**目录**

[第1章 概述 5](" \l "_Toc5816)

[1.1 目的 5](" \l "_Toc451)

[1.2 适用范围 5](" \l "_Toc7841)

[1.3 适用版本 5](" \l "_Toc15798)

[第2章 操作系统的基本安装 6](" \l "_Toc4186)

[2.1 基本安装 6](" \l "_Toc5625)

[第3章 账号口令 6](" \l "_Toc9448)

[3.1 检查是否已正确配置密码最短使用期限 6](" \l "_Toc3939)

[3.2 检查是否已正确配置密码长度最小值 6](" \l "_Toc26126)

[3.3 检查是否已正确配置“强制密码历史” 7](" \l "_Toc19429)

[3.4 检查是否已正确配置帐户锁定时间 7](" \l "_Toc6216)

[3.5 检查是否已正确配置帐户锁定阈值 8](" \l "_Toc18202)

[3.6 检查是否已正确配置“复位帐户锁定计数器”时间 8](" \l "_Toc5545)

[3.7 检查是否按照权限、责任创建、使用用户账号 8](" \l "_Toc5149)

[3.8 检查是否已更改管理员帐户名称 9](" \l "_Toc10446)

[第4章 认证授权 9](" \l "_Toc3905)

[4.1 检查是否已删除可远程访问的注册表路径和子路径 9](" \l "_Toc12353)

[4.2 检查是否已限制匿名用户连接 10](" \l "_Toc19046)

[4.3 检查是否已限制可关闭系统的帐户和组 10](" \l "_Toc22008)

[4.4 检查是否已限制可从远端关闭系统的帐户和组 11](" \l "_Toc28915)

[4.5 检查是否已限制“取得文件或其它对象的所有权”的帐户和组 11](" \l "_Toc17370)

[4.6 检查是否已正确配置“允许本地登录”策略 12](" \l "_Toc2251)

[4.7 检查是否已正确配置“从网络访问此计算机”策略 12](" \l "_Toc17781)

[4.8 检查是否已删除可匿名访问的共享和命名管道 13](" \l "_Toc24497)

[第5章 日志审计 13](" \l "_Toc2114)

[5.1 检查是否已正确配置审核(日志记录)策略 13](" \l "_Toc12529)

[5.2 检查是否已正确配置应用程序日志 14](" \l "_Toc30509)

[5.3 检查是否已正确配置系统日志 14](" \l "_Toc11604)

[5.4 检查是否已正确配置安全日志 15](" \l "_Toc21306)

[第6章 协议安全 15](" \l "_Toc8101)

[6.1 检查是否已修改默认的远程桌面(RDP)服务端口 15](" \l "_Toc31361)

[6.2 检查是否已启用并正确配置源路由攻击保护 16](" \l "_Toc31302)

[6.3 检查是否已开启Windows防火墙 16](" \l "_Toc6102)

[6.4 检查是否已启用并正确配置SYN攻击保护 17](" \l "_Toc16055)

[6.5 检查是否已启用并正确配置ICMP攻击保护 18](" \l "_Toc2260)

[6.6 检查是否已禁用失效网关检测 18](" \l "_Toc30194)

[6.7 检查是否已正确配置重传单独数据片段的次数 19](" \l "_Toc29991)

[6.8 检查是否已禁用路由发现功能 19](" \l "_Toc26891)

[6.9 检查是否已正确配置TCP“连接存活时间” 20](" \l "_Toc10570)

[6.10 检查是否已启用并正确配置TCP碎片攻击保护 20](" \l "_Toc889)

[6.11 检查是否已启用TCP/IP筛选功能 21](" \l "_Toc6167)

[6.12 检查是否已删除SNMP服务的默认public团体 21](" \l "_Toc21741)

[第7章 其他配置操作 22](" \l "_Toc16847)

[7.1 检查是否已安装防病毒软件 22](" \l "_Toc5799)

[7.2 检查是否已启用并正确配置Windows自动更新 22](" \l "_Toc29843)

[7.3 检查是否已启用“不显示最后的用户名”策略 23](" \l "_Toc30885)

[7.4 检查是否已正确配置“提示用户在密码过期之前进行更改”策略 23](" \l "_Toc14684)

[7.5 检查是否已正确配置“锁定会话时显示用户信息”策略 24](" \l "_Toc23845)

[7.6 检查是否已禁用Windows硬盘默认共享 24](" \l "_Toc6640)

[7.7 检查是否已启用并正确配置屏幕保护程序 25](" \l "_Toc7499)

[7.8 检查是否已启用并正确配置Windows网络时间同步服务(NTP) 25](" \l "_Toc3957)

[7.9 检查是否已关闭Windows自动播放 26](" \l "_Toc2032)

