Расследование инцидентов в ОС Windows

Оглавление

Краткий обзор

В настоящее время сложно кого-либо удивить атаками на компьютеры и компьютерные сети. Для атак активно используется Интернет, электронная почта и другие каналы связи. Такие действия подвергают организации правовым и финансовым рискам и часто требуют проведения внутренних компьютерных расследований.

В данной статье мы с вами обсудим процессы и инструментальные средства, которые можно использовать при проведении компьютерных расследований. В ходе расследования будут использоваться инструментальные средства Windows Sysinternals (http://go.microsoft.com/?linkId=6013253) – утилиты, используемые для исследования компьютеров на базе ОС Windows, а также внутренние команды и инструментальные средства Windows.

При этом часть политик и процедур, используемых в ходе расследования, могут также использоваться для восстановления хода происшествия.

Компьютерная модель расследования

Согласно Warren G. Kruse II и Jay G. Heiser, авторов книги «Computer Forensics: Incident Response Essentials», компьютерные расследования это – "сохранение, идентификация, извлечение, документация и интерпретация компьютерных носителей для анализа первопричины". Компьютерная модель расследования показывает логическую модель проведения расследования.

Четыре стадии расследования, применяются специалистами при работе с цифровыми доказательствами. В ходе расследования специалисты:

1. **Оценивают ситуацию.** Проводят анализ области расследования и предпринимаемых действий.
2. **Накапливают данные.** Собирают, защищают и сохраняют оригинальные доказательства.
3. **Анализируют данные.** Исследуют и сопоставляют цифровые доказательства с теми событиями, которые представляют реальный интерес, что в дальнейшем позволит понять ход атаки.
4. **Подготавливают отчет о проведенном расследовании.** Собирают и упорядочивают собранную информацию и составляют окончательный отчет.

Детально стадии проведения расследования мы с вами рассмотрим ниже.

Инициирование процесса расследования

Прежде, чем вы начнете свое расследование, вы должны инициировать процесс расследования.

Перед тем, как проводить расследование, вы должны понять, будете ли вы привлекать юристов для проведения административного (уголовного) преследования злоумышленника. Если вы примете решение, что это необходимо, то вы должны привлечь правоохранительные органы, если ваше руководство не решит поступить иначе. Вместе с тем необходимо понимать, что это можно сделать и на более поздних стадиях проведения расследования.

Однако необходимо понимать, что в первую очередь необходимо предотвратить дальнейшее нанесение ущерба злоумышленниками. Ведь расследование важно, но гораздо важнее защитить организацию от возможного ущерба, если, конечно, нет проблемы государственной безопасности.

Аудитория

В первую очередь, данная статья предназначена для специалистов в области информационной безопасности и IT, которые нуждаются в понимании общих принципов построения компьютерных

расследований, включая многие процедуры, которые могут быть использованы в таких расследованиях.

Оценка ситуации

Рассмотрим, как провести полную оценку ситуации, установить область инцидента и определить требуемые ресурсы для проведения внутреннего расследования.

Уведомление руководства организации и получение разрешения на проведение внутреннего расследования

Для проведения внутреннего расследования компьютерного инцидента, вы должны получить соответствующее разрешение вашего руководства, если ваша политика безопасности не предусматривает инцидентное разрешение. В таком случае вы должны провести полную оценку ситуации и определить дальнейшие шаги. Для этого вам необходимо сделать следующее:

- Если в вашей организации не существует написанной политики по реагированию на инциденты, то вы обязаны письменно уведомить руководство и получить письменное разрешение от уполномоченного лица о проведении компьютерного расследования.
- В ходе расследования вы обязаны документировать все действия, связанные с расследованием. Тем самым вы сможете гарантировать, что есть точное и законченное описание событий и решений, произошедших в ходе инцидента и ответа на инцидент. В дальнейшем эта документация может использоваться в суде для описания действий, проводимых в ходе расследования.
- В зависимости от контекста инцидента и при отсутствии угрозы государственной безопасности вашей главной задачей является защитить организацию от нанесения дальнейшего ущерба. После того, как безопасность организации обеспечена, следующими задачами являются восстановление услуг и расследование инцидента.

Вместе с тем вам следует учитывать, что ваши решения и доказательства могут быть оспорены в суде, поскольку компьютерное доказательство – весьма сложный процесс и различные исследования могут дать разные результаты и разные заключения.

Обзор политик и процедур

Начиная компьютерное расследование, крайне важно понимать политики и процедуры, принятые в компании, к которым вы можете обратиться в ходе расследования. Обратите внимание на следующие важные соображения:

- Имеете ли вы законные полномочия для проведения расследования?
- Существуют ли принятые в вашей организации политики и процедуры, в которых описаны правила обращения с конфиденциальной информацией?
- Описаны ли в этих политиках и процедурах правила проведения внутреннего расследования в случае инцидента?
  Ведь не секрет, что во многих компаниях соответствующие политики и процедуры отсутствуют или не рассмотрены и не согласованы с юристами. А, кроме того, не все служащие и посетители уведомлены об их существовании. Если вы не уверены в ваших полномочиях, проконсультируйтесь с вашим руководством и юристами.

