Windows 日志配置操作

日志配置

1、审核登录

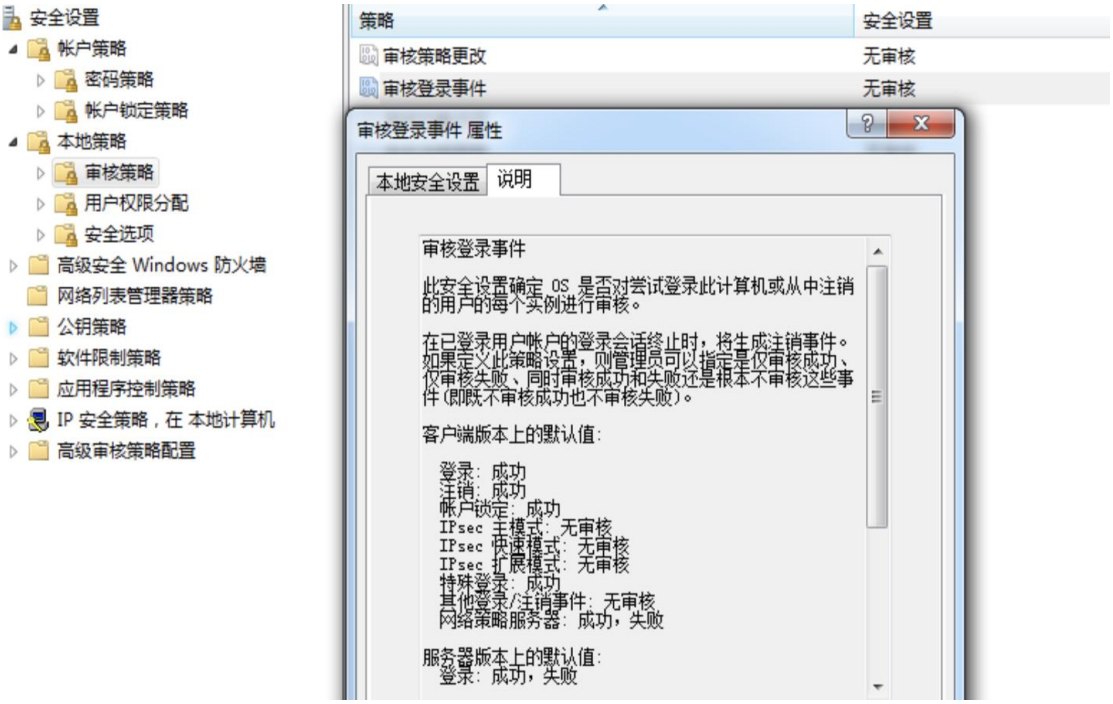
设备应配置日志功能，对用户登录进行记录。记录内容包括用户登录使用的帐户、登录是否成功、登录时间、以及远程登录时间、及用户使用的 IP 地址。

思考：

当电脑被攻击以后，就能通过这些信息定位到黑客是通过什么方式、什么时间、使用什么 IP 登录的，方便之后的攻击溯源。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 审核策略 中，设置 审核登录事件。



