ФЕДЕРАЛЬНОЕ АГЕНТСТВО ОБРАЗОВАНИЯ

ДИМИТРОВГРАДСКИЙ ИНСТИТУТ ТЕХНОЛОГИЙ,

УПРАВЛЕНИЯ И ДИЗАЙНА

Лабораторная работа №7
по курсу: “Методы и средства защиты информации”
“Основы безопасности в Windows 2000/XP”

Выполнил студент гр. ВТ-41:
Потеренко А.Г.
Проверил преподаватель:
Петлинский В.П.

Димитровград 2006г.

1. Пароли в Windows 2000/XP

Несомненно, самым главным аспектом при анализе безопасности Windows 2000/XP является сохранность паролей учетных записей с правами Администратора, т.к. знание пароля позволяет получить полный доступ к этому компьютеру как локально, так и по сети, поэтому мы начнем с описания того, как Windows 2000/XP работает с паролями на вход в систему (сразу же уточним, что практически все нижесказанное относится и к ОС Windows 2003).

1.1. Хранение паролей в Windows 2000/XP

Информация об учетных записях пользователей хранится в ветке "HKEY_LOCAL_MACHINE\SAM" (SAM - Security Account Manager) реестра. А так как в Windows 2000/XP все ветки реестра "физически" расположены на диске в каталоге %SystemRoot%\System32\Config в нескольких файлах, то и эта ветка - не исключение. Она располагается в файле SAM. Отметим, что этот файл по умолчанию недоступен для чтения никому, даже Администратору, но все-таки к нему можно получить доступ. К файлу SAM (а также к остальным файлам без расширений в этой директории - system, software и др.) нет доступа по той причине, что Windows 2000/XP используют реестр "на лету" - т.е. при внесении в реестр изменений они становятся доступны сразу же и перезагрузка компьютера не требуется, но для этого системе нужно иметь монопольный доступ к файлам реестра. Напомним, что в операционных системах Windows 95/98/ME реестр хранится в файлах system.dat и user.dat, которые загружаются однократно при загрузке системы и при изменениях в реестре требуется перезагрузка компьютера для того, чтобы эти изменения вступили в силу.

Windows 2000/XP хранит пароли пользователей не в "явном" виде, а в виде хэшей (hash), т.е. фактически в виде "контрольных сумм" паролей. Рассмотрим хранение паролей пользователей подробнее. Среди сложной структуры SAM-файла нам интересна структура, называемая V-блок. Она имеет размер 32 байта и содержит в себе хэш пароля для локального входа - NT Hash длиной 16 байт, а также хэш, используемый при аутентификации доступа к общим ресурсам других компьютеров - LanMan Hash или просто LM Hash, длиной также 16 байт. Алгоритмы формирования этих хэшей следующие:

Формирование NT Hash:

- Пароль пользователя преобразуется в Unicode-строку.
- Генерируется хэш на основе данной строки с использованием алгоритма MD4.
- Полученный хэш шифруется алгоритмом DES, причем в качестве ключа используется RID (т.е. идентификатор пользователя). Это необходимо для того, чтобы два пользователя с одинаковыми паролями имели разные хэши. Напомним, что все пользователи имеют разные RID-ы (RID встроенной учетной записи Администратора равен 500, встроенной учетной записи Гостя равен 501, а все остальные пользователи последовательно получают RID-ы, равные 1000, 1001, 1002 и т.д.).

Формирование LM Hash:

- Пароль пользователя преобразуется в верхний регистр и дополняется нулями до длины 14 байт.
- Полученная строка делится на две половинки по 7 байт и каждая из них по отдельности шифруется алгоритмом DES, на выходе которого получаем 8-байтный хэш - в сумме же имеем один хэш длиной 16 байт.
- Далее LM Hash дополнительно шифруется так же, как и в шаге 3 формирования NT Hash.

Для повышения безопасности хранения паролей, начиная с 3-го Service Pack'a в Windows NT (и во всех последующих NT-системах, вплоть до Windows 2003), полученные хэши дополнительно шифруются еще одним алгоритмом с помощью утилиты syskey. Т.е. к вышеописанным алгоритмам добавляется еще 4-й шаг - получение с помощью syskey нового хэша от хэша, полученного на шаге 3.

Ниже мы рассмотрим методы доступа к SAM-файлу и извлечения из него хэшей.

1.2. Методы доступа к SAM-файлу и импорт хэшей

Как уже было сказано, ни прочитать этот файл, ни отредактировать нет никакой возможности - при попытке чтения этого файла Windows сообщает о нарушении совместного доступа, т.к. для системы этот файл всегда открыт и запись в него производит только сама Windows.

Информацию из него можно извлечь даже в работающей системе, но только из-под учетной записи Администратора. Здесь есть два метода получения данных - метод программы PWDUMP (который используется в программах PWDUMP, LC4, LC+4 и др.) и метод с использованием планировщика задач (используется в программе SAMInside).

Метод PWDUMP вкратце работает так - программа подключается к системному процессу LSASS и с его правами (и его же методами) извлекает хэши из ветки SAM реестра, т.е. фактически из SAM-файла. **Метод же планировщика** работает так - по умолчанию в Windows 2000/XP системная утилита Scheduler имеет права пользователя SYSTEM, т.е. полный доступ к системе. Поэтому, если назначить Планировщику задание сохранить определенную ветку реестра в файл, к примеру, то он в назначенное время сохранит ее на диск. После чего из этого файла извлекаются хэши всех пользователей этого компьютера.

А что делать, если пароля Администратора нет и, соответственно, его прав тоже? Тогда злоумышленнику остается делать следующее - если на компьютере установлено несколько операционных систем, то загружаясь в любую из них (даже в Linux) можно получить доступ к системному диску Windows 2000/XP и скопировать SAM-файл в другой каталог, чтобы потом "в спокойной обстановке" загрузить его в нужную программу для восстановления из него паролей.

Более того, существуют программы, способные изменять информацию прямо в SAM-файле, меняя и добавляя пользователей, а также их пароли (например, программа Offline NT Password & Registry Editor). Правда, для этого также необходимо загружаться в другую ОС и иметь полный доступ к системному диску Windows 2000/XP.

Даже если системный диск Windows имеет файловую систему NTFS, то все равно можно получить к нему доступ, используя загрузочную дискету, созданную в программе NTFSDos Pro. Затем, после загрузки с нее, примонтировать нужный NTFS-раздел и скопировать с него нужные файлы.

Если же вы администрируете сервер сети на основе Windows 2000/XP, то учитывайте, что кража вашего SAM-файла может привести к тому, что в руках злоумышленника окажутся не только ваш пароль, но и пароли всех пользователей сети (т.е. их пароли на вход в Windows), т.к. все эти пользователи имеют свои учетные записи на сервере.

Как мы говорили выше, в современных NT-системах применяется дополнительное шифрование хэшей алгоритмом syskey. До недавнего времени хэши из SAM-файла, скопированного из этих ОС, расшифровке не поддавались, т.к. этот алгоритм достаточно сложен, нигде не публиковался и практически не анализировался. Но теперь можно извлекать хэши, даже из зашифрованных этим алгоритмом SAM-файлов, используя программу SAMInside. Правда, для декодирования хэшей этой программе необходим еще и файл SYSTEM, расположенный там же, где и SAM, т.к. в нем хранятся некоторые ключи реестра, необходимые для дешифрования хэшей алгоритмом syskey. Этот файл также открыт только для системы, но, как мы выяснили выше, если можно получить доступ к SAM-файлу, то и файл SYSTEM копируется теми же способами.

Из вышесказанного вытекают **следующие рекомендации**:

- На вашем компьютере не должно быть установлено никаких других систем (Windows 98/ME, Linux и пр.), кроме той ОС, которую вы используете в работе - Windows 2000 или Windows XP.
- Системный диск обязательно должен иметь файловую систему NTFS и жестко разграниченные права доступа к каталогам на этом диске.
- Нужно запретить загрузку с любых устройств, кроме системного диска - дисковода, CD-ROM'а, внешних накопителей и пр. Для этого нужно оставить в BIOS загрузку только с нужного диска и установить пароль на вход в BIOS. А для исключения сброса CMOS-памяти на материнской плате (при которой теряются и все ваши собственные настройки в BIOS, включая пароль на вход в него) опломбируйте системный блок или же установите его в такое место, при котором доступ к нему жестко регламентирован либо же просто невозможен никому, кроме вас. Последние версии BIOS разных производителей не поддаются на "универсальные" пароли (типа "AWARD_SW" для старых BIOS фирмы AWARD), поэтому запрет на физический доступ к компьютеру делает изменение пароля на вход в BIOS невозможным практически на 100%.
- На сетевых серверах максимально снизить количество перезагрузок компьютера и лишить права на перезагрузку всех групп пользователей, кроме учетной записи Администратора.

Файлы:
%SystemRoot%\system32\config\SAM
%SystemRoot%\system32\config\system

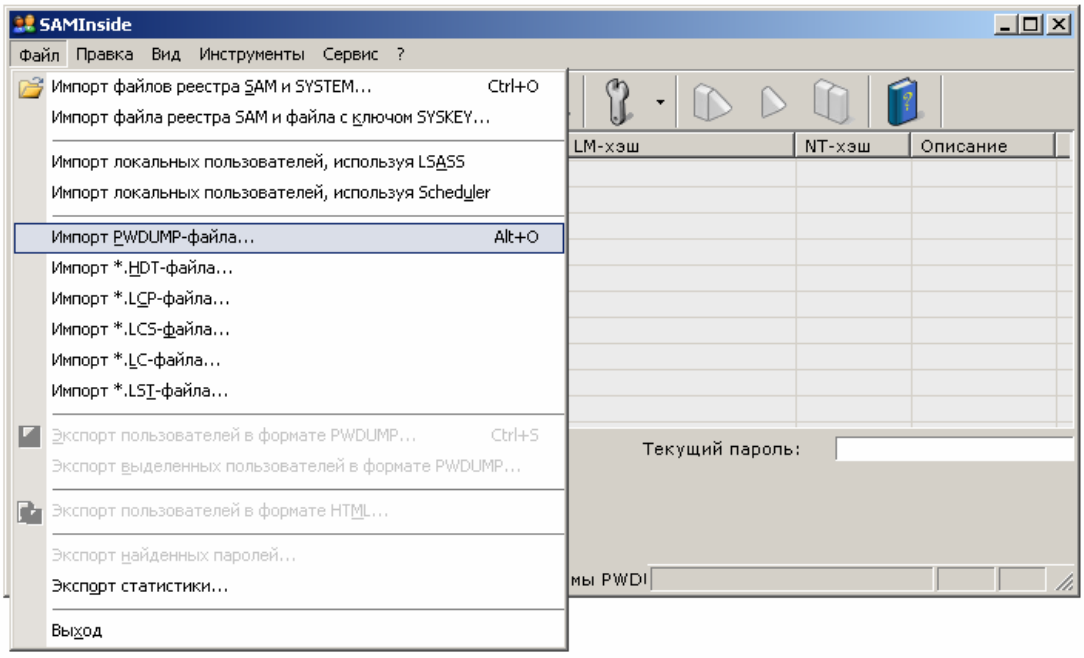
Копии этих файлов:
%SystemRoot%\Repair\SAM
%SystemRoot%\Repair\system

