

练习一 WindowsServer2008R2 系统安全

任务一 用户权限管理

【实验目的】

- 了解 SID
- 掌握权限基本原则及设置方法
- 掌握磁盘配额设置方法

【实验人数】

每组 1 人

【系统环境】

Windows

【网络环境】

交换网络结构

【实验工具】

【实验类型】

验证型

【实验原理】

【实验步骤】

本练习单人为一组。

首先使用“快照 X”恢复 Windows 系统环境。

一. SID 查看

在命令提示符中输入命令行：

```
whoami /user
```

将会得到类似图 1-1-1 所示信息：

```
PS C:\Users\admin> whoami /user
用户信息
-----
用户名                               SID
=====
win-16t1mj0rafa\admin S-1-5-21-844603714-92929292-3612905635-1000
```

图 1-1-1 查看主机 SID

二. 权限的四项基本原则演示

1. 拒绝优先原则

(1) 创建新用户

左键开始菜单栏->管理工具->计算机管理，如图 1-1-2(a)所示，然后选择系统工具|本地用户和组|用户，右键选择“新用户”，如图 1-1-2(b)所示。

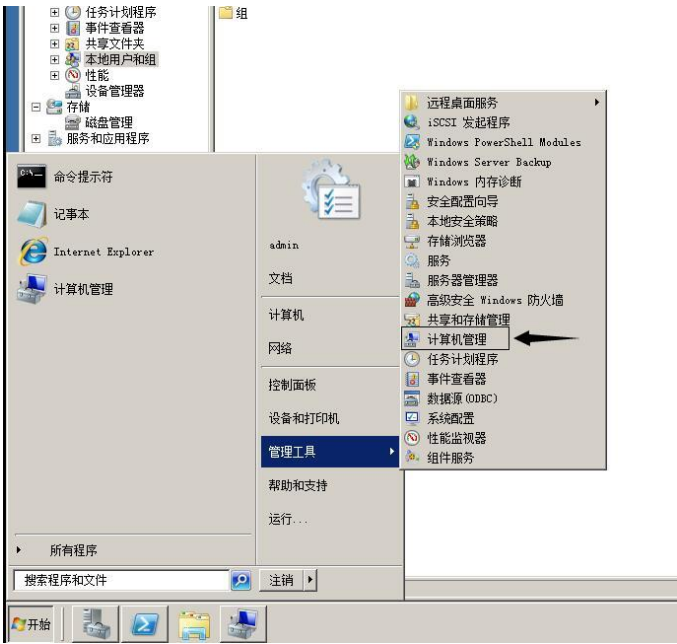


图 1-1-2(a) 打开计算机管理

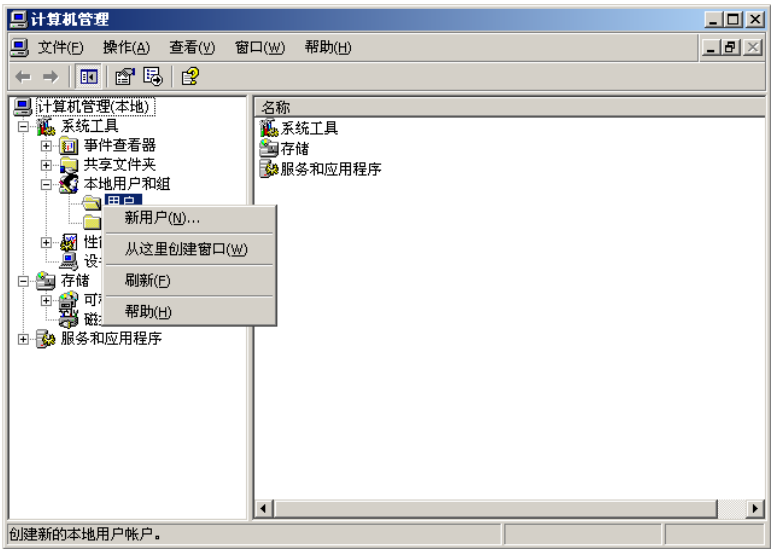


图 1-1-2(b) 创建新用户

在弹出的新用户对话框中，填写用户名 test1，并设置“密码永不过期”。单击“创建”按钮创建用户。

(2) 创建组

右键单击本地用户和组 | 组，选择“新建组”。在弹出的对话框中新建两个组 A 和 B，并将刚刚新建的 test1 用户添加到组 A 和组 B 中，点击选择用户界面中的“高级”按钮，点击“立即查找”，便可以在搜索结果中找到刚添加的 test1 用户，如图 1-1-3 所示。



