第3章　实验内容

3.1　数据恢复

3.1.1　实验类型

验证型，2学时，必选实验。

3.1.2　实验目的

计算机磁盘属于磁介质，所有磁介质都存在剩磁效应的问题，保存在磁介质中的信息会使磁介质不同程度地永久性磁化，所以磁介质上记载的信息在一定程度上是抹除不净的，通过一定的技术手段可以将已抹除信息的磁盘上的原有信息提取出来。

另外，由于计算机文件系统的实现原理，文件的删除并没有将文件的数据内容从磁盘上删除，通过一定的技术手段可以将删除的文件恢复出来。

通过该实验，使学生认识到电磁泄露现象引起的数据恢复、硬件损坏、文件删除等实现数据恢复的内容。

3.1.3　题目描述

使用数据恢复软件 EasyRecovery 进行文件恢复。

3.1.4　实验要求

理解磁盘数据恢复的原理，认识数据恢复技术对信息安全的影响。能够使用数据恢复软件 EasyRecovery 进行文件恢复。

提高要求：能够对磁盘数据进行彻底清除。

3.1.5　相关知识

1. 剩磁效应

计算机主机及其附属电子设备，如视频显示终端、打印机等，在工作时不可避免地会产生电磁波辐射，这些辐射中携带有计算机正在进行处理的数据信息。尤其是显示器，由于显示的信息是给人阅读的，是不加任何保密措施的，所以其产生的辐射是最容易造成泄

密的。使用专门的接收设备将这些电磁辐射接收下来，经过处理，就可恢复还原出原信息。

国外对计算机设备的辐射问题早已有研究，在1967年的计算机年会上美国科学家韦尔博士发表了阐述计算机系统脆弱性的论文，总结了计算机4个方面的脆弱性，即处理器的辐射、通信线路的辐射、转换设备的辐射和输出设备的辐射。这是最早发表的研究计算机辐射安全的论文，但当时没有引起人们的注意。1983年，瑞典的一位科学家发表了一本名叫《泄密的计算机》的小册子，其中再次提到计算机的辐射泄露问题。1985年，荷兰学者艾克在第三届计算机通信安全防护大会上公开发表了他的有关计算机视频显示单元电磁辐射的研究报告，同时在现场做了用一台黑白电视机接收计算机辐射泄露信号的演示。他的报告在国际上引起强烈反响，从此人们开始认真对待这个问题。据有关报道，国外已研制出能在一千米之外接收还原计算机电磁辐射信息的设备，这种信息泄露的途径使敌对者能及时、准确、广泛、连续而且隐蔽地获取情报。计算机电磁辐射泄密问题已经引起了各个国家的高度重视，要防止机密信息被窃取，必须采取防护和抑制电磁辐射泄密的专门技术措施，这方面的技术措施有干扰技术、屏蔽技术和Tempest技术。

计算机磁盘属于磁介质，所有磁介质都存在剩磁效应的问题，保存在磁介质中的信息会使磁介质不同程度地永久性磁化，所以磁介质上记载的信息在一定程度上是抹除不净的，使用高灵敏度的磁头和放大器可以将已抹除信息的磁盘上的原有信息提取出来。据一些资料的介绍，即使磁盘已改写了12次，但第一次写入的信息仍有可能复原出来。这使涉密和重要磁介质的管理以及废弃磁介质的处理都成为很重要的问题。国外有的甚至规定记录绝密信息资料的磁盘只准用一次，用后必须销毁，不准抹后重录。

2. 文件删除原理

存储在硬盘中的每个文件都可分为两部分：文件头和存储数据的数据区。文件头用来记录文件名、文件属性、占用簇号等信息。文件头保存在一个簇并映射在FAT表(文件分配表)中，而真实的数据则是保存在数据区当中的。平常所做的删除，其实是修改文件头的前两个代码，这种修改映射在FAT表中，就为文件做了删除标记，并将文件所占簇号在FAT表中的登记项清零，表示释放空间，这也就是平常删除文件后，硬盘空间增大的原因。而真正的文件内容仍保存在数据区中，并未得以删除。要等到以后的数据写入，把此数据区覆盖掉，才算是彻底把原来的数据删除。如果不被后来保存的数据覆盖，它就不会从磁盘上抹掉。用Fdisk分区和Format格式化和文件的删除类似，只是前者改变的是分区表，后者修改的是FAT表，都没有将数据从数据区直接删除。

3. 某一分区被误格式化或文件丢失或误删除的恢复

对于FAT格式的文件结构，文件删除仅仅是把文件的首字节改为E5H，其余的内容并没有被修改，因此可以比较容易恢复。可以使用后面介绍的数据恢复软件轻松地把误删除或意外丢失的文件找回来。不过特别注意的是，在发现文件丢失后，准备使用恢复软件时，千万不要在本机安装这些恢复工具，因为软件的安装可能恰恰把刚才丢失的文件覆盖掉。最好使用能够从光盘直接运行的数据恢复软件，或者把硬盘挂在别的机器上进行

恢复。

特别是文件存储在C盘的情况下，如果发现主要文件被误删除或意外丢失时，这时应该立即关闭电源，用软盘启动进行恢复或把硬盘挂接到其机器上进行处理。

误格式化的情况可以使用UNFORFAT或EasyRecovery等工具进行处理。但是如果使用的是Format X:/U命令进行的格式化，那么这种情况是无法恢复的。