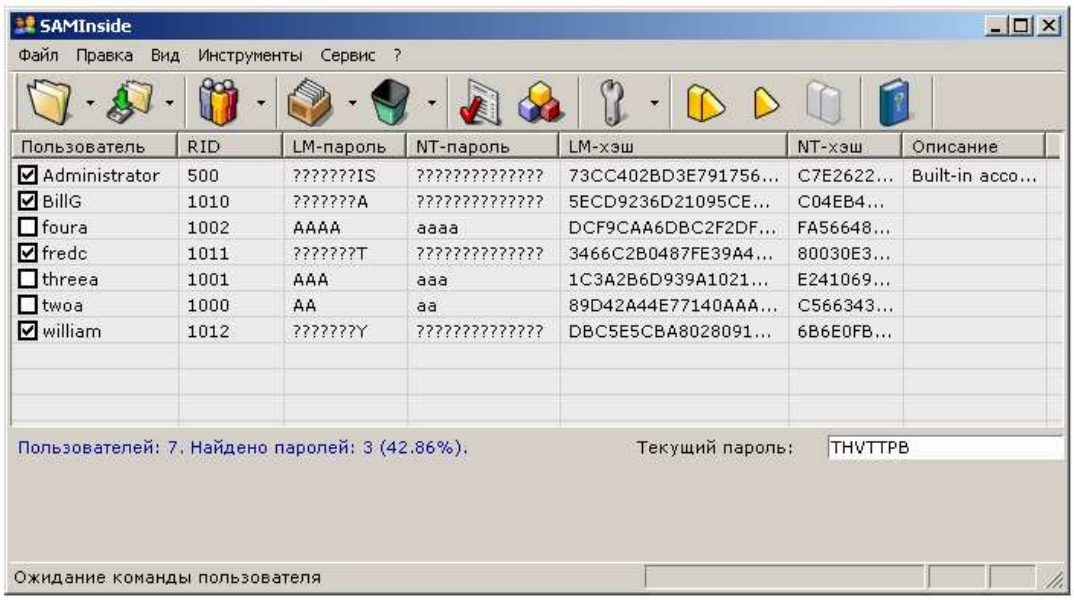
2. Восстановление/Взлом паролей пользователей

Используем программу SAMInside. При распаковке архива в текущей директории находится файл SAMInside_Test1.txt. Выполним импорт этого файла с использованием **"Import from PWDUMP file"** - импорт пользователей из текстового файла в формате программы PWDUMP.

Вид работы программы SAMInside после первоначального анализа файла SAMInside_Test1.txt:

```
BillG:1010:5ECD9236D21095CE7584248B8D2C9F9E:C04EB42B9F5B114C86921C4163AEB5B1:::
Administrator:500:73CC402BD3E791756C3D3B817E02809D:C7E2622D76D3F001CF08B0753646BBCC:Built-in account for administering the computer/domain::
fredc:1011:3466C2B0487FE39A417EAF50CFAC29C3:80030E356D15FB1942772DCFD7DD3234:::
twoa:1000:89D42A44E77140AAAAD3B435B51404EE:C5663434F963BE79C8FD99F535E7AAD8:::
william:1012:DBC5E5CBA8028091B79AE2610DD89D4C:6B6E0FB2ED246885B98586C73B5BFB77:::
threea:1001:1C3A2B6D939A1021AAD3B435B51404EE:E24106942BF38BCF57A6A4B29016EFF6:::
foura:1002:DCF9CAA6DBC2F2DFAAD3B435B51404EE:FA5664875FFADF0AF61ABF9B097FA46F:::
```





Алгоритмы MD4 и DES (применяемые для формирования LM Hash и NT Hash) считаются необратимыми, точнее скажем так - их обратимость математически еще не доказана. Поэтому получение паролей из хэшей прямыми математическими методами невозможно. Остается только одно - перебирать пароли, формировать хэши на основе этих паролей и сравнивать хэши с теми, которые получены из SAM-файла. Если хэши совпадают, то и пароль, который сформировал такой же хэш - верный. Таким образом, для получения пароля Администратора, нужно получить доступ к SAM-файлу, а затем с помощью программы-переборщика паролей, попытаться восстановить нужный пароль.

И тут мы сталкиваемся с одним неприятным для пользователей (и приятным для взломщиков) моментом - как мы помним, LM Hash формируется на основе "половинок" по 7 символов исходного пароля и имеет максимальную длину исходного пароля в 14 символов. Поэтому для восстановления 14-символьного пароля с алфавитом в N символов нужно перебрать не N^14 вариантов, а 2 * (N^7) вариантов, что несоизмеримо меньше! К примеру, при попытке восстановить пароль "MARGARITA", используя в качестве алфавита только латинские буквы, в программе SAMInside (к примеру), мы моментально найдем вторую часть пароля - "TA", а затем спустя некоторое время - и первую часть пароля - "MARGARI", т.к. эта программа ищет обе половинки пароля одновременно!

Поэтому "сложный" (на первый взгляд) 14-символьный пароль по LM Hash восстанавливается как два "простых" пароля по 7 символов. Более того - при формировании LM Hash пароль переводится в верхний регистр, поэтому хэши от паролей "ADMIN", "Admin" и "admin" будут одинаковыми!

Другое дело - NT Hash. Здесь пароль не "разбивается" на части и максимальная длина пароля составляет 128 символов. Да еще и учитывается регистр букв пароля. Поэтому вышеприведенные пароли дадут разные хэши!

Соответственно, для восстановления пароля из латинских букв нужно использовать в качестве алфавита уже 52 символа (26 заглавных латинских символов и 26 строчных), а не только 26 заглавных, как при восстановлении пароля по LM Hash.

Важное замечание: если пароль пользователя больше 14 символов, то Windows 2000/XP автоматически отключают формирование LM Hash, оставляя только NT Hash, а, как мы уже говорили, восстановить пароль по NT Hash гораздо сложнее. Отключить формирование LM Hash также можно через реестр. В Windows XP, к примеру, для этого нужно в ветви

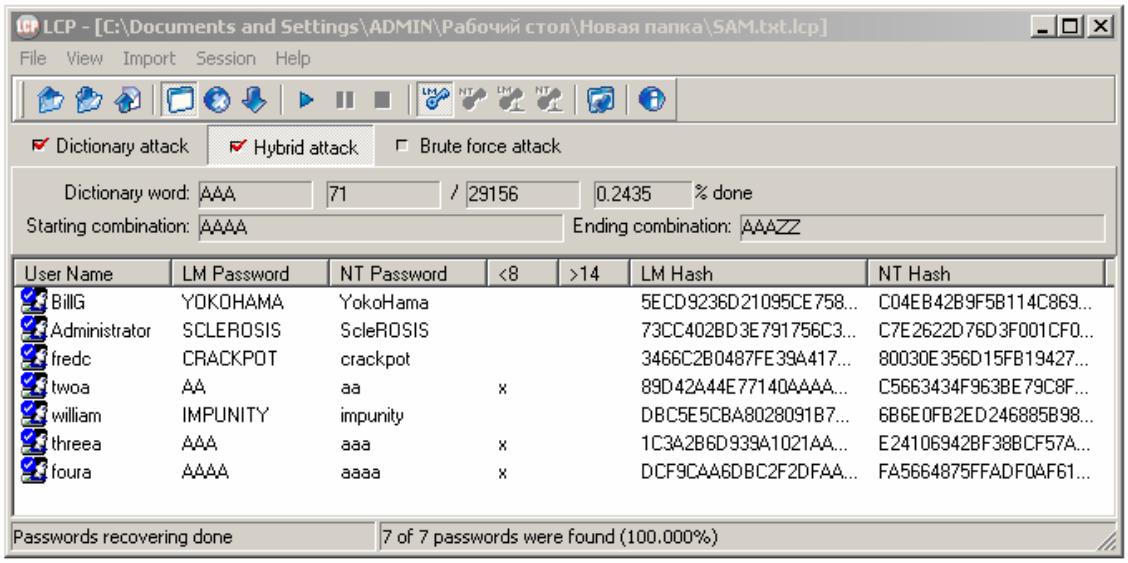
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

создать параметр "nolmhash" типа DWORD со значением 1.

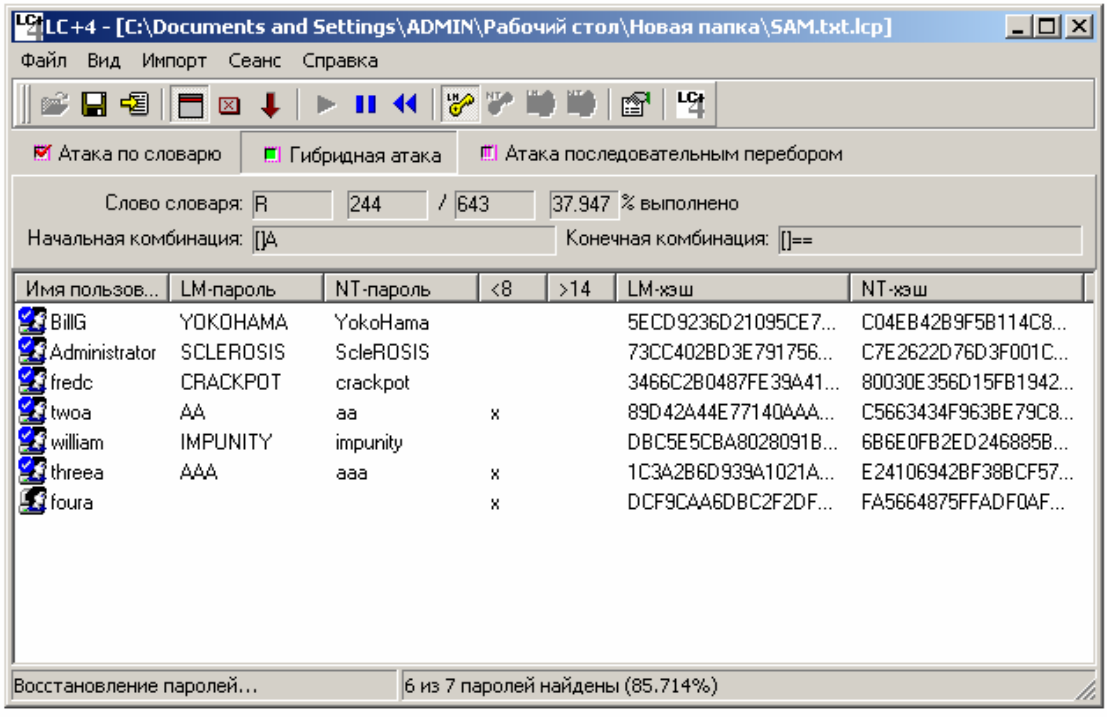
Таким образом, придерживайтесь следующих рекомендаций:

- Ваши пароли на вход в Windows должны быть длиннее 14 символов или же отключите формирование LM Hash, т.е. оставьте потенциальному взломщику возможность восстанавливать ваш пароль только по NT Hash.
- Пароли должны иметь символы как в верхнем, так и в нижнем регистрах!

