WINDOWS 账户口令破解

1. 实验概述

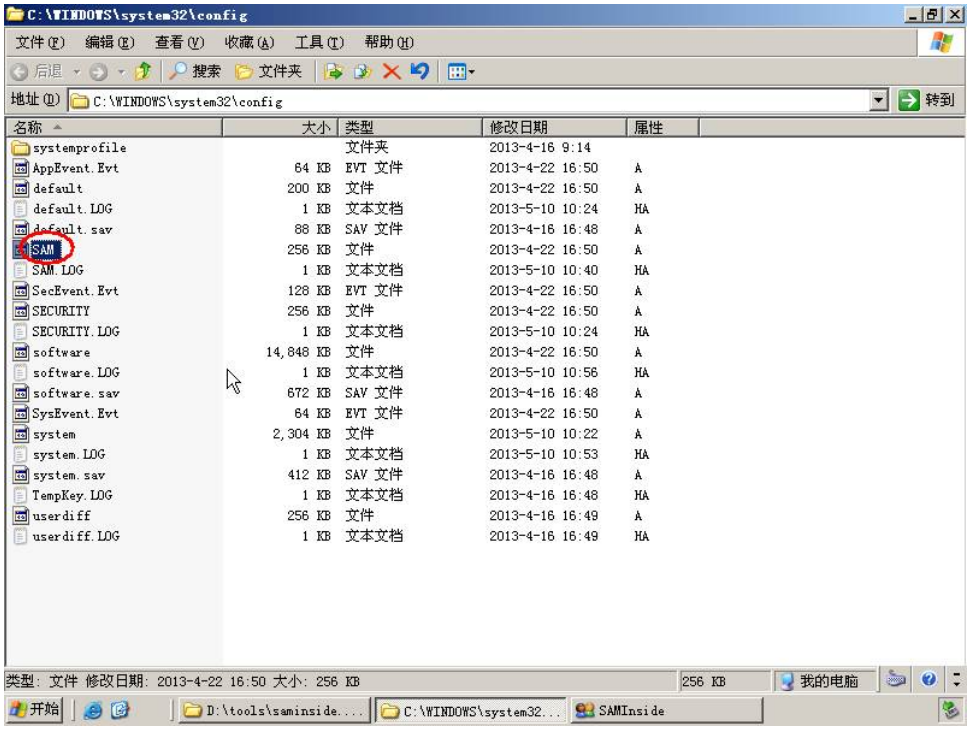
Windows 操作系统的账户口令使用了哈希进行存储，可以使用字典或彩虹表进行暴力破解。SAMInside 是常用于口令哈希破解的一款工具。

实验目的：了解 Windows 账户口令破解的原理；熟练使用 Windows 账户口令破解工具。

2. 工具介绍

SAMInside 是一款实用型 Windows 密码恢复工具，从 SAM 注册文件中提取用户名以及密码。Saminside 可以获取包括 Windows 2008 Server 以下操作系统的用户密码哈希值，在获取这些哈希值后可以通过彩虹表或者字典等来进行破解，进而获取系统的密码。

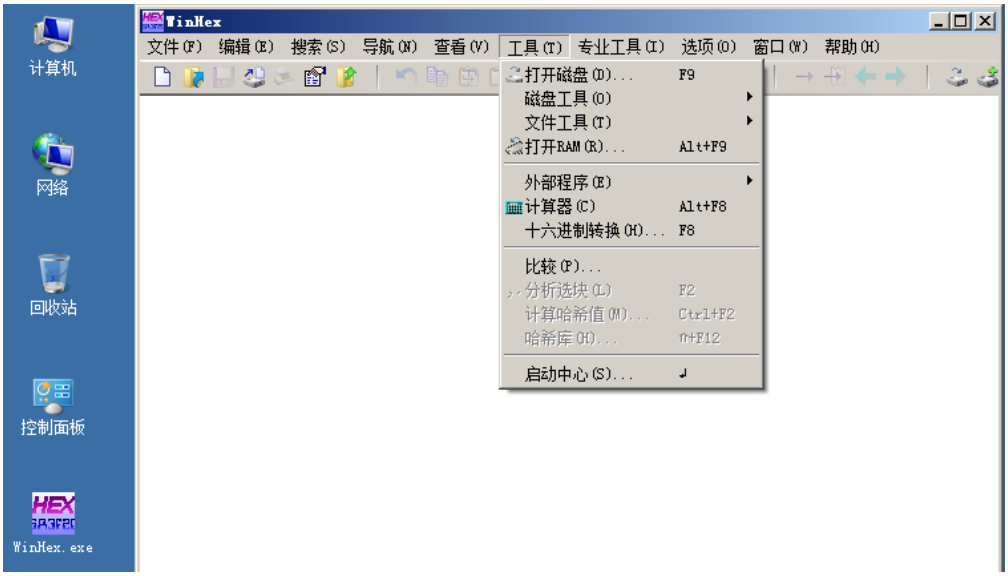
SAM 文件位于系统根目录下 c:\WINDOWS\system32\config。该文件无法直接复制，需要使用 WinHex 工具将其导出，同时还要复制导出 SYSTEM 这个文件。



