облегчает весь процесс анализа.

In article methods and algorithms of data processing about safety events in system of monitoring of events of safety are developed, the new universal format for representation of events of auditing system is offered. The new structure will allow implementing data presentation of widespread auditing systems in the formalized kind convenient for the further processing and the automatic analysis. It promotes acceleration of data processing of events. At processing the accessory of each event to classes of events is defined. The given decision allows allocating the most dangerous (a class of events-alarms) from all events that, in turn, facilitates all process of the analysis.

Введение

Наблюдение за действиями программ и компонентов операционной системы рабочего места является одним из важных компонентов системы безопасности информационной системы. В операционных системах существует несколько принципиально различных методов сбора событий, связанных с файловой системой: перехват запроса к драйверу файловой системы и перехват системных вызовов операционной системы.

Рассмотрим второй метод, который является наиболее распространенным.

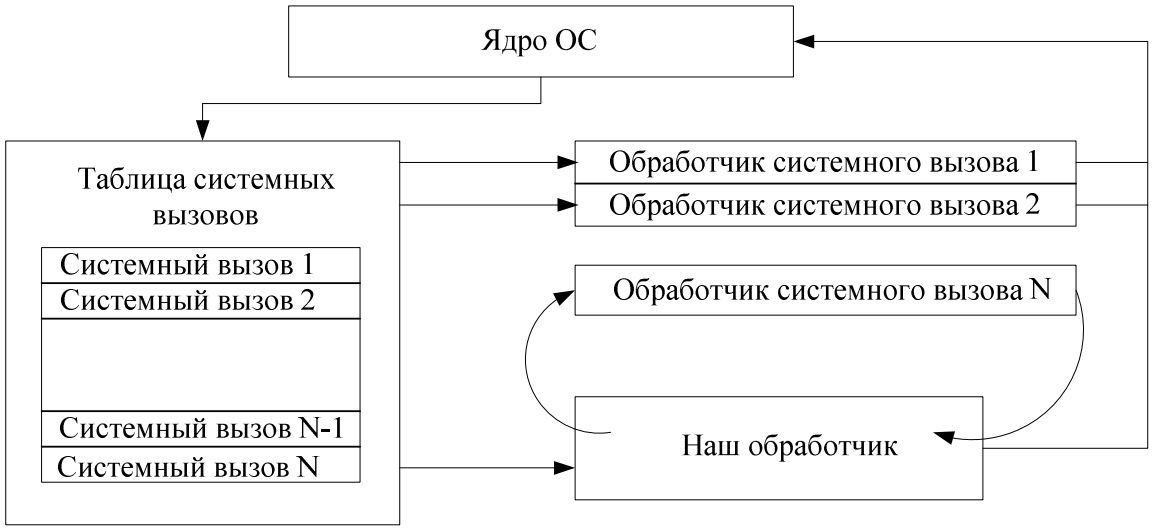

Рис. 1 - Схема перехвата системных вызовов операционной системы

Возможности регистрации событий безопасности реализованы в сетевых операционных системах (ОС) и прикладном программном обеспечении (ПО). Однако, ощутимый эффект от использования средств аудита достигается лишь тогда, когда зарегистрированные данные о событиях безопасности могут быть оперативно проанализированы. Только в этом случае становится возможным своевременное обнаружение вредоносных воздействий на элементы информационной системы – компьютеры, программное обеспечение, передаваемые и хранящиеся данные и т.д. Наличие подсистем регистрации событий безопасности является одним из основных требований, которое присутствует во всех совре-

менных стандартах и руководящих документах по информационной безопасности компьютерных систем[1].

Одним из наиболее важных этапов в системе мониторинга событий безопасности является этап первоначальной обработки данных из журналов аудита.

Постановка задачи

Целью статьи является упрощение процесса анализа событий безопасности посредством введения нового формата представления данных о событиях безопасности, а также уменьшение времени поиска нужного типа событий среди всего журнала аудита путем разделения событий на классы по уровню опасности.

Анализ данных

Анализ форматов и структур представления данных о событиях безопасности, принятых в существующих системах аудита позволяет определить и выделить основные поля данных, характеризующие события безопасности, и разработать универсальный формат для внутреннего представления событий безопасности в системе.

В ОС семейства Linux каждая строка текстового файла журнала аудита является отдельной записью о событии[2]. Значения отдельных полей разделяются пробелом. Каждая строка – запись о событии обычно содержит следующую информацию:

- дату и время регистрации события;
- символьный идентификатор модуля, зарегистрировавшего событие;
- подробное описание события.

