УДК 004.056
https://www.doi.org/10.47813/rosnio.4.2025.2006
EDN LJMFBY

Сопоставительный анализ инструментов аудита событий безопасности на примере доступа к объектам в ОС WINDOWS и ОС LINUX на начальном этапе осуществления IT-форензика

Н.О. Стрелков, А.Д. Закурдаев*

Национальный исследовательский университет «МЭИ», ул. Красноказарменная, 14, стр.1. Москва, 111250, Россия

*E-mail: zakurdayev.a@inbox.ru

Аннотация. В статье проведен сравнительный анализ инструментов аудита доступа к объектам в ОС Windows и Linux для задач IT-форензики. Исследование акцентирует различия в подходах к мониторингу событий безопасности: Windows (журнал безопасности, Sysmon, GPO) обеспечивает удобство настройки, но ограничен нагрузкой, а Linux (auditd) предоставляет детализацию на уровне системных вызовов, требуя экспертных знаний. Результаты показали, что Linux эффективнее для расследований благодаря глубине данных, тогда как Windows упрощает управление через графические интерфейсы. Предложена интеграция инструментов с SIEM-системами для гибридных сред.

Ключевые слова: аудит событий безопасности, доступ к объектам, ОС Windows, ОС Linux, IT-форензик.

Comparative analysis of security event audit tools using the example of access to objects in WINDOWS and LINUX OS at the initial stage of IT forensics

N.O. Strelkov, A.D. Zakurdaev*

National Research University "MPEI", Krasnokazarmennaya st., 14, building 1. Moscow, 111250, Russia

*E-mail: zakurdayev.a@inbox.ru

Abstract. The article provides a comparative analysis of tools for auditing access to objects in Windows and Linux OS for IT forensics tasks. The study highlights the differences in approaches to monitoring security events: Windows (security log, Sysmon, GPO) provides ease of configuration, but is limited by the load, while Linux (auditd) provides detail at the level of system calls, requiring expert knowledge. The results showed that Linux is more effective for investigations due to the depth of data, while Windows simplifies management through graphical interfaces. Integration of tools with SIEM systems for hybrid environments is proposed.

Keywords: security event audit, object access, Windows OS, Linux OS, IT forensic.

.

1. Введение

Рост числа кибератак и ужесточение регуляторных требований (например, ФЗ-152 «О персональных данных», GDPR) повышают значимость IT-форензики для расследования инцидентов. Аудит событий безопасности – ключевой этап форензик-анализа, позволяющий восстановить хронологию действий злоумышленника. Однако различия в подходах к аудиту в ОС Windows и Linux затрудняют разработку универсальных методик, что актуализирует проведение сопоставительного анализа.

В статье впервые проведено сравнение инструментов аудита доступа к объектам в контексте IT-форензики с учетом особенностей архитектуры Windows и Linux. Предложены критерии оценки эффективности инструментов для задач расследования киберпреступлений. Результаты исследования позволяют организациям и предприятиям оптимизировать настройку аудита в гетерогенных средах, улучшить детализацию журналов для расследований и обеспечить соответствие стандартам информационной безопасности (ГОСТ Р ИСО/МЭК 27001, PCI DSS).

Проблемы аудита в Windows изучались в работах Russinovich M. и Solomon D. [1], где детально описаны механизмы SACL/DACL. Для Linux ключевые исследования проведены авторами документации auditd (Red Hat) и в работе Bauer M. [2]. Российские ученые, такие как Федотов Н.Н. [3], акцентируют роль журналов событий в расследованиях. Зарубежные авторы, включая Carrier B. («File System Forensic Analysis»), подчеркивают важность кроссплатформенного подхода. Однако вопросы сравнительного анализа инструментов аудита для этапа форензик-аудита все еще остаются малоизученными.

Нормативная база исследования. Назначение и состав подсистемы аудита операционных систем определяется в соответствии с российским и Международным стандартом ГОСТ Р ИСО/МЭК 15408 99 «Информационная технология. Методы и средства обеспечения безопасности», а также ГОСТ Р ИСО/МЭК 15408-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий [4, 5].

2. Постановка задачи (Цель исследования)

IT-форензик представляет собой междисциплинарную область, объединяющую методы анализа цифровых данных для расследования инцидентов. В отличие от традиционной финансовой экспертизы, она фокусируется на работе с электронными артефактами:

журналами событий, метаданными файлов и следами деятельности в сетевых протоколах. Специалисты в этой области используют инструменты криминалистики для восстановления цепочки событий и предоставления юридически значимых доказательств. В некоторых источниках IT-форензик называют киберкриминалистикой. Таким образом, основной целью IT-форензика является исследование информации, расположенной на цифровых устройствах в связи с компьютерными преступлениями [6].

Как указывают В.П. Суйц и И.И. Анушевский [7], форензик осуществляется в несколько этапов: 1) предварительный (форензик-аудит), 2) аналитический (сбор и анализ полученной от клиента информации), 3) оценочный этап (выявление недостатков в системе внутреннего контроля), 4) заключительный (отчет о результатах форензика и рекомендации по внесению изменений в систему внутреннего контроля с целью предотвращения мошенничества). Рассмотрим подробно первый этап IT-форензика – аудит.

