电子科技大学 计算机科学与工程（网络空间安全）学院

标 准 实 验 报 告

（实验）课程名称 信息对抗综合设计实验

电子科技大学教务处制表

电 子 科 技 大 学

实 验 报 告

学生姓名： 黄鑫 学号： 2021050901013 指导教师：汪小芬

实验地点： 主楼 A2-413-1 实验时间：2023.10.10

一、实验室名称：主楼 A2-413-1

二、实验项目名称：SHA 散列破解

三、实验学时：4

四、实验原理：

（1）安全哈希算法（Secure Hash Algorithm）：对于长度小于 2^64 位的消息，SHA1 会产生一个 160 位的消息摘要。该算法的思想是接收一段明文，然后以一种不可逆的方式将它转换成一段（通常更小）密文，也可以简单的理解为取一串输入码（称为预映射或信息），并把它们转化为长度较短、位数固定的输出序列即散列值（也称为信息摘要或信息认证代码）的过程。散列函数值可以说是对明文的一种“指纹”或是“摘要”所以对散列值的数字签名就可以视为对此明文的数字签名。

(2)口令：也称通行字（password），应该说是保护计算机和域系统的第一道防护门，如果口令被破解了，那么用户的操作权和信息将很容易被窃取。所以口令安全是尤其需要关注的内容。

(3)口令的攻击方式: 词典攻击、强行攻击、组合攻击、常见攻击方式的比较、其他攻击方式

(4) 口令破解方式概述:手工破解、自动破解

手工破解：手工破解攻击者要猜测口令必须手动输入。要完成这一攻击，必须知道用户的 userID 并能进入被攻系统的登陆状态。这种方法简单但费时。其步骤为：产生可

能的口令列表按口令的可能性从高到低排序输入每个口令如果系统允许访问则成功如果没有成功，则重试。注意不要超过口令的限制次数

自动破解：只要得到了加密口令的副本，就可以离线破解。这种破解在脱机的情况下完成的，速度快。其原因是使用了程序搜索一串单词来检查是否匹配，这样的话就能同时破解多个口令。自动破解的步骤找到可用的 userID 找到所用的加密算法获取加密口令创建可能的口令名单对每个单词加密对所有的 userID 观察是否匹配重复以上过程，直到找到所有口令为止

