# Windows安全原理与技术

## — 第十二章：安全审核

王轶骏， Eric Ericwyj@sjtu.edu.cn

SJTU.INFOSEC.A.D.T, 2008

# 安全审核的必要性

- 如果安全体系被突破了，那么我们...
  - 需要知道系统遭受何种攻击，如何才能恢复系统。
  - 需要知道系统存在什么漏洞。
  - 需要获取攻击者留下的证据。

安全审核就是飞机上的“黑匣子”

# Windows 2000/XP/Server 2003中的审核

- Windows 2000/XP/Server 2003中的审核是对计算机上用户活动和系统活动过程（称之为事件）的跟踪。
- 事件被分别记录到六种日志中：
  - 应用程序日志
  - 系统日志
  - 安全日志

  在所有的Windows 2000中均存在
  - 目录服务日志
  - 文件复制日志
  - DNS服务器日志。

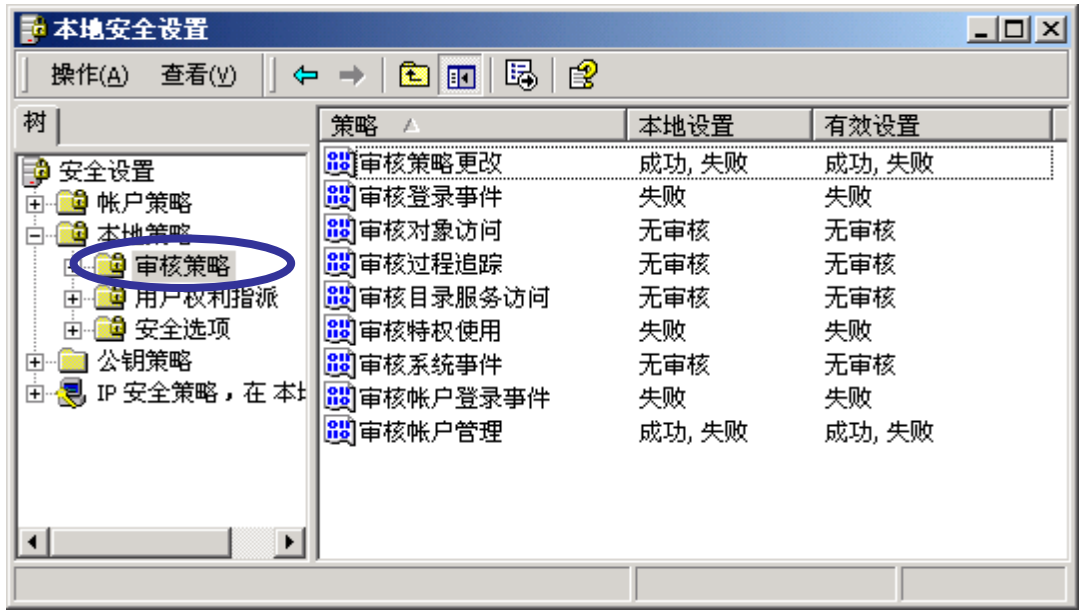
  依赖于特定的服务

# 事件日志的类型

- 应用服务日志
  - 记录了应用程序和系统产生的事件。
  - 任何厂商开发的应用程序都可以用审核系统将自己注册，并向应用程序日志中写入事件。
- 系统日志
  - 含有Windows 2000系统自身产生的事件，以及驱动程序等组件产生的事件。
- 安全日志
  - 含有关于安全事件的信息，其中包括与监视系统、用户和进程的活动相关的信息，以及关于启动失败等安全服务的消息。