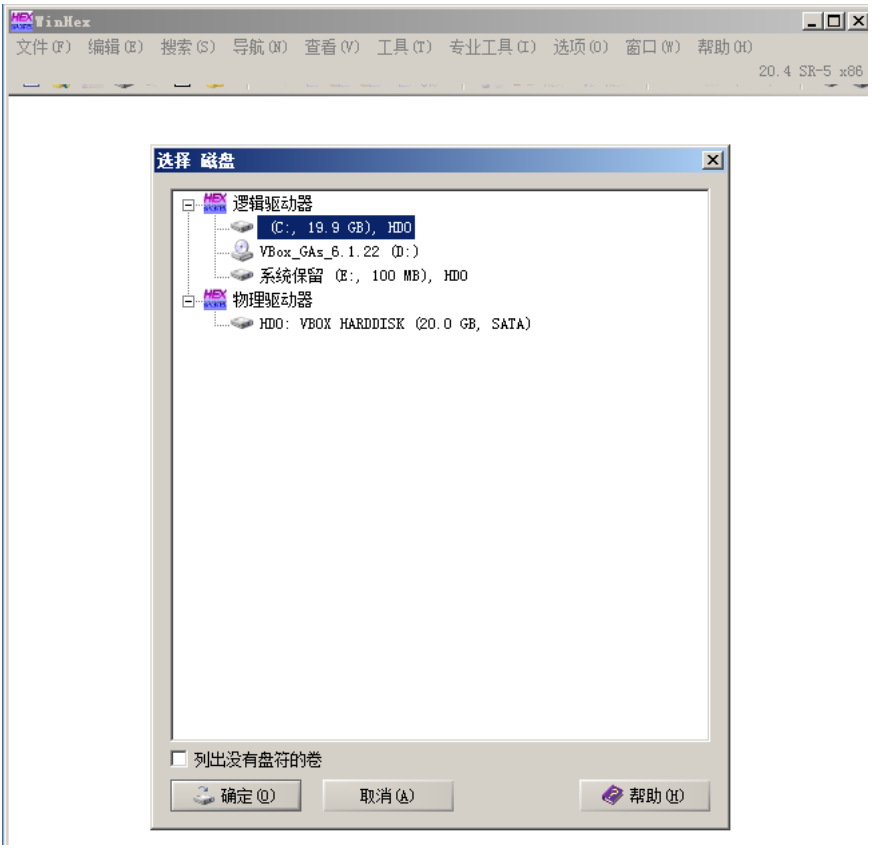
3. 实验内容

3.1 使用 WinHex 复制 SAM 文件

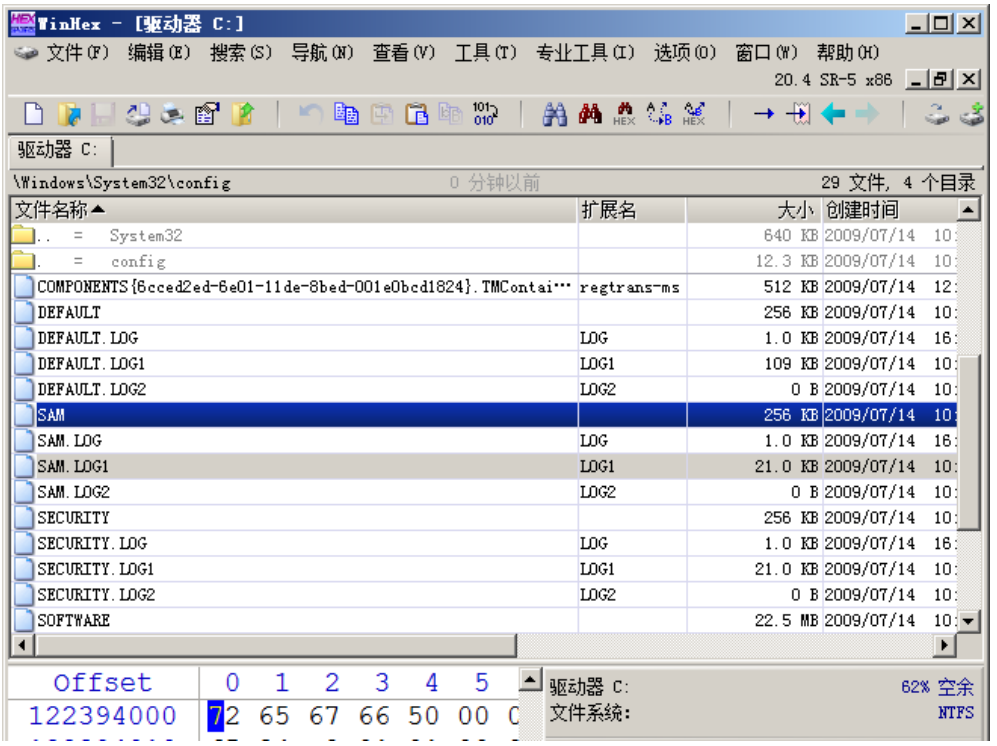