五、实验目的：

了解 SHA 密码加密原理、学习 SHA 散列暴力破解的过程

六、实验内容：

通过 MD5SHAFX 加解密工具进行简单 SHA 密码的加解密流程执行，根据教程熟悉 SHA 散列暴力破解的过程。

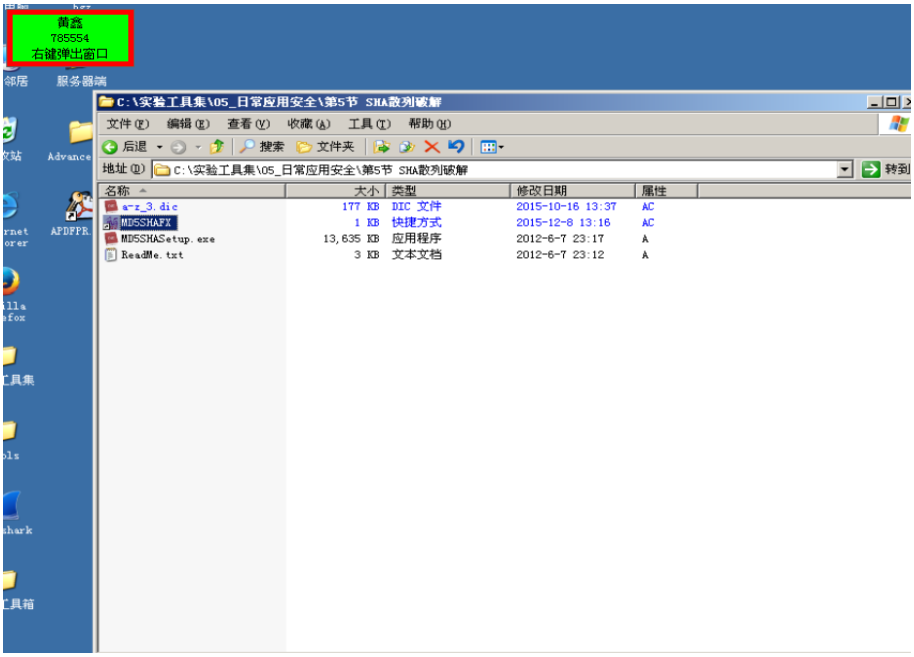
七、实验器材（设备、元器件）：

windows server 2003

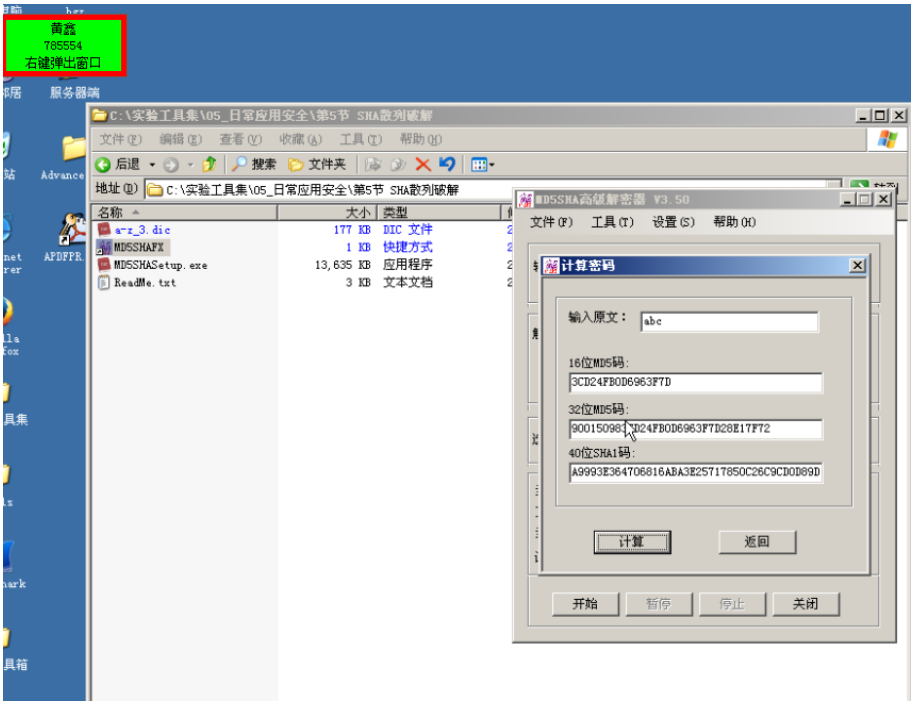
MD5SHAFX 加解密工具

八、实验步骤：

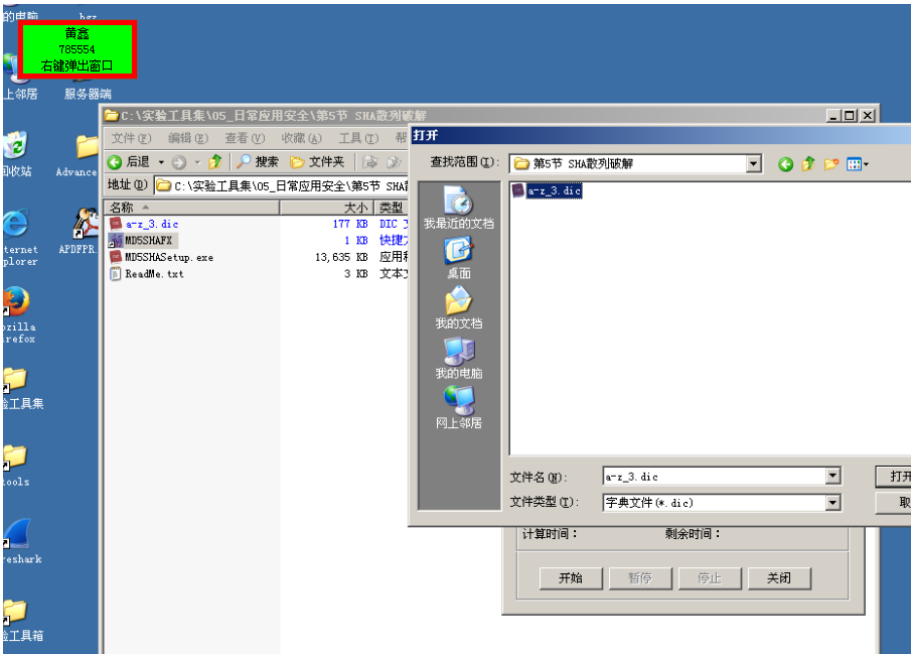
（1）在 C:\实验工具集\05_日常应用安全\第 5 节 SHA 散列破解中，找到【MD5SHAFX】并双击打开。



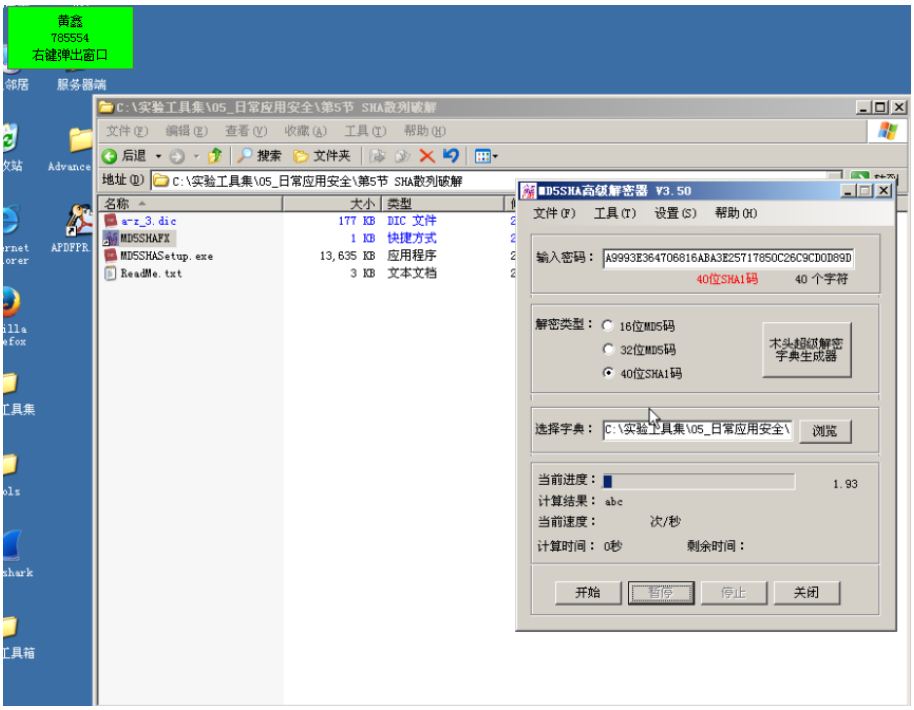
（2）在【输入原文】中输入需要加密的原文，如 abc，点击【计算】，即可计算出对应的散列值。



（3）点击【浏览】，选择字典。在 C:\实验工具集\05_日常应用安全\第 5 节 SHA 散列破解中的 a-z_3.dic。



（4）点击【开始】，即可进行暴力破解，爆破结果如下。



九、实验数据及结果分析：

原码：abc

16 位 MD5 加密：3CD24FB0D6963F7D

32 位 MD5 加密：900150983cd24fb0d6963f7d28e17f72

40 位 SHA1 加密：A9993E364706816ABA3E25717850C26C9CD0D89D

SHA1 暴力破解得到原文：abc

验证正确

十、实验结论：

通过 MD5SHAFX 加解密工具进行了’abc’的加密，分别得到了 16 位 MD5 加密，32 位 MD5 加密，40 位 SHA1 加密的结果，然后对 40 位 SHA1 加密的结果选择相应的字典进行反向暴力破解，得到的结果与源码对应结果一直，验证正确。

十一、总结及心得体会：

本实验通过了解 SHA 密码加密原理和进行 SHA 散列暴力破解的过程，强调了密码安全的关键性。使用 MD5SHAFX 工具对"abc"进行 SHA1 加密并成功进行暴力破解验证，加强了对密码保护和安全性的认识。

十二、对本实验过程及方法、手段的改进建议：

虽然本实验介绍了基本的密码破解方法，但密码破解是一个广泛的领域，包括更多的高级技术和防护方法。建议将更多关于密码学和密码安全的内容纳入实验，包括更多的密码破解技术和如何应对这些威胁。除了了解密码破解的方法，也应该强调密码安全的实践。教授学生如何创建强密码、使用密码管理器来管理密码、定期更改密码等实际应用的安全建议。

报告评分：

指导教师签字：

电子科技大学 计算机 学院

标 准 实 验 报 告

（实验）课程名称 信息对抗综合实验

电子科技大学教务处制表

电 子 科 技 大 学

实 验 报 告

学生姓名：黄鑫　学 号：2021050901013　指导教师：汪小芬

实验地点：主楼 A2-413-1　　实验时间：10.10

一、实验室名称：主楼 A2-413-1

二、实验项目名称：pwdump 导出本地 sam 散列

三、实验学时：4

四、实验原理：

Windowshash 由二部分组成，分别是 LM HASH&NT HASH。Windows 系统关于 hash 的组成如下：

用户名称:RID:LM-HASH 值:NT-HASH 值

1.LMHASH 生成规则

（1）用户的密码被限制为最多 14 个字符。

（2）用户的密码转换为大写。

（3）系统中用户的密码编码使用了 OEM 内码页。

（4）密码不足 14 字节将会用 0 来补全。

（5）固定长度的密码被分成两个 7byte 部分。每部分转换成比特流，在分 7bit 为一组末尾加 0，组成新的编码。

（6）上步骤得到的 8byte 二组，分别作为 DESkey 为“KGS!@#$%”进行加密。

（7）将二组 DES 加密后的编码拼接，得到最终 LMHASH 值。

2. NThash 生成原理

IBM 设计的 LMHash 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，NTLMHash 便应运而生。假设明文口令是”123456”，首

先转换成 Unicode 字符串，与 LMHash 算法不同，这次不需要添加 0 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。0×80 之前的标准 ASCII 码转换成 Unicode 码,就是简单地从 0x 变成 0×00。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 0×00。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，就得到了最后的 NTLMHash。