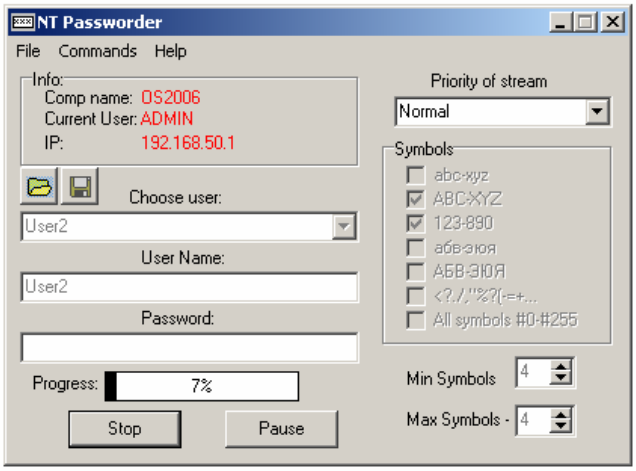
Внешний вид работы программы LCP 5.04 с тем же файлом SAMInside_Test1.txt:



Внешний вид работы программы LC+4 4.02 с тем же файлом SAMInside_Test1.txt:

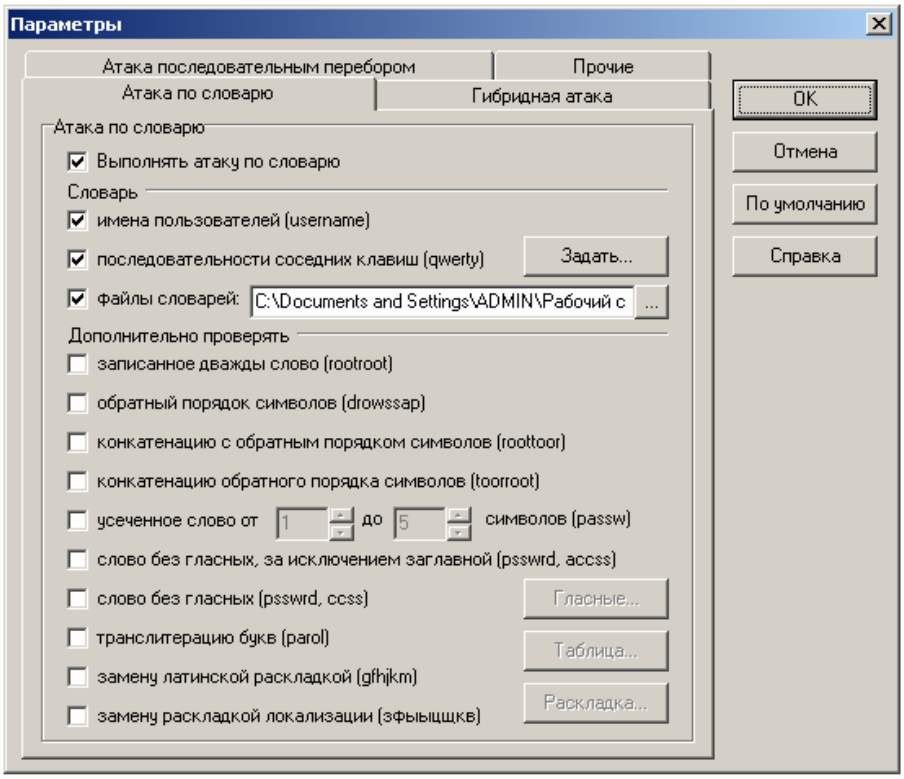


Внешний вид работы программы NT Passworder 1.0, выполняющий атаку полным перебором:

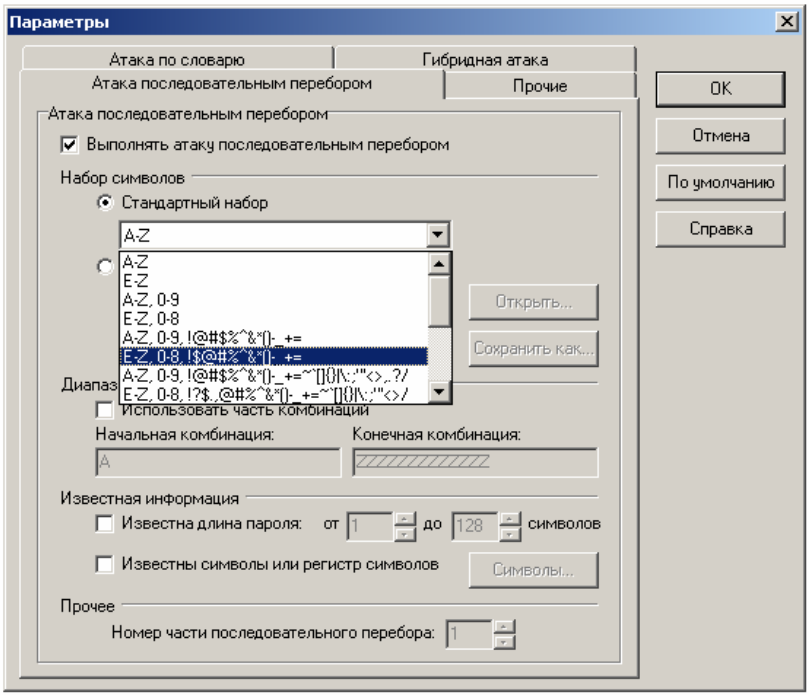


3. Виды атак паролей

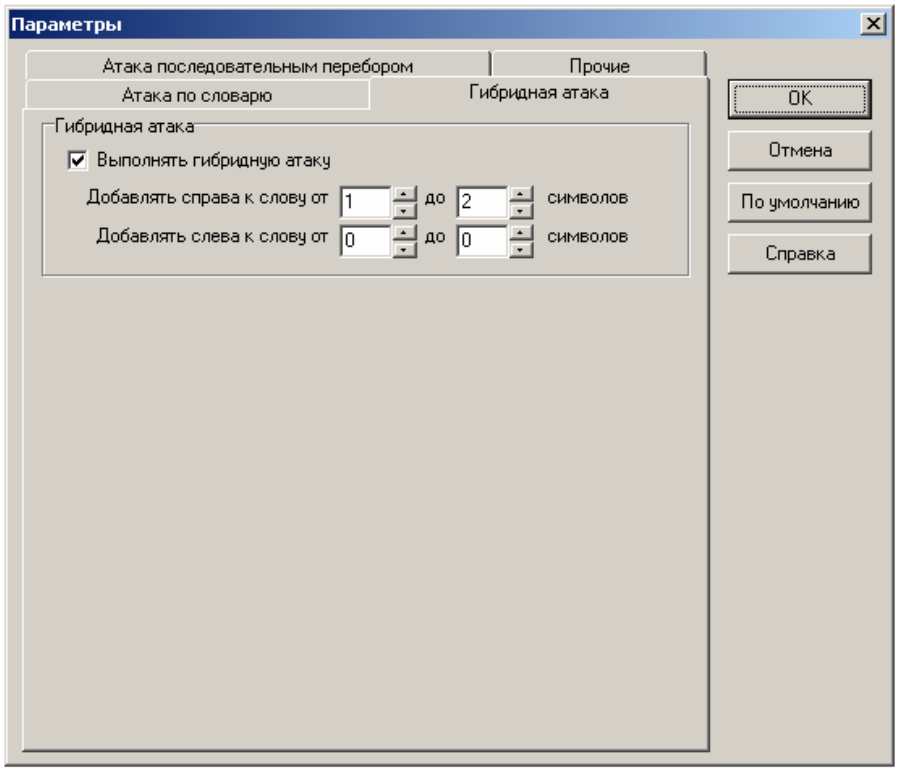
- Атака по словарю



- Атака последовательным перебором



- Гибридная атака



4. Теория и практика аудита и восстановления паролей Windows NT/2000/XP

Получение хэшей паролей

Существует несколько путей получения хэшей паролей, зависящих от их местонахождения и имеющегося доступа. Хэши паролей могут быть получены следующими способами: **из файла SAM** или его резервной копии, непосредственно **из реестра** операционной системы локального или удаленного компьютера, из реестра или **Active Directory** локального компьютера или удаленного компьютера внедрением DLL, посредством перехвата аутентификационных пакетов в сети.

Получение хэшей паролей из файла SAM

Учетные записи пользователей, содержащие в том числе имя пользователя и его пароль, хранятся в реестре Windows NT/2000/XP, а именно в той его части, которая находится в файле SAM (Security Account Manager (англ.) - диспетчер защиты учетных записей). Этот файл можно найти на диске в каталоге %SystemRoot%\system32\config, на диске аварийного восстановления системы или на резервной магнитной ленте.

К файлу SAM в каталоге %SystemRoot%\system32\config нельзя получить доступ, пока Windows NT/2000/XP загружена, так как он открыт операционной системой. Если имеется физический доступ к машине, необходимо скопировать файл, загрузив на этой машине другую копию операционной системы или другую операционную систему. Если Windows NT/2000/XP установлена на диске с файловой системой NTFS, то для MS-DOS и Windows 95/98/Me дополнительно нужны программы, обеспечивающие доступ к диску с NTFS из этих операционных систем. В MS-DOS могут быть использованы NTFSDOS и NTFSDOS Professional, в Windows 95/98/Me - NTFS for Windows 98 (авторами являются Mark Russinovich, Bryce Cogswell). Для доступа из операционной системы Linux требуется включение поддержки NTFS. Также можно загрузиться с дискеты и скопировать файл SAM, предварительно запустив обеспечивающую доступ к разделам с NTFS программу. После этого нужно выполнить импорт файла SAM. Извлечение хэшей паролей из файла SAM было разработано и впервые реализовано в программе SAMDump (автор Дмитрий Андрианов). При импорте файла SAM осуществляется получение списка учетных записей пользователей, содержащихся в файле SAM. Процесс импорта файла SAM подобен получению хэшей паролей методом pwdump за исключением того, что вместо функций Windows API, обеспечивающих работу с реестром Windows, используется их эмуляция. При выполнении импорта файла SAM из программы SAMDump все нелатинские буквы, имеющиеся в именах пользователей, будут искажены. Программа LC+4 лишена этого недостатка.

