УДК 004.056.5

АНАЛИЗ ИСТОЧНИКОВ СОБЫТИЙ И ОПРЕДЕЛЕНИЕ НАИБОЛЕЕ ЗНАЧИМЫХ СОБЫТИЙ ДЛЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.В.Михальченко

студентка института приоритетных технологий кафедры информационной безопасности

Волгоградский государственный университет

lana.mixalchenko@yandex.ru

Аннотация: Для обеспечения информационной безопасности нередко проводится мониторинг событий. Мониторинг событий предполагает отслеживание всех инцидентов, происходящих в информационной системе. На сегодняшний день все больше компаний сталкивается с необходимостью обработки журналов событий, которые могут регистрируются в информационных системах. В статье рассмотрены источники событий безопасности информационной системы. Были классифицированы источники событий на системные и сетевые. Подробно были рассмотрены системные источники событий, а именно, журнал событий безопасности Windows. В нем были проанализированы важные события для мониторинга информационной безопасности, на которые следует обратить внимание специалисту по защите информации. В сетевых источниках событий были выделены два способа отслеживания передачи пакета по сети: стандарт отправки и регистрации сообщений syslog и протокол SNMP с функцией trap. Был сделан вывод о том, какой источник событий является наилучшим с точки зрения информативности, а также исходя из тенденции атак за предыдущий год.

Ключевые слова*:* информационная безопасность, мониторинг событий, события безопасности, журнал событий безопасности Windows, syslog, SNMP.

ANALYSIS OF EVENTS SOURCES AND DETERMINATION OF THE MOST IMPORTANT EVENTS FOR MONITORING INFORMATION SECURITY

S. V. Mikhalchenko

Student of the Institute of Priority Technologies of the Information Security Department

Volgograd state University

lana.mixalchenko@yandex.ru

Annotation: To ensure information security, events are often monitored. Monitoring events involves tracking all incidents occurring in the information system. To date, more and more

companies are faced with the need to process event logs that can be registered in information systems. The article considers the security events sources of the information system. Event sources were classified into system and network events. We considered system event sources in detail, that called the Windows security event log. It analyzed important events for monitoring information security, which should be addressed to the information security specialist. In the network sources of events two methods of tracking packet transmission over the network were identified: the standard for sending and registering syslog messages and the SNMP protocol with the trap function. It was concluded which source of events is best from the point of view of information, and also based on the tendency of attacks for the previous year.

Keywords: information security, event monitoring, security events, Windows security event log, syslog, SNMP.

Одним из важных компонентов при обеспечении информационной безопасности (ИБ) является анализ событий в информационных системах (ИС). Поэтому в организации для этого должна отводиться существенная часть денежных средств. Чтобы денежные средства не были потрачены впустую, должна быть создана такая система, которая бы в минимальные сроки обнаруживала то или иное событие, способное причинить вред, либо указывающее на проблему или сбой в системе.

В качестве источников таких событий могут быть:

1. Системные источники
    - журнал событий Windows.
2. Сетевые источники
    - стандарт отправки и регистрации сообщений syslog;
    - протокол SNMP с функцией trap.

Для такого количества событий нужно создавать специальные программы или приложения, например:

1. Журналы событий.

Например, в системе Windows разработан специальный журнал событий, где пользователь мог бы просматривать все события и анализировать их. В журнале Windows хранится системная информация. Эта информация разбита на разделы:

❖ Журнал приложений – сведения, связанные с работой приложений и программ. Например, программа управления базой данных может зарегистрировать событие о файловой ошибке в журнале приложений. События, регистрируемые в журнале приложений, определяются разработчиками соответствующих приложений.