NTLM Hash:32ED87BDB5FDC5E9CBA88547376818D4。

五、实验目的：

1.理解 pwdump 导出 SAM 的原理

2.学习 pwdump 导出 SAM 的过程

六、实验内容：

使用本地 pwdump 导出本机 sam，对于结果进行下一步的破解以及分析

七、实验器材（设备、元器件）：

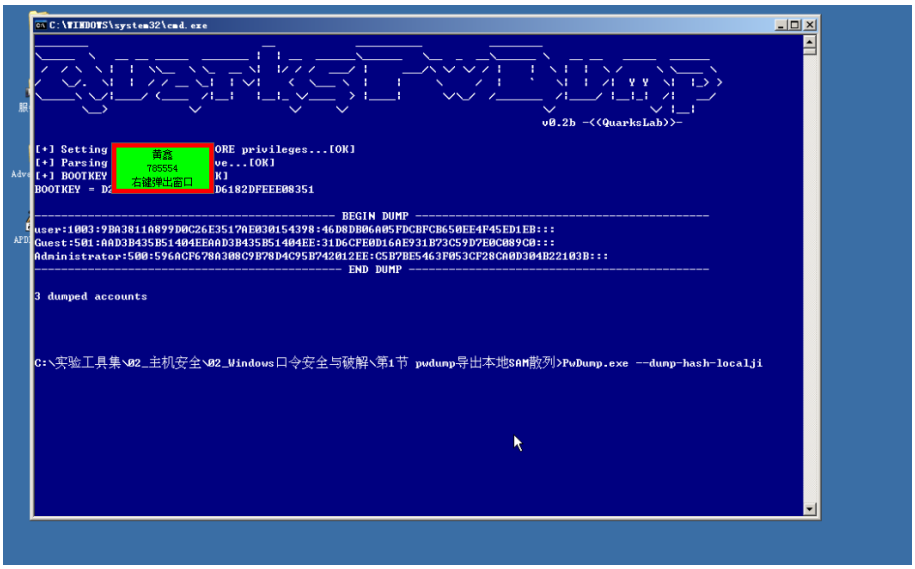
windows server 2003 虚拟机

pwdump 工具

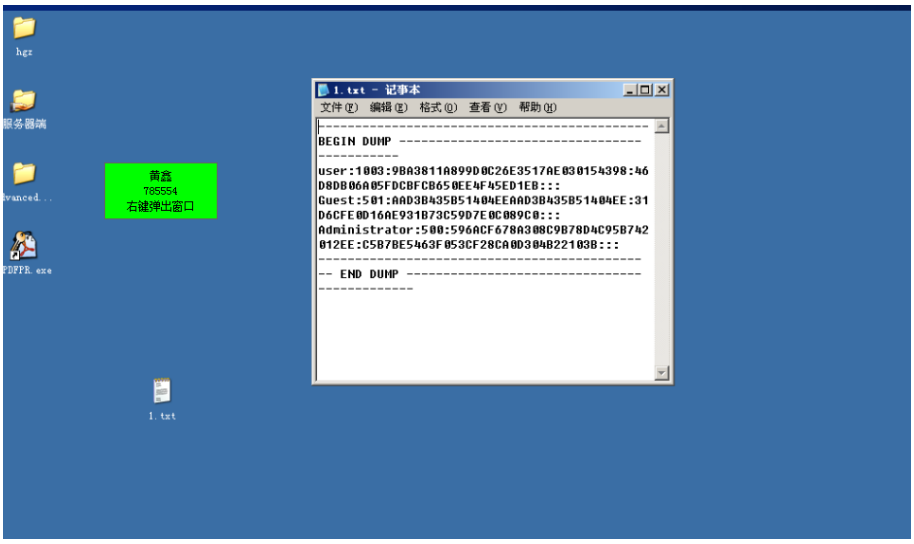
八、实验步骤：

（1）打开开始菜单，找到“运行”,输入 cmd。

（2）找到 Pwdump 工具，工具位置在(C:\实验工具集\02_主机安全\02_Windows 口令安全与破解\第 1 节 pwdump 导出本地 SAM 散列)。在 cmd 命令行中输入：cd C:\实验工具集\02_主机安全\02_Windows 口令安全与破解\第 1 节 pwdump 导出本地 SAM 散列。继续在 cmd 中输入命令：pwdump.exe。如图 3 所示。进入了 pwdump 的界面，我们输入 pwdump.exe --dump-hash-local 命令，即可获得当前用户名的 SAM 值。



（3）我们成功的获得了当前用户表的 hash 值，至此实验结束。如果遇到闪退 BUG，可执行 pwdump.exe --dump-hash-local>1.txt，这样 SAM 信息会被导出在 pwdump.exe 目录下的 1.txt 中。



九、实验数据及结果分析：

成功获取用户 sam 值，总共有三部分组成，user、guest、adiministrator，最终导入本地 txt 文件，然后进行下一步的导入分析。

十、实验结论：

pwdump 能够成功导出系统 sam 值

十一、总结及心得体会：

在这个实验中，我们学习了如何使用 pwdump 工具来导出本地 SAM 散列。本

地 SAM（Security Account Manager）数据库存储了 Windows 操作系统用户账户的安全信息，包括用户密码的散列值。pwdump 是一个常用的工具，可以帮助我们提取这些散列值，并在后续的研究、渗透测试或安全审计中发挥重要作用。

十二、对本实验过程及方法、手段的改进建议：

除了使用 pwdump 工具之外，还可以探索其他获取密码散列的方法和工具。例如，使用更安全的方法来获取散列，如使用 Windows API 进行访问，或者使用更加隐蔽的技术进行密码破解。

报告评分：

指导教师签字：

电子科技大学 计算机科学与工程（网络空间安全）学院

标 准 实 验 报 告

（实验）课程名称 信息对抗综合设计实验

电子科技大学教务处制表

电 子 科 技 大 学

实 验 报 告

学生姓名： 黄鑫 学号： 2021050901013 指导教师：汪小芬

实验地点： 主楼 A2-413-1 实验时间：2023.10.10

一、实验室名称：主楼 A2-413-1

二、实验项目名称：Windows 本地密码破解

三、实验学时：4

四、实验原理：

(1)口令：也称通行字（password），应该说是保护计算机和域系统的第一道防护门，如果口令被破解了，那么用户的操作权和信息将很容易被窃取。所以口令安全是尤其需要关注的内容。

(3)口令的攻击方式: 词典攻击、强行攻击、组合攻击、常见攻击方式的比较、其他攻击方式

(4) 口令破解方式概述:手工破解、自动破解

手工破解：手工破解攻击者要猜测口令必须手动输入。要完成这一攻击，必须知道用户的 userID 并能进入被攻系统的登陆状态。这种方法简单但费时。其步骤为:产生可能的口令列表按口令的可能性从高到低排序输入每个口令如果系统允许访问则成功如果没有成功，则重试。注意不要超过口令的限制次数

自动破解：只要得到了加密口令的副本，就可以离线破解。这种破解在脱机的情况下完成的，速度快。其原因是使用了程序搜索一串单词来检查是否匹配，这样的话就能同时破解多个口令。自动破解的步骤找到可用的 userID 找到所用