- Проконсультируйтесь с вашими юристами во избежание потенциальных проблем неправильной обработки результатов проведенного расследования. В число таких проблем могут входить:
    - Персональные данные скомпрометированных клиентов;
    - Нарушение любых государственных законов;
    - Несение уголовной или административной ответственности за перехват электронных сообщений;
    - Просмотр чувствительной или привилегированной информации. Данные, которые могут поставить под угрозу конфиденциальность информации клиента, должны быть сделаны доступными как часть связанной с расследованием документации, если это непосредственно использовалось в проведении расследования.
- В дальнейшем гарантируйте конфиденциальность клиентских данных:
    - Все данные должны надежно храниться, при этом контроль за доступом к ним должен быть ужесточен;
    - По окончании расследования все данные, включая документацию, в течение периода времени, согласованного с юристами или в соответствии с законодательством, должны находиться под пристальным вниманием. Если данные – потенциальная часть уголовного дела, то необходима консультация с правоохранительными органами.
- В случае судебного иска необходимо поддерживать и тщательно хранить все цифровые копии доказательств, в том числе проводить другие необходимые мероприятия для обеспечения сохранности всего доказательства. В случае если вы не обеспечите безопасное хранение доказательств, вы не обеспечите доверие собранным в ходе расследования доказательствам. Сохранность доказательств достигается при наличии документации, поддающейся проверке.

Создание группы проведения расследований

Для успешного проведения внутреннего компьютерного расследования чрезвычайно важно определить группу реагирования на инциденты. Идеальным является создание группы до того, как она реально потребуется для возможного расследования. Чрезвычайно важно, чтобы члены группы имели навыки проведения подобных расследований. При этом необходимо учесть следующее:

- Определите человека (людей) которые понимают, как нужно проводить расследование. Идеальным будет проведение обучения на соответствующих курсах. Помните, что в случае проведения слушаний в суде, навыки и умения человека, проводившего расследование будут тщательно исследоваться.
- Назначьте членов группы расследования и определите их обязанности.
- Назначьте одного из членов группы как технического руководителя. Как правило, технический руководитель должен иметь опыт участия в проведении расследований и иметь достаточные технические знания. Не забывайте, что члены группы проведения расследования должны иметь более высокую квалификацию, чем подозреваемые.
- Для обеспечения защиты информации и личной безопасности группы расследования ее состав должен оставаться в тайне.
- В случае отсутствия в организации должным образом подготовленного персонала, к расследованию может привлекаться доверенная внешняя группа, обладающая необходимыми знаниями.

- В случае проведения расследования вам необходимы гарантии, что каждый член группы обладает необходимыми полномочиями для решения поставленной задачи. Данный пункт особенно важен в случае привлечения внешней группы по проведению расследований.

Важно! Так как некоторые цифровые доказательства являются энергозависимыми, то критическим фактором проведения расследования становится время.

Полная оценка ситуации

Для определения приоритета соответствующих действий и распределения ресурсов группы расследования критически важна полная оценка ситуации. Данная оценка определяет текущее и потенциальное воздействие инцидента на бизнес организации, позволяет идентифицировать затронутую инфраструктуру и как можно полнее оценить ситуацию. Вместе с тем эта информация позволит вам быстрее определить соответствующее направление работы.

Для получения полной оценки ситуации:

- Для описания ситуации используйте всю возможную ситуацию, ее потенциальные опасности, потенциально затрагиваемые стороны и, если возможно, информацию о подозреваемой стороне
- Идентифицируйте возможные воздействия на вашу организацию. Оцените, затрагивает ли инцидент данные ваших клиентов, финансовые данные или конфиденциальные данные компании. Не забудьте оценить потенциальное влияние инцидента на связи с общественностью. Стоит учесть, что данная оценка, вполне вероятно, будет вне полномочий служб информационных технологий и информационной безопасности и, возможно, должна быть сделана при поддержке руководства и юристов компании
- В течение расследования проанализируйте воздействие инцидента на бизнес организации. Перечислите количество времени и ресурсов, необходимых для полной ликвидации последствий инцидента, время простоя, стоимость поврежденного оборудования, оцените возможную потерю доходов и стоимость разглашенной конфиденциальной информации. Учтите, что такая оценка должна быть реалистичной. Фактические затраты на преодоление последствий инцидента будут определены позднее
- Проанализируйте возможные нематериальные потери – воздействие на репутацию организации, мораль служащих и т.д. Не стоит раздувать серьезность инцидента. Этот анализ необходим вам только для того, чтобы понять область инцидента. Фактические потери от инцидента будут определены позднее. Вероятнее всего, что данная оценка потерь будет вне компетенции служб информационных технологий и информационной безопасности и будет выполняться руководством вместе с юристами и другими подразделениями.

