

ЛАБОРАТОРНАЯ РАБОТА № 1

По дисциплине: защита информации

Тема занятия: **Вскрытие паролей. Saminside**

Цель занятия: Познакомиться с программой Saminside, узнать критерии подбора пароля.
Научиться настраивать систему на безопасные пароли.

Количество часов: 2

Содержание работы:

1. Знакомство с интерфейсом Saminside. Критерии подбора пароля
2. Тест на безопасность пароля
3. Настройка системы на проверку безопасности пароля

Методические указания по выполнению:

Описание программы

Программа Saminside предназначена для восстановления паролей пользователей Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows 7.

Программа содержит свыше 10 видов импорта данных и позволяет использовать 6 видов атак для восстановления паролей пользователей:

- Атака полным перебором;
- Атака распределенным перебором;

Данный вид атаки позволяет использовать для восстановления паролей несколько компьютеров, распределение между ними обрабатываемые пароли. Этот вид атаки включается автоматически, когда пользователь устанавливает количество компьютеров, участвующих в атаке, более одного.

- Атака по маске;

Данный вид атаки используется, если есть определенная информация о пароле. Например:

- Пароль начинается с комбинации символов "12345";
- Первые 4 символа пароля – цифры, остальные – латинские буквы;
- Пароль имеет длину 10 символов и в середине пароля есть сочетание букв "admin";
- И т.д.

Настройки перебора по маске позволяют сформировать маску для перебираемых паролей, а также установить максимальную длину перебираемых паролей. Установка маски заключается в следующем – если вы не знаете N-й символ пароля, то включите N-й флагок маски и в соответствующем текстовом поле укажите маску для этого символа. Если же вы заранее знаете определенный символ пароля, то впишите его в N-е текстовое поле и снимите флагок маски.

В программе используются следующие символы маски:

- ? – Любой печатаемый символ (ASCII-коды символов 32...255).

A – Любая заглавная латинская буква (A...Z).
a – Любая строчная латинская буква (a...z).
S – Любой специальный символ (!@#...).
N – Любая цифра (0...9).
1...8 – Любой символ из соответствующего пользовательского набора символов.

– Атака по словарям;

*Словарь – это текстовый файл, состоящий из часто употребляемых паролей типа
123; admin; master; и т.д.*

– Гибридная атака;

возможность добавлять к проверяемым паролям до 2 символов справа и слева, что позволяет восстанавливать такие пароли как "master12" или "#admin".

– Атака по предварительно рассчитанным Rainbow-таблицам.

Данный вид атаки использует Rainbow-технологию (<http://project-rainbowcrack.com>) для создания предварительно рассчитанных таблиц.

Тест на безопасность пароля

1. Создать пользователя с простым паролем (напр. 5;123;asdf)

*Пуск -> Панель управления -> Учетные записи пользователей -> Создание учетной записи
Вводите имя, устанавливаете пароль*

2. Применить программу для подбора пароля saminside (какое время займет? записать)

Запустить -> Файл -> Scheduler

Устанавливаем галочку напротив учетной записи, созданной в первом пункте

Аудит -> Атака по словарям -> запуск

3. Изменить пароль на более длинный осмысленный (напр. admin; magic и т.п.) атака по словарю
4. Повторить пункт 2
5. Изменить пароль на случайный неосмысленный (напр. KG4s8DcvM5)
6. Повторить пункт 2. Ждать разумное время 3-5 мин (приступить к выполнению заданий из следующего топика)

Настройка системы на проверку безопасности пароля

1. Панель управления -> Администрирование -> Локальные параметры безопасности

- ✓ настроить мин длину пароля >8
- ✓ сложность включить

2. Попытаться изменить пароль, вводя слабый пароль (1п. предыдущего топика), убедиться, что система не позволит вводить небезопасный пароль.

Сделать выводы, убрать за собой (удалить пользователя, вернуть параметры в исходные)

Вопросы для защиты лабораторной работы:

1. Какой вид атаки отработает наиболее эффективно для каждого из далее приведенных паролей:
a) hjkl b) cat67 c) 8794 d) KG4s8DcvM5
2. Какой вид атаки необходимо применить, если известно, что пароль содержит 9 символов: шестым из которых является буква, а в седьмой и восьмой позициях находятся цифры «56»?
3. Какими параметрами должен обладать «сильный» пароль?