Discovery & Audit

Проблематика

Привилегированные аккаунты являются плацдармом внутренних и внешних атак, так как представляют собой кратчайшие пути к наиболее ценным данным компаний. Управление ими и их защита начинается с их обнаружения и оценки рисков безопасности, связанных с каждым из них. Однако систематический процесс идентификации и защиты всех привилегированных аккаунтов представляет собой серьезную проблему из-за их большого числа, отсутствия ретроспективы смены их статусов и документации, а также из-за смены сотрудников.

Типично, что число разделяемых и привилегированных аккаунтов в 2-3 раза больше числа пользователей в компании. Разделяемые аккаунты существую повсюду: на рабочих станциях, переносных компьютерах, серверах, в БД, средствах защиты и сетевом оборудовании, виртуальных машинах, коде приложений, веб-приложениях – процесс поиска становится практически невозможным без специального инструмента, предназначенного для их обнаружения и идентификации. Проблема осложняется тем, что сотрудники и внешние пользователи, управляющие аккаунтами, меняются или покидают компанию, часто унося столь важные знания. Несмотря на попытки документирования и отслеживания привилегированных аккаунтов, всегда значительная их часть остается недокументированной, в силу их наследования или расширения бизнеса.

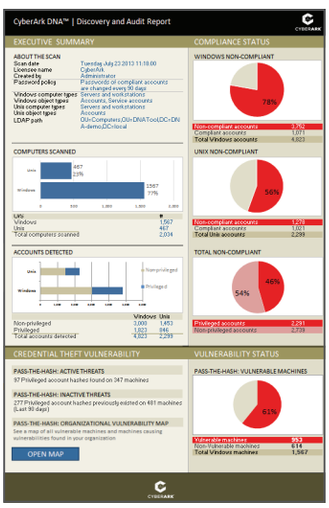
Определение нахождения привилегированных аккаунтов и их числа – только первый шаг к пониманию связанных с ними рисков и уязвимостей. Старые, статичные пароли так же, как и хеши паролей в сети порождают высокий риск компрометации учетных данных. Например, атаки типа Pass-the-Hash используют уязвимости хешей для получения привилегий или доступа к ценным активам и данным. Как результат, полное понимание проблем безопасности привилегированных аккаунтов требует полного сканирования сети, аудита учетных данных и хранения хешей паролей.

Обследование, аудит и понимание уязвимостей привилегированных аккаунтов может решить следующие проблемы:

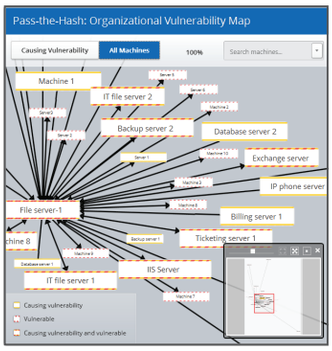
- **Безопасность и риск-менеджмент:** Если степень риска не понятна, подразделения ИТ и безопасности не владеют информацией, требуемой для его снижения.
- **Аудит и соответствие:** При отсутствии в компании четкого понимания об объеме и местонахождениях привилегированных аккаунтов, у аудитора не будет достаточной информации для завершения аудита.
- **Управление проектом:** Если компания озаботилась проблемой привилегированных аккаунтов, расчет бюджета и ресурсов на внедрение окажутся невозможными без четкой картины проблемы.

CyberArk DNA™ сканирует Вашу сеть, чтобы:

- Найти привилегированные аккаунты
- Четко оценить риски, с ними связанные
- Идентифицировать все привилегированные пароли, ключи SSH, и хэши паролей уязвимые для атак Pass-the-Hash
- Собрать полную и исчерпывающую информацию для аудита



Пример отчета для менеджмента для легкой идентификации проблем



Визуальные карты хэшей паролей и SSH ключей

Решение и основные выгоды

Discovery & Audit (CyberArk DNA™) – это запатентованный, автономный, легкий в использовании инструмент, раскрывающий масштаб проблемы привилегированных аккаунтов в компании. Решение обеспечивает исчерпывающий список всех привилегированных аккаунтов в сети, отчет об ассоциированных с ними паролях и узлах, уязвимых для атак Pass-the-Hash.

Пары SSH ключей, включая повреждённые пары (с утраченной частью пары), их статус в том числе возраст, характеристики шифрования, статус соблюдения и доверительные отношения по всей организации.