Другой способ получить файл SAM в операционной системе Windows NT, причем не требующий перезагрузки машины, - это копирование его из каталога %SystemRoot%\repair или с диска аварийного восстановления. Каждый раз, когда в Windows NT создается диск аварийного восстановления с помощью программы RDISK, файл SAM запаковывается и сохраняется в файл sam._, являющийся резервной копией файла SAM. Файл sam._ представляет из себя архив в формате cabinet. Этот файл может быть распакован командой "expand sam._ sam". Недостатком этого способа является то, что с момента создания диска аварийного восстановления пароли могли измениться и, возможно, файл sam._ содержит устаревшие данные. В программе LC+4 имеется встроенная возможность импорта файла SAM и из файла sam._, избавляющая от необходимости использования программы expand. При импорте списка учетных записей

пользователей из файла sam._ он предварительно распаковывается, затем выполняется непосредственно импорт файла SAM.

Файл SAM также копируется, когда создается полная резервная копия. Если имеется доступ к резервной копии, можно восстановить файл SAM из %SystemRoot%\system32\config на другую машину и затем извлечь из него хэши паролей. Недостатком и этого способа также является то, что с момента последнего сеанса создания резервной копии пароли могли измениться.

Существует служебная программа SYSKEY, впервые появившаяся в составе Service Pack 3 для Windows NT. Программа SYSKEY дополнительно зашифровывает хэши паролей учетных записей, что делает импорт файла SAM вышеупомянутым способом бесполезным. **SYSKEY** может использоваться в одном из трех вариантов:

- сгенерированный ключ шифрования записывается на локальный жесткий диск в зашифрованном виде;
- сгенерированный ключ шифрования записывается на дискету, которая должна быть вставлена во время загрузки операционной системы;
- для получения ключа шифрования берется пароль, выбранный администратором и вводимый во время загрузки операционной системы.

Служебная программа SYSKEY в операционной системе Windows NT для дополнительной защиты паролей учетных записей после установки Service Pack соответствующей версии должна быть активизирована вручную. В операционных системах Windows 2000/XP программа SYSKEY изначально присутствует и активизирована.

Импорт файла SAM, дополнительно зашифрованного SYSKEY, впервые был реализован в программе SAMInside. Для выполнения импорта необходимо последовательно открыть файлы SAM и SYSTEM, предварительно скопировав их из каталога %SystemRoot%\system32\config. Резервные копии файлов также могут находиться в каталоге %SystemRoot%\repair, если ранее выполнялась архивация.

Получение хэшей паролей из реестра операционной системы

При получении хэшей паролей из реестра операционной системы осуществляется непосредственный доступ к реестру. Для выполнения импорта информации необходимо иметь административные права на компьютере, дамп паролей учетных записей которого требуется создать. Если компьютер не является локальным, то должен быть разрешен удаленный доступ к реестру и иметься соответствующие права. Получение хэшей данным способом впервые стало возможным в программе pwdump (автор Jeremy Allison). При выполнении импорта информации этим способом с помощью программы pwdump имена пользователей, содержащие нелатинские буквы, будут искажены. Для получения хэшей паролей из реестра рекомендуется воспользоваться LC+4.

Если программа SYSKEY активизирована, хэши паролей дополнительно зашифровываются. Выполнение импорта при этом становится бесполезным так же, как и импорт файла SAM, т.к. пароли по дополнительно зашифрованным хэшам восстановлены не будут.

Получение хэшей паролей внедрением DLL

Данный метод был разработан и реализован в программе **pwdump2** (автор Todd A. Sabin). Получение хэшей паролей методом pwdump2 возможно вне зависимости от того, была активизирована программа SYSKEY или нет. Для создания дампа паролей методом pwdump2 необходимо иметь право SeDebugPrivilege. По умолчанию только пользователи группы администраторов имеют его, поэтому нужно иметь административные права для использования этого метода. Использование метода pwdump2 возможно только на локальной машине.

Метод pwdump2 использует для создания дампа паролей способ, называемый внедрением DLL. Один процесс вынуждает другой процесс (lsass.exe), используя его идентификатор процесса, загружать DLL (samdump.dll) и выполнять некоторый код из DLL в адресном пространстве другого процесса (lsass.exe). Загрузив samdump.dll в **lsass** (системная служба LSASS - Local Security Authority Subsystem), программа использует тот же самый внутренний API, что msv1_0.dll, чтобы обратиться к хэшам паролей. Это означает, что она может получить хэши без выполнения таких действий, как перемещение их из реестра и дешифрование. Программа не заботится ни о том, каковы алгоритмы шифрования, ни каковы ключи.

Метод, использующийся в программе pwdump2, был доработан для получения хэшей паролей не только с локальной, но и с удаленной машины в программах pwdump3/pwdump3e (автор Phil Staubs). На удаленный компьютер копируются исполняемый файл службы и файл DLL. После копирования файлов на удаленном компьютере создается и запускается новая служба, выполняющая те же действия, что и программа pwdump2 на локальном компьютере. Далее выполняется удаление службы и файлов, ранее скопированных. Передача информации об учетных записях пользователей производится через раздел реестра на удаленном компьютере, временно создаваемый и уничтожаемый после завершения копирования данных. В программе pwdump3e выполняется дополнительное шифрование передаваемых данных по алгоритму Diffie-Hellman для сохранения конфиденциальности при их возможном перехвате при передаче по сети. Использование данного метода также требует административных прав на той машине, информацию об учетных записях пользователей с которой хочется получить.

Если административные права на локальном компьютере отсутствуют, можно воспользоваться уязвимостью операционных систем Windows NT/2000/XP, заключающейся в замене экранной заставки, запускаемой при отсутствии регистрации пользователя операционной системы в течение некоторого времени (по умолчанию интервал времени составляет 15 минут для Windows NT/2000, 10 минут - для Windows XP). Для этого файл %SystemRoot%\system32\logon.scr заменяется на требуемый исполняемый файл (например, cmd.exe), который будет запущен операционной системой вместо экранной заставки с правами системы. Замена может быть выполнена способом, используемым при копировании файла SAM.

Доступ к диску с NTFS с возможностью записи осуществим с помощью NTFSDOS Professional или NTFS for Windows 98. Далее выполняются действия по получению хэшей методом pwdump2 или pwdump3/pwdump3e.

Перехват аутентификационных пакетов в сети

Даже если программа SYSKEY установлена и активизирована, не имеется необходимого доступа к удаленному или локальному компьютеру, существует возможность получения хэшей паролей учетных записей пользователей. Этим способом является перехват аутентификационных пакетов в сети (sniffing (англ.) - вынюхивание). Клиентская машина обменивается с сервером аутентификационными пакетами каждый раз, когда требуется подтверждение прав пользователя. Необходимо, чтобы компьютер находился в сетевом сегменте пользователя или ресурса, к которому он обращается. Программа для перехвата аутентификационных пакетов (sniffer (англ.) - вынюхиватель), встроенная в LC4, работает на машинах с Ethernet-адаптером и в Windows NT/2000/XP, и в Windows 95/98/Me. Программу LC4 в режиме перехвата аутентификационных пакетов нужно оставить запущенной на некоторое время для сбора достаточного количества хэшей паролей. Полученные данные необходимо сохранить в файл, после чего в программе LC+4 выполнить импорт файла сеанса LC4.

Для препятствования получения хэшей паролей этим способом фирмой Microsoft было разработано расширение существующего механизма аутентификации, называемое NTLMv2. Его использование становится возможным после установки Service Pack, начиная с Service Pack 4 для Windows NT.

Восстановление паролей

Пароль может быть получен различными способами: *атакой по словарю*, *последовательным перебором* и *гибридом атаки по словарю и последовательного перебора*.

При атаке по словарю последовательно вычисляются хэши для каждого из слов словаря или модификаций слов словаря и сравниваются с хэшами паролей каждого из пользователей. При совпадении хэшей пароль найден. Преимущество метода - его высокая скорость. Недостатком есть то, что таким образом могут быть найдены только очень простые пароли, которые имеются в словаре или являются модификациями слов словаря.

Последовательный перебор комбинаций (**brute force** (англ.) - грубая сила (дословно), решение "в лоб") использует набор символов и вычисляет хэш 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 содержится в выбранном наборе, тем больше времени может пройти, пока перебор комбинаций не закончится.

При восстановлении паролей **гибридом атаки по словарю и последовательного перебора** к каждому слову или модификации слова словаря добавляются символы справа и/или слева. Для каждой получившейся комбинации вычисляется хэш, который сравнивается с хэшами паролей каждого из пользователей.

После получения хэшей паролей можно начать восстановление паролей. Двумя основными типами файла, содержащими хэши паролей, являются PwDump - (passwords dump (англ.) - дамп паролей) и Sniff-файл.

Каждая строка PwDump-файла имеет следующий формат:

"ИмяПользователя:RID:LM-хэш:NT-хэш:ПолноеИмя,Описание:ОсновнойКаталогПользователя:"

Каждая из 7-символьных половин пароля зашифрована независимо от другой в LM-хэш по алгоритму DES (бывший федеральный стандарт США), NT-хэш получается в результате шифрования всего пароля по алгоритму MD4 (фирмы RSA Security, Inc.). LM-хэш содержит информацию о пароле без учета регистра (в верхнем регистре), а NT-хэш - с учетом регистра. После имени пользователя имеется уникальный идентификатор учетной записи RID (relative identifier (англ.) - относительный идентификатор), который для получения хэшей не используется. Идентификатор встроенной учетной записи администратора равен 500, гостевой учетной записи - 501. LM-хэш присутствует для совместимости с другими операционными системами (LAN Manager, Windows for Workgroups, Windows 95/98/Me и т.д.). Его наличие упрощает восстановление паролей. Если длина NT-пароля превышает 14 символов, LM-хэш соответствует пустому паролю. При существовании LM-хэша восстановление сначала осуществляется по LM-хэшу, после нахождения LM-пароля используется NT-хэш для определения NT-пароля.

