МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,

СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»

(СПбГУТ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет инфокоммуникационных сетей и систем

Кафедра защищенных систем связи

Дисциплина Безопасность компьютерных сетей

ЛАБОРАТОРНАЯ РАБОТА №2

Шифрование и расшифровка данных с помощью хакерских инструментов

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

Студент:

Громов А. А., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Проверил:

Ушаков И. А.

Лабораторная работа. Шифрование и расшифровка данных с помощью хакерских инструментов

Задачи

Часть 1. Создание и шифрование файлов

Часть 2. Восстановление паролей зашифрованного ZIP-файла

1. Общие сведения и сценарий

Что делать, если вы работаете в крупной корпорации, в которой действует корпоративная политика относительно съемных носителей? В частности, указано, что только зашифрованные ZIP-документы можно скопировать на портативные USB-накопители.

В этом сценарии финансовый директор уехал из города в командировку и связался с вами, запросив неотложную помощь. Будучи в командировке вне города, он попытался распаковать важные документы из зашифрованного ZIP-файла на USB-накопителе. Однако пароль, предоставленный для открытия ZIP-файл, недействителен. Финансовый директор связался с вами, чтобы выяснить, можете ли вы что-то сделать в этой ситуации.

**Примечание**. Предоставленный сценарий простой и служит только в качестве примера.

Иногда доступны инструменты для восстановления потерянных паролей. Это особенно верно в ситуациях, аналогичных описанной, когда аналитик по кибербезопасности может получить полезные сведения от финансового директора, например о длине пароля и представление о том, каким он может быть. Знание соответствующей информации значительно облегчает попытки восстановления паролей.

Среди программ для восстановления паролей ― hashcat, John the Ripper, Lophtcrack и другие. В нашем случае мы будем использовать **fcrackzip** — это простая служебная программа Linux для восстановления паролей зашифрованных ZIP-файлов.

Помните, что эти же инструменты могут быть использованы киберпреступниками для обнаружения неизвестных паролей. Хотя у них нет доступа к некоторым полезным сведениям, затратив некоторое время, можно обнаружить пароли для открытия зашифрованных ZIP-файлов. Количество затрачиваемого времени зависит от сложности и длины пароля. Более длинные и более сложные пароли (сочетание различных типов символов) более надежны.

В этой лабораторной работе вам предстоит:

* создать и зашифровать образцы текстовых файлов;
* расшифровать зашифрованный ZIP-файл.

**Примечание**. Эту лабораторную работу следует использовать только в учебных целях. Методы, представленные здесь, НЕ должны использоваться для защиты действительно конфиденциальных данных.

1. Необходимые ресурсы

* Виртуальная машина рабочей станции CyberOps
* Доступ к Интернету

1. Создание и шифрование файлов

В этой части лабораторной работы вы создадите несколько текстовых файлов, которые будут использоваться для создания зашифрованных ZIP-файлов на следующем шаге.

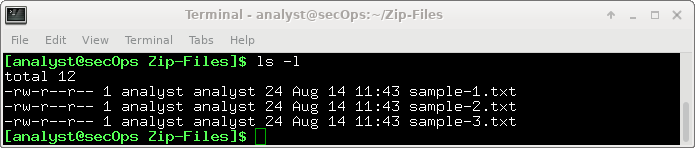
* 1. Создание текстовых файлов.
     1. Запустите виртуальную машину рабочей станции CyberOps.
     2. Откройте окно терминала. Убедитесь, что вы находитесь в главном каталоге analyst. В противном случае введите **cd ~** в командной строке терминала.
     3. Создайте новую папку с именем Zip-Files, используя команду **mkdir Zip-Files**.
     4. Перейдите в этот каталог, используя команду **cd Zip-Files**.
     5. Введите следующие команды для создания трех текстовых файлов.

