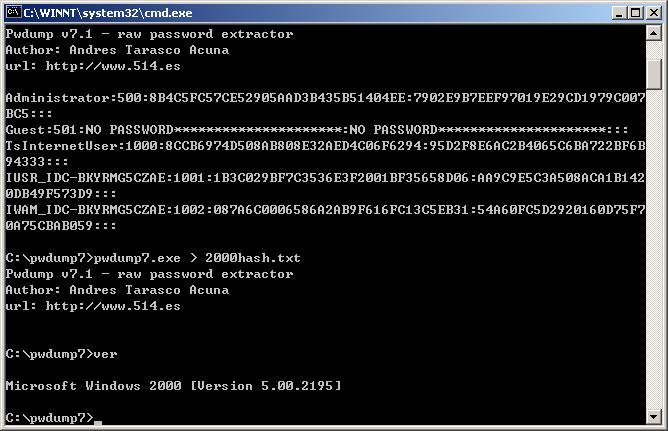
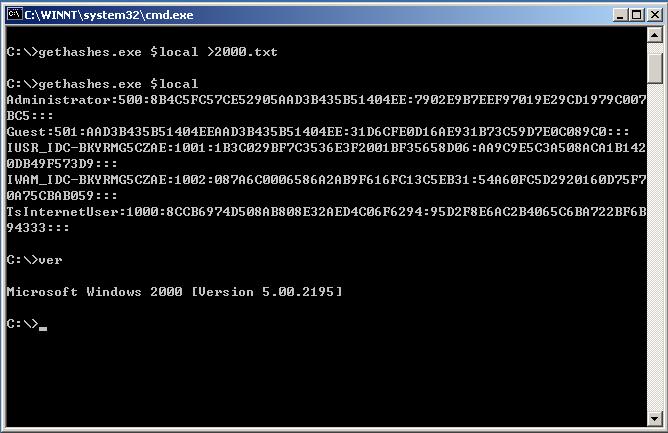
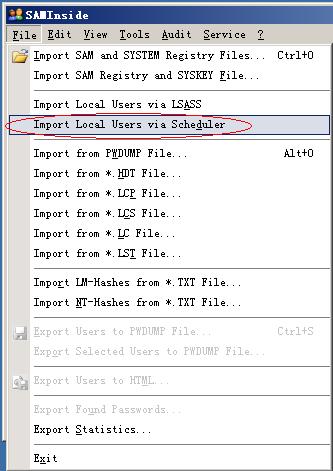
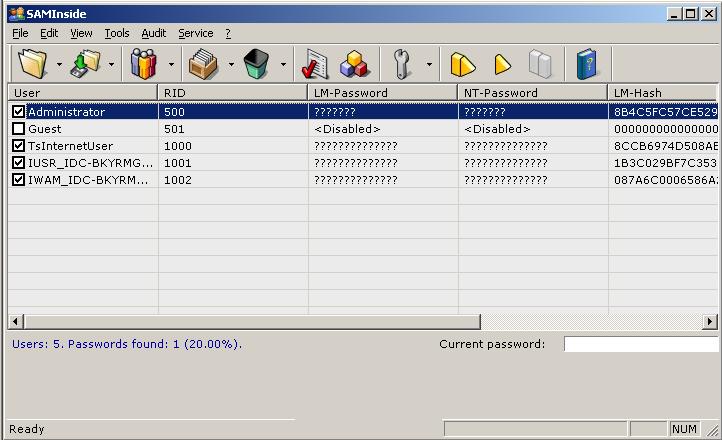
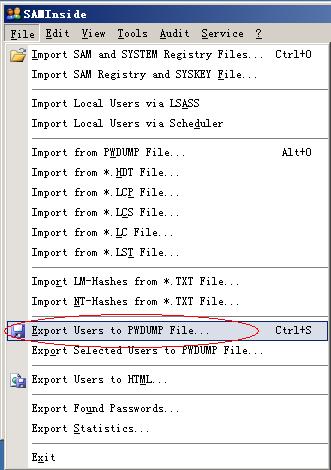
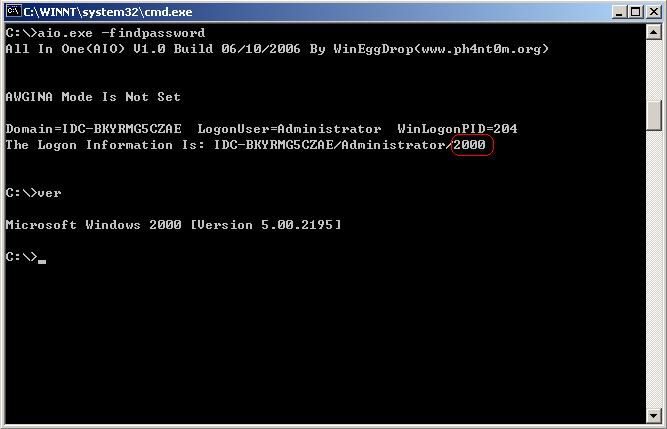
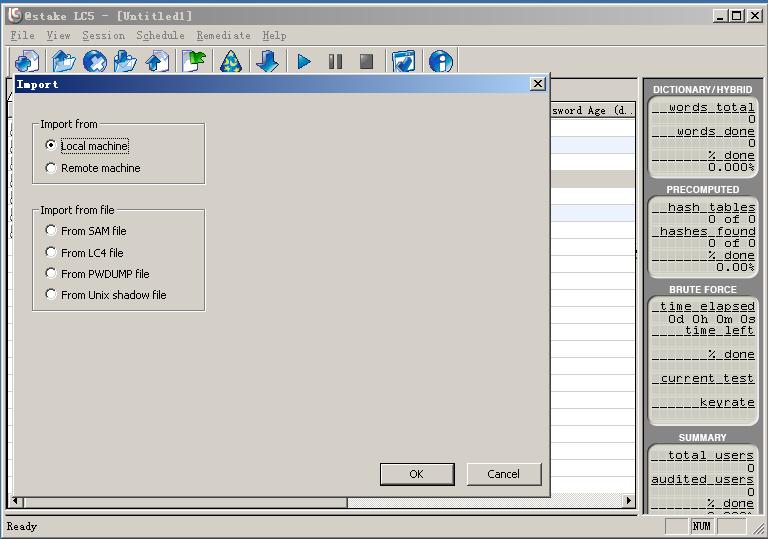
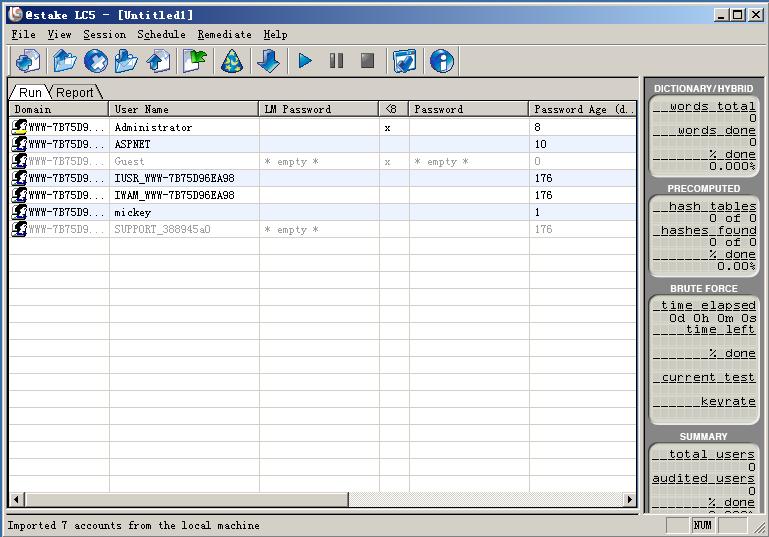
