Восстановление паролей пользователя из кэшированных записей домена

Passcape Software

1 Введение

Вам, наверное, должно быть известно, что операционные системы на базе Windows NT сохраняют, а точнее кэшируют, пароли пользователя на локальной машине. Это сделано для того, чтобы иметь возможность подключаться к серверу даже если логон сервер по каким-либо причинам недоступен. В этом случае, пользователь будет иметь доступ к сетевым ресурсам, которые не требуют доменной проверки.

2 Кэширование паролей в Windows NT

Говоря в общем и целом, операционные системы Windows NT используют два вида кэширования паролей:

1. Общее кэширование
2. Кэширование на уровне домена

Нас в данном случае, интересует последнее. Кэширование на уровне домена обеспечивает как минимум две функциональности:

- Доступ к ресурсам машины когда контроллер домена недоступен. К примеру, некий пользователь лэптопа использует учетную запись домена для входа в лэптоп, который присоединен к домену. Затем, пользователь перемещает свой лэптоп в такое место, где домен становится недоступен. В этом случае, Windows использует кэшированные данные для локального входа в систему и обеспечения доступа к локальным ресурсам компьютера.
- Single Sign-On (SSO) - функциональность, которая обеспечивает единократную сетевую аутентификацию, используя данные, полученные при первом интерактивном входе, и исключая их повторное введение.

Если кэширование домена отключено, то при попытке входа на сервер будет выдано сообщение:

The system can not log you on now because the domain **DOMAIN_NAME** is not available

Если контроллер домена недоступен и информация пользователя, необходимая для входа, сохранена в кэше, пользователь увидит диалог со следующим приглашением:

A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on may not be available.

3 Установка опций кэширования

Количество кэшируемых записей, хранящихся на стороне клиента
Редактируя реестр, можно самому устанавливать необходимое количество предыдущих попыток входа, которые будут кэшироваться операционной системой. Это значение может варьироваться от 0 до 50. Причем если задать 0, то кэширование будет отключено. По умолчанию Windows запоминает 10 предыдущих входов. Кэширование контролируется следующим ключом реестра:

Ключ реестра:	**HKLM\Software\Microsoft\Windows NT\Current Version\Winlogon**
Имя параметра:	**CachedLogonsCount**
Тип данных:	**REG_SZ**
Значения:	**0 - 50**

Уведомление о входе при использовании кэшированных записей
Если вы попытаетесь подключиться к домену (используя рабочую станцию на базе Windows) и контроллер домена будет недоступен, вы не увидите сообщений об ошибке, поэтому, возможно, не заметите, что вошли используя кэш домена. Если вы хотите настроить Windows так, чтобы каждый раз при входе с кэшированными паролями показывалось соответствующее предупреждение, установите следующие два ключа реестра:

Ключ реестра:	**HKLM\SOFTWARE\Microsoft \Windows NT\CurrentVersion\Winlogon**
Имя параметра:	**ReportControllerMissing**
Тип данных:	**REG_SZ**
Значение:	**TRUE**

Затем, для каждого пользователя системы:

Ключ реестра:	**HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon**
Имя параметра:	**ReportDC**
Тип данных:	**REG_DWORD**
Значение:	**1**

4 Безопасность кэширования паролей домена

Термин *'кэшированные пароли домена'* не отражает в полной мере того, как Windows кэширует и хранит приватную информацию. Начиная с Windows 2000, имя пользователя и пароль не хранятся в явном виде. Напротив, система хранит хэш пароля, слегка модифицированный при помощи соли (т.е. salted hash), которая в свою очередь генерируется на основе имени пользователя в формате юникод.

Если потенциальный хакер попытается проделать простейший криптоанализ, то, по утверждению Microsoft, из данного алгоритма шифрования можно вывести следующие выводы:

- Предварительные таблицы (precompiled tables) должны быть созданы для каждой соли.

- Хэш не может быть использован для входа в другую систему.