的加密算法获取加密口令创建可能的口令名单对每个单词加密对所有的 userID 观察是否匹配重复以上过程，直到找到所有口令为止

（5）Windows 口令破解工具

五、实验目的：

理解 LC5 破解本地 SAM 散列的原理、学习 LC5 破解本地 SAM 散列的过程

六、实验内容：

本次环境是模拟黑客在已经获得目标机 HASH 的情况下，通过 LC5 的密码字典对目标 HASH 进行破解

七、实验器材（设备、元器件）：

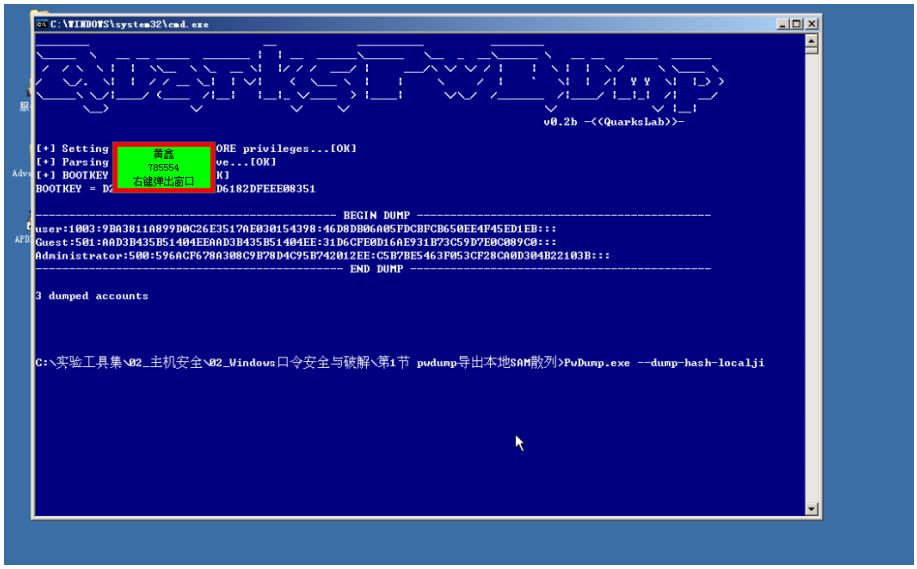
windows server 2003

Pwdump 工具

LC5 加密破解工具

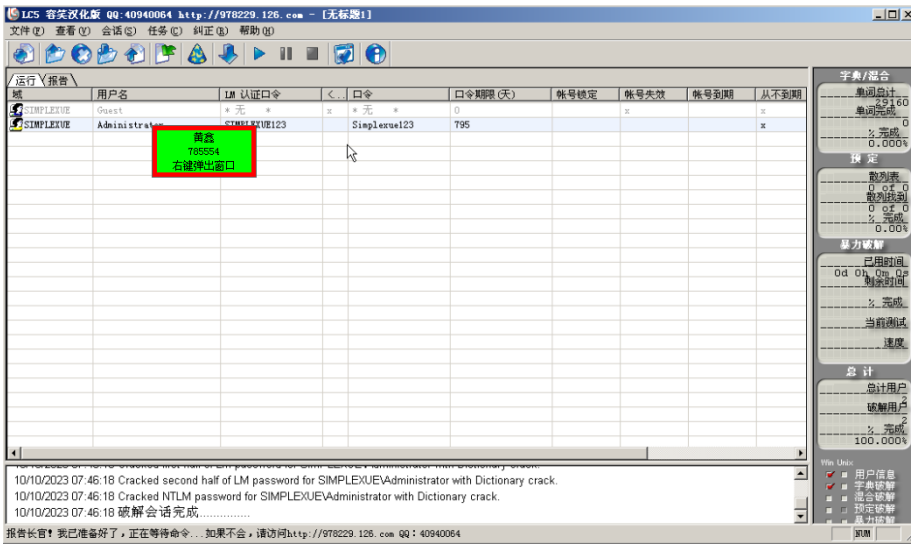
八、实验步骤：

（1）找到 Pwdump 工具，工具位置在(C:\实验工具集\02_主机安全\02_Windows 口令安全与破解\第 1 节 pwdump 导出本地 SAM 散列)。在 cmd 命令行中输入：cd C:\实验工具集\02_主机安全\02_Windows 口令安全与破解\第 1 节 pwdump 导出本地 SAM 散列。继续在 cmd 中输入命令：PwDump.exe.进入了 pwdump 的界面，我们输入 PwDump.exe --dump-hash-local 命令，即可获得当前用户名的 SAM。

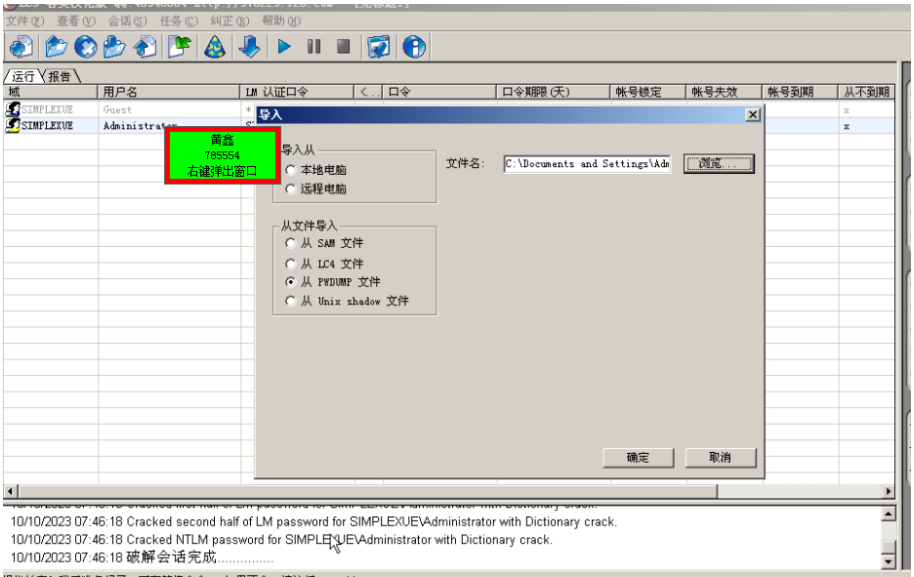


（3）右键标记，复制到文本中，并保存到桌面上。

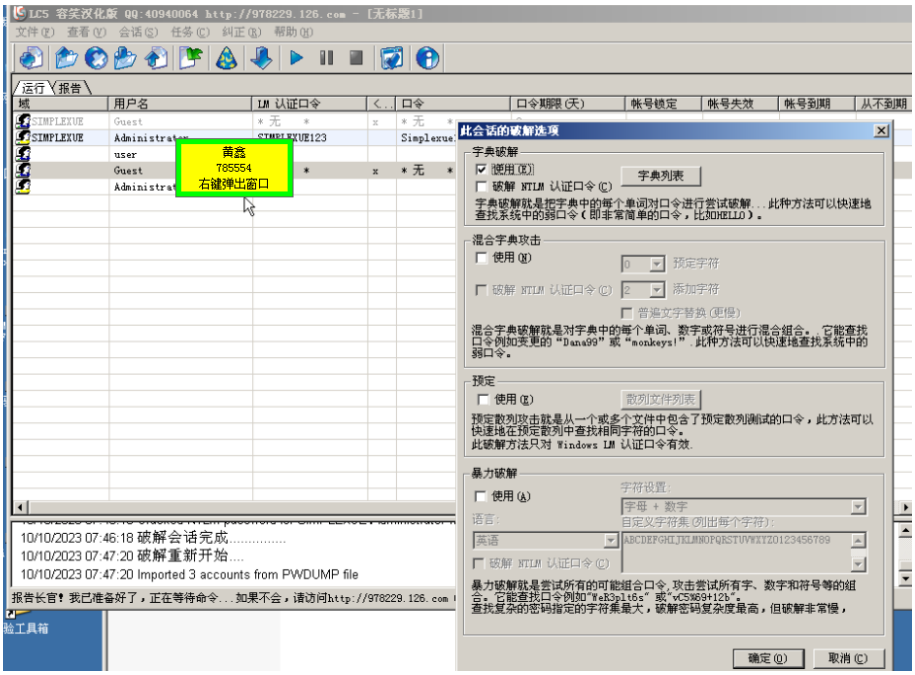
(4) 获得系统密码打开 C:\实验工具集\02_主机安全\02_Windows 口令安全与破解\第二节 LC5 破解本地 SAM 散列，打开 lc5 文件夹后，打开 lc5.exe（若弹出向导，单击下一步直至完成）。