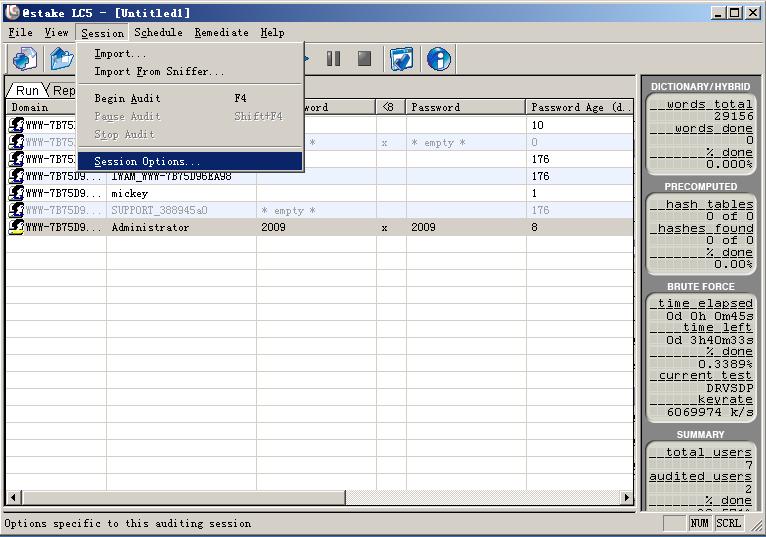
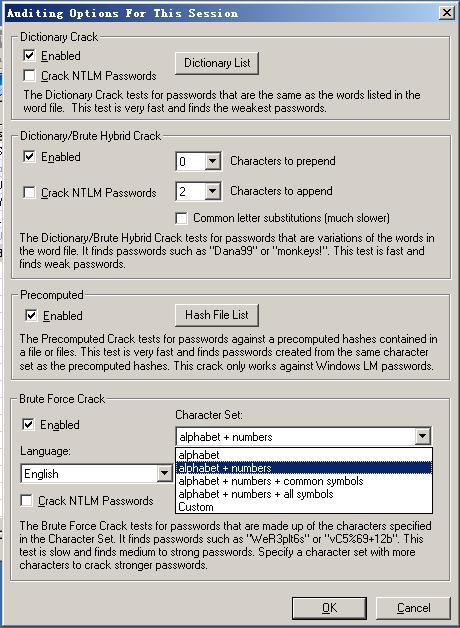
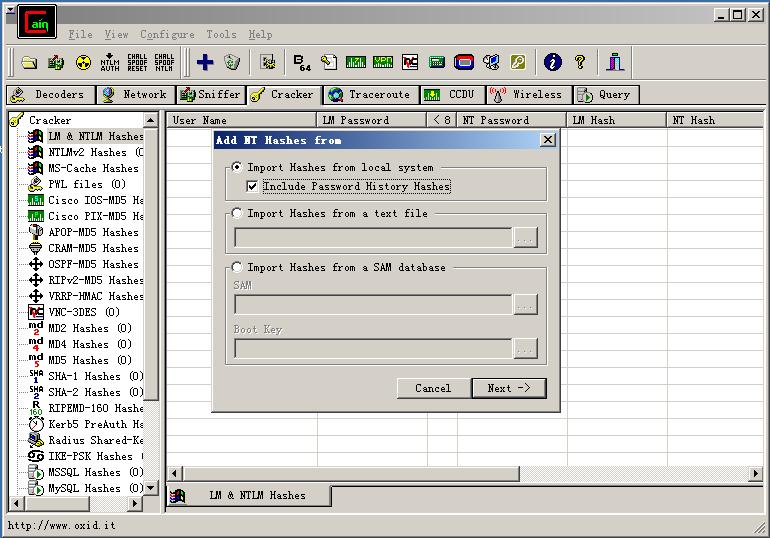
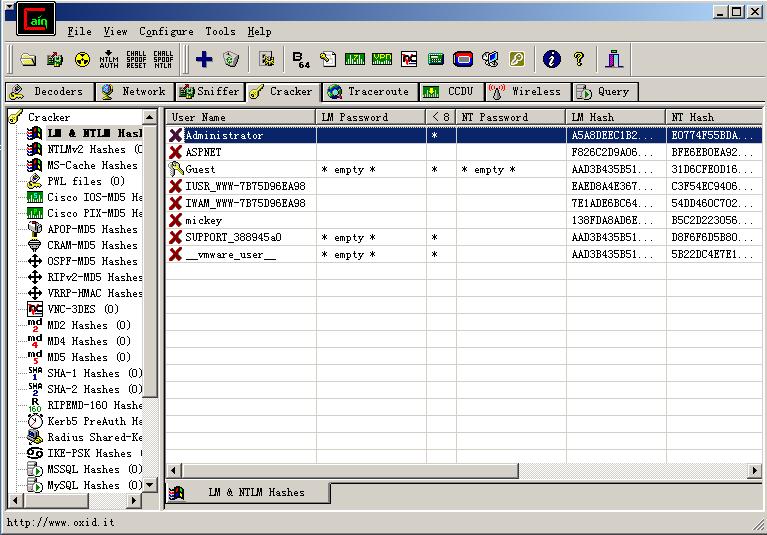
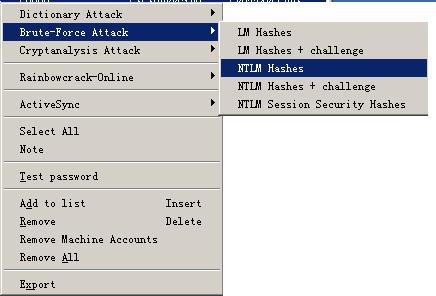
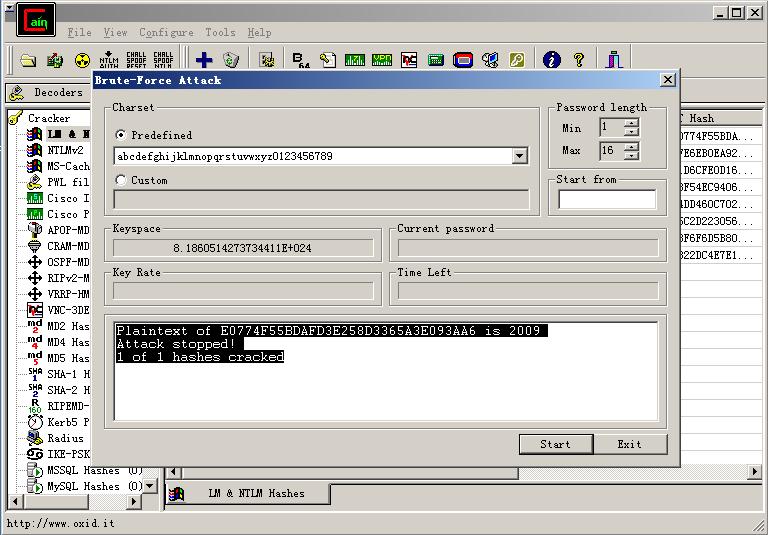
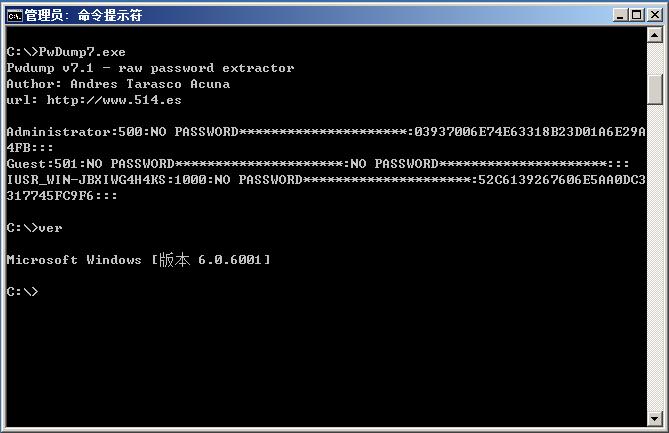
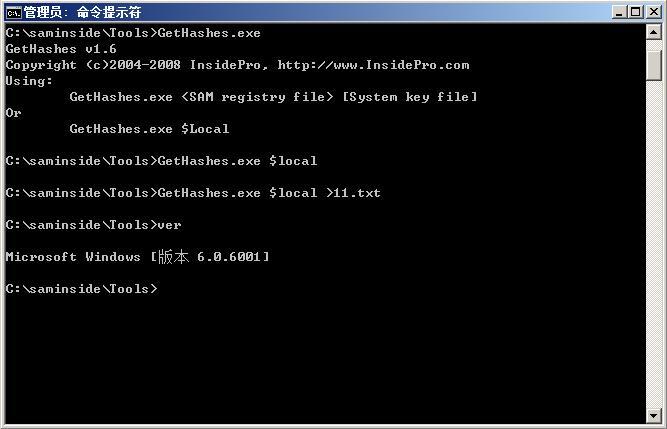
