**Министерство науки и высшего образования Российской Федерации**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»**

**(ВлГУ)**

Отчет о научно-исследовательской работе

по теме

«Повышение привилегий в операционной системе Windows»

Специальность 10.03.01 – «Информационная безопасность»

|  |  |  |
| --- | --- | --- |
| Руководитель |  | к.т.н доцент кафедры ИЗИ Монахов Ю.М. |
|  | (подпись, дата) | (ФИО) |
| Студент |  | ст. гр. ИБ-121 Махров Д.И. |
|  | (подпись, дата) | (ФИО) |

Владимир 2023

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

ОС – Операционная система

ПО – Программное обеспечение

LSA – Локальный орган безопасности

LSASS – Подсистема проверки подлинности локальной системы безопасности

Winlogon – Интерактивный диспетчер входа в систему

LogonUI – Пользовательский интерфейс входа в систему

Netlogon – Служба сетевого входа

SRM – Монитор безопасности

UAC – Контроль учетных записей пользователей

SID – Идентификатор безопасности

DLL – Динамическая подключаемая библиотека

SRM – Монитор безопасности

CVE – Общие уязвимости и угрозы

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 4](#_Toc147458691)

[1 СИСТЕМА БЕЗОПАСНОСТИ ОС WINDOWS 10 6](#_Toc147458692)

[1.1 Компоненты безопасности Windows 10 6](#_Toc147458693)

[1.2 Контроль учетных записей пользователей 9](#_Toc147458694)

[1.3 Идентификаторы безопасности, маркер доступа и контроль целостности. 9](#_Toc147458695)

[2 АТАКИ НА ПОВЫШЕНИЕ ПРИВИЛЕГИЙ 11](#_Toc147458696)

[2.1 Методы атак на повышение привилегий 11](#_Toc147458697)

[ЭКСПЕРИМЕНТАЛЬНАЯ ЧАСТЬ 16](#_Toc147458698)

[ЗАКЛЮЧЕНИЕ 21](#_Toc147458699)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 22](#_Toc147458700)

ВВЕДЕНИЕ

23 страницы, 5 рисунков

**Актуальность темы.** В современном мире операционная система Windows является одной из наиболее распространенных и используемых в компьютерных системах. Ее популярность обусловлена простотой использования, широким функционалом и возможностью настройки под различные задачи. Тем не менее в Windows существует множество уязвимостей, которые могут быть использованы для проведения различных атак, что может привести к серьезным последствиям для безопасности данных.

Многим службам операционной системы требуются специальные привилегии для выполнения своих задач. Программная ошибка в привилегированном сервисе открывает путь к компрометации системы в виде несанкционированного получения привилегий.

В худшем случае злоумышленник может получить привилегии администратора или системы. Это означает, что преступник может получить доступ к конфиденциальной информации, в частности к паролям, банковским счетам, кредитным картам жертвы, личным данным, таким как адреса, телефоны, электронные адреса, коммерческой информации, если атака была направлена на организацию и т.д. Такого рода атаки также проводятся с целью изменения настроек системы, установки вредоносного ПО и последующего распространения вредоносного ПО на другие компьютеры в сети.

В целом, изучение атак направленных на повышение привилегий для последующего их предотвращения очень важно для обеспечения безопасности систем и защиты конфиденциальных данных пользователей.

**Объектом исследования** является операционная система Windows 10.

**Предметом исследования** являются уязвимости операционной системы Windows 10 и ПО, установленного в системе.

**Целью исследования** является повышение безопасности операционной системы Windows 10 путем экспериментальной проверки уязвимости системы и установленного ПО к различным атакам, направленных на повышение привилегий.

**Задачами исследования** являются:

Составление списка актуальных эксплойтов с помощью которых можно получить более высокие уровни доступа к системе.

Экспериментальная проверка эксплойтов на работоспособность на тестовом стенде.

**Методами исследования** являются систематический обзор литературы с последующим критическим анализом, эксперимент.

1 СИСТЕМА БЕЗОПАСНОСТИ ОС WINDOWS 10

1.1 Компоненты безопасности Windows 10

Одним из главных инструментов для реализации конкретных информационных технологий являются информационные системы, задача обеспечения безопасности которых является приоритетной, так как от сохранения конфиденциальности, доступности и целостности информационных ресурсов зависит результат деятельности информационных систем. Операционная система является важнейшим программным компонентом любой вычислительной машины, поэтому от уровня реализации политики безопасности в каждой конкретной операционной системе во многом зависит и общая безопасность информационной системы.

В любой среде, предоставляющей доступ к одним и тем же физическим или сетевым ресурсам сразу нескольким пользователям, остро стоит вопрос предотвращения неавторизованного доступа к конфиденциальным данным. Операционная система, наряду с отдельными пользователями, должна иметь возможность защитить файлы, память и настройки конфигурации от нежелательного просмотра и изменения. Средства безопасности операционной системы включают в себя такие вполне очевидные механизмы, как учетные записи, пароли и защита файлов. Они также включают в себя такие менее заметные механизмы, как защита операционной системы от повреждения, недопущение осуществления ряда действий со стороны менее привилегированных пользователей и запрещение неблагоприятного воздействия пользовательских программ на программы других пользователей или на операционную систему.