Для проведения идентификации, анализа и документирования сетевой инфраструктуры и компьютеров, затронутых инцидентом, необходимо выполнить следующее:

- Идентифицируйте сеть (сети), вовлеченную в инцидент, количество, типы и роли затронутых инцидентом компьютеров.
- Изучите топологию сети, включая детальную информацию о серверах, сетевых аппаратных средствах, системах сетевой защиты, подключениях к Интернет.
- Идентифицируйте внешние запоминающие устройства.
- Идентифицируйте любые удаленные компьютеры, подключаемые к вашей компьютерной сети.

- В случае необходимости (если вам требуется оперативный анализ), фиксируйте сетевой трафик. Данный тип анализа необходим вам в том случае, если в сети продолжается подозрительный трафик. Microsoft ® Windows XP и Windows Server 2003 включают встроенные сетевые инструментальные средства сбора данных для фиксирования локального сетевого трафика – Netcap и Rasdiag. Вместе с тем вы можете использовать Windows Network Monitor (NetMon) и Windows Sysinternals TDIMon[1] для сетевого анализа данных.
  Важно! Network sniffing (фиксация сетевого трафика) может нарушить режим секретности. Это зависит от собранного контента. Поэтому стоит быть чрезвычайно осторожным при разворачивании подобных средств сбора данных.
- Для исследования состояния приложений и операционных систем на компьютерах, которые затрагивает ваше расследование, используйте инструментальные средства. В этом случае полезными средствами являются файлы журналов Windows, Windows Sysinternals PsTools.
- Для исследования и документирования затронутых файлов и серверов приложений используйте инструментальные средства Windows Sysinternals: PsTools, PsFile, ShareEnum и лог-файлы Windows.
  Важно! Часть информации, которая будет собрана в результате этой оценки, будет зафиксирована вашими инструментами в реальном времени. Вы должны гарантировать надежную сохранность любых записей или сгенерированных файлов регистрации, чтобы предотвратить потерю этих энергозависимых данных.

Для получения завершенного понимания ситуации выполните следующее:

- Сформируйте временной график. Это особенно важно для глобальных инцидентов. Документ должен содержать возможные несоответствия между датой и временем рабочих станций и службой времени Windows Server 2003.
- Идентифицируйте всех вовлеченных в инцидент лиц и возьмите у них интервью. Это чрезвычайно важно для понимания ситуации. Интервью должны проводиться опытными сотрудниками.
- Документируйте все результаты интервью. Вам они потребуются позже для полного понимания ситуации.
- Восстановите и сохраните информацию (файлы журналов) внешних и внутренних устройств сети, таких как систем сетевой защиты и маршрутизаторов, которые могли бы находиться на возможном пути атаки.
- Общедоступную информацию, типа IP-адреса и имени домена, для возможной идентификации атакующего можно получить с помощью Windows Sysinternals Whois http://go.microsoft.com/?linkId=6013254

Собранная вами информация может пригодиться для подготовки плана восстановления после инцидента.

Сбор доказательств

На стадии сбора доказательств вы должны гарантировать, что правильно определили результат стадии оценки ситуации. В результате данной стадии вы должны получить детальный документ, содержащий информацию, которую вы посчитаете необходимой и обеспечивающий отправную точку для

[1] Инструментальные средства Windows Sysinternals могут быть загружены по адресу http://www.microsoft.com/technet/sysinternals/default.mspx

следующей стадии. Кроме всего прочего нужно учесть, что если инцидент становится больше чем просто внутреннее расследование и требует обращения в правоохранительные органы, то вполне возможно, что все процессы, используемые для сбора доказательств, могут быть использованы независимым третьим лицом (группой лиц) для достижения тех же результатов.

Такой документ должен содержать следующую информацию:

- Начальная оценка воздействия инцидента на бизнес организации.
- Детальная топология сети с подробными указаниями о том, какие компьютерные системы и каким образом скомпрометированы.
- Результаты беседы с пользователями и администраторами скомпрометированных систем.
- Результаты любых юридических и сторонних взаимодействий.
- Сообщения и файлы журналов, сгенерированные инструментальными средствами, используемыми на стадии оценки.
- Предложенное направление и план действий

Важно! Создание непротиворечивой, точной и детальной документации в ходе компьютерного расследования поможет в дальнейшем ходе расследования. Эта документация часто становится критическим фактором для успеха проекта и поэтому ее создание никогда не должно пропускаться. Создаваемая вами документация является доказательством, которое может использоваться в последующих юридических процедурах. Прежде, чем вы начнете выполнение следующей стадии проведения расследования, вы должны гарантировать, что получили итоговую документацию, созданную на стадии оценки.