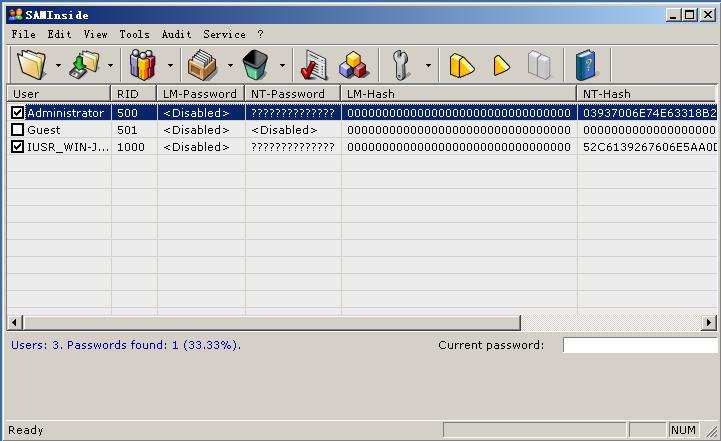
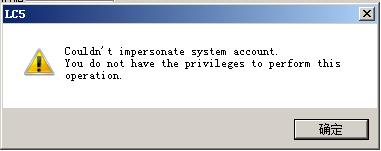
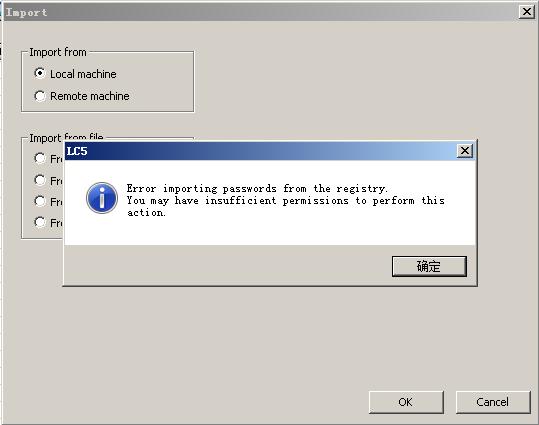
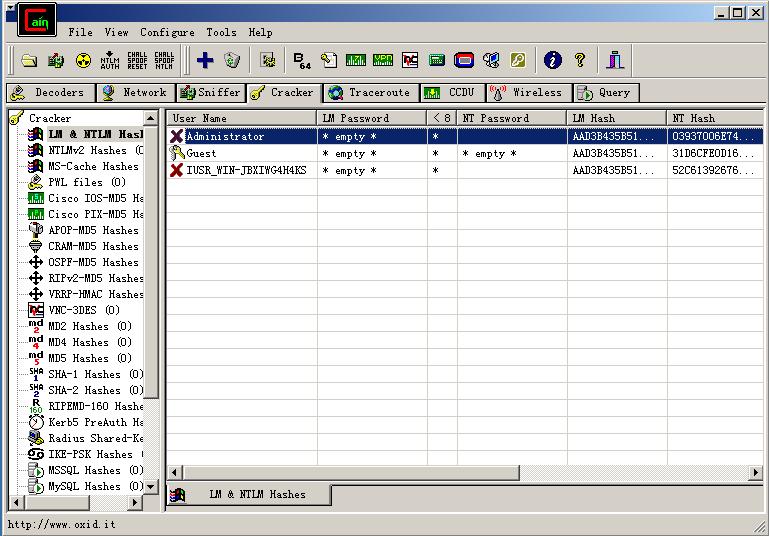
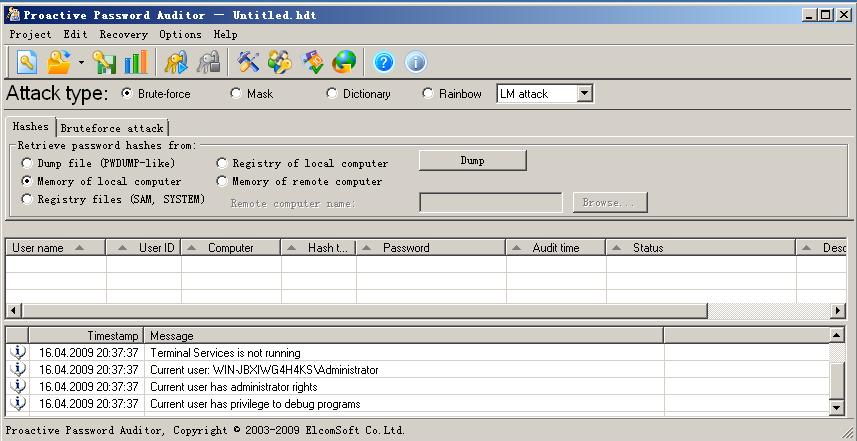
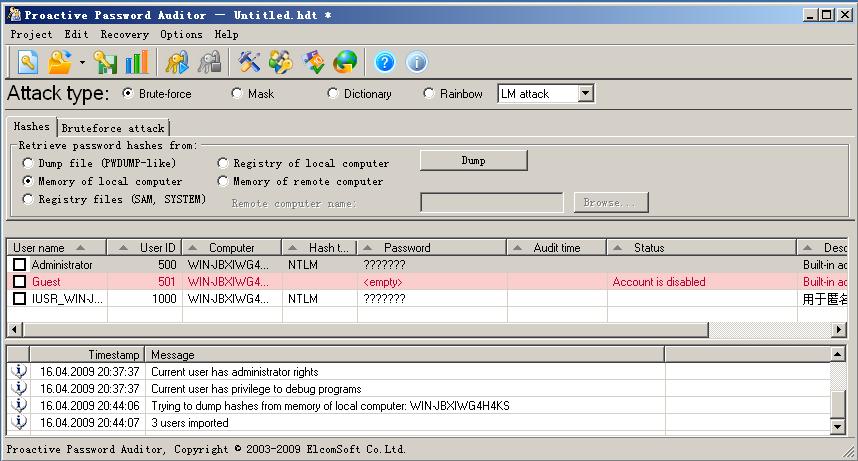
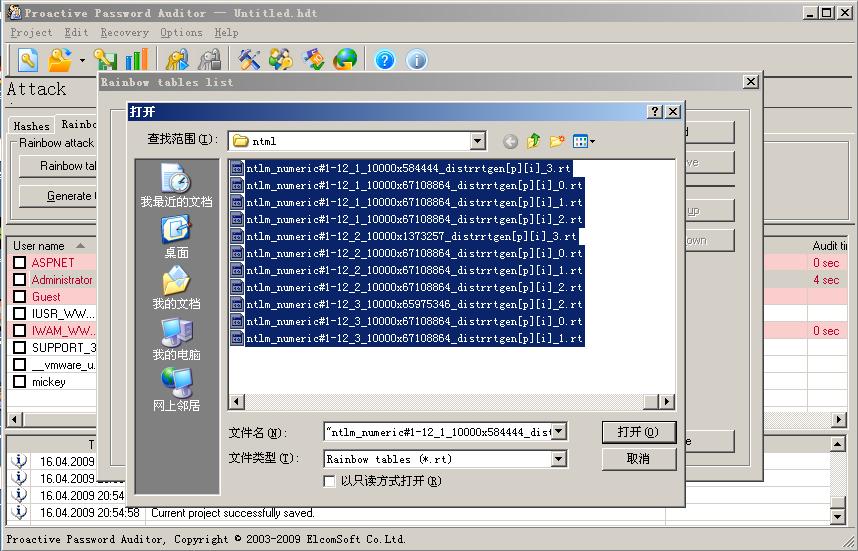
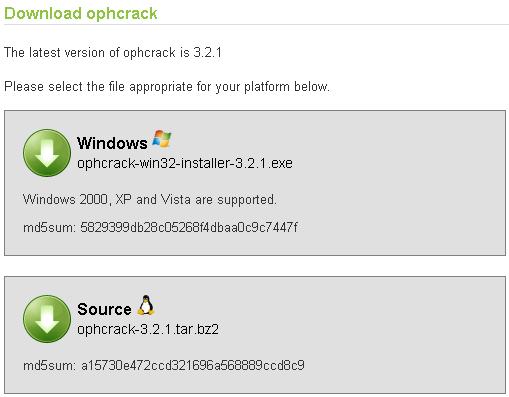