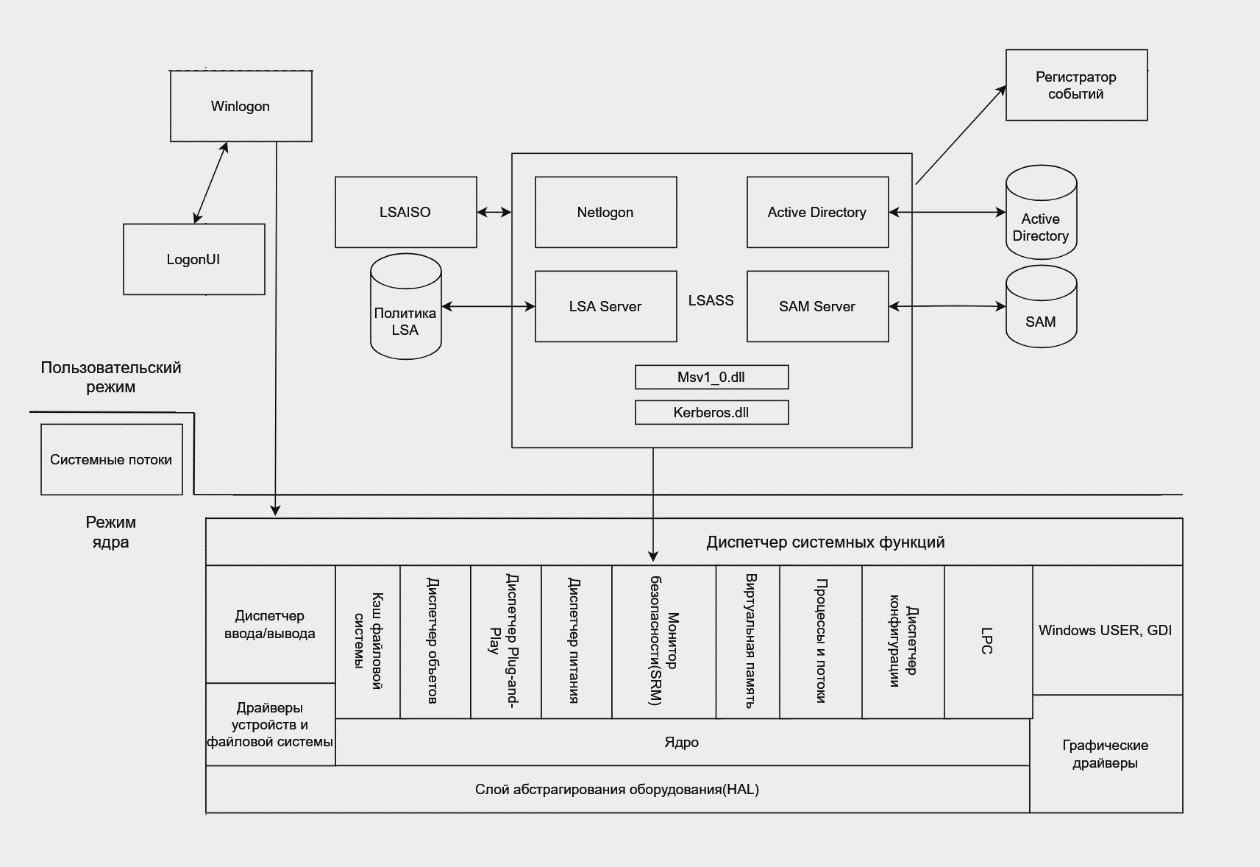


Рисунок 1 – Компоненты безопасности Windows 10

В реализацию системы безопасности Windows входят следующие компоненты и базы данных:

1. Подсистема проверки подлинности локальной системы безопасности – Local Security Authority subsystem (LSASS). Отвечает за политику безопасности локальной системы которая, определяет пользователей, обладающих правом входить в систему, политики паролей, привилегии, предоставленные пользователям и группам, и настройки проверки безопасности системы.

2. LSAISO. Используется для хранения хешей маркеров безопасности пользователей – вместо хранения самих маркеров в памяти LSASS.

3. База данных политики LSASS. База данных, в которой содержатся настройки политики безопасности локальной системы. Она включает информацию, определяет, у кого есть права на доступ к системе и каким образом осуществляется этот доступ, кому и какие привилегии назначены и какие виды проверки безопасности следует выполнять.

4. Диспетчер учетных данных в системе защиты – Security Accounts Manager (SAM). Служба, отвечающая за управление базой данных, содержащей имена пользователей и определения групп на локальной машине. SAM-служба реализована в виде библиотеки Samsrv.dll и загружается в процесс LSASS.

5. База данных SAM. База данных, которая хранит данные учетных записей и соответствующую информацию о безопасности для локальных пользователей и локальных групп.