4. 数据恢复范围

1）误操作类

误删除、误格式化、误分区、误克隆等。

2）破坏类

病毒分区表破坏、病毒FAT、BOOT区破坏、病毒引起的部分DATA区破坏。

3）软件破坏类

Format、Fdisk、IBM-DM、PartitionMagic和Ghost等（注：冲零或低级格式化后的硬盘将无法修复数据）。

4）硬件故障类

0磁道损坏、硬盘逻辑锁、操作时断电、硬盘芯片烧毁、软盘/光盘/硬盘无法读盘。

5）加密解密

Zip、Rar、Office文档、Windows 2000/XP系统密码。

5. 彻底删除文件的方法

那么，如何让被删除的文件无法恢复呢？如果将文件删除后重新写入新数据，反复多次后原始文件就可能找不回了。但操作起来比较麻烦，而且也不够保险。因此最好能借助一些专业的删除工具来处理，例如O&O SafeErase可以设置5种删除级别，默认的Highest Security（最高级别的安全删除）算法将使用预设规则重写数据35次，可让原始数据变得“面目全非”。

6. 数据恢复软件EasyRecovery简介

EasyRecovery是世界著名数据恢复公司Kroll Ontrack的技术杰作。其Professional版更是囊括了磁盘诊断、数据恢复、文件修复、E-mail修复全部4大类19个项目的各种数据文件修复和磁盘诊断方案。本实验使用的就是EasyRecovery Professioanl，版本为11.1共享版，目前在网上可以很方便地找到。

EasyRecovery在修复过程中不对原数据进行改动，只是以读的形式处理要修复的分区。它不会将任何数据写入它正在处理的分区。EasyRecovery可运行于Windows 95、98、NT、2000以及XP，并且它还包括了一个实用程序用来创建紧急启动软盘，以便在不能启动进入Windows的时候在DOS下修复数据。

EasyRecovery修复范围：

- 修复主引导扇区（MBR）；
- 修复BIOS参数块（BPB）；

- 修复分区表；
- 修复文件分配表(FAT)或主文件表(MFT)；
- 修复根目录；
- 受病毒影响；
- 格式化或分区；
- 误删除；
- 由于断电或瞬间电流冲击造成的数据毁坏；
- 由于程序的非正常操作或系统故障造成的数据毁坏。

3.1.6 实验设备

主流配置PC一台，要求安装Windows 7操作系统，数据恢复软件EasyRecovery11.1。

3.1.7 实验步骤

(1) 从指导老师处得到数据恢复软件EasyRecovery。

(2) 安装软件。

(3) 运行数据恢复软件EasyRecovery，如图3-1-1所示。

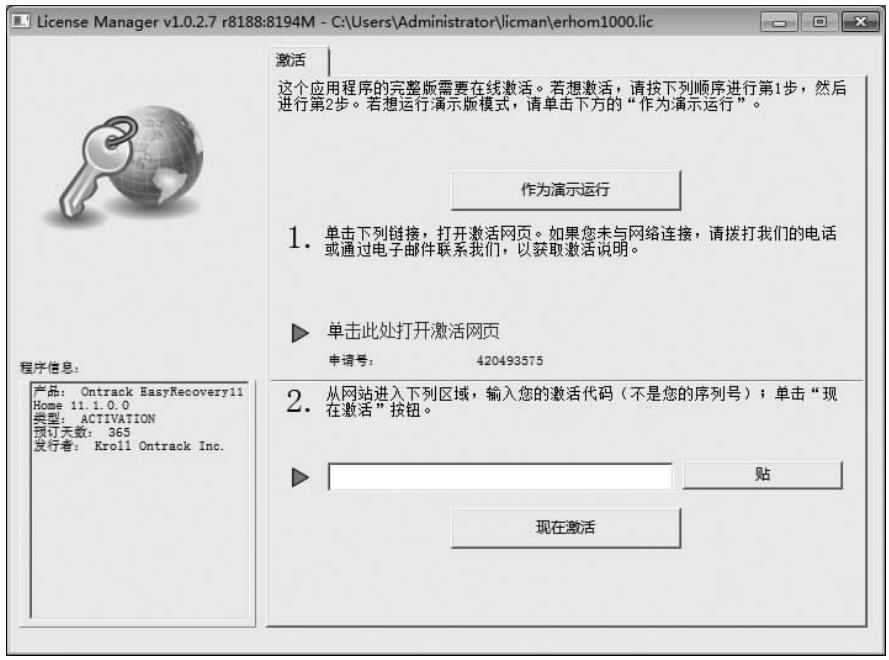

图3-1-1 启动界面

单击“作为演示运行”按钮，如图 3-1-2 所示。

图 3-1-2　单击“作为演示运行”按钮后的界面

单击“继续”按钮，如图 3-1-3 所示。

图 3-1-3　单击“继续”后进入软件数据恢复界面

① 硬盘驱动器：从内部硬盘或其他大容量存储设备中恢复数据；

② 存储设备：从闪盘或其他移动闪存媒体恢复数据；

③ 光学媒体：从光学媒体如 CD、CD-R/W、DVD、DVD-R/W 等；

④ 多媒体/移动设备：从多媒体或移动设备中恢复数据，如数码相机、MP3、智能电话等；

⑤ RAID 系统：恢复 RAID 系统的数据。

(4) 在 E 盘根目录，创建文件“密件.txt”，内容为“密码：123456”，并将其复制到优盘，然后删除该文件。

(5) 将优盘插入到 USB 接口，并双击桌面的快捷方式 Ontrack EasyRecovery Professional，启动数据恢复软件。

(6) 进入到数据恢复界面，选择“存储设备”，并单击“继续”按钮，如图 3-1-4 所示。

图 3-1-4　软件数据恢复界面中选择“存储设备”

(7) 单击“继续”按钮，如图 3-1-5 所示。

(8) 单击“继续”按钮，如图 3-1-6 所示。

(9) 单击“继续”按钮，如图 3-1-7 所示。

(10) 单击“继续”按钮，如图 3-1-8 所示。

(11) 文件搜索完成后，如图 3-1-9 所示。

(12) 找到要恢复的文件“密件.txt”，单击工具栏上的“保存“按钮，如图 3-1-10 所示。

(13) 并单击“保存”按钮，文件恢复成功。

图 3-1-5　选择要恢复数据的优盘

图 3-1-6　选择恢复数据的类型为“恢复已删除的文件”

图 3-1-7　恢复数据选项核查界面

图 3-1-8　数据恢复进度界面

(14) 在桌面上找到“密件.txt”,双击打开文件,如图 3-1-11 所示。

3.1.8　实验思考

(1) 为什么删除的磁盘文件能够恢复回来?

