# Дисциплина «Защита информации»

# Лабораторная работа № 1

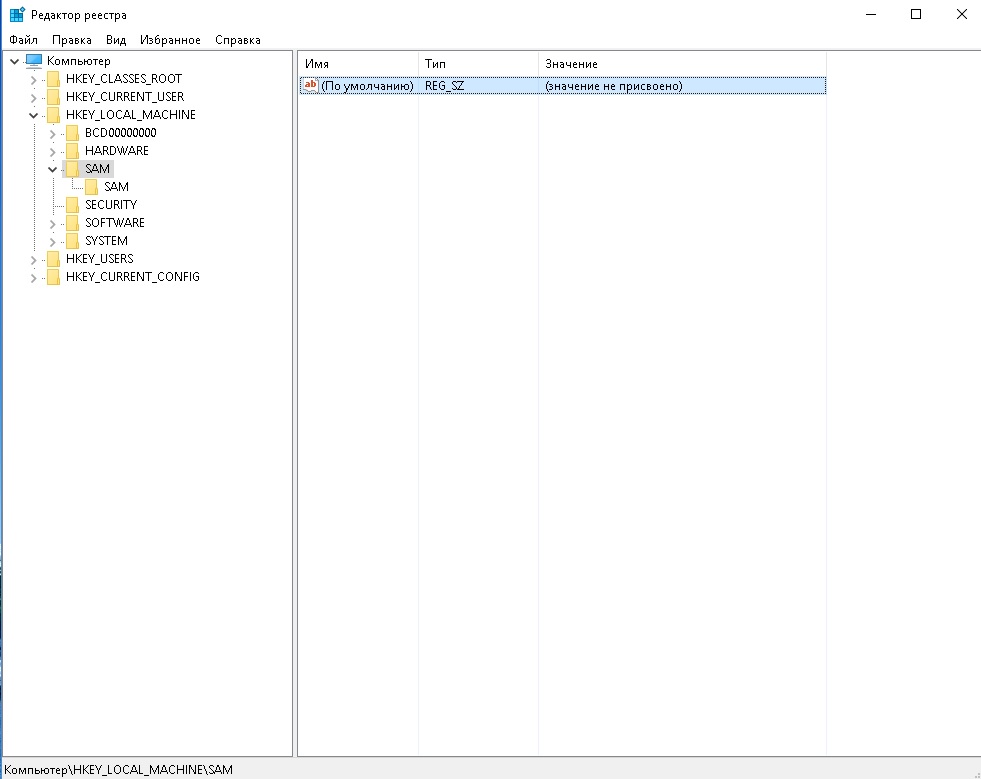
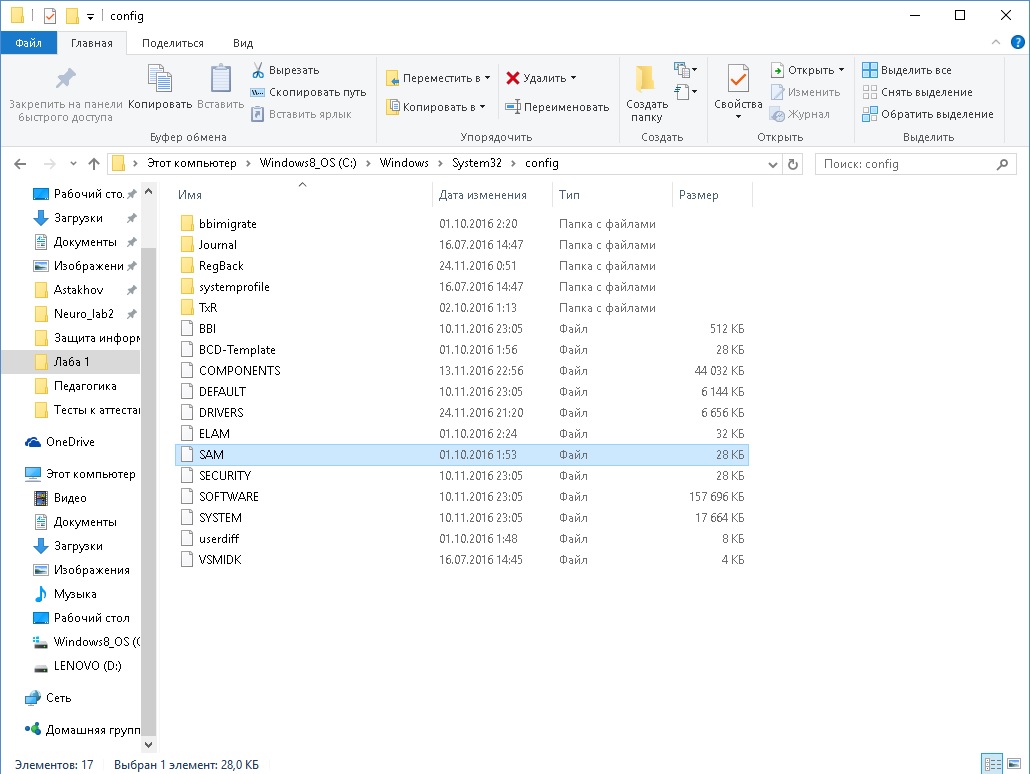
**Восстановление паролей в Windows XP**