События могут регистрироваться различными модулями. Например, идентификатор модуля «$AUDIT» обозначает, что событие зарегистрировано основным модулем аудита. Для записей о событиях, генерируемых этим модулем характерна структура подробного описания события, состоящая из следующих полей:

- идентификатор типа события;
- идентификатор пользователя (UID), в сеансе которого произошло событие;
- идентификатор группы пользователя (GID), в сеансе которого произошло событие;
- информация об операции (функции) и ее параметрах.

В ОС семейства Microsoft Windows NT для доступа к данным аудита необходимо использовать специальные функции, которые обеспечивают считывание данных аудита в буферы в оперативной памяти, формат которых хорошо документирован[2].

Запись о событии аудита в ОС семейства Microsoft Windows NT содержит следующую информацию[3]:

- порядковый номер события;
- время регистрации и время записи события (включая дату);
- идентификаторы типа события;
- категория аудита, к которой относится событие;
- идентификатор безопасности субъекта, в сеансе которого произошло событие;
- дополнительные параметры события, зависящие от типа события. Данные хранятся и представляются в двоичном виде.

С учетом рассмотренных структур данных, описывающих события безопасности **в** существующих распространенных системах аудита, можно разработать некоторый универсальный формат для представления событий аудита в системе, который бы способствовал ускорению обработки данных событий. При этом новый формат должен полно описывать событие.

Структура нашего представления событий безопасности в системе должна содержать следующие поля данных:

- N – порядковый номер события. Тип значения – целое число.
- RegistrationTime – время регистрации события. Тип значения – дата.
- StartTime – время начала обработки. Тип значения – дата.
- EventID – идентификатор разновидности события. Тип значения – целое число.
- EventType – идентификатор типа события. Тип значения – целое число.
- EventCategory – идентификатор категории (группы разновидностей событий), к которой относится событие. Тип значения – целое число.
- EventClasss – класс события – промежуточный результат обработки события в системе, класс события определяется системой на основе анализа данной структуры, описывающей событие. Тип значения - целое число.

- SourceName – имя источника события или модуля, зарегистрировавшего событие. Тип значения – строка символов.
- UserName – имя пользователя в сеансе которого зарегистрировано событие. Тип значения – строка символов.
- Domain – имя домена пользователя. Тип значения – строка символов.
- Host – идентификатор (имя или сетевой адрес) компьютера, на котором зарегистрировано событие. Тип значения – строка символов.
- EventParameters – дополнительные параметры события, зависящие от разновидности события. Тип значения - строка символов.

Такая структура позволяет осуществить представление данных распространенных систем аудита в формализованном виде, удобном для дальнейшей обработки и автоматического анализа.

Рассмотрим этап обработки (алгоритм), когда данные из распространенных систем аудита переводятся в новый вид, на основе которого будет проводиться анализ.

Предположим, что данные размещены в буфере.