6. Active Directory. Служба каталогов, которая содержит базу данных, хранящую информацию об объектах в домене. Домен является совокупностью компьютеров и связанных с ними групп безопасности, которые управляются как единое целое. Active Directory хранит информацию об объектах в домене, куда включаются пользователи, группы и компьютеры. В Active Directory хранится информация о паролях и привилегиях для пользователей и групп домена.

7. Интерактивный диспетчер входа в систему (Winlogon). Процесс пользовательского режима, отвечающий за управление интерактивными сеансами входа в систему.

8. Пользовательский интерфейс входа в систему (LogonUI). Процесс пользовательского режима, который предоставляет пользователям интерфейс, используемый ими для самоидентификации в системе.

9. Служба сетевого входа (Netlogon). Служба Windows, которая создает защищенный канал, по которому отправляются запросы по безопасности.

10. Монитор безопасности – Security Reference Monitor (SRM). Этот компонент режима ядра выполняет проверку доступа к объектам, генерирует записи журнала аудита и управляет правами пользователей, также называемыми привилегиями. Это компонент исполнительной системы: Ntoskrnl.exe.

1.2 Контроль учетных записей пользователей

Контроль учетных записей пользователей (UAC) является ключевой частью безопасности Windows. Контроль учетных записей снижает риск вредоносных программ, ограничивая возможность выполнения вредоносного кода с правами администратора.

Предусмотрено четыре уровня контроля от самого жесткого, при включении которого будут отображаться уведомления при изменении параметров пользователем и программами до полного отключения функции. Приложения с более низким уровнем целостности не могут изменять данные в приложениях с более высоким уровнем целостности. Когда обычный пользователь пытается запустить приложение, которому требуется маркер доступа администратора, контроль учетных записей требует, чтобы пользователь предоставлял допустимые учетные данные администратора.

1.3 Идентификаторы безопасности, маркер доступа и контроль целостности.

Вместо использования имен, которые не всегда могут быть уникальными, для идентификации всего, что производит в системе действия, Windows использует идентификаторы безопасности – SID. Идентификатор безопасности используется для уникальной идентификации субъекта безопасности или группы безопасности. Субъекты безопасности могут представлять любую сущность, которая может быть проверена операционной системой, например, учетной записью пользователя, учетной записью компьютера или потоком, или процессом, выполняющимся в контексте безопасности учетной записи пользователя или компьютера. Идентификатор безопасности хранится в базе данных безопасности. Если идентификатор безопасности используется в качестве уникального идентификатора для пользователя или группы, он никогда не может использоваться повторно для идентификации другого пользователя или группы.

При каждом входе пользователя система создает маркер доступа для этого пользователя. Этот маркер предоставляет контекст безопасности для любых действий, выполняемых пользователем на этом компьютере.

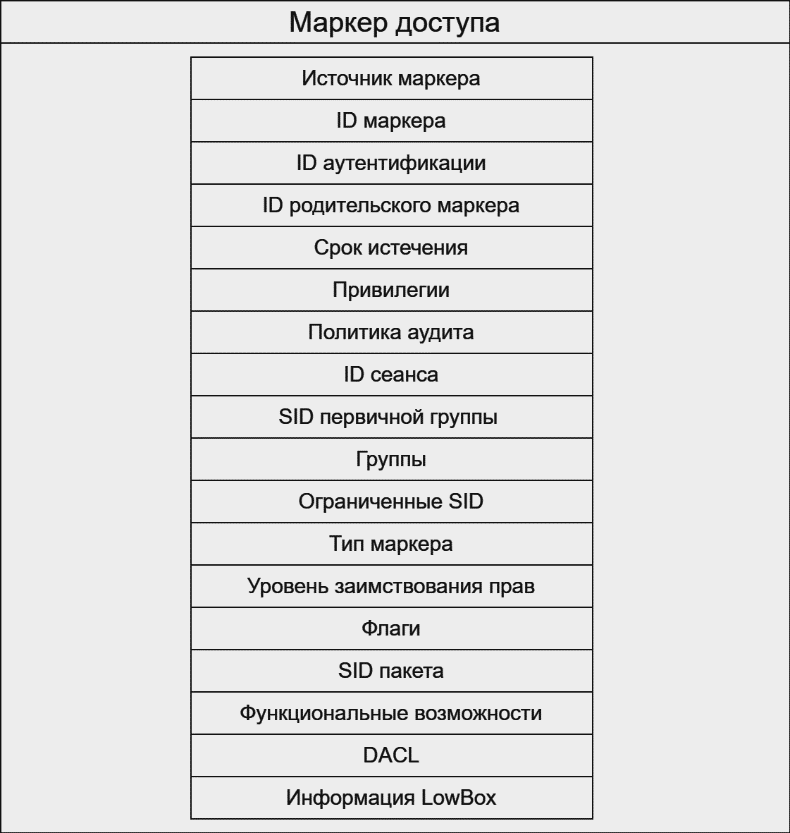


Рисунок 2 – Компоненты маркера доступа

Уровни целостности могут заменить разграничительный доступ, чтобы провести различия между процессом и объектами, запущенными от имени одного и того же пользователя и находящимися в его владении, предоставив возможность изоляции кода и данных в рамках учетной записи пользователя. Обязательный контроль целостности (MIC) позволяет монитору обращений (SRM) располагать более подробной информацией о природе вызывающего процесса путем его ассоциации с уровнем целостности. Он также предоставляет информацию о доверии, необходимую для доступа к объекту путем определения для него уровня целостности. В ОС Windows существуют пять уровней целостности со своими SID-идентификаторами: Ненадежный (0) (Untrusted), Низкий (1) (Low), Средний (2) (Medium), Высокий (3) (High), Системный (4) (System).

