Windows NT中的密码缓存

Passcape Software

1 介绍

你可能已经知道，基于Windows NT的操作系统在本地机器上存储或更准确地说，缓存域账户的密码。这样做是为了让用户在登录服务器因某种原因无法使用时也能登录他们的账户。在这种情况下，用户将可以访问任何不需要用户验证的网络资源。

2 Windows NT中的密码缓存

Windows NT operating systems use two general types of password caching:

- General caching
- Domain-level caching

The domain-level caching provides at least two functionalities:

1. Provide access to computer resources even if a domain controller is not available. For example, on a laptop user logs on to his domain account. Then the user moves the laptop to a place where the domain is not available. In such a case, Windows would use cached data for logging on to the system locally and ensuring access to the local resources of the computer.
2. Single Sign-On (SSO) - the functionality carries out a one-time network authentication using data obtained during the first interactive sign-on and excluding the reentering of it.

If the domain caching is disabled, an attempt to logon to the server should cause the following message:

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

If the domain controller is not available, the system uses data saved in a cache previously. So the prompt message will look a bit differently:

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 设置缓存选项

存储在客户端的缓存凭证的数量

通过编辑Windows注册表，你可以手动设置所需的登录尝试次数，以便按操作系统进行缓存。该值可能在0到50之间变化。如果该值被设置为0，缓存将被禁用。默认情况下，Windows存储10次成功的登录尝试。缓存是通过以下注册表键控制的：

Key name: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon**
Value name: **CachedLogonsCount**
Data Type: **REG_SZ**

Values: **0 - 50**

关于使用域缓存密码的通知
默认情况下，如果你试图连接到一个域（使用基于Windows的工作站），而域控制器是不可用的，你将不会看到任何警告信息，因此，几乎不会注意到已经使用缓存的凭证登录。如果你想把Windows配置成每次使用缓存密码登录时都会显示相应的警告，请设置这两个注册表键：

Key name: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows NT\CurrentVersion\Winlogon**
ValueName: **ReportControllerMissing**
Data Type: **REG_SZ**
Values: **TRUE**

然后针对系统的每个用户：

Key name:
HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
ValueName: **ReportDC**
Data Type: **REG_DWORD**
Values: **1**

4 域名缓存证书的安全性

术语 "域缓存凭证 "并不能完全反映Windows缓存和存储私人信息的方式。从Windows 2000开始，用户密码不以明文形式存储。相反，系统存储的是密码哈希值，用盐稍作修改（即盐化哈希值），其中盐是Unicode格式的用户名称。

微软声称，从这种加密算法可以得出以下结论：
- 预计算表不适用，因为使用的是盐化哈希值
- DCC哈希值不能用于在其他系统上签名

从另一个角度来探讨这个问题可能会发现：
- 可以为别名创建预计算表，即为已知的用户名创建预计算表；例如，为内置的管理员或访客账户创建预计算表。另一方面，这可能会变成浪费时间，因为内置的管理员或访客账户并不经常启用，说得不好听一点就是。
- 为了完全消除登录到其他系统的可能性，域名也应该和用户名一起添加。

5 对域名缓存密码的潜在攻击

一个潜在的坏人，为了获得对计算机的访问权，可以很容易地添加一个新的或用他自己的值覆盖一个现有的哈希值。这个过程假定了对计算机的物理访问。

然而，仅仅改写或替换缓存密码并不能让潜在的恶意攻击者访问私人用户数据、加密文件、受DPAPI保护的数据（Internet Explorer、Outlook、Windows Mail、WPA密码和其他数据）。

6 域名缓存的证书--从内部来看

域缓存数据被加密存储在Windows注册表的以下位置。
HKEY_LOCAL_MACHINE\SECURITY\Cache。二进制值NL$x表示单个缓存记录，其中'x'代表记录编号。对这个注册表键的访问只授予系统。

每条记录包含：

- 关于用户的扩展信息。即：用户的短名和全名，最后一次访问的时间，系统中的标识符，域名，域名的DNS名称，登录域，脚本，用户配置文件的路径，主目录，主目录驱动器，组中的成员，等等。
- 私人信息，包括密码哈希值、额外的秘密和Pbkdf2迭代计数器（在Windows Vista及以后的操作系统中用于加密）。