Выполнение DNA-сканирования это простой, автоматический процесс, не требующий инсталляции агентов и не создающий нагрузку на пропускную способность сети. С этим быстрым, удобным для обследования инструментом, администратор ИТ или ИБ сможет получить детальное представление о количестве привилегированных аккаунтов, статусе и уязвимости каждого из них в форме элементарного отчета или через простой интерфейс.

CyberArk DNA ответит на вопросы:

- На каких сетевых серверах присутствуют привилегированные аккаунты?
- Какие аккаунты имеют расширенные привилегии?
- Какие из привилегированных аккаунтов не соответствуют политике безопасности, например, чьи пароли не менялись более 60 дней?
- Создавали ли внешние пользователи или третьи лица привилегированные аккаунты на сервере?
- Остались ли backdoor-аккаунты в списанных системах?
- Какие узлы уязвимы для атак Pass-the-Hash и сколько их?
- Как может быть реализована атака в сети компании?
- Сколько ключей SSH и повреждённых пар существуют в сети?
- Доступ к каким серверам и ресурсам в сети можно получить с помощью SSH ключей , и откуда?

Получение исчерпывающего отчета о привилегированных аккаунтах, их учетных данных и уязвимостях позволяет подразделениям ИТ и ИБ эффективно управлять и защищать привилегированные аккаунты. Оперативная идентификация рисков безопасности позволяет снизить их вероятность и потенциальный ущерб бизнесу. Аудит проходит проще и эффективнее. Абсолютные знания о ландшафте угроз привилегированных аккаунтов становятся понятны для принятия решения об их защиты.

Возможности

CyberArk DNA предоставляет следующие ключевые возможности:

- **Простота процедуры сканирования –** элементарный трехэтапный процесс, не требующий установки ПО, сканирует все каталоги для поиска привилегированных, разделяемых и общих аккаунтов на рабочих станциях и серверах.
- **Графическое предоставление результата** – простой, лаконичный формат для менеджмента о рисках и соответствии аккаунтов.
- **Детальная отчетность – детальный отчет** является единственной верной версией обо всех привилегированных аккаунтах, уязвимостях Pass-the- Hash и статусе каждого аккаунта.
- **Схема уязвимостей Pass-the-Hash** иллюстрирует как злоумышленник может использовать уязвимости Pass-the-Hash через связь узлов для доступа к целевой системе.
- **Карта доверий ключей SSH** - визуальное отображение всех ключей SSH (включая повреждённые пары) иллюстрирует доверительные отношения, которые позволяют доступ к привилегированным учетным записям.
- **Индикативное оповещение** – отчет содержит индикаторы о проблемах, таких как некорректное использование аккаунта и уязвимости Pass-the-Hash.
- **Глубокое сканирование с минимальным воздействием на производительность** – многопоточное приложение, расходуя минимум пропускной способности сети и процессорной мощности, без внесения каких-либо изменений, в режиме «только чтение», быстро проводит сканирование контроллеров доменов и целевых машин.

Выгоды

По обнаружению каждого привилегированного аккаунта определяется степень риска
быстрый, точный отчет о числе и статусах позволяет немедленно засечь неизвестные или неверно управляемые аккаунты и действовать без промедления.

Уязвимости к конкретным атакам становятся очевидны
идентификация хешей привилегированных паролей обеспечивает понимание ключевых уязвимостей Pass-the-Hash, оптимизируя планирование и внедрение.

Сокращение ценного времени и затрат на подготовку к аудиту
аудиторы получают достоверный, скоррелированный и исчерпывающий отчет о состоянии привилегированных аккаунтов, заменяющий сложные и затратные методы получения такой информации.

Прозрачность проблем и решений привилегированных аккаунтов
просто и достоверно представляется масштаб проблемы, оптимальный подход к планированию, бюджетированию и развертыванию решения.

Внедрение полноценного решения
Cyber-Ark, лидер рынка предлагает всесторонние средства для контроля, мониторинга, управления и наблюдения за привилегированными аккаунтами. Это готовое решение начинается с критичной функции аудита и обнаружения всех привилегированных аккаунтов в сети.

Спецификации

CyberArk DNA™ работает под управлением
- Windows 7

Сканируемые системы

32-х и 64-битные версии всех платформ

Windows Workstations:
- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows 8

Windows Servers:
- Windows 2000
- Windows 2003
- Windows 2008
- Windows 2012

Unix:
- RHEL 4-6
- Solaris Intel 10
- SUSE
- Fedora
- Oracle
- CentOS

Сетевые протоколы :
- Windows:
- Windows File and Print Sharing
- Windows (WMI)

Unix:
- SSH