- ❖ Журнал установки – данные об установке приложений, сбои при установке.
- ❖ Журнал системы – содержит события, записываемые системными компонентами Windows. Типы событий, которые регистрируются компонентами системы, определены на уровне операционной системы.
- ❖ Журнал пересылаемых событий - используется для хранения событий, собранных с удаленных компьютеров.
- ❖ Административный журнал – содержится информация для конечных пользователей, администраторов и персонала технической поддержки. Кроме того, какая проблема возникла, указывает на то, как ее решить.
- ❖ Журнал операций – записи в этом журнале служат для анализа и диагностики проблем или событий. Они могут использоваться для запуска средств или задач при возникновении соответствующих проблем или событий. Примером события в журнале операций является добавление или удаление принтера из системы.
- ❖ Аналитический журнал – сюда записываются события, описывающие работу программ и неполадки, происходящие во время работы с приложениями, которые пользователь сам устранить не может.
- ❖ Отладочный журнал – используется разработчиками программного обеспечения для устранения неполадок в программах.

Событию ИС может соответствовать несколько записей в журнале событий, что следует учесть при анализе.

- ❖ Журнал безопасности – успешные и неуспешные попытки входа в систему, использование каких-либо ресурсов (создание, открытие и удаление файлов).

С точки зрения ИБ этот журнал является самым информативным. В нем указаны как раз те события, которые могут служить основанием для подозрения атаки. Поэтому этот журнал следует рассмотреть подробней.

События в журнале безопасности фиксируется, согласно настроенным политикам аудита. Из большого количества событий здесь стоит выделить события, представленные в таблице 1 [3].

Таблица 1 – Важные события безопасности

Категория	Идентификатор события	Описание события
	4771	Сбой предварительной проверки подлинности Kerberos (ядра ОС).

Аудит событий входа учетной записи	4768	Запрошен аутентификационный билет Kerberos (TGT)
	4772	Ошибка запроса билета проверки подлинности Kerberos
Аудит управления учетными записями	4728,4732,4756	Все три события указывают на то, что указанный пользователь был добавлен в определенную группу. Обозначены: Глобальная, Локальная и Общая соответственно для каждого идентификатора.
	4741	Была создана учетная запись компьютера
	4740	Учетная запись пользователя была заблокирована после нескольких попыток входа
	4723,4724	Была предпринята попытка изменить/сбросить пароль учетной записи
Аудит системных событий	1102	Указанный пользователь очистил журнал безопасности
	4816	RPC (Remote Procedure Call – удаленный вызов процедур) обнаружено нарушение целостности при расшифровке входящего сообщения
	5025	Служба брандмауэра Windows остановлена
Аудит входа/выхода	4624	Успешный вход в систему
	4625	Отказ входа в систему
	4649	Обнаружена атака с повторением.
	4800	Рабочая станция заблокирована.
Аудит доступа к службе каталогов	5136	Объект службы каталогов был изменен
	5141	Объект службы каталогов удален
Аудит доступа к объектам	4657	Значение реестра было изменено
	4660	Объект был удален
	4663	Была предпринята попытка получить доступ к объекту
	4719	Политика аудита системы была изменена

Аудит изменения политики		
	4905	Была предпринята попытка отменить регистрацию источника событий безопасности.
	4717	Учетной записи предоставлен доступ к системе безопасности
	4704	Назначены привилегии пользователю
Аудит использования привилегий	4672	Особые привилегии назначены новому сеансу входа

2. Стандарт отправки и регистрации сообщений syslog.

Выше были перечислены события, которые имеют отношения к программам, приложениям и службам. Но события происходят не только на программном уровне, но и на сетевом. Чтобы отслеживать такие события существует стандарт отправки и регистрации сообщений, называемые syslog. Он стал стандартным средством для системного журналирования в системах семейства Unix и Linux, а позже стал использоваться и на других операционных системах. С помощью этого протокола устройства могут пересылать информацию о событиях серверам syslog, собирающим информацию о событиях. Устройства с поддержкой syslog позволяют создавать сообщения и отправлять их на сервер. Каждое такое сообщение содержит определение категории и уровня серьезности, что позволяет персоналу незамедлительно реагировать на критические ситуации.