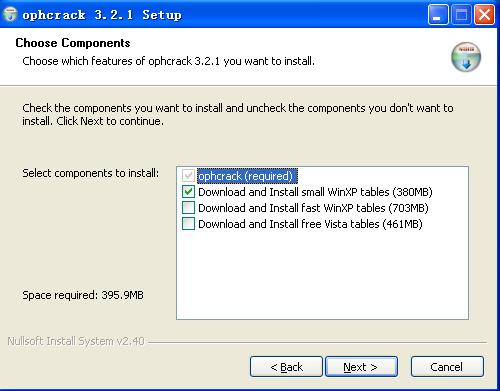
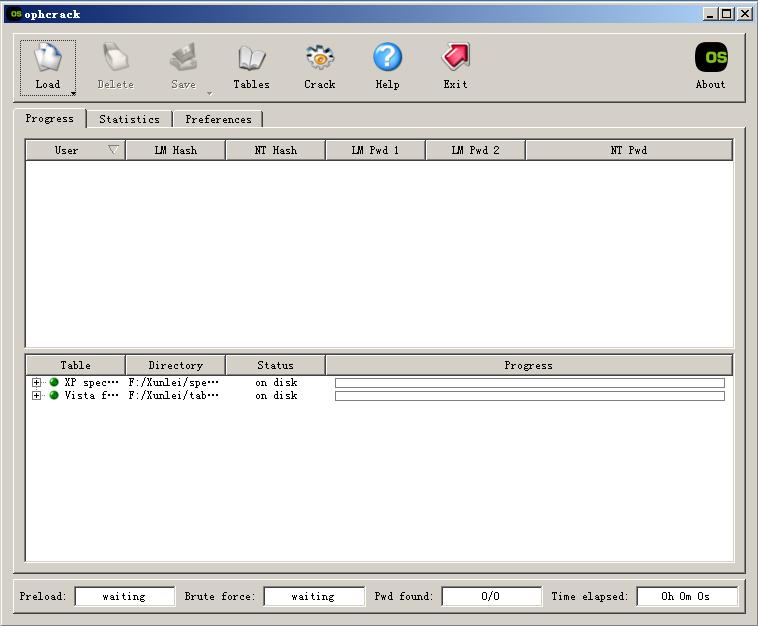
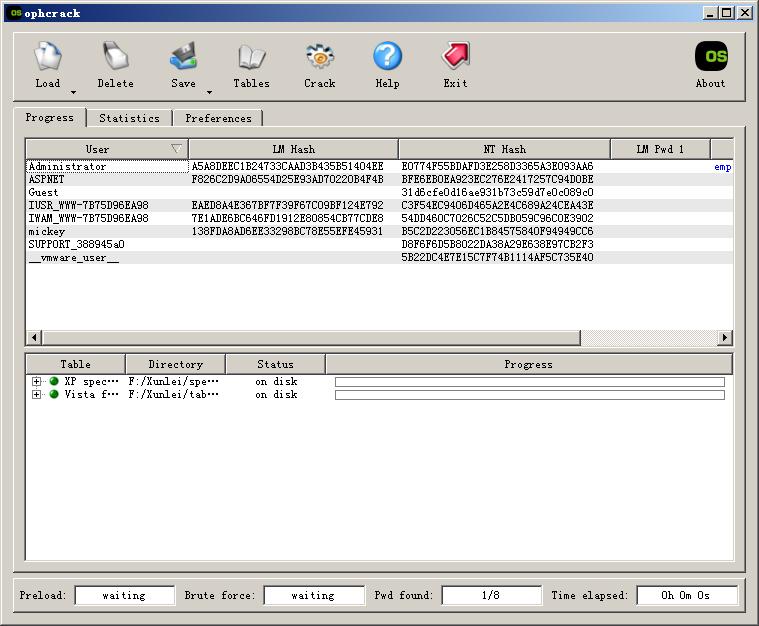
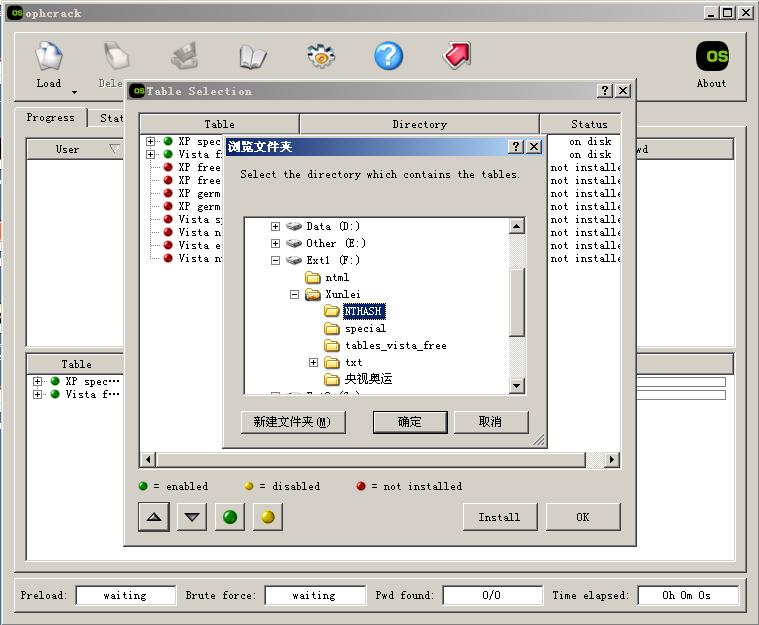
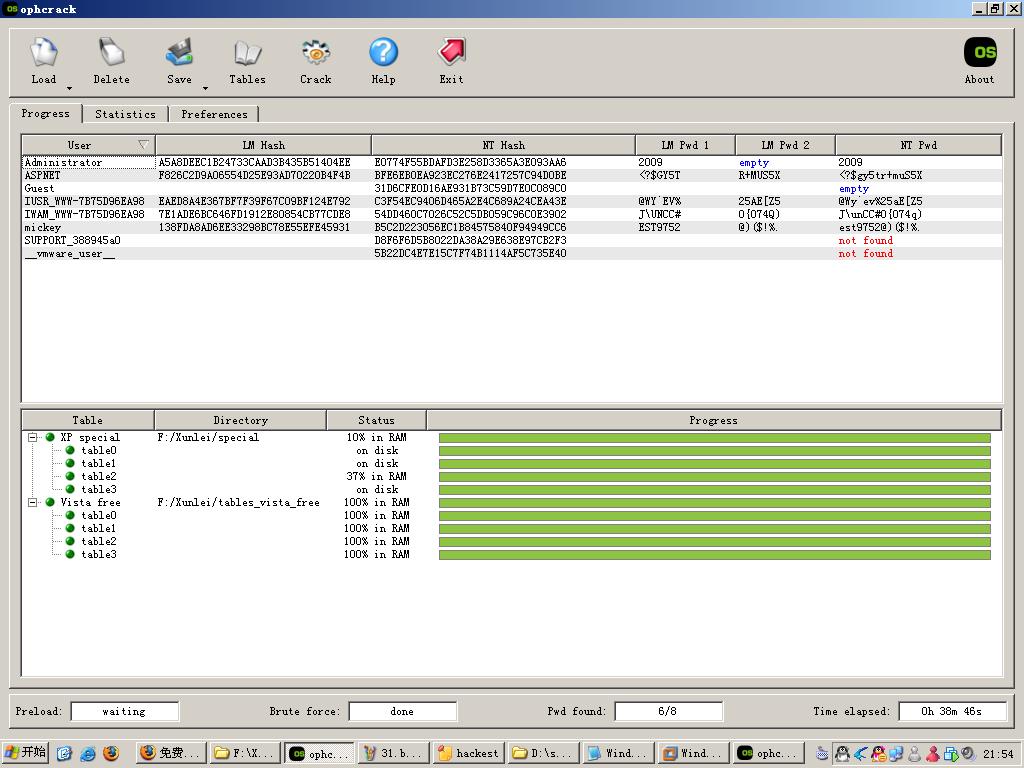
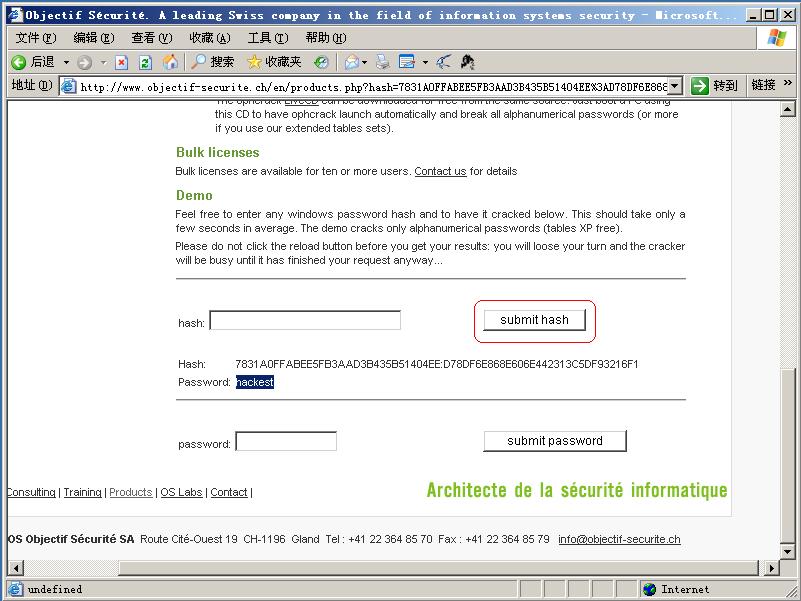
要破解一个程序的密码，要先了解它的一些背景知识。先来简单说一下Windows系统密码的加密算法。早期SMB协议（SMB是Server Message Block的简写，这个协议用于共享文件，共享打印机，共享串口等用途，我们之所以能够在windows的网络邻居下访问一个域内的其他机器，就是通过这个协议实现的）在网络上传输明文口令。后来出现"LAN Manager Challenge/Response"验证机制，简称LM，它是如此简单以至很容易被破解。微软提出了WindowsNT挑战/响应验证机制，称之为NTLM。现在已经有了更新的NTLMv2以及Kerberos验证体系。Windows加密过的密码口令，我们称之为hash（中文：哈希），Windows的系统密码hash默认情况下一般由两部分组成：第一部分是LM-hash，第二部分是NTLM-hash。  
  