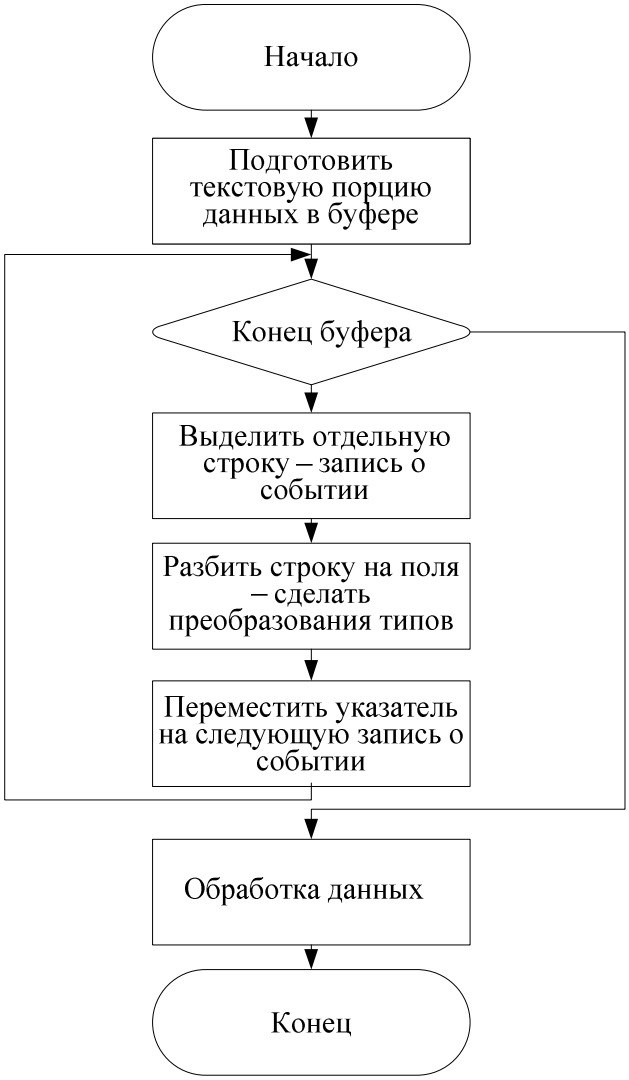

Рис. 2 – Алгоритм преобразования данных в новый вид

Проанализируем данные, которые мы извлекли из журнала аудита. Разделим все события на классы в зависимости от важности. То есть на основании полей записи будем относить события к какому-нибудь классу.

Каждое событие должно подвергнуться проверке на соответствие множествам правил, задающих классы событий. После проверки (при реализации – некоторая функция) поле EventClass получит значение, которое будет показывать принадлежность события к некоторому классу. Причем возможен случай, когда событие принадлежит сразу к нескольким классам.

Выделим следующие классы:

1. Архивные – это все события безопас-

ности, регистрируемые на компьютерах сети.

2. Отказы – это события, связанные с отказами в предоставлении доступа, а также со сбоями в работе средств обеспечения безопасности.

3. Информативные – это события, которые целесообразно отфильтровывать от всех архивных событий, поскольку они содержат важную информацию о важных происшествиях. Наличие этого класса объясняется тем, что обычно журналы аудита содержат большое количество малоинформативных событий, присутствие которых затрудняет дальнейший анализ, поэтому целесообразно отделять информативные события и, возможно, хранить их отдельно от архивных.

4. Предостережения – это класс важных событий, сигнализирующих о возникновении опасных ситуаций. Администраторы безопасности обязательно должны быть проинформированы о событиях этого класса, однако эти события не требуют немедленного оповещения.

5. Тревоги – это класс особо важных событий, сигнализирующих о возникновении особо опасных ситуаций, в случае обнаружения которых необходимо немедленно оповестить администратора безопасности.

Рассмотрим признаки событий, по которым можно добавлять к некоторому классу.

1. Архивные события

Причисление события к классу архивных событий не требует никаких условий. Любое событие, зарегистрированное на любом компьютере сети, может быть отнесено к классу архивных событий.

Таким образом, функция определения для класса архивных событий не зависит от полей данных записи о событии.

2. События-отказы

В среде ОС семейства Microsoft Windows NT события, содержащие информацию об отказах в доступе к ресурсам, могут быть однозначно идентифицированы по значению поля EventType записи о событии. Если поле EventType имеет значение EVENTLOG_AUDIT_FAILURE, то это означает, что событие сообщает о попытке доступа, закончившейся отказом в доступе.

Таким образом, функция определения для класса событий-отказов зависит от значения одного поля данных записи о событии.

3. Информативные события

В среде ОС семейства Microsoft Windows NT информативные события могут быть отделены от малоинформативных событий путем проверки идентификатора разновидности события, то есть поля EventID.

При настройке сетевой системы мониторинга событий безопасности администратор задает список идентификаторов информативных событий или список идентификаторов малоинформативных событий. Во втором случае, к информативным событиям относятся все события за исключением тех, идентификаторы которых перечислены в списке. Способ задания идентификаторов информативных событий не играет роли, поскольку метод их использования в процессе анализа не зависит от способа их задания при настройке системы.

В среде ОС семейства Microsoft Windows NT идентификаторы событий безопасности принимают значения от 512 до 1023. Другие диапазоны значений идентификаторов отведены для событий не связанных с безопасностью. Это позволяет применить быстрый метод определения принадлежности события к классу информативных событий.

То есть, для того чтобы определить относится ли некоторое событие к классу информативных событий достаточно проверить идентификатор разновидности события (поле EventID структуры TEventLogR.ec).

4. **События-предостережения и события-тревоги**

Для задания признаков событий, которые необходимо отнести к классам событий-предостережений или событий-тревог необходимо использовать сложные правила, способные описать ограничения, налагаемые на большинство полей структуры-события (структуры TEventLogR.ee).

