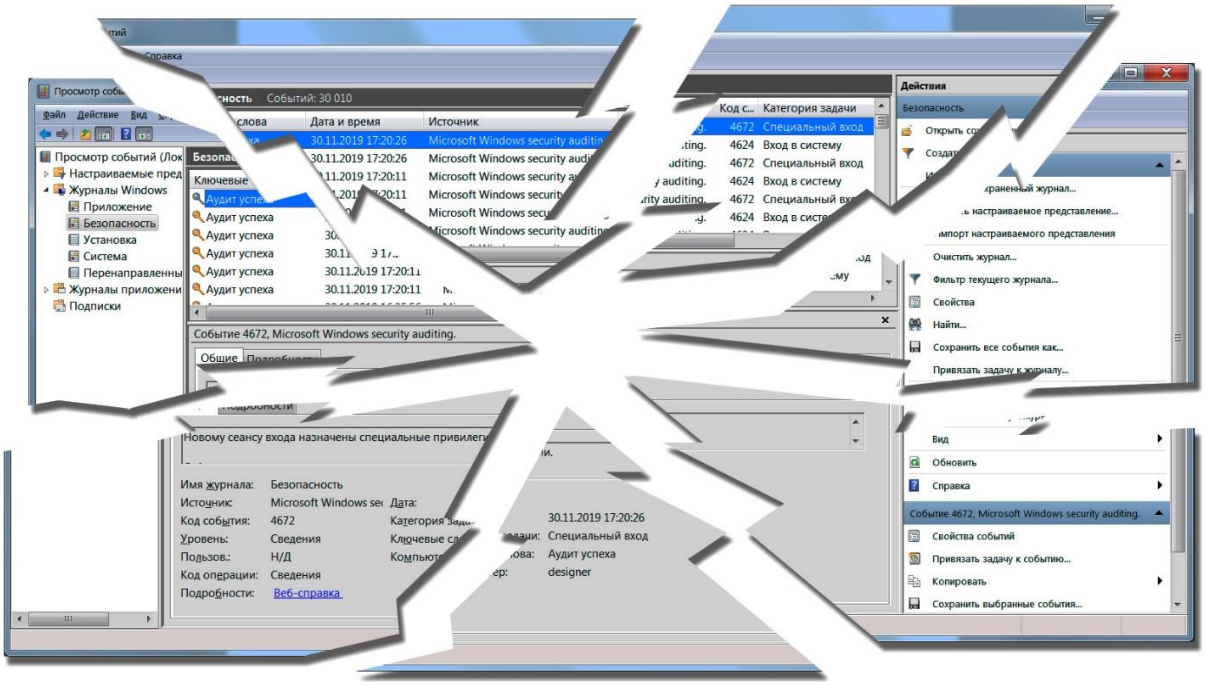
Проблемы в системе журналирования событий безопасности ОС Windows



В операционных системах семейства Windows реализована довольно неплохая система журналирования событий безопасности. О ней в различных публикациях и обзорах написано много чего хорошего, но эта статья будет про другое. Здесь мы поговорим о проблемах и недоработках в этой системе. Некоторые из рассматриваемых проблем будут некритичными, лишь осложняющими процедуры анализа событий, другие же будут представлять весьма серьезные угрозы безопасности.

Выявленные проблемы проверялись на Windows 7 Максимальная (русская версия), Windows 7 Professional (английская версия), Windows 10 Pro (русская версия), Windows Server 2019 Datacenter (русская версия). Все операционные системы были полностью обновлены.

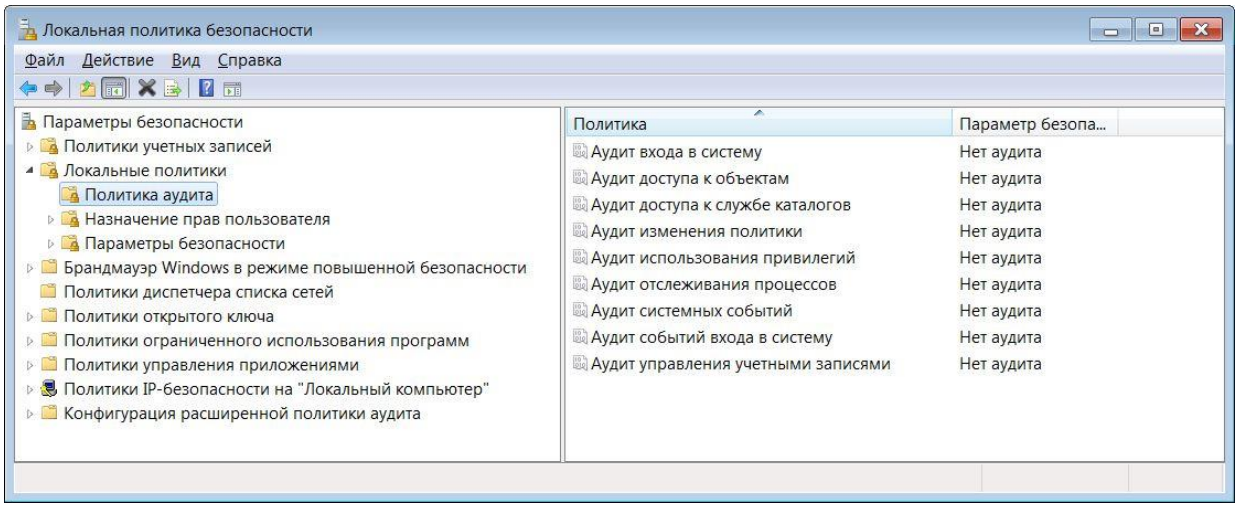
Проблема № 1. Неудачная система управления параметрами аудита

Наличие проблемы подтверждено на Windows 7/10/Server 2019.