2、审核策略

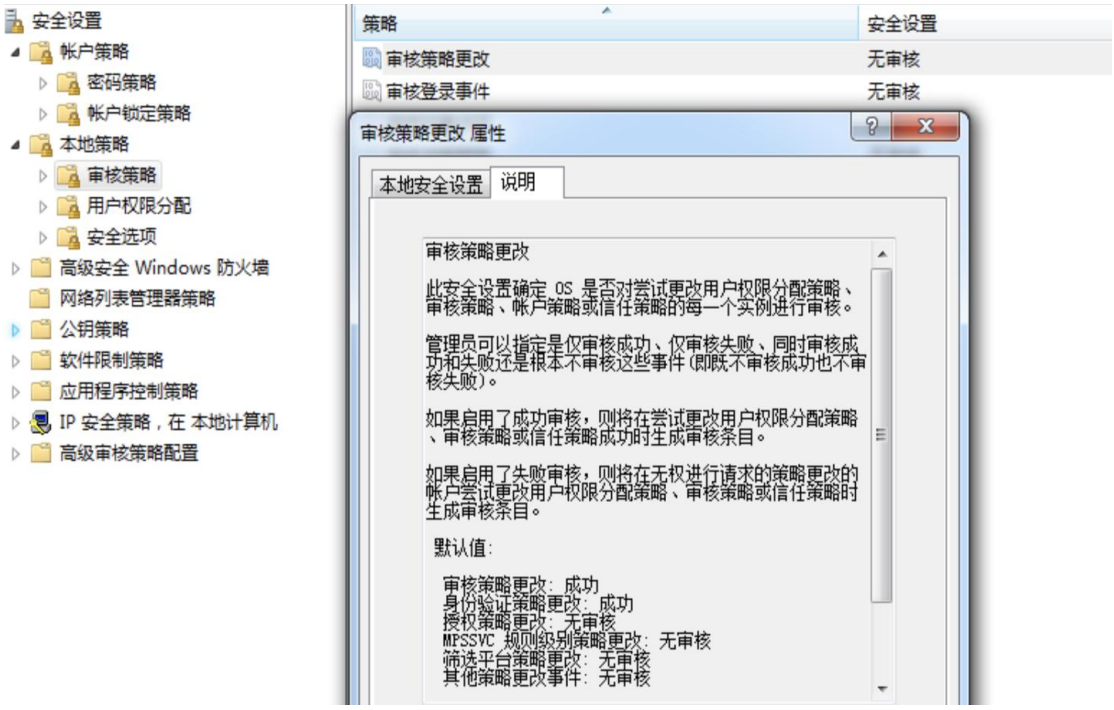
启用本地安全策略中对 Windows 系统的审核策略更改，成功和失败操作都需要审核。

思考：

看说明知道这是一个 OS 对尝试更改用户权限进行审核，如黑客通过 net localgroup administrators 1234 /add 进行用户提权，这边就能查看到相关信息，是否提权成功或失败，就能知道攻击者拿到了多大权限。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 审核策略 中，设置 审核策略更改。