图 1-1-3 创建新组并添加用户

(3) 在本地磁盘 C 中新建名为 test 的文件夹，在里面新建文本文件 test.txt，内容任意。

(4) 右键单击 test.txt 文件，选择“属性”，在“安全”选项卡中，单击“添加”按钮，将包含 test1 用户的组 A、B 添加进来，将组 A 的权限设置成“允许完全控制”，组 B 的权限设置成“拒绝读取”。

(5) 注销当前用户，使用新建的 test1 用户登录，进入本地磁盘 C:\test 目录，访问



test 文件。访问结果如图所示。

2. 权限最小原则

(1) 注销当前用户，使用 administrator 用户登录系统，新建用户 test2，默认情况下用户 test2 隶属组为：_____ (1)_____。

(2) 注销当前用户，使用 test2 用户登录系统，进入 C:\WINDOWS 系统目录，尝试修改其中的文件，操作结果：_____ (2)_____。



3. 权限继承原则

(1) 注销当前用户，使用 administrator 用户登录系统，新建用户 test31、test32。

(2) 在本地磁盘 C 中新建名为 test3 的文件夹，在此文件夹中新建 test3.txt，内容任意，将 test3 文件夹权限设置成对 test31 用户完全控制，test32 用户只可以读取；并设置 test31, test32 用户其隶属于 Remote Desktop Users 组。

(3) 分别使用 test31、test32 用户登录系统，访问目录 C:\test3\test3.txt，并修改 test3.txt 文件，其访问结果为：_____ (3)_____。

4. 权限累加原则

(1) 注销当前用户，使用 administrator 用户登录系统，新建用户 test4，默认隶属 Users 组。

(2) 在本地磁盘 C 中新建名为 test4 的文件夹，然后在 test4 文件夹中再新建文件夹 subtest4。

(3) 设置文件夹 subtest4 权限，对 test4 只有写权限。

(4) 设置文件夹 test4 权限，对 test4 只有读取和运行的权限。

(5) 注销当前用户，使用 test4 用户登录系统，访问目录 C:\test4\subtest4，证实 test4 用户对此目录拥有的权限？_____ (4)_____。

三. NTFS 分区上分配磁盘配额

(1) 注销当前用户, 使用 administrator 用户登录系统, 新建用户 test5, 默认隶属 Users 组。

(2) 在本地磁盘 C 中点击鼠标右键, 选择“属性”, 打开磁盘属性菜单, 选择磁盘属性对话框中的“配额”选项卡。勾选“启用配额管理”和“拒绝将磁盘空间给超过配额限制的用户”, 点击“配额项”按钮, 进入配额项管理。选择“配额”菜单中的“新建配额项”, 进入选择用户界面添加 test5 用户, 在“添加新配额项”界面中勾选“将磁盘空间限制为”, 调整配额值为 5M, “将警告等级”设为 1KB, 单击“确定”按钮, 完成配额添加。

(3) 注销当前用户, 使用 test5 用户登录系统, 在磁盘 C 中新建一个文件夹 test5, 向 test5 文件夹中添加文件, 记录文件大小超过 5M 时的情况 (5) 。