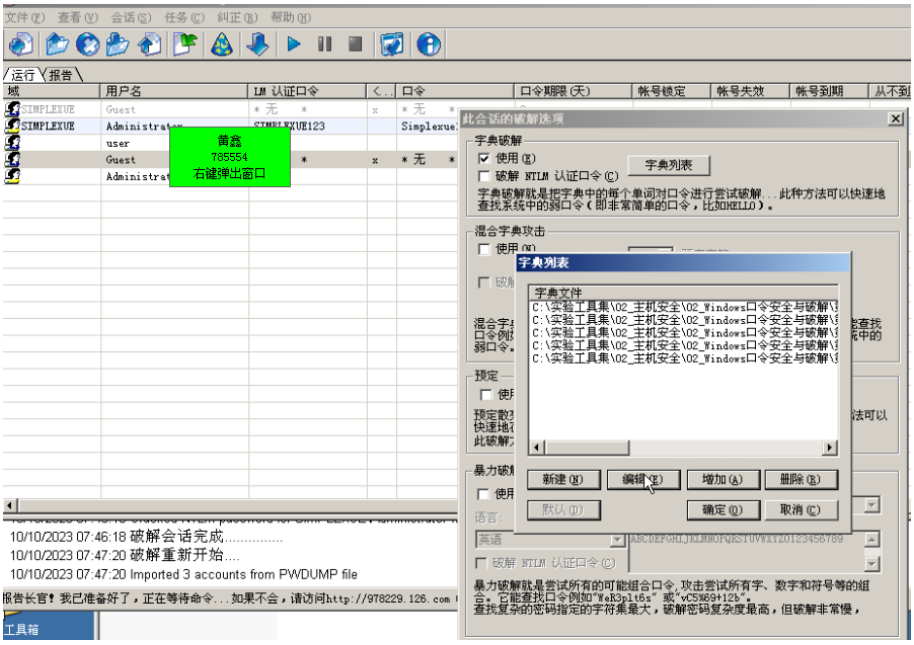
(5)打开绿色标识”导入”并选择”PWDUMP 文件导入”选项。单击”浏览”按钮,选择我们已经保存到桌面上的密码文件,单击确定。



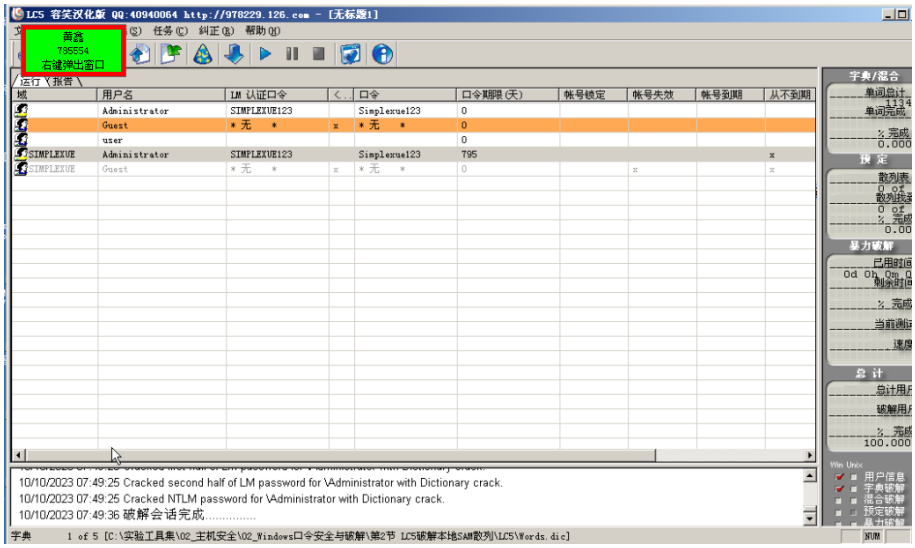
(6)选择我们存放 hash 值的文档。单击”会话”->”会话选项”，导入密码表格。



(7)单击”字典列表”->”增加”->选择字典文件->单击”确定”按钮（字典文件在软件目录下，以 dic 结尾），单击确定。



(8)点击”开始破解”按钮，开始破解。密码被成功破解出来。至此，LC5 破解本地 SAM 实验完成。



九、实验数据及结果分析：

初始口令：SIMPLEXUE123

破解得到：simplexue123

验证正确

十、实验结论：

通过本地运行 pwdump 工具导出本地散列，然后利用 LC5 破解工具，对于初始口令进行破解，对于一般复杂度的口令可以在几秒内进行破解，最后验证结果得到正确。

十一、总结及心得体会：

通过这次实验，我学到了如何使用工具来导出本地 SAM 散列并使用 LC5 破解工具来尝试恢复口令。这让我认识到了口令安全的重要性，以及黑客可能采取的方法。在保护计算机和系统安全方面，我更明白了需要采取一系列措施，如使用强密码、定期更改口令和监控系统的安全性。同时，我也了解到了黑客可能使用的工具和技术，这有助于我更好地了解网络安全的挑战和应对方法。

十二、对本实验过程及方法、手段的改进建议：

在实验过程中，应明确强调只能在合法的环境下进行口令破解实验，不得用于非法目的。这有助于强调道德和合法性。对 LC5 破解工具的使用可以提供更多解释，例如，为什么选择特定的字典文件，如何创建更强密码等信息，以帮助读者更好地理解口令破解的细节。

报告评分：

指导教师签字：

电子科技大学 计算机 学院

标 准 实 验 报 告

（实验）课程名称 信息对抗综合实验

电子科技大学教务处制表

电 子 科 技 大 学

实 验 报 告

学生姓名：黄鑫　　学 号：2021050901013　指导教师：汪小芬

实验地点：主楼 A2-413-1　　实验时间：10.10

一、实验室名称：主楼 A2-413-1

二、实验项目名称：saminside 破解本地 sam 散列

三、实验学时：4

四、实验原理：

Windowshash 由二部分组成，分别是 LM HASH&NT HASH。Windows 系统关于 hash 的组成如下：

用户名称:RID:LM-HASH 值:NT-HASH 值

1.LMHASH 生成规则

（1）用户的密码被限制为最多 14 个字符。

（2）用户的密码转换为大写。

（3）系统中用户的密码编码使用了 OEM 内码页。

（4）密码不足 14 字节将会用 0 来补全。

（5）固定长度的密码被分成两个 7byte 部分。每部分转换成比特流，在分 7bit 为一组末尾加 0，组成新的编码。

（6）上步骤得到的 8byte 二组，分别作为 DESkey 为“KGS!@#$%”进行加密。

（7）将二组 DES 加密后的编码拼接，得到最终 LMHASH 值。

2. NThash 生成原理

IBM 设计的 LMHash 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，NTLMHash 便应运而生。假设明文口令是”123456”，首

先转换成 Unicode 字符串，与 LMHash 算法不同，这次不需要添加 0 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。0×80 之前的标准 ASCII 码转换成 Unicode 码,就是简单地从 0x 变成 0×00。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 0×00。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，就得到了最后的 NTLMHash。