# Теоретическое введение

## База данных SAM

Сведения об учетных записях (пара- имя пользователя =login+пароль в зашифрованном виде ) хранятся в БД SAM ( Security Account Manager - диспетчер защиты учетных записей). Если Windows NT/2000/XP/2003/Vista/7 является контроллером домена, то в БД SAM будут хранится все пароли домена.

БД SAM хранится в ветке реестра HKEY\_LOCAL\_MACHINE\SAM\. Т.к. все ветки реестра в Windows NT/2000/XP/2003/Vista/7 хранятся в системном каталоге Windows , в папке \System32\Config в нескольких файлах, то и эта ветка - не исключение. Она располагается в файле SAM (без расширений).



Пока Windows NT/2000/XP/2003/Vista загружена и работает, файл SAM недоступен для чтения никому, даже пользователю с правами Администратора , потому что он постоянно открыт ОС для того, чтобы изменения в нем сразу становились доступными , без перезагрузки. В Windows 95/98/Me реестр хранился в файлах system.dat и user.dat , которые загружались однократно при загрузке системы. Поэтому для внесения изменений в реестр требовалась перезагрузка.

## LM и NT хеши

Пароли в Windows NT/2000/XP/2003/Vista хранятся в виде хэшей. ( в зашифрованном виде ). Приче каждый пароль хранится в двух вариантах - в двух 16-байтовых хэшах, образуемых по разным алгоритмам. Сделано это в целях обратной совместимости. Первый алгоритм -

так наз. LM-hash, это устаревший алгоритм , существующий для совместимости с аутентификацией в сетях LAN Manager(Windows 95/98/Me ). Второй алгоритм - NT-hash , это значительно более совершенный алгоритм , специально созданный для Win NT.

Обычно хранятся оба хэша - LM-hash и NT-hash. Однако в нек. случаях ОС вычисляет только один из них. Например, если пароль содержит более 14 символов, то в БД SAM будет занесен только NT-hash . Если пользователь домена Windows NT/2000/XP/2003 / Vista изменит свой пароль , работая на ПК с Windows for Workgroups, то в его учетной записи останется только пароль Lan Manager (LM-hash). Алгоритмы формирования этих хэшей следующие.

**Формирование LM-hash**

1. Пароль преобразуется в ВЕРХНИЙ регистр и дополняется до длины 14 байт нулями.

2. Полученная строка делится на 2 половики по 7 байт, каждая из которых по отдельности шифруется алгоритмом DES, на выходе которого получается 8-байтовый хэш. В целом получается один хэш длиной 16 байт.

3. Полученный хэш вновь шифруется алгоритмом DES, но в качестве ключа используется RID (идентификатор пользователя).Это необходимо, чтобы два пользователя с одинаковыми паролями имели разные хэши.ВСЕ пользователи имеют РАЗНЫЕ RID -ы ( RID администратора == 500, Guest ==501, а все остальные получают последовательно RID== 1000,1001,1002 и т.д.).