# 安全审核策略的设置

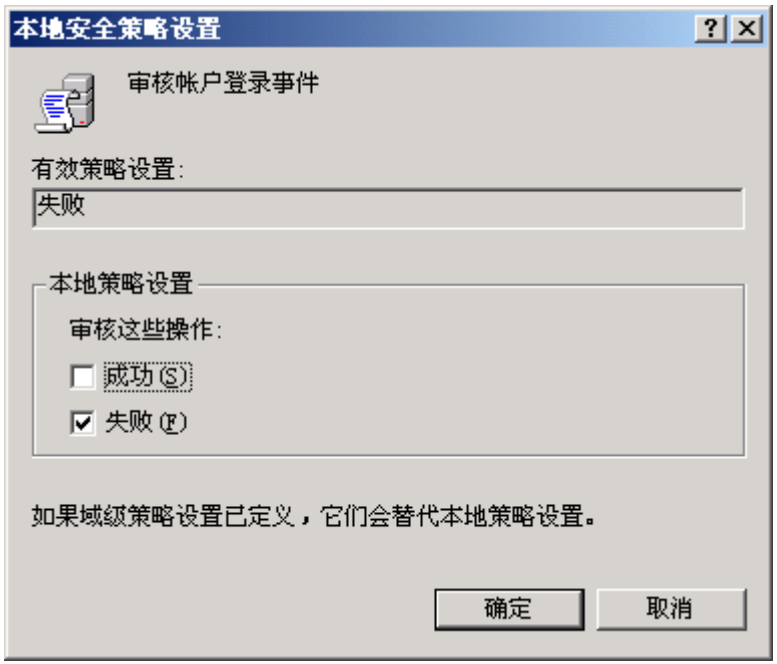
- 选择系统要审核的事件类型：
  - 策略更改
  - 登录事件
  - 对象访问
  - 过程追踪
  - 目录服务访问
  - 特权使用
  - 系统事件
  - 账户登录事件
  - 账户管理




“本地安全策略”（“组策略”→“计算机设置”→“Windows设置”）→“安全设置”→“本地策略”→“审核策略”

- 指明是否要跟踪成功的事件还是失败的事件

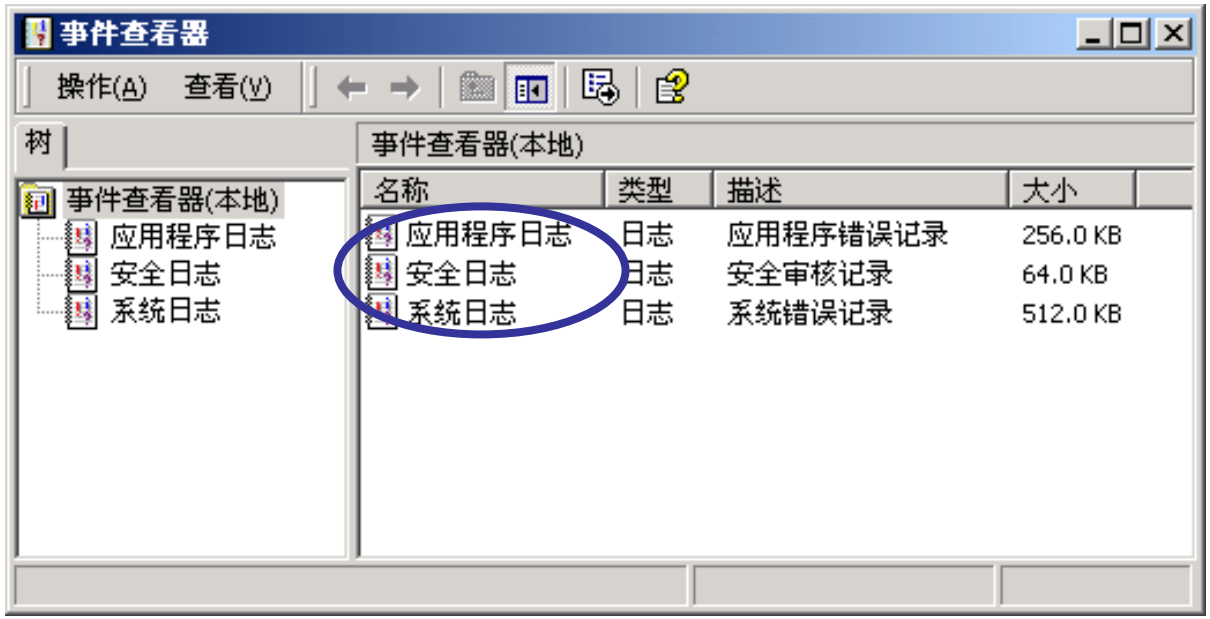
双击某一项审核策略，如“审核帐户登录事件”