Каждая строка Sniff-файла имеет следующий формат:

"ИмяПользователя:3:ЗапросСервера:LM-ответ:NT-ответ"

LM-ответ получается в результате шифрования LM-хэша, NT-ответ - в результате шифрования NT-хэша. Шифрование выполняется по алгоритму DES таким образом, что определить LM- и NT-пароль можно только при проверке всего пароля. Кроме того, в каждом случае используется свой запрос сервера. Поэтому на определение паролей по Sniff-файлу потребуется значительно больше времени.

Изменение паролей пользователей без их восстановления

Если восстановление паролей пользователей Windows NT/2000/XP не требуется, возможно их изменение при имеющемся доступе к локальному компьютеру. Изменение паролей делается с помощью программы Offline NT Password & Registry Editor (автор Petter Nordahl-Hagen). Выполняется загрузка с дискеты с операционной системой Linux, выбор пользователя для изменения пароля, вычисление хэша пароля и

модификация файла SAM на диске с операционной системой. Программа поддерживает Windows NT/2000/XP, в т.ч. с активизированной служебной программой SYSKEY.

Рекомендации администратору Windows NT/2000/XP

На машинах с Windows NT/2000/XP:
• сделать недоступным для вскрытия системный блок компьютера для предотвращения возможного отключения жесткого диска с операционной системой или подключения другого диска;
• в Setup разрешить загрузку только с жесткого диска, чтобы не допустить загрузку с другого носителя;
• установить пароль на вход в Setup, не позволяя отменить запрет на загрузку с другого носителя;
• Windows NT/2000/XP должна быть единственной операционной системой, установленной на машине, что делает невозможным копирование и замену файлов из других операционных систем;
• использовать только файловую систему NTFS, отказаться от использования FAT и FAT32;
• удостовериться в Windows NT, что установлен Service Pack 3 или более поздний и активизирована служебная программа SYSKEY;
• использовать встроенную в операционные системы Windows 2000/XP возможность шифрования файлов посредством EFS (Encrypting File System (англ.) - файловая система с шифрованием), являющейся частью NTFS5;
• запретить удаленное управление реестром, остановив соответствующую службу;
• отменить использование особых общих папок ADMIN$, C$ и т.д., позволяющих пользователю с административными правами подключаться к ним через сеть. Для этого необходимо добавить в реестр параметр AutoShareWks (для версий Workstation и Prosessional) или AutoShareServer (для версии Server) типа DWORD и установить его в 0 в разделе

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters

Диапазон: 0-1, по умолчанию - 1.
0 - не создавать особые общие ресурсы;
1 - создавать особые общие ресурсы.

• запретить или максимально ограничить количество совместно используемых сетевых ресурсов;
• ограничить анонимный доступ в операционных системах Windows NT/2000, позволяющий при анонимном подключении получать информацию о пользователях, политике безопасности и общих ресурсах. В Windows NT/2000 нужно добавить в реестр параметр RestrictAnonymous типа DWORD в разделе

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA

Диапазон: 0-2, по умолчанию - 0 для Windows NT/2000, 1 - для Windows XP.
0 - не ограничивать, положиться на заданные по умолчанию разрешения;
1 - не разрешать получать список учетных записей и имен пользователей;
2 - не предоставлять доступ без явных анонимных разрешений (недоступно в Windows NT).

• если в сети отсутствуют клиенты с Windows for Workgroups и Windows 95/98/Me, то рекомендуется отключить LM-аутентификацию, так как это существенно затруднит восстановление паролей при перехвате аутентификационных пакетов злоумышленником. Если же такие клиенты присутствуют, то можно включить использование аутентификации только по запросу сервера. Это можно сделать, активизировав расширение механизма аутентификации NTLMv2. Для его активизации необходимо добавить в реестр следующие параметры:

• LMCompatibilityLevel типа DWORD в разделе

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA

Диапазон: 0-5, по умолчанию - 0.
0 - посылать LM- и NT-ответы, никогда не использовать аутентификацию NTLMv2;
1 - использовать аутентификацию NTLMv2, если это необходимо;
2 - посылать только NT-ответ;
3 - использовать только аутентификацию NTLMv2;
4 - контроллеру домена отказывать в LM-аутентификации;
5 - контроллеру домена отказывать в LM- и NT-аутентификации (допустима только аутентификация NTLMv2).

• NtlmMinClientSec или NtlmMinServerSec типа DWORD в разделе

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\MSV1_0

Диапазон: объединенные по логическому ИЛИ любые из следующих значений:
0x00000010 - целостность сообщений;
0x00000020 - конфиденциальность сообщений;
0x00080000 - безопасность сеанса NTLMv2;
0x20000000 - 128-битное шифрование.

• запретить отображение имени пользователя, который последним регистрировался в операционной системе, в диалоговом окне регистрации. Для этого нужно добавить в реестр строковый параметр DontDisplayLastUserName и установить его в 1 в разделе

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Диапазон: 0-1, по умолчанию - 0.
0 - отображать имя последнего пользователя;
1 - не отображать имя последнего пользователя.

• запретить запуск экранной заставки при отсутствии регистрации пользователя операционной системы в течение некоторого времени. Для этого нужно в реестре значение параметра ScreenSaveTimeOut установить в 0 в разделе

HKEY_USERS\.DEFAULT\Control Panel\Desktop

• **при выборе паролей Windows NT/2000/XP соблюдать следующие правила**:
→ не выбирать в качестве пароля или части пароля любое слово, которое может являться словом словаря или его модификацией;
→ длина пароля в Windows NT должна быть не менее 7 символов (при максимально возможной длине пароля в 14 символов), в Windows 2000/XP - более 14 символов (при максимально возможной длине пароля в 128 символов);
→ пароль должен содержать символы из возможно большого символьного набора. Нельзя ограничиваться только символами A-Z, желательнее использовать в пароле и буквы, и цифры, и специальные символы (причем в каждой из 7-символьных половин пароля, если длина пароля менее или равна 14);
→ символы пароля, являющиеся буквами, должны быть как верхнего, так и нижнего регистра, что затруднит восстановление пароля, производимое по NT-хэшу;
• своевременно выполнять установку пакетов исправлений и обновлений операционной системы;
• переименовать административную и гостевую учетные записи, отключив при этом последнюю;
• избегать наличия учетной записи с именем и паролем, совпадающими с административной, на другом компьютере в качестве обычной учетной записи;
• иметь только одного пользователя с административными правами;
• задать политику учетных записей (блокировку учетных записей после определенного числа ошибок входа в систему, максимальный срок действия пароля, минимальную длину пароля, удовлетворение пароля требованиям сложности, требование неповторяемости паролей и т.д.);
• установить аудит неудачных входов;
• воспользоваться программами из пакета Microsoft Security Tool Kit, в частности HFNetChk и Microsoft Baseline Security Analyzer (написаны Shavlik Technologies, LLC для Microsoft), проверяющими наличие установленных обновлений и имеющихся ошибок в настройке системы безопасности;
• периодически выполнять аудит паролей, используя программу LC+4 или подобные ей.

5. Формирование безопасных паролей

Конечно же, кроме полного перебора всех вариантов пароля, применяются и другие методы - гибридная атака или атака по маске, а также атака по словарю. Эти методы более эффективны, нежели полный перебор и в некоторых случаях позволяют гораздо быстрее находить пароли, так что поговорим о создании таких паролей, которые очень трудно или практически невозможно восстановить.

Распространено заблуждение о том, что длинный пароль - это сложный пароль. Ничего подобного! Разве сложным будет пароль "12345678901234567890"? Он набирается за несколько секунд - ничего сложного. Или пароль "administrator12345"? Или пароль "qwertqwertqwertqwert"? Помните, что длинный пароль - не обязательно СЛОЖНЫЙ пароль. Конечно, вышеприведенные пароли можно использовать на практике, но все-таки они остаются достаточно уязвимыми. Но ведь мы-то хотим получить совсем "пуленепробиваемый" пароль?

Тогда давайте рассмотрим, сколько всего комбинаций потребуется для перебора, к примеру, всех 7-символьных паролей, если использовать только латиницу? Правильно - 26^7. А если добавить к этим символам цифры? Тогда - 36^7, что существенно больше. Отсюда следует простой вывод - чем больше в пароле будет использовано символов из разных символьных наборов, которыми пользуются взломщики паролей, тем сложнее будет восстановить пароль, т.к. для перебора всех вариантов придется формировать алфавит, состоящий из всех символов. Нетрудно подсчитать, что перебор всех 7-символьных паролей с алфавитом из заглавных букв латиницы (26 символов), кириллицы (33 символа), цифр (10 символов), специальных символов !@#$%... (32 символа) и пробела - всего 102 символа при скорости в 5 миллионов паролей в секунду займет... около 265 дней. А если пароль не 7 символов а 10, 14, 20... Понятно, что такие колоссальные сроки взлома не устроят ни одного злоумышленника.

И поэтому при восстановлении пароля алфавит, т.е. набор символов для перебора, сужают. Но нам-то нужно затруднить восстановление нашего пароля! Поэтому мы должны наоборот расширять применение символов из разных наборов - ведь взломщик-то изначально не знает наш пароль!

К примеру, добавление к паролю "12345678901234567890" символа '?' справа или слева уже существенно затруднит его восстановление (ведь взломщик, даже если и знает, что в пароле есть цифры и "какой-то специальный символ", то ему придется перебирать алфавитом не в 10 символов - только цифры, а 10 + 32, т.е. цифры + специальные символы, что существенно затруднит взлом пароля). А если добавить пару пробелов? Или несколько русских/английских букв? А если еще использовать и символы

разного регистра (а при формировании NT Hash, как мы помним, регистр символа также имеет значение)? Таким образом, подобный пароль восстановить в приемлемые сроки невозможно.

Отсюда еще одно важное правило:

• Ваши пароли обязательно должны содержать символы из различных символьных наборов!

Также нужно иметь в виду, что один из распространенных способов восстановления паролей - атака по словарю (при котором проверяются пароли, представляющие собой известные слова, словосочетания, клавиатурные комбинации и т.п.) становится бесполезным при атаке на пароли с добавлением символов из других символьных наборов. Действительно, пароль "MASTER" легко взломается с помощью среднестатистического словаря, а восстановить пароль "$MASTER$" таким методом будет уже невозможно.

Можно возразить, что можно использовать и короткий пароль из различных символов типа "FЭ1_$", но практика показывает, что как раз такие пароли и являются сложными для запоминания, нежели какое-либо памятное вам слово или комбинация символов с добавлением (или предварением) нескольких "малораспространенных" символов. К примеру, если ваш "любимый" пароль - "123456" и вы пользуетесь русской версией Windows XP (а в ней при вводе пароля на вход в систему по умолчанию стоит русский язык), то после 123456 понажимайте несколько раз клавишу '`' (находится слева от клавиши '1') с зажатой/отжатой клавишей Shift и вы получите пароль "123456ЁёЁёЁёЁёЁё" или "123456~`~`~`~`~`" при английской раскладке клавиатуры, что тоже неплохо. В таком пароле нет же ничего сложного! Запоминается (и вводится) моментально, но взлом очень затруднен, даже если взломщик имеет в распоряжении не один компьютер для восстановления паролей, а целую сеть. Конечно, теоретически взломщик может при переборе случайно попасть на похожий набор символов. Но вероятность такого события ненамного выше угадывания самого пароля, поэтому такой вариант мы исключаем.