「注」向文件夹 test5 中添加文件时, 可以新建一个 bmp 画图文件, 用画图工具编辑该图片, 只要增加图片大小即可使文件存储空间变大。

【思考问题】

1. 如何访问没有读取权限的目录下的文件（非继承）。

任务二 审核策略设置

【实验目的】

- 了解计算机审核的重要性
- 掌握使用 Windows 自带审核策略的使用方法
- 掌握 Windows 事件查看器的使用方法

【实验人数】

每组 1 人

【系统环境】

Windows

【网络环境】

交换网络结构

【实验工具】

监控器工具

【实验类型】

验证型

【实验原理】

【实验步骤】

本练习单人作为一组。

一. 设置并验证“审核对象访问”策略

1. 设置“审核对象访问”策略

依次进入“开始” | “程序” | “管理工具” | “本地安全策略”，启动本地安全策略管理器。进入管理器定位到如下分支：“安全设置” | “本地策略” | “审核策略”，选择“审核对象访问”项，双击该项（或单击右键菜单中的属性）进入属性页。选中“审核这些操作”中的“成功”、“失败”复选框。然后单击“确定”按钮完成设置策略操作。同样方法，将其它审核策略设置为“无审核”，如图 1-1-4 所示。










策略 ▲	安全设置
 审核策略更改	无审核
 审核登录事件	无审核
 审核对象访问	成功, 失败
 审核过程跟踪	无审核
 审核目录服务访问	无审核
 审核特权使用	无审核
 审核系统事件	无审核
 审核帐户登录事件	无审核
 审核帐户管理	无审核

图 1-1-4 本地审核策略

2. audit 目录文件审核

(1) C 盘下新建 audit 文件夹。

(2) audit 目录下新建文本文件 general.txt（在启动审核前创建文件）。

(3) 设置 audit 文件夹属性，在属性对话框中依次点选“安全” | “高级” | “审核” | “添加”，在“选择用户或组”对话框的“输入要选择的对象名称”文本框中输入“everyone”，单击“确定”按钮。在弹出的“audit 的审核项目”对话框中，选中“创建文件/写入数据”对应的“成功”与“失败”复选按钮，单击“确定”按钮，直至完成。

(4) 为了能够清晰分析后续审核事件，建议先将系统已有审核条目清除。具体做法如下：通过系统“管理工具”打开“事件查看器”，点选左侧“Windows 日志->安全”分支，右键单击该项，选择“清除所有事件”。

(5) 对 general.txt 文件进行写入操作，并保存。刷新“事件查看器” | “Windows 日志->安全”分支，结合实验原理“常用审核事件 ID”部分，回答下列问题：