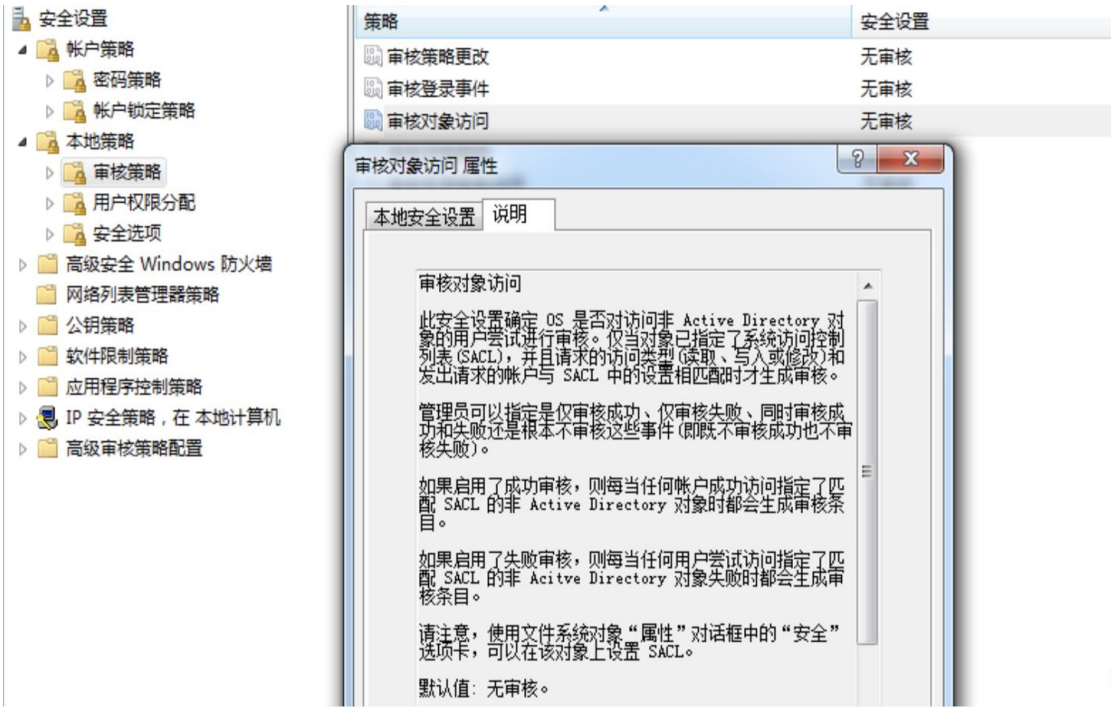


3、审核对象访问

启用本地安全策略中对 Windows 系统的审核对象访问，成功和失败操作都需要审核。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 审核策略 中，设置 审核对象访问。

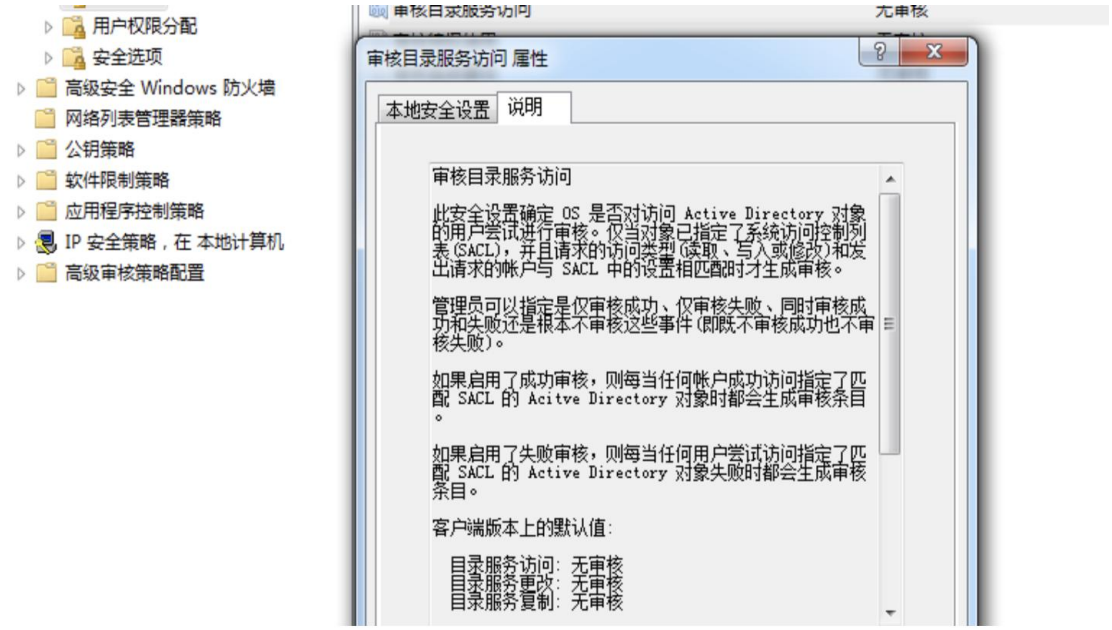


4、审核事件目录服务访问

启用本地安全策略中对 Windows 系统的审核目录服务访问，仅需要审核失败操作。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 审核策略 中，设置 审核目录服务器访问。