[7.10 检查是否已关闭不必要的服务-DHCP Client 26](" \l "_Toc9863)

[7.11 检查系统是否已安装最新补丁包和补丁 26](" \l "_Toc5085)

[7.12 检查所有磁盘分区的文件系统格式 27](" \l "_Toc3319)

[7.13 检查是否已正确配置服务器在暂停会话前所需的空闲时间量 27](" \l "_Toc18697)

[7.14 检查是否已启用“当登录时间用完时自动注销用户”策略 28](" \l "_Toc7843)

[7.15 域环境：检查是否已启用“需要域控制器身份验证以解锁工作站”策略 28](" \l "_Toc16527)

[7.16 检查是否已禁用“登录时无须按 Ctrl+Alt+Del”策略 29](" \l "_Toc29200)

[7.17 域环境：检查是否已正确配置“可被缓存保存的登录的个数”策略 29](" \l "_Toc22895)

[7.18 域环境：检查是否已正确配置域环境下安全通道数据的安全设置 30](" \l "_Toc10910)

[7.19 域环境：检查是否已启用“域环境下需要强会话密钥”策略 30](" \l "_Toc28770)

[7.20 检查共享文件夹的权限设置是否安全 31](" \l "_Toc17807)

[7.21 检查是否已启用Windows数据执行保护(DEP) 31](" \l "_Toc6986)

[7.22 检查是否已创建多个磁盘分区 31](" \l "_Toc70)

[7.23 检查是否已禁止Windows自动登录 32](" \l "_Toc11512)

[7.24 检查是否已关闭不必要的服务-Simple TCP/IP Services 32](" \l "_Toc10590)

[7.25 检查是否已关闭不必要的服务-Simple Mail Transport Protocol (SMTP) 33](" \l "_Toc11369)

[7.26 检查是否已关闭不必要的服务-Windows Internet Name Service (WINS) 33](" \l "_Toc31621)

[7.27 检查是否已关闭不必要的服务-DHCP Server 34](" \l "_Toc679)

[7.28 检查是否已关闭不必要的服务-Remote Access Connection Manager 34](" \l "_Toc22604)

[7.29 检查是否已关闭不必要的服务-Message Queuing 34](" \l "_Toc31982)

# 概述

## 目的

本文规定了WINDOWS 操作系统主机应当遵循的操作系统安全性设置标准，本文档旨在指导系统管理人员或安全检查人员进行WINDOWS 操作系统的安全合规性检查和配置。

服务器安全基线是指为满足安全规范要求，考虑到信息安全管理的三+四个特性：保密性、完整性、可用性、可审计性、可靠性、抗抵赖性。服务器安全配置必须达到的标准，一般通过检查安全配置参数是否符合安全标准或公司标准来度量。主要包括了账号配置安全、口令配置安全、授权配置、日志配置、IP通信配置等方面内容，这些安全配置直接反映了系统自身的安全脆弱性。

## 适用范围

本配置标准的使用者包括：服务器系统管理员、安全管理员和相关使用人员。

本配置标准适用的范围包括： WINDOWS 服务器。

## 适用版本

适用于Windows Server服务器。

# 操作系统的基本安装

## 基本安装

（1） 使用NTFS文件系统来最小化安装操作系统。

（2） 管理员账号须设置较复杂的口令（由数字、大小写字母和特殊字符组成），长度在12位以上，其中管理员口令应一机一密码，不同机器之间不应相同。

（3） 断开网络安装完操作系统后，在业务网专用区域内连接网络进行系统升级，并打开Windows自动更新服务。

（4） 升级完成后，安装前述光盘中的杀毒软件并进行更新。

# 账号口令

## 检查是否已正确配置密码最长使用期限

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查密码最长使用期限 |
| **安全基线项说明** | 长期修改密码会提高密码暴露风险，所以为了提高系统的保密性。需要检查密码最长使用期限。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\帐户策略\密码策略”，在右边窗格中找到“密码最长存留期(使用期限)”，配置为非0值。如果希望“强制密码历史”有效，则需要将密码最长使用期限设置为大于 0 的值。 |
| **基线符合性判定依据** | <=90 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置密码长度最小值

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查密码长度最小值 |
| **安全基线项说明** | 长度小的口令存在被爆破出的风险，所以为了保证密码的安全，提高保密性  需要检查口令最小长度 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\帐户策略\密码策略”，在右边窗格中找到“密码长度最小值”，配置为不小于标准值的值。 |
| **基线符合性判定依据** | >=8  根据公司规定和等级保护要求，要求密码最小值要大于等于8位 |
| **备注** | 等级：可选 / 评分：3 |