域缓存数据的加密涉及LSA秘密NL$KM，它持有绑定到本地系统r的64字节主密钥。NL$KM位于SECURITY注册表文件中，反过来，它也是用SYSKEY加密的。

因此，整个域名记录解密方案看起来是这样的：

- SYSKEY + LSA Master Key + NL$KM = DCC Master Key
- DCC Master Key + NL$x entry = Decrypted DCC entry

一旦缓存的域名条目被解密，我们就能获得用户账户的加盐哈希值。加盐的哈希值可以用来猜测明文登录密码。

对于Windows 2000-2003: hash = MD4 (MD4(用户密码) + lowercase(用户名))

从Windows Vista开始，加密算法有了一些变化。现在，它是用SHA-1哈希值的额外迭代来执行的。

hash = PBKDF2_SHA(MD4 (MD4(user password)+lowercase(user name)), iterations)

默认情况下，迭代计数器等于10240。

7 恢复域缓存凭证的实用指南

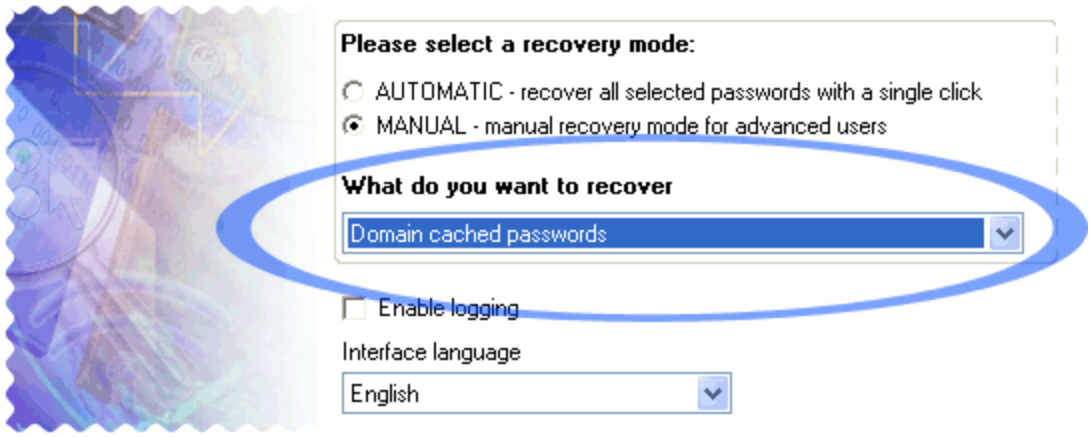
在整个恢复过程中，我们需要的唯一工具是 Network Password Recovery Wizard. 让我们将整个工作流分为三部分：