[analyst@secOps Zip-Files]$ **echo Это образец текстового файла > sample-1.txt**

[analyst@secOps Zip-Files]$ **echo Это образец текстового файла > sample-2.txt**

[analyst@secOps Zip-Files]$ **echo Это образец текстового файла > sample-3.txt**

* + 1. Убедитесь, что файлы созданы, с помощью команды **ls**.



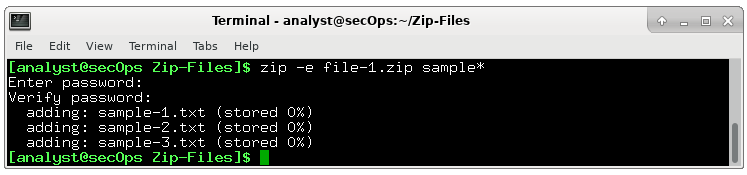
* 1. Запакуйте в архив и зашифруйте текстовые файлы.

Затем мы создадим несколько зашифрованных ZIP-файлов с использованием паролей различной длины. Для этого все три текстовых файла будут зашифрованы с помощью служебной программы **zip**.

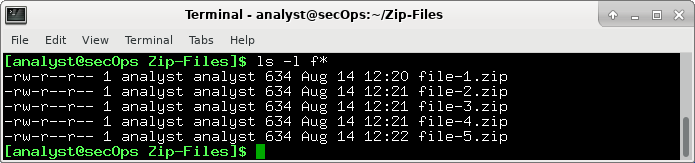
* + 1. Создайте зашифрованный ZIP-файл с именем **file-1.zip**, содержащий три текстовых файла с помощью следующей команды:

[analyst@secOps Zip-Files]$ **zip –e file-1.zip sample\***

* + 1. При появлении запроса пароля введите односимвольный пароль по своему выбору. В этом примере введена буква **B**. Введите ту же букву при появлении запроса подтверждения.

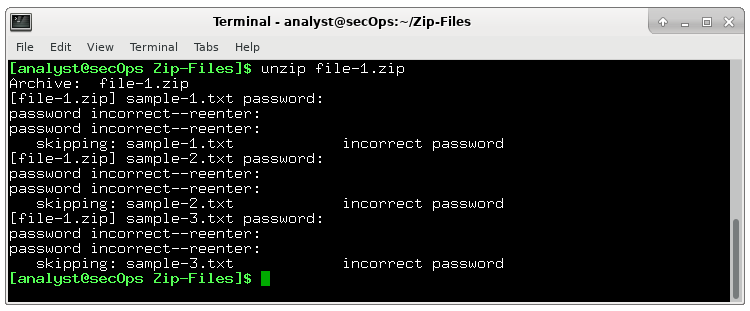


* + 1. Повторите процедуру для создания 4 других файлов
* **file-2.zip** с двухсимвольным паролем по вашему выбору. В нашем примере используется **R2**.
* **file-3.zip** стрехсимвольным паролем по вашему выбору. В нашем примере используется **0B1**.
* **file-4.zip** с 4-символьным паролем по вашему выбору. В нашем примере используется **Y0Da**.
* **file-5.zip** с 5-символьным паролем по вашему выбору. В нашем примере используется **C-3P0**.
  + 1. Убедитесь, что все ZIP-файлы были созданы с помощью команды **ls -l f\***.



* + 1. Попробуйте открыть zip-файл с помощью неверного пароля, как показано.