Эффективное обеспечение информационной безопасности невозможно без систематического мониторинга действий пользователей и процессов. Регистрация событий в хронологическом порядке позволяет не только оперативно выявлять нарушения политик доступа, но и анализировать root-причины инцидентов. Например, фиксация неудачных попыток входа может указать на попытку брутфорс-атаки. Кроме того, сам факт наличия системы аудита оказывает профилактическое воздействие, сокращая число преднамеренных нарушений со стороны сотрудников.

Наиболее распространенные в России ОС – это ОС Windows (которая уходит из государственных учреждений вследствие замены на доверенное ПО) и ОС Linux. У каждой ОС есть, несомненно, свои достоинства и недостатки, отметим, что ОС Windows монолитна по своей архитектуре (многие программы интегрирован в саму ОС) и широко использует RPC-механизм, позволяющий компьютерам из сети давать указания пользовательскому компьютеру выполнить какие-либо действия, тогда как ОС Linux является модульной системой и не зависит от RPC-механизма.

3. Методы и материалы исследования

В рамках заявленной темы исследования остановимся подробно на аудите событий доступа к объектам, а в качестве критериев сравнения выберем следующие:

1. Гибкость настройки (возможность фильтрации событий).
2. Детализация записей (время, пользователь, объект).

3. Интеграция с SIEM-системами.
4. Соответствие стандартам (ГОСТ Р ИСО/МЭК 15408).

В среде Windows для мониторинга доступа к объектам применяются следующие инструменты: встроенное журналирование (позволяет настраивать аудит для конкретных папок, разделов реестра или принтеров через графический интерфейс), Sysmon (расширенный инструмент из пакета Sysinternals, отслеживающий создание процессов, модификацию системных файлов и подозрительную сетевую активность с привязкой к хешам исполняемых файлов), групповые политики (централизованное управление настройками аудита в доменных средах через GPO), командная строка (с её помощью можно включить аудит из командной строки, например, вывести доступные категории аудита, включить аудит успешных событий доступа к объектам файловой системы и вывести настройки категории аудита).

Перед активацией аудита в Windows администратор должен определить категории отслеживаемых событий. По умолчанию система не регистрирует действия пользователей, что требует ручной настройки через оснастку «Локальные политики безопасности». Например, для мониторинга доступа к файлам необходимо активировать подкатегорию «Аудит доступа к объектам»; задать триггеры для успешных/неудачных попыток; назначить SACL для целевых объектов через свойства файла или папки.

Политика аудита создается в следующей последовательности:

1. *Разрешение или включение аудита*. Эта задача решается с помощью параметров Audit Policy шаблона. Сначала необходимо определить, какие политики будут включены на уровне локальной машины, а затем настроить раздел Audit Policy тематической группы Local Policies с помощью консоли и применить внесенные изменения. Аудит включается после определения соответствующей политики в шаблоне и применения этого шаблона.
2. *Создание определенной политики в базе данных*. Например, чтобы установить таблицу SACL (System Access Control List) для файла secret.txt, можно использовать раздел File System шаблона. Поместив в него путь к файлу, можно дважды щелкнуть на представляющем файл объекте и установить в открывшемся окне параметры SACL.
3. *Применение политики*. Наконец следует использовать консоль Security Configuration and Analysis или команду *secedit* для применения политики. Применяя утилиту *secedit* в командных файлах, можно запрограммировать проведение такого аудита в часы,

когда нагрузка в сети минимальна, а затем проанализировать полученные результаты в удобное время.

4. *Аудит файлов и папок* разрешается с помощью групповой политики для Active Directory и локальной политики для отдельного компьютера. Затем с помощью проводника выбираются конкретные файлы, а также типы событий доступа для аудита.

В Windows администраторы могут отслеживать доступ к конкретным объектам Active Directory. Кроме того, они могут отслеживать применение пользователями особых привилегий, вход пользователей в систему, неудачные попытки доступа и выход из системы.

Каждый ресурс в Windows содержит дескриптор безопасности, состоящий из двух ключевых компонентов: DACL (определяет права доступа для пользователей и групп) и SACL (задает правила аудита, указывая, какие операции (чтение, изменение) и для каких субъектов (администраторы, гости) должны регистрироваться в журнале). Таким образом, аудит в Windows осуществляется при помощи следующих инструментов: журнал безопасности, AuditPol, Sysmon. Особенности аудита в данной ОС, следующие: аудит активируется через групповые политики (GPO) или AuditPol; SACL определяет, какие события (успех/отказ) записываются для объектов, события доступа к файлам (ID 4663) содержат данные о пользователе, пути и типе операции. Основным недостатком системы аудита является высокая нагрузка на систему при детальном аудите.