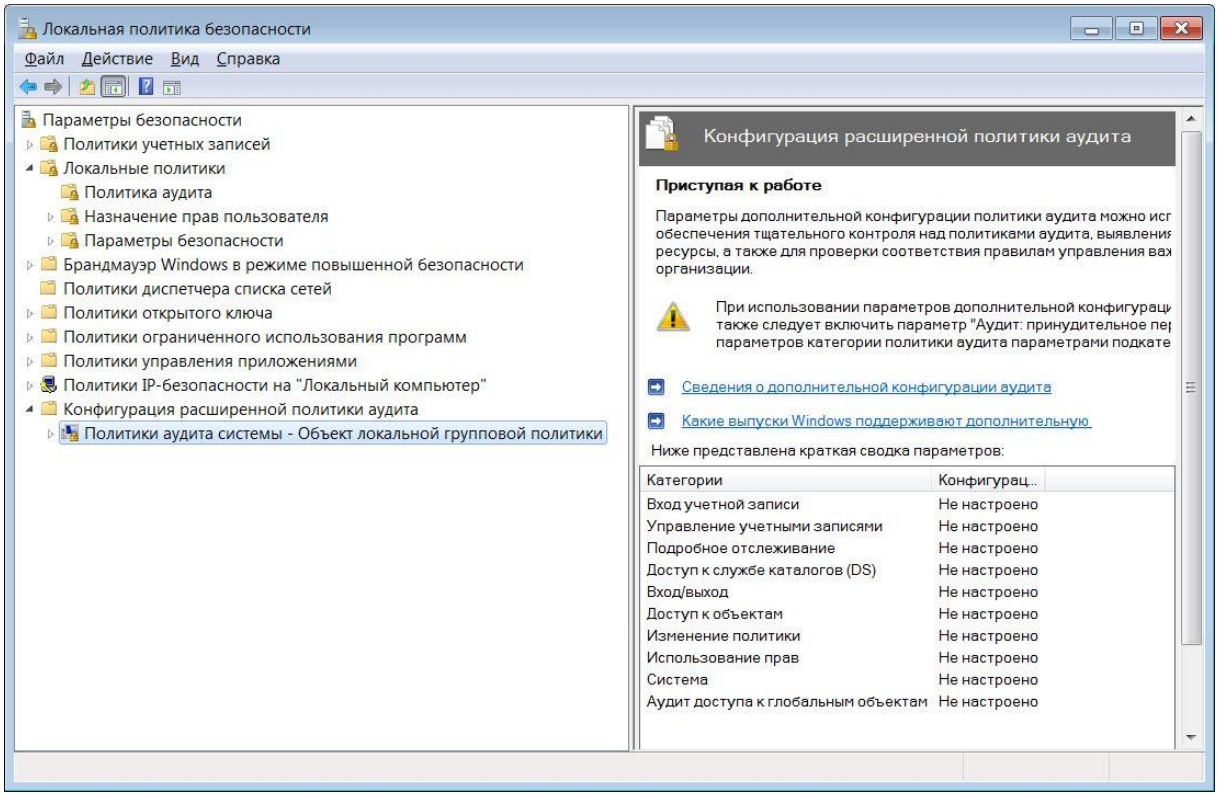
Описание проблемы

Возьмем Windows 7 и проинсталлируем ее с параметрами по умолчанию. Домен вводить не будем. Посмотрим настройки аудита событий безопасности. Для этого откроем оснастку «Локальные политики безопасности» (secpol.msc, или «Панель управления → Администрирование → Локальные политики безопасности») и посмотрим базовые

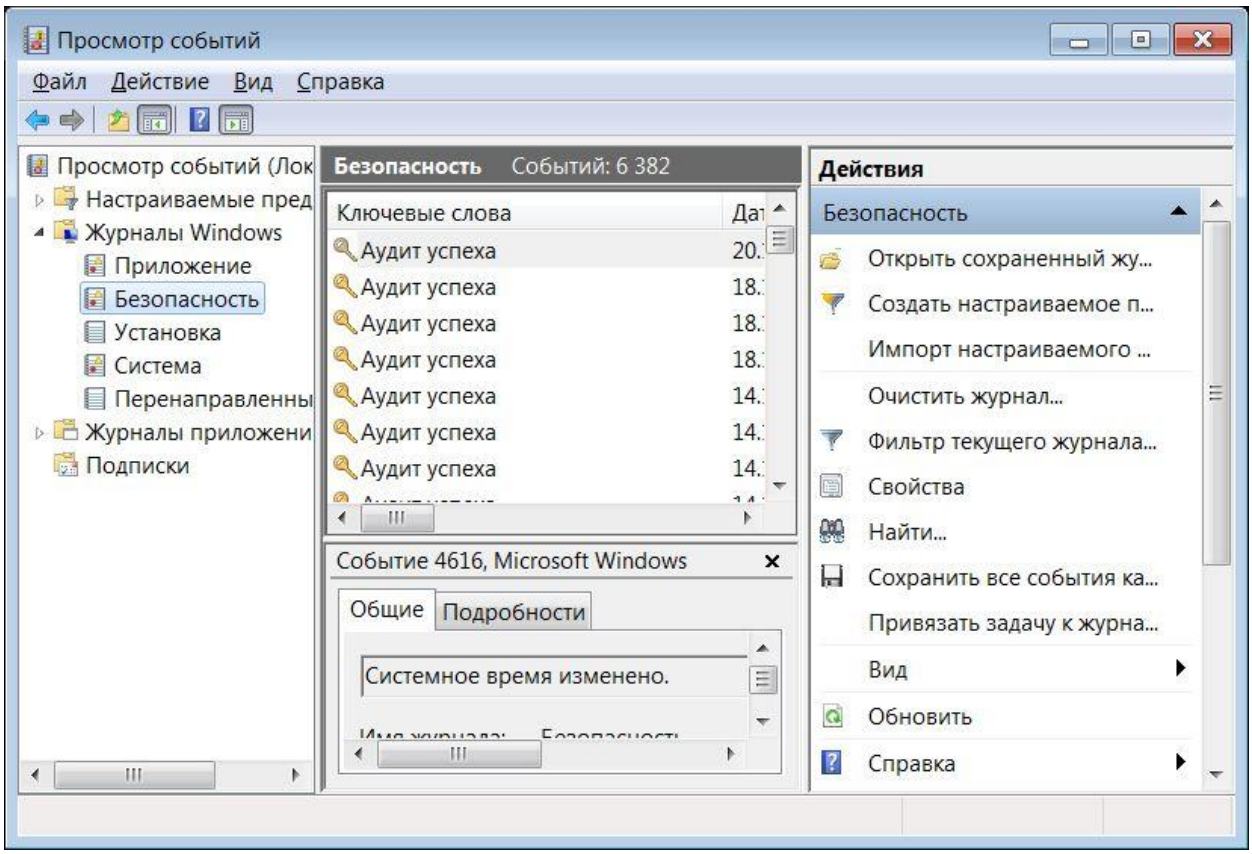
настройки аудита («Параметры безопасности → Локальные политики → Политики аудита»).