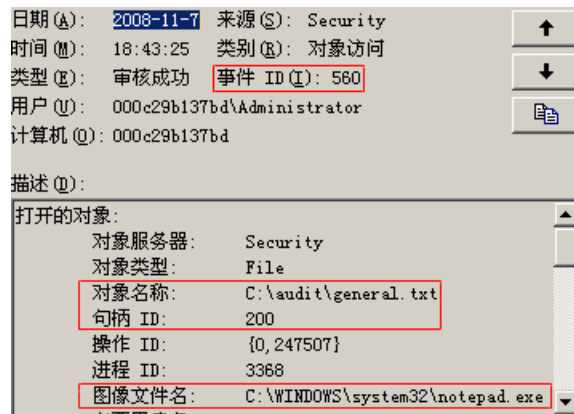


图 1-1-5 事件详细信息 1

针对写入数据操作，系统的审核事件序列是：_____。

解释序列事件：_____。

_____。

_____。

(6) 调换步骤

(2) (3) (4) 步的顺序改为(4) (3) (2)（在启动审核后创建文件），重新进行此部分实验，回答下列问题：

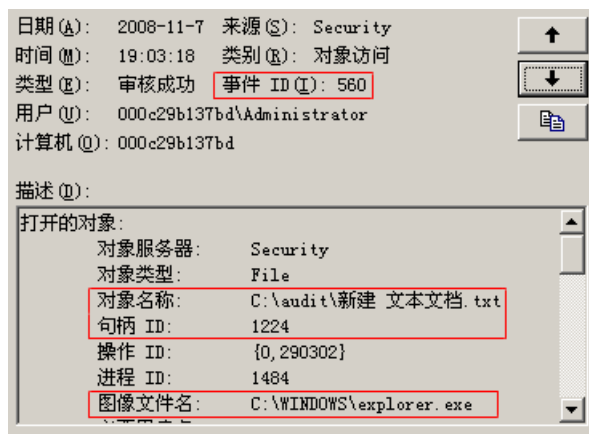


图 1-1-6 事件详细信息 2

针对创建文件操作，系统的审核事件序列是：_____。

解释序列事件：_____。

针对写入数据操作，系统的审核事件序列是：_____。

解释序列事件：_____

_____。

(7) 重新设置 audit 文件夹审核策略，仅对“读取属性”事件进行审核，回答下列问题：

仅针对读取数据操作，系统的审核事件序列是：_____。

解释序列事件：_____。

(8) 可尝试对其它事件进行审核，如删除、更改权限等。

二. 文件事件审计

(1) 单击工具栏“监控器”按钮，打开监控器工具。在左侧向导栏中选择“文件监控”，进入文件监控视图。

(2) 单击菜单栏“选项”|“设置”，在“设置”对话框中可以设置文件监控所要监控的目录、监控进程和操作类型（新建文件、删除文件、文件写操作，修改文件属性）。单击“确定”按钮应用设置。

(3) 单击监控器工具栏按钮，开始文件监控，在指定目录或使用指定应用程序进行新建文件等操作，观察监控视图的审计信息。

【思考问题】

1. 说明策略制定与事件监测的区别？
2. FAT 文件系统是否支持实验中进行的文件审核？

任务三 主机安全加固

【实验目的】

- 了解安全加固概念
- 掌握安全加固流程
- 熟悉安全加固技术

【实验人数】

每组 2 人

【系统环境】

Windows

【网络环境】

交换网络结构

【实验工具】

X-Scan

【实验类型】

验证型

【实验原理】

见《原理篇》实验 1 | 练习一|任务五。

【实验步骤】


下面以主机 A、B 为例，说明实验步骤。

实验主机	实验角色	系统环境
主机 A	测试主机	Windows
主机 B	待加固主机	Windows

首先使用“快照 X”恢复 Windows 系统环境。

一. 漏洞扫描及测试

1. 漏洞扫描

主机 A 进入实验平台，单击工具栏“X-Scan”按钮启动 X-Scan 工具，点击“设置”|“扫描参数”，在“指定 IP 范围”中填入主机 B 的 IP 地址，进入“全局设置”|“扫描模块”，单击“全选”|“确定”。单击工具栏上按钮开始扫描，根据检测报告，完成下表：

Xscan 扫描不出结果

表 1-1-1 检测报告表

系统类型		
开放端口及服务（端口/服务）	端口	服务
	21	
	23	

	80	
	135	
	139	
	445	
系统用户		

2. 漏洞测试

(1) 主机 A 建立 ipc\$ 空连接

主机 A 在命令行下输入如下命令：

```
net use \\主机 B 的 IP\ipc$ "" /user:""
```

当出现“命令成功完成”提示时，说明建立连接成功。

主机 A 删除刚刚建立的空链接。命令如下：

```
net use \\主机 B 的 IP\ipc$ /delete
```

(2) 主机 A 通过 NetBIOS 获得主机 B 信息

主机 A 在命令行下执行如下命令：

```
nbtstat -A 主机 B 的 IP
```

获取不到信息

获得主机 B 的信息包括：主机名_____，MAC 地址_____。

(3) 主机 A 通过 telnet 远程登录主机 B

主机 B 需要先开启 TELNET 服务端 服务。

主机 A 在命令行下执行如下命令：

```
telnet 主机 B 的 IP
```

出现如下提示：

```
您将要您的密码信息送到 Internet 区内的一台远程计算机上。这可能不安全。您还要送
吗(y/n):
```

输入“n” | “Enter”，利用扫描到的弱口令用户，登录主机 B。

此时会提示：

```
Access Denied! Specified user is not a member of TelnetClients group.
Server administrator must add this user to the above group.
```

在主机 B 中将若口令用户添加到 TelnetClients 用户组中。

在主机 B 的 C 盘下新建名称为“jlcsc”的文件夹，命令为_____。通知主机 B 主机查看 D 盘是否出现名为“jlcsc”的文件夹 _____，观察文件夹创建时间为_____。