## 检查是否已正确配置“强制密码历史”

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查“强制密码历史”个数 |
| **安全基线项说明** | 强制密码历史的意思是，系统会记住以前的密码历史，在修改密码的时候不可与以前的密码相同，修改相同的密码会提高密码的暴露性。所以为了提高保密性，需要检查是否已正确配置“强制密码历史” |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\帐户策略\密码策略”，在右边窗格中找到“强制密码历史”，配置为不小于标准值的值。 |
| **基线符合性判定依据** | >=2  根据等级保护要求，要求强制密码历史个数要大于等于1 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置帐户锁定时间

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查帐户锁定时间 |
| **安全基线项说明** | 账户锁定时间的意思是：当用户登录失败次数过多时，系统锁定账户的时间  为了防止爆破风险，提高系统的保密性。需要检查是否已正确配置账户锁定时间。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\帐户策略\帐户锁定策略”，在右边窗格中找到“帐户锁定时间”，配置为不小于标准值的值。要配置此设置必须先配置“帐户锁定阈值”。当配置为0时，检测到的实际值为-1。 |
| **基线符合性判定依据** | [5,8] |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置帐户锁定阈值

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查帐户锁定阈值  检查帐户锁定阈值是否不为0 |
| **安全基线项说明** | 账户锁定阈值的意思是：用户失败登录的最大次数。主要作用是为了防止爆破的风险，提高系统的保密性。所以需要检查是否正确配置账户锁定阈值。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\帐户策略\帐户锁定策略”，在右边窗格中找到“帐户锁定阈值”，配置为标准值以内的值。 |
| **基线符合性判定依据** | 5  根据等级保护要求，设置标准值为5 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置“复位帐户锁定计数器”时间

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查“复位帐户锁定计数器”时间 |
| **安全基线项说明** | “复位账户锁定计数器”是指确定登录尝试失败之后和登录尝试失败计数器被复位为 0 次失败登录尝试之前经过的分钟数。有效范围为 1 到 99,999 分钟之间  如果定义了帐户锁定阈值，则该复位[时间](https://baike.baidu.com/item/%E6%97%B6%E9%97%B4" \t "https://baike.baidu.com/item/_blank)应小于或等于帐户锁定[时间](https://baike.baidu.com/item/%E6%97%B6%E9%97%B4" \t "https://baike.baidu.com/item/_blank)。默认值是无，因为只有当指定了帐户锁定阈值时，该[策略](https://baike.baidu.com/item/%E7%AD%96%E7%95%A5" \t "https://baike.baidu.com/item/_blank)设置才有意义。为了提高保密性，需要检查配置“复位账户锁定计数器”时间 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设\安全设置\帐户策略\帐户锁定策略”，在右边窗格中找到“复位(重置)帐户锁定计数器”，配置为不小于标准值的值 |
| **基线符合性判定依据** | 5 |
| **备注** | 等级：可选 / 评分：1 |

# 认证授权

## 检查是否已删除可远程访问的注册表路径和子路径

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查可远程访问的注册表路径和子路径  检查可远程访问的注册表路径 |
| **安全基线项说明** | 注册表是设备配置信息的数据库，其中大部分信息是敏感的。恶意用户可以使用它促进未经授权活动。但是整个注册表中分配的默认ACL相当严格，并且有助于保护注册表免受未经授权的用户访问，这一事实可降低此类攻击的风险 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“网络访问: 可远程访问的注册表路径和子路径”，配置为空。Windows2000和WindowsXP没有此设置，不需配置。 |
| **基线符合性判定依据** | /.+/  注意：远程管理工具（如MBSA和Configuration Manager）需要远程访问注册表，以正确监视和管理这些计算机。如果从可访问路径列表中删除默认注册表路径，则此类远程管理工具可能会失败。 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已限制匿名用户连接

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已禁止SAM帐户的匿名枚举  检查是否已禁止SAM帐户和共享的匿名枚举 |
| **安全基线项说明** | 未经授权的用户可以匿名列出帐户名，并使用该信息执行社交工程攻击或尝试猜测密码。 社交工程攻击者试图以某种方式欺骗用户以获取密码或某种形式的安全信息。为了提高系统的保密性、可靠性，需要检查是否限制匿名用户连接。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“网络访问: 不允许 SAM 帐户的匿名枚举”，配置为“启用”(在Windows2000下，无此设置，不检查此项)。  打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“网络访问: 不允许 SAM 帐户和共享的匿名枚举”，配置为“启用”(在Windows2000下，将“对匿名连接的额外限制”配置为“不允许枚举SAM账号和共享”)。 |
| **基线符合性判定依据** | =1 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已限制可关闭系统的帐户和组