[analyst@secOps Zip-Files]$ **unzip file-1.zip**

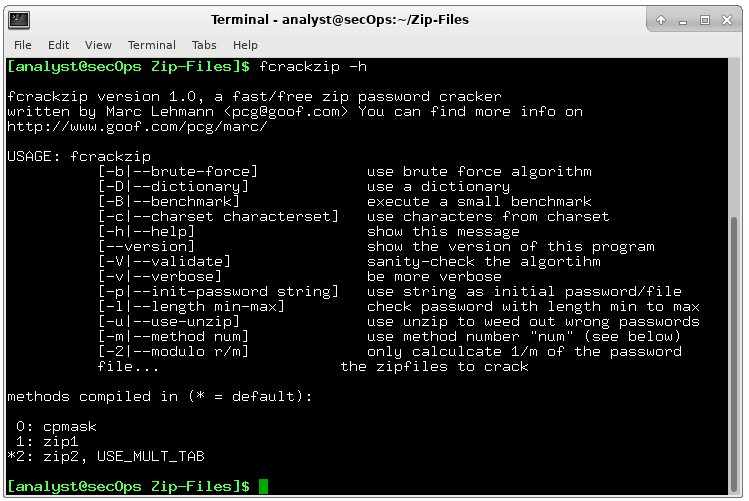


1. Восстановление паролей зашифрованных ZIP-файлов

В этой части лабораторной работы потерянные пароли из зашифрованных ZIP-файлов будут восстановлены с помощью служебной программы **fcrackzip**. Fcrackzip выполняет поиск в каждом ZIP-файле, предоставленном для зашифрованных файлов, и пытается угадать пароль методом полного перебора.

ZIP-файлы с паролями различной длины были созданы, чтобы выяснить, как длина пароля влияет на время, необходимое, чтобы раскрыть пароль.

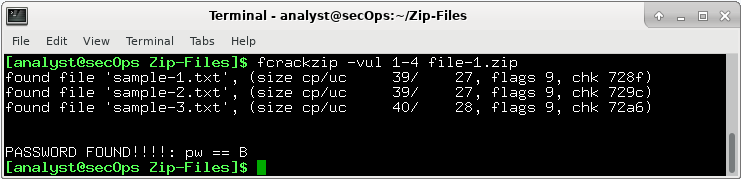
* 1. Введение в fcrackzip
     1. В окне терминала введите команду **fcrackzip –h** для просмотра соответствующих параметров команды.

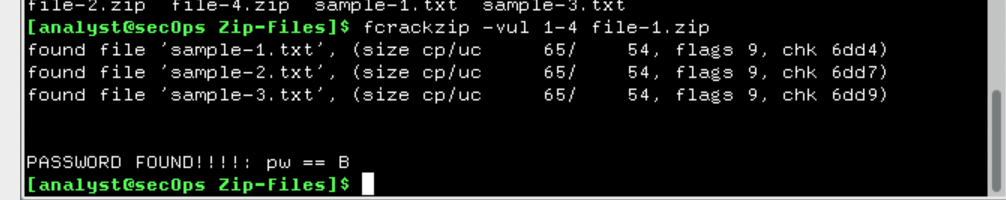


В наших примерах будут использованы параметры команды **–v-u** и **-l**. Параметр -l будет указан последним, потому что он задает длину пароля. Вы можете поэкспериментировать с другими параметрами.

* 1. Восстановление паролей с помощью fcrackzip
     1. Теперь попытайтесь восстановить пароль файла **file-1.zip**. Напоминаем, что он был зашифрован с использованием пароля длиной в один символ. Поэтому используйте следующую команду **fcrackzip**:

[analyst@secOps Zip-Files]$ **fcrackzip -vul 1-4 file-1.zip**



****

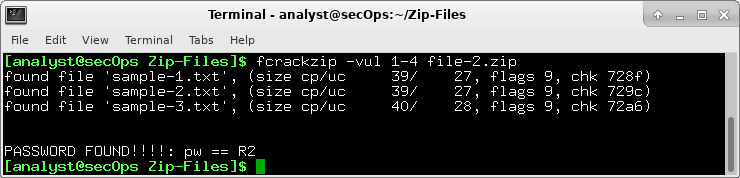
**Примечание**. Возможно, была задана длина пароля менее 1–4 символов.

