第 3 章

口令攻击和防护

3.1 概　　述

身份认证是验证主体的真实身份与其所声称的身份是否相符的过程，它是信息系统的第一道安全防线，如果身份认证系统被攻破，那么信息系统其他所有安全措施将形同虚设，因此，身份认证是信息系统其他安全机制的基础。

口令(Password)俗称密码，是由数字、字母等构成的一个字符串，是只有用户自己和计算机信息系统知道的秘密信息，基于口令的认证简单易行，是最常用的身份认证方式。口令攻击是最易被攻击者考虑的攻击途径，攻击者会采用多种方法试图猜出用户设置的口令，尤其是猜测出管理员的口令以进入系统实施进一步破坏。从安全的角度来说，对口令攻击进行防范、在口令攻击发生时进行告警是安全防护的一个重要内容。

3.2 口令攻击技术

3.2.1 Windows 系统下的口令存储

口令认证机制是 Windows 系列操作系统提供的最基本的身份认证方式。Windows 操作系统口令采用两种加密算法加密后存储在 SAM(Security Account Manager)数据库中，一般位于 $SystemRoot/System32/Config/目录下，每个用户信息格式形如：Administrator:500:C8825DB10F2590EAAAD3B435B51404EE:683020925C5D8569C23AA724774CE6CC:::，其中 Administrator 为用户名，500 为 RID 号，C8825DB10F2590EAAAD3B435B51404EE 为口令经 LM-Hash 算法加密后的值，683020925C5D8569C23AA724774CE6CC 为口令经 NTLM-Hash 算法加密后的值。

LM-Hash 算法过程如下。

(1) 将用户口令字中的小写字母改写成大写字母。当口令长度大于 14 个字符时只取 14 个，当口令长度不足 14 个时用空格(ASCII 码值 0X20)补足为 14 个字符。

(2) 将用户口令所确定的 14 个字符按前 7 个和后 7 个分为两组，记为 K1 和 K2。

(3) 分别以 K1 和 K2 为密钥，用 DES 算法对固定明文 P0 加密，产生两个 8 字节的密文 C1、C2。其中 P0 为魔术字符串"KGS! @＃$%"，转化为十六进制值为 0X4843532140232425。

(4) 将两个 8 字节密文 C1、C2 连接为 16 字节的散列值。

LM Hash 算法采用了比较弱的 DES 加密算法，且不管用户设置的口令有多长，算法仅对前 14 个字符进行加密，因而采用增加口令长度、变换大小写等方法对增强口令安全无用，这种算法比较容易被破解，不够安全。为了保持向后兼容性，Windows Vista 之前的版本仍保留了这种加密机制。此后微软又提出了新的口令加密机制 NTLM Hash，其加密过程是将用户口令转换成 Unicode 编码，再利用 MD4 算法进行加密，就得到了最后的 NTLM Hash 值。NTLM Hash 算法采用了较安全的单向加密算法 MD4，且用户可通过增加口令长度、变换字母大小写等方法增强口令安全，相对于 LM Hash 算法来说，安全性更强，Windows Vista 之后的 Windows 系统中仅存储 NTLM Hash 算法加密的密文。

3.2.2　Linux 系统下的口令存储

Linux 是类 Unix 系统，基本沿用 Unix 中的安全机制。Linux 中所有与用户相关的信息存储在系统中的/etc/passwd 文件中，该文件是一个典型的数据库文件，每一行都由 7 个部分组成，每两个部分之间用冒号分隔开，包含用户的登录名、经过加密的口令等，其基本格式为：

```
username: password:uid:gid:comments:directory:shell
```

这 7 个部分分别描述了以下信息：用户名、口令、用户 ID、用户组 ID、用户描述、用户主目录、用户的登录 Shell，下面分别描述。

(1) 用户名：用户的登录名。

(2) 口令：用户的口令，以加密形式存放。该域值如为 x 表示口令存储在/etc/shadow 中。

(3) 用户 ID(UID)：系统内部以 UID 标识用户，范围为 0～32767 之间的整数。

(4) 用户组 ID(GID)：标志用户所在组的编号。将用户分组管理是 Unix 类操作系统对权限管理的一种有效方式。假设有一类用户都要赋予某个相同的权限，对用户分别授权将会很复杂，但如果把这些用户都放入一个组中，再给组授权，就容易多了。一个用户可以属于多个不同的组。组的名称和信息放在另一个系统文件/etc/group 中，与用户标识符一样，GID 的范围也是 0～32767 之间的整数。

(5) 用户描述：这个域中记录的是用户本人的一些情况，如用户名称、电话和地址等。该域的作用随着系统功能的增强，已经失去了原来的意义。一般情况下，约定该域存放用户的基本信息，也有的系统不需要该域。

(6) 用户主目录：这个域用来指定用户的主目录(home)，当用户成功进入系统后，他就会处于自己的用户主目录下。

一般情况下，管理员将在一个特定的目录里依次建立各个用户的主目录，目录名一般就是用户的登录名。用户对自己的主目录有完全控制的权限，其他用户对该目录的权限需要管理员手动分配。如果没有指定用户的主目录，用户登录时将可能被系统拒绝或获得对根目录的访问权，这是非常危险的。

(7) 用户的登录 Shell：Shell 程序是一个命令行解释器，它能够读取用户输入命令，并将执行结果返回给用户，实现用户与操作系统的交互，它是用户进程的父进程，用户进程多由 Shell 程序来调用执行。在 Unix 系统中有很多 Shell 程序，如/bin/sh、/bin/csh、/

bin/ksh 等，每种 Shell 程序都具有不同的特点，但基本功能是一样的。

在 Linux 中，用户登录时通常要求输入用户名、口令信息，用户名是标识，它告诉计算机该用户是谁，而口令是确认数据。Linux 使用改进的 DES 算法（通过调用 crypt()函数实现）对其加密，并将结果与存储在数据库中的加密用户口令进行比较，若两者匹配，则说明该用户为合法用户，否则为非法用户。

为了防止口令被非授权用户盗用，对其设置应以复杂、不可猜测为标准。一个好的口令应该满足长度和复杂度要求，并且定期更换，通常，口令以加密的形式表示，由于/etc/passwd 对任何用户可读，常成为口令攻击的目标，在后期的 Unix 版本以及所有 Linux 版本中，引入了影子文件的概念，将密码单独存放在/etc/shadow 中，而原来/etc/passwd 文件中存放口令的域用 x 来标记。文件/etc/shadow 只对 root 用户拥有读权，对普通用户不可读，以进一步增强口令的安全。

3.2.3 口令攻击的常用方法

口令攻击常用的方法包括字典攻击、暴力破解、混合破解。

字典攻击是一种典型的网络攻击手段，利用字典库中的数据不断进行用户名和口令的反复试探。一般攻击者都拥有自己的攻击字典，其中包括常用的词、词组、数字及其组合等，并在攻击过程中不断充实、丰富自己的字典库，攻击者之间经常也会交换各自的字典库。

暴力破解是让计算机尝试所有可能的口令，最终达到破解口令的目的。

混合破解介于字典破解和暴力破解之间，字典攻击只能发现字典库中的单词口令，暴力破解虽然一定能破解口令，但速度慢、破解时间长。混合破解综合了字典破解和暴力破解的优缺点，使用字典单词并以在单词尾部串接几个字母和数字的方法来反复试探用户名和口令，最终找到正确的口令。