Как видно, аудит не настроен. Теперь посмотрим расширенные политики аудита («Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита системы — Объект локальной групповой политики»).



Тут аудит тоже не настроен. Раз так, то по идее никаких событий безопасности в журналах быть не должно. Проверяем. Откроем журнал безопасности (eventvwr.exe, или «Панель управление → Администрирование → Просмотр событий»).



Вопрос: «Откуда в журнале безопасности события, если аудит вообще не настроен ?!»

Объяснение

Чтобы разобраться в причине подобного поведения, надо залезть «под капот» операционной системы. Начнем с того, что разберемся с базовыми и расширенными политиками аудита.

До Windows Vista были только одни политики аудита, которые сейчас принято называть базовыми. Проблема была в том, что гранулярность управления аудитом в то время была очень низкой. Так, если требовалось отследить доступ к файлам, то включали категорию базовой политики «Аудит доступа к объектам». В результате чего помимо файловых операций в журнал безопасности сыпалась еще куча других «шумовых» событий. Это сильно усложняло обработку журналов и нервировало пользователей.

Microsoft услышала эту «боль» и решила помочь. Проблема в том, что Windows строится по концепции обратной совместимости, и внесение изменений в действующий механизм управления аудитом эту совместимость бы убило. Поэтому вендор пошел другим путем. Он создал новый инструмент и назвал его расширенными политиками аудита.

Суть инструмента заключается в том, что из категорий базовых политик аудита сделали категории расширенных политик, а те, в свою очередь, разделили на подкатегории, которые можно отдельно включать и отключать. Теперь при необходимости отслеживания

доступа к файлам в расширенных политиках аудита необходимо активировать только подкатегорию «Файловая система», входящую в категорию «Доступ к объектам». При этом «шумовые» события, связанные с доступом к реестру или фильтрацией сетевого трафика, в журнал безопасности попадать не будут.

Гигантскую путаницу во всю эту схему вносит то, что наименования категорий базовых политик аудита и расширенных не совпадают, и по началу может показаться, что это абсолютно разные вещи, однако это не так.

Приведем таблицу соответствия наименования базовых и расширенных категорий управления аудитом

Наименование базовых политик аудита	**Наименование расширенной политики аудита**
Аудит доступа к службе каталогов	Доступ к службе каталогов (DS)
Аудит доступа к объектам	Доступ к объектам
Аудит использования привилегий	Использование прав
Аудит входа в систему	Вход/выход
Аудит событий входа в систему	Вход учетной записи
Аудит изменения политики	Изменение политики
Аудит системных событий	Система
Аудит управления учетными записями	Управление учетными записями
Аудит отслеживания процессов	Подробное отслеживание

Важно понимать, что и базовые и расширенные категории по сути управляют одним и тем же. Включение категории базовой политики аудита приводит к включению соответствующей ей категории расширенной политики аудита и, как следствие, всех ее подкатегорий. Во избежание непредсказуемых последствий Microsoft не рекомендует одновременное использование базовых и расширенных политик аудита.

Теперь настало время разобраться с тем, где хранятся настройки аудита. Для начала введем ряд понятий:

1. *Эффективные политики аудита* — информация, хранящаяся в оперативной памяти и определяющая текущие параметры работы модулей операционной системы, реализующих функции аудита.
2. *Сохраненные политики аудита* — информация, хранящаяся в реестре по адресу HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv и используемая для определения эффективных политик аудита после перезагрузки системы.

Рассмотрим различные средства администрирования и укажем, какие параметры аудита они отображают, а какие устанавливают. Данные в таблице получены на основании экспериментов.

Наименование средства	Отображаемые политики аудита	Сохраняемые политики аудита
«Базовые политики аудита» оснастки «Локальные политики безопасности»	Эффективные политики аудита	Эффективные политики аудита, сохраненные политики аудита
«Расширенные политики аудита» оснастки «Локальные политики безопасности»	Файл %SystemRoot%\System32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv	
Утилита auditpol	Сохраненные параметры аудита	Эффективные параметры аудита, сохраненные параметры аудита

Поясним таблицу на примерах.

Пример 1

Если запустить утилиту auditpol на просмотр параметров аудита: `auditpol /get /category:*`, то будут отображены сохраненные параметры аудита, то есть те, что хранятся в реестре по адресу HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv.

Пример 2

Если же запустить эту же утилиту, но уже на установку параметров: `auditpol /set /category:*`, то будут изменены эффективные настройки аудита и сохраненные параметры аудита.

Отдельного комментария требует порядок отображения параметров аудита в «Базовых политиках аудита» оснастки «Локальные политики безопасности». Категория базовой политики аудита отображается как установленная, если установлены все подкатегории соответствующей ей расширенной политики аудита. Если хотя бы одна из них не установлена, то политика будет отображаться как не установленная.