Но даже данный пароль не является идеальным, т.к. содержит повторяющиеся символы - т.е. на 16 символов пароля, длина алфавита, с помощью которого можно восстановить данный пароль, равна 8 символам, что существенно меньше, чем 16. Таким образом, "идеальным" паролем будет такой, в котором нет ни одного повторяющегося символа.

Поэтому дадим заключительный совет по формированию паролей:

• Подключите свою фантазию! Придумать легкий для запоминания, но нереальный для взлома пароль крайне просто. Пусть ваш пароль будет очень легким для вас, но крайне сложным для взломщика. И, конечно же, этот пароль не должен совпадать с какими-либо другими паролями - на ICQ, ваш почтовый ящик или рассылку. Т.е. пароль на вход в систему должен быть УНИКАЛЬНЫМ! Тогда вы можете быть уверены в том, что даже если каким-либо способом будет получен доступ к SAM-файлу, злоумышленник все равно не восстановит пароль Администратора, а значит и не получит и доступа к вашему компьютеру.

6. Встроенные средства безопасности Windows 2000/XP

Несомненно, одним из главных инструментом для создания защищенного компьютера под Windows 2000/XP являются "Политики учетных записей" и "Локальные политики безопасности", вызываемые из меню Настройки → Панель Управления → апплет "Администрирование". Множество параметров безопасности удобнее настраивать именно оттуда.

Политика паролей (Политики учетных записей)

Макс. срок действия пароля
Мин. длина пароля
Мин. срок действия пароля
Пароль должен отвечать требованиям сложности
Требовать неповторяемости паролей
Хранить пароли всех пользователей в домене, используя обратимое шифрование

Политика блокировки учетной записи (Политики учетных записей)

Блокировка учетной записи на
Пороговое значение блокировки
Сброс счетчика блокировки через

Назначение прав пользователя (Локальные политики)

Архивирование файлов и каталогов
Восстановление файлов и каталогов
Вход в качестве пакетного задания
Вход в качестве службы
Добавление рабочих станций к домену
Доступ к компьютеру из сети
Завершение работы системы
Загрузка и выгрузка драйверов устройств
Закрепление страниц в памяти
Замена маркера уровня процесса
Запретить вход в систему через службу терминалов

Запуск операций по обслуживанию тома
Извлечение компьютера из стыковочного узла
Изменение параметров среды оборудования
Изменение системного времени
Локальный вход в систему
Настройка квот памяти для процесса
Обход перекрестной проверки
Овладение файлами или иными объектами
Олицетворение клиента после проверки подлинности
Отказ в доступе к компьютеру из сети
Отказ во входе в качестве пакетного задания
Отказать во входе в качестве службы
Отклонить локальный вход
Отладка программ
Принудительное удаленное завершение
Профилирование загруженности системы
Профилирование одного процесса
Работа в режиме операционной системы
Разрешать вход в систему через службу терминалов
Разрешение доверия к учетным записям при делегировании
Синхронизация данных службы каталогов
Создание глобальных объектов
Создание журналов безопасности
Создание маркерного объекта
Создание постоянных объектов совместного использования
Создание страничного файла
Увеличение приоритета диспетчирования
Управление аудитом и журналом безопасности

Параметры безопасности (Локальные политики)

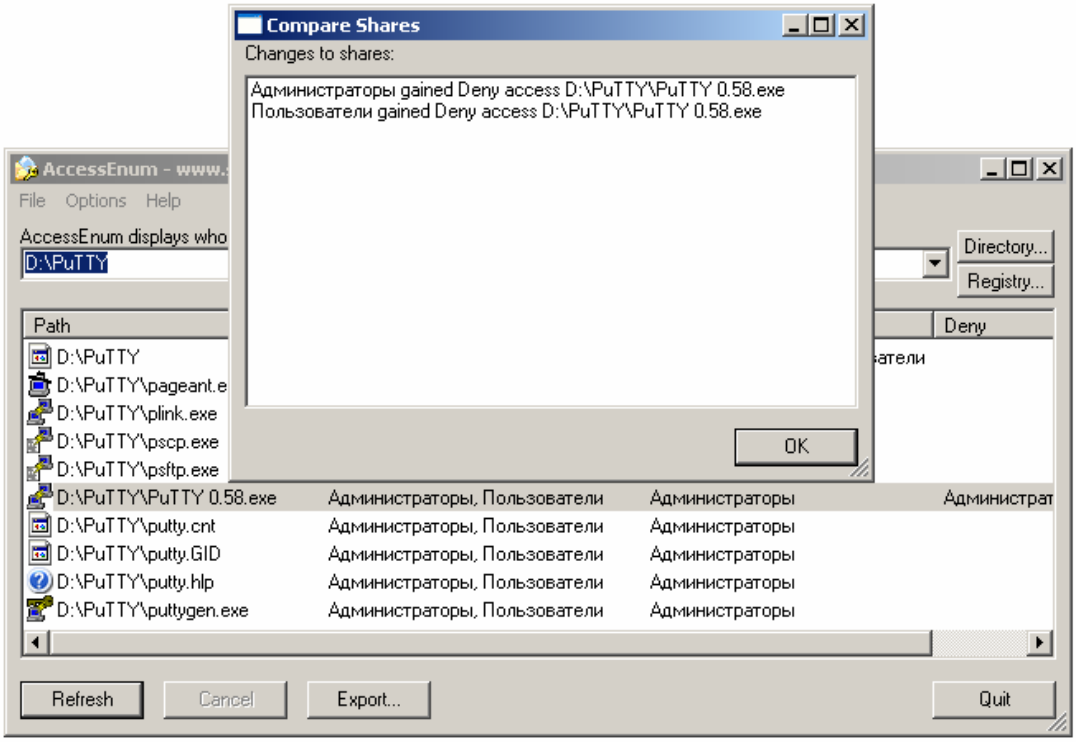
DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)
DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language)
Аудит: аудит доступа глобальных системных объектов
Аудит: аудит прав на архивацию и восстановление
Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности
Доступ к сети: Разрешить трансляцию анонимного SID в имя
Завершение работы: очистка страничного файла виртуальной памяти
Завершение работы: разрешить завершение работы системы без выполнения входа в систему
Интерактивный вход в систему: поведение при извлечении смарт-карты
Интерактивный вход в систему: требовать смарт-карту
Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему
Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)
Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее
Интерактивный вход в систему: не отображать последнего имени пользователя
Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL
Интерактивный вход в систему: текст сообщения для пользователей при входе в систему
Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера
Клиент сети Microsoft: использовать цифровую подпись (всегда)
Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)
Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам
Консоль восстановления: разрешить автоматический вход администратора
Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам
Контроллер домена: запретить изменение пароля учетных записей компьютера
Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию
Контроллер домена: требования подписывания для LDAP сервера
Сервер сети Microsoft: Длительность простоя перед отключением сеанса
Сервер сети Microsoft: использовать цифровую подпись (всегда)
Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)
Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа
Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC)
Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC)
Сетевая безопасность: не хранить хеш-значений LAN Manager при следующей смене пароля
Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы
Сетевая безопасность: требования подписывания для LDAP клиента
Сетевая безопасность: уровень проверки подлинности LAN Manager
Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей Обычная - локальные пользователи удостоверяются как они сами
Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями
Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями
Сетевой доступ: не разрешать сохранение учетных данных или цифровых паспортов .NET для сетевой проверки подлинности пользователя
Сетевой доступ: пути в реестре доступны через удаленное подключение
Сетевой доступ: разрешать анонимный доступ к именованным каналам
Сетевой доступ: разрешать анонимный доступ к общим ресурсам
Сетевой доступ: разрешать применение разрешений для всех к анонимным пользователям
Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания
Системные объекты: владелец по умолчанию для объектов, созданных членами группы администраторов
Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок)
Системные объекты: учитывать регистр для подсистем, отличных от Windows

Устройства: запретить пользователям установку драйверов принтера
Устройства: поведение при установке неподписанного драйвера
Устройства: разрешать отстыковку без входа в систему
Устройства: разрешено форматировать и извлекать съемные носители
Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям
Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям
Учетные записи: ограничить использование пустых паролей только для консольного входа
Учетные записи: Переименование учетной записи администратора
Учетные записи: Переименование учетной записи гостя
Учетные записи: Состояние учетной записи 'Администратор'
Учетные записи: Состояние учетной записи 'Гость'
Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала
Член домена: максимальный срок действия пароля учетных записей компьютера
Член домена: отключить изменение пароля учетных записей компьютера
Член домена: требует стойкого ключа сеанса (Windows 2000 или выше)
Член домена: цифровая подпись данных безопасного канала, когда это возможно
Член домена: шифрование данных безопасного канала, когда это возможно