В Linux мониторинг безопасности реализуется через демона *auditd*, который перехватывает системные вызовы (*open, execve*) на уровне ядра. Для настройки используются *audit.rules* (файл правил, фильтрующий события по UID, GID или пути к файлу); *aureport* (утилита для генерации сводок по зарегистрированным инцидентам); (*ausearch* — инструмент поиска в журналах с поддержкой фильтров по временным меткам или типам событий). Аудит в Linux осуществляется при помощи следующих инструментов: *auditd*, *aureport*, правила через *auditctl*. При этом мониторинг системных вызовов (*open*, *whrite*) реализуется через правила в *audit.rules*, гибкая фильтрация осуществляется по UID, GID, пути; журналы хранятся в /var/log/audit/. Основным недостатком является сложность настройки аудита для новичков.

4. Полученные результаты

Представим сравнительный анализ инструментов аудита в обеих ОС в соответствии с указанными критериями (см. таблицу 1):

Таблица 1. Сравнительный анализ инструментов аудита в ОС Windows и ОС Linux.

Критерий	Windows	Linux
Детализация	Высокая (SACL, метаданные)	Максимальная (системные вызовы)
Гибкость	Зависит от GPO	Высокая (на уровне ядра)
Интеграция с SIEM	Через агенты (WEF, Sysmon)	Нативная поддержка (*auditd*)
Соответствие ГОСТ	Частичное	Полное (для сертифицированных дистрибутивов)

5. Выводы

Инструменты аудита событий безопасности и доступа к объектам в ОС Windows и Linux имеют свои особенности**. В ОС Windows** для аудита используется журнал, доступ к которому осуществляется с помощью административной функции «Просмотр событий» в «Панели управления Windows». Возможна регистрация входа пользователей в систему, доступа субъектов к объектам, доступа к службе каталогов Active Directory и других событий.

В ОС Linux для аудита событий используется системный журнал System Log. Также многие Unix-системы имеют средства централизованного сбора информации о событиях (сообщениях) безопасности — сервис syslog. Кроме того, для расширенного аудита событий в обеих операционных системах можно использовать утилиту **Sysmon**, которая входит в набор Sysinternals и предназначена для отслеживания активности в системе и записи детализированной информации о событиях.

Интеграция расширенного аудита событий с помощью Sysmon в SC SIEM предоставляет пользователям следующие преимущества:

1. *Детальный мониторинг* – сбор данных о процессах, сетевой активности, изменениях файлов и реестра в Windows/Linux.
2. *Оперативное обнаружение* – анализ аномалий (подозрительные процессы, несанкционированные правки) для быстрого реагирования на угрозы.
3. *Контроль и соответствие* — прозрачность операционных процессов, упрощающая аудит политик безопасности и нормативов.
4. *Кросс-платформенность*— единый мониторинг гибридных сред, снижающий сложность управления.

5. *Поддержка расследований* – собранные Sysmon данные могут быть использованы для проведения внутренних расследований и судебных экспертиз, предоставляя важные доказательства в случае инцидентов, связанных с информационной безопасностью.

Таким образом, в статье представлена разработанная автором методика сравнения инструментов аудита для решения задач форензики, выявлены преимущества *auditd* (Linux) в детализации событий, но отмечена сложность его настройки для неопытного пользователя, предложен подход интеграции Sysmon и auditd в SCADA-системы для централизованного мониторинга. Обоснованность выводов подтверждена экспериментами с настройкой аудита в Windows 10 и Astra Linux. Установлено, что Linux предоставляет более глубокие данные для расследований, но требует экспертных знаний. Таким образом, ОС Windows для аудита событий необходима настройка политики аудита, в ОС Linux используется системный журнал (System Log), в котором регистрируются любые события. ОС Linux эффективнее для форензик-аудита, так содержит лучшие механизмы по обеспечению безопасности.

Список литературы

1. Russinovich M. Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (7th ed.) / M. Russinovich, D. Solomon, A. Ionescu // Microsoft Press. – 2021. – P. 800.
2. Bauer M. Linux Server Security: Hack and Defend / M. Bauer. – Wiley, 2016. – 432 p.
3. Федотов Н.Н. Форензика-компьютерная криминалистика / Н.Н. Федотов. – М., Юридический Мир, 2007. – 432 с.
4. ГОСТ Р ИСО/МЭК 15408 99 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». – URL: https://docs.cntd.ru/document/1200029952 (дата обращения 12.05.2025).
5. ГОСТ Р ИСО/МЭК 15408-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – URL: https://docs.cntd.ru/document/1200101777 (дата обращения 12.05.2025).
6. Агуреев И.А. Форензика - инструмент защиты информации в условиях цифровой экономики / И.А. Агуреев, А.Д. Закурдаев // Тенденции развития интернет и цифровой экономики: Труды VII Международной научно-практической конференции,

Симферополь, 30- мая – 01 июня 2024 года. – Симферополь: ИП Зуева, 2024. – С. 227-228. – URL: https //elaibrary.ry/item.asp?id=67952519 (дата обращения 12.05.2025).

7. Суйц В.П. Форензик-экспертиза: сущность и основные методы организации финансовых расследований в компаниях / В.П. Суйц, И.И. Анушевский // Вестник Московского университета. Серия 6. Экономика. – 2019. – № 3. – URL: https://cyberleninka.ru/article/n/forenzik-ekspertiza-suschnost-i-osnovnye-metody-organizatsii-finansovyh-rassledovaniy-v-kompaniyah (дата обращения: 12.05.2025).