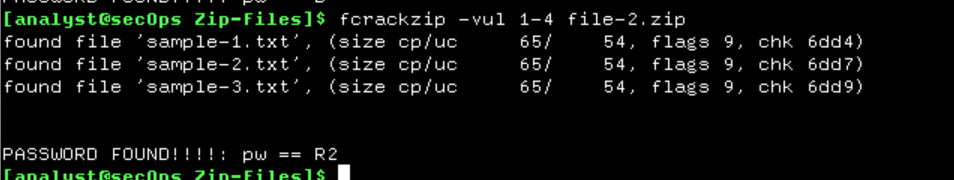
Сколько времени требуется для раскрытия пароля?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Теперь попытайтесь восстановить пароль файла **file-2.zip**. Напоминаем, что для шифрования использовался двухсимвольный пароль. Поэтому используйте следующую команду **fcrackzip**:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-2.zip**



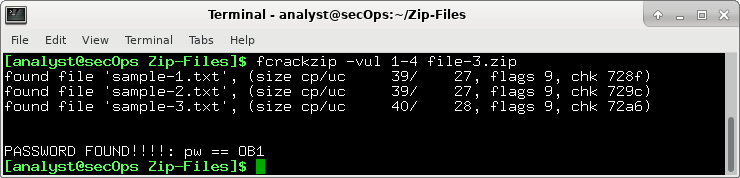
****

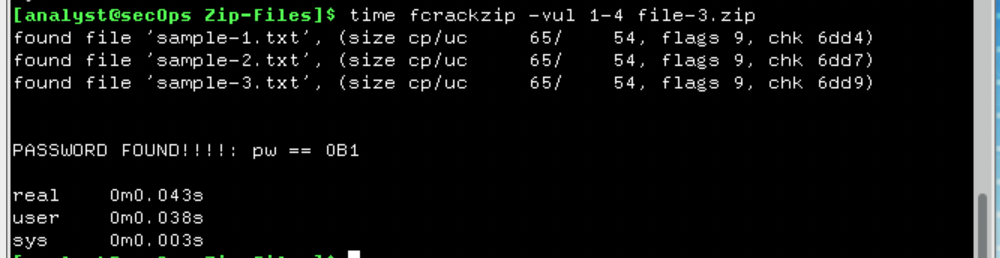
Сколько времени требуется для раскрытия пароля?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Повторите процедуру и восстановите пароль файла **file-3.zip**. Напоминаем, что для шифрования использовался трехсимвольный пароль. Измерьте время, чтобы выяснить, как долго происходит раскрытие трехсимвольного пароля. Используйте следующую команду **fcrackzip**:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-3.zip**



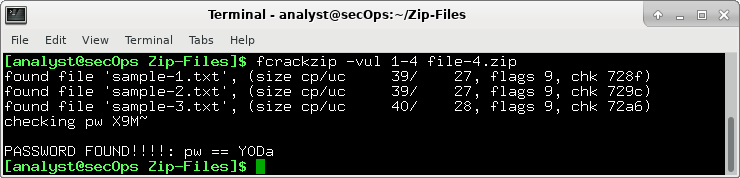
****

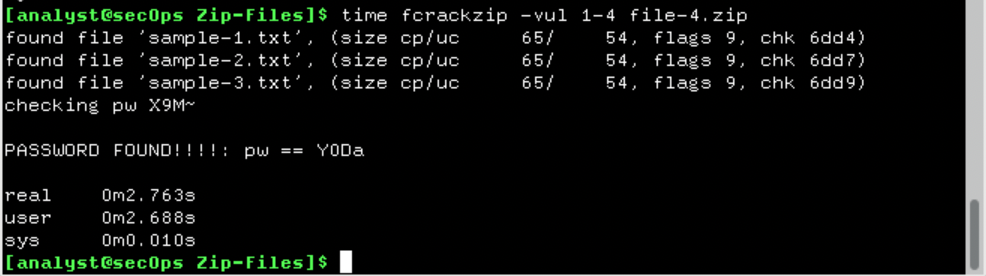
Сколько времени требуется для раскрытия пароля?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Сколько времени требуется для взлома паролей из четырех символов? Повторите процедуру и восстановите пароль файла **file-4.zip**. Измерьте время, чтобы выяснить, как долго происходит раскрытие пароля с помощью следующей команды **fcrackzip**:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-4.zip**