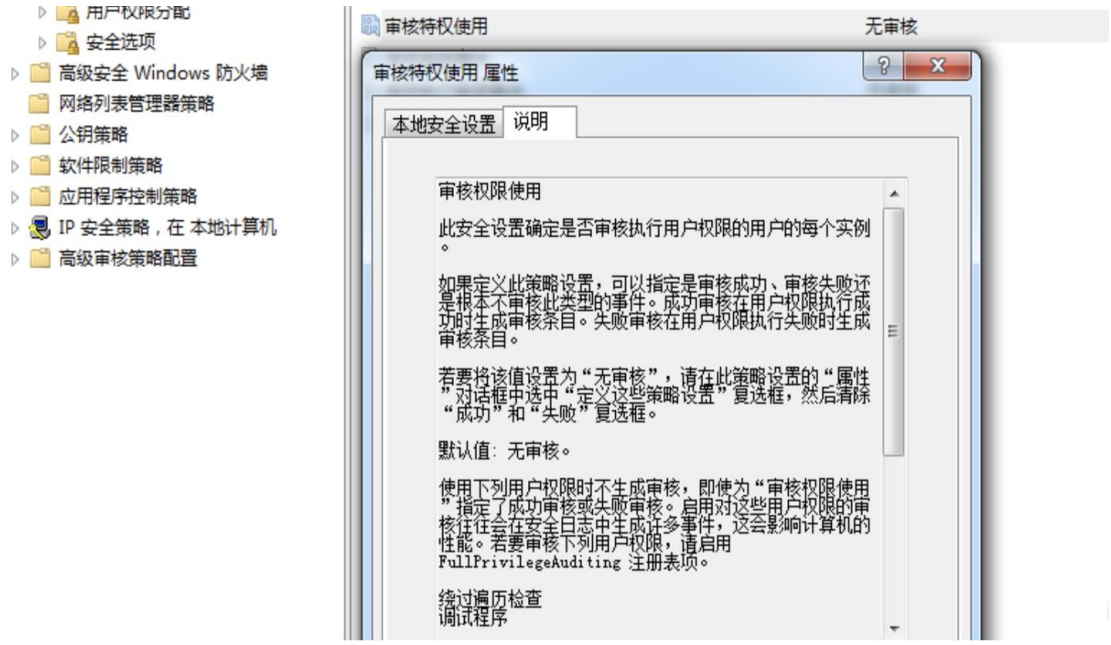


5、审核特权使用

启用本地安全策略中对 Windows 系统的审核特权使用，成功和失败操作都需要审核。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 审核策略 中，设置 审核特权使用。

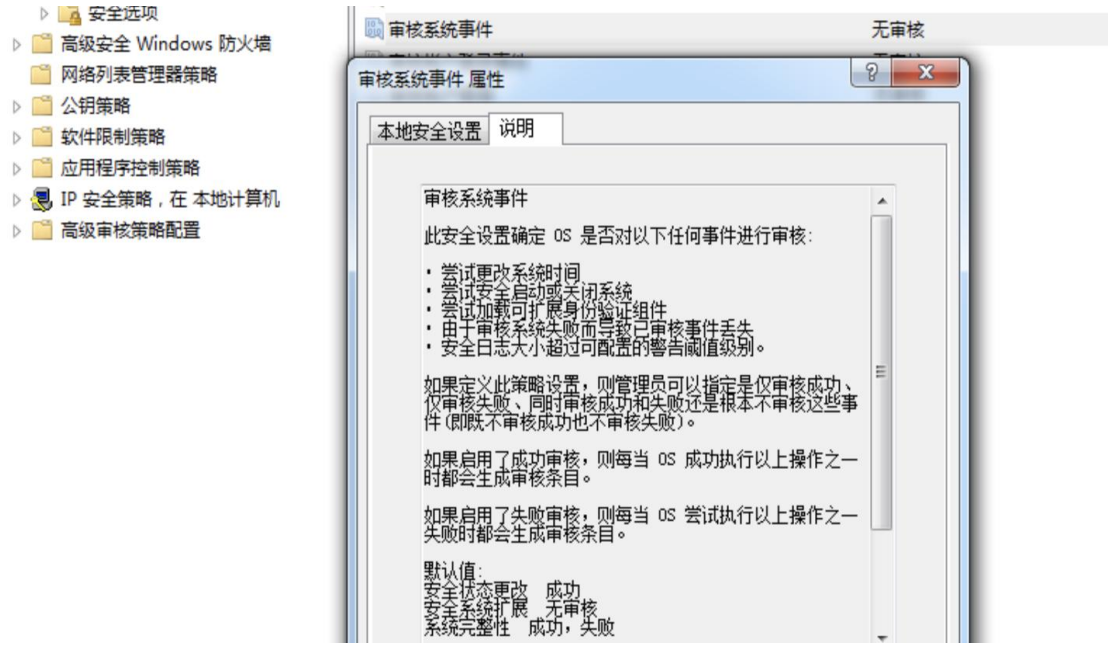


6、审核系统事件

启用本地安全策略中对 Windows 系统的审核系统事件，成功和失败操作都需要审核。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 审核策略 中，设置 审核系统事件。