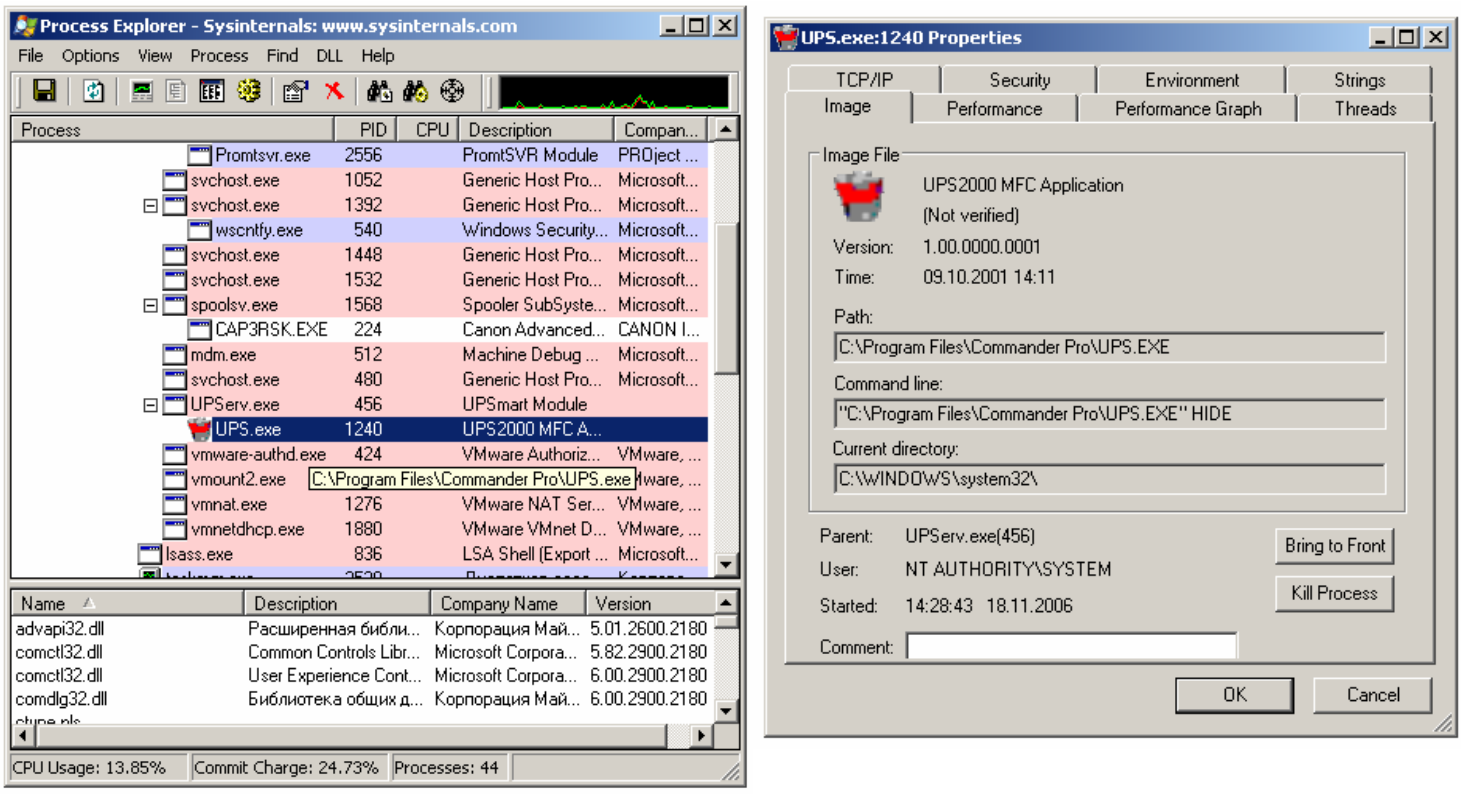
7. Информация о процессах и файлах

Для безопасной работы необходимо иметь четкую картину использования ресурсов в вашей системе. Стандартные средства Windows, например, taskmanager обладают недостаточной функциональностью. В этом случае могут помочь утилиты сторонних производителей. В данном пункте работы вам необходимо изучить возможности ряда бесплатных утилит. В том числе:

- анализирующей безопасность файловой системы - AccessEnum (графический режим)
  Показывает, кто имеет доступ к файлам и папкам в пределах директории. Хотя каждый файл/директория исследованы, AccessEnum показывает только те разрешения, которые отличаются от их родительской папки, позволяя Вам быстро определить отклонения в вашей политике безопасности.
  Также позволяет сравнивать разрешения, которые были сохранены в момент времени T_1 с разрешениями, которые установлены на данный момент времени.



- показывающий ресурсы занятые процессами - ProcExp (графический режим)
  Есть возможность просмотреть какие dll файлы использует тот или иной процесс, просмотреть свойства выбранного dll, найти нужный Handle или dll, задать приоритет процесса, просотреть свойства процесса, убить процесс и т.п.



Приведем пример отображения свойств одного из процессов системы PID: 1240.

- показывающий ресурсы занятые процессами и процессы, использующие файл/каталог - handle (режим командной строки).

```
d:\handle -p BCResident.exe
Handle v2.2
Copyright (C) 1997-2004 Mark Russinovich
Sysinternals - www.sysinternals.com
------------------------------------------------------------------------------
BCResident.exe pid: 1960 OS2006\ADMIN
    c: File          C:\Program Files\Jetico\BestCrypt
  788: Section       \BaseNamedObjects\MSCTF.Shared.SFM.MO
  7a0: Section       \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1060284298-1078145449-839522115-1003SFM.DefaultS-1-5-
                                                                                21-1060284298-1078145449-839522115-1003
  7b8: Section       \BaseNamedObjects\CiceroSharedMemDefaultS-1-5-21-1060284298-1078145449-839522115-1003
  7c4: File          C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9
  7c8: File          C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9

d:\handle -a
System pid: 4 NT AUTHORITY\SYSTEM
    4: Process       System(4)
    8: Thread        System(4): 12
    c: Key           HKLM\SYSTEM\ControlSet001\Control\Session Manager\Memory Management\PrefetchParameters
   10: Key           \REGISTRY
   14: Key           HKLM\SYSTEM\Setup
   18: Key           HKLM\HARDWARE\DESCRIPTION\System\MultifunctionAdapter
   1c: Key           HKLM\SYSTEM\WPA\MediaCenter
   20: Key           HKLM\SYSTEM\WPA\Key-CJ27J3P2XV9J9JCPB4DVT
   24: Key           HKLM\SYSTEM\WPA\PnP
   28: Key           HKLM\SYSTEM\WPA\SigningHash-6KCM6KFTX6MD62
   2c: Key           HKLM\SYSTEM\ControlSet001\Control\ProductOptions
   30: Key           HKLM\SYSTEM\ControlSet001\Services\Eventlog
   34: Event         \Security\TRKWKS_EVENT
   38: Key           HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 2\Scsi Bus 0
   3c: Thread        System(4): 356
   40: Thread        System(4): 340
   44: Key           HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 2\Scsi Bus 0\Target Id 0
   48: Thread        System(4): 368
   4c: Thread        System(4): 352
   50: Thread        System(4): 348
   54: Thread        System(4): 212
   58: Thread        System(4): 204
   5c: Key           HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 2
   60: Thread        System(4): 336
   64: Key           HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 2\Scsi Bus 0\Target Id 0\Logical Unit Id 0
   68: Thread        System(4): 208
   6c: File          \Device\Tcp
   70: Key           HKLM\HARDWARE\DEVICEMAP\Scsi
   74: Key           HKLM\SYSTEM\ControlSet001\Control\Video\{8B7C2FC9-4F53-4CB7-AED3-50E7570F6CEF}\0000\VolatileSettings
   78: File
   7c: Key           HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 2\Scsi Bus 0\Initiator Id 15
   80: File
   84: Key           HKLM\HARDWARE\DESCRIPTION\System\MultifunctionAdapter
```

```
   88: File
   8c: Thread        System(4): 164
   90: Key           HKLM\HARDWARE\DESCRIPTION\System\MultifunctionAdapter
   94: File          \Device\Gpc
   98: File
   9c: Thread        System(4): 156
   ……
```

8. Безопасность при работе в сети

Если компьютер под управлением Windows 2000/XP подключен к сети, то, конечно же, он становится уязвим и для сетевых атак. Поэтому безопасность при работе в сети также включает в себя несколько рекомендаций. Во-первых, вы должны знать сетевые параметры настройки вашего компьютера. Для определения базовых настроек стека протоколов TCP/IP служит команда "ipconfig /all ", выполняемая в режиме командной строки.

Использование

```
ipconfig [/? | /all | /release [адаптер] | /renew [адаптер] |
          /flushdns | /displaydns /registerdns |
          /showclassid адаптер |
          /setclassid адаптер [устанавливаемый_код_класса_dhcp] ]
```

Где

адаптер — Полное имя или имя, содержащие подстановочные знаки "*" и "?" (* - любое количество знаков, ? - один любой знак). См. примеры

ключи:

/?	Отобразить это справочное сообщение.
/all	Отобразить полную информацию о настройке параметров.
/release	Освободить IP-адрес для указанного адаптера.
/renew	Обновить IP-адрес для указанного адаптера.
/flushdns	Очистить кэш разрешений DNS.
/registerdns	Обновить все DHCP-аренды и перерегистрировать DNS-имена
/displaydns	Отобразить содержимое кэша разрешений DNS.
/showclassid	Отобразить все допустимые для этого адаптера коды (IDs) DHCP-классов.
/setclassid	Изменить код (ID) DHCP-класса.

Работа утилиты

```
C:\>ipconfig /all

Настройка протокола IP для Windows

        Имя компьютера  . . . . . . . . . : os2006
        Основной DNS-суффикс  . . . . . . :
        Тип узла. . . . . . . . . . . . . : неизвестный
        IP-маршрутизация включена . . . . : нет
        WINS-прокси включен . . . . . . . : нет

VMware Network Adapter VMnet8 - Ethernet адаптер:

        DNS-суффикс этого подключения . . :
        Описание  . . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet8
        Физический адрес. . . . . . . . . : 00-50-56-C0-00-08
        Dhcp включен. . . . . . . . . . . : нет
        IP-адрес  . . . . . . . . . . . . : 192.168.6.1
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . :

VMware Network Adapter VMnet1 - Ethernet адаптер:

        DNS-суффикс этого подключения . . :
        Описание  . . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet1
        Физический адрес. . . . . . . . . : 00-50-56-C0-00-01
        Dhcp включен. . . . . . . . . . . : нет
        IP-адрес  . . . . . . . . . . . . : 192.168.50.1
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . :
```

Даже когда вы не предоставляете свои каталоги в общий доступ, то можете заметить, что в системе существуют так называемые "административные" ресурсы 'C$', 'D$', 'E$' и т.д., а также 'Admin$' и 'IPC$'. Они предназначены для удаленного администрирования компьютера. Даже если их удалить, то при следующей загрузке они появятся снова. Чтобы запретить их создание, в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters нужно установить равным "0" параметр типа REG_DWORD "AutoShareServer" для сервера или параметр "AutoShareWks" для рабочей станции.

Однако, этот метод не запретит создание ресурса IPC$, для этого нужно создать командный файл (BAT или CMD) файл со следующей строкой:

```
net share ipc$ /delete
```

и вставить запуск этого файла в Автозагрузку (кстати, таким же путем можно удалять и остальные ресурсы со знаком '$').

Если вы администрируете домен Windows NT/2000 или целую сеть вам понадобится информация о разделяемых ресурсах в домене/сети. В этом может помочь утилита ShareEnum Марка Русиновича.

Теперь поговорим о таком распространенном сетевом явлении, как перехват паролей на вход в сеть. Не секрет, что обычно эти пароли также являются и паролями на вход в Windows, поэтому их перехват аналогичен воровству SAM-файла и восстановлению из него паролей пользователей.