--------------------------------------引文开始----------------------------------------------  
  
一、如何从明文口令生成LM-Hash？  
  
1、假设明文口令是"Welcome"，首先全部转换成大写WELCOME，再做如下变换：  
"WELCOME" -> 57454C434F4D4500000000000000  
先把WELCOME转换成十六进制形式，在明文口令不足14字节的情况下，后面添加0x00补足14字节。有些书上介绍添加空格(0x20)补足14字节，这是错误的，   
2、然后切割成两组7字节的数据，分别经str\_to\_key()函数处理得到两组8字节数据：

57454C434F4D45 -str\_to\_key()-> 56A25288347A348A  
00000000000000 -str\_to\_key()-> 0000000000000000  
  
3、这两组8字节数据将做为DESKEY对魔术字符串"KGS!@#$%"进行标准DES加密：  
  
"KGS!@#$%" -> 4B47532140232425  
  
56A25288347A348A -对4B47532140232425进行标准DES加密-> C23413A8A1E7665F  
0000000000000000 -对4B47532140232425进行标准DES加密-> AAD3B435B51404EE  
  
4、将加密后的这两组数据简单拼接，就得到了最后的LM-Hash  
  
Welcome的LM-Hash: C23413A8A1E7665FAAD3B435B51404EE。  
  
显然，由于明文口令一开始就全部转换成大写，导致多个明文口令对应一个LM-Hash。反过来，在穷举破解LM-Hash时，得到的有可能不是原始口令，因为不可能确定大小写。仔细观察前述SMB身份验证过程，即使这里得到的不是原始口令(大小写有差别)，同样可以通过SMB身份验证。这种转换成大写的行为减小了穷举破解难度。  
  
另一个弱点，当明文口令小于8字节时，LM-Hash后8字节的计算过程总是这样的：  
  
00000000000000 -str\_to\_key()-> 0000000000000000   
  
对4B47532140232425进行标准DES加密-> AAD3B435B51404EE  
  
这也将减小穷举破解难度。  
  
IBM设计了这个LM-Hash算法，魔术字符串"KGS!@#$%"的意义无从考证。这个算法称之为"哈希"不怎么妥当，由于是标准DES加密，完全是可逆的。当然，由于要穷举的是DESKEY本身，与传统所说的可逆有区别。  
  
二、如何从明文口令生成NTLM-Hash？  
  
IBM设计的LM-Hash算法存在几个弱点，微软在保持向后兼容性的同时提出了自己的挑战响应机制，所以，NTLM-Hash应运而生。  
  
1、假设明文口令是"123456"，首先转换成Unicode字符串，与LM-Hash算法不同，这次不需要添加0x00补足14字节：  
  
"123456" -> 310032003300340035003600  
  
从ASCII串转换成Unicode串时，使用little-endian序，微软在设计整个SMB协议时就没考虑过big-endian序，ntoh\*()、hton\*()函数不宜用在SMB报文解码中。0x80之前的标准ASCII码转换成Unicode码，就是简单地从0x??变成0x00??。此类标准ASCII串按little-endian序转换成Unicode串，就是简单地在原有每个字节之后添加0x00。  
  
2、对所获取的Unicode串进行标准MD4单向哈希，无论数据源有多少字节，MD4固定产生128-bit的哈希值，16字节：  
  
310032003300340035003600 -进行标准MD4单向哈希-> 32ED87BDB5FDC5E9CBA88547376818D4  
  
3、就得到了最后的NTLM-Hash  
  
123456的NTLM-Hash: 32ED87BDB5FDC5E9CBA88547376818D4。  
  
NTLM-Hash与LM-Hash算法相比，明文口令大小写敏感，但无法根据NTLM-Hash判断原始明文口令是否小于8字节，摆脱了魔术字符串"KGS!@#$%"。  
  
MD4是真正的单向哈希函数，穷举做为数据源出现的明文，难度较大。问题在于，微软一味强调NTLM-Hash的强度高，却避而不谈一个事实，为了保持向后兼容性，NTLM-Hash缺省总是与LM-Hash一起使用的。这意味着NTLM-Hash强调再高也是无助于安全的，相反潜在损害着安全性。增加NTLM-Hash后，首先利用LM-Hash的弱点穷举出原始明文口令的大小写不敏感版本，再利用NTLM-Hash修正出原始明文口令的大小写敏感版本。  
  
--------------------------------------引文结束----------------------------------------------  
  
实战  
  
理论准备得差不多了，进入实战阶段。当你已经得到Windows的系统权限后，如何才能获得管理员的密码hash呢？不同版本的Windows的hash获取方法不一样。用到的工具有pwdump7.exe、GetHashes.exe、SAMInside.exe、LC5、Cain、Proactive Password Auditor、Ophcrack。下面将会详细介绍如何抓取各Windows版本的系统密码hash。  
  
1、Windows 2000  
  
比较老的一个Windows版本，同时也有好几个子版本，现在还在不少服务器上跑着，虽然性能和安全性都有点跟不上时代的脚步了，但是我们也不能放过。本文主要针对服务器目标，所以测试系统为Windows 2000 高级服务器版，打了SP4补丁的，已更新所有补丁，如图1。  
  
[](http://www.hackest.cn/images/31/1.jpg)  
  
2000下可以用pwdump7.exe来抓取系统用户的hash，命令格式：pwdump7.exe >2000hash.txt，意思为抓取所有用户hash，并写入2000hash.txt这个文本文件，如图2。  
  
[](http://www.hackest.cn/images/31/2.jpg)  
  
也可以用SAMInside自带的小工具GetHashes.exe，命令格式：GetHashes.exe $local >2000.txt，意思是抓取所有用户hash并写入2000.txt这个文本文件，如图3。  
  
[](http://www.hackest.cn/images/31/3.jpg)  
  
还可以用图形界面的SAMInside，打开SAMInside，点击“File”，然后点击“Import local Users via Scheduler”，稍等一会就成功抓取到hash了，如图4、图5。  
  
[](http://www.hackest.cn/images/31/4.jpg)  
  
[](http://www.hackest.cn/images/31/5.jpg)  
  
因为这个是利用Windows的计划任务来抓取的，所以Task Scheduler服务必须启动，否则抓不出来。抓到hash之后还要导出，以方便用其它更强大的破解工具进行破解工作。如果要导出所有用户的hash，就点击“File”，然后点击“Export Users to PWDUMP File...”，然后保存为txt文本即可。如果只需要其中一个用户的hash，就选“Export Selected Users to PWDUMP File...”，同样保存为txt文本即可，如图6。  
  