Если подойти к этому с другой стороны, то может оказаться что:

- Можно создать предварительные таблицы для алиасов, т.е. для уже известных имен, например для встроенного администратора или гостя. С другой стороны, это, возможно, будет пустой тратой времени, потому что кэшированные записи встроенного админа, как бы это сказать, встречаются не часто.
- Чтобы в полной мере исключить возможность входа в другую систему, необходимо было пароль наряду с именем пользователя, посолить еще и именем домена.

5 Потенциальные атаки на кэшированные пароли домена

Потенциальный злоумышленник для доступа к компьютеру может добавить новый или переписать хэш своим собственным значением. Процедура подразумевает физический доступ к компьютеру. Единственная утилита на сегодняшний день, которая позволяет переписывать или менять хэш на свое собственное значение, - Network Password Recovery Wizard.

Однако, простое переписавание/замена кэшированного пароля не дает потенциальному злоумышленнику доступ к зашифрованным файлам, к приватным данным, зашифрованным при помощи DPAPI (например, пароли Internet Explorer, Outlook, Windows Mail, WPA и т.д.).

6 Кэширование паролей домена - взгляд изнутри

Кэшированные записи домена хранятся в зашифрованном виде в реестре Windows в ветке реестра **HKEY_LOCAL_MACHINE\SECURITY\Cache**. Двоичное значение с именем **NL$x** - соответствуют одной кэшированной записи. Где x - номер записи. Доступ к этой вестке реестра имеет только система. Каждая запись содержит:

- Расширенную информацию о пользователе. А именно: его краткое и полное имя, последнее время доступа, идентификатор в системе, имя домена, имя днс домена, домен входа, скрипт, путь к профилю пользователя, домашний каталог, диск домашнего каталога, членство в группах и др.
- Приватную информацию, которая состоит и хэша пароля, дополнительных секретах и счетчика итераций Pbkdf2 (для Windows Vista и, возможно, более поздних операционных систем)

В шифровании кэшируемых записей домена принимает участие LSA секрет с именем **NL$KM**, который хранит в себе 64 байтный мастер ключ, привязанный к локальной системе. NL$KM располагается в файле реестра SECURITY и в свою очередь тоже зашифрован при помощи SYSKEY.

Таким образом, общая схема расшифровки записи домена выглядит так:

1. SYSKEY + LSA Master Key + NL$KM = DCP Master Key
2. DCP Master Key + NL$x entry = Decrypted DCP entry

После расшифровки кэшированной записи домена мы получаем доступ к хэшу пользователя.

Вкратце, алгоритм шифрования пароля можно описать вот таки образом.
Для Windows 2000-2003: hash = **MD4** (**MD4**(user password) + lowercase(user name))

Начиная с Windows Vista алгоритм свертки пароля немного изменился. Теперь он поставлен в многотысячный цикл и скорость перебора должна быть даже меньше, чем у WPA-PSK:
h = **MD4** (**MD4**(user password) + lowercase(user name))
hash = **PBKDF2_SHA**(h, iterations)

По умолчанию, значение iterations равно 10240. Заметьте, что количество SHA проходов будет в несколько раз больше этого значения.