Пример 3

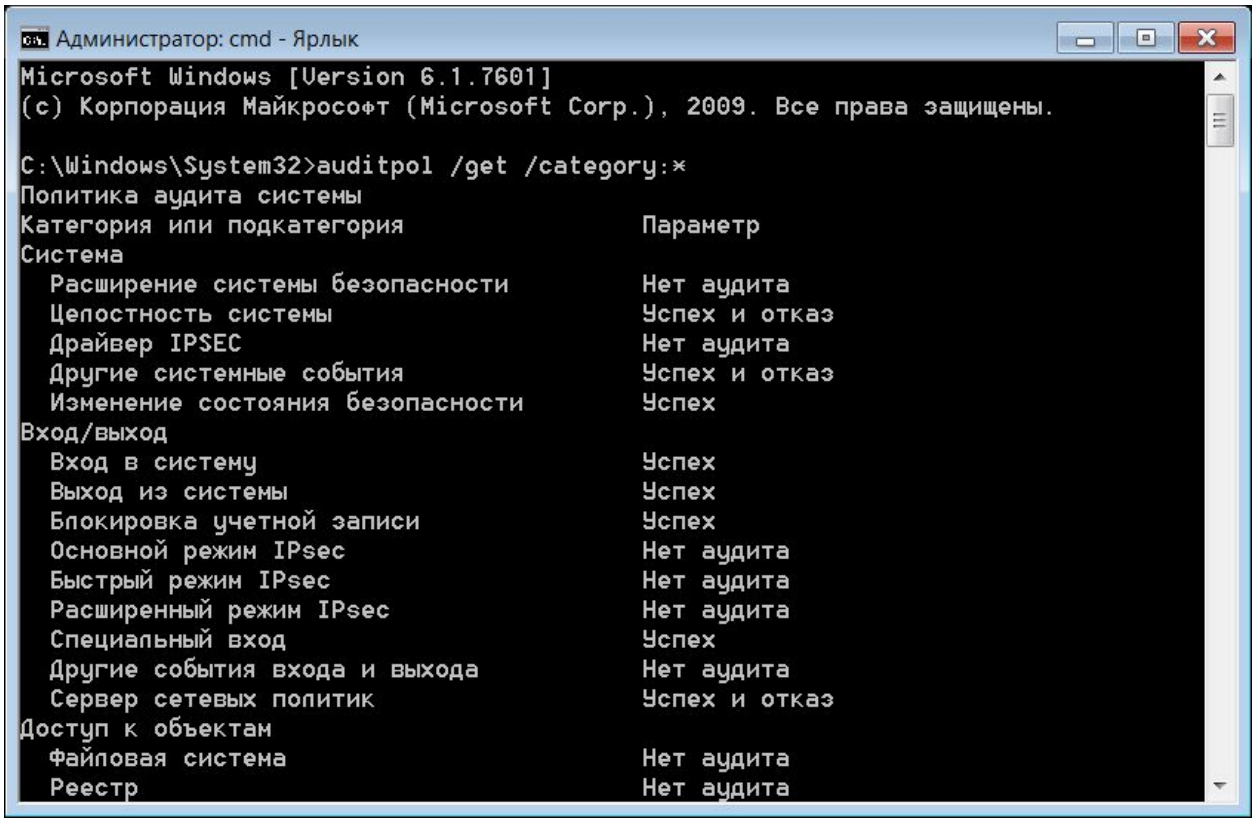
Администратор с помощью команды `auditpol /set /category:*` установил все подкатегории аудита в режим «Аудит успехов». При этом если зайти в «Базовые политики аудита» оснастки «Локальные политики безопасности», то напротив каждой категории будет установлено «Аудит успеха».

Пример 4

Теперь администратор выполнил команду `auditpol /clear` и сбросил все настройки аудита. Затем он установил аудит файловой системы, выполнив команду `auditpol /set /subcategory:"Файловая система"`. Теперь, если зайти в «Базовые политики аудита» оснастки «Локальные политики безопасности», то все категории будут определены в состояние «Нет аудита», так как ни одна категория расширенной политики аудита не определена полностью.

Сейчас, наконец-то, мы сможем ответить на вопрос, откуда логи в свежеустановленной операционной системе. Все дело в том, что после инсталляции аудит в Windows настроен

и определен в сохраненных параметрах аудита. В этом можно убедиться, выполнив команду `auditpol /get /category:*`.



В «Базовых политиках аудита» оснастки «Локальные политики безопасности» эти сведения об аудите не отображаются, так как во всех категориях не определена одна или более подкатегорий. В «Расширенных политиках аудита» оснастки «Локальные политики безопасности» эти сведения не отображаются, так как оснастка работает только с параметрами аудита, хранящимися в файле %SystemRoot%\System32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv.

В чем суть проблемы?

По началу может показаться, что все это и не проблема вовсе, но это не так. То, что все инструменты показывают параметры аудита по разному, создает возможность к злонамеренному манипулированию политиками и, как следствие, результатами аудита.

Рассмотрим вероятный сценарий

Пусть в корпоративной сети работает технологическая рабочая станция на базе Windows 7.

Машина не включена в домен и выполняет функции робота, ежедневно отправляющего отчетность в контролирующие органы. Злоумышленники тем или иным образом получили на ней удаленный доступ с правами администратора. При этом основная цель злоумышлеников — шпионаж, а задача — оставаться в системе незамеченными. Злоумышленники решили скрытно, чтоб в журнале безопасности не было событий с кодом 4719 «Аудит изменения политики», отключить аудит доступа к файлам, но при этом

чтобы все инструменты администрирования говорили, что аудит включен. Для достижения поставленной задачи они выполнили следующие действия:

1. На атакуемой рабочей станции предоставили себе права на запись к ключу реестра HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv и экспортировали этот ключ в файл с именем "+fs.reg".
2. На другом компьютере импортировали данный файл, перезагрузились, а затем с помощью auditpol отключили аудит файловой системы, после чего экспортировали указанный выше ключ реестра в файл "-fs.reg".
3. На атакуемой машине импортировали в реестр файл "-fs.reg".
4. Создали резервную копию файла %SystemRoot%\System32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv, расположенного на атакуемой машине, а затем удалили из него подкатегорию «Файловая система».
5. Перезагрузили атакуемую рабочую станцию, а затем подменили на ней файл %SystemRoot%\System32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv ранее сохраненной резервной копией, а также импортировали в реестр файл "+fs.reg"

В результате всех этих манипуляций в журнале безопасности нет записей об изменении политики, все инструменты показывают, что аудит включен, а по факту он не работает.

Проблема № 2. Неудачная реализация журналирования операций удаления файлов, каталогов и ключей реестра

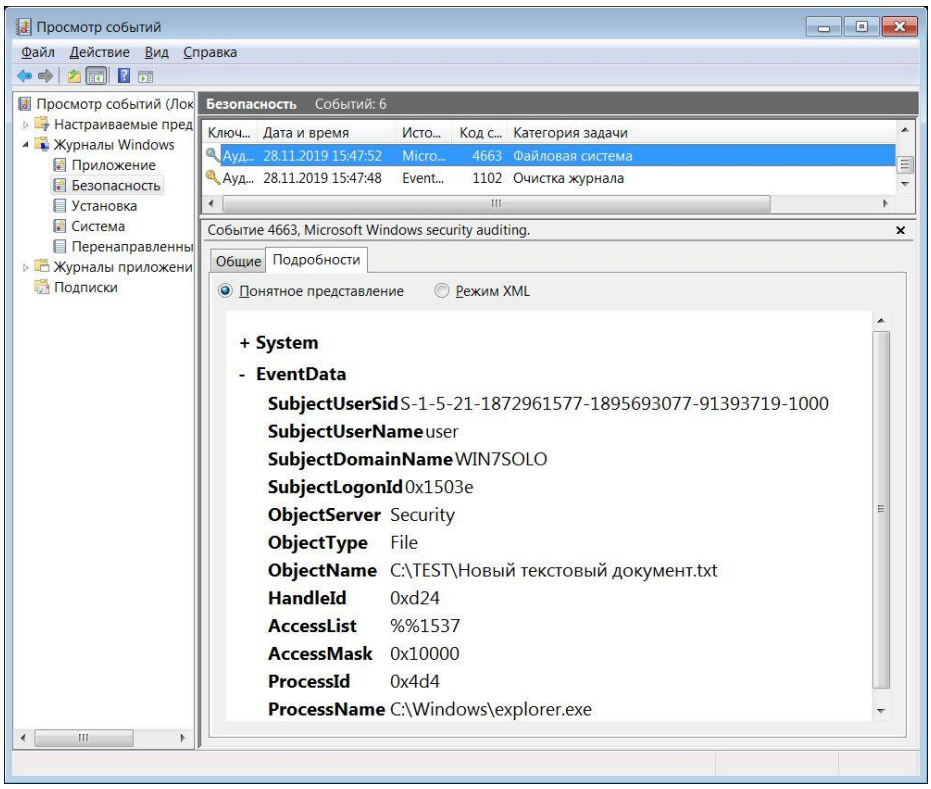
Наличие проблемы подтверждено на Windows 7/10/Server 2019.