按口令破解的时机，口令破解又分为在线和离线两种方式。在线破解是指攻击者在口令登录提示框中输入不同的随机口令来猜测正确的口令。目前，大多数账户都会设置一个账户锁定阈值（比如 5 次），当不成功登录次数超过阈值后就不允许登录，这样就可以锁定攻击者。因为在线猜测的局限性，今天大多数口令攻击采用离线破解的方式。利用离线破解方法，攻击者窃取口令密文文件（通常为摘要文件），破解时可以采用字典攻击或暴力破解方法，依次产生口令，然后生成这些口令的摘要（称为候选口令），将这些摘要与窃取到的摘要值进行比对，如果找到匹配项，则攻击者就能知道与摘要匹配的口令了，这种破解方法的效率比较低。改进方法是可以预先计算各口令的摘要值记录在数据文件中，在需要时直接调用数据文件破解，可以大幅度提高破解的效率，事先构造的 Hash 摘要数据文件被称为 Table 表，最有名的就是 Rainbow Table，也即彩虹表，后续实验中会依次采用字典攻击、暴力破解和彩虹表实施口令破解。

3.3 Windows 系统环境下的口令破解实验

3.3.1 实验目的

掌握 Windows 系统环境下的口令散列的提取方法；掌握利用 LC6 进行口令破解的

方法；理解设置复杂口令原则的必要性。

3.3.2　实验内容及环境

1. 实验内容

本实验主要通过 LC6(L0phtCrack 6)利用字典攻击、暴力破解实现对本地 Windows 系统的口令破解，并通过设置不同复杂度的口令来验证口令复杂度对口令破解难度的影响。

2. 实验环境

主流配置计算机一台，安装 Windows 7 操作系统、LC6 软件和 PWDUMP 7 软件。

LC6 是一款口令破解工具，管理员也可以使用该工具检测用户设置的口令是否安全，被普遍认为是当前最好、最快的 Windows 系统管理员账号口令破解工具。

PWDUMP 是一款 Windows 系统环境下的密码破解和恢复辅助工具。它可以将 Windows 系统环境下的口令散列，包括 NTLM 和 LM 口令散列从 SAM 文件中提取出来，并存储在指定的文件中。

3.3.3　实验步骤

1. 安装并运行 LC6

正确安装 LC6 软件后运行 LC6，出现如图 3.1 所示的 LC6 向导，向导通过 5 个步骤完成口令破解相关参数的设置。

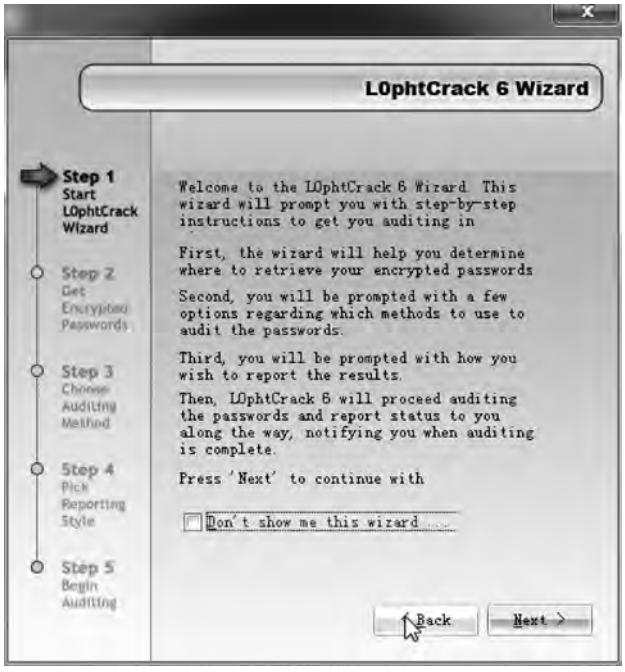

图 3.1　LC6 向导

2. 以默认设置破解本地账户口令

向导中的默认设置是以字典攻击方式破解本地账户口令信息，按照默认设置破解口令结果如图 3.2 所示，界面显示当前系统中的活动用户 lenovo 的口令为空。

图 3.2 破解系统账户口令

3. 添加测试用户

运行 cmd.exe，用 net user 命令给系统添加一个测试用户，并为该用户设置一个纯数字的口令，如图 3.3 所示。

图 3.3 为系统添加测试用户

4. 用 PWDUMP 导出口令散列

在命令行里运行 PWDUMP 工具，将导出的 Windows 系统 SAM 文件内容保存在 1.txt 文档中，如图 3.4 所示。

5. 查看 SAM 文件内容

打开 C:\PWDUMP 7\1.txt，可以看到 PWDUMP 7 将 Windows 系统环境下的口令散列从 SAM 文件中提取出来了，由于 Windows vista 之后的版本不再存储 LM 加密的密文信息，所以原来存储 LM 密文的用户信息的第三个域均为空，显示为 NO PASSWORD，如图 3.5 所示。

图 3.4　用 PWDUMP 导出口令散列

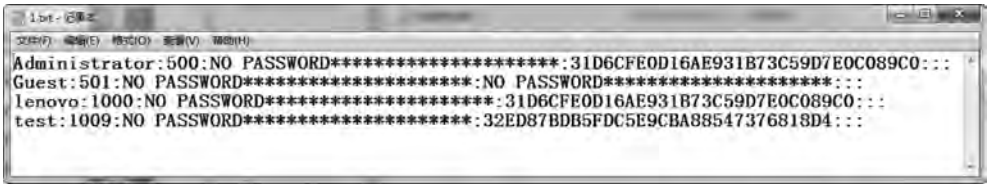

图 3.5　导出的口令散列内容

6. 设置口令破解方式

在 LC6 主界面上单击 Session Options 图标，出现如图 3.6 所示的界面，该界面主要用于设置口令破解参数，默认情况下采用字典攻击方式破解 LM 口令，由于在 Windows 7 操作系统中不存储 LM 口令，因而需要勾选 Crack NTLM Passwords 选项，设置为采用字典攻击方式破解 NTLM 口令，单击 Dictionary 图标，可以编辑查看字典文件。

7. 加载破解目标

L6 软件启动时就已经为用户建立了一个默认的会话，在此基础上单击 Import Hashes 图标，加载要破解的系统信息，在选项卡 Import from file 中选择 From PWDUMP，单击右侧的 Browse 按钮，选择 PWDUMP 文件，这里选择刚刚利用 PWDUMP 工具导出的 1.txt 文件，设置完成后，单击 OK 按钮，完成口令文件的导入，如图 3.7 所示。

8. 实施破解

单击工具栏上的 Begin 图标开始破解，可以发现 test 用户的口令 123456 被成功破解，如图 3.8 所示。

修改 test 用户的口令，设置为 A123DF，按照刚才的步骤重新加载口令文件，采用字典攻击的方式进行攻击，可以看到无法攻击成功，原因是字典文件中不包含口令 A123DF，如果在字典中加入该口令，则可破解口令。