Сбор данных

В данном разделе мы с вами обсудим, как собрать данные, необходимые для проведения расследования. Стоит учесть, что некоторые данные, получаемые в ходе расследования, энергозависимы и могут быть легко повреждены. Поэтому вы должны гарантировать, что соответствующие данные собраны правильно и правильно сохранены для проведения анализа.

Формируйте компьютерный инструментарий для проведения расследования

Для грамотного и своевременного проведения расследования вашей организации потребуется коллекция аппаратных и программных средств для сбора данных в ходе расследования. Такой инструментарий должен содержать ноутбук с набором соответствующих программных средств, операционных систем с соответствующими обновлениями, мобильными носителями, сетевым оборудованием и набором соответствующих кабелей. Идеально создать такой инструментарий заранее. Причем члены группы должны быть ознакомлены с инструментальными средствами до проведения расследования.

Сбор доказательств

Сбор цифровых доказательств выполняется локально или по сети. Преимуществом локального сбора данных является большее управление компьютером и соответствующими данными. Однако необходимо понимать, что локальный сбор данных не всегда возможен.

Важно! При использовании инструментальных средств для сбора данных важно определить вначале, был ли установлен rootkit[2].

В случае сбора данных по сети, вы должны учитывать тип собираемых данных и те усилия, которые для этого потребуются.

Рекомендуемый процесс сбора данных:

1. Создайте точную документацию, которая позволит вам идентифицировать и подтвердить подлинность собранных доказательств. Вы должны гарантировать, что обращаете внимание на любые потенциально интересные элементы и регистрируете любые действия, которые могли бы быть позже признаны важными в процессе расследования. Ключом к успешному расследованию является надлежащая документация, включая следующую информацию:
    a. Кто выполнил действие и почему?
    b. Что этим пытались достигнуть?
    c. Как конкретно выполнено действие?
    d. Какие при этом использованы инструменты и процедуры?
    e. Когда (дата и время) выполнено действие?
    f. Какие результаты достигнуты?
2. Определить необходимые методы проведения расследования. Как правило, используется комбинация автономных и интерактивных методов проведения расследования.
    a. При проведении автономных расследований дополнительный анализ выполняется на **поразрядной копии оригинального доказательства**[3]. Автономный метод расследования применяется всегда, когда это возможно, так как это уменьшает риск повреждения оригинального доказательства. Однако стоит учесть, что данный метод может использоваться только в тех случаях, когда может быть создана соответствующая копия и не может быть использован для сбора некоторых энергозависимых данных.
    b. При проведении интерактивного расследования анализ выполняется на оригинальном оперативном доказательстве. Лица, участвующие в проведении расследования, должны быть особенно осторожны ввиду риска модификации доказательств.
3. Идентифицировать и задокументировать потенциальные источники данных, включая:
    a. Серверы. Информация включает роль сервера, файлы логов, файлы данных, приложения.
    b. Лог-файлы внутренних и внешних сетевых устройств.
    c. Внутренние аппаратные компоненты (например сетевые адаптеры).
    d. Внешние порты – Firewire, USB и PCMCIA.
    e. Запоминающие устройства, включая жесткие диски, сетевые запоминающие устройства, сменные носители.
    f. Переносные мобильные устройства – PocketPC, Smartphone и MP3-плееры.

---

[2] Rootkits - программные компоненты, которые управляют компьютером и скрывают свое существование от стандартных диагностических инструментальных средств. Поскольку rootkits работают на низком аппаратном уровне, они могут прервать и изменить системные вызовы. Один из доступных инструментов для выявления наличия rootkits в системе, является Microsoft ® Windows Sysinternals RootkitRevealer (http://go.microsoft.com/?linkId=6013255).

[3] Поразрядная копия - законченная копия всех данных из целенаправленного источника, включая информацию загрузочного сектора, разделов и свободного дискового пространства.