(2) 怎样才能彻底地删除文件? 如何使用 GPL 通用公开授权文件删除软件 Eraser 将文件彻底删除?

图 3-1-9　找到需要恢复的文件“密件.txt”

图 3-1-10　选择恢复文件的保存位置

图 3-1-11　发现文件的内容

3.2　操作系统安全评估与检测

3.2.1　实验类型

综合型，4 学时，必选实验。

3.2.2　实验目的

操作系统本身设计的安全性可能比较高，但可能由于使用和配置的不当，造成操作系统实际的安全性能降低。通过操作系统安全评估，发现主机和网络设备的漏洞和安全隐患。通过实验，使学生认识操作系统安全评估与检测的重要性，掌握操作系统安全评估与检测的内容和方法。

3.2.3　题目描述

使用 Windows 基线分析器 MBSA 对操作系统进行安全评估。

3.2.4　实验要求

能够使用 MBSA 实现对本地和远程的 Windows 操作系统实现安全评估。

3.2.5　相关知识

信息系统安全评估过程包括 3 个阶段，分别是文档审查阶段、现场检测阶段和综合评估阶段。评估依据有《信息系统安全保障通用评估准则》及各行业系统评估标准。评估结果以报告的形式给出，通常包括《信息系统安全现场核查报告》、《信息系统安全测试报告》

以及《信息系统安全综合评估报告》等。系统安全评估主要可以划分为操作系统安全评估和应用服务系统安全评估，操作系统的安全评估主要针对操作系统的漏洞、不当的配置，而应用服务的安全评估是针对运行于操作系统之上的软件系统。应用系统安全评估的对象包含非附属于操作系统的软件产品（如数据库、业务系统）提供的各种服务，如 Web 服务、Mail 服务、数据库等应用进行一个全面的安全评估。通过对系统的安全评估，还可以提供针对系统的优化建议和加固服务，使系统和应用能够抵御各种安全威胁。

Windows 系统的“漏洞”就像它的 GUI（图形界面）一样“举世闻名”，几乎每个星期都有新的漏洞被发现。这些漏洞常被计算机病毒和黑客们用来非法入侵计算机，进行大肆破坏。虽然微软会及时发布修补程序，但是发布时间是随机的，而且这些漏洞会因 Windows 软件版本的不同而发生变化，这就使得完全修补所有漏洞成为头号难题。

解决这个难题的简单方法就是利用特定的软件对 Windows 系统进行扫描，检查是否存在漏洞，哪些方面存在漏洞，以便及时修补。

微软开发的免费软件——微软基准安全分析器（Microsoft Baseline Security Analyzer，MBSA），该软件能对 Windows、Office、IIS、SQL Server 等软件进行安全和更新扫描（如表 3-2-1 所示），扫描完成后会用“X”将存在的漏洞标示出来，并提供相应的解决方法指导修补。

表 3-2-1　MBSA 支持的微软产品

产　品　名	安全扫描	更新扫描
Windows Server 2003/XP/2000，NT 4.0	是	是
Exchange Server 5.5 及更高版本	否	是
IIS 4.0 及更高版本	是	是
IE 5.01 及更高版本	是	是
Office 2000 及更高版本	是	是
SQL Server 7.0 及更高版本	是	是
Windows Media Player 6.4 及更高版本	否	是

MBSA 只能在 Windows 2000/XP/2003 系统上运行。在微软的官方网站上可以下载到最新版的 MBSA，而且只需要按照“安装向导”的提示操作即可完成安装过程。安装完成后，依次单击“开始”→“程序”→Microsoft Baseline Security Analyzer 1.2.1 程序项（或双击“桌面”上的 Microsoft Baseline Security Analyzer 1.2.1 快捷图标），就可弹出 MBSA 的主窗口。

3.2.6　实验设备

主流配置 PC 一台，Windows 2000 操作系统，Windows 基线分析器 MBSA。

3.2.7 实验步骤

(1) 单击 MBSA 主窗口中的 Scan a computer(或 Pick a computer to scan)菜单,将弹出 Pick a computer to scan 对话框,如图 3-2-1 所示。