1. 域缓存记录的解密
2. 解密记录的分析
3. 所选条目的密码恢复

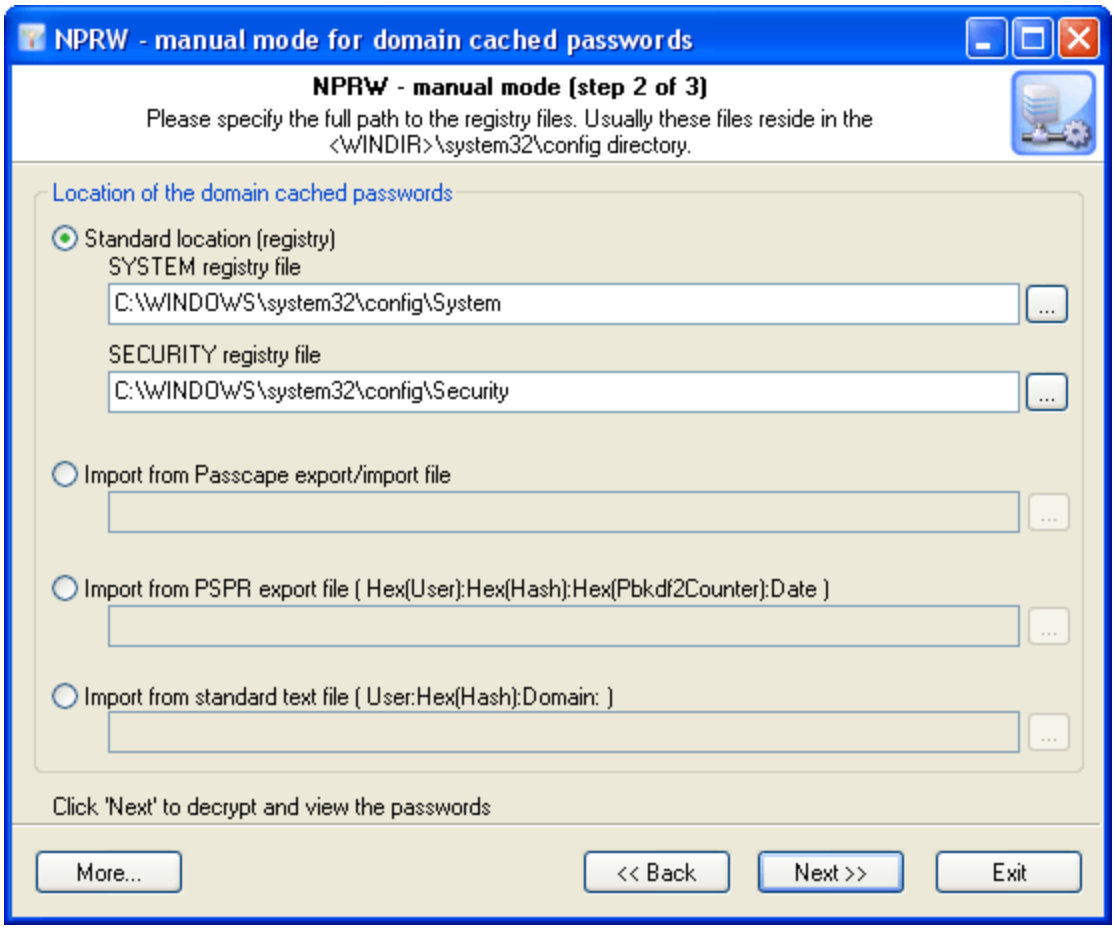
所以，让我们开始吧。

1.域缓存记录的解密

启动应用程序，从下拉菜单中选择要恢复的内容：域缓存密码。如果缓存的记录在本地计算机上，请自信地启动自动模式并继续。



手动操作模式更加灵活，允许用户手动选择数据源，无论是标准位置（注册表文件）、Passcape的本地导入/导出文件还是从其他程序导入的数据。

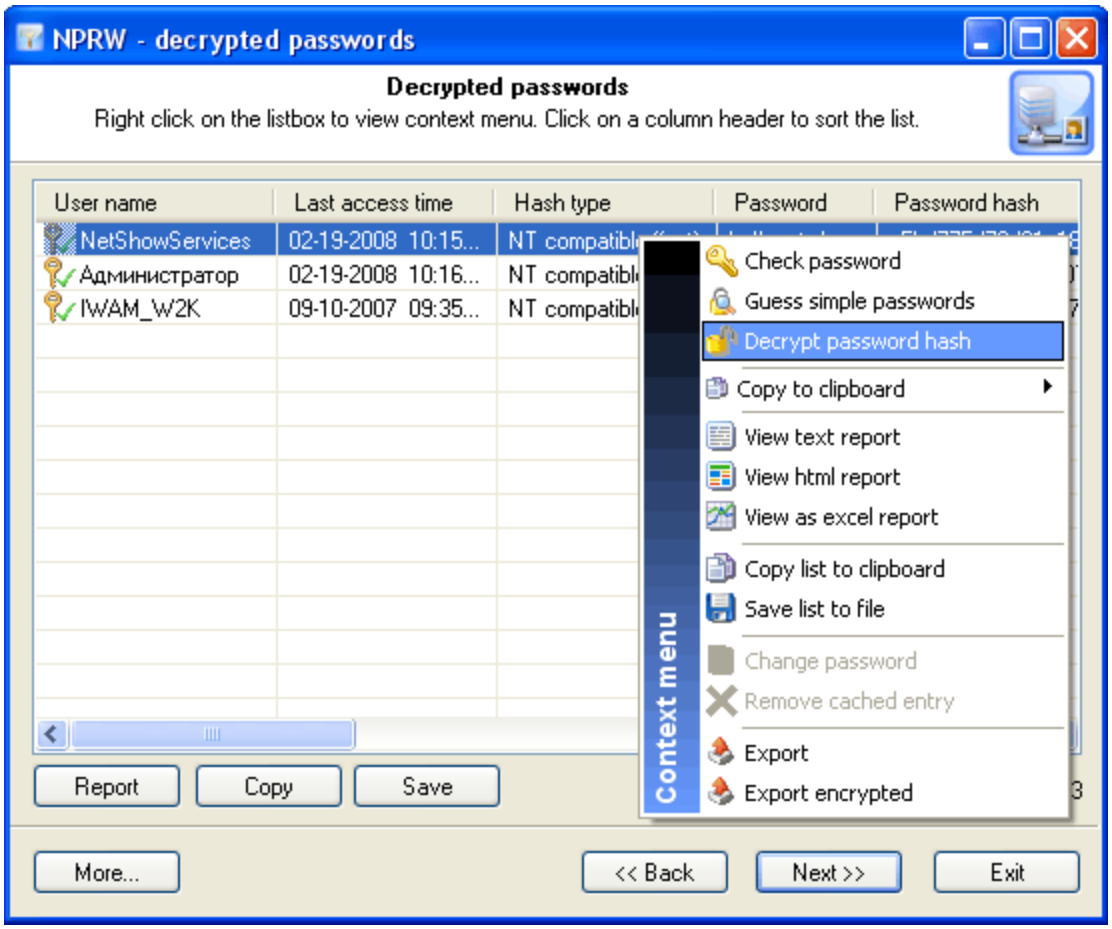


单击“下一步”，等待程序完成输入数据的处理。

2.解密记录的分析

成功解密并导入凭据后，用户应获得解密记录的列表。每个记录有几个数据字段；例如，用户名、服务器、组成员等。

通过右键单击打开上下文菜单，可以使用程序的扩展功能。对于整个列表：复制、保存、查看报告或导出整个列表。对于单个记录：更改密码、删除记录、验证密码、通过搜索简单和常用的组合恢复密码，或发起全面攻击。



在对所选密码发起攻击之前，请注意这两个字段："密码"和"哈希类型"。有时，不使用完全可扩展的攻击，而是启动简单的攻击，就可以轻松猜测缓存的密码。在这种情况下，明文密码将显示在"密码"字段中，记录将标记相应的图标。