Описание проблемы

На одну операцию удаления файла, каталога или ключа реестра операционная система генерирует последовательность событий с кодами 4663 и 4660. Проблема в том, что из всего потока событий данную парочку не так уж просто связать друг с другом. Для того чтобы это сделать, анализируемые события должны обладать следующими параметрами:

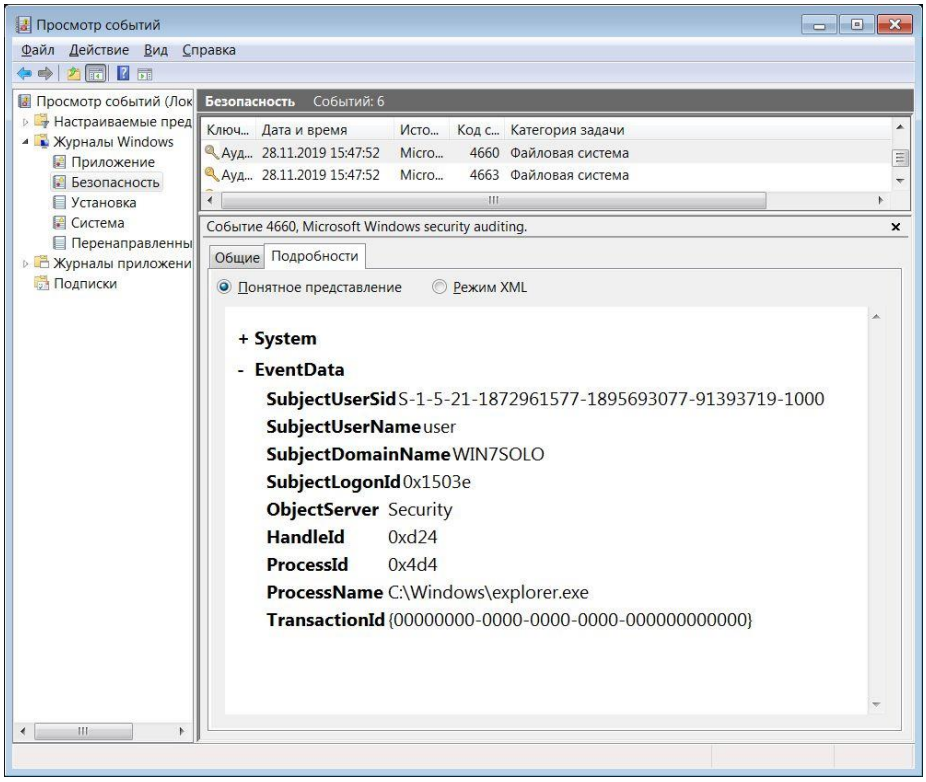
Событие 1. Код 4663 «Выполнена попытка получения доступа к объекту». Параметры события:

«ObjectType» = File.
«ObjectName» = имя удаляемого файла или каталога.
«HandleId» = дескриптор удаляемого файла.
«AcessMask» = 0x10000 (Данный код соответствует операции DELETE. С расшифровкой всех кодов операций можно ознакомиться на сайте Microsoft).



Событие 2. Код 4660 «Объект удален».
Параметры события:

«HandleId» = «HandleId события 1»
«System\EventRecordID» = «System\EventRecordID из события 1» + 1.



С удалением ключа (key) реестра всё то же самое, только в первом событии с кодом 4663 параметр «ObjectType» = Key.

Отметим, что удаление значений (values) в реестре описывается другим событием (код 4657) и подобных проблем не вызывает.

Особенности удаления файлов в Windows 10 и Server 2019

В Windows 10 / Server 2019 процедура удаления файла описывается двумя способами.

1. Если файл удаляется в корзину, то как и раньше — последовательностью событий 4663 и 4660.
2. Если же файл удаляется безвозвратно (мимо корзины), то одиночным событием с кодом 4659.

Случилось странное. Если раньше для определения удаленных файлов нужно было мониторить совокупность событий 4663 и 4660, то сейчас Microsoft «пошла пользователям на встречу», и вместо двух событий теперь надо мониторить три. Также стоит отметить, что процедура удаления каталогов не поменялась, она как и раньше состоит из двух событий 4663 и 4660.

В чем суть проблемы?

Проблема заключается в том, что узнать кто удалил файл или каталог, становится нетривиальной задачей. Вместо банального поиска соответствующего события по журналу безопасности необходимо анализировать последовательности событий, что вручную делать довольно трудоемко. На хабре даже по этому поводу была статья: «Аудит удаления и доступа к файлам и запись событий в лог-файл средствами Powershell».

Проблема № 3 (критическая). Неудачная реализация журналирования операции переименования файлов, каталогов и ключей реестра

Наличие проблемы подтверждено на Windows 7/10/Server 2019.

Описание проблемы

Эта проблема состоит из двух подпроблем:

1. В событиях, генерируемых системой во время переименования, нигде не фиксируется новое имя объекта.
2. Процедура переименования очень похожа на удаление. Отличить ее можно только по тому, что за первым событием с кодом 4663, с параметром «AcessMask» = 0x10000 (DELETE) **не идет** событие 4660.

Стоит отметить, что применительно к реестру эта проблема распространяется только на ключи (keys). Переименование значений (value) в реестре описывается

последовательностью событий 4657 и подобных нареканий не вызывает, хотя, конечно, было бы гораздо удобней, если бы было только одно событие.