(4) 主机 A 通过 ftp 访问主机 B

主机 A 打开 IE 浏览器,在地址栏中输入“ftp://主机 B 的 IP 地址”,能否访问 能。

注」需要先开启 FTP 服务,在服务器管理器中添加新的角色 Web 服务 (IIS),创建角色时选择开启 FTP 服务,



在管理工具打开“Internet 信息服务 (IIS) 管理器”



在站点名称选项下右键选择“添加 FTP 站点”，设置根目录为 C 盘下 test 文件夹（如不存在则新建文件夹），ip 地址选择 B 主机 IP，勾选自动启动 FTP 站点，SSL 选无。身份验证选择匿名和基本，授权为所有用户，权限为读取和写入。在 c 盘 test 文件夹下新建一个 test.txt 文档，通过 A 主机浏览器输入 <ftp://B 主机 IP> 即可访问 B 主机的 FTP 服务。



3. 发布检测报告

主机 A 将 D:\ExpNIC\Common\Tools\X-Scan\log 目录下的*_report.html 文件复制到本机 D:\Work 目录下。

二. 安全加固实施

1. 分析检测报告

主机 B 进入主机 A 的共享目录，单击“开始”|“运行”，输入“\\主机 A 的 IP”，根据检测报告，查看自己存在的安全隐患。

2. 关闭 ipc\$空连接

主机 B 单击“开始”|“管理工具”|“服务”，双击“Server”，在“启动类型”下拉列表中选择“禁用”，单击“停止”|“应用”|“确定”（出现“停止其他服务”提示时，选择是即可）。

主机 A 建立 ipc\$空连接，命令如下：

```
net use \\主机 B 的 IP\ipc$ "" /user:""
```

出现提示：_____。

3. 禁用 NetBIOS

主机 B 单击“开始”|“设置”|“控制面板”|“网络连接”，鼠标右键“本地连接”|“属性”|“Internet 协议 (TCP/IP)”|“高级”|“WINS”，单击“禁用 TCP/IP 上的 NetBIOS”|“确定”，结束本地连接设置。

主机 A 通过 NetBIOS 获取主机 B 信息，在命令行下执行如下命令：

```
nbtstat -A 主机 B 的 IP
```

出现提示：_____。

4. 关闭 445 端口

445 端口在 Windows 2000 Server 或 Windows Server 2003 系统中发挥的作用与 139 端口是完全相同的。它也是提供局域网中文件或打印机共享服务。不过该端口是基于 CIFS 协议（通用因特网文件系统协议）工作的，而 139 端口是基于 SMB 协议（服务器协议族）对外提供共享服务。在“网络攻防”|“实验 4”|“练习一”中，就是利用 445 端口提供的服务漏洞进行攻击。通常加固的方法是停止提供的服务或者为系统安装补丁。

(1) 验证 445 端口是否开启

主机 B 在命令行中输入如下命令：

```
netstat -an
```

查看到 445 端口处于 Listening：

TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING

(2) 若主机不需要文件共享服务，可以通过修改注册表来屏蔽 445 端口

主机 B 单击“开始”|“运行”，输入“regedit”，单击“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\NetBT\Parameters”，右键右侧空白处，选择“新建”|“DWORD 值”，名称为 SMBDeviceEnabled，值为 0，修改完后重启计算机。