2 АТАКИ НА ПОВЫШЕНИЕ ПРИВИЛЕГИЙ

Повышение (эскалация) привилегий – это процесс получения пользователем или программой дополнительных привилегий на компьютере или в сети. Несанкционированное повышение привилегий пользователя достигается с помощью уязвимостей, ошибок в конфигурации операционной системы и программного обеспечения.

Выделяют две формы повышения привилегий: вертикальная и горизонтальная.

Вертикальное повышение привилегий означает, что пользователь с низким уровнем привилегий получает доступ к функциям, относящимся к более высокому уровню привилегий. При атаке с вертикальным повышением привилегий злоумышленник, так сказать, продвигается вверх по лестнице привилегий. В большинстве атак с повышением привилегий злоумышленник сначала входит в систему с учетной записью пользователя низкого уровня. Затем он может искать уязвимые места в системе, которые могут быть использованы для повышения его привилегий.

Горизонтальное повышение привилегий означает, что пользователь имеет доступ к личным данным или доступным другим пользователям функциям. При горизонтальном повышении привилегий злоумышленник является обычным пользователем низкого уровня, который получает доступ к информации других обычных пользователей. Другими словами, злоумышленник не получает никаких расширенных привилегий; он просто принимает чью-либо личность.

## 2.1 Методы атак на повышение привилегий

Повышение привилегий состоит из методов, которые злоумышленники используют для получения разрешений более высокого уровня в системе или сети. Злоумышленники часто могут входить в сеть и исследовать ее с непривилегированным доступом, но для достижения своих целей им требуются повышенные разрешения. Распространенные подходы заключаются в использовании слабых мест системы, неправильных конфигураций и уязвимостей.

1. Использование механизмов контроля разграничения привилегий

Злоумышленники могут обойти механизмы, предназначенные для контроля повышения привилегий, чтобы получить разрешения более высокого уровня. Большинство современных систем содержат встроенные механизмы контроля прав доступа, которые предназначены для ограничения привилегий, которые пользователь может выполнять на компьютере. В ОС Windows данный механизм обозначен как «Контроль учетных записей пользователей Windows» (UAC).

2. Манипулирование токенами доступа

Злоумышленники могут изменять токены доступа для работы в контексте безопасности другого пользователя или системы для выполнения действий и обхода контроля доступа. Windows использует токены доступа для определения владельца запущенного процесса. Пользователь может манипулировать токенами доступа, чтобы запущенный процесс выглядел так, как будто он является дочерним процессом другого процесса или принадлежит кому-то другому, а не пользователю, запустившему процесс. Когда это происходит, процесс также принимает контекст безопасности, связанный с новым токеном.

3. Выполнение автозапуска загрузки или входа в систему

Злоумышленники могут настроить параметры системы для автоматического запуска программы во время загрузки системы или параметры входа в систему, чтобы получить привилегии более высокого уровня в скомпрометированных системах.

4. Сценарий входа в систему

Злоумышленники могут использовать сценарии входа в Windows, автоматически выполняемые при инициализации входа в систему. Windows позволяет запускать сценарии входа в систему каждый раз, когда определенный пользователь или группа пользователей входит в систему.

5. Создать или изменить службы Windows

Злоумышленники могут создавать или изменять службы Windows для многократного выполнения вредоносных действий. Когда Windows загружается, она запускает программы или приложения, называемые службами, которые выполняют фоновые системные функции. Информация о конфигурации службы Windows, включая путь к исполняемому файлу службы или программам/командам восстановления, хранится в реестре Windows.

Злоумышленники могут установить новую службу или изменить существующую службу для запуска вредоносного кода при запуске, чтобы сохраниться в системе. Службы могут быть созданы с правами администратора, но выполняются с правами СИСТЕМЫ, поэтому злоумышленник также может использовать службу для повышения привилегий.

6. Изменение политики домена

Злоумышленники могут изменять параметры конфигурации домена, чтобы обойти защиту и/или повысить привилегии в средах домена. Домены предоставляют централизованные средства управления тем, как компьютерные ресурсы (например, компьютеры, учетные записи пользователей) могут действовать и взаимодействовать друг с другом в сети. Политика домена также включает параметры конфигурации, которые могут применяться между доменами в среде с несколькими доменами.