7 Практическое руководство по восстановлению паролей пользователей

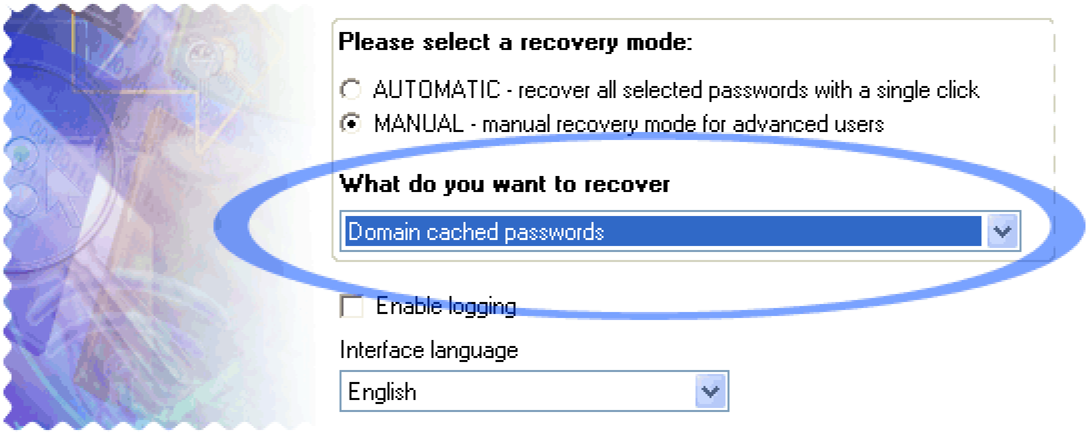
Для работы нам потребуется лишь один инструмент - программа Network Password Recovery Wizard в последней версии которой добавилась поддержка восстановления кэшированных записей. Разобьем условно всю работу на три части:

1. Расшифровка кэшированных записей домена
2. Анализ полученных данных
3. Восстановление пароля выбранной записи

Итак, приступим.

1. Расшифровка кэшированных записей домена

Запускаем программу и из выпадающего меню выбираем, что мы хотим восстановить: Domain Cached Passwords. Если кэшированные записи находятся на локальном компьютере, смело выставляем автоматический режим и вперед.



Please select a recovery mode:

○ AUTOMATIC - recover all selected passwords with a single click

● MANUAL - manual recovery mode for advanced users

What do you want to recover

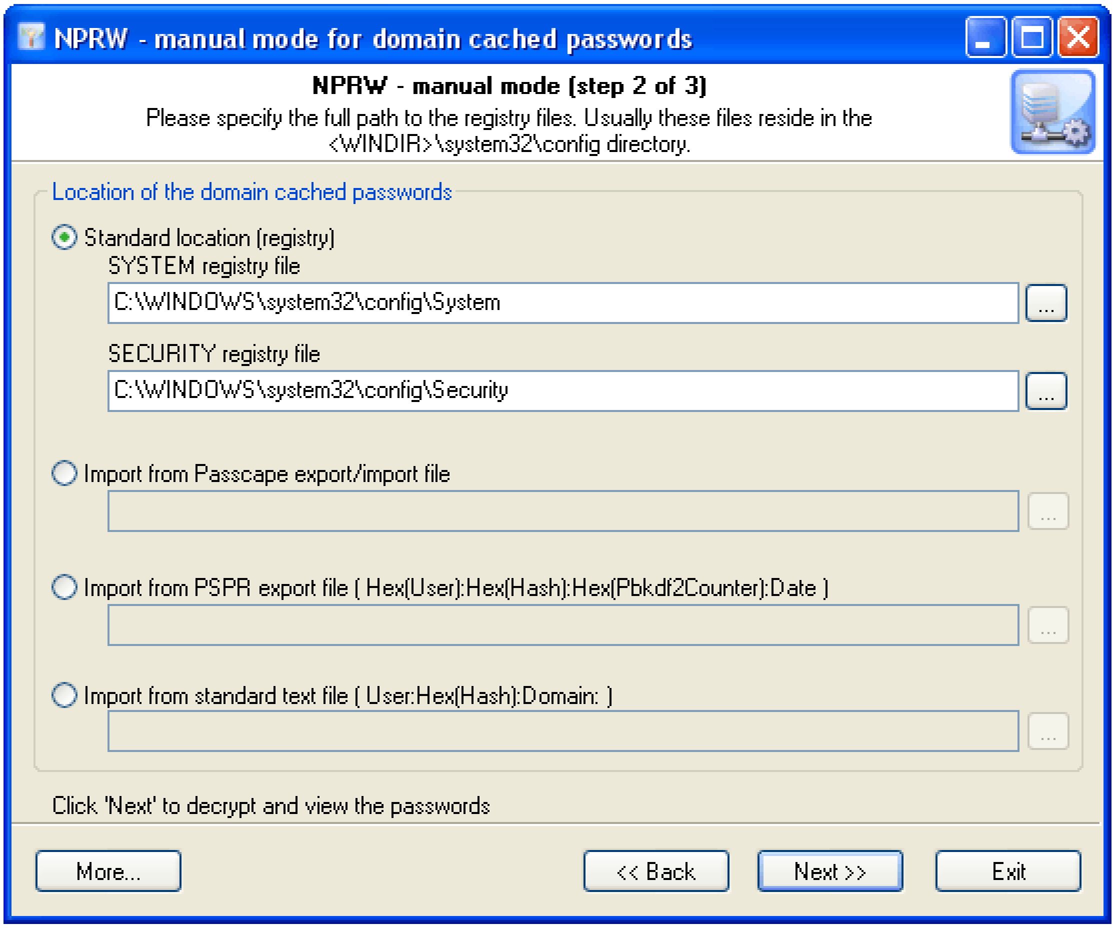
Domain cached passwords

□ Enable logging

Interface language

English

Ручной режим работы более гибкий и предоставляет пользователю самому выбрать источник исходных данных, будь-то стандартное размещение (файлы реестра), родной файл экспорта/импорта Passcape или же из файл импорта, используемый в других программах.



NPRW - manual mode (step 2 of 3)

Please specify the full path to the registry files. Usually these files reside in the <WINDIR>\system32\config directory.

Location of the domain cached passwords

● Standard location (registry)

SYSTEM registry file

C:\WINDOWS\system32\config\System

SECURITY registry file

C:\WINDOWS\system32\config\Security

○ Import from Passcape export/import file

○ Import from PSPR export file (Hex(User):Hex(Hash):Hex(Pbkdf2Counter):Date)

○ Import from standard text file (User:Hex(Hash):Domain:)

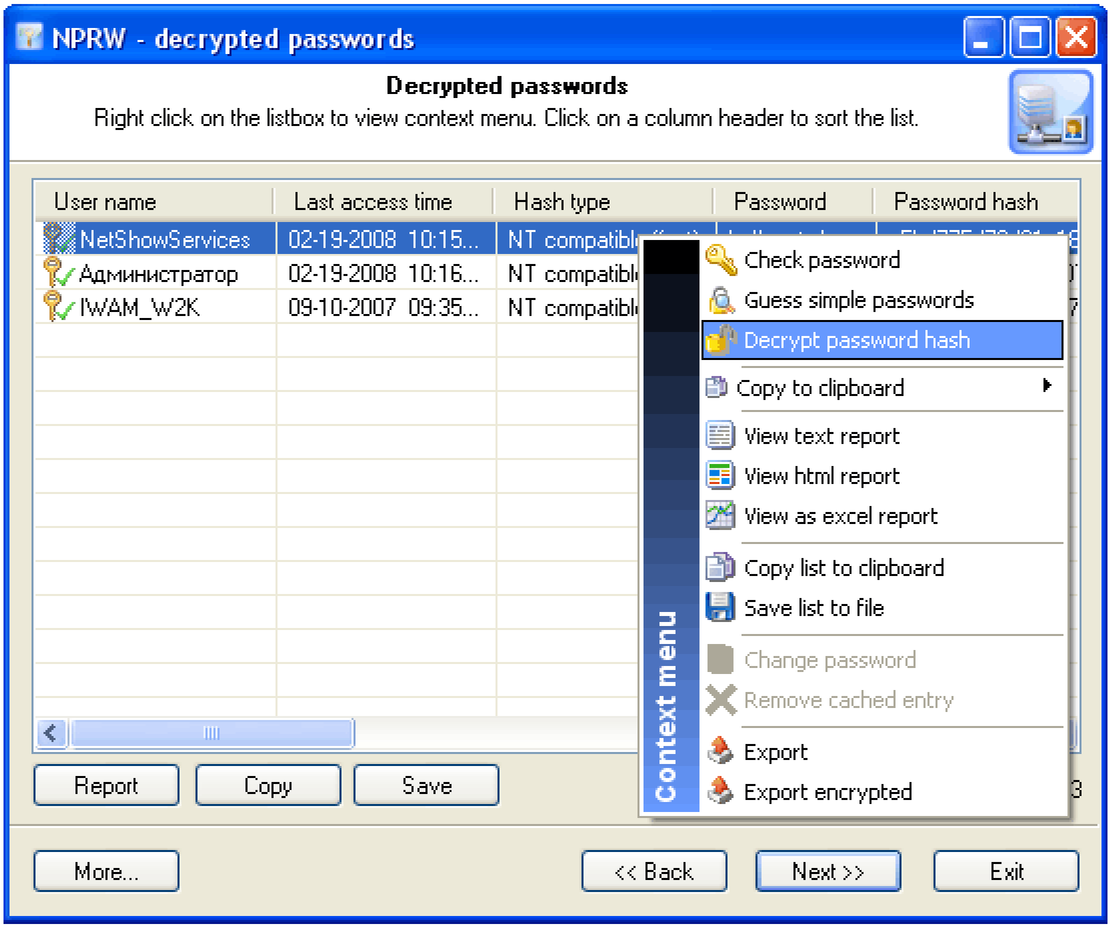
Click 'Next' to decrypt and view the passwords