"哈希类型"字段包含密码哈希类型，可以是以下三种类型之一："NT兼容即时"-即时恢复，"Win2K兼容快速"-以每秒数百万密码的速度快速恢复或"Vista，慢速"-在现代计算机上，恢复速度仅为每秒数百个密码。

3.所选条目的密码恢复
因此，要开始所选记录的密码恢复，请右键单击它，然后在上下文菜单上选择“解密密码哈希”。这将打开“解密方法”对话框。描述所有类型的攻击是没有意义的。有关详细信息，请参阅程序手册。

不熟练的用户可能会问一个完全合理且连贯的问题：“虽然有很多方法，但无法100%保证恢复。应该发起哪种攻击来提高成功完成的概率？”

为了选择攻击的类型和顺序，我们建议遵循该算法，该算法适用于大多数情况下的广泛密码类型
- 首先，启用 初步攻击 选项（如果可用）。它有助于恢复简单和常用的组合。
- 第二，如果您知道您正在寻找的密码的任何细节，最好先尝试 掩码攻击 或 基字攻击 具体来说，如果您知道密码的一部分，那么使用掩码攻击将更有效。如果您知道密码的基本组成部分，或者，例如，您知道密码，但不记得密码中的大写和小写字符序列，则基字攻击会更好地完成此任务。

