Лабораторна робота – Створення та збереження надійних паролів

Цілі та задачі

Зрозуміти концепцію надійного пароля.

Частина 1: Дослідження концепцій створення надійного пароля.

Частина 2: Дослідження концепцій безпечного збереження паролів.

Довідкова інформація / Сценарій

Паролі широко використовуються для захисту доступу до ресурсів. Зловмисники можуть використовувати багато методів для розкриття паролів користувачів та отримання несанкціонованого доступу до ресурсів або даних.

Щоб краще захистити себе, важливо розуміти, що робить пароль надійним і як його безпечно зберігати.

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету

Частина 1: Створення надійного пароля

Надійні паролі мають відповідати вимогам, які перелічені в порядку важливості:

1) Користувач може легко запам'ятати пароль.
2) Для будь-якої іншої людини вгадати цей пароль не є тривіальною задачею.
3) Вгадати або розкрити цей пароль не є тривіальною задачею для програми.
4) Пароль має бути складним, містити цифри, символи та суміш літер у верхньому та нижньому регістрах.

Виходячи з вищезазначеного переліку, перша вимога, мабуть, є найважливішою, оскільки вам потрібно ваш пароль пам'ятати. Наприклад, пароль **#4ssFrX^-aartPOknx25_70!xAdk<d!** вважається надійним, оскільки він задовольняє останнім трьом вимогам, але його буде дуже важко запам'ятати.

Багато організацій вимагають, щоб паролі містили комбінацію цифр, символів та літер у нижньому та верхньому регістрах. Паролі, які відповідають цій політиці, вважаються підходящими, якщо вони легко запам'ятовуються. Нижче наведено приклад політики щодо вибору пароля для типової організації:

- Довжина пароля має бути мінімум 8 символів.
- Пароль повинен містити символи у верхньому і нижньому регістрах.
- Пароль має містити хоча б одну цифру.
- Пароль має містити хоча б один неалфавітний символ.

Проаналізуйте характеристики надійного пароля та загальну політику вибору паролів, наведену вище. Чому в політиці не враховуються перші два пункти? Поясніть.

_____

_____

_____

_____

_____

_____

Гарною практикою створення надійних паролів є вибір чотирьох або більше випадкових слів і їх поєднання. Пароль **televisionfrogbootschurch** надійніший ніж **J0n@than#81**. Зверніть увагу, що, хоча другий пароль відповідає описаним вище правилам, програми зламу паролів дуже ефективні при визначенні цього типу пароля. Хоча багато політик створення паролів не дозволять використання першого пароля, **televisionfrogbootschurch**, він набагато надійніший ніж другий. Користувачу простіше його запам'ятати (особливо якщо він асоціюється з зображенням), він дуже довгий і фактор випадковості ускладнює визначення такого пароля.

Використовуючи онлайн-інструмент для створення паролів, створіть паролі на основі загальної політики компанії щодо створення паролів, яка була описана вище.

a. Відкрийте веб-браузер і перейдіть на http://passwordsgenerator.net

b. Виберіть параметри, які відповідають політиці вибору пароля.

c. Згенеруйте пароль.

Чи легко запам'ятати згенерований пароль?

_____

_____

Використовуючи онлайн-інструмент для створення паролів, створіть паролі на основі випадкових слів. Зауважте, що оскільки слова з'єднані разом, вони не розглядаються як словарні слова.

d. Відкрийте веб-браузер і перейдіть на http://preshing.com/20110811/xkcd-password-generator/

e. Згенеруйте новий пароль з випадкових слів, натиснувши **Generate Another!** у верхній частині веб-сторінки.

f. Чи легко запам'ятати згенерований пароль?

_____

_____

Відповіді можуть бути різними. Але дуже ймовірно, що такий пароль буде легко запам'ятати.

Частина 2: Безпечне зберігання паролів

Якщо користувач вирішить використовувати менеджер паролів, на першу характеристику надійного пароля можна не зважати, оскільки користувач завжди має доступ до менеджера паролів. Зверніть увагу, що деякі користувачі довіряють свої паролі лише власній пам'яті. Менеджери паролів, як локальні, так і віддалені, використовують сховище паролів, яке може бути скомпрометовано.

Сховище менеджера паролів має бути надійно зашифровано, і доступ до нього має жорстко контролюватися. За допомогою програм для мобільних телефонів та веб-інтерфейсів, хмарні менеджери паролів надають своїм користувачам безперебійний доступ у будь-який час.

Популярним менеджером паролів є LastPass.

Створіть пробний обліковий запис LastPass:

a. Відкрийте веб-браузер і перейдіть на https://lastpass.com/

b. Натисніть **Start Trial** для створення пробного облікового запису.

c. Заповніть поля, як зазначено в інструкції.

d. Встановіть майстер-пароль. Цей пароль дає вам доступ до вашого облікового запису LastPass.

e. Завантажте та встановіть клієнта LastPass відповідно до своєї операційної системи.

f. Відкрийте клієнт і увійдіть до системи за допомогою майстер-пароля LastPass.

g. Дослідіть менеджер паролів LastPass.

Коли ви додаєте паролі до Lastpass, де вони зберігаються?

_____

Окрім вас, щонайменше, один інший суб'єкт має доступ до паролів. Хто цей суб'єкт?

_____

Хоча зберігати всі ваші паролі в одному місці може бути досить зручно, цей підхід має недоліки. Як ви думаєте, які це недоліки?

_____

_____

_____

Частина 3: Що тепер для вас означає надійний пароль?

Використовуючи характеристики надійного пароля, наведені на початку цієї лабораторної роботи, виберіть пароль, який легко запам'ятати, але важко вгадати. Складність паролів важлива, якщо вона не впливає на більш важливі вимоги, такі як придатність для легкого запам'ятовування.

Якщо використовується менеджер паролів, вимога до простоти запам'ятовування може бути скасована.

Нижче наведений короткий підсумок:

Обирайте пароль, який можете запам'ятати.

Обирайте пароль, який ніхто не зможе асоціювати з вами.

Обирайте різні паролі і ніколи не використовуйте один і той самий пароль для різних сервісів.

Складність паролів - це гарна практика, доки не призводить до проблем з їх запам'ятовуванням.