# 事件日志的管理

- 事件查看器

“开始”→“程序”→“管理工具”→“事件查看器”
（或者“开始”->“运行”，输入“eventvwr”）



# 事件类型及其含义

| 事件类型 | 描述 |
| --- | --- |
| 错误 | 重要的问题，如数据丢失或功能丧失。例如，如果在启动期间服务加载失败，则会记录错误。 |
| 警告 | 不是非常重要但将来可能出现的问题事件。例如，如果磁盘空间较小，则会记录一个警告。 |
| 信息 | 描述应用程序、驱动程序或服务成功操作的事件，例如成功地加载网络驱动程序时会记录一个信息事件。 |
| 成功审核 | 审核安全访问尝试成功。例如，将用户成功登录到系统上的尝试作为“成功审核”事件记录下来。 |
| 失败审核 | 审核安全访问尝试失败。例如，如果用户试图访问网络驱动器失败，该尝试就会作为“失败审核”事件进行记录。 |

# 事件日志属性的设置

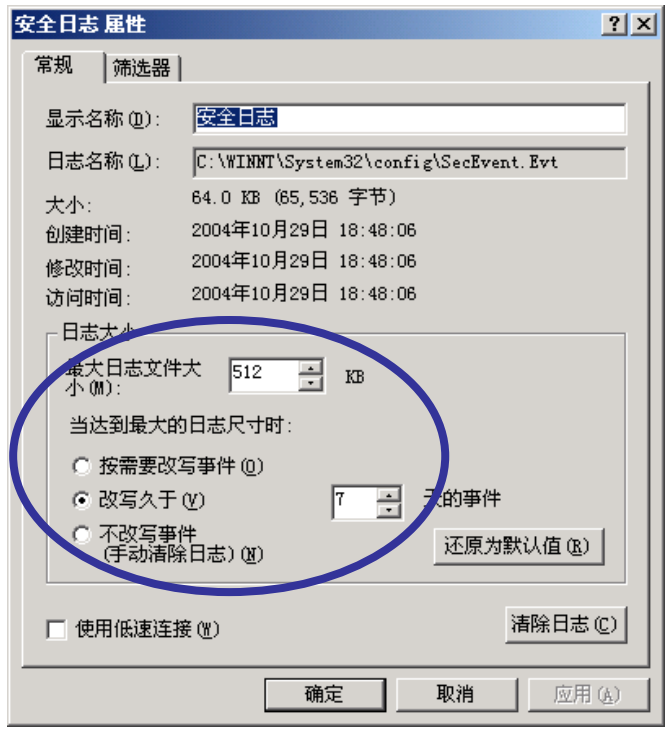
- 在“事件查看器”管理工具中设置
  - 在“事件查看器”中选择“应用程序日志”/“安全日志”/“系统日志”→ “属性”
- 通过“组策略”设置
  - “计算机配置”→ “Windows设置” → “安全设置” → “事件日志”

# 事件日志的属性

- 日志最大值
- 日志保留方式

当事件日志被填满，即达到最大值时，该如何处理原有的日志。

  - 按需要改写
    - 不管保留时间的要求如何都覆盖以前的事件
    - 容易覆盖潜在的重要事件（原来的）
  - 按日期改写
    - 覆盖所保留时间之前的事件
    - 容易不记录重要的事件（新的）
  - 不改写
    - 从不覆盖事件，需要手工清除
    - 不记录新的事件（新的）