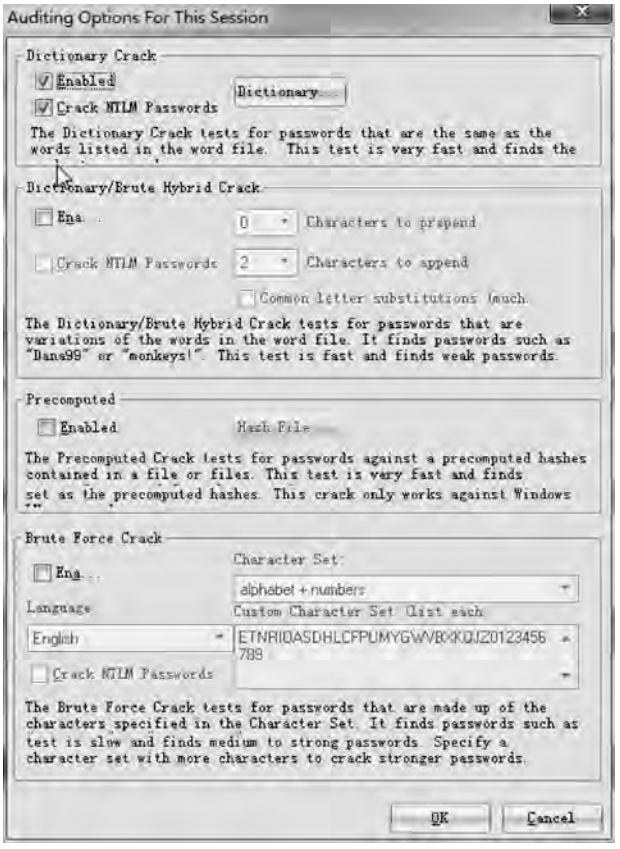

图 3.6　设置口令破解方式

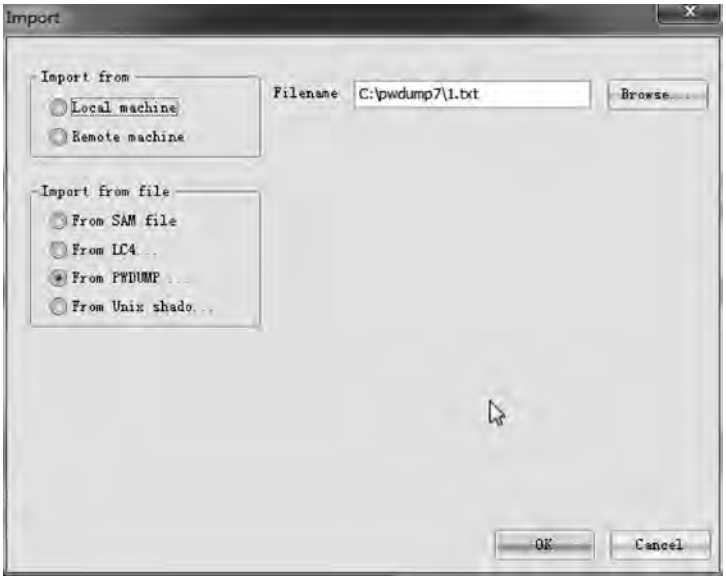

图 3.7　设置口令文件导入方式

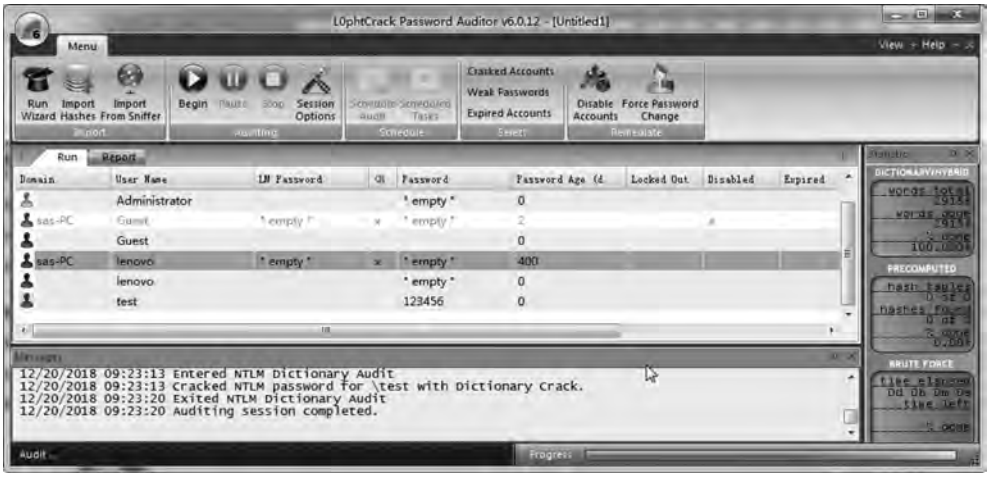

图 3.8　本地用户口令被破解

9. 暴力破解

打开 Auditing Options For This Session 界面，在 Brute Force Crack 栏中勾选 Enabled，在右侧的 Character Set 栏中设置暴力破解方式，设置完成后单击 OK 按钮，如图 3.9 所示。

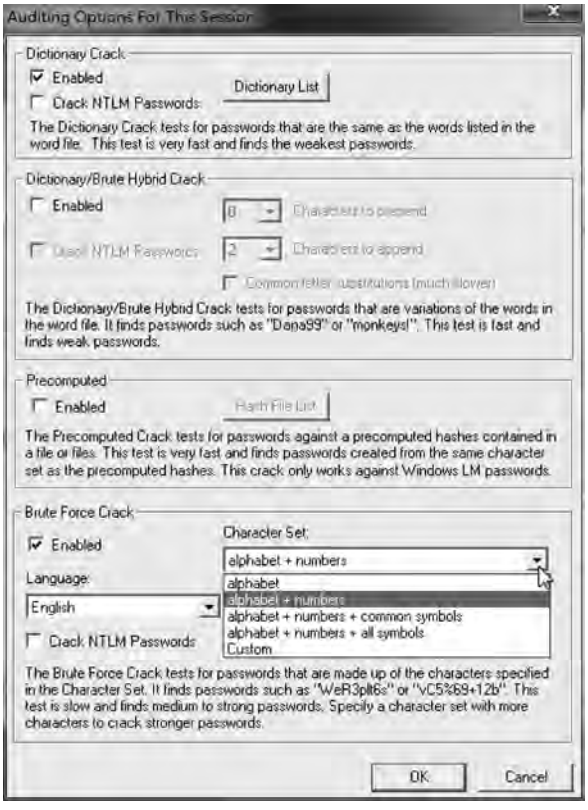

图 3.9　设置口令破解方式为暴力破解

单击主界面工具栏上的 Begin 图标开始破解，等待一段时间可以看到口令被破解。设置不同位数和字符集的口令，以观察利用暴力破解方法进行口令猜测的时间。

3.4 采用彩虹表进行口令破解实验

3.4.1 实验目的

理解彩虹表(Rainbow Table)口令破解的原理，掌握利用 Ophcrack 工具进行口令提取、散列表加载和口令破解的方法。

3.4.2 实验内容及环境

1. 实验内容

本实验通过使用开源彩虹表破解工具 Ophcrack 对 Windows 系统环境下的口令进行破解。

2. 实验环境

主流配置计算机一台，安装 Windows 7 操作系统、Ophcrack 软件和彩虹表文件 vista_proba_free.zip。

彩虹表是一个庞大的、针对各种可能的字母组合预先计算好的哈希值的集合，其各种算法都有，可以快速破解各种密码。越是复杂的密码，需要的彩虹表就越大，主流彩虹表的大小都是在 100GB 以上，本实验采用的是 600MB 的彩虹表，它只能破解较为简单的口令，破解复杂的口令需要下载更大的彩虹表。

Ophcrack 是一个使用彩虹表来破解 Windows 操作系统口令散列的程序，它是基于 GPL 发布的开源程序，利用内嵌的工具可以提取 Windows SAM 文件的散列值进行破解。对于 LM(LAN Manager)散列，使用免费的彩虹表，可以在短至几秒内破解最多 14 个英文字母的口令，成功率达 99.9%。对于 Windows Vista 之后的系统，SAM 中已经不再存储 LM 散列，而只存储 NTLM 散列，从 Ophcrack2.3 版开始可以破解 NTLM 散列。对于 NTLM 散列，一般的彩虹表破解能力大大降低，本实验仅针对 7 位小写字母组成的口令，使用该工具可以在较短时间内破解。