主机 B 执行如下命令：

```
netstat -an
```

此时 445 端口是否开启_____。

(3) 若主机需要开启文件共享，则可通过安装系统补丁，预防攻击。方法参见“网络攻防”|“实验 4 缓冲区溢出”|“练习一 缓冲区溢出攻击”中的步骤。

5. 禁止 Telnet 服务。

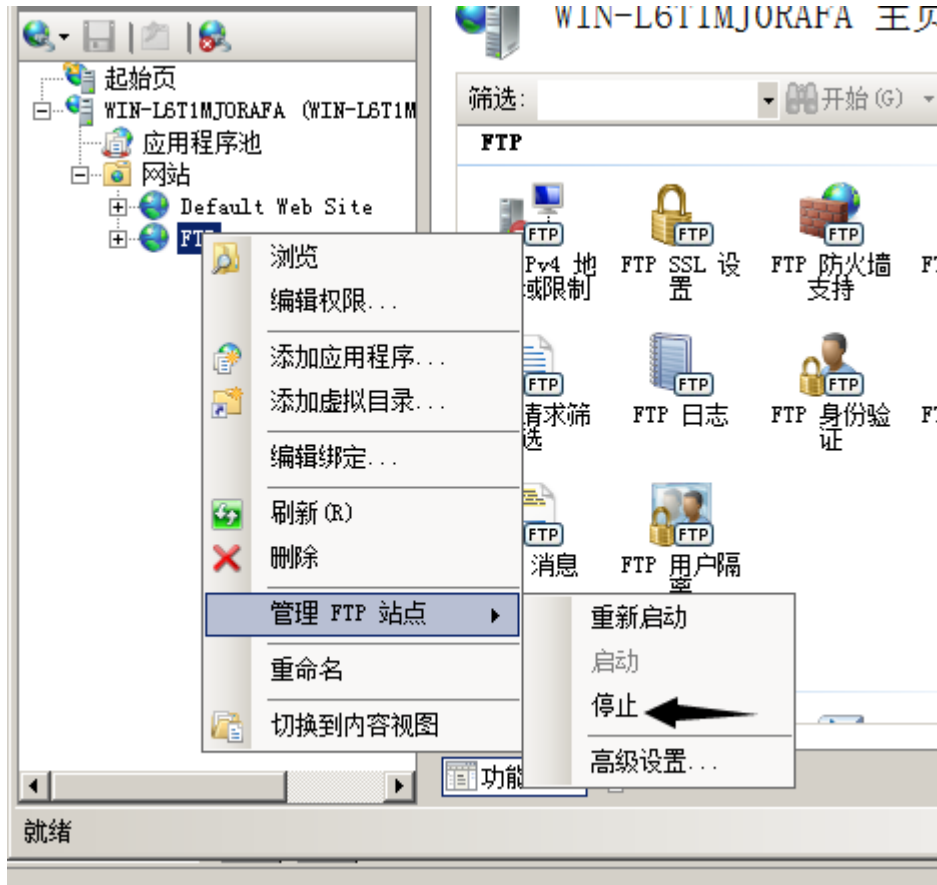
主机 B 单击“开始”|“管理工具”|“服务”，双击“Telnet”，在“启动类型”下拉列表中选择“禁用”，单击“停止”|“应用”|“确定”。

主机 A 重新 telnet 主机 B，出现提示_____。

6. 禁止 ftp 服务

主机 B 单击“开始”|“管理工具”|“Internet 信息服务（IIS）管理器”，在网站目录下，找到 FTP，右键，选择管理 FTP 站点，停止。

主机 B 查看 21 端口是否关闭，在 DOS 下执行如下命令：



```
netstat -an
```

主机 B 的 21 端口是否关闭？_____

主机 A 通过 ftp 访问主机 B，结果如何？_____

7. 修改存在弱口令账号

针对检测报告主机 B 存在用户名为“test”，密码为“1234”的弱口令帐户，更改 test 用户的密码为“jlcssadmin”，在命令行下输入命令如下：

```
net user test jlcssadmin
```

三. 加固测试

(1) 主机 A 使用 X-Scan 再次对主机 B 进行扫描，根据本次检测报告，对比第一次生成的检测报告，完成下表：

XSCAN 无法扫描到存活主机

表 1-1-2 加固测试检测报告

对比项	加固前	加固后
扫描时间		
漏洞数量		
警告数量		
提示数量		
是否发现安全漏洞		
是否检测到 NetBIOS 信息		

(2) 有兴趣的同学可以参考“网络攻防”|“实验 2”|“练习二 模拟攻击方法”的实验步骤，对加固后的主机 B 进行模拟攻击测试。

【思考问题】

1. 搜集关于数据库和网络加固的相关知识。