В чем суть проблемы?

Помимо затруднения поиска операций переименования файлов подобная особенность журналирования не позволяет отследить полный жизненный цикл объектов файловой системы или ключей реестра. В результате чего на активно используемом файловом сервере становится крайне затруднительно определить историю файла, который многократно переименовывался.

Проблема № 4 (критическая). Невозможно отследить создание каталога и ключа реестра

Наличие проблемы подтверждено на Windows 7/10/Server 2019.

Описание проблемы

Windows не позволяет отследить создание каталога файловой системы и ключа реестра. Это заключается в том, что операционная система не генерирует событие, в котором содержалось бы имя создаваемого каталога или ключа реестра, и параметры которого указывали бы на то, что это именно операция создания.

Теоретически по косвенным признакам выявить факт создания каталога возможно. Например, если он создавался через «Проводник», то в процессе создания будут сгенерированы события опроса атрибутов нового каталога. Проблема в том, что если создать каталог через команду `mkdir`, то вообще никакие события не генерируются. Всё то же самое справедливо и для создания ключей в реестре.

В чем суть проблемы?

Эта проблема существенно затрудняет проведение расследований инцидентов информационной безопасности. Нет никаких разумных объяснений тому, что в журналах не фиксируется данная информация.

Проблема № 5 (критическая). Сбойные параметры аудита в русских версиях Windows

Наличие проблемы подтверждено на русских редакциях Windows 7/10/Server 2019.

Описание проблемы

В русских версиях Windows есть ошибка, приводящая систему управления аудитом безопасности в нерабочее состояние.

Симптомы

Изменение расширенных политик безопасности не оказывает никакого влияния на эффективные параметры аудита, или, другими словами, политики не применяются. Например, администратор активировал подкатегорию «Вход в систему», перезагрузил систему, запускает команду `auditpol /get /category:*`, а данная подкатегория остается не активной. Проблема актуальна как для доменных компьютеров, управляемых через групповые политики, так и для не доменных, управляемых с помощью локального объекта групповой политики, конфигурируемого через оснастку «Локальные политики безопасности».

Причины

Проблема возникает, если администратор активировал хотя бы одну из «сбойных» подкатегорий расширенных политик аудита. К подобным сбойным категориям, в частности, относятся:

1. Использование прав --> Аудит использования прав, затрагивающих конфиденциальные данные. GUID: {0cce9228-69ae-11d9-bed3-505054503030}.
2. Использование прав --> Аудит использования прав, не затрагивающих конфиденциальные данные. GUID: {0cce9229-69ae-11d9-bed3-505054503030}.
3. Доступ к объектам --> Аудит событий, создаваемых приложениями. GUID:{ 0cce9222-69ae-11d9-bed3-505054503030}.

Рекомендации по решению проблемы

Если проблема еще не произошла, то не активируйте указанные «сбойные» подкатегории. Если события этих подкатегорий очень нужны, то пользуйтесь утилитой auditpol для их активации или же управляйте аудитом с помощью базовых политик.

Если проблема произошла, то необходимо:

1. Из каталога доменной групповой политики удалить файл \Machine\microsoft\windows nt\Audit\audit.csv
2. Со всех компьютеров, на которых были выявлены проблемы с аудитом, удалить файлы: %SystemRoot%\security\audit\audit.csv, %SystemRoot%\System32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv

В чем суть проблемы?

Наличие данной проблемы уменьшает количество событий безопасности, которые можно контролировать штатным образом через расширенные политики аудита, а также создает угрозы отключения, блокирования и дестабилизации управления системой аудита в корпоративной сети.

Проблема № 6 (критическая). Будь проклят «Новый текстовый документ.txt..., а также Новый точечный рисунок.bmp»

Наличие проблемы подтверждено на Windows 7. Проблема отсутствует в Windows 10/Server 2019.

Описание проблемы

Это очень странная проблема, которая была обнаружена чисто случайно. Суть проблемы в том, что в операционной системе есть лазейка, позволяющая обойти аудит создания файлов.

Подготовительная часть:

1. Возьмем свежеустановленную Windows 7.
2. Сбросим все настройки аудита с помощью команды `auditpol /clear`. Данный пункт необязательный и служит только для удобства анализа журналов.
3. Установим аудит файловой системы, выполнив команду `auditpol /set /subcategory:"Файловая система"`.
4. Создадим каталог C:\TEST и назначим ему параметры аудита для учетной записи «Все»: «Создание файлов / Запись данных», «Создание папок / Дозапись данных», «Запись атрибутов», «Запись дополнительных атрибутов», «Удаление вложенных папок и файлов», «Удаление», «Смена разрешений», «Смена владельца», то есть все, что связано с записью данных в файловую систему.