3.4.3 实验步骤

1. 添加账户

在系统中运行 cmd.exe，用 net user 命令修改 test 用户的口令为 7 位小写字母口令，如图 3.10 所示。

2. 安装运行 Ophcrack

按默认配置安装 Ophcrack，运行 ophcrack.exe，主界面如图 3.11 所示。

3. 安装彩虹表

将彩虹表文件 vista_proba_free.zip 解压，打开 Ophcrack，单击工具栏上的 Tables 按钮，进入彩虹表安装对话框，如图 3.12 所示，在 Tables 栏中选择 Vista probabilistic free，

图 3.10　添加测试用户

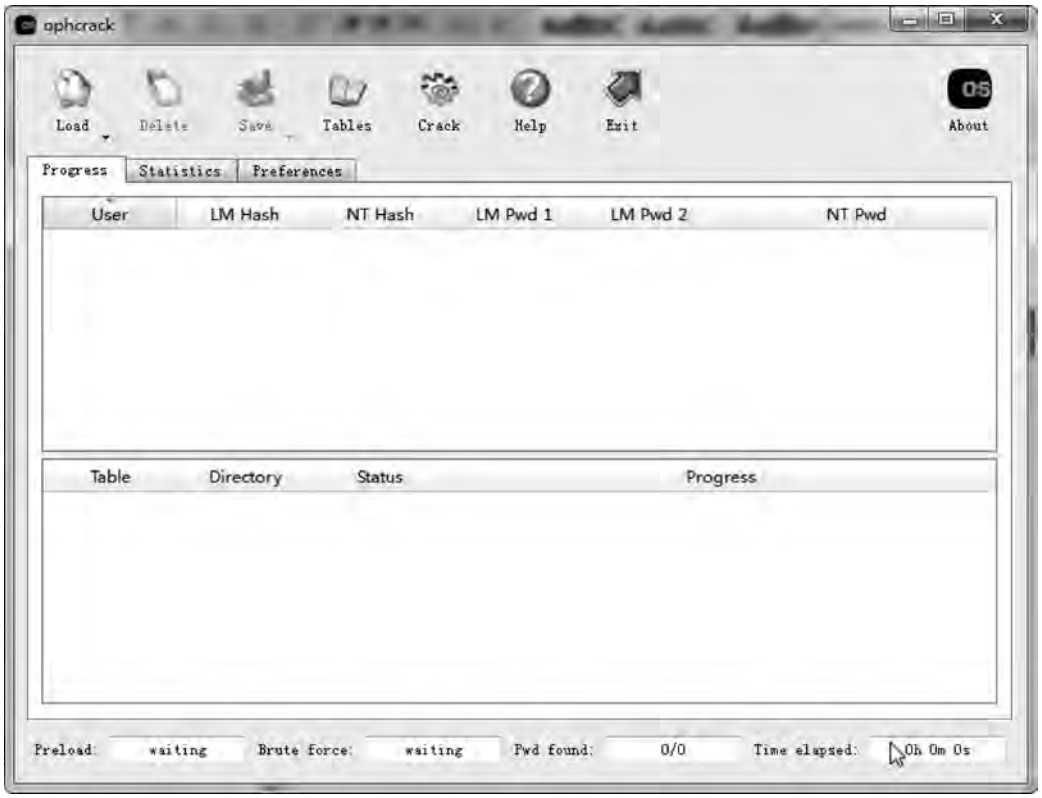

图 3.11　Ophcrack 主界面

单击 Install 按钮，选择彩虹表文件 vista_proba_free 路径，单击 OK 按钮。

4. 选择散列文件加载方式

在 Ophcrack 主界面上，单击 load 图标，在其下拉菜单中选择 Local SAM with samdump2 散列加载方式，如图 3.13 所示。

从 SAM 文件中提取口令散列并加载，如图 3.14 所示。

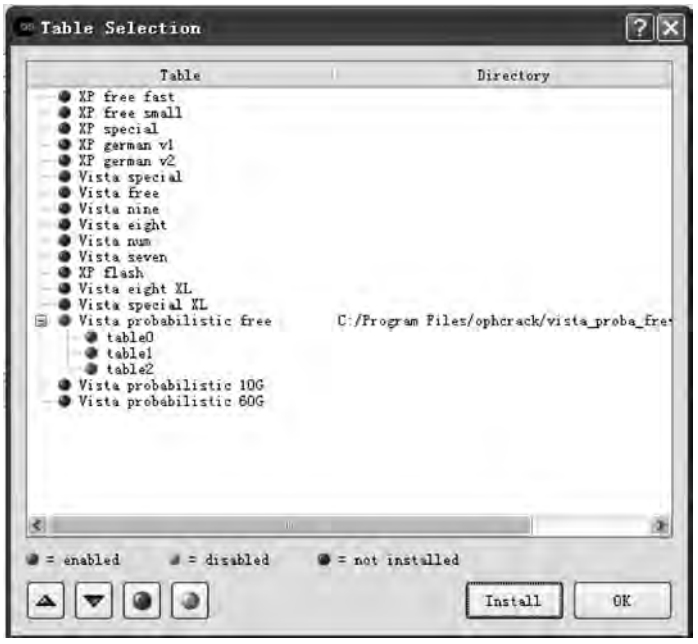

图 3.12　安装彩虹表

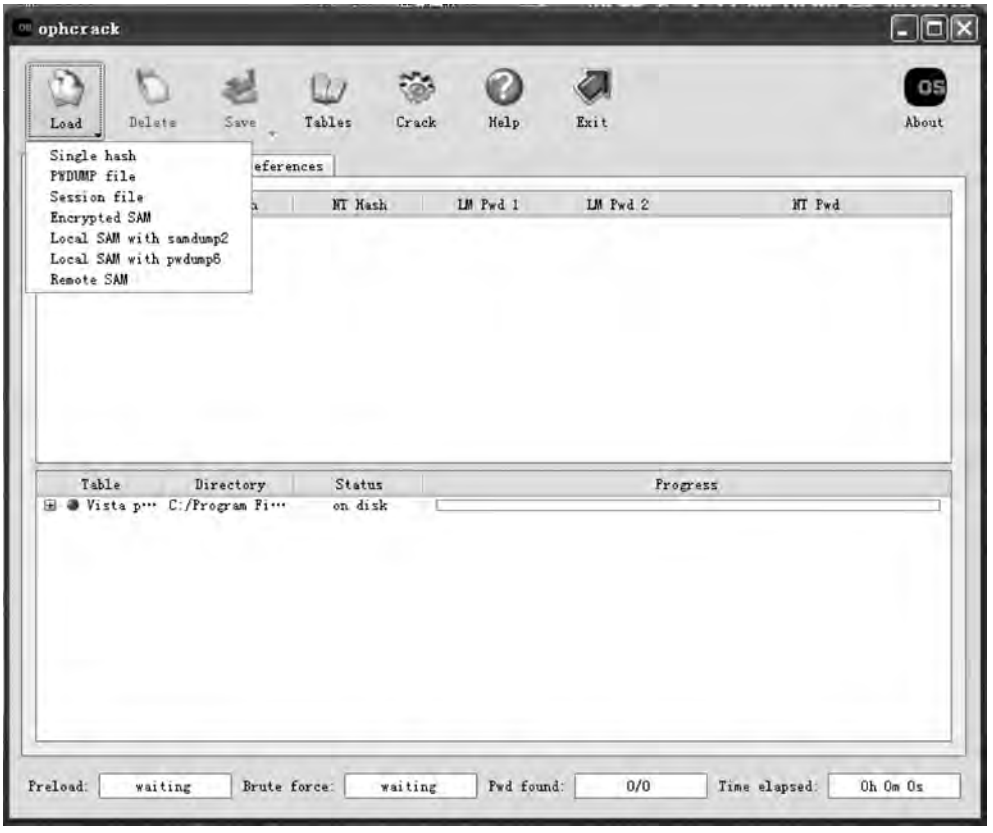

