**服务器基本安全策略配置**

windows服务器安全策略设置

为加强windows服务器的安全性，针对windows服务器运行的程序和服务，制定相关安全策略。

一、 服务器基本情况

二、 计算机安全策略配置

(一) 修改远程桌面端口：将默认端口XXX修改为XXX。

(二) 帐户：对系统管理员默认帐户administrator进行重命名，停用guest用户。

(三) 开启windows防火墙：

Ø 取消网络连接中的文件和打印共享。

Ø 在例外里面添加远程桌面端口XXX。

Ø 在防火墙高级设置时勾选Web 服务和安全的Web服务。

Ø 在防火墙开放FTP端口XX。

Ø 开放短信发送平台端口：XXX

(四) 禁用无关服务。

Ø Print spooler  打印服务

Ø Wireless configuration  无线服务

Ø Routing and Remote Access 在局域网以及广域网环境中为企业提供路由服务。

Ø NTLMSecuritysupportprovide：telnet服务和Microsoft Serch服务使用。

Ø Telnet 允许远程用户登录到此计算机并运行程序。

Ø Remote Desktop Help Session Manager：远程协助服务。

Ø Error Reporting Service 收集、存储和向 Microsoft 报告异常应用程序。

Ø Remote Registry  远程注册表操作。

(五) 禁止IPC空连接：打开注册表，找到Local\_Machine\System\CurrentControlSet\Control\LSA-RestrictAnonymous 把这个值改成”1”即可。

(六) 删除默认共享：打开注册表，找到HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters，新建 AutoShareServer类型是REG\_DWORD把值改为0。

(七) 策略配置

1. 组策略配置:gpedit—>计算机配置—>windows设置—>安全设置—>本地策略。

Ø 在用户权利分配下，从通过网络访问此计算机中删除Power Users和Backup Operators;

Ø 启用不允许匿名访问SAM帐号和共享;

Ø 启用不允许为网络验证存储凭据或Passport;

Ø 从文件共享中删除允许匿名登录的DFS$和COMCFG;

Ø 启用交互登录：不显示上次的用户名;

Ø 启用在下一次密码变更时不存储LANMAN哈希值;

Ø 禁止IIS匿名用户在本地登录。

2. 本地安全策略设置:

　　开始菜单—>管理工具—>本地安全策略

A、本地策略——>审核策略

Ø 审核策略更改　成功　失败

Ø 审核登录事件　成功　失败

Ø 审核对象访问失败

Ø 审核过程跟踪　无审核

Ø 审核目录服务访问失败

Ø 审核特权使用失败

Ø 审核系统事件　成功　失败

Ø 审核账户登录事件　成功　失败

Ø 审核账户管理　成功　失败

注：在设置审核登陆事件时选择记失败，这样在事件查看器里的安全日志就会记录登陆失败的信息。

B、本地策略——>用户权限分配

Ø 关闭系统：只有Administrators组、其它全部删除。

Ø 通过终端服务拒绝登陆：加入Guests、User组

Ø 通过终端服务允许登陆：只加入Administrators组，其他全部删除。

C、本地策略——>安全选项

Ø 交互式登陆：不显示上次的用户名　启用

Ø 网络访问：不允许SAM帐户和共享的匿名枚举启用

Ø 网络访问：不允许为网络身份验证储存凭证　启用

Ø 网络访问：可匿名访问的共享　全部删除

Ø 网络访问：可匿名访问的名全部删除

Ø 网络访问：可远程访问的注册表路径全部删除

Ø 网络访问：可远程访问的注册表路径和子路径全部删除

D：本地策略>软件限制策略>其它规则

Ø 新建规则不允许运行以下文件: scrrun.dll,shell.dll，QQ.exe,thunder.exe,telnet.exe等等。随着维护的深入，逐步追加服务器不需要运行的应用程序。

三、 安全策略的作用

对服务器进行以上的设置和相关策略的制定，可以有效的增加服务器的自身防御能力，防止黑客利用常见的攻击手段和方法对服务器进行入侵和破坏。