Windows7操作系统加固措施

为应对Windows7（以下简称“Win7”）操作系统停止更新后带来的安全风险，以及目前我校部分用户继续使用Win7的实际现状，建议在Win7操作系统上做好加固措施，具体措施如下。

**1、更新或安装“360安全卫士win7盾甲个人版（免费）”**

下载地址：[http://down.360safe.com/360win7](http://down.360safe.com/360win7/360win7_setup_v2.exe)

![C:\Users\fengyingwei\AppData\Roaming\Tencent\Users\42396593\QQ\WinTemp\RichOle\]S9}0$CUJE%C5@]@)7V`DG2.png]()

**Win7遁甲**



**2、禁用Guest账户和无关账户**

Guest账户为黑客入侵打开了方便之门，黑客使用Guest账户可以进行提权。禁用Guest账户是最好的选择。

操作流程：进入“控制面板->管理工具->计算机管理->本地用户和组->用户->Guest”

“账户已禁用”打勾启用

**加固后：**

![C:\Users\fengyingwei\AppData\Roaming\Tencent\Users\42396593\QQ\WinTemp\RichOle\MRA@KC~T]9UAH9EZZOX`I(I.png]()

**3.密码策略加强**

操作系统、用户身份鉴别信息应具有不易被冒用的特点，口令应复杂并定期更换。

操作流程：进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”;

“密码必须符合复杂度要求” 设 置为“启用”

“密码长度最小值”设置为“8个字符”

“密码最长使用期限”设置为“90天”

“强制密码历史”设置为“记住5个密码”

“用可以还原的加密来存储密码”设置为“禁用”

**加固前：**



**加固后：**



**4.账户锁定策略加强**

对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过5 次（不含5 次），锁定该用户使用的账号。

操作流程：进入“控制面板->管理工具->本地安全策略”，在“帐户策略->帐户锁定策略”：

“账户额锁定阀值”设置为 5 次、“账户锁定时间”设置为 15分钟

**加固前：**



**加固后：**



**5.设置安全审计**

在主机的审核策略上设置日志审核策略

操作流程：进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”

在主机的审核策略上设置日志审核策略：

审计帐户登录事件： 成功，失败

审计帐户管理： 成功，失败

审计目录服务访问： 成功，失败

审计登录事件： 成功，失败

审计对象访问： 成功，失败

审计策略更改： 成功，失败

审计特权使用： 成功，失败

审计系统事件： 成功，失败

审计过程追踪： 成功，失败

**加固前:**



**加固后:**



**6.启用主机安全选项的"关机前清除虚拟内存页面"**

启用主机安全选项的“关机前清除虚拟内存页面

操作流程:进入“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项

关机：清除虚拟页面文件内存”设置为“已启用”

**加固前：**



**加固后：**



**7.关闭远程会话功能**

操作流程:进入“桌面‘计算机’图标->鼠标右键-属性->远程设置->远程”

**设置后:**



**8.备份数据**

及时备份重要数据，这样就算遇到了极具杀伤性的病毒，也可以通过恢复数据轻松解决。

现代教育技术中心

2021年4月14日