Уровни важности сообщений бывают 8 видов [1]:

- 0 или Emergency - аварийные сообщения. Содержат данные, описывающие события, затрагивающие множество сервисов. Сигнализируют о неработоспособности системы.
- 1 или Alert - тревожные сообщения. Содержат данные, описывающие возникшие в основной системе события, требующие немедленного вмешательства.
- 2 или Critical - критические сообщения. Содержат данные, описывающие возникшие во вторичной системе события, требующие немедленного вмешательства.
- 3 или Error - сообщения об ошибках. Содержат данные, описывающие события, требующие внимания, но не предполагающие немедленного вмешательства. Например: локальный сертификат не пригоден, обнаружены некорректные данные в базе данных, связанные с LSP(конфигурационный файл политики), невозможно загрузить политику безопасности, ошибка в записи маршрутизации.

- 4 или Warning - предупреждения о возможных проблемах. Содержат данные, описывающие события, которые могут потенциально привести к возникновению проблем, если не будут предприняты соответствующие действия. Примерами могут служить: Обнаружена некорректная политика, конвертирование политики не делается, неуспешная попытка соединение в качестве ответчика, удаление локального сертификата.
- 5 или Notice - сообщения о нормальных, но важных событиях. Содержат данные, описывающие необычные события, не являющиеся ошибкой. Например, старт консоли, завершение консоли, пользователь успешно создан или удален, пароль пользователя успешно сменен, произошло изменение в привилегиях пользователя, включен Host-режим, превышено ограниченное количество сессий, старт и остановка сертификата, добавление локального сертификата в базу данных.
- 6 или Informational - информационные сообщения. Содержат данные, которые могут потребоваться для составления отчетов и т.п. Такие данные могут быть вида: команда успешно обработана консолью, установлено соединение, закрытие соединения, информация о лицензии продукта, IPSec-соединение не установилось из-за превышения количества, разрешенного лицензией.
- 7 или Debug - отладочные сообщения. Содержат данные, полезные для разработчиков программного обеспечения, такие как: выбран локальный сертификат, не найден сертификат партнера, либо этот сертификат непригодный, запрос на создание соединения, ошибка инициализирования создания соединения, обнаружение устройства NAT.

3. Протокол SNMP с функцией trap.

Кроме журнала syslog, существует протокол SNMP, у которого есть функция так называемой «ловушки» или SNMP trap [2]. Подобные сигналы отправляются устройствами для того, чтобы оповестить администратора сети о наступлении каких-то критических событий. В сообщении SNMP-trap содержится структурированная информация, состоящая из имени переменной SNMP (OID) и её значения. К примеру, признаком того, что сервер перешел в режим питания от UPS может быть сообщение, в котором содержится переменная, отвечающая за режим питания со значением. Такие ситуации требуют незамедлительного вмешательства обслуживающего персонала, и поэтому устройство само инициирует отправку сигнала по протоколу SNMP.

Проанализировав статистику по видам атак были выделены 3 самых популярных вида [4] : вредоносное ПО, компрометация учетных данных и социальная инженерия. Такие атаки отражаются на уровне ОС, например, в журнале регистрации событий Windows. Поэтому

рационально выбрать именно его для анализа событий, происходящих в информационной системе.

Литература

1. И. В. Потуремский, А. В. Мурыгин Система мониторинга узлов локальной вычислительной сети на основе протокола syslog // Сибирский журнал науки и технологий – 2010. – №4. – С35-39.
2. «Основы протокола SNMP 2 - е издание» - Спб.: М / ООО «Символ плюс», 2012. – 517 с.
3. 10 критически важных event ID для мониторинга [Электронный ресурс] – Режим доступа: https://habrahabr.ru/company/netwrix/blog/148501/
4. Актуальные киберугрозы II квартал 2017г [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2017-rus.pdf