1. 打开桌面上的 WinHex 程序，选择“工具-打开磁盘”选项，如下图：



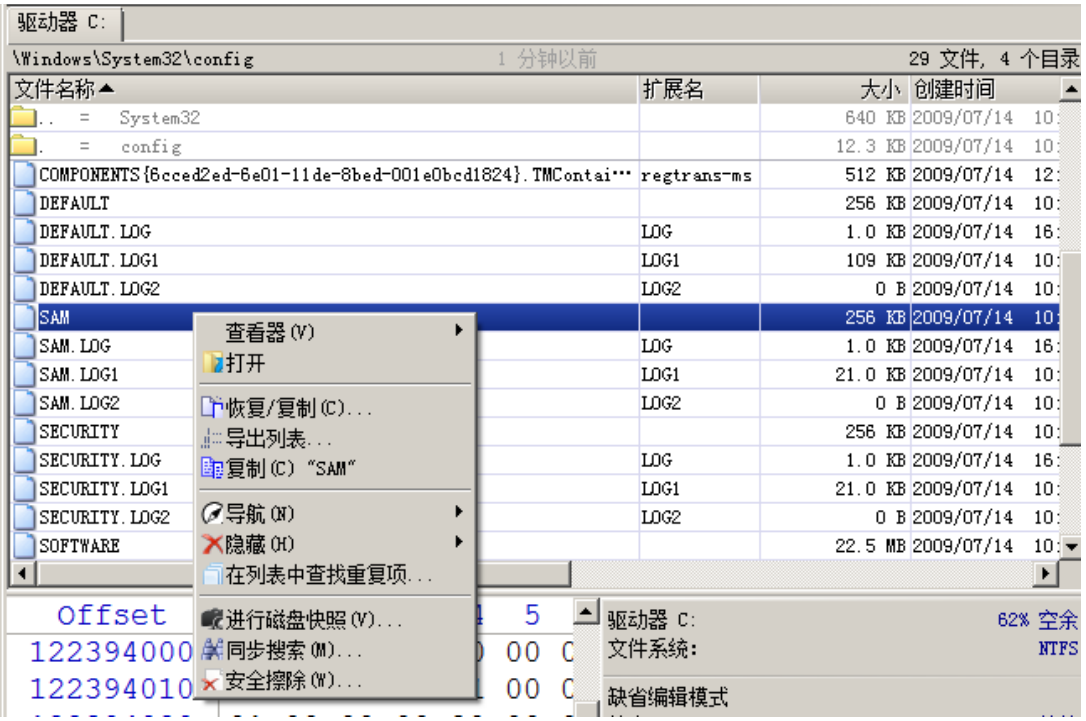