7. Выполнение по событию

Злоумышленники могут повысить привилегии, используя системные механизмы, которые запускают выполнение на основе определенных событий. Атаке могут быть подвержены программы по умолчанию, которые могут редактироваться пользователями, администраторами или программами, имеющими доступ к реестру, заставки, специальные возможности Windows, Инфраструктура/фреймворк совместимости приложений, профили PowerShell, установщик пакетов.

8. Эксплойты

Злоумышленники могут использовать уязвимости программного обеспечения в попытке повысить привилегии. Эксплуатация уязвимости программного обеспечения происходит, когда злоумышленник использует программную ошибку в программе, службе или в программном обеспечении или ядре операционной системы для выполнения кода, контролируемого злоумышленником. При первоначальном получении доступа к системе злоумышленник может работать в рамках процесса с более низкими привилегиями, что не позволит ему получить доступ к определенным ресурсам в системе. Могут существовать уязвимости, обычно в компонентах операционной системы и программном обеспечении, обычно работающем с более высокими разрешениями, которые можно использовать для получения более высоких уровней доступа к системе.

9. Внедрение процесса

Злоумышленники могут внедрить код в процессы, чтобы обойти защиту, основанную на процессах, а также, возможно, повысить привилегии. Инъекция процесса – это метод выполнения произвольного кода в адресном пространстве отдельного живого процесса. Запуск кода в контексте другого процесса может открыть доступ к памяти процесса, системным/сетевым ресурсам и, возможно, к повышенным привилегиям. Выполнение посредством внедрения процесса также может избежать обнаружения продуктами безопасности, поскольку выполнение маскируется под легитимный процесс. При проведении атаки злоумышленники могут внедрять библиотеки динамической компоновки (DLL) в процессы, переносимые исполняемые файлы (PE) в процессы, внедрить вредоносный код в процессы через очередь асинхронного вызова процедур (APC), внедрить вредоносный код в процессы через обратные вызовы локального хранилища потоков (TLS), внедрить вредоносный код в процессы через файловую систему /proc, внедрить вредоносный код в процесс через дополнительную оконную память (EWM).

10. Допустимые учетные записи

Злоумышленники могут получать учетные данные существующих учетных записей (аккаунтов по умолчанию, учетных записей домена, локальных учетных записей, облачных аккаунтов) и использовать их в качестве средства получения первоначального доступа, сохранения, повышения привилегий или уклонения от защиты. Скомпрометированные учетные данные также могут предоставить злоумышленнику повышенные привилегии для определенных систем или доступ к ограниченным областям сети. Злоумышленники могут отказаться от использования вредоносных программ или инструментов в сочетании с законным доступом, который предоставляют эти учетные данные, чтобы затруднить обнаружение их присутствия.

**ЭКСПЕРИМЕНТАЛЬНАЯ ЧАСТЬ**

В качестве первого эксперимента была выбрана уязвимость c идентификатором CVE–2022–21999 – уязвимость, связанная с повышением привилегий через диспетчер очереди печати Windows. Аналитики NVD (Национальная база данных об уязвимостях) дали оценку уязвимости в 4,6 балла и присвоили ей уровень MEDIUM.

Диспетчер очереди печати Windows – это встроенный компонент на всех рабочих станциях и серверах Windows, а также основной компонент интерфейса печати. Диспетчер очереди печати – это исполняемый файл, который управляет процессом печати. Управление печатью включает в себя получение местоположения правильного драйвера принтера, загрузку этого драйвера, буферизацию вызовов высокого уровня в задание на печать, планирование задания на печать и т.д. Диспетчер очереди печати загружается при запуске системы и продолжает работать до тех пор, пока операционная система не будет выключена.

Пользователь ly4k загрузил эксплойт под CVE–2022–21999 на свой Github.

Эксплойт выполняет следующие шаги:

1. Создает временную базовую директорию, которая будет использоваться для директории диспетчера очереди печати. Позже она будет превращена в точку перенаправления.
2. Создает новый локальный принтер «Microsoft XPS Document Writer v4»
3. Устанавливает директорию нового принтера в временную базовую директорию.
4. Создает точку перенаправления на нашей временной базовой директории, чтобы указать на директорию драйвера принтера.
5. Принудительно перезапускает диспетчер очереди печати, чтобы создать директорию, загрузив AppVTerminator.dll в диспетчер.
6. Записывает DLL в новую директорию внутри директории драйвера принтера.
7. Загружает DLL в диспетчер очереди печати.