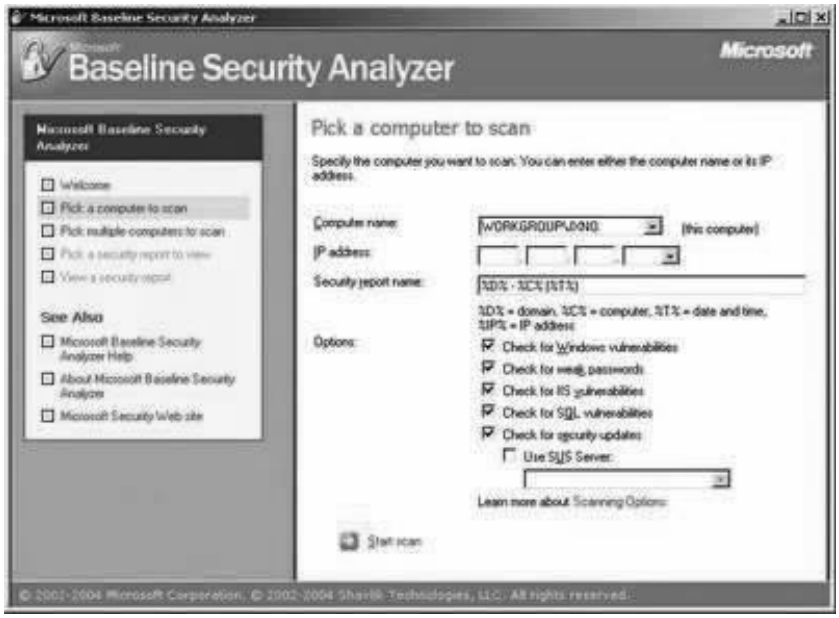

图 3-2-1 选择被扫描的计算机

要想让 MBSA 成功扫描计算机,需在此对话框中进行正确的参数设置。

(2) 设定要扫描的对象。

告诉 MBSA 要扫描的计算机是扫描成功的基础。MBSA 提供两种方法。

方法 1:在 Computer name 文本框中输入计算机名称,格式为“工作组名\计算机名”。

在默认情况下,MBSA 会显示运行 MBSA 的计算机的名称,“WORKGROUP”是所运行 MBSA 的计算机所属的工作组名称,“JXNO”是计算机名称。

方法 2:在 IP address 文本框中输入计算机的 IP 地址。在此文本框中允许输入在同一个网段中的任意 IP 地址,但不能输入跨网段的 IP,否则会提示 Computer not found.(计算机没有找到)的信息。

(3) 设定安全报告的名称格式。

每次扫描成功后,MBSA 会将扫描结果以“安全报告”的形式自动地保存起来。MBSA 允许自行定义安全报告的文件名格式,只要在 Security report name 文本框中输入文件格式即可。

MBSA 提供两种默认的名称格式:"%D%-%C%(%T%)"(域名-计算机名(日期戳))和"%D%-%IP%(%T%)"(域名-IP 地址(日期戳))。

(4) 设定扫描中要检测的项目。

MBSA 允许检测包括 Office、IIS 等在内的多种微软软件产品的漏洞。在默认情况下,无论计算机是否安装了以上软件,MBSA 都要检测计算机上是否存在以上软件的漏洞。这不但浪费扫描时间,而且影响扫描速度。可以根据实际情况进行选择,对于一些没有安装的软件可以不选,例如:若没有安装 SQL Server,则可不选中 Check for SQL vulnerabilities 复选项,这样能缩短扫描时间,提高扫描速度。

基于这点考虑,MBSA 提供了让用户自主选择检测项目的功能。只要选中(或取消) Options 中某个复选项,就可让 MBSA 检测(或忽略)该项目。

不过,允许自主选择的项目只有 Check for Windows vulnerabilities(检查 Windows 的漏洞)、Check for weak passwords(检查密码的安全性)、Check for IIS vulnerabilities (检查 IIS 系统的漏洞)、Check for SQL vulnerabilities(检查 SQL Server 的漏洞)等 4 项。

至于其他项目(如 Office 软件的漏洞等)MBSA 会强制扫描。

(5) 设定安全漏洞清单的下载途径。

MBSA 的工作原理是:以一份包含了所有已发现的漏洞的详细信息(如什么软件隐含漏洞、漏洞存在的具体位置、漏洞的严重级别等)的安全漏洞清单为蓝本,全面扫描计算机,将计算机上安装的所有软件与安全漏洞清单进行对比。如果发现某个漏洞,MBSA 就会将其写入到安全报告中。

因此,要想让 MBSA 准确地检测出计算机上是否存在漏洞,安全漏洞清单的内容是否是最新的就至关重要了。

由于新的漏洞不断被发现,所以要像更新防病毒软件的病毒库一样,及时更新安全漏洞清单。MBSA 提供了两种更新方法。

方法 1:从微软官方网站上下载

微软会在它的官方网站上及时发布最新的安全漏洞清单,所以 MBSA 被默认设置为每一次扫描时自动链接到微软官方网站下载最新的安全漏洞清单。如果已经下载了最新的安全漏洞清单,则可取消 Check for security updates 复选项。否则应该选中此复选项,以确保安全漏洞清单的内容是最新的。

此方法适用于能连入 Internet 的计算机。

方法 2:从 SUS 服务器上下载

有些局域网中架设了软件升级服务(Software Update Services,SUS)服务器,所以此类可以选择此方法下载最新的安全漏洞清单,只要选中 Use SUS Server 复选框,并在其下的文本框中输入 SUS 的地址即可。

(6) 根据自身情况设置好各项参数后单击 Start Scan 菜单,将弹出 Scanning 对话框,MBSA 将开始扫描指定的计算机,如图 3-2-2 所示。

(7) 扫描完成后,MBSA 会将扫描的结果以安全报告的形式保存到"X:\Documents and Settings\username\SecurityScans"(X 指 Windows 的系统分区符,username 是操作 MBSA 的人员姓名)文件夹中。此时,MBSA 还会自动弹出 View security report 对话窗,将刚生成的安全报告的内容显示出来,如图 3-2-3 所示。