图 3.13　选择口令散列加载方式

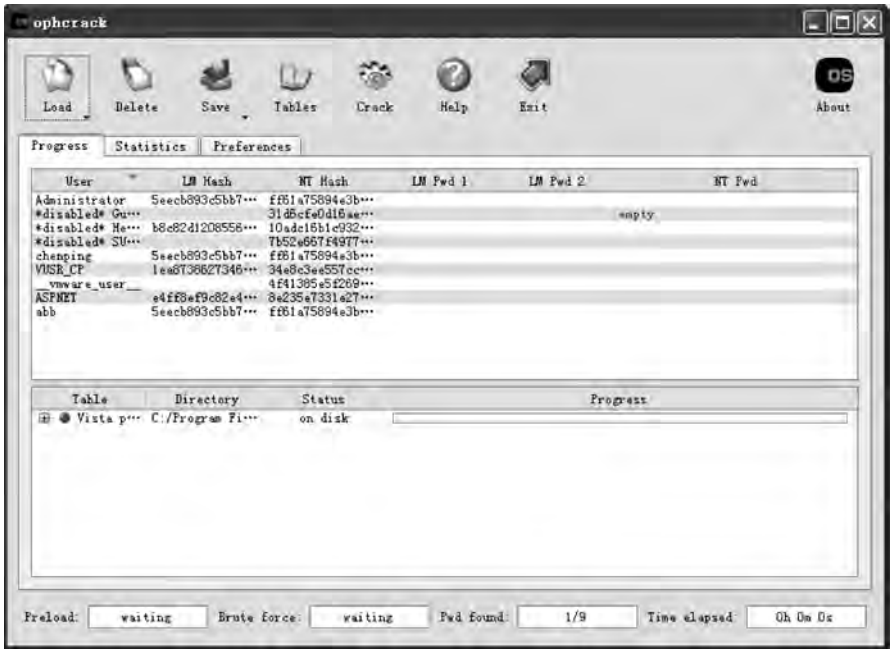

图 3.14　加载口令散列

5. 利用彩虹表进行口令破解

在图 3.14 中单击 Crack 图标，用彩虹表进行口令破解。在破解过程中可以单击 Statistics 标签，查看彩虹表的状态，如图 3.15 所示。

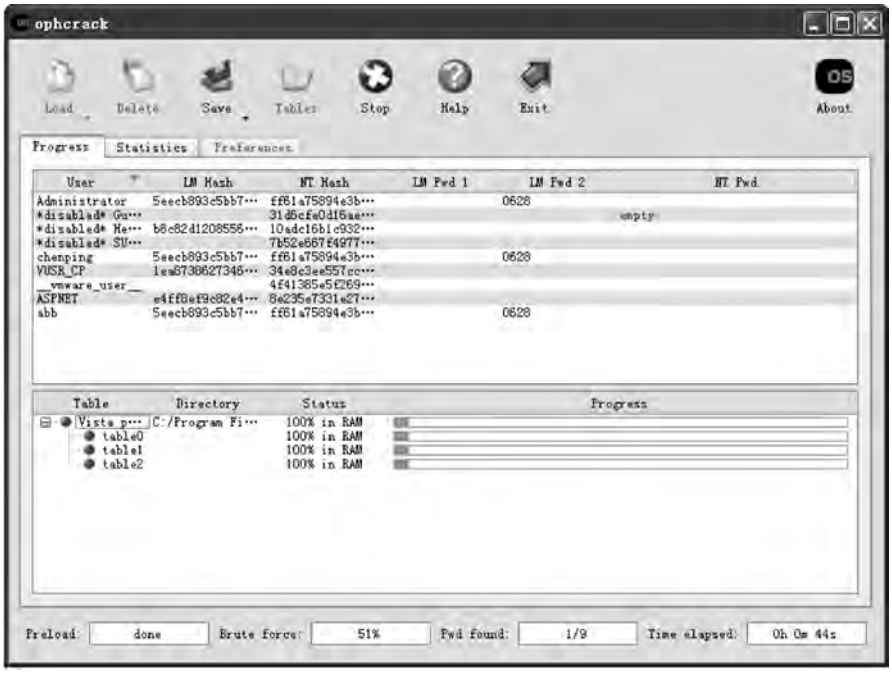

图 3.15　用彩虹表进行口令破解

6. 口令破解成功

破解结束后可以看到 Ophcrack 成功破解了用户 test 的口令，如图 3.16 所示。请读者设置不同位数和字符集的口令，以观察利用彩虹表进行口令猜测的时间，并记录。

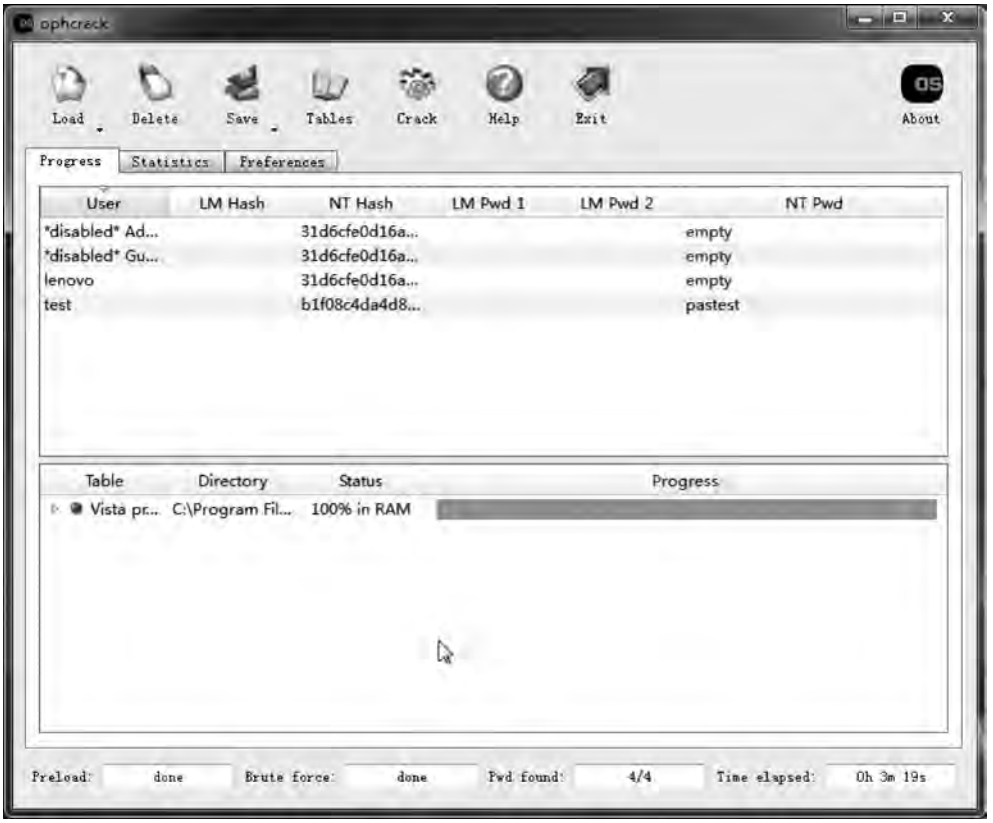

图 3.16　利用彩虹表成功破解口令

3.5　Linux 系统口令破解实验

3.5.1　实验目的

掌握 Linux 口令散列的提取方法，掌握使用 John the Ripper 进行口令破解的方法。

3.5.2　实验内容及环境

1. 实验内容

本实验通过使用 John the Ripper 工具完成对 Linux 系统环境下的口令散列的破解。需要掌握 Linux 系统环境下口令散列的提取方法，以及使用 John the Ripper 进行口令破解的过程。