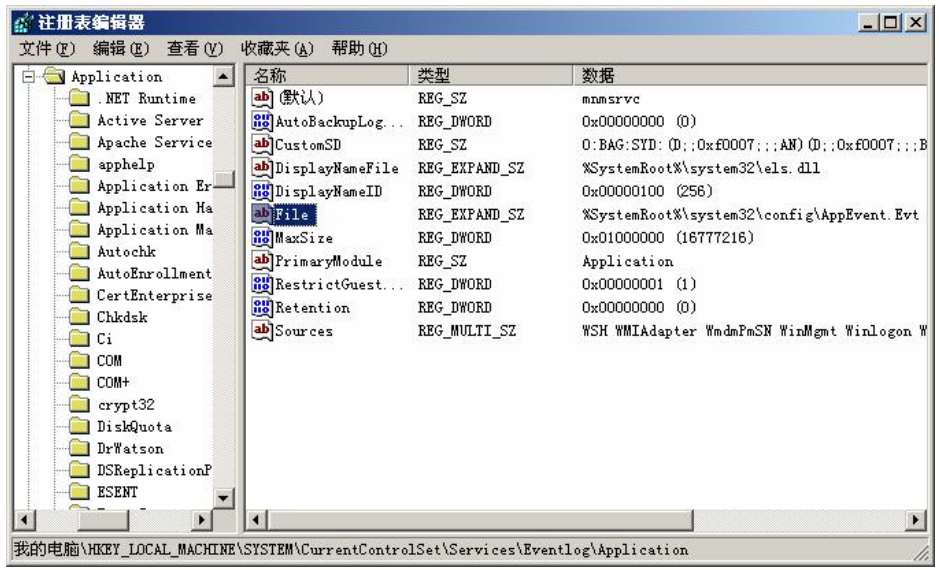


# 事件日志的文件存储路径

- 默认情况如下
  - 安全日志文件：
    %systemroot%\System32\config\SecEvent.EVT
  - 系统日志文件：
    %systemroot%\System32\config\SysEvent.EVT
  - 应用程序日志文件：
    %systemroot%\System32\config\AppEvent.EVT

# 事件日志的移位及保护

- 修改日志文件存放位置
  - 打开注册表，进入到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog
    位置，找到Application、Security、System这几个子键，它们分别对应“应用程序日志”、“安全日志”和“系统日志”。
  - 比如展开Application子键，其中File项的键值就是“应用程序日志”文件存放的位置。可将它改成想要另行存放的位置“D:\log”文件夹下。

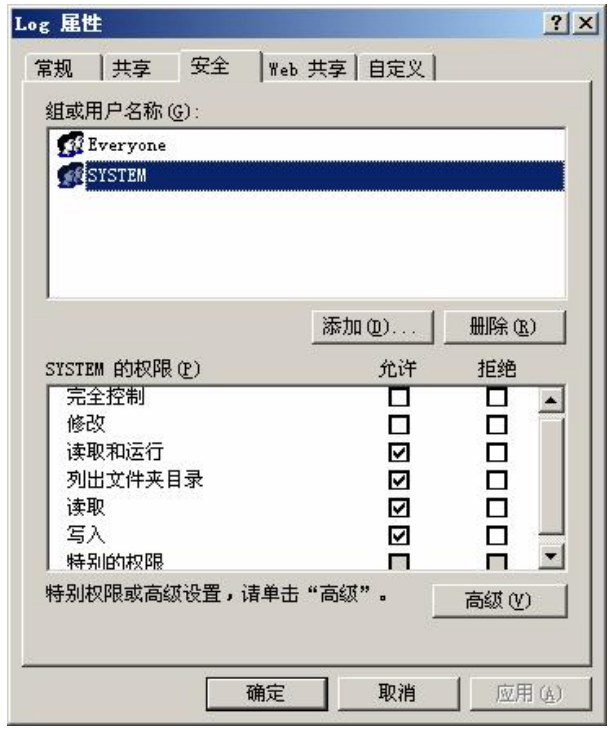


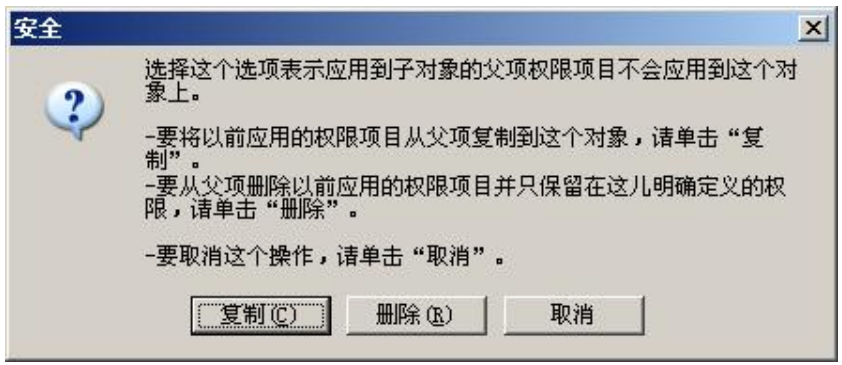
# 事件日志的移位及保护（续）

- 转移事件日志文件
  - 在D:盘建立目录LOG，并将日志文件“%systemroot%/system32/config/appevent.evt”复制到该文件夹下。
- 确认日志存放路径的转移结果
  - 重启计算机后，打开“事件查看器”查看“应用程序日志” 的属性。
  - 同样可依次更改其他日志文件的存放位置。