Жмем '*Далее*' и ждем результатов обработки.

2. Анализ полученных данных

При удачной расшифровке или импорте данных, пользователю будет предложен список расшифрованных записей. Каждая запись имеет несколько полей. Например, имя пользователя, сервер, членство в группах и т.д.

Вызов контекстного меню правой кнопкой мыши позволяет задействовать расширенные возможности программы. Для всего списка: скопировать, сохранить, просмотреть отчет или экспортировать весь список. Для отдельной записи: сменить пароль, удалить запись, проверить пароль, угадать пароль, перебирая простейшие и часто встречаемые комбинации, или запустить полноценную атаку.



NPRW - decrypted passwords

Decrypted passwords

Right click on the listbox to view context menu. Click on a column header to sort the list.

User name	Last access time	Hash type	Password	Password hash
NetShowServices	02-19-2008 10:15...	NT compatibl		
Администратор	02-19-2008 10:16...	NT compatibl		
IWAM_W2K	09-10-2007 09:35...	NT compatibl		

Перед запуском атаки на пароль выбранной записи, обратите внимание на два поля. Это поле *'Password'* и *'Hash type'*. Иногда кэшированный пароль можно найти не прибегая к полной атаке. В этом случае, если программа нашла пароль, он будет находиться в поле *'Password'*, а сама запись помечена соответствующей иконкой

Поле *'Hash type'* содержит тип хэша пароля, который может быть *'NT compatible instant'* - мгновенная расшифровка, *'Win2K compatible fast'* - быстрое восстановление со скоростью несколько миллионов паролей в секунду или *'Vista, slow'* - скорость восстановления всего лишь несколько сот паролей в секунду на современном компьютере.

3. Восстановление пароля выбранной записи

Итак, для начала восстановления пароля выбранной записи, щелкаем на ней правой кнопкой мыши и из контекстного меню выбираем *'Decrypt password hash'*. Появится диалог с выбором метода расшифровки, стандартный для всех программ Passcape Software. Нет смысла описывать все типы атак, более подробную информацию можно найти на страницах, посвященных расшифровке паролей Opera или Мастер Пароля Firefox.

Неискушенный пользователь может задаться вполне справедливым и логичным вопром: "100% гарантии восстановления нет, методов много, с какой атаки лучше начать для повышения вероятности ее успешного завершения?".