2. 选择逻辑驱动器 C 盘，如下图：



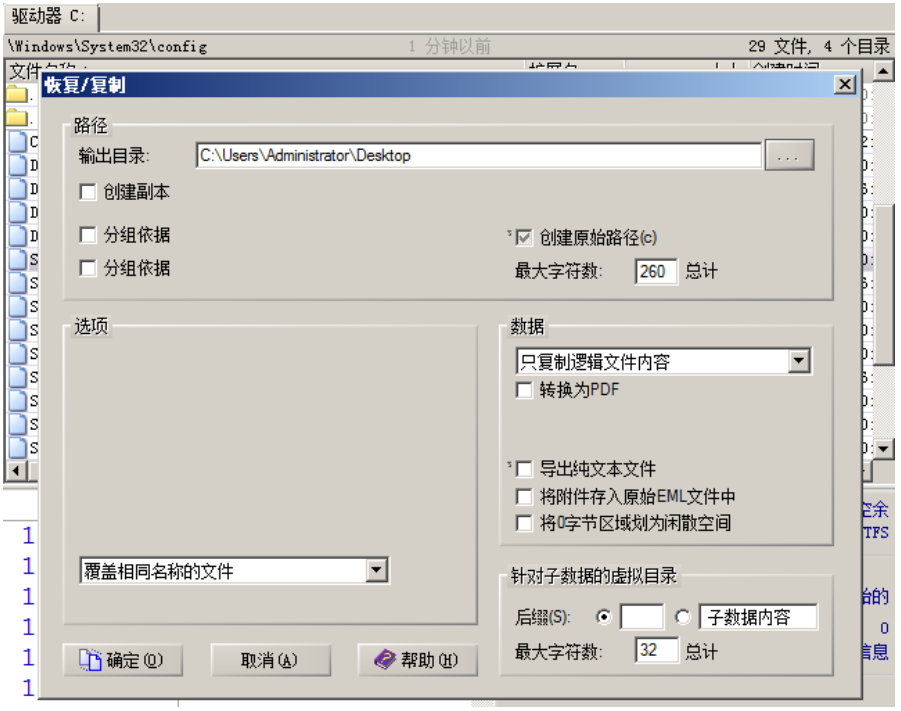
3. 进入后，按目录 Windows\System32\config 找到 SAM 文件，如下图：