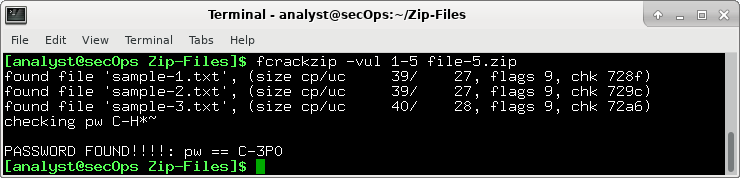
****

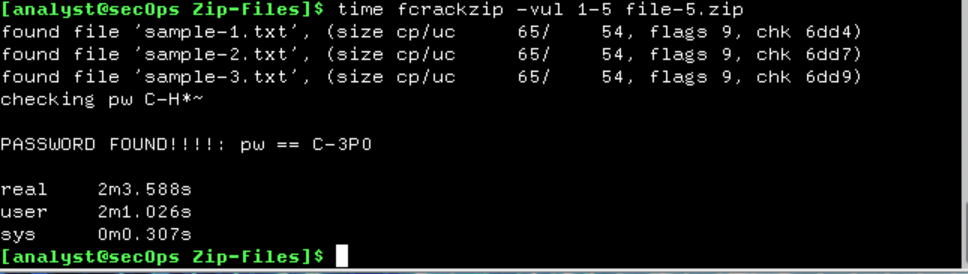
Сколько времени требуется для раскрытия пароля?

0m2s

* + 1. Сколько времени требуется для взлома паролей из пяти символов? Повторите процедуру и восстановите пароль файла **file-5.zip**. Длина пароля составляет 5 символов, поэтому необходимо назначить параметру команды **-l** значение **1-5**. Еще раз узнаем, сколько времени займет обнаружение пароля с помощью следующей команды **fcrackzip**:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-5 file-5.zip**



****

Сколько времени требуется для раскрытия пароля?

2m 1s

* + 1. Восстановите 6-символьный пароль с помощью команды fcrackzip

Похоже, для раскрытия более длинных паролей требуется больше времени, поэтому они оказываются более безопасными. Однако 6-символьный пароль не отпугнет киберпреступника.

Как вы считаете, сколько времени потребуется для раскрытия 6-символьного пароля с помощью fcrackzip?

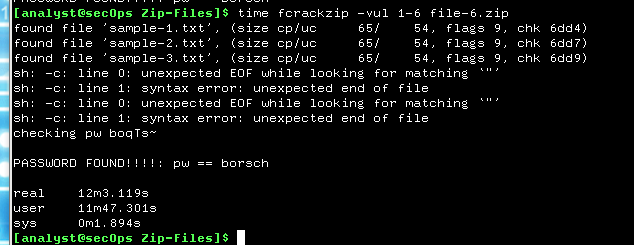
Много

Для того чтобы ответить на этот вопрос, создайте файл с именем **file-6.zip** с использованием 6-символьного пароля по своему выбору. В нашем примере использован **JarJar**.

[analyst@secOps Zip-Files]$ **zip –e file-6.zip sample\***

* + 1. Повторите процедуру, чтобы восстановить пароль файла **file-6.zip** с использованием следующей команды **fcrackzip**:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-6 file-6.zip**



Сколько времени требуется для раскрытия пароля с помощью fcrackzip?

12m 3sec

Простая истина заключается в том, что более длинные пароли более надежны, так как требуется больше времени, чтобы их раскрыть.

Какую длину вы рекомендуете для надежного пароля?

От 8ми символов в длину (с использованием заглавных и прописных букв, цифр, спец. символов)