Лабораторная работа №1.

Изучение методики полного перебора (брутфорс).

Цель работы: сформировать практические навыки использования атаки полным перебором.

Задачи: изучить принцип атаки полным перебором. Автоматизировать атаку полным перебором на примере подбора пароля к архиву WinRAR.

Введение

Брутфорс - метод подбора пароля путем обыкновенного перебора возможных комбинаций, подобно подбору необходимого ключа к замку из связки имеющихся. Преимущество такого метода взлома - его эффективность: с определенной долей вероятности можно подобрать любой пароль. Вопрос в том, сколько времени на это понадобится. Простые пароли ломаются за часы-дни, сложные можно подбирать тысячалетиями. Однако из-за специфических аспектов человеческой психологии, а именно: природной лени человека и выбора “простых” паролей или последовательностей символов в пароле, злоумышленникам упрощается задача. Таким образом, атаки полным перебором актуальны и в настоящее время.

Данная лабораторная работа будет посвящена изучению метода полного перебора и способа его реализации.

Ход работы: необходимо написать программу, реализующую принцип атаки полным перебором на запароленом архиве WinRAR.

Синтаксис командной строки

WinRAR допускает управление из командной строки. Общий синтаксис командной строки таков:

`WinRAR <команда> -<ключ1> -<ключN> <архив> <файлы…> <@файл-список…> <путь для извлечения\>`

команда	Комбинация символов, определяющая действие, которое будет выполнять WinRAR. См. "Список команд WinRAR".
ключ	Ключи используются для определения специфических действий, степени сжатия, типа архива и пр. См. "список ключей WinRAR".
архив	Имя обрабатываемого архива.
файлы	Имена обрабатываемых файлов.
файл-список	Файлы-списки - это обычные текстовые файлы, содержащие имена файлов для обработки. Каждое имя файла должно быть указано на отдельной строке и начинаться с первой позиции строки. В файл-список допускается помещать комментарии,

	признак начала комментария - символы //. Например, для архивирования файлов *.txt из папки c:\work\doc, файлов *.bmp из папки c:\work\image и всех файлов из папки c:\work\misc можно создать backup.lst, содержащий следующие строки: c:\work\doc*.txt //резервная копия текстов c:\work\image*.bmp //резервная копия рисунков c:\work\misc После этого для архивирования достаточно будет выполнить команду: winrar a backup @backup.lst
путь для извлечения	Используется только с командами e и x и указывает папку, в которую нужно извлекать файлы. Если эта папка не существует, то она будет создана.

Примечания

а) Если не указаны ни файлы, ни файл-список, то подразумевается шаблон *.*, т.е. WinRAR обработает все файлы.

б) Если при создании архива не указано его расширение, то WinRAR будет использовать формат архива по умолчанию, выбранный в профиле архивации по умолчанию, но если вы хотите указать тип архива явно, то это можно сделать добавлением расширения .rar или .zip к имени архива.

Если при распаковке архива не указано его расширение, то WinRAR считает, что это архив .rar, т.е. маска '*' (без кавычек) означает все архивы с расширением .rar. Если требуется обработать все архивы, не имеющие в имени расширения, то нужно использовать маску '*.' (без кавычек). Маска *.* выбирает все файлы. Символы подстановки (шаблоны) можно использовать в большинстве операций, таких как извлечение, тестирование и многих других, однако при архивировании и удалении шаблоны запрещены.

в) Ключи, введённые в командной строке, имеют более высокий приоритет, чем соответствующие установки в диалоговом окне конфигурации, т.е. используются параметры, заданные ключами.

г) Для команд **C, E, S, T, RR, K** и **X** в имени архива допускается использовать шаблоны, поэтому одной командой можно обработать сразу нескольких архивов. Более того, если вместе с этими командами указать ключ **-r**, то поиск архивов будет вестись и во всех вложенных папках.