可以根据安全报告的 Score 列中不同颜色的图标来简单区分被扫描的计算机上哪些

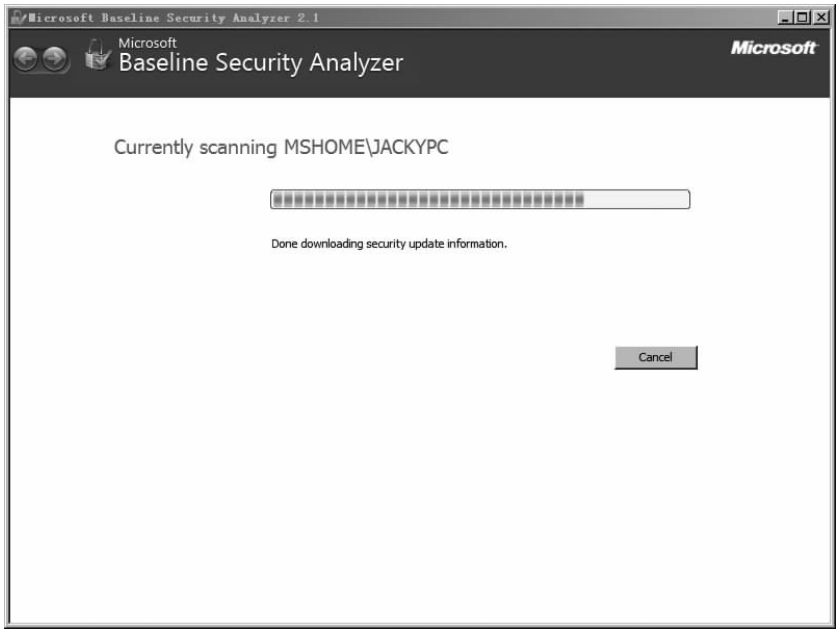

图 3-2-2　扫描过程

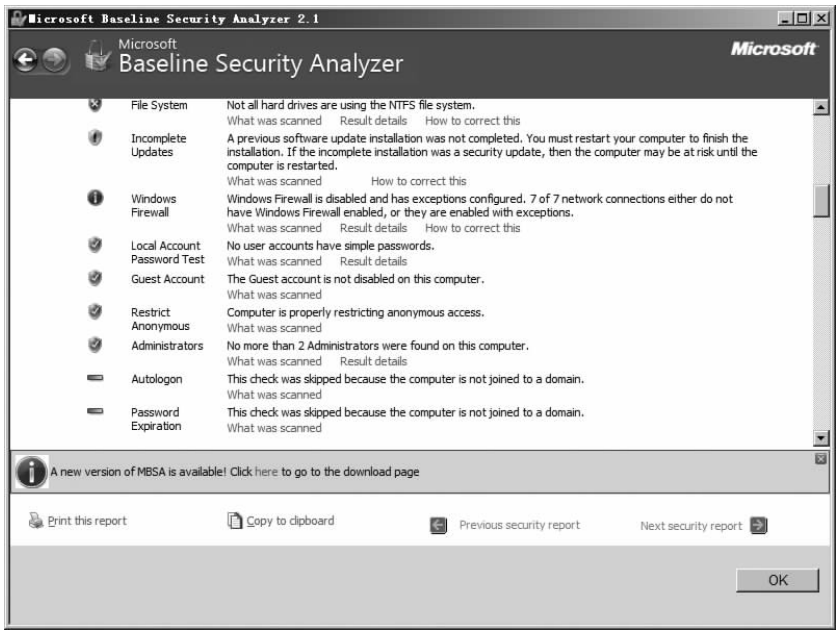

图 3-2-3　扫描结果

方面存在漏洞，哪些方面需要改进，如下所示。

① 绿色的√图标表示该项目已经通过检测。

② 红色(或黄色)的×图标表示该项目没有通过检测，即存在漏洞或安全隐患。

③ 蓝色的＊图标表示该项目虽然通过了检测但可以进行优化，或者是由于某种原因

MBSA 跳过了其中的某项检测。

④ 白色的 i 图标表示该项目虽然没有通过检测，但问题不很严重，只需要进行简单的修改即可。

但是这种判断方法很不准确，正确的方法是查看检测项目的 Result 列中是否含有 How to correct this(如何修正它)选项。只要有项目存在，就应该单击 How to correct this 选项。然后根据提供的解决方法，或是下载相应的补丁程序，或是修改相关的设置，就可修正存在的问题。

例如：安全报告提示 IE Zones(IE 区域设置)项目没有通过检测，单击 How to correct this 选项后都将弹出信息提示窗(如图 3-2-4 所示)，根据 Solution(解决方法)处的文字信息得知，只要按照 Instructions(提示信息)中的步骤更改 IE 的区域设置值即可解决。

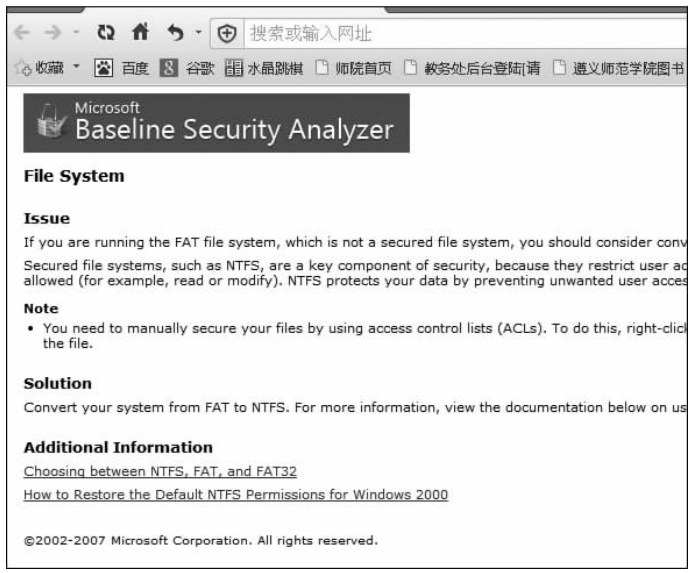

图 3-2-4 提示信息

(8) 扫描多台计算机。

此项功能是“扫描一台计算机”功能的延伸，只是将扫描对象扩大到网络中的一个域或 IP 地址段，它的工作原理与“扫描一台计算机”相同，即以安全漏洞清单为蓝本，对指定域(或 IP 地址段)中的所有计算机逐一进行扫描，如图 3-2-5 所示。