如果您没有关于您要查找的密码的信息，请遵循以下步骤：
1. 运行AI攻击，将突变和索引选项设置为最小。
2. 如果找不到密码，请重试并将突变选项设置为“正常”级别，并将索引设置为“深度”。
3. 在禁用突变选项的情况下启动字典攻击。
4. 启用突变选项时启动字典攻击；变异的深度取决于可用时间和攻击速度。搜索在国家键盘布局中键入的密码时，应将突变深度设置为“强”。
5. 选择并下载在线词典，并重复步骤3-4。
6. 在禁用突变选项的情况下启动通行短语攻击。
7. 启用突变选项并将其设置为最大生产力，启动通行短语攻击。这将允许猜测在国家键盘布局中键入的密码。
8. 选择并下载在线通行短语词典，并重复步骤6-7。
9. 使用短语生成规则启动组合字典攻击。
10. 选择并下载用于组合攻击的在线词典，然后重复步骤9。
11. 选择暴力攻击的字符集，启动攻击。
12. 如有必要，选择新角色集或完成旧角色集，并重复暴力攻击；例如.步骤11。

步骤1-2-扫描本地系统的明文密码。
步骤3-5-提取单字密码。
步骤6-10-生成多字密码。
步骤11-12-穷举搜索。

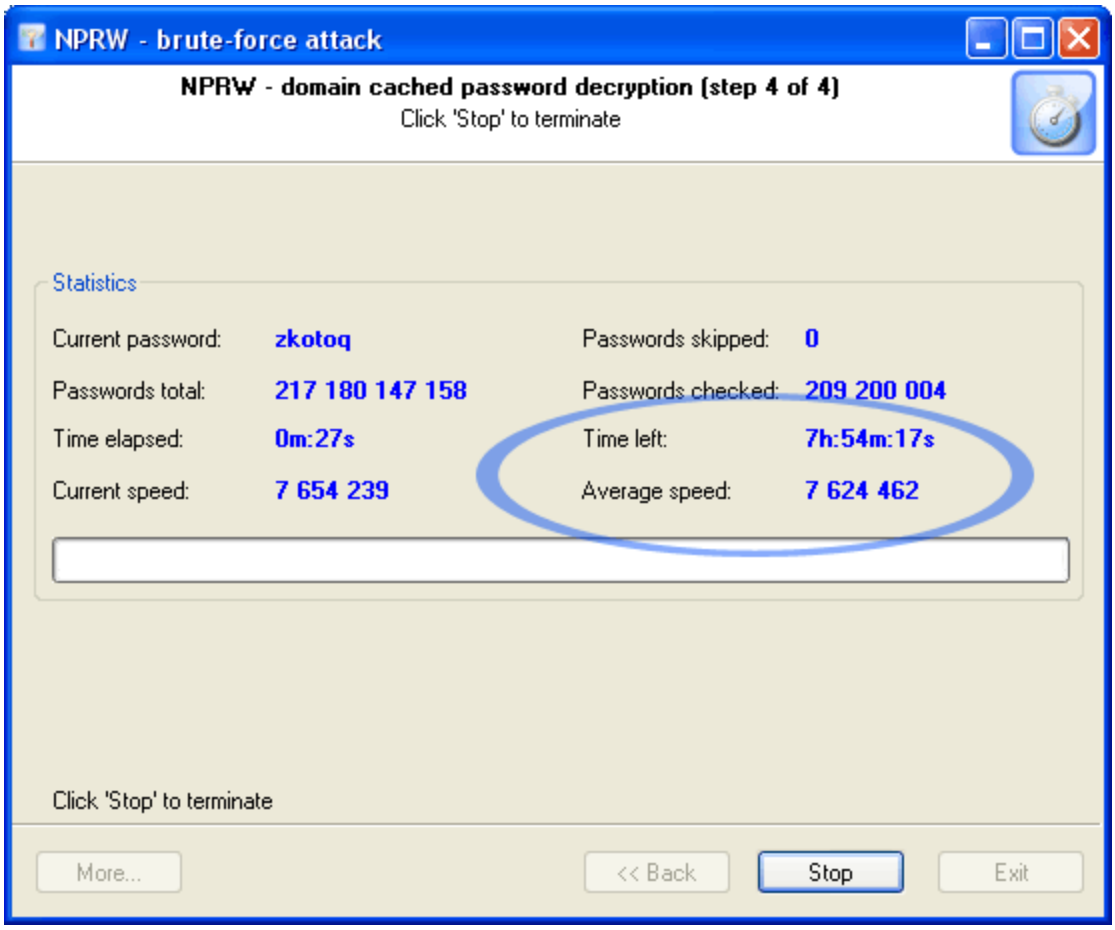
8 结束语

在解密Windows 2000域缓存凭据时，您可以充分利用各种攻击。然而，在恢复与Windows Vista兼容的域缓存时，除了字典攻击之外，很难认真考虑其他攻击。