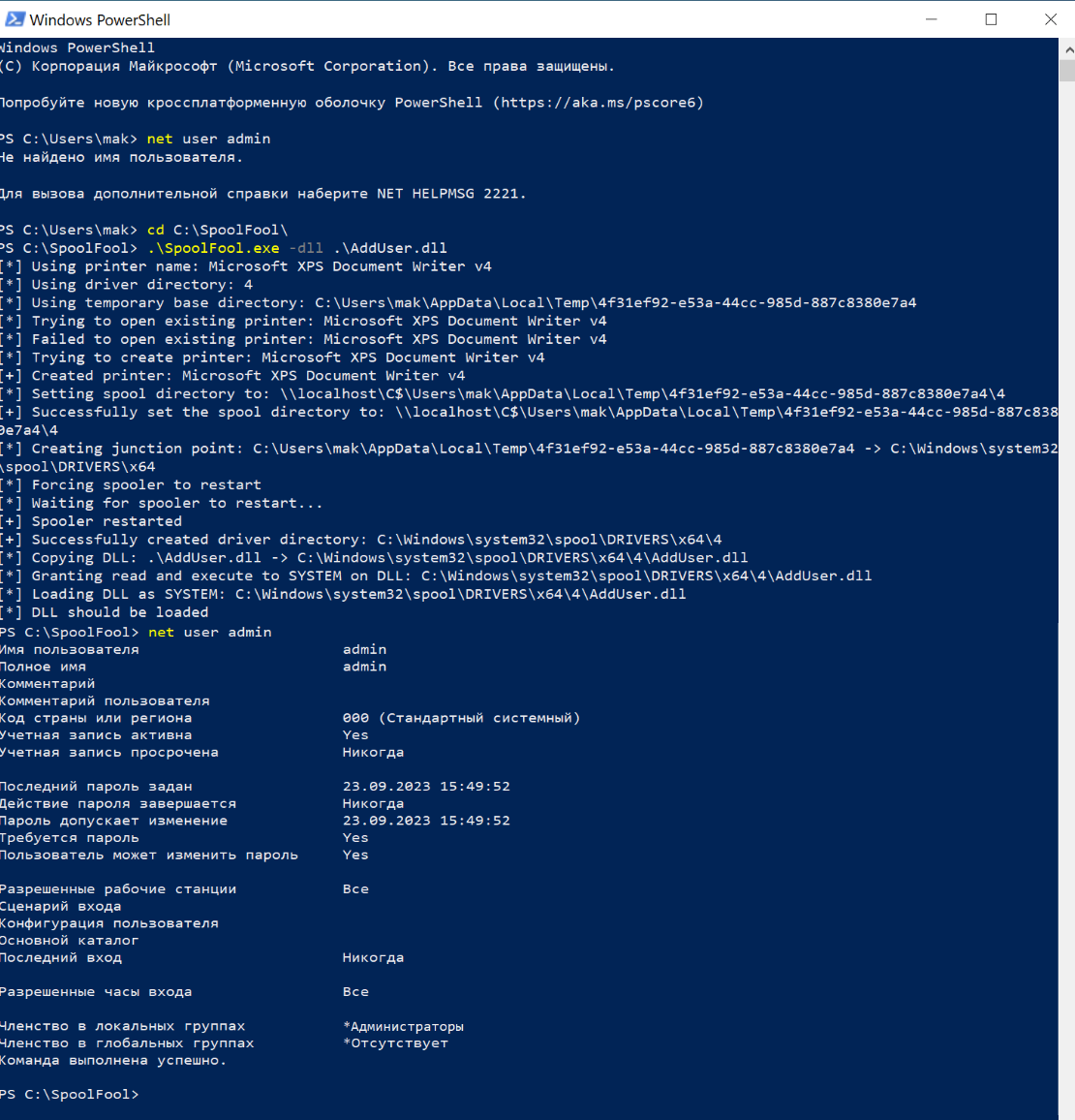


Рисунок 3 – эксплойт в действии

DLL, используемая в этом примере, создаст нового локального администратора с именем “admin”.

В качестве второго эксперимента была выбрана уязвимость c идентификатором CVE–2023–38831 – уязвимость в программе-архиваторе WinRAR.

Популярность WinRAR как условно-бесплатного продукта с более чем 500 миллионами пользователей по всему миру становится палкой о двух концах, привлекая как обычных пользователей, так и злоумышленников, стремящихся использовать его уязвимости.

В версиях WinRAR от RARLabs до 6.23 была обнаружена уязвимость, которая может быть использована злоумышленниками для выполнения произвольного кода через специально созданный архив ZIP. Уязвимость возникает из-за неправильной обработки ZIP-архивов, содержащих безобидные файлы, такие как обычные документы PDF, вместе с папками, имеющими те же имена. Когда пользователь пытается получить доступ к безобидному файлу, архив может содержать папку с похожим названием, содержащую исполняемый файл. Это вредоносное содержимое внутри папки обрабатывается во время попытки получения доступа к безобидному файлу, облегчая выполнение произвольного кода.