注意：MBSA 只能扫描网络中安装了 Windows NT 4.0/2000/XP/2003 操作系统的计算机，而不能扫描 Windows 9X/Me 系统的计算机。

具体的操作步骤如下。

第一步：单击 MBSA 主窗口中的 Scan more than one computer(或 Pick multiple computer to scan)菜单，将弹出 Pick multiple computer to scan 对话框。

在此对话框中也要进行必要的、准确的设置。但由于此功能是“扫描一台计算机(Scan a computer)”功能的扩展，所以 Security report name 和 Options 处的设置可以参照操作。

不同的是“指定要扫描的对象”方面：只要在 Domain name 文本框中输入要被扫描的

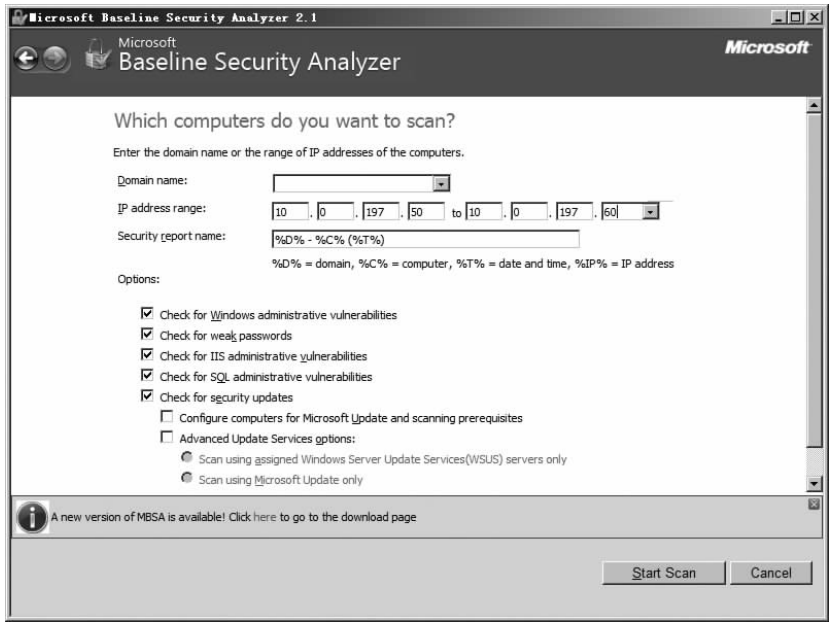

图 3-2-5　扫描多台计算机

域的名称，或在 IP address range 文本框中输入要被扫描的 IP 地址范围，就能让 MBSA 扫描某个域（或 IP 地址段）中的所有计算机。

注意：无论域（或 IP 地址段）中的所有计算机安装的软件是否相同，MBSA 都将依据 Options 处的设置“一视同仁”地扫描每台计算机。

第二步：设定好各项参数后单击 Start Scan 菜单，将弹出 Scanning 对话框，如图 3-2-6

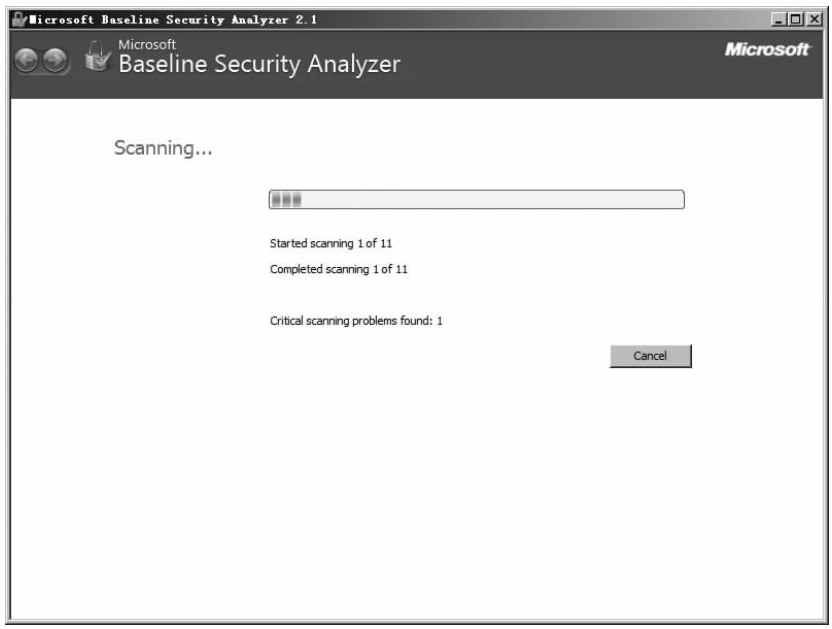

图 3-2-6　扫描过程

所示，MBSA 将依次扫描域（或 IP 地址段）中的每台计算机。完成扫描所需要的时间与被扫描的计算机数量和设置的扫描项目有关。

第三步：与“扫描一台计算机”功能不同的是，扫描结束后，将弹出 Unable to scan all computers 对话框。在此对话框中，将列举没有扫描成功的计算机名（或 IP 地址）及原因。扫描失败的原因有两种，如图 3-2-7 所示。