д) Некоторые команды и ключи применимы только к архивам RAR, некоторые — к архивам RAR и ZIP, а некоторые — к архивам всех поддерживаемых форматов. Это зависит от возможностей, заложенных в формат архива.

е) Команды и ключи не зависят от регистра символов, поэтому вы можете набирать их как строчными, так и прописными буквами.

ж) Если какой-либо компонент командной строки содержит пробелы, он должен быть заключён в двойные кавычки.

Примеры
Добавить папку "c:\latest data" в архив Info.rar
WinRAR a Info.rar "c:\latest data"

Распаковать архив Info.rar в папку d:\data
WinRAR x Info.rar d:\data\

Список команд

A	Добавить файлы в архив
C	Добавить архивный комментарий
CH	Изменить параметры архива
CV	Преобразовать архивы
CW	Записать в файл комментарий архива
D	Удалить файлы из архива
E	Извлечь файлы из архива, игнорируя пути
F	Освежить имеющиеся файлы в архиве
I	Найти строку в архивах
K	Заблокировать архив
M	Переместить файлы и папки в архив
R	Восстановить повреждённый архив
RC	Воссоздать недостающие тома
RN	Переименовать файлы в архиве
RR[N]	Добавить информацию для восстановления
RV[N]	Создать тома для восстановления
S[имя]	Преобразовать архив в самораспаковывающийся
S-	Удалить SFX-модуль
T	Протестировать файлы в архиве
U	Обновить файлы в архиве
X	Извлечь файлы из архива с полными путями

Список ключей

--	Прервать дальнейший поиск ключей в командной строке
-@[+]	Запретить [разрешить] списки файлов
-ac	Снять атрибут "Архивный" после архивации или извлечения
-ad	Добавить к пути назначения имя архива
-af<тип>	Указать формат архива
-ag [формат]	Добавить к имени архива текущую дату и время
-ai	Игнорировать файловые атрибуты
-ao	Добавить файлы с установленным атрибутом "Архивный"
-ap<путь>	Установить путь внутри архива
-as	Синхронизировать содержимое архива
-av	Добавить электронную подпись
-av-	Запретить добавление/проверку электронной подписи
-cfg-	Игнорировать профиль по умолчанию и переменную окружения
-cl	Преобразовать имена файлов в нижний регистр
-cp<имя>	Выбрать профиль упаковки
-cu	Преобразовать имена файлов в верхний регистр
-df	Удалить файлы после архивации
-dh	Открывать совместно используемые файлы
-dr	Удалить файлы в Корзину
-ds	Не сортировать файлы при архивации
-dw	Уничтожить (затереть) файлы после архивации
-ed	Не добавлять пустые папки
-en	Не добавлять блок "Конец архива"
-ep	Исключить пути из имён
-ep1	Исключить из пути базовую папку
-ep2	Сохранять полные пути файлов
-ep3	Сохранять полные пути, включая букву диска
-e[+]<атр>	Задать исключение или включение файлов из/в обработку по маске атрибутов
-f	Освежить имеющиеся файлы
-hp[пароль]	Шифровать и данные, и заголовки файлов
-iadm	Запрашивать административный доступ для SFX-архива
-ibck	Запустить WinRAR как фоновый процесс в системном лотке
-	Отправить архив по электронной почте

ieml[.][адрес]	
-iicon<имя>	Указать значок для SFX-модуля
-iimg<имя>	Указать логотип для SFX-модуля
-ilog[имя]	Записывать протокол ошибок в файл
-inul	Не выводить сообщения об ошибках
-ioff	Выключить компьютер
-k	Заблокировать архив
-kb	Сохранять на диске файлы, извлечённые с ошибками
-log[формат][=имя]	Записывать имена в файл-протокол
-m<n>	Установить метод сжатия
-mc<параметры>	Указать дополнительные параметры сжатия
-md<n>	Установить размер словаря
-ms[список]	Указать типы файлов для архивирования без сжатия
-mt<потоки>	Установить число потоков
-n<файл>	Включить в обработку только указанный файл
-n@<файл-список>	Включить в обработку только файлы, указанные в файле-списке
-oc	Установить NTFS-атрибут "Сжатый"
-or	Переименовывать файлы автоматически
-os	Сохранить потоки NTFS
-ow	Обработать информацию о правах доступа к файлам
-o[+,-]	Установить режим перезаписи
-p[пароль]	Установить пароль
-r	Обрабатывать вложенные папки
-r-	Запретить рекурсию (обработку вложенных папок)