7、审核帐户登录事件

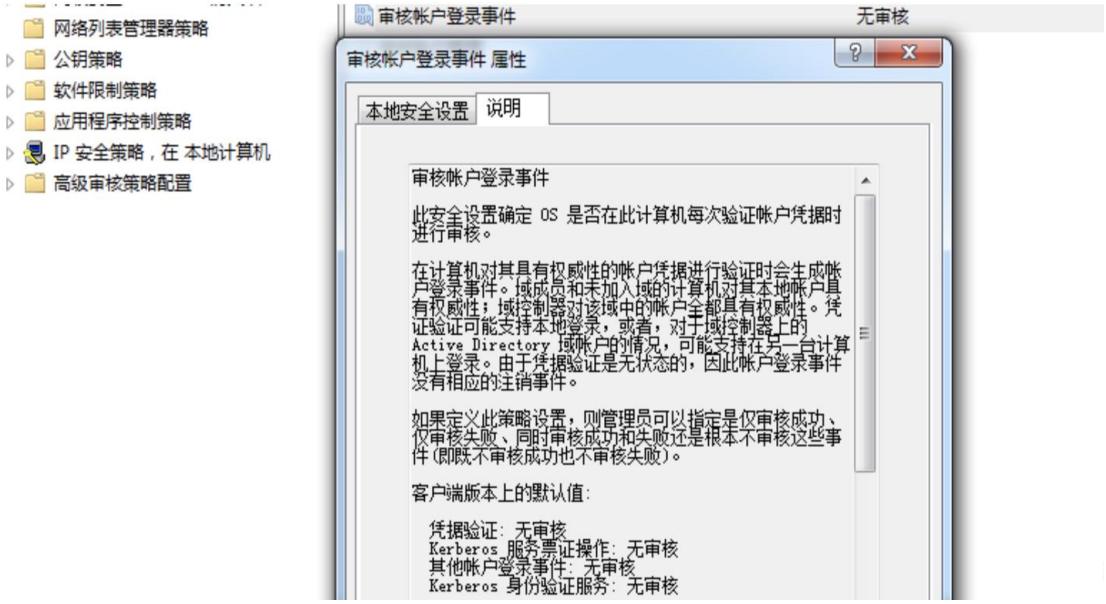
启用本地安全策略中对 Windows 系统的审核帐户登录事件，成功和失败操作都要审核。

思考：

主要防止域用户被攻击之后，想通过用户来登录本地账户，对这类行为进行审核。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 审核策略 中，设置 审核帐户登录事件。

