STRONGPASS.

Описание функциональных характеристик.

О программе

Программа для ЭВМ “Strongpass” (далее - Strongpass) - это инструмент проактивной защиты от использования слабых паролей. В момент, когда пользователь или администратор пытается установить новый пароль для учетной записи, Strongpass проверяет новый пароль на надежность. Если пароль по результатам проверок признается небезопасным, то пользователь или администратор не сможет установить новый пароль.

Strongpass не заменяет настройки групповых политик Windows или Linux, устанавливающие требования к сложности пароля, а дополняет их и предназначен для совместной работы с ними. За счет собственных проверок Strongpass позволяет минимальными средствами резко повысить сложность атаки на инфраструктуру компании и минимизировать риски проникновения с использованием слабых паролей пользователей.

Основные результаты, которые достигаются при использовании Strongpass:

– для атакующего резко повышается время подбора пароля. Особенно сильно это будет проявляться при онлайн атаках подбора пароля и при наличии средств защиты ограничивающих количество запросов в единицу времени (rate limit). В зависимости от целей атакующего данный вектор может быть признан бесперспективным и атака будет прекращена по инициативе самого атакующего;
– за счет повышенного количества событий неудачных аутентификаций у службы ИБ появляется дополнительное время и данные для обнаружения и блокировки атакующего.

Продукт не имеет собственного графического интерфейса, т.к. не взаимодействует с Пользователем напрямую. Взаимодействие с пользователем происходит через штатные интерфейсы и механизмы Windows, FreeIPA, ALD Pro, предназначенные для смены или установки пароля.

Функциональные характеристики

– проверка по базе из 847 млн. слабых и скомпрометированных паролей за 1 секунду. Все пароли в базе хранятся в хэшированном виде без возможности восстановления пароля в открытом виде в приемлемые сроки;
– не нужен доступ в интернет. Все проверки производятся локально в собственной инфраструктуре;
– не зависит от того кто пытается установить пароль: администратор или обычный пользователь;
– интеграция со стандартными механизмами установки, смены пароля в Linux, Windows и контроль попыток установки пароля используя эти механизмы:
  – командная строка (FreeIPA, ALD Pro, Active Directory);
  – графический интерфейс (FreeIPA, ALDPro, Active Directory);
  – powershell (только Active Directory);
  – веб-интерфейсы OWA, ADFS (только Active Directory).
– работает совместно с парольными политиками и дополняет их своими проверками;

– проверки происходят при:
  – принудительной смене пароля учетной записи системным администратором (“сброс” пароля);
  – смене пароля самим пользователем;
  – создании новых учетных записей.
– журналирование результатов проверки:
  – Windows Event Log (Windows);
  – текстовый файл (Linux).
– режим «демонстрации» (проверки производятся, но реальной блокировки слабых паролей не происходит);
– исключение из проверок по имени пользователя;
– проверки по собственному списку запрещенных слов, последовательностей символов.

Собственный список запрещенных паролей, последовательностей символов требуется, если необходимо дополнительно усилить парольную политику в компании, либо если необходимо исключить слова характерные для компании. Наиболее часто в качестве частей пароля используется:
– название компании, где работает сотрудник;
– последовательные символы на клавиатуре (например qaz, zxcv и т.д.)
– числа по возрастанию или убыванию (например: 123, 12345 и т.д.)

Особенности проверок по собственному списку запрещенных слов, последовательностей символов:
– все сравнения регистронезависимые;
– производится поиск:
  – подстроки
  – обратной подстроки
– производится оценка “похожести” пароля (пароль отличается от пароля в списке до 3х символов включительно).

Пример использования списка запрещеных слов, последовательностей символов

Включите в свой список запрещенных слов, паролей, например, слово `strongpass`. Все пароли использующие это или похожее слово нельзя будет использовать в качестве нового пароля. На схеме указано какие пароли будут заблокированы и почему.