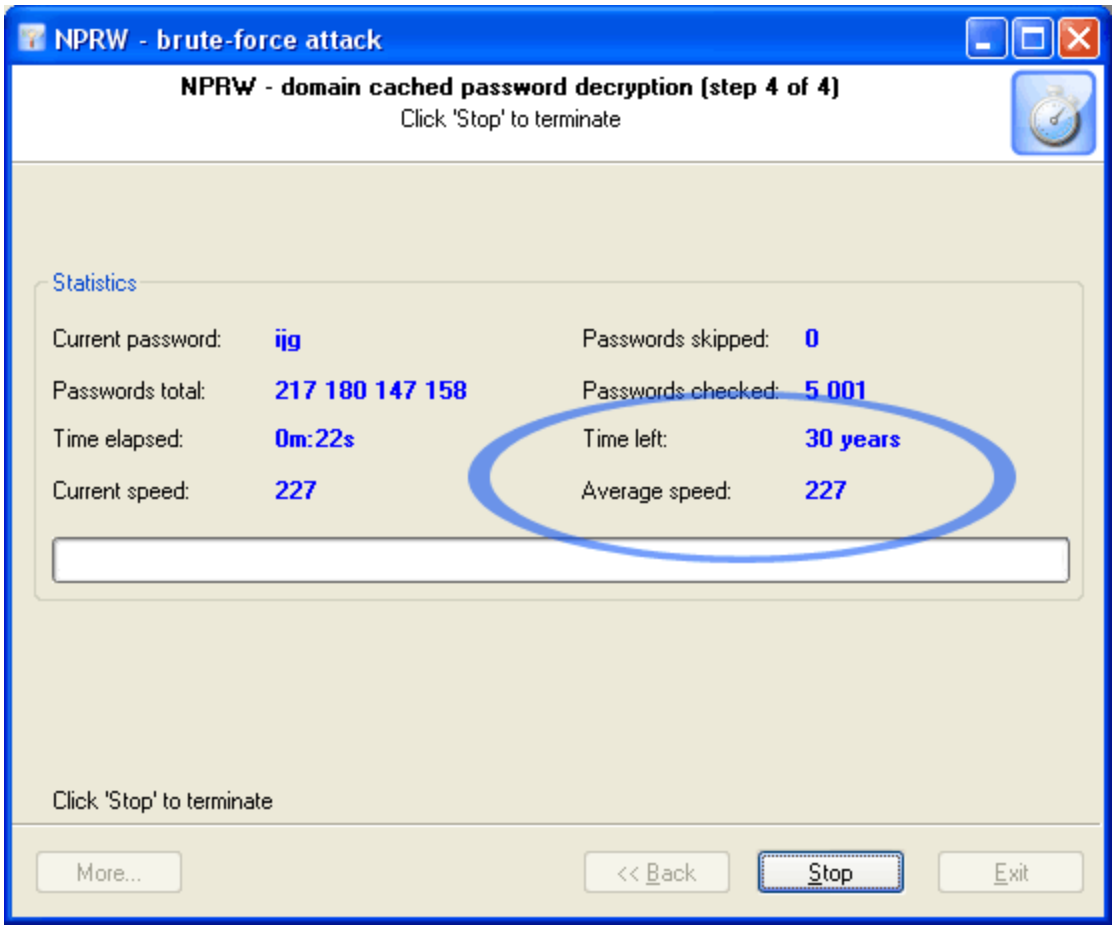
让我们计算一下在这两种情况下完成彻底搜索并恢复一个简单的八字符密码需要多长时间。要搜索整个a..z字符范围，我们需要验证的密码组合不是太多，也不是太少，而是217 180 147 158。

现在，让我们看看时间。

恢复Windows 2000、XP和2003域缓存凭据



恢复Windows Vista缓存凭据



9 附录

C++ algorithm for validating domain cached password in 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 );
}
```