### Формирование NT-hash

1. Пароль преобразуется в UNICODE - строку.

2. Генерируется хэш на основе данной строки с использованием алгоритма MD4.

3. Полученный хэш шифруется алгоритмом DES, причем в качестве ключа используется RID пользователя.

### Программа Syskey

Для повышения безопасности хранения паролей, начиная с Wil1dows NT с Service Pack 3 (и во всех последующих ­ОС, вплоть до Windows .Vista), полученные хеши Дополнительно шифруются еще одним алrоритмом с помощью утилиты syskey. Те. к вышеописанным алrоритмам добавляется еще 4­й шаr ­ - получение с помощью syskey нового хеша от хеша, полученнoro на шаrе 3.

SYSKEY может использовaться в одном из трех вариантов:

1) сrенерированный ключ запуска записывается на локальный жесткий диск в реестр в зашифрованном виде;

2) для получения ключа запуска берется пароль, выбранный администратором и вводимый во время загрузки операционной системы;

3) сrенерированный ключ запуска записывается на дискету. которая должна быть вставлена во вреwя заrрузки операционной системы.

По умолчанию используется первый вариант (хранение кл юча запуска в реестре). Служебная nporpaммa SYSKEY в операционной системе Windows NT для дополнительной защиты паролей учетных записей после установки Se­vice Pack соответствующей версии должна быть активирована вручную. В операционных системах Windows 2000/ХР/20ОЗIVistа nporpaмма SYSKEY изначально присутствует и активизирована.

### Определение сложного пароля

Неформально простой пароль – такой, который можно восстановить быстро, т.е. за 15 с- 15 мин на «среднем», «типовом» ПК, ноутбуке. Если программа не позволяет быстро восстановить пароль, то он называется сложным.

По Microsoft сложный пароль должен удовлетворять как минимум трем условиям :

1. Количество используемых символов. Длина пароля больше или равна 7. Пароль, состоящий из 20 символов значительно сложнее подобрать, чем пароль, состоящий из 5 символов.

2. Использование нескольких групп символов, а именно:

2.1.) Большие и малые (заглавных и прописных) буквы ЛАТИНСКОГО алфавита- A..Z,a..z.

2.2) Использование цифр 0..9

2.3) Использование знаков препинания И специальных символов (\*&@#%^)

2.4)\* Большие и малые (заглавных и прописных) буквы РУССКОГО алфавита- А..Я,а..я.

3. Запрещается использование:

3.1. личной информации : ФИО студента, родителей, бабушки,дедушки , год рождения, любимая марка сигарет, автомобиля, любимые книги , авторы и т.п.

3.2. нецензурной ( обсценной) лексики. По сведениям журнала Хакер такие пароли составляют прибл 25% в русском секторе Интернета.

3.3. паролей вида : 12345, йцукен, qwerty, пароль, password, student, teacher, gamer и.т.п. Т.е. входящих списки САМЫХ ПОПУЛЯРНЫХ паролей вида: TOP100,TOP1000 и т.п.

Пароль НЕ удовлетворяющий хотя бы трем условиям можно назвать простым.

## Режимы работы программ "восстановление паролей"

1. При атаке по словарю последовательно вычисляются хэш-значения для каждого из слов словаря или модификаций слов словаря и сравниваются с хэш-значениями паролей каждого из пользователей. При совпадении хэш-значений пароль найден. Преимущество метода - его высокая скорость. Недостатком является то, что таким образом могут быть найдены только очень простые пароли, которые имеются в словаре или являются модификациями слов словаря. Успех реализации данной атаки напрямую зависит от качества и объема используемого словаря (несложно отыскать подобные готовые словари в Интернете).

2. Последовательный перебор всех возможных комбинаций (brute force (англ.) - грубая сила, решение "в лоб") использует набор символов и вычисляет хэш-значение для каждого возможного пароля, составленного из этих символов. При использовании этого метода пароль всегда будет определен, если составляющие его символы присутствуют в выбранном наборе. Единственный недостаток этого метода - большое количество времени, которое может потребоваться на определение пароля. Чем большее количество символов (букв разного регистра, цифр, спецсимволов) содержится в выбранном наборе, тем больше времени может пройти, пока перебор комбинаций не закончится.