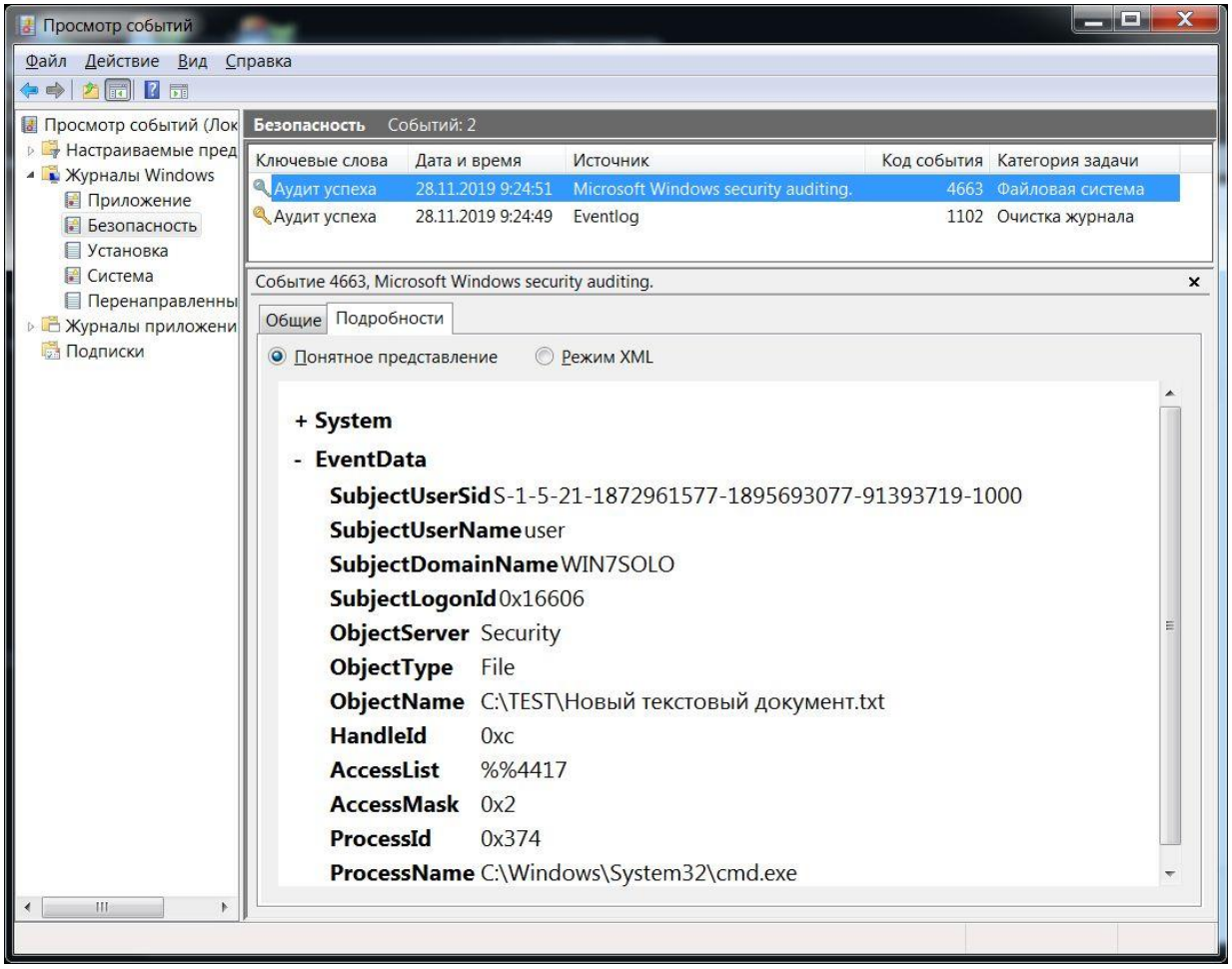
Для наглядности перед каждым экспериментом будем очищать журнал безопасности операционной системы.

Эксперимент 1.
Делаем:

Из командной строки выполним команду: `echo > "c:\test\Новый текстовый документ.txt"`
Наблюдаем:

По факту создания файла в журнале безопасности появилось событие с кодом 4663,

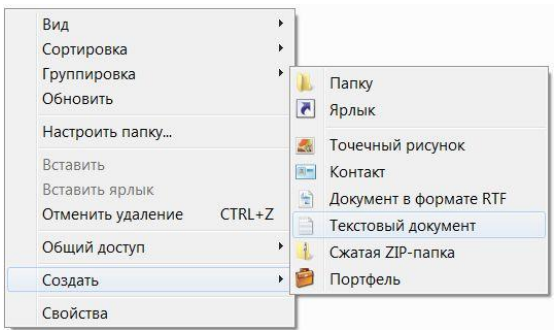
содержащее в поле «ObjectName» имя создаваемого файла, в поле «AccessMask» значение 0x2 («Запись данных или добавление файла»).



Для выполнения следующих экспериментов очистим папку и журнал событий.

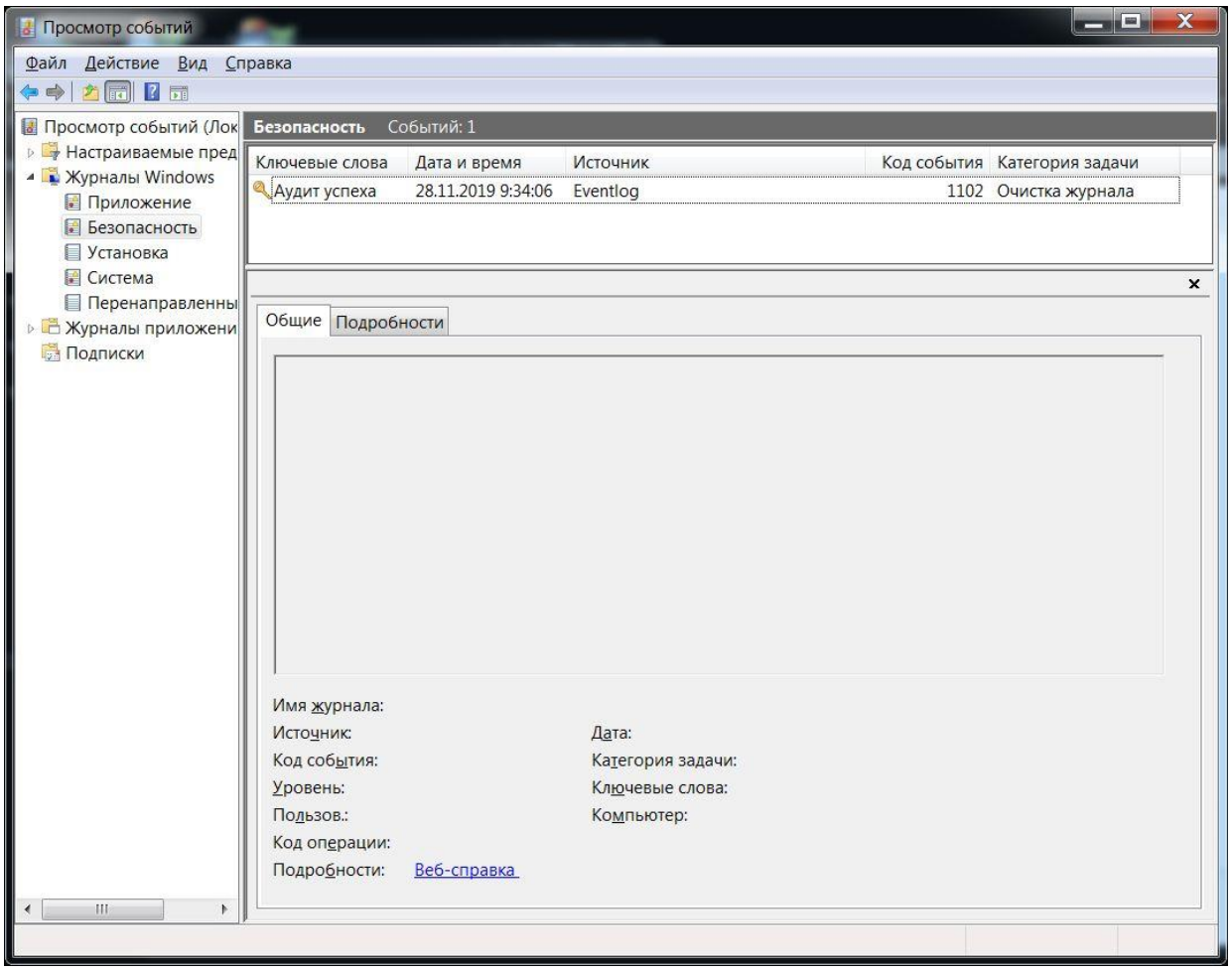
Эксперимент 2.
Делаем:

Через «Проводник» откроем папку C:\TEST и с помощью контекстного меню «Создать --> Текстовый документ», вызываемому по клику правой кнопки мыши, создаем файл «Новый текстовый документ.txt».



