Лабораторная работа. Создание и хранение надежных паролей

Задачи

Понять, что такое надежный пароль.

Часть 1. Понятие надежного пароля

Часть 2. Надежно ли хранятся ваши пароли?

Исходные данные/сценарий

Пароли широко используются для обеспечения доступа к ресурсам. Злоумышленники используют самые различные способы для того, чтобы узнать пароли пользователей и получить несанкционированный доступ к ресурсам или данным.

Чтобы защитить себя, важно понимать, что представляет собой надежный пароль и как его следует хранить.

Необходимые ресурсы

- ПК или мобильное устройство с доступом в Интернет

Часть 1: Создание надежного пароля

Чтобы создать надежный пароль, необходимо соблюсти 4 основных требования, перечисленных в порядке важности.

1) Пользователь должен легко запомнить пароль.
2) Другие лица не должны быть способны угадать этот пароль.
3) Никакая программа не должна уметь быстро подбирать пароль.
4) Пароль должен быть сложным, содержать цифры, символы и заглавные и строчные буквы.

В соответствии с приведенным выше списком первое требование, возможно, является самым важным, потому что вам будет необходимо запомнить этот пароль. Например, пароль считается надежным, потому что удовлетворяет всем трем последним требованиям, но его очень сложно запомнить.

Большинство организаций требует, чтобы пароль состоял из комбинации цифр, символов и заглавных и строчных букв. Пароли, соответствующие этой политике, вполне допустимы, но только если пользователю будет легко их запомнить. Ниже приводится пример политики составления пароля, действующей в типичной организации.

- Пароль должен быть длиной минимум 8 символов.
- Пароль должен включать заглавные и строчные буквы.
- Пароль должен содержать цифру.
- Пароль должен содержать символ (не букву и не цифру).

Проанализируйте характеристики надежного пароля и общую политику создания пароля, представленную выше. Почему данная политика противоречит первым двум пунктам? Поясните ответ.

_____

_____

_____

_____

_____

_____

Для создания надежных паролей мы рекомендуем составлять цепочку из четырех или более случайных слов и связывать их друг с другом. Пароль **televisionfrogbootschurch** надежнее, чем **J0n@than#81**. Несмотря на то что второй пароль полностью соответствует приведенным выше политикам, программы для взлома пароля достаточно эффективны, чтобы вычислить такой тип пароля. Хотя пароль **televisionfrogbootschurch** не будет принят большинством политик создания паролей, на самом деле он намного надежнее, чем второй пароль. Пользователю проще его запомнить (особенно потому, что он связан с образом), он очень длинный, а сам набор слов настолько случаен, что делает задачу его взлома практически неосуществимой.

Используя онлайн-инструмент генерации паролей, создайте пароли на основе политики, описанной выше.

a. Откройте веб-браузер и перейдите по ссылке: http://passwordsgenerator.net.

b. Выберите варианты в соответствии с заданной политикой создания паролей.

c. Создайте пароль.

   Легко ли запомнить созданный пароль?

   _____

   _____

   При использовании онлайн-инструмента для создания паролей пароли создаются на основе случайных слов. Так как слова слиты вместе, их нельзя вычленить как отдельные словарные статьи (т. е. слова из словаря).

d. Откройте веб-браузер и перейдите по ссылке: http://preshing.com/20110811/xkcd-password-generator/.

e. Создайте случайный словарный пароль, нажав кнопку **Generate Another! (Создать другой!)** вверху веб-страницы.

f. Легко ли запомнить созданный пароль?

   _____

   _____

Часть 2: Надежное хранение паролей

Если пользователь решит использовать менеджер паролей, первое правило надежного пароля будет нарушено, так как пользователю нужно будет все время обращаться к менеджеру паролей. Заметим, что отдельные пользователи хранят свои пароли только в своей памяти. Менеджеры паролей (как локальные, так и удаленные) должны иметь хранилище паролей, а оно может быть скомпрометировано.

Хранилище менеджера паролей должно быть надежно зашифровано, а доступ к нему должен тщательно контролироваться. Облачные менеджеры паролей обеспечивают бесперебойный доступ

для своих пользователей в любое время через мобильные приложения на телефонах и веб-интерфейсы.

Популярным менеджером паролей является сервис Last Pass.

Создайте пробную учетную запись в сервисе Lastpass.

a. Откройте веб-браузер и перейдите по ссылке: https://lastpass.com/.

b. Щелкните **Получить LastPass Free (Get LastPass Free)**, чтобы создать пробную учетную запись.

c. Заполните поля в соответствии с инструкцией.

d. Задайте мастер-пароль. С этим паролем вы будете входить в свою учетную запись LastPass.

e. Загрузите и установите клиент LastPass для своей операционной системы.

f. Откройте клиент и войдите в него со своим мастер-паролем LastPass.

g. Изучите менеджер паролей LastPass.

Когда вы добавляете пароли в Lastpass, где они хранятся?

_____

Помимо вас, к вашим паролям имеет доступ как минимум еще одно лицо. Кто это лицо?

_____

Если все пароли хранятся в одном месте, наверняка в этом есть недостатки. Подумайте, какие?

_____

_____

_____

Часть 3: Что же тогда надежный пароль?

Опираясь на характеристики надежного пароля, приведенные в начале этой лабораторной работы, выберите пароль, который было бы легко запомнить, но трудно подобрать. Сложные пароли вполне допустимы, если только они не противоречат более важным требованиям, например возможности легко их запоминать.

При использовании менеджера паролей необходимость в легком запоминании пароля отпадает.

Итак, резюме.

Выбирайте пароль, который можете запомнить.

Выбирайте пароль, который ни у кого не будет ассоциироваться лично с вами.

Выбирайте разные пароли и никогда не используйте один и тот же пароль для разных сервисов.

Сложные пароли использовать можно, только если их будет просто запомнить..