NTLM Hash:32ED87BDB5FDC5E9CBA88547376818D4。

五、实验目的：

1.理解 saminside 破解本地 sam 散列的原理

2.学习 saminside 破解本地 sam 散列的过程

六、实验内容：

通过 pwdump 工具得到本地 sam 序列后，使用 saminside 破解本地 sam 散列

七、实验器材（设备、元器件）：

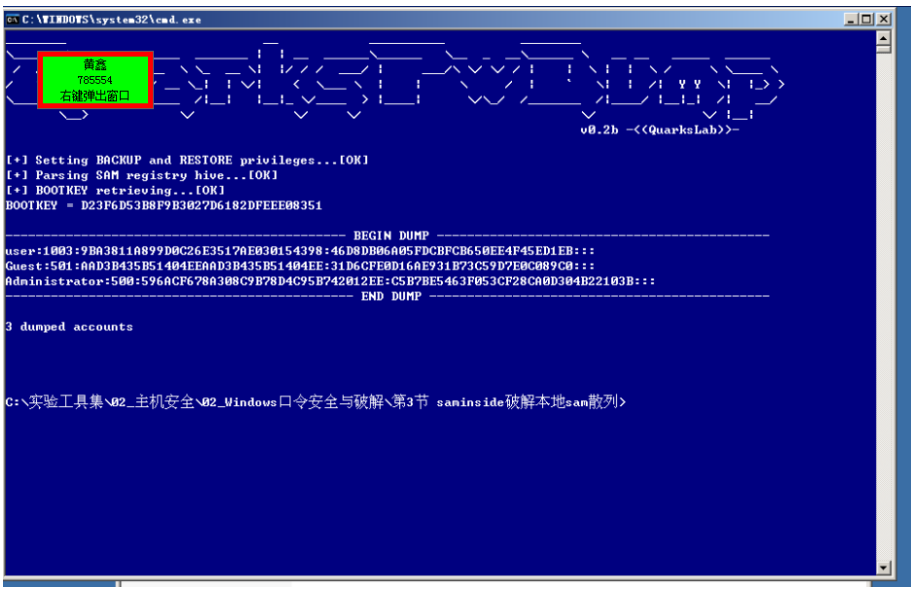
windows server 2003 虚拟机

pwdump 工具

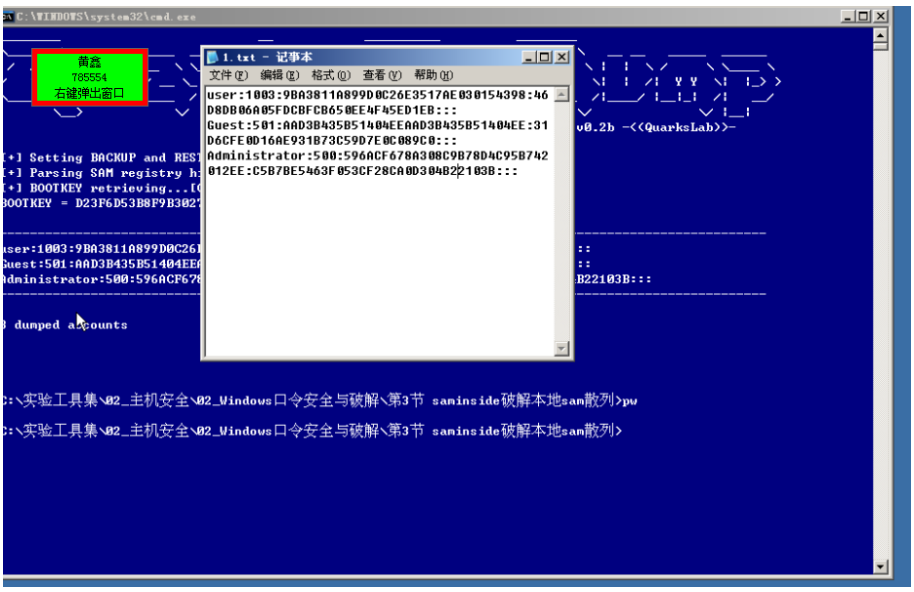
saminside 密码破解工具

八、实验步骤：

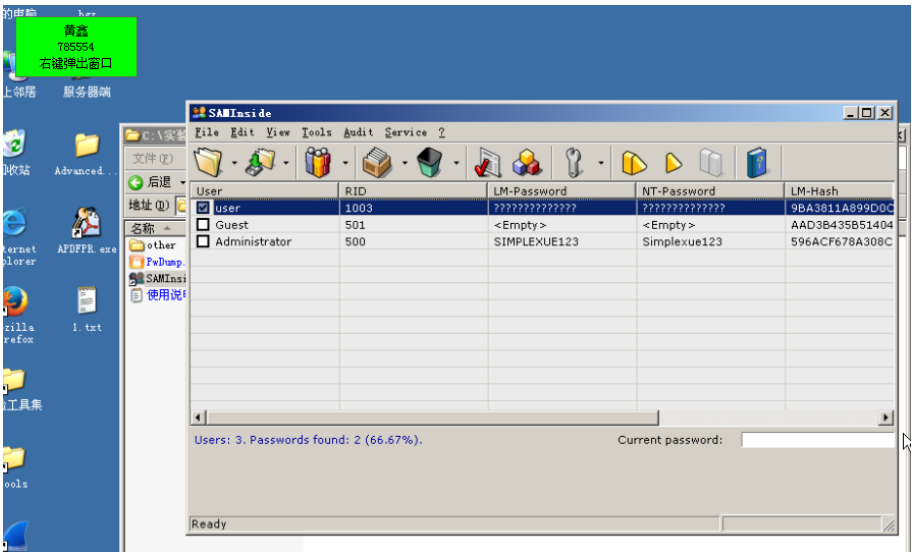
（1）打开 cmd 命令行，切换至 C:\实验工具集\02_主机安全\02_Windows 口令安全与破解\第 3 节 saminside 破解本地 sam 散列，在 cmd 下打开 PwDump.exe。直接在 cmd 中输入命令 pwdump.exe。以上就是进入了 pwdump 的界面，我们输 PwDump.exe--dump-hash-local 命令，即可获得当前用户名的 SAM。我们成功的获得了当前用户表的 hash 值.