Наблюдаем:

В журнале событий данное действие никак не отразилось!!! Также никаких записей не будет, если с помощью того же контекстного меню создать «Точечный рисунок».



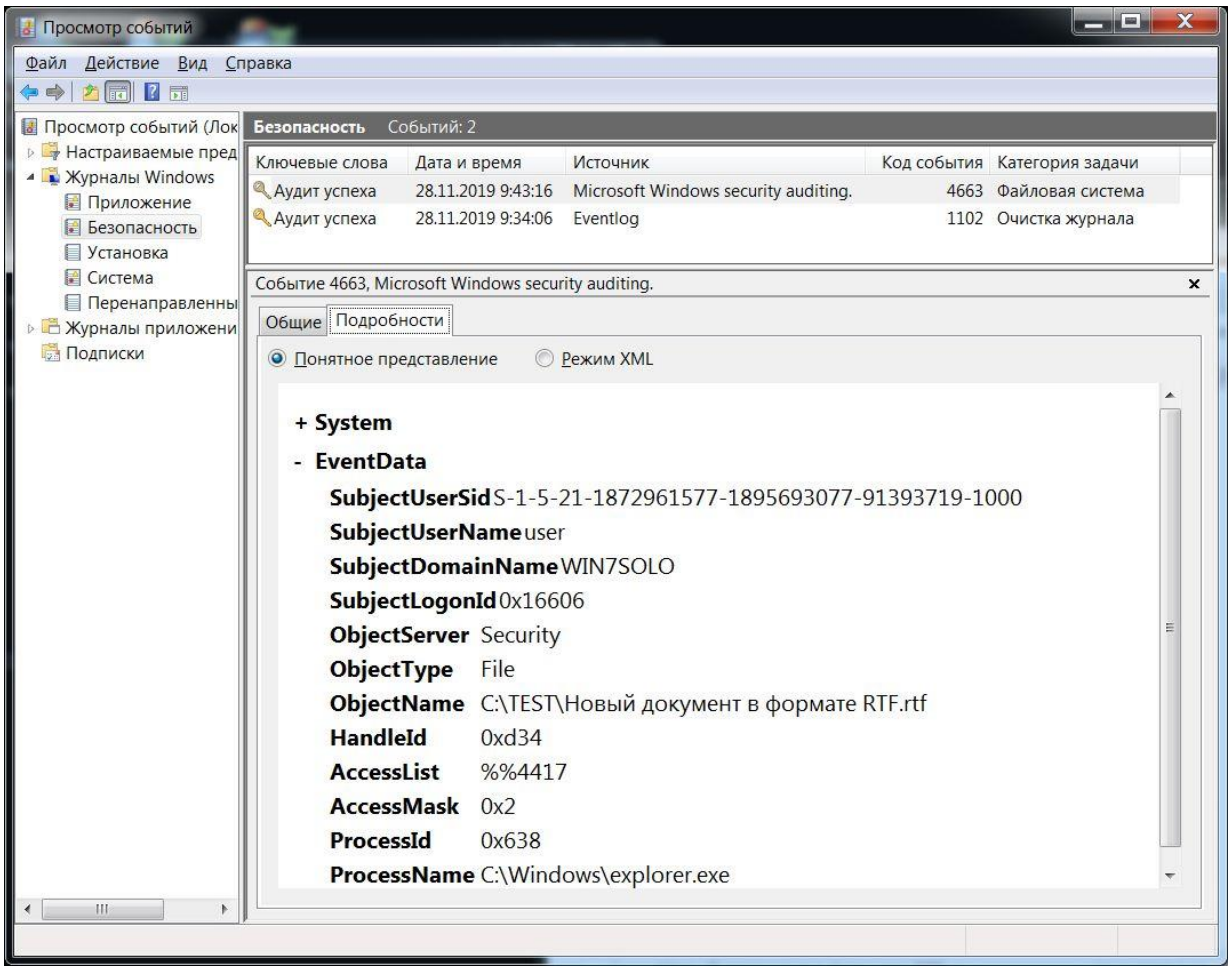
Эксперимент 3.

Делаем:

Через «Проводник» откроем папку C:\TEST и с помощью контекстного меню «Создать --> Документ в формате RTF», вызываемому по клику правой кнопки мыши, создаем файл «Новый документ в формате RTF.rtf».

Наблюдаем:

Как и в случае с созданием файла через командную строку в журнале появилось событие с кодом 4663 и соответствующим наполнением.



В чем суть проблемы?

Конечно создание текстовых документов или картинок особого вреда не представляет. Однако, если «Проводник» умеет обходить журналирование файловых операций, то это смогут сделать и вредоносы.

Данная проблема является, пожалуй, наиболее значимой из всех рассмотренных, поскольку серьезно подрывает доверие к результатам работы аудита файловых операций.

Заключение

Приведенный перечень проблем не исчерпывающий. В процессе работы удалось споткнуться о еще довольно большое количество различных мелких недоработок, к которым можно отнести использование локализованных констант в качестве значений параметров ряда событий, что заставляет писать свои анализирующие скрипты под каждую локализацию операционной системы, нелогичное разделение кодов событий на близкие по смыслу операции, например, удаление ключа реестра — это последовательность событий 4663 и 4660, а удаление значения в реестре — 4657, ну и еще по мелочи…

Справедливости ради отметим, что несмотря на все недостатки система журналирования событий безопасности в Windows имеет большое количество положительных моментов. Исправление указанных здесь критических проблем может вернуть системе корону лучшего решения по журналированию событий безопасности из коробки.

MAKE WINDOWS SECURITY EVENT LOGGING GREAT AGAIN!