[](http://www.hackest.cn/images/31/6.jpg)  
  
操作都比较简单吧。SAMInside同时也是一个破解工具，可以对抓取的hash进行简单的破解工作，还自带了一个常用字典，还可以结合彩虹表进行破解，如果密码不是太复杂，在这里就可以得到密码明文了。  
  
  
顺便提一下Windows 2000下的另一个得到管理员密码的方法，用aio.exe（aio是All In One的缩写，是一些小工具的集合）直接读取内存中的密码，Windows 2003 SP1、SP2补丁没有打的话，也可以这样读取出来密码明文。命令格式：aio.exe -findpassword，成功读出了密码，密码为2000，如图7。  
  
[](http://www.hackest.cn/images/31/7.jpg)  
  
此方法只有在管理员登录了，而又没有注销的情况下才可以成功读出密码

2、Windows XP&Windows 2003  
  
参照上面抓2000的，步骤都差不多。不过比较推荐用SAMInside抓取，因为pwdump7不太稳定，有时候抓到的hash不一定正确，甚至还有可能抓不出来……图行界面下用SAMInside抓取，命令行下用SAMInside自带的那个小工具GetHashes.exe抓取，hash一般保存为txt文件即可。下面再介绍一些上面没提到的工具如何抓取hash，这些工具自己能抓，也能破解，比较强大。聪明的读者可能会发现上面提到的工具只出场了一部分，还有好几个都还没有露面，嘿嘿……下面就来介绍下另外几个强大的工具。  
  
LC5  
  
如果要用LC5抓取本机的hash，就依次打开“Session”->“Import”->“Local machine”稍等片刻就可以成功抓取到hash了，如果你要导入破解hash，就选“Import from file”->“From PWDUMP file”导入即可进行破解，如图8、图9。  
  
[](http://www.hackest.cn/images/31/8.jpg)  
  
[](http://www.hackest.cn/images/31/9.jpg)  
  
再点击小三角形按钮就可以开始破解了。当然你还可以对破解做一些调整，“Session”->“Session Options...”，在“Btute Force Crack”选项里的“Character Set:”里可以设置字符集，默认选的是alphabet+numbers，字母和数字，如图10、图11。  
  
[](http://www.hackest.cn/images/31/10.jpg)  
  
[](http://www.hackest.cn/images/31/11.jpg)  
  
LC5是非常强大的，可以这么说，只要你的hash是正确的，就没有破不出来的密码，前提是你有足够的时间！  
  
Cain  
  
Cain我相信很多喜欢嗅探的朋友都会知道，但是你知不知道它除了嗅探之外还具备了强大的密码破解功能呢？如何用Cain来抓取hash呢，同样十分简单（试想像一下，你一边开着Cain嗅同网段其它机器的时候，一边破解已控制目标的管理员密码是一件多么酷的事情）。安装Cain所需驱动WinPcap，才能启动Cain，不过如果你只是用它来破解密码，而不需要嗅探类操作的话，打开Cain的时候它提示缺少什么文件就在安装目录建一个同名dll文件即可打开（欺骗Cain，让它为我们服务，不过这样做当然不具备嗅探类功能）。点选“Cracker”->“LM&NTLM Hashes”，然后点下右边空白处，蓝色+号按钮即可激活，然后点击它，弹出“Add NT Hashes from”->“Import Hashes from local system”->勾选“Include Password History Hashes”，然后Next，hash就抓出来了，如图12、图13。  
  
[](http://www.hackest.cn/images/31/12.jpg)  
  
[](http://www.hackest.cn/images/31/13.jpg)  
  
右键单击你要破解的用户，“Brute-Force Attack”->“NTLM Hashes”->“Start”，就会开始暴力破解了，如果你的密码足够简单，很快就有得出结果，当然你同样可以像LC5一样选择你觉得可能的字符集，以改善破解速度，还可以自定义字符集。Administrator的密码为2009，轻松破解，如图14、图15。  
  
[](http://www.hackest.cn/images/31/14.jpg)  
  
[](http://www.hackest.cn/images/31/15.jpg)  
  
3、Windows Vista&Windows 7&Windows 2008  
  
为什么要把Vista及其后面的Windows系统版本分开说明呢，当然是有原因的。在Windows 2008中，微软对SAM和SYSKEY采取了与之前版本Windows不同的加密方法，尤其加密采用的NTLM-Hash算法远比之前的LM-Hash更复杂得多，这使得之前用于Windows NT/2000/XP上的破解管理员密码的方法统统失效了（其实只是Windows 2008默认状态下把LM-hash禁用了，所以就增加了破解难度）。  
  
先来试下2000/XP/2003下的那些工具，测试系统版本：Windows Server Enterprise SP1（企业版），已更新所有补丁程序。pwdump7.exe可以运行，但是抓出来的hash明显与之前的不同，LM-hash那段都是星号，原因就是前面说过的Windows 2008禁用了LM-hash，如图16。  
  
[](http://www.hackest.cn/images/31/16.jpg)  
  
GetHashes.exe没有成功抓到hash，生成的txt文件为空白，如图17。  
  
[](http://www.hackest.cn/images/31/17.jpg)  
  
SAMInside也可以运行，成功抓取到了hash，不过LM-hash段全为0，要注意使用最新版本，如图18。  
  
[](http://www.hackest.cn/images/31/18.jpg)  
  
再来看看LC5，安装运行，N久后提示“Couldn't impersonate system account.You do not have the privileges to perform this operation.”确定之后继续提示“Error importing passwords from the registry.You may have insufficient permissions to perform this action.”大致意思是说我没有权限执行这个操作，可是我是以管理员身份运行的LC5的，它自己不行所以就很委婉地推托说是我权限不够。不过LC5的公司已经被人收购了N久，版本也没有再更新，在新的Windows 2008下表现令人失望也情有可愿，如图19、图20。  
  
[](http://www.hackest.cn/images/31/19.jpg)  
  
[](http://www.hackest.cn/images/31/20.jpg)  
  
而且拿pwdump7.exe和SAMInside抓取的hash导入LC5也同样无法破解，一点小三角形开始按钮便马上停止。这一轮，LC5被淘汰。

接下来轮到Cain了，轻松抓取，不过Windows 2008的密码默认不允许使用简单密码，所以给密码破解提高了难度，细心的朋友可能会发现，LM-hash段显示的并不是SAMInside的一串0，而是清一色的AAD3B435B51404EEAAD3B435B51404EE，具体原因聪明的朋友自己分析下为什么，呵呵，如图21。  
  
[](http://www.hackest.cn/images/31/21.jpg)  
  
这里要提的一点是Cain抓的hash格式和别的工具抓的不太一样，需要自己处理下才能导入破解，要不然别的工具直接导入的话，会无法识别。示例如下：  
  
SAMInside：  
Administrator:500:NO PASSWORD\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*:03937006E74E63318B23D01A6E29A4FB:::  
  