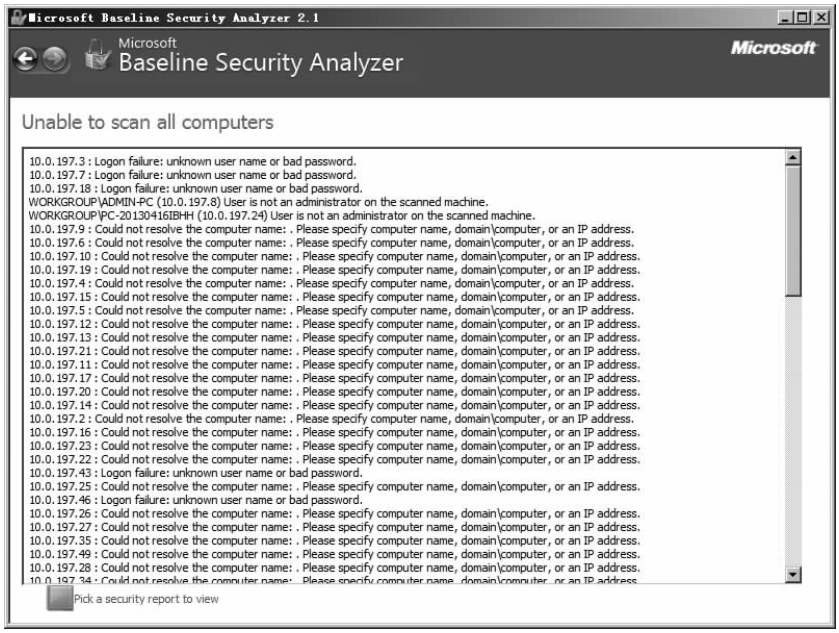

图 3-2-7　出现某些主机不能被扫描

- User is not an administrator on the scanned machine.：被扫描的计算机没有超级管理员权限。

造成这种情况出现的原因主要是没有以 Administrator 的管理员登录操作 MBSA 的计算机或者被扫描的计算机设置了登录密码。

- This is not a Windows NT/2000/XP/2003 Server or Workstation.：被扫描的计算机不是 Windows NT 4.0/2000/XP/2003 系统。

造成这种情况出现的原因是被扫描的计算机没有安装 Windows NT 4.0/2000/XP/2003 操作系统，可能安装了 Windows 9X/Me 系统，或者安装了非 Windows 操作系统，如 Linux 等；或者，被扫描的根本就不是计算机，可能是其他网络设备，如路由器等。

第四步：在 Unable to scan all computers 对话窗的底部还会显示以下菜单之一，以引导进行下一步操作。

- 若显示 Continue 菜单：说明此次扫描中没有一台计算机扫描成功。单击此菜单后将返回到 MBSA 的主窗口。
- 若显示 Pick a security report to view 菜单：说明此次扫描中至少有一台计算机成功地完成扫描并生成了安全报告。单击此菜单后将弹出 Pick a security report to view 对话窗。此时，MBSA 将显示所有扫描成功的计算机的安全报告，供选择

查看其详细内容。

说明：此时无论扫描成功的计算机是几台，MBSA 都不会生成综合性的安全报告，而是为每一台计算机生成各自单独的安全报告。

第五步：选择、查看安全报告。

单击 MBSA 主窗口中的 Pick a security report to view（或 View existing security reports）菜单，将弹出 Pick a security report to view 窗口。在此窗口中，MBSA 将列出已有的所有安全报告清单（包括安全报告名、生成日期等信息），双击安全报告名就可查看其详细内容，如图 3-2-8 所示。

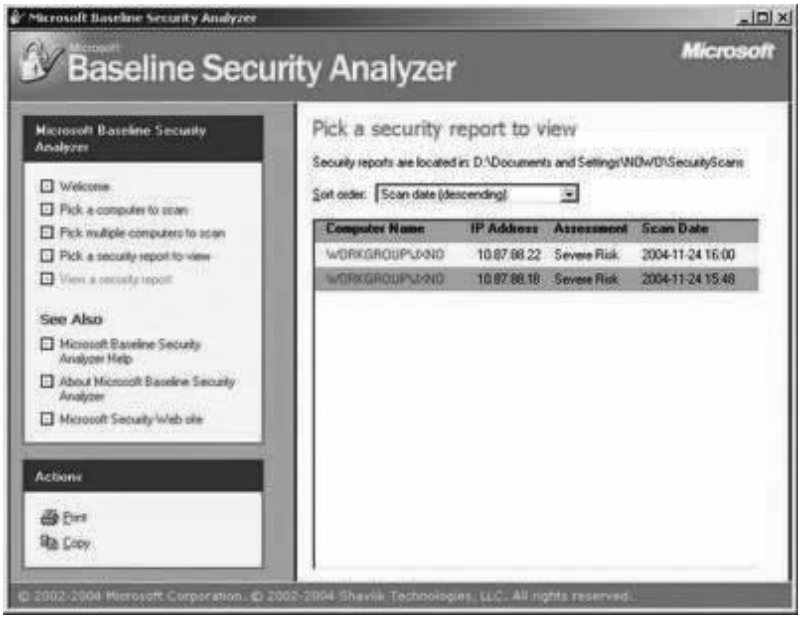

图 3-2-8　扫描结果

安全报告的具体内容、格式、操作方法与“扫描一台计算机”部分的第三步和第四步大同小异，可以参照操作。

（9）命令行用法。

MBSA 不但能以 GUI 界面运行，还能在命令提示符下运行，执行其安装目录下的 mbsacli.exe 文件就能实现。mbsacli.exe 文件不仅提供了丰富、灵活的参数，而且还支持两种语法结构。