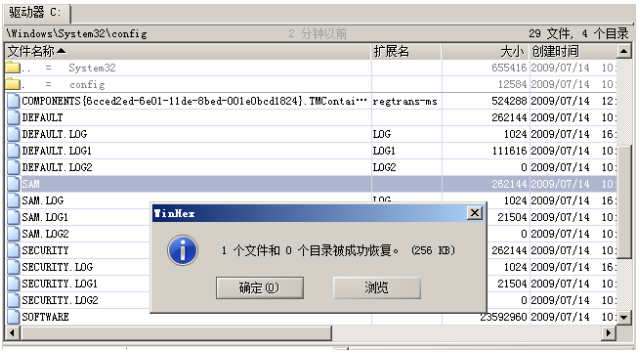


4. 右键选择将 SAM 文件恢复/复制，如下图：

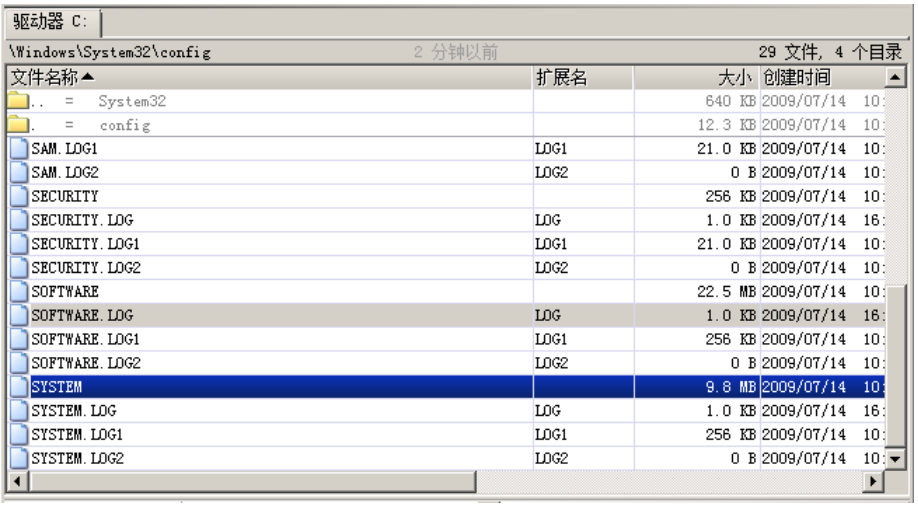


5. 指定导出 SAM 文件的路径，如下图：



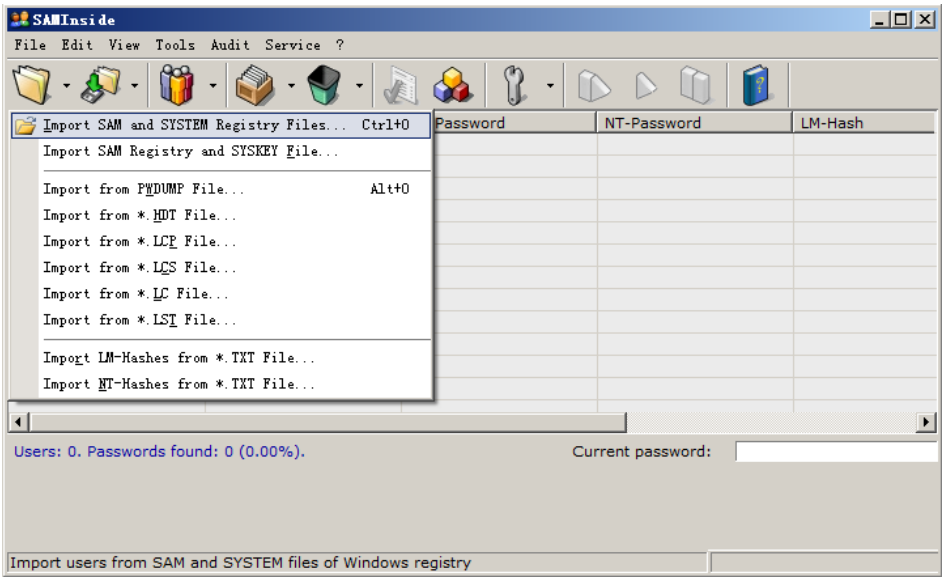


6. 用同样的方式将 SYSTEM 文件也导出到桌面，如下图：

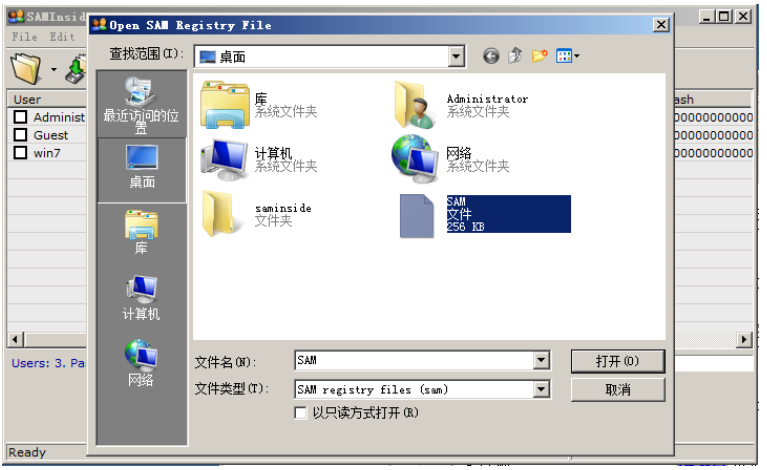


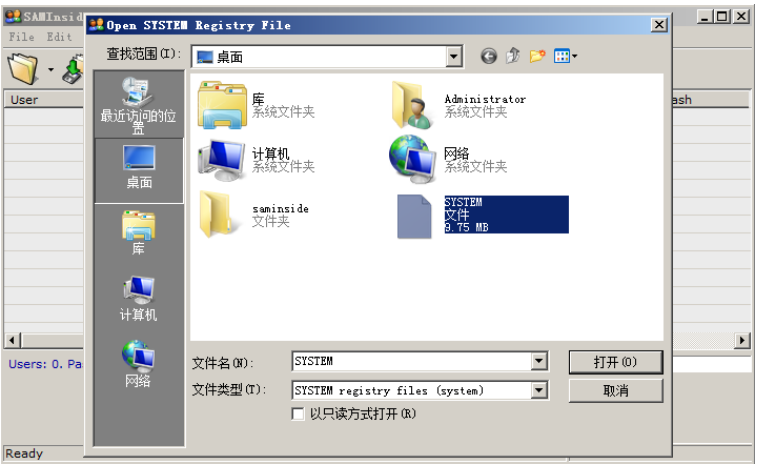
3.2 使用 SAMInside 破解口令