4. При фиксировании энергозависимых данных тщательно рассматривайте порядок сбора данных. Учтите, что энергозависимое доказательство может быть легко разрушено при выключении питания.
5. Используйте следующие методы сбора данных:
    a. Если вам необходимо извлечь любые устройства внутренней памяти, то необходимо проверить, чтобы все энергозависимые данные были зафиксированы, а затем выключить компьютер.
    b. Решите, удалить ли запоминающее устройство или использовать вашу собственную систему для фиксирования данных. Учтите, что возможна ситуация, когда вы не сможете удалить запоминающее устройство из-за проблем несовместимости или из-за аппаратной несовместимости.
    c. Создайте поразрядную копию доказательства на резервном носителе, гарантируя что оригинальное доказательство защищено от записи. Весь последующий анализ данных должен выполняться на этой копии, а не на оригинальном доказательстве.
    Важно! Произведите поразрядное копирование с помощью таких средств как EnCase от Guidance Software (http://www.guidancesoftware.com/) или FTK от AccessData (http://www.accessdata.com/).
    d. Документируя запоминающие устройства, гарантируйте включение информации об их конфигурации. Обратите внимание на изготовителя и модель оборудования, параметры настройки перемычки, объем устройства, тип интерфейса и состояние диска.
6. Проверьте собранные вами данные. Если есть возможность, создайте контрольные суммы и цифровые подписи, чтобы гарантировать, что скопированные данные идентичны оригиналу. Учтите, что в некоторых случаях (например, наличие сбойных секторов на носителе данных) вы не сможете создать абсолютную копию. Однако вы должны гарантировать, что получили наилучшую копию, которую можно было создать с доступными инструментальными средствами. Для вычисления криптографических хешей по алгоритмам MD5 или SHA1 вы можете использовать Microsoft File Checksum Integrity Verifier (http://www.microsoft.com/downloads/details.aspx?FamilyID=b3c93558-31b7-47e2-a663-7365c1686c08&DisplayLang=en) (FCIV).

Хранение и архив

После того, как вы собрали доказательства и они уже готовы к анализу, чрезвычайно важно архивировать и хранить их таким образом, чтобы гарантировать целостность.

Лучшими способами хранения и архивации данных являются:

- Хранение данных в физически безопасном месте.
- Документирование физического и сетевого доступа к этой информации.
- Гарантия того, что неуполномоченный персонал по сети или иным способом не имеет доступа к доказательствам.
- Защита комнат и оборудования, в которых хранятся носители, содержащие доказательства, от воздействия электромагнитных полей и статического электричества.
- Изготовление не менее двух копий доказательств, собранных вами в ходе расследования. При этом одна из копий должна храниться в безопасном месте вне основного здания.
- Необходимо гарантировать, что доказательство защищено как физически (например, помещая его в сейф) так и в цифровой форме (например, назначая пароль на носители данных).

- Необходимо ясно и понятно документировать весь процесс хранения информации доказательства.
- Создайте журнал контроля, который включает следующую информацию:
    - имя человека, исследующего доказательство;
    - точная дата и время начала работы с доказательством;
    - точная дата и время его возврата в хранилище.

Анализ данных

В данном разделе мы обсудим различные подходы к анализу доказательств, собранных на стадии сбора данных внутреннего расследования.

Важно! Часто необходим интерактивный анализ данных, в ходе которого исследуется сам компьютер. При этом интерактивный анализ выполняется из-за ограничения времени на расследование или фиксирование энергозависимых данных. При проведении данного типа анализа необходимо быть крайне осторожным, чтобы не испортить доказательства.

Анализируйте сетевые данные

При проведении многих расследований необходимо анализировать сетевые данные. При этом используется следующая процедура:

1. Исследуйте сетевые лог-файлы на наличие любых событий, которые могут представлять для вас интерес. Как правило, лог-файлы содержат огромные объемы данных, так что Вы должны сосредоточиться на определенных критериях для событий, представляющих интерес. Например, имя пользователя, дата и время, или ресурс, к которому обращались во время инцидента.
2. Исследуйте систему сетевой защиты, прокси-сервер, систему обнаружения вторжения и лог-файлы служб удаленного доступа.
3. Рассмотрите лог-файлы сетевого монитора для определения событий, произошедших в сети.
4. С помощью любого сниффера рассмотрите сетевые пакеты.
5. Определите, зашифрованы ли сетевые подключения, которые вы исследуете.

Анализируйте данные рабочих станций

Данные рабочих станций (PC) включают информацию о таких компонентах, как операционная система и установленные приложения. Используйте следующую процедуру, чтобы анализировать копию данных, полученных вами на стадии сбора данных.

1. Идентифицируйте собранные вами материалы. Стоит учесть, что собранных с рабочих станций данных будет намного больше, чем необходимо для анализа инцидента. Следовательно, вы заранее должны выработать критерии поиска событий, представляющих интерес для расследования. Например, вы можете использовать Microsoft Windows® Sysinternals Strings tool для поиска файлов, расположенных в папке \Windows\Prefetch. Эта папка содержит информацию о том, где, когда и какие приложения были запущены.
2. Исследуйте данные операционной системы и любые данные, загруженные в память компьютера, для того, чтобы определить, выполняются ли (подготовлены к запуску) любые злонамеренные приложения или процессы. Например, для того, чтобы увидеть, какие

программы будут выполнены в процессе загрузки или входа в систему, можно использовать Windows Sysinternals AutoRuns.

3. Исследуйте выполняющиеся прикладные программы, процессы, сетевые подключения. Например, вы можете найти прикладные программы с соответствующими названиями, но стартовавшие из ненормативных мест. Для выполнения подобных задач можно использовать Windows Sysinternals ProcessExplorer, LogonSession и PSFile.