Для выбора типа и последовательности атак, рекомендуем использовать следующий алгоритм, который применим в большинстве случаев ко всем типам паролей:
Во-первых, включите опцию предварительной атаки, если она есть. Она поможет восстановить простые и часто встречающиеся комбинации.
Во-вторых, если вам известно что-либо об искомом пароле, лучше вначале запустить атаку по маске, либо атаку по ключевому слову. Причем, если вам известна часть пароля, лучше использовать атаку по маске. Если вы знаете базовую составляющую пароля или, к примеру, знаете слово пароля, но забыли последовательность заглавных и строчных букв, то вам в первую очередь подойдет атака по ключевому слову.

Если никакой информации об искомом пароле нет, а так чаще всего и бывает, руководствуйтесь следующей последовательностью действий:

1. запуск интеллектуальной атаки с минимальной мутацией и индексацией
2. повтор интеллектуальной атаки с установленными опциями мутации паролей и индексации в light и normal соответственно
3. запуск атаки по словарю без включенной опции мутации
4. запуск атаки по словарю с включенной опции мутации, степень мутации зависит от наличия свободного времени и скорости атаки. Для поиска паролей, набранных в национальной раскладке, необходимо выставить опцию сильной мутации.
5. выбор и загрузка онлайн словарей и повтор шагов 3 - 4
6. запуск атаки по фразе без включенной опции мутации
7. запуск атаки по фразе с включенной опции мутации, установленной на максимальную эффективность. Это позволит найти пароли, набранные в национальной раскладке клавиатуры.
8. выбор и загрузка онлайн словарей фраз и повтор шагов 6 - 7
9. запуск комбинированной атаки по словарям с заданными правилами генерации фраз
10. выбор и загрузка онлайн словарей для комбинированной атаки повтор шага 9
11. выбор чарсета для атаки полным перебором, запуск перебора
12. при необходимости, выбор нового или дополнение старого набора символов и повтор атаки грубой силой, т.е. шага 11.

Шаги 1-2 - поиск паролей, хранящихся локально в вашей системе.
Шаги 3-5 - поиск паролей, состоящих из одного слова.

Шаги 6-10 - поиск паролей, состоящих из нескольких слов.
Шаги 11-13 - полный перебор.