Ниже мы рассмотрим так называемую защищенную NT challenge/response (NTLM) аутентификацию, при этом процедура входа в сеть (если сетью управляет сервер) следующая:

- Компьютер передает серверу запрос об аутентификации пользователя.
- Сервер генерирует случайную 8-байтовую последовательность данных (так называемый "Challenge") и передает его компьютеру.
- Компьютер, получив Challenge, на основе его и пароля, который ввел пользователь с помощью функций хэширования генерирует LanMan Hash (а при отключении формирования LanMan Hash генерируется NT Hash). В этом случае длина хэша составляет уже 24 байта.
- Компьютер передает полученный хэш серверу.
- Сервер, в свою очередь, также генерирует хэш, используя те же входные данные (пароль, хранящийся на сервере и Challenge, который в пределах одной сессии одинаковый для сервера и для компьютера-клиента).
- Затем сервер сверяет оба полученных хэша и возвращает результат аутентификации.

При данной схеме избегается передача пароля в незашифрованном виде. Но, несмотря на это, по этим хэшам также можно восстановить пароли. Перехват хэшей может происходить с любого компьютера в сети, работающего под любой ОС и для этих целей используют программы LC4, PacketCatch, WinSniffer, NTSniffer и другие программы-"снифферы", т.е. программы, анализирующие сетевой трафик. Для восстановления же паролей к перехваченным хэшам обычно используются программы LC4, PacketInside и LC+4.

Для защиты от перехвата паролей используются следующие методы:

- Использование более защищенных методов аутентификации - NTLM v2 и Kerberos.
- Использование в структуре сети коммутаторов или же полноценных маршрутизаторов, тогда компьютер A (к примеру) физически не сможет перехватить пакеты, которыми обмениваются компьютер B и сервер C.

И, конечно же, обязательным условием для безопасной работы в сети является наличие файрволла. При грамотной настройке он практически на 100% защитит ваш компьютер от сетевых атак.

9. Безопасность прикладных программ/сервисов

Разумеется, безопасность Windows зависит не только от самой ОС, но и от программ/сервисов, которыми вы пользуетесь. Никакая защита Windows не поможет, если, к примеру, через уязвимость в Internet Explorer можно закачать себе троян или несанкционированно выполнить вредоносный код.

Не пользуйтесь Интернетом под аккаунтом Администратора - лучше создайте для этих целей отдельную учетную запись с правами обычного пользователя, чтобы попытки проникнуть на ваш компьютер через уязвимости браузеров или других интернет-утилит не принесли злоумышленнику успеха.

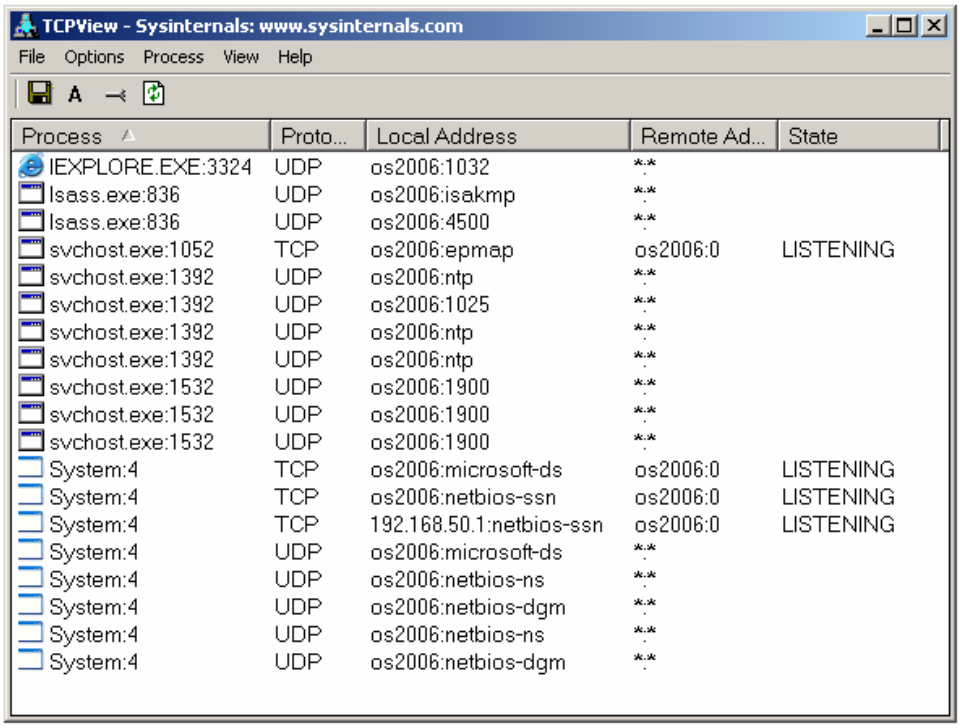
По возможности пользуйтесь только последними версиями программ, с которыми вы работаете, следите за обновлениями этих программ, устанавливайте все патчи, хотфиксы (hotfixes) и заплатки для Windows, Internet Explorer и др. программ, чтобы оперативно устранять возникающие уязвимости.

Пользуйтесь антивирусом, периодически скачивайте антивирусные базы, не запускайте скачанные из Интернета программы без проверки на вирусы и трояны, не запускайте файлы, полученные по почте, если только они не получены из очень надежного источника, файлы же от подозрительных отправителей вообще удаляйте сразу.

Настройте службы на вашем компьютере таким образом, чтобы работали только те сервисы, которые необходимы именно вам, в частности желательно запретить удаленное управление реестром, остановив одноименную службу.

Пользуйтесь возможностями шифрования данных средствами Windows 2000/XP с помощью EFS (Encrypting File System).

Для контроля служб(сервисов), используемых в вашей системе, вам понадобится средство аналогичное "netstat -ap" в Linux. К сожалению команда netstat в Windows не поддерживает эту опцию. Поэтому вам придется использовать ещё пару утилит Марка Русиновича - Tcpview (графическая утилита) и tcpvcon (утилита командной строки).




```
C:\>d:\tcpvcon.exe -ac
TCP,C:\WINDOWS\system32\svchost.exe,1052,LISTENING,os2006:epmap,os2006:0
TCP,System,4,LISTENING,os2006:microsoft-ds,os2006:0
TCP,System,4,LISTENING,os2006:netbios-ssn,os2006:0
TCP,System,4,LISTENING,os2006:netbios-ssn,os2006:0
UDP,System,4,,os2006:microsoft-ds,*:*
UDP,C:\WINDOWS\system32\lsass.exe,836,,os2006:isakmp,*:*
UDP,C:\WINDOWS\system32\lsass.exe,836,,os2006:4500,*:*
UDP,C:\WINDOWS\System32\svchost.exe,1392,,os2006:ntp,*:*
UDP,C:\WINDOWS\System32\svchost.exe,1392,,os2006:1025,*:*
UDP,C:\Program Files\Internet Explorer\iexplore.exe,3324,,os2006:1032,*:*
UDP,C:\WINDOWS\system32\svchost.exe,1532,,os2006:1900,*:*
UDP,C:\WINDOWS\System32\svchost.exe,1392,,os2006:ntp,*:*
UDP,System,4,,os2006:netbios-ns,*:*
UDP,System,4,,os2006:netbios-dgm,*:*
UDP,C:\WINDOWS\system32\svchost.exe,1532,,os2006:1900,*:*
UDP,C:\WINDOWS\System32\svchost.exe,1392,,os2006:ntp,*:*
UDP,System,4,,os2006:netbios-ns,*:*
UDP,System,4,,os2006:netbios-dgm,*:*
UDP,C:\WINDOWS\system32\svchost.exe,1532,,os2006:1900,*:*
```

10. Использование менеджера обновлений

В предыдущем разделе работы была предложена рекомендация - "По возможности пользуйтесь только последними версиями программ, с которыми вы работаете, следите за обновлениями этих программ, устанавливайте все патчи, хотфиксы (hotfixes) и заплатки для Windows, Internet Explorer и др. программ, чтобы оперативно устранять возникающие уязвимости.

Для автоматизации этого процесса необходимо использовать программы - менеджеры обновлений. В данной работе вам необходимо изучить работу с бесплатной компонентой - анализатором патчей (HFNetChk) менеджера обновлений от фирмы Shavlik Technologies. HFNetChk запускается в режиме командной строки и использует несколько способов получения списков обновлений - из Интернет или из локальных файлов уже полученных из репозитариев обновлений. Вам необходимо опробовать второй способ, так как при первом необходимо использовать подключение к Интернет.

Установите анализатор HFNetChk из самораспаковывающегося архива. Изучите его возможности. Определите требуемые обновления для вашей системы используя списки обновлений из файлов mssecure.cab или MSSecure.XML.

Опции данной утилиты

```
hfnetchk.exe [-trace] [-h hostname] [-i ipaddress] [-d domainname]
             [-n][-r range] [-history] [-t threads] [-b] [-ver]
             [-o output] [-x datasource] [-v] [vv] [-s suppression]
             [-nosum] [-sum] [-u username] [-p password] [-f outfile]
             [-proxy] [-pxip] [-pxpt] [-pxp] [-pxu] [-pxd] [-pxs] [-ms]
             [-fh hostfile] [-fip ipfile] [-about] [-fq ignorefile]

-h hostname    : Определяет NetBIOS имя машины для сканирования. Текущая машина - localhost
-i ipaddress   : IP адрес машины для сканирования
-r range       : Диапазон IP адресов машин для сканирования
```

-t threads : Число потоков при выполнении сканирования
-x datasource : Определяет xml источник содержащий hotfix информацию
-v verbose : Показывает подробную информация о патчах, которые не были найдены

Результат работы программы

```
C:\Program Files\Shavlik Technologies\HFNetChk>hfnetchk.exe -v -x d:\MSSecure.XML
Shavlik Technologies Network Security Hotfix Checker 3.86
Copyright (C) 2001-2002 Shavlik Technologies, LLC
Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com), 651-426-6624
All Rights Reserved
Attempting to load d:\MSSecure.XML.
================================================================
Scan performed Sat Nov 18 19:04:17 2006
Shavlik Technologies Network Security Hotfix Checker, 3.86
Using XML data version = 1.1.2.273  Last modified on 12/1/2004.
Scanning OS2006
..
Done scanning OS2006
---------------------------
OS2006 (192.168.50.1)
---------------------------

        * WINDOWS XP SP2

        Information
        All necessary hotfixes have been applied.

        * INTERNET EXPLORER 6 SP2

        Information
        There are no entries for Internet Explorer 6 SP2 in the XML file.

        * WINDOWS MEDIA PLAYER 6.4 GOLD

        Warning                 MS01-056        Q308567
        File C:\WINDOWS\system32\dxmasf.dll has a file version [6.4.9.1125]
        that is greater than what is expected [6.4.9.1121]. - File
        C:\WINDOWS\system32\msdxm.ocx has a file version [6.4.9.1130] that
        is greater than what is expected [6.4.9.1121].
```