Суть общего метода определения принадлежности события к классам событий-предостережений и событий тревог можно проиллюстрировать так:

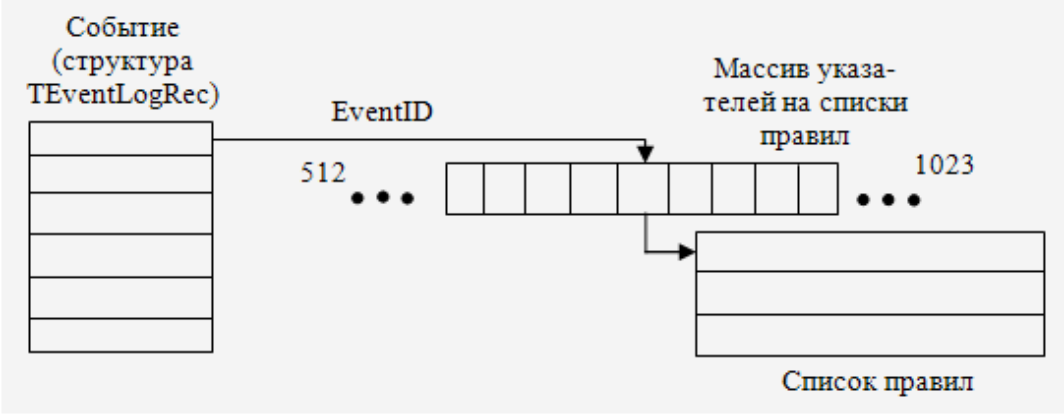

Рис.3 - Метод определения принадлежности события к классам событий-предостережений или событий-тревог

Все правила, определяющие признаки событий предостережений и событий-тревог, группируются в списки правил по идентификатору разновидности события. Таким образом, значение поля идентификатора разновидности события EvID в структуре записи о событии TEventLogRec является первичным признаком поиска, позволяющим существенно сократить количество правил, которые необходимо просмотреть для дальнейшего анализа события. По идентификатору EvID определяется элемент массива указателей – указатель на список правил, задающих крите-рии для других полей записи о событии.

Анализ событий на принадлежность к классам событий-предостережений или событий-тревог целесообразно проводить одновременно, поскольку эти классы отличаются друг от друга лишь требуемой реакцией системы на события указанных классов. Способ описания правил и метод их использования одинаков для обоих классов. Поэтому правила, задающие критерии принадлежности событий к указанным классам целесообразно хранить в одних и тех же списках, идентифицируя правила разных классов по некоторому признаку, включенному в структуру правила.

Для анализа события на принадлежность к классам событий-предостережений или событий-тревог последовательно перебираются правила, находящиеся в списке правил для заданного значения EvID. В этих правилах задаются условия, налагаемые на следующие поля записи о событии:

- GTime – дата и время регистрации события;
- EvType – тип события;
- SourceModule – модуль, зарегистрировавший событие;
- Host – имя компьютера, на котором произошло событие;
- UserName – имя пользователя;
- Domain – домен пользователя;

EvParams – дополнительные параметры события.

Выводы

Поскольку все события в системе имеют разные степени опасности, то нет необходимости в просмотре и анализе малоинформативных событий. Предложенный формат можно использовать в целях упрощения анализа базы событий в системе. В данной классификации класс событий-предостережений и событий-тревог сигнализируют о возникновении опасных и особо опасных ситуаций. Эти классы и вызывают особый интерес. Таким образом, внедрение предлагаемого формата представления данных сократит время, необходимое для обнаружения конфликтных ситуаций в системе и определения степени опасности.

Список литературы:

1. Люцарев В.С., Ермаков К.В., Рудный Е.Б., Ермаков И.В. Безопасность компьютерных сетей на основе Windows Ш\-М.:Изд.отдел «Русская редакция», 1998.-304с.
2. Брагг Р. Система безопасности Windows 2000. пер. с англ., - М: Издательский дом «Вильяме», 2001. - 592 с.
3. Немет Э., Снайдср Г., Сибс С, Хейн Т. UNIX: руководство системного администратора. Для профессионалов, пер. с англ., - С-Пб: Питер, К: Издательская группа BHV, 2002. - 928 с.
4. Фролов А. В., Фролов Г. В. Программирование для Windows NT. - М.: ДИАЛОГ-МИФИ, 1996.

Поступила в редакцию 23.12.2009