2. 实验环境

主流配置计算机一台，安装 Ubuntu 14.04 操作系统和软件 John the Ripper 1.8.0。

John the Ripper是一个快速的口令破解工具。该软件支持目前大多数的加密算法，如DES、MD4和MD5等，可用于破解Windows、Linux系统口令。John the Ripper提供了4种破解模式。

1）简单破解模式(single crack mode)

这种破解模式主要针对用户设置的口令跟用户名相同或只是用户名的简单变形，如某个账号为admin，口令是admin888、admin123等。在使用这种破解模式时，John the Ripper会根据口令文件中的用户名进行破解，并且基于用户名使用多种字词变化规则进行口令猜测，以增加口令破解的成功率。

2）字典破解模式(wordlist crack mode)

这种破解模式需要用户指定一个字典文件，John the Ripper读取字典中的单词进行破解。John the Ripper自带了一个字典文件password.lst，里面包含了一些经常用来作为口令的单词。

3）增强破解模式(incremental mode)

也即暴力破解方式，这种方式会自动尝试所有可能的字符组合进行口令破解，破解时间较长。

4）外挂破解模式(external mode)

在该模式下用户可以使用自己用C语言编写的破解程序进行口令破解。

3.5.3　实验步骤

(1) 进入Ubuntu系统，以root用户身份执行Linux命令useradd test，添加test用户，再执行passwd test命令，更改用户口令。为验证暴力破解，可以将口令更改为6位纯数字口令，如图3.17所示。

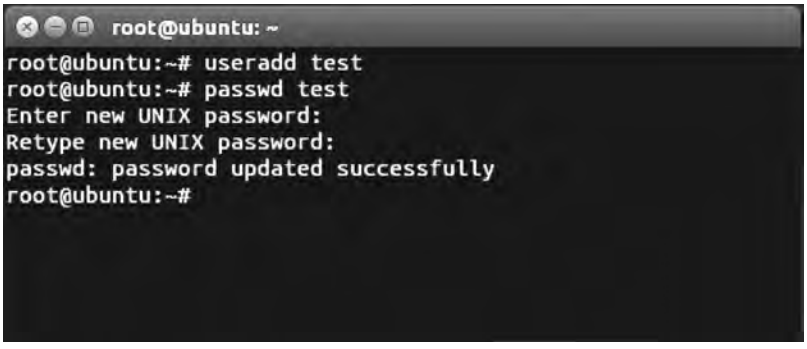

图3.17　添加测试用户

(2) 获取安装包John-1.8.0.tar.gz，利用指令tar -xvzf解压该压缩包，得到源代码，如图3.18所示。

(3) 进入刚刚解压的目录下，阅读README和DOC目录下的相关帮助文档，了解软件的安装和使用方法。

(4) 进入john-1.8.0/src目录，依次执行make; make clean linux-x86-64命令，其中linux-x86-64是Linux系统类型，可以根据实际情况进行选择，如图3.19所示。

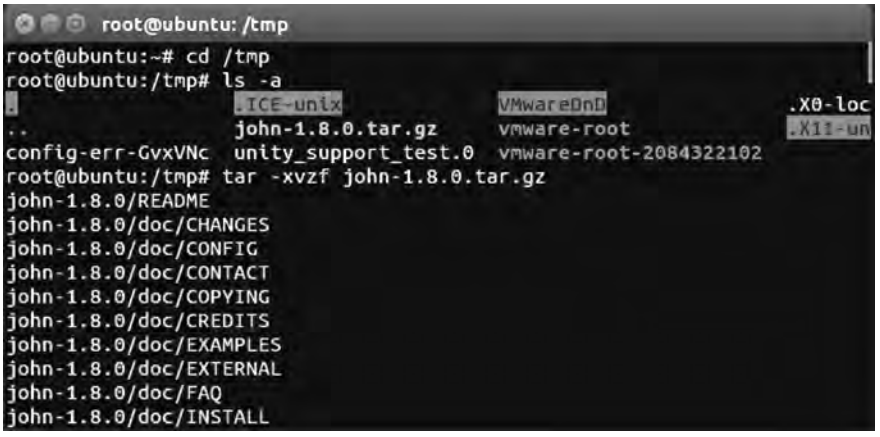

图 3.18 解压得到 John the Ripper 源代码

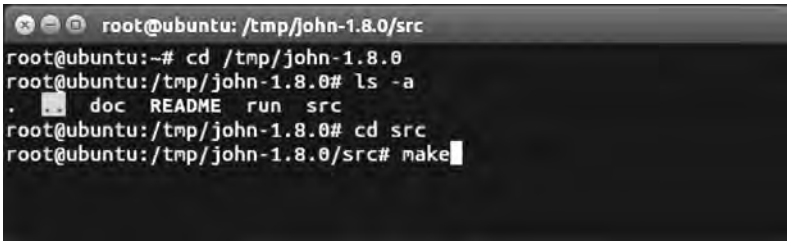

图 3.19 John the Ripper 源代码编译和软件的安装

(5) 编译完成后进入 run 目录,可以看到该目录下生成了一些可执行文件,如图 3.20 所示。

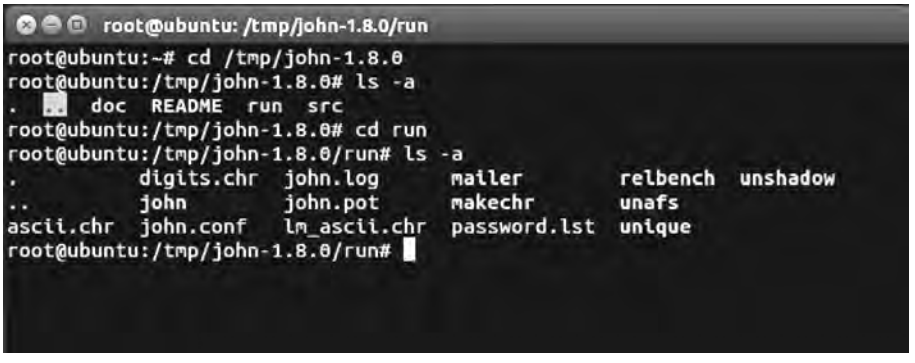

图 3.20 编译完成 John the Ripper 软件

(6) 查看帮助文档,了解破解命令的使用方式。输入命令:./unshadow /etc/passwd /etc/shadow > myshadow,将/etc/passwd 和/etc/shadow 合二为一到文件 myshadow 中,用于将用户名和加密后的口令存储在一个文件中,如图 3.21 所示。

(7) 进入 john/run 目录下,运行命令开始破解 Linux 口令文件,前面介绍过 John the Ripper 支持 4 种破解模式,我们验证其中的字典破解模式。首先采用系统默认的字典文