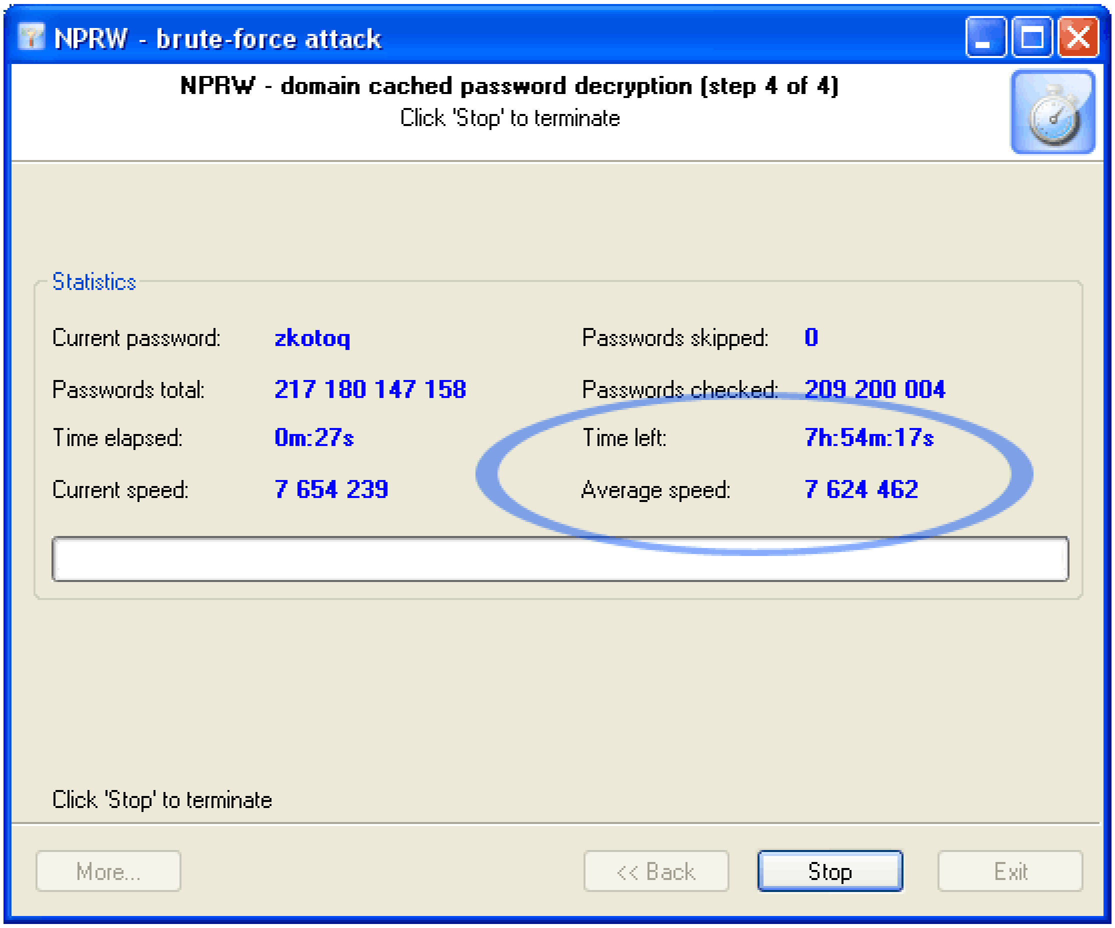
8 Заключение

Конечно, если скорость атаки составляет миллионы паролей в секунду, как в случае с Windows 2000 совместимыми паролями домена (помните поле *'Hash type'* в списке кэшированных записей?), можно воспользоваться преимуществами всех видов атак в полной мере. Однако, при переборе хэшей от Windows Vista, со скоростью всего лишь в пару сотен паролей, трудно всерьез рассчитывать на что-то, кроме атаки по словарю.

Давайте посмотрим на примере, сколько потребуется времени для проведения атаки перебором и нахождения простейшего восьмисимвольного пароля в том и другом случае. Итак, чтобы перебрать весь диапазон символов a..z, нам потребуется проверить ни много ни мало - 217 180 147 158 паролей.

Теперь смотрим тайминги.

Восстановление кэшированных хэшей Windows 2000, XP, 2003



NPRW - brute-force attack

NPRW - domain cached password decryption (step 4 of 4)