Cain：  
Administrator:"":"":AAD3B435B51404EEAAD3B435B51404EE:03937006E74E63318B23D01A6E29A4FB  
为了加强通用性，在此提醒大家hash格式统一以第一种为准，也就是SAMInside所抓取的那个格式！  
  
ppa  
  
下面轮到Proactive Password Auditor（以下简称ppa），这是一个商业软件（就是要钱的那种），不过官方提供60天试用版本，功能无限制，低版本有破解版。该软件需要安装，界面如图22。  
  
[](http://www.hackest.cn/images/31/22.jpg)  
  
如果你要抓取Windows 2008的本机hash，那直接点击Dump即可抓取，默认是从“Memory of local computer”本地计算机内存抓取。该软件还支持注册表抓取，SAM文件抓取，同时支持远程抓取hash，轻松抓到hash，如图23。  
  
[](http://www.hackest.cn/images/31/23.jpg)  
  
也支持导入hash破解，同时还支持暴力破解、字典破解、彩虹表破解。这里着重介绍下彩虹表破解。首先要明白，彩虹表是什么东西呢？  
  
什么是彩虹表？  
  
彩虹表就是一个庞大的、针对各种可能的字符组合预先计算好的哈希值的集合，不一定是针对MD5算法的，各种算法的都有，有了它可以快速的破解各类密码。越是复杂的密码，需要的彩虹表就越大，现在主流的彩虹表都是100G以上。  
  
要用ppa配合彩虹表破解的方法也比较简单，Attack选择“Rainbow”->“NTLM attack”->“Rainbow tables list...”->“Add”选择导入彩虹表文件，格式一般为\*.rt，我下载了国外一个免费的彩虹表，目前大小为207GB，完整表还会更大。导入所有彩虹表后，点击“Recovery”->“Start recovery”开始破解，如图24、图25。  
  
[](http://www.hackest.cn/images/31/24.jpg)  
  
[](http://www.hackest.cn/images/31/25.jpg)  
  
这个软件个人感觉跑纯数学密码超级快，即使是14位长的纯数字密码，也用不了几秒钟！ppa支持Vista和2008下破解。  
  
Ophcrack  
  
下面该轮到本文最有价值的软件——Ophcrack出场了！Ophcrack是一个免费的在配合彩虹表的基础上破解Windows系统密码的工具。效率相当可观，它配备了一个Windows下的图形用户界面并且支持多平台运行。而且还可以下载官方的Ophcrack LiveCD刻录成光盘，就可以走到哪破到哪了！其官方网站为http://Ophcrack.sourceforge.net/，可以到官方下载安装，如图26。  
  
[](http://www.hackest.cn/images/31/26.jpg)  
  
Ophcrack所用的彩虹表和常规的彩虹表不太一样，它识别不了\*.rt格式的彩虹表，只认官方的彩虹表。常规的彩虹表无法破解Vista、Windows 7、Windows 2008的密码hash。免费的彩虹表官方只提供三个：XP free small (380MB)、XP free fast (703MB)、Vista free (461MB)，其它更为强大的一些彩虹表则需要收取一定费用。安装的时候需要注意，可以选择是否下载官方彩虹表，如果你想安装好软件后另外自己下载则去掉勾选的选项即可，如图27。  
  
[](http://www.hackest.cn/images/31/27.jpg)  
  
安装完毕，界面比较清爽吧，如图28。  
  
[](http://www.hackest.cn/images/31/28.jpg)  
  
因为官方收费的一些表被国外的一些网站公布了，所以我下了两个比较常用的表：一个是XP special (7.5GB)；另一个是Vista special (8.0GB)，官方标价为99美元/个。至于更大的表则没有下载，其实有这两个表基本上都够用的了。别看它表体积不大，但威力不容小觑。似乎是做过某种优化和压缩，打开Ophcrack，“Load”->“Local SAM”，然后一个黑窗口闪过（其实到Ophcrack的安装目录就可以发现，它其实是用pwdump6来抓取hash的，不过pwdump6相对pwdump7来说比较稳定）成功抓取hash，图是在Windows 2003下操作的，因为Ophcrack用的是pwdump6，无法在Windows 2008及Vista下抓取hash（可以考虑替换pwdump6为pwdump7来改善这一功能，不过我没有成功，技术有限啊-\_-），如图29、图30。  
  
[](http://www.hackest.cn/images/31/29.jpg)  
  
[](http://www.hackest.cn/images/31/30.jpg)  
  
Tables标签下可以看到已安装的彩虹表，如果安装软件的时候没有下载官方彩虹表，后期下载完彩虹表后可以在Tables里进行安装，如图31。  
  
[](http://www.hackest.cn/images/31/31.jpg)  
  
然后就可以按Crack进行破解了。虽然说Ophcrack抓取hash的能力有所不足，相对在Vista下而言，但是我们可以用其他的hash抓取工具获得hash后再导入破解。来看看Ophcrack的破解成果图吧，密码14位，如图32。  
  
[](http://www.hackest.cn/images/31/32.jpg)  
  
需要注意的是，Vista下抓取的hash需要用Vista的彩虹表来破解，否则会破解失败！不过据说BitLocker加密也被国外黑客破解了，不过找不到相关资料，所以不再深入讨论，有兴趣的朋友可以自己测试。  
  
在线查询hash的网站：<http://www.objectif-securite.ch/en/products.php>，不过在线查询只允许查tables XP free的表，在线查询的时候需要注意hash的格式。比如用户名和密码都是hackest的hash为：  
hackest:1011:7831A0FFABEE5FB3AAD3B435B51404EE:D78DF6E868E606E442313C5DF93216F1:::  
我们只需要把7831A0FFABEE5FB3AAD3B435B51404EE:D78DF6E868E606E442313C5DF93216F1复制填入hash后面的框，再点击submit hash即可进行查询，同时也支持输入密码返回hash值，如图33。  
  
[](http://www.hackest.cn/images/31/33.jpg)  
  
Vista如果开启BitLocker则以上方法均无效，根本无法抓取到hash，不过好在BitLocker默认是关闭的，不是特别需要的用户一般不会开启它。  
  
后记  
  
当然了，破解至关重要的主hash的正确性，限制是密码的长度是否超过14位，还有密码所组成的字符集，甚至是中文的密码就无法破解。为什么密码长度超过14位也无法破解呢，因为NTLM-hash只支持到14位，目前还没有突破的方法。只要你认真阅读过本文，我相信你已经能破解绝大部分的Windows系统密码hash了，当然如果管理员用了组策略限制某个用户的密码有限期限为24小时，而第二天又自动启用另一个随机的密码，那破解密码就完全没有意义了（曾在美国某服务器遇到过这种变态级的管理员）。Windows下的密码就差不多说完了，那Linux下的系统密码又如何破解呢？其实更加简单（曾经在Ubuntu8.10下用john秒杀了我自己的密码）