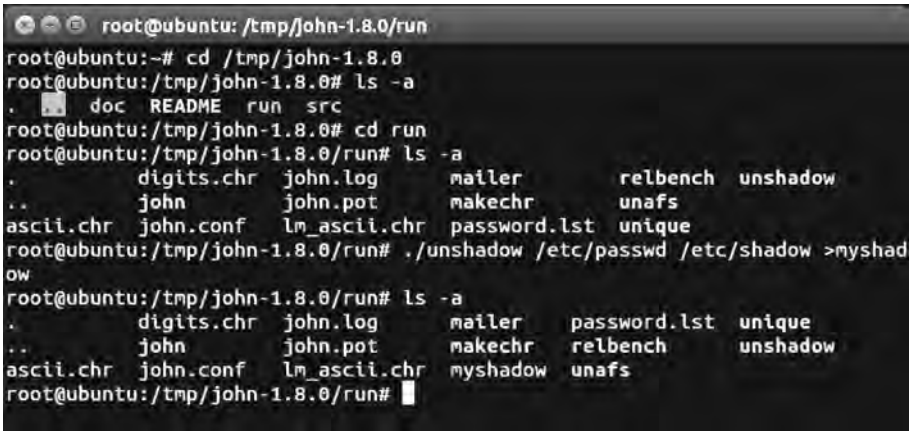

图 3.21　合并/etc/passwd 和/etc/shadow

件 password.lst 进行破解，如图 3.22 所示，可以看到运行结果提示当前系统中有 3 个用户，其中 test 用户的口令设置比较简单，很容易就破解出来了，其他两个用户的口令无法破解。

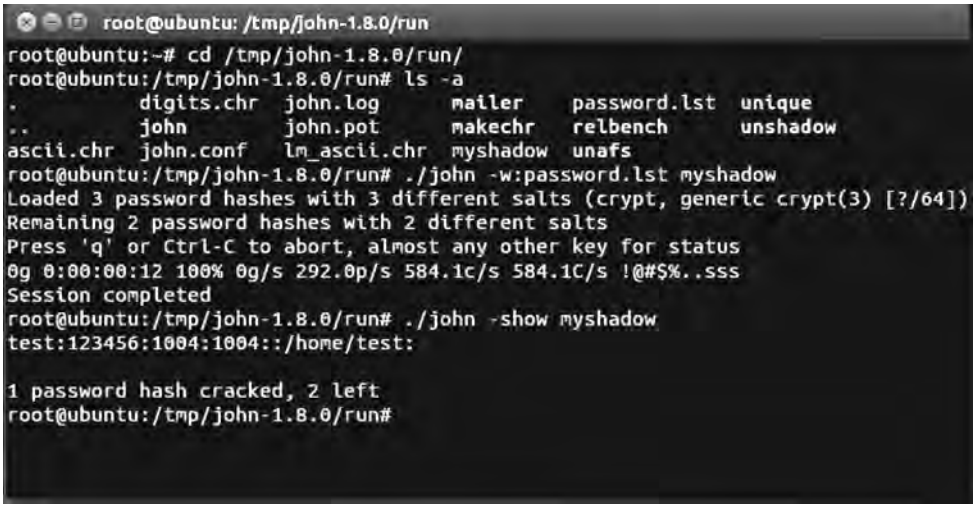

图 3.22　实施字典破解

(8) 请读者在系统默认的字典文件 password.lst 中增加其他两个用户的口令，重新进行字典攻击，验证是否能破解。

3.6　远程服务器的口令破解实验

3.6.1　实验目的

掌握对远程服务器口令的字典攻击方法，以及通过查看日志发现口令攻击的方法。

3.6.2 实验内容及环境

1. 实验内容

架设 FTP 服务器，利用远程口令枚举工具进行字典攻击，并通过配置服务器进行日志记录，利用日志分析口令枚举过程。

2. 实验环境

实验拓扑如图 3.23 所示，实验需要主流配置计算机两台，一台作为 FTP 服务器，安装 Windows 7 操作系统和 FileZilla Server 软件；另一台作为攻击机，安装 Windows 7 操作系统和 Fscan 软件，IP 地址设置如图 3.23 所示。

图 3.23 实验拓扑图

FileZilla 是免费开源的 FTP 软件，分为客户端版本和服务器版本。FileZilla 客户端具有快速、界面清晰、能管理多站点等特点，是一种方便、高效的 FTP 客户端工具；而 FileZilla Server 则是一个小巧并且支持 FTP 和 SFTP 的 FTP 服务器软件。本次实验利用 FileZilla 的服务器版本软件快速搭建一个 FTP 服务器。

Fscan：是基于命令行的 FTP 弱口令扫描小工具，其速度非常快，且使用简单。

3.6.3 实验步骤

1. 安装 FileZilla Server 软件

在 FTP 服务器上安装 FileZilla Server 软件，安装过程中需要设置安装路径、FTP 监听端口，按照默认选项安装完毕后，打开软件，首先进入连接服务器界面，如图 3.24 所示，输入正确参数后单击 OK 按钮，进入如图 3.25 所示的 FileZilla Server 主界面。

图 3.24 连接 FTP 服务器

2. 添加测试用户

在图 3.25 中依次选择菜单 Edit→Users，或单击工具栏的用户图标，进入用户添加界面，如图 3.26 所示。单击 Add 按钮，添加用户 test，勾选 Password 选项，输入测试口令。

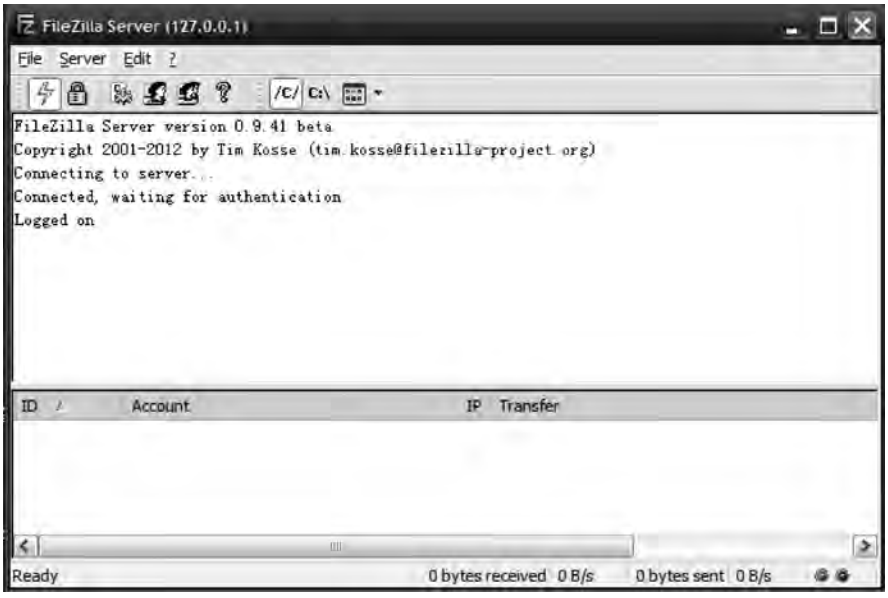

图 3.25　FileZilla Server 主界面

图 3.26　用户添加界面

3. 配置破解字典

将 ftpscan 工具软件复制到攻击机上，在 ftpscan 目录中，找到文件 username.dic 和 password.dic，为验证口令字典破解过程，将刚创建的 FTP 用户的用户名和口令分别添加在这两个文件中，如图 3.27 和图 3.28 所示。

