任务一　注册表安全设置

【实验目的】

- 了解注册表的作用
- 掌握注册表的安全设置及修改方法

【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。

一．注册表安全设置

1．　清空可远程访问的注册表路径

WindowsServer2008 操作系统提供了注册表的远程访问功能，只有将可远程访问的注册表路径设置为空，才能有效地防止黑客利用扫描器通过远程注册表读取计算机的系统信息及其它信息。

打开系统“管理工具”，选择“本地安全策略”，将“本地策略”|“安全选项”中的“网络访问：可远程访问的注册表路径、可远程访问的注册表路径和子路径”两项策略清空。如图 1-1-7 所示。

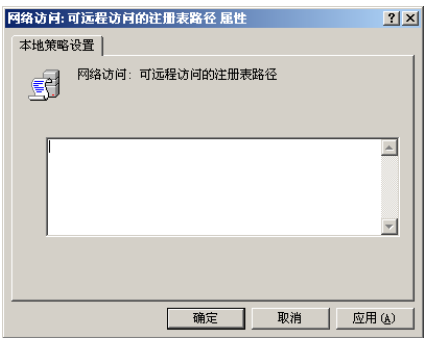

图 1-1-7　设置可远程访问的注册表路径

2. 关闭自动保存隐患

WindowsServer2008 操作系统在调用应用程序出错时，系统会自动将一些重要的调试信息保存起来，以便日后维护系统时查看，不过这些信息很有可能被黑客利用，一旦获取的话，各种重要的调试信息就会暴露无疑。

(1) 双击 C:\WINDOWS\regedit.exe 文件或直接在“开始丨运行”（Win+R）中输入 regedit，打开“注册表编辑器”，如图 1-1-8 所示。

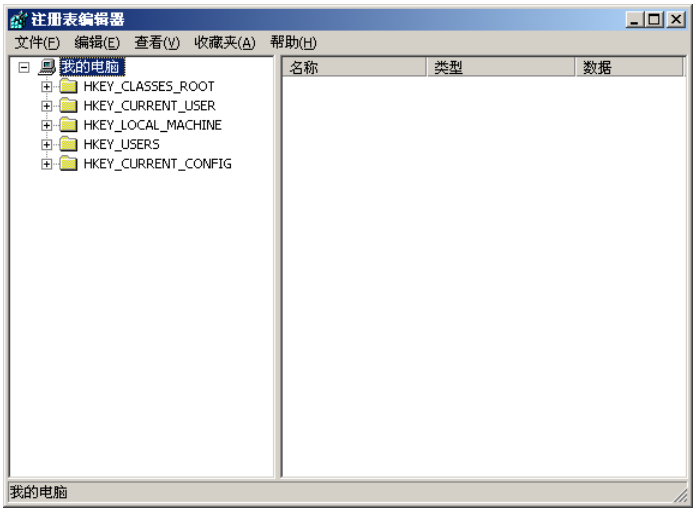

图 1-1-8　注册表编辑器

(2) 依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug 分支，新建“Auto”项的键值为 0。

3. 关闭资源共享隐患

为了给局域网用户相互之间传输信息带来方便，WindowsServer2008 系统提供了文件和打印共享功能，不过我们在享受该功能带来便利的同时，共享功能也给黑客入侵提供了方便。

通过网上邻居设置“本地连接”，在“本地连接 属性”的“常规”选项卡中，取消勾选“Microsoft 网络的文件和打印机共享”。

右击屏幕右下角网络选项图标选择“打开网络和共享中心”，点击页面左侧“更改高级共享设置”，将“家庭或工作”和“公用”两种网络情况下的“文件和打印机共享”选项下选择为“关闭文件和打印机共享”。

4. 关闭页面交换隐患

WindowsServer2008 操作系统中的页面交换文件中，其实隐藏很多重要隐私信息，这些信息都是在动态中产生的，要是不及时将它们清除，就很有可能成为黑客的入侵突破口。

打开注册表编辑器，定位到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement 分支，设置 ClearPageFileAtShutdown 项的键值为 1。

5. 防火墙 TTL 主机类型探测

(1) 打开系统控制台输入命令：

```
ping 127.0.0.1 或 ping localhost
```

查看返回 TTL 值_____。

(2) 打开注册表编辑器，定位到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters，新建 DefaultTTL(DRORD 格式)值为十进制 110。重启系统，使用 ping 命令查看本机 TTL 值_____。