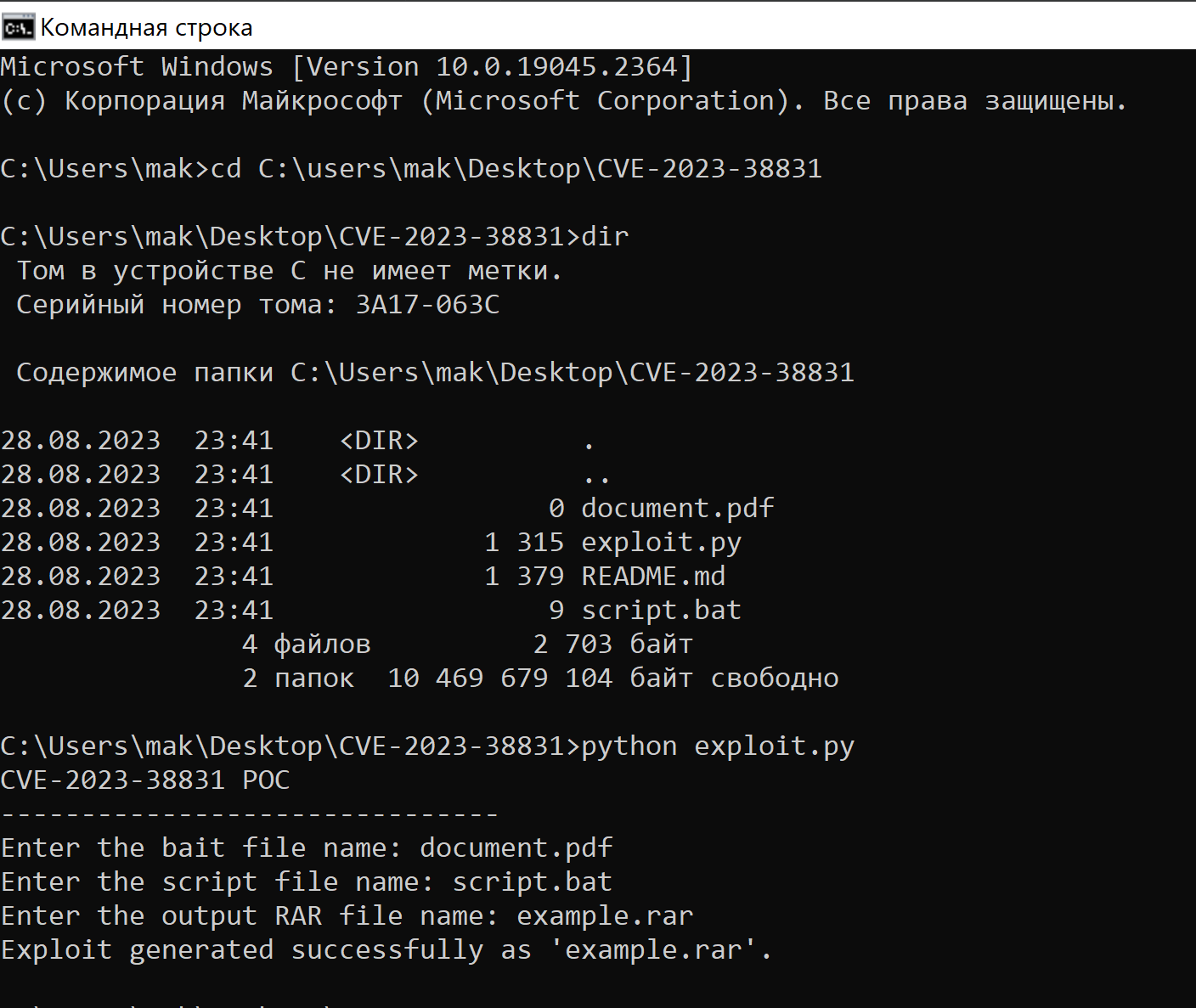


Рисунок 4 – Содержимое папки с эксплойтом, создание зараженного архива

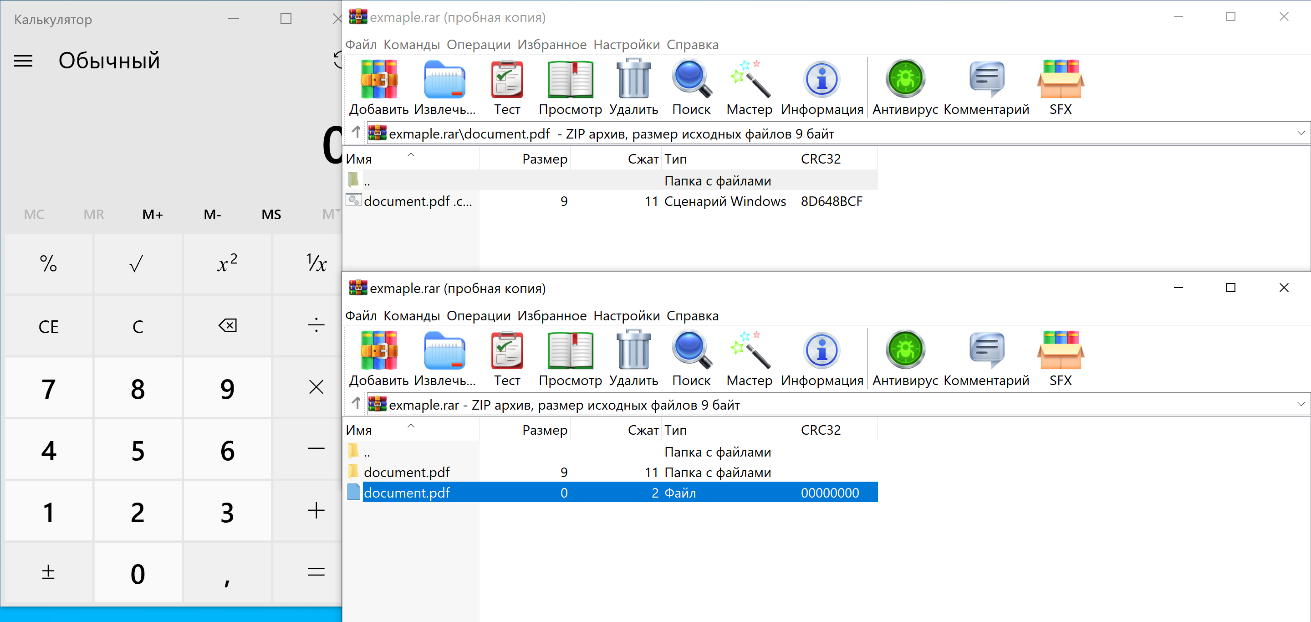


Рисунок 5 – пример использования

При попытке открыть файл document.pdf двойным нажатием в WinRAR версии ниже 6.23 пользователю не предлагается выбрать приложение для открытия этого самого файла. В место этого запускается document.pdf.cmd (Сценарий Windows), который находится в папке document.pdf

В этом конкретном случае сценарий лишь запускает процесс calc.exe, но злоумышленник может использовать вредоносный исполняемый файл, через который получит более высокий уровень доступа к системе.

В рамках научно-исследовательской работы также рассматривались уязвимости с идентификаторами CVE–2023–36874 и CVE-2023–21752 – уязвимости в Службе регистрации ошибок Windows(WER) и в службе резервного копирования Windows.

Служба WER – это привилегированная служба, роль которой заключается в анализе различных проблем с программным обеспечением, которые могут возникнуть на хосте Windows, и сообщении о них. Основная проблема уязвимости CVE–2023–36874 заключается в том, что API CreateProcess, запущенный в режиме олицетворения, будет следовать любому перенаправлению файловой системы, установленному злоумышленником, но будет использовать токен безопасности вызывающего процесса, а не имитированный токен, чтобы установить контекст безопасности процесса.

Отслеживаемая как CVE–2023–21752 уязвимость, которая позволяет обычному пользователю выполнить произвольный код на хосте для удаления файлов из указанного пути хранения из службы резервного копирования и восстановления Windows. Это действие доступно только привилегированным пользователям. Эксплойт может быть использован для повышения привилегий на хосте от обычного пользователя до системного.

Пользователь Wh04m1001 загрузил эксплойты как под CVE–2023–36874, так и под CVE–2023–21752 на свой Github.

В связи с проблемами во время компиляции кода, в научно-исследовательской работе представлены лишь краткие описания данных уязвимостей.