图 3.27 在文件 username.dic 中添加新增用户名信息

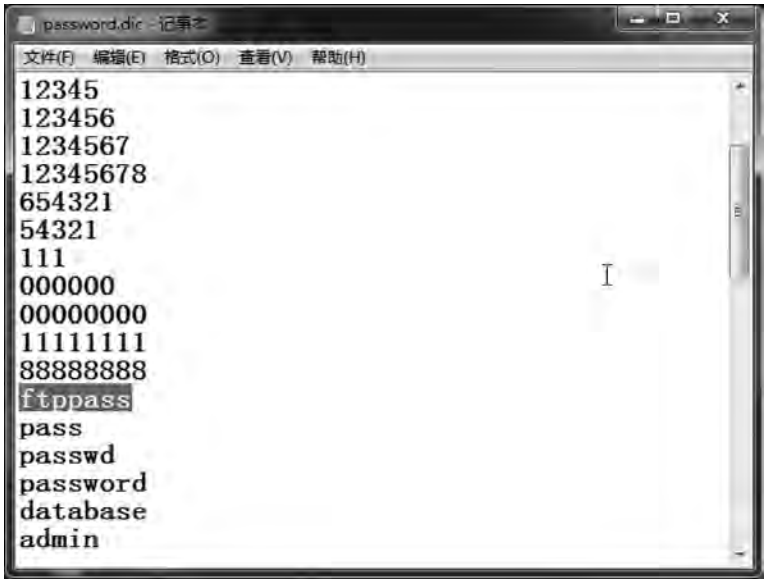

图 3.28 在文件 password.dic 中添加新增用户口令信息

4. 实施口令破解

在攻击机的命令行界面中，执行命令“ftpscan.exe 192.168.188.8”针对 FileZilla FTP 服务器进行在线破解，可以看到口令破解成功，如图 3.29 所示。

5. 配置服务器日志记录

在 FileZilla FTP 服务器主界面，选择 Edit→Settings 项，打开服务器配置对话框，单击左侧列表框里的 Logging，进入日志配置界面，勾选 Enable logging to file 选项，如图 3.30 所示。

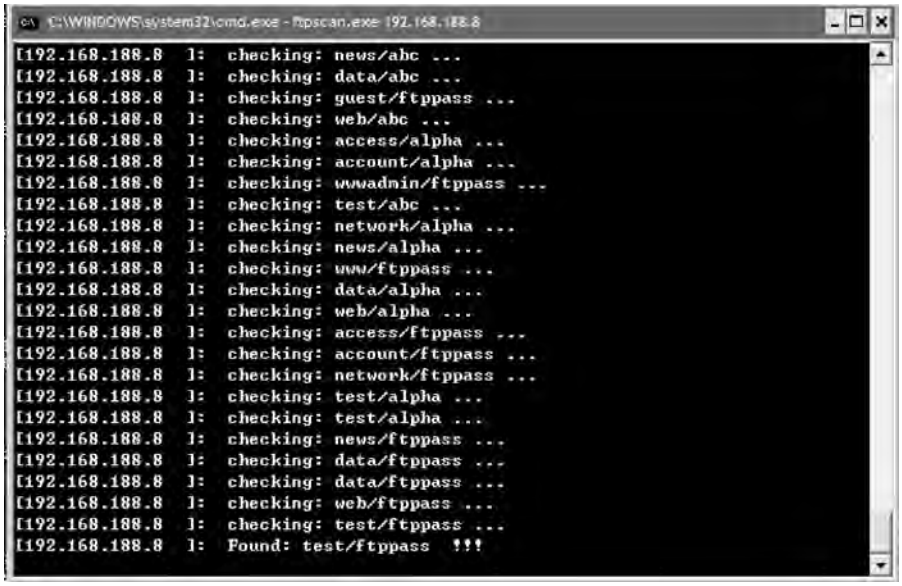

图 3.29　对 FileZilla FTP 服务器进行口令破解

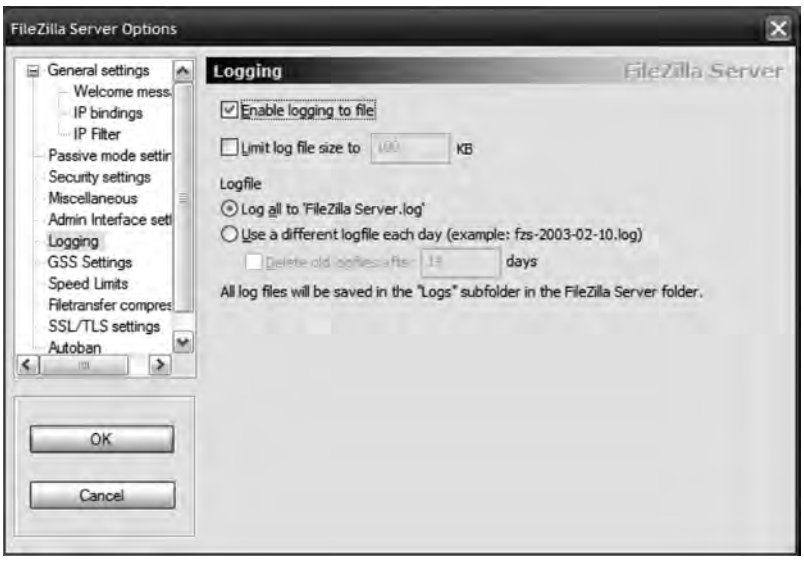

图 3.30　配置服务器日志记录

6. 查看日志文件中的口令破解记录

在配置日志选项后，再次从攻击机进行口令破解尝试。进入 FileZilla FTP 服务器安装目录下的 log 子目录，默认路径为 C:\Program File\FileZilla Server\Logs，打开 FileZilla Server.Logs 文件，可以看到大量来自同一 IP 地址的连接尝试记录，如图 3.31 所示。

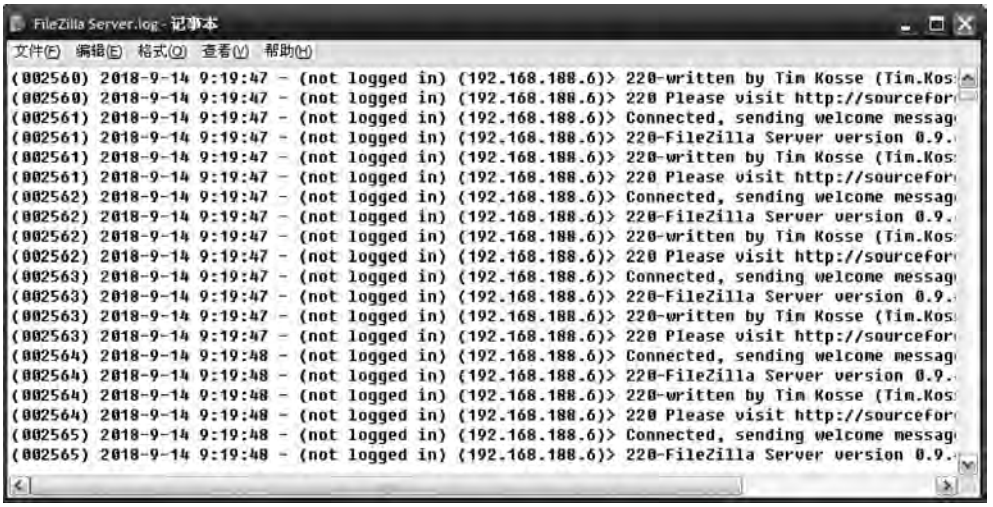

图 3.31 查看日志文件

3.7 练 习 题

(1) 列举一两种本书未介绍的本地口令破解工具,通过实验掌握其使用方法,记录实验过程。

(2) 在 3.4 节的实验中,由于 Windows 7 系统不存储 LM 散列,无法进行针对 LM 散列的破解实验。请在 Windows XP 系统环境下安装 Ophcrack 工具,通过实验体会 Ophcrack 破解 LM 散列的难度,并与对 NTLM 散列的破解难度进行对比。

(3) 在 3.6 节的实验中,进行 FileZilla FTP 服务器口令远程破解的同时,利用 Wireshark 嗅探器,在同一网段进行监听,以查看用户名和口令是否明文发送。

(4) 在 Linux 中,在默认字典文件中增加系统用户的口令,用 John the Ripper 的字典攻击方法进行破解,验证是否能破解成功所有用户口令。

(5) 在 Linux 中,增加一个用户,设置其口令为其用户名的变形,请采用简单(single)破解方法进行破解,验证是否能够成功破解。