Анализируйте носители данных

Носители данных, собранные вами в ходе стадии сбора данных, будут содержать много файлов. Однако вам придется проанализировать эти файлы, чтобы определить их причастность (или непричастность) к инциденту. Ввиду огромного количества файлов, эта процедура может быть чрезвычайно сложной.

Для того чтобы извлечь и проанализировать данные, расположенные на собранных носителях данных, можно использовать следующую процедуру:

1. Проведите автономный анализ поразрядной копии оригинального доказательства.
2. Определите, использовалось ли шифрование данных (Encrypting File System (EFS) в Windows Microsoft). Для установления факта применения EFS вам потребуется исследование определенных ключей реестра[4]. Просмотреть необходимые ключи можно, используя статью «Encrypting File System in Windows XP and Windows Server 2003» (http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/cryptfs.mspx) из Microsoft TechNet. Если вы подозреваете, что шифрование данных все же использовалось, то вам придется определить, сможете ли вы фактически прочитать зашифрованные данные. Эта возможность будет зависеть от многих обстоятельств: версии Windows, входит ли данный компьютер в домен, каким образом был развернут EFS. Для получения дополнительной информации о EFS можно обратиться к статье «The Encrypting File System» (http://www.microsoft.com/technet/security/guidance/cryptographyetc/efs.mspx) на Microsoft TechNet. Существуют внешние инструментальные средства восстановления EFS, например Advanced EFS Data Recovery (http://www.elcomsoft.com/aefsdr.html) от компании Elcomsoft.
3. В случае необходимости распакуйте любые сжатые файлы.
4. Создайте дерево каталогов. Может быть очень полезно графически представить структуру каталогов и файлов на носителях данных, чтобы затем эффективно анализировать файлы.
5. Идентифицируйте файлы, представляющие интерес. Если вы знаете, какие файлы затронул инцидент безопасности, вы можете вначале сосредоточить расследование на этих файлах. Для сравнения известных файлов (входящих в состав операционной системы или прикладных программ) могут использоваться наборы хешей, созданные National Software Reference Library http://www.nsrl.nist.gov/. Для категорирования и идентификации файлов можно использовать информационные сайты типа http://www.filespecs.com/ , Wotsit's Format (http://www.wotsit.org/), http://www.processlibrary.com/ и Microsoft DLL Help (http://support.microsoft.com/dllhelp/Default.aspx).
6. Исследуйте реестр для получения информации о процессе загрузки компьютера, установленных приложениях (включая загружаемые в процессе запуска) и т.д. Для получения информации о системном реестре и детального описания содержания системного реестра, см. Windows Server 2003 Resource Kit Registry Reference

[4] Реестр - база данных, содержащая информацию о конфигурации ОС Windows

http://technet2.microsoft.com/WindowsServer/en/library/56a33a88-a7b2-4f21-ab5e-5c62d728619f1033.mspx?mfr=true. Для исследования реестра доступны различные инструментальные средства, включая RegEdit, входящий в состав операционной системы Windows, Windows Sysinternals RegMon for Windows http://go.microsoft.com/?linkId=6013256 и Registry Viewer <http://www.accessdata.com/products/> от AccessData.

7. Исследовать содержание всех собранных файлов, чтобы идентифицировать те из них, которые могли бы представлять интерес.
8. Изучить файлы метаданных, представляющие интерес, используя инструментальные средства типа Encase от Guidance Software (http://www.guidancesoftware.com/), The Forensic Toolkit (FTK) от AccessData (http://www.accessdata.com/) или ProDiscover от Technology Pathways (http://www.techpathways.com/). Следует учесть, что атрибуты файла (метка времени) могут показать время создания, последнего обращения и последнего изменения, которые могут быть полезны при исследовании инцидента.
9. Для просмотра идентифицированных файлов используйте специальные средства просмотра этих файлов, что позволит просматривать файлы без использования создавшего эти файлы оригинального приложения. Обратите внимание, что выбор средства просмотра определяется типом файла. Если средство просмотра не доступно, используйте оригинальное приложение для исследования файла.

После того, как вы проанализируете всю доступную информацию, вы сможете подготовить заключение. Однако на этой стадии чрезвычайно важно быть очень осторожным и гарантировать, что вы не обвините невиновную сторону. Если вы уверены в ваших результатах, то можете начать подготовку отчета.

Подготовка отчета о расследовании

В данном разделе мы рассмотрим создание итогового отчета по вашему расследованию. В процессе создания отчета используется два шага.

Сбор и упорядочение информации для отчета

В ходе расследования на каждой стадии создавались промежуточные отчеты о совершении определенных действий. На данной стадии вы должны упорядочить эту информацию по соответствующим категориям. Для этого:

1. Соберите всю документацию и примечания, полученные на всех стадиях проведения расследования.
2. Идентифицируйте те части из документации, которые соответствуют целям расследования.
3. Идентифицируйте факты, поддерживающие выводы, которые затем вы будете делать в отчете.
4. Создайте список всех доказательств, которые будут представлены в отчете.
5. Перечислите любые заключения, которые затем будут представлены в вашем отчете.
6. Классифицируйте информацию, собранную вами, чтобы гарантировать, что ясный и краткий отчет – результат расследования.