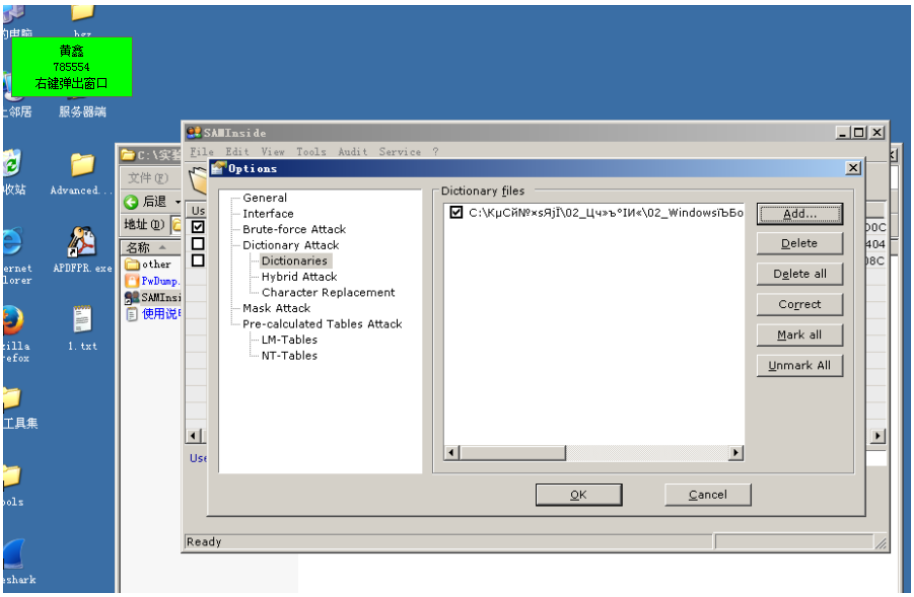
（2）右键标记，复制到文本中，并保存到桌面上。



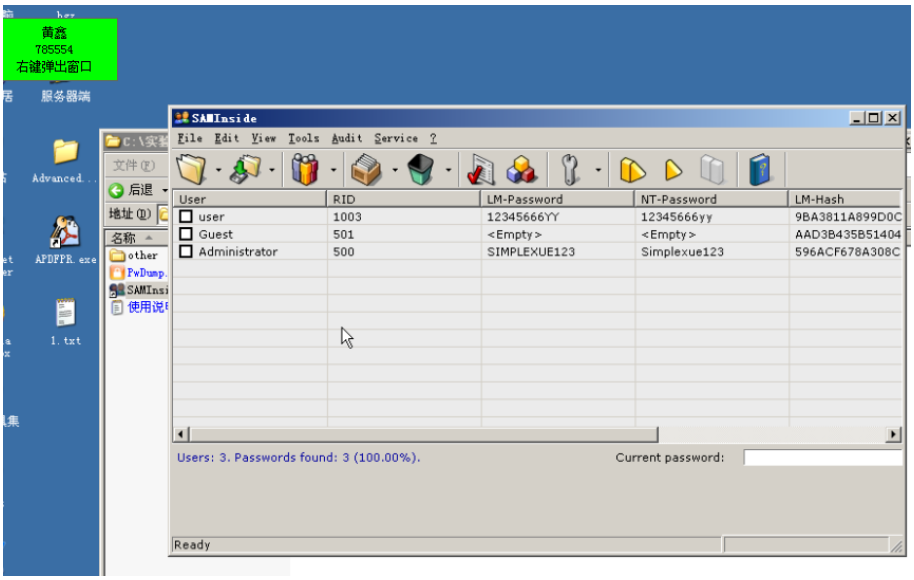
（3）打开 C:\实验工具集\02_主机安全\02_Windows 口令安全与破解\第 3 节 saminside 破解本地 sam 散列文件夹，打开 SAMInside.exe。导入我们保存在桌面的 HASH 值文档。选中要破解的账户。点击’audit’,依次勾选‘NT-HASH ATTACK’和’ Dictionary ATTACK ‘。点击工具箱下的 opintos 选项。



（4）选择 Dictionaries 选项。选择‘add‘,选项，添加 C:\实验工具集\02_主机安全\02_Windows 口令安全与破解\第 3 节 saminside 破解本地 sam 散列\other\SAMInside\Dictionaries 文件夹下的 InsidePro(Mini).dic 密码字典。



（5）选择开始按钮，密码被破解出来，至此实验结束。



九、实验数据及结果分析

所有密码都被破解出来，LM-Password:SIMPLEXUE123,NT-Password:simplexue123,然后可以通过对应的工具看出 Hash 值，经过验证结果正确。

十、实验结论：

Saminside 能够成功破解本地 sam 散列

十一、总结及心得体会：

Saminside 作为一种密码破解工具，为我们提供了对密码安全的实践认识。通过理解和学习 Saminside 破解本地 SAM 散列的过程，我对密码破解技术有了更深入的了解，并加深了对密码安全的重要性的认识。在实际应用中，我们应该采取适当的措施来保护个人和组织的密码安全，以防止密码被破解和滥用。

十二、对本实验过程及方法、手段的改进建议：

密码破解工具的存在提醒我们密码的安全性至关重要。建议在实验过程中加强密码策略的意识，使用强密码并定期更换密码。此外，推广使用多因素认证等更安全的身份验证方法。

报告评分：

指导教师签字：

电子科技大学 计算机 学院

标 准 实 验 报 告

（实验）课程名称 信息对抗综合实验

电子科技大学教务处制表

电 子 科 技 大 学

实 验 报 告

学生姓名：黄鑫　　学 号：2021050901013　指导教师：汪小芬

实验地点：主楼 A2-413-1　　实验时间：10.10

一、实验室名称：主楼 A2-413-1

二、实验项目名称：Opcrack 挂彩虹表破解本地 sam 散列

三、实验学时：4

四、实验原理：

彩虹表是一个用于加密散列函数逆运算的预先计算好的表,常用于破解加密过的密码散列。一般主流的彩虹表都在 100G 以上。查找表常常用于包含有限字符固定长度纯文本密码的加密。这是以空间换时间的典型实践,在每一次尝试都计算的暴力破解中使用更少的计算能力和更多的储存空间,但却比简单的每个输入一条散列的翻查表使用更少的储存空间和更多的计算性能。使用加盐的 KDF 函数可以使这种攻击难以实现令。

为了保证后台数据安全,现在的做法都是使用哈希算法对明文密码进行加密存储.由于哈希算法不可逆向,因此由密码逆向出明文运算就成了不可能。起初黑客们通过字典穷举的方法进行破解,这对简单的密码和简单的密码系统是可行的,但对于复杂的密码和密码系统,则会产生无穷大的字典.为了解决逆向破解的难题,黑客们就产生了彩虹表的技术。

为了解决所需要字典大小，减少产生和查找字典的时间,黑客选择性存储一个较小的可逆向的长链的密码的哈希值。虽然在破解单个密文,使用哈希链接的方式需要更多的计算时间的反向查找，但字典要小得多，因此可以存储更长的密码的哈希值。彩虹表是此链接技术的一种改进，并提供一种称为碰撞链的解决方

案。其基于 MartinHellman 理论(基于内存与时间的权重理论)