一种是 MBSA 标准的命令行语法结构，即“mbsacli 参数”格式。在命令提示符下运行“mbsacli/?”（仅双引号内的文字）命令可以显示详细的语法信息。另一种是模拟补丁检查工具 HFNetChk 的命令行语法结构，即“mbsacli /hf 参数”格式。运行“mbsacli /hf/?”（仅双引号内的文字）命令可以显示详细的语法信息。

mbsacli.exe 还能用于各种脚本环境中，如命令脚本（.bat 或.cmd 文件）、WSH 脚本（.vbs 或.js 文件）等。通过这些脚本的调用，结合 Windows 系统的其他功能（如“计划任务”功能）就能实现对计算机的灵活扫描。

此外，在 MBSA 的安装目录下还有两个文本文件，编辑它们就能定制 MBSA 的扫描过程和方式。

services.txt 文件包含了 MBSA 要扫描的服务（见图 3-2-9），默认值为 MSFTPSVC、TlntSvr、W3SVC 和 SMTPSVC 服务。添加（或删除）服务名可以让 MBSA 进行（或忽略）对该服务的检测。

图 3-2-9　扫描的服务

NoExpireOk.txt 文件包含了 MBSA 不扫描的账户名，如 IUSR_*、IWAM_*、SUPPORT_*、SQLDebugger 等，如图 3-2-10 所示。删除（或添加）账户名可以让 MBSA 增加（或忽略）对该账户的检测。

（10）注意事项。

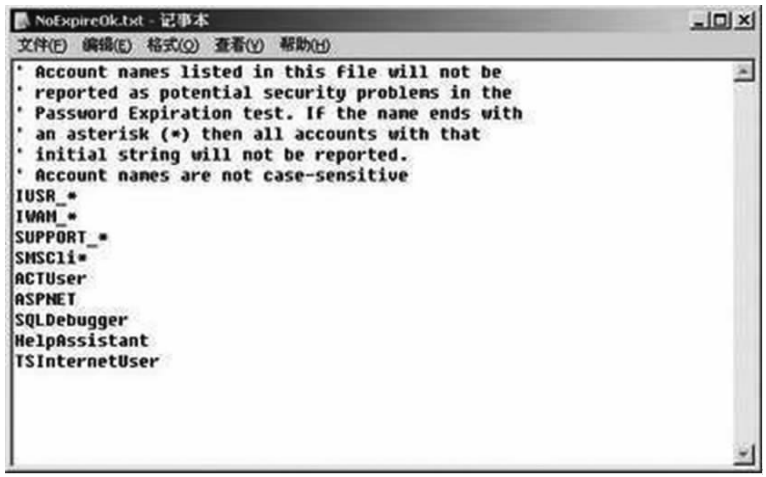

图 3-2-10　扫描的账号

MBSA 虽然好用，但是在使用过程中还需要注意以下事项。

① MBSA 对 Windows、Office、IIS 等软件进行的扫描包括以下两种。

- “安全扫描”是指扫描以上软件是否进行了安全的配置，如 IIS 锁定工具是否已运行，文件系统的类型是否都采用了 NTFS 格式等。
- “更新扫描”是指扫描以上软件是否安装了最新的补丁程序。

② MBSA 执行的是微软所谓的“基准扫描”，即只扫描和报告 Windows Update 定义的“关键更新”，而不是扫描和报告所有的更新。而且 MBSA 不会自动安装更新，需要另行操作完成。否则，漏洞依然存在。

③ MBSA 是基于 IE 页面开发的，所以要运行 MBSA 需要 Internet Explorer 5.01 以上才行，而且 IE 的所有设置项都会影响 MBSA 的运行。

④ 每次扫描后生成的安全报告是以明码格式保存到固定的文件夹中。因此，容易被黑客利用从而找出计算机的漏洞所在。所以建议对安全报告另行处理（如打印、备份到其他目录等），然后彻底删除 SecurityScans 文件夹中的所有文件，以防被他人利用。

总之，为了确保计算机系统的安全，除了安装安全防护软件（如杀毒软件、防火墙等）外，及时安装漏洞补丁程序是非常重要的。但怎么才能知道哪些补丁程序还没有安装呢？使用了 MBSA 就可以知道得一清二楚。而且 MBSA 具有其他同类软件无法比拟的优点：除了能检查 Windows 的漏洞，还能检测 Office、IIS 等微软产品的漏洞。故建议使用 Windows 2000/XP/2003 的下载该软件，用它检测出计算机中隐含的漏洞和安全隐患，尽早修补，以增强计算机的安全性。

当然，除了 MBSA 之外，还有很多免费或共享漏洞扫描工具（如 HFNetChk、LANguard Network Security Scanner 等），它们的功能也很实用，有兴趣的可以一试。

3.2.8 实验思考

（1）Windows 操作系统常见的不安全配置包括哪些方面？

（2）安全评估与安全检测的区别和联系是什么？

3.3 数据加密与鉴别

3.3.1 实验类型

综合型，8 学时，必选实验。

3.3.2 实验目的

密码技术是实现网络信息安全的核心技术，是保护数据最重要的工具之一。密码技术在保护信息安全方面所起的作用体现为保证信息的机密性、数据完整性、验证实体的身份和数字签名的抗否认性。通过实验，使学生掌握古典密码、对称密码体制、非对称密码体制、消息认证、数字签名和信息鉴别等密码算法的特点和密钥管理的原理，能够使用数据加密技术解决相关的实际应用问题，理解密码分析的特点。