1. 打开桌面上的 saminside 文件夹里的 saminside 程序，选择“Import SAM and SYSTEM Registry Files…”

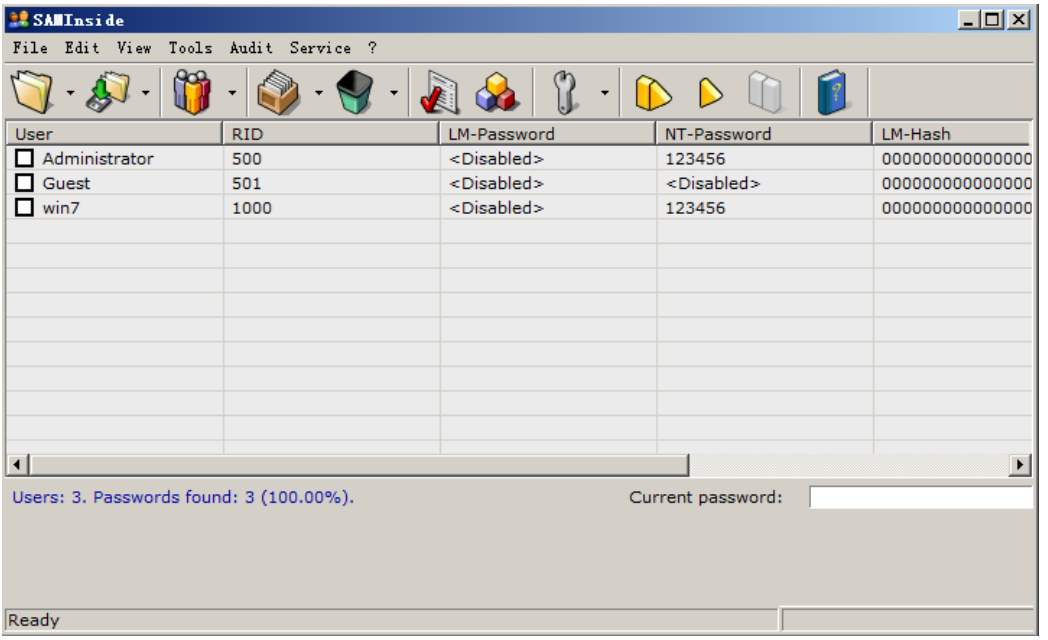


2. 找到之前导出到桌面的 SAM 和 SYSTEM 文件，打开导入到 saminside：





3. 打开成功后，自动破解出口令密码：



抵御口令破译攻击的最好方法是执行强制的口令防范政策。例如要求用户设想的口令很难被猜到。如口令应该至少有 8 位，包括数字、字母及特殊字符(如！@#$%)；口令应不包括字典字。为了进一步保障安全，一些口令自动设置工具可以帮助用户设计复杂的口令。

4. 实验报告提交

请完成上述整个实验内容，将整个实验过程以报告的形式记录，并上传提交到实训教学系统中。