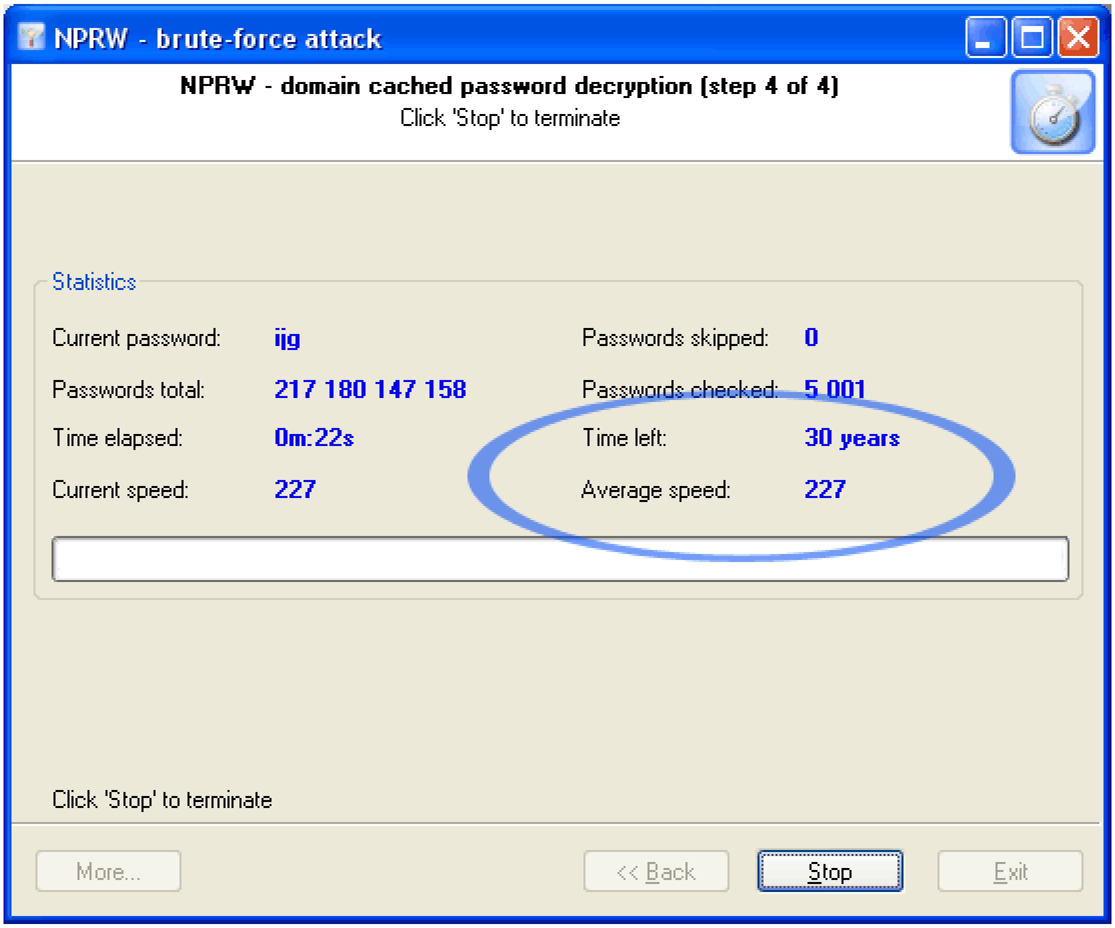
Click 'Stop' to terminate

Statistics

Current password:	zkotoq	Passwords skipped:	0
Passwords total:	217 180 147 158	Passwords checked:	209 200 004
Time elapsed:	0m:27s	Time left:	7h:54m:17s
Current speed:	7 654 239	Average speed:	7 624 462

Click 'Stop' to terminate

Восстановление кэшированных хэшей Windows Vista



NPRW - domain cached password decryption (step 4 of 4)
Click 'Stop' to terminate

Statistics

Current password: ijg
Passwords total: 217 180 147 158
Time elapsed: 0m:22s
Current speed: 227
Passwords skipped: 0
Passwords checked: 5 001
Time left: 30 years
Average speed: 227

Click 'Stop' to terminate

9 Приложение

Алгоритм проверки хэша пароля кэшированной записи в Windows 2000, XP, 2003:

```
BOOL CheckCachedDomainPassword(LPCTSTR cszUserName, LPCTSTR cszPassword, BYTE
pCheckHash[0x10])
{
   WCHAR wsz[256];
   BYTE pHash[0x10];
   INT iLen;

   iLen=strlen(cszPassword);
   MultiByteToWideChar(CP_ACP,MB_PRECOMPOSED,cszPassword,iLen,wsz,256);
   Md4Init();
   Md4Update((LPBYTE)wsz,iLen*2);
```

```
    Md4Final(pHash);

    iLen=strlen(cszUserName);
    MultiByteToWideChar(CP_ACP,MB_PRECOMPOSED,cszUserName,iLen,wsz,256);
    CharLowerW(wsz);
    Md4Init();
    Md4Update(pHash,0x10);
    Md4Update((LPBYTE)wsz,iLen*2);
    Md4Final(pHash);

    return ( memcmp(pCheckHash,pHash,0x10)==0 );
}
```