3. При восстановлении паролей гибридом атаки по словарю и последовательного перебора к каждому слову или модификации слова словаря добавляются символы справа и/или слева (123parol). Помимо этого может осуществляться проверка использования: имен пользователей в качестве паролей; повторения слов (dogdog); обратного порядка символов слова (elpoep); транслитерации букв (parol); замену букв кириллицы латинской раскладкой (gfhjkm).

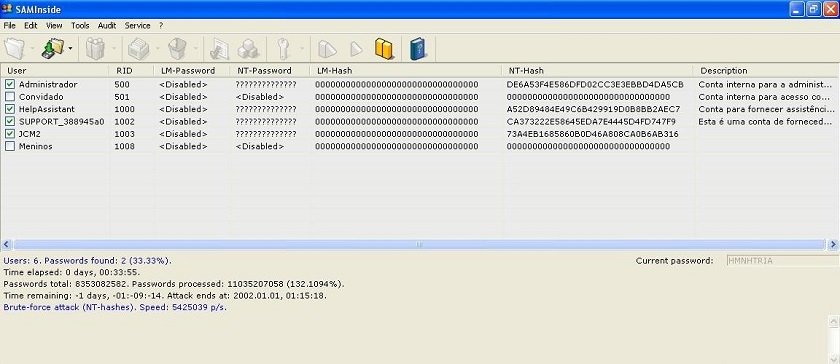
4. Метод маски . Если известно, что на конкретном месте в пароле стоят символы из конкретной группы, то это обычно ускоряет перебор как минимум на ПОРЯДОК ( в 10 раз) для одного известного символа.

5. Радужный метод. Состоит в изпользовании готовой таблицы/ БД хэшей. (метод обратного индекса в БД). Недостаток метода – БД хэшей имеют размеры порядка ГИГАбайт,

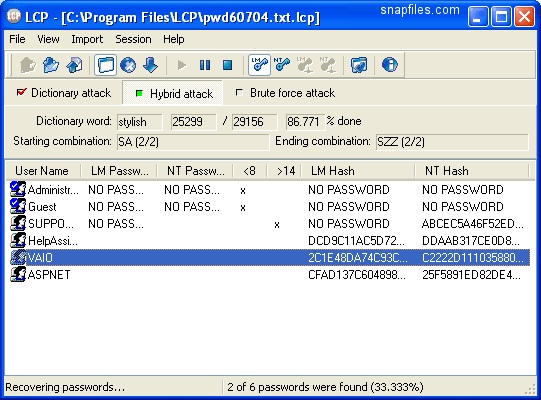
# Практические задания

1. Установить виртуальную машину с Windows NT/2000/XP.
2. Скачать одну из программ для восстановления паролей.(например Cain & Abel) или взять в директории 1-й лабораторной работы.
3. Практически определить параметры пароля, который восстанавливается этими программами за практически приемлемое время. - например 5-15 минут.
4. На основании формулы геометрической прогресии или формулы Андерсона привести примеры паролей которые будут восстанавливаться 1час- 1 сутки-1 неделю- 1 месяц-1 год.
5. Сделать выводы. Оформить лабораторную работу.

### Пример выполнения практической части



Восстановление паролей в SamInside



Восстановление паролей в LCP

Пароль: hm.87631

H=8\* =8\* =52,8 бита

Сложность пароля: 52,8 бита.

Формула Андерсона:

T== 

где V-скорость перебора паролей в секунду.

Т=14,5 лет.

# Контрольные вопросы

1. Объясните в каком виде хранятся пароли в Windows XP. Что такое LM NT - хэши. Зачем нужна утилита syskey.

2. 4 основных режима программ для восстановления паролей. Их ++ и --.

3. Что такое условно простой/сложный пароль по Майкрософт?

4 Что такое подсоленный пароль?

**Литература.**

1. Скляров. Хакерские фишки.

2. Xaker.ru

3. Алферов, Зубов, Кузьмин, Черемушкин. Основы криптографии.2-е изд.М.Гелиос.2002 г.

4. Википедия.