-r0	Обрабатывать вложенные папки только по шаблону
-ri	Установить приоритет и время простоя
-rr[N]	Добавить информацию для восстановления
-rv[N]	Создать тома для восстановления
-s	Создать непрерывный архив
-s<N>	Создать непрерывные группы, используя счётчик файлов
-sc<набор символов>[объекты]	Указать набор символов (и объекты)
-se	Создать непрерывные группы, используя расширения файлов
-sfx[имя]	Создать самораспаковывающийся архив
-sl<размер>	Обрабатывать файлы размером меньше указанного
-sm<размер>	Обрабатывать файлы размером больше указанного
-sv	Создать независимые непрерывные тома
-sv-	Создать зависимые непрерывные тома
-s-	Запретить создание непрерывных архивов
-t	Протестировать файлы после архивирования
-ta<дата>	Обрабатывать файлы, изменённые после указанной даты
-tb<дата>	Обрабатывать файлы, изменённые до указанной даты
-tk	Сохранять исходное время архива
-tl	Установить время архива по самому новому файлу
-tn<время>	Обрабатывать файлы не старее, чем указанный период времени
-to<время>	Обрабатывать файлы более старые, чем указанный период времени
-ts<m,c,a>	Сохранить/восстановить время файлов (модификации, создания, последнего доступа)
-u	Обновить файлы
-v<n>[k,b,f,m,M,g,G]	Создать многотомный архив
-vd	Очищать сменный диск перед архивацией на него

-ver[n]	Управление версиями файлов
-vn	Использовать старую схему именования томов
-vp	Делать паузу перед каждым томом
-w<путь>	Задать папку для временных файлов
-x<файл>	Не обрабатывать указанный файл
-x@<файл-список>	Не обрабатывать файлы, указанные в файле-списке
-y	Подразумевать ответ "Да" на все запросы
-z<файл>	Прочитать комментарий архива из файла

Коды возврата WinRAR

В случае успешного окончания операции WinRAR завершает работу с нулевым (0) кодом возврата. Если код возврата отличается от нулевого, это говорит о том, что произошла какая-то ошибка.

Код возврата	**Описание**
0	Операция успешно завершена.
1	Предупреждение. Произошли некритические ошибки.
2	Произошла критическая ошибка.
3	Неверная контрольная сумма CRC32. Данные повреждены.
4	Предпринята попытка изменить заблокированный архив.
5	Произошла ошибка записи на диск.
6	Произошла ошибка открытия файла.
7	Ошибка при указании параметра в командной строке.
8	Недостаточно памяти для выполнения операции.
9	Ошибка при создании файла.
10	Нет файлов, удовлетворяющих указанной маске, и параметров.
255	Операция была прервана пользователем.

Задание.

1) Создать архив WinRAR с численным паролем
   - максимальная длина пароля – 4 цифры
   - пароль может состоять из нулей (0000)

2) Разработать программу, подбирающую пароль к архиву путем полного перебора и извлекающую содержимое запароленного архива.

3) После успешного подбора пароля программа должна :
   - остановить выполнение (не проверять дальнейшие комбинации)
   - вывести пароль пользователю

Отчет должен содержать:

- Текстовое описание хода выполнения работы (используемые механизмы, внешние программы, ключи и т.д.)
- Исходный код программы
- Скриншоты работы программы