Напишите отчет

После упорядочения информации вы должны использовать ее для создания итогового отчета. Данный отчет, являясь итогом расследования, должен быть изложен ясно и кратко. Кроме того, необходимо учитывать аудиторию, для которой он предназначен.

В отчете должны быть следующие разделы:

1. **Цель отчета**. Ясно объясните цель отчета, аудиторию, на которую он рассчитан, и причины создания данного отчета.
2. **Авторы отчета**. Перечислите всех авторов и соавторов отчета, включая их позиции, обязанности в течение расследования.
3. **Краткое описание инцидента**. Опишите инцидент, объясните его воздействие. Описание должно быть составлено таким языком, чтобы нетехнический человек мог понять, что и каким образом произошло.
4. **Доказательства**. Обеспечьте описания доказательств, которые были получены в ходе расследования. При описании доказательств укажите, как оно было получено, когда, кем и каким образом.
5. **Подробности**. Обеспечьте детальное описание того, как были проанализированы доказательства, какие методы анализа при этом использовались. Объясните результаты анализа. Перечислите процедуры, которыми сопровождалось расследование и использованные методы анализа. Включите в отчет доказательства ваших результатов.
6. **Заключение.** Суммируйте результат расследования. Процитируйте определенные доказательства, чтобы доказать заключение, однако не указывайте чрезмерно подробно как было получено это доказательство. Заключение должно быть максимально ясно и однозначно.
7. **Приложения**. Включите любую основную информацию, упомянутую в отчете, типа сетевых диаграмм, документов, описывающие используемые компьютерные процедуры расследования и краткие обзоры технологий, используемые при проведении расследования. Важно, чтобы приложения обеспечили достаточно информации для читателя отчета, с тем, чтобы понять суть инцидента настолько полно насколько возможно.

Приложение: Инструменты

Таблица 1.

Значки инструментов

Значок	Описание
	Инструмент командной строки
	Инструмент с интерфейсом графического интерфейса пользователя, который требует инсталляции и изменяет целевой диск

В следующих таблицах приведена информация о различных инструментальных средствах, которые могут быть использованы в компьютерных расследованиях.

Инструментальные средства Windows Sysinternals

Таблица 2.

Windows Sysinternals Описание инструментальных средств

Тип инструмента	Название	Описание
	AccessChk v2.0 http://go.microsoft.com/?linkId=6013259	Отображает, к каким файлам, ключам реестра или сервисам Windows имеет доступ пользователь или группа, выбранная вами
	AccessEnum v1.3 http://go.microsoft.com/?linkId=6013259	Показывает, кто имеет доступ к определенным каталогам, файлам и ключам реестра компьютера. Используйте эту утилиту для того, чтобы найти места, где должным образом не применены разрешения
	Autoruns v8.53 http://go.microsoft.com/?linkId=6013259	Показывает список программ, запускаемых автоматически в процессах загрузки компьютера и входа пользователя. При этом также отображается полный список местоположений файлов и ключей системного реестра, в которых соответствующие приложения сконфигурированы для автозагрузки
	Autorunsc v8.53 http://go.microsoft.com/?linkId=6013259	Версия командной строки программы Autoruns (описана ранее)
	Diskmon http://go.microsoft.com/?linkId=6013259	Фиксирование всех действий вашего жесткого диска
	DiskView http://go.microsoft.com/?linkId=6013259	Дисковая утилита с графическим интерфейсом. Средство просмотра содержимого диска
	Du v1.3 http://go.microsoft.com/?linkId=6013259	Отображение использования диска (чтение-запись) конкретным каталогом
	Filemon v7.03 http://go.microsoft.com/?linkId=6013259	Отображение всей деятельности файловой системы в реальном масштабе времени
	Handle v3.2 http://go.microsoft.com/?linkId=6013259	Отображает открытые файлы и процесс, который открыл эти файлы
	ListDLLs v2.25 http://go.microsoft.com/?linkId=6013259	Показывает все DLL, которые загружены в данное время, включая номера версий (отображают полные имена путей загруженных модулей)
	LogonSessions v1.1 http://go.microsoft.com/?linkId=6013259	Показывает активные сеансы входа в систему
	PendMoves v1.1 http://go.microsoft.com/?linkId=6013259	Показывает какие файлы будут переименованы и удалены при следующей перезагрузке
	Portmon v3.02 http://go.microsoft.com/?linkId=6013259	Показывает активность последовательного и параллельного порта, в том числе части данных, посылаемых и получаемых соответствующими портами
	Process Explorer v10.2 http://go.microsoft.com/?linkId=6013259	Показывает файлы, ключи реестра и другие объекты, которые порождают открытые процессы, какие DLL при этом загружены, владельцев соответствующих процессов и т.д.
	PsExec v1.72 http://go.microsoft.com/?linkId=6013259	Дистанционно запускает процессы
	PsFile v1.01 http://go.microsoft.com/?linkId=6013259	Показывает открытые файлы
	PsInfo v1.71 http://go.microsoft.com/?linkId=6013259	Отображает информацию о компьютере