**ЗАКЛЮЧЕНИЕ**

В ходе выполнения НИР:

1. Рассмотрена система безопасности ОС Windows 10.

2. Рассмотрены основные механизмы проведения атак, направленных на повышение привилегий.

3. Экспериментально протестированы несколько эксплойтов.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Provos N., Friedl M., Honeyman P. Preventing Privilege Escalation. 12th USENIX Security Symposium. (2003)
2. <https://empyreal96.github.io/nt-info-depot/CS490_Windows_Internals/15_security.pdf>
3. Yosifovich P., Lonescu A., Russinovich M., Solomon D. Windows Internals Seventh Edition. Part 1. System architecture, processes, threads, memory management, and more. (2017)
4. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф., Безопасность операционных систем : учебное пособие. (2007)
5. Stallings W., Brown L. Computer Security: Principles and Practice, 4th Global Edition (2018)
6. <https://support.microsoft.com/en-us/windows/about-user-account-control-settings-d5b2046b-dcb8-54eb-f732-059f321afe18>
7. <https://learn.microsoft.com/ru-ru/windows-server/identity/ad-ds/manage/understand-security-identifiers>
8. Fernandez E., Testing UAC on Windows 10, Article. (2017)
9. <https://attack.mitre.org/tactics/TA0004/>
10. Palermo, Elizabeth. “What Is Privilege Escalation?” Tom’s Guide, Tom’s Guide, 18 Dec. 2013,
11. <https://github.com/ly4k/SpoolFool>
12. <https://research.ifcr.dk/spoolfool-windows-print-spooler-privilege-escalation-cve-2022-22718-bf7752b68d81>
13. <https://nvd.nist.gov/vuln/detail/CVE-2022-21999S>
14. <https://github.com/HDCE-inc/CVE-2023-38831>
15. <https://hdce.medium.com/cve-2023-38831-winrar-zero-day-poses-new-risks-for-traders-684911befad2>
16. <https://github.com/Wh04m1001/CVE-2023-36874>
17. <https://www.crowdstrike.com/blog/falcon-complete-zero-day-exploit-cve-2023-36874/>
18. <https://github.com/Wh04m1001/CVE-2023-21752>
19. <https://www.cloudsek.com/threatintelligence/cve-2023-21752-privilege-escalation-vulnerability-on-windows-backup-service>