# 事件日志的移位及保护（续）

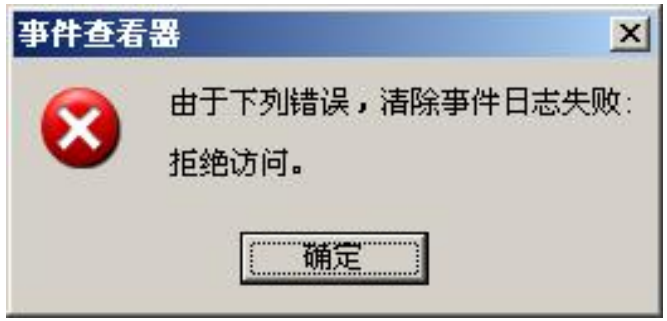
- 设置事件日志文件的访问权限
  - 选择日志保存文件夹，右键“属性”→“安全”→“高级”，将“允许将来自父系的可继承权限传播给该对象”复选框的选择去掉，在弹出的对话框中选择“复制”。
  - 删除在“组或用户名称”中除“SYSTEM”、“Everyone”以外的所有组，给予“SYSTEM”除完全控制和修改外的所有权限，只给“Everyone”读取权限。



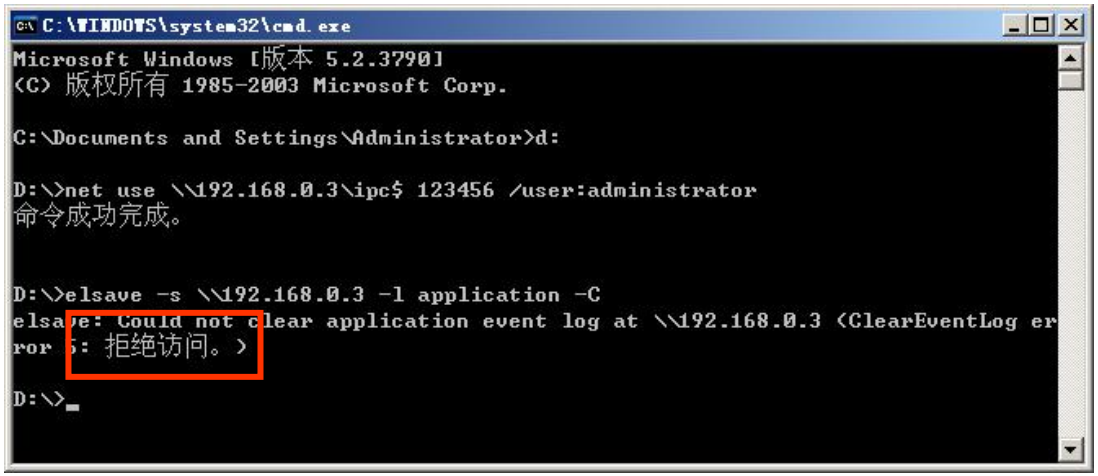



# 事件日志的移位及保护（续）

- 确认日志文件无法被清除。
  - 尝试用“事件查看器”来清除日志。



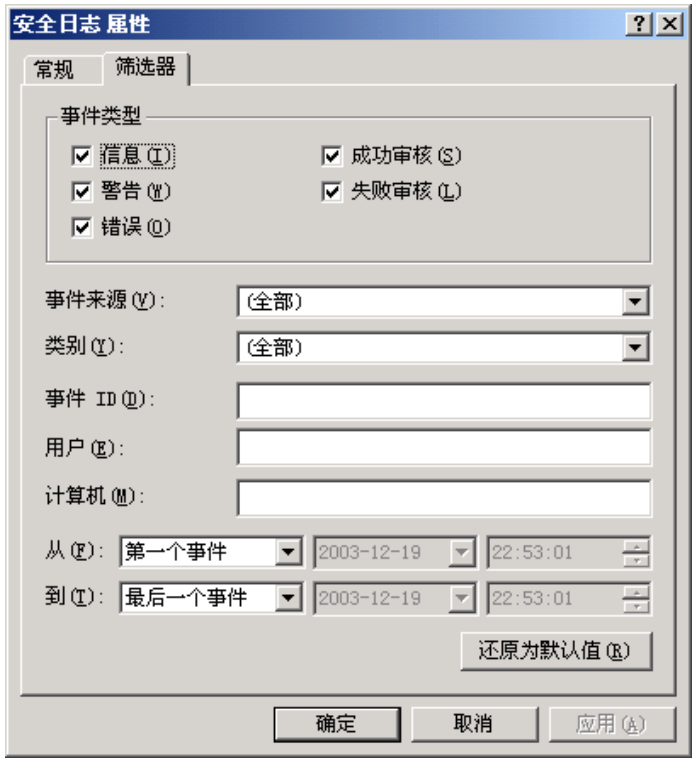

  - 尝试用日志清除工具“Elsave”来清除日志。



# 事件日志的筛选

- 可以在事件查看器中定义筛选器以查找特定的事件。
  - 事件类型
  - 事件来源
  - 事件类别
  - 事件ID
  - 用户
  - 计算机
  - 日期间隔

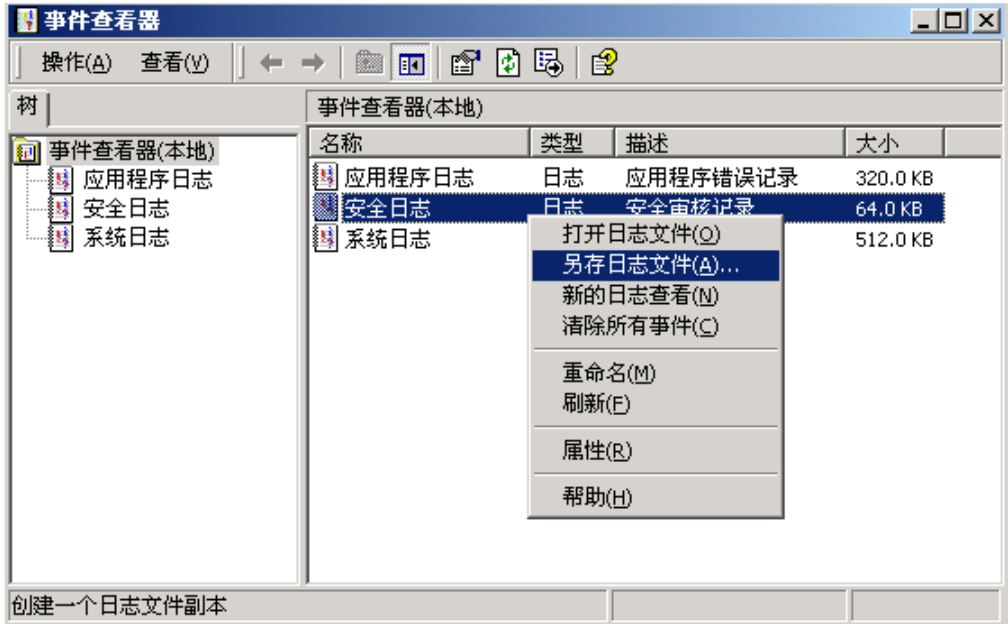
打开“事件查看器”→选择“安全日志”（或其他）→“属性”→“筛选器”



# 事件日志的转储

- 通过“事件查看器”

  打开“事件查看器”→选择“安全日志”（或其他）→“另存日志文件”




存储格式为“*.evt”（二进制文件）

## 使用Dumpel.exe（Dump Event Log Tool）

- 包含在Microsoft的Resource kit工具包中
- 可将事件日志转储到以制表符分隔的文本文件中，便于进一步的筛选和过滤
- dumpel -s \\server -f filename -l log
  - -s \\server： 输出远程计算机日志，若是本地则可省略。
  - -f filename：输出日志的位置和文件名。
  - -l log log： 可选的为 system、security、application等。

把目标服务器 192.168.0.3 上的系统日志转存为 backupsystem.log

dumpel –s \\192.168.0.3 -l system -f backupsystem.log

SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

# Any Questions ?

确定 取消