	PsList v1.27 http://go.microsoft.com/?linkId=6013259	Отображает информацию о процессах и потоках
	PsLoggedOn v1.32 http://go.microsoft.com/?linkId=6013259	Отображает список учетных записей пользователей, которые в данный момент времени подключены к компьютеру
	PsLogList v2.63 http://go.microsoft.com/?linkId=6013259	Записи файла регистрации событий дампа
	PsService v2.2 http://go.microsoft.com/?linkId=6013259	Просмотр и контроль служб
	Regmon v7.03 http://go.microsoft.com/?linkId=6013259	Показывает в реальном времени все обращения к реестру
	RootkitRevealer http://go.microsoft.com/?linkId=6013259	Обнаружение и удаление rootkits
	ShareEnum v1.6 http://go.microsoft.com/?linkId=6013259	Сканирование общих ресурсов сети и просмотр их параметров безопасности, чтобы выявить и устранить ненадлежащие параметры настройки
	Streams v1.53 http://go.microsoft.com/?linkId=6013259	Показывает альтернативные потоки данных файловой системы NTFS
	Strings v2.3 http://go.microsoft.com/?linkId=6013259	Поиск ANSI и UNICODE строк в двоичных файлах
	TCPVcon v2.34 http://go.microsoft.com/?linkId=6013259	Отображает активные сокеты
	TCPView v2.4 http://go.microsoft.com/?linkId=6013259	Показывает все открытые TCP и UDP соединения и соответствующие названия процессов
	TDIMon v1.01 http://go.microsoft.com/?linkId=6013259	Показывает информацию TCP/IP
	Tokenmon v1.01 http://go.microsoft.com/?linkId=6013259	Отображает всю связанную с защитой деятельность, включая вход в систему, выход из системы, использование привилегий

Команды Windows

Таблица 5.

Информация о командах Windows

Тип команды	Название	Описание
	Arp	Отображает ARP-таблицу
	Date	Отображает текущую дату
	Dir	Отображает список файлов и подкаталогов
	Doskey	Хронология команд для отрытого командного окна
	Ipconfig	Показывает текущую IP-конфигурацию
	Net	Обновление, исправление или отображение сети или сетевых соединений
	Netstat	Отображает статистику и информацию о текущем подключении
	Time	Отображает (устанавливает) текущее время
	Find	Поиск текстовой строки в одном или нескольких файлах

	Schtasks	Позволяет администратору создавать, удалять, изменять и опрашивать запланированные задачи в локальной или удаленной системе. Заменяет AT.exe
	Systeminfo	Эта команда позволяет администратору получить сведения о конфигурации системы
	Vol	Вывод метки и серийного номера тома диска
	Hostname	Вывод имени компьютера
	Openfiles	Эта команда позволяет администратору вывести список файлов и папок, которые были открыты в системе
	FCIV (File Checksum Integrity Verifier) http://support.microsoft.com/kb/841290	Создание хешей на базе алгоритов MD5 или SHA1
	Notepad	Используется для проверки метаданных, ассоциированных с файлом
	Reg	Используется для просмотра, модификации, экспорта, сохранения или удаления ключей, значений и ветвей реестра
	Netcap http://technet2.microsoft.com/WindowsServer/en/library/7e8e71a0-16c2-46ce-bd40-fa8ea0dbeb5e1033.mspx?mfr=true	Сбор информации трассировки из командной строки
	Sc	Утилита командной строки для связи с NT Service Controller и сервисами
	Assoc	Просмотр и изменение сопоставлений файлов
	Ftype	Просмотр и изменение типов файлов, сопоставленных с расширением имен файлов
	Gpresult	Отображает результирующую политику (RSoP) для указанного пользователя и компьютера.
	Tasklist	Отображает список приложений и связанные с ними задачи/процессы, которые исполняются в текущий момент на локальном или удаленном компьютере.
	MBSA Microsoft Baseline Security Analyser http://www.microsoft.com/technet/security/tools/mbsahome.mspx	Сканер безопасности от Microsoft
	Rsop.msc	Показывает результирующий набор политик
	Rasdiag http://technet2.microsoft.com/WindowsServer/f/?en/library/e38acbb8-c414-4ac7-b301-	Сбор диагностический информации об удаленных сервисах

	be0293a157f91033.mspx	