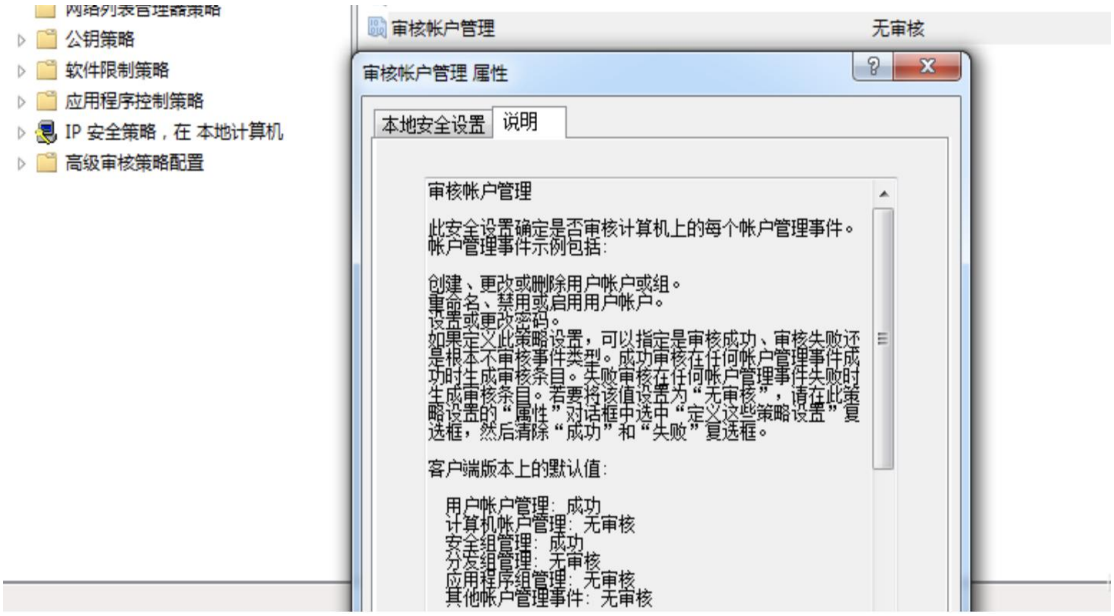


8、审核帐户登录管理

启用本地安全策略中对 Windows 系统的审核帐户管理，成功和失败操作都要审核。

操作步骤

本地安全策略，在 本地策略 > 审核策略 中，设置 审核帐户管理。

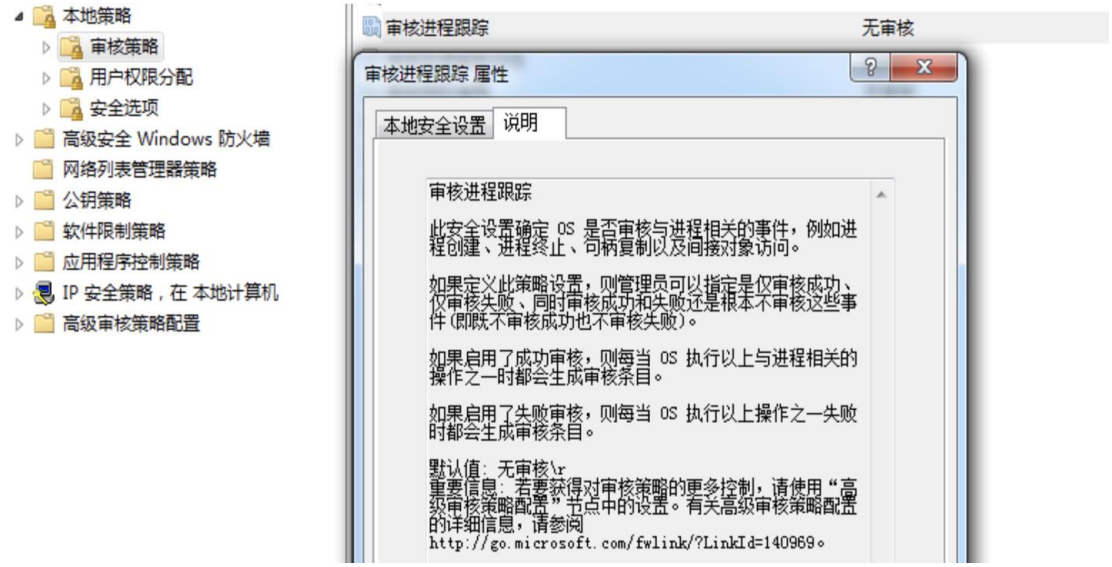


9、审核进程追踪

启用本地安全策略中对 Windows 系统的审核进程追踪，仅失败操作需要审核。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 审核策略 中，设置 审核进程追踪。



10、日志文件大小

设置应用日志文件大小至少为 8192 KB，可根据磁盘空间配置日志文件大小，记录的日志越多越好。并设置当达到最大的日志尺寸时，按需要轮询记录日志。

思考:

日志满时将其存档不覆盖，主要是为了当发生安全事件时进行溯源。

操作步骤

打开 控制面板 > 管理工具 > 事件查看器，配置 应用日志、系统日志、安全日志 属性中的日志大小，以及设置当达到最大的日志尺寸时的相应策略。