彩虹表打大小依据需要而定，有上 T 数据的彩虹表，也有几百 M 的数据，不同的情况下选择不同的彩虹表，可以快速得到结果。

五、实验目的：

1. 理解 Opcrack 挂彩虹表破解本地 sam 散列的原理
2. 学习 Opcrack 挂彩虹表破解本地 sam 散列的过程

六、实验内容：

使用 Opcrack 挂彩虹表破解本地 sam 散列

七、实验器材（设备、元器件）：

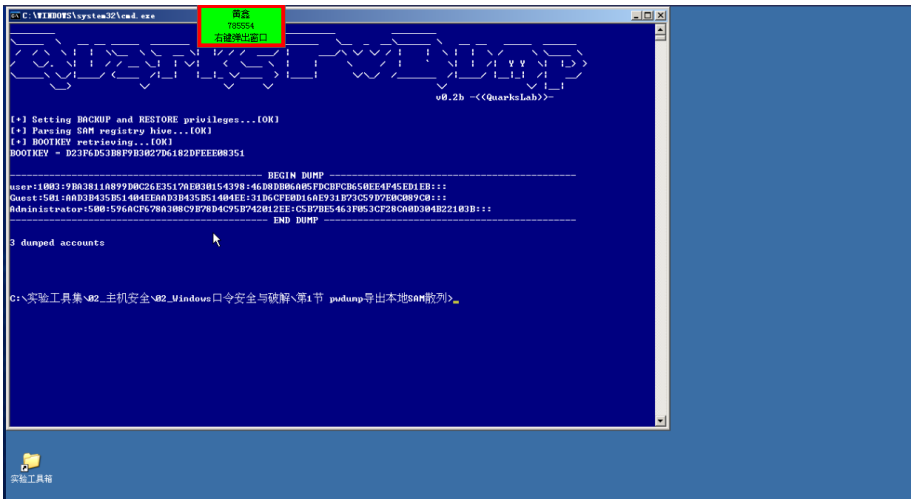
windows server 2003 虚拟机

pwdump 工具

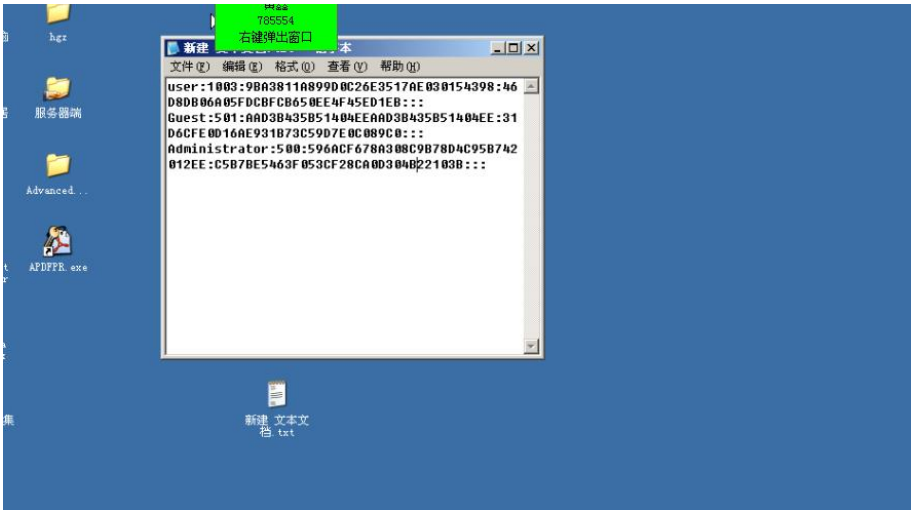
Opcrack 工具

八、实验步骤：

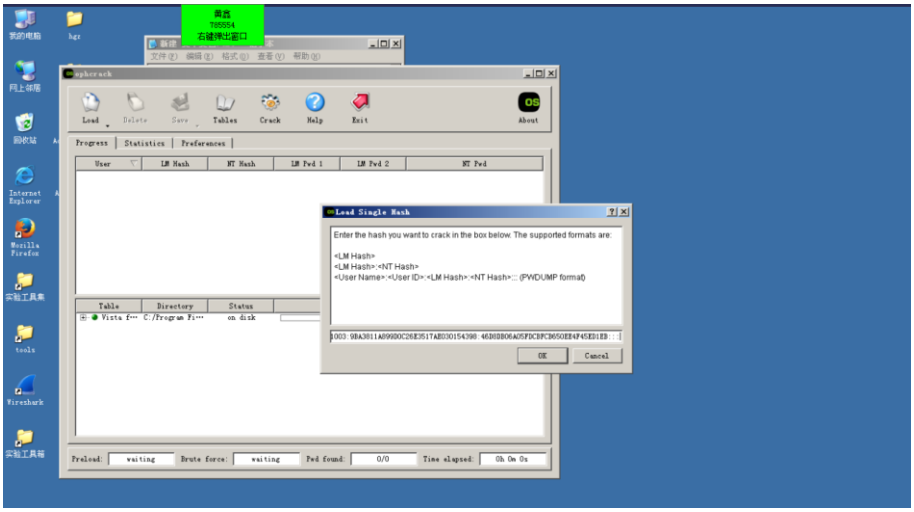
（1）获得系统 SAM 值打开 cmd 命令行，切换至 C:\实验工具集\02_主机安全\02_Windows 口令安全与破解\第 3 节 saminside 破解本地 sam 散列，在 cmd 下打开 PwDump.exe。直接在 cmd 中输入命令 pwdump.exe。以上就是进入了 pwdump 的界面，我们输 PwDump.exe--dump-hash-local 命令，即可获得当前用户名的 SAM，我们成功的获得了当前用户表的 hash 值。



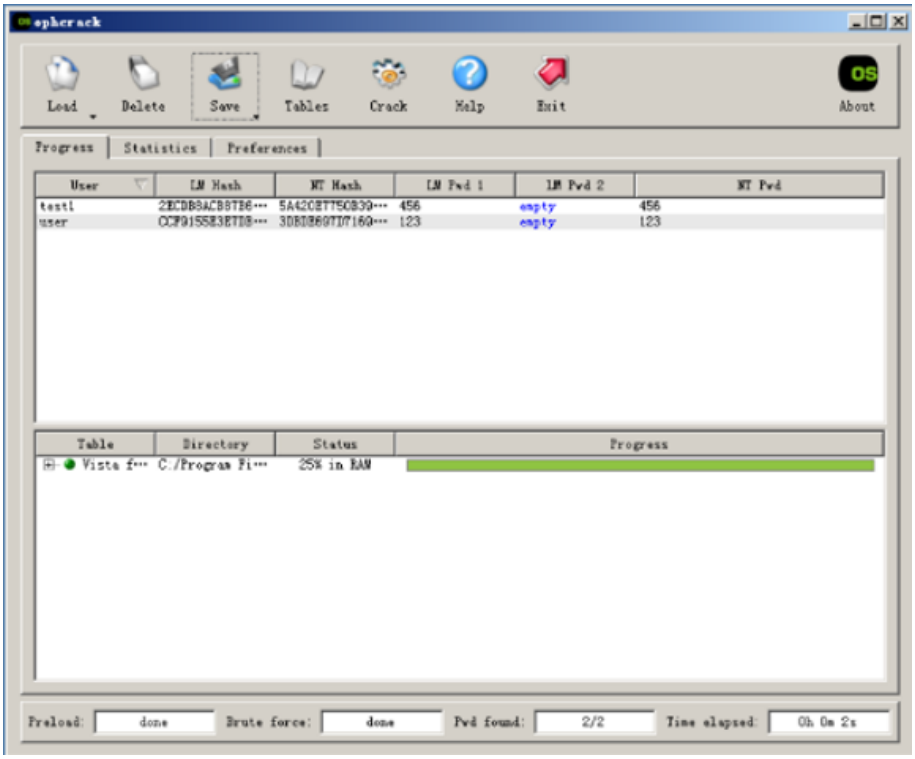
（2）右键标记，复制到文本中，并保存到桌面上。如图 3 所示



（3）使用 Opcrack 挂彩虹表破解本地 sam 打开 C:\实验工具集\02_主机安全\02_Windows 口令安全与破解\第 4 节 Opcraack 挂彩虹表破解本地 SAM 散列文件夹中的 ophcrack.exe 点击”Load”按钮,选择 Single hash。把我们保存在文档中的 hash 单独复制出来。确定后,我们点击软件的 Crack。点击工具箱下的 opintos 选项。



（4）等待破解，成功后会在软件中显示。



九、实验数据及结果分析：

只有部分密码被破解，复杂度较高的密码难以被破解

十、 实验结论：

尽管本次实验成功破解了部分密码，但仍有一部分密码未能被破解。这可能是由于密码强度较高、密码长度较长或者不在所使用的彩虹表中等原因导致的。

十一、总结及心得体会：

Opcrack 作为一种彩虹表破解工具，展示了其在破解弱密码方面的有效性。对于密码弱度较低、长度较短或常见密码等，Opcrack 能够快速找到匹配的散列值，从而成功破解密码。这表明使用强密码是至关重要的，以提高密码的安全性。

十二、对本实验过程及方法、手段的改进建议：

在实验中，可以尝试使用更大、更全面的彩虹表来提高破解密码的成功率。彩虹表的大小和覆盖范围直接影响破解的效果，因此可以考虑使用更多的资源来构建更强大的彩虹表。

报告评分：

指导教师签字：