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查可关闭系统的帐户和组 |
| **安全基线项说明** | 可以关闭系统的账户和组必须是管理员权限和组，所以为了提高系统的可靠性，需要检查是否限制关闭系统的账户和组 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\用户权限分配”，在右边窗格中找到“关闭系统”，配置为仅含有“Administrators”用户组 |
| **基线符合性判定依据** | S-1-5-32-544 , administrators |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已限制可从远端关闭系统的帐户和组

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查可从远端关闭系统的帐户和组 |
| **安全基线项说明** | 可以远端关闭系统的账户和组必须是管理员权限和组，所以为了提高系统的可靠性，需要检查是否限制关闭系统的账户和组 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\用户权限分配”，在右边窗格中找到“从远程系统强制关机”，配置为仅含有“Administrators”用户组 |
| **基线符合性判定依据** | S-1-5-32-544 , administrators |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已限制“取得文件或其它对象的所有权”的帐户和组

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查“取得文件或其它对象的所有权”的帐户和组 |
| **安全基线项说明** | 分配此用户权限可能会带来安全风险。 由于对象的所有者可以完全控制它们，因此仅向受信任的用户分配此用户权限。所以为了提高系统可靠性，需要检查是否限制“取得文件或其他对象的所有权”的账户和组。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\用户权限分配”，在右边窗格中找到“取得文件或其他对象的所有权”，配置为仅含有“Administrators”用户组。 |
| **基线符合性判定依据** | S-1-5-32-544 , administrators |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置“允许本地登录”策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查允许本地登录的用户和组 |
| **安全基线项说明** | 依据系统情况来设置允许本地登录的用户和组，主要是为了提高系统的保密性、可靠性。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\用户权限分配(用户权利指派)”，在右边窗格中找到“(允许)在本地登录”，配置为指定授权用户或组。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置“从网络访问此计算机”策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查允许从网络访问此计算机的用户和组 |
| **安全基线项说明** | 依据系统情况来设置从网络访问计算机登录的用户和组，主要是为了提高系统的保密性、可靠性。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\用户权限分配(用户权利指派)”，在右边窗格中找到“从网络访问此计算机”，配置为指定授权用户或组。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已删除可匿名访问的共享和命名管道

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查可匿名访问的共享  检查可匿名访问的命名管道 |
| **安全基线项说明** | 空会话是一个漏洞，可通过环境中设备上的各种共享文件夹来利用它。为了提高系统的可靠性，需要检查是否删除可匿名访问的共享和命名管道。 |
| **检测操作步骤** | 运行“regedit”打开注册表，来到  HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\LanmanServer\Parameters位置，将NullSessionPipes和NullSessionShares这两个参数清空“注意，不要保留空格或者换行，即保持光标位于首位” |
| **基线符合性判定依据** | 可以启用此策略设置，以限制未经身份验证的用户对除 NullSessionPipes 和 NullSessionShares 条目中列出的所有服务器管道和共享文件夹以外的所有服务器管道和共享文件夹的空会话访问。 |
| **备注** | 等级：可选 / 评分：1 |

# 日志审计

## 检查是否已正确配置审核(日志记录)策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查“审核对象访问”级别  检查“审核登录事件”级别  检查“审核目录服务访问”级别  检查“审核帐户登录事件”级别  检查“审核系统事件”级别  检查“审核策略更改”级别  检查“审核帐户管理”级别  检查“审核特权使用”级别  检查“审核进程跟踪”级别 |
| **安全基线项说明** | 为了提高系统的可审计性，需要检查是否正确配置审核日志记录策略。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\审核策略”，在右边窗格中找到“审核对象访问”，勾选“成功”和“失败”。然后参考项目名称一 一 检查 |
| **基线符合性判定依据** | 勾选“成功”“失败” |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置应用程序日志

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查应用程序日志文件达到最大大小时的动作的序号  检查应用程序日志文件最大大小 |
| **安全基线项说明** | 为了提高系统的可审计性，需要检查是否正确配置应用程序日志。 |
| **检测操作步骤** | 打开命令提示符，运行命令“eventvwr.msc”打开事件查看器，浏览到路径“事件查看器(\Windows日志)\应用程序(日志)”，右键点击“应用程序(日志)”，打开其属性对话框，切换到“常规”选项卡，配置“日志文件达到最大大小时”为“按需要改写(覆盖)事件”。  打开命令提示符，运行命令“eventvwr.msc”打开事件查看器，浏览到路径“事件查看器(\Windows日志)\应用程序(日志)”，右键点击“应用程序(日志)”，打开其属性对话框，切换到“常规”选项卡，配置“日志文件最大大小”为不小于标准值(注意：标准值为16进制表示)的值。 |
| **基线符合性判定依据** | “按需要改写事件”  >=0x800000 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置系统日志

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查应用系统文件最大大小  检查系统日志文件达到最大大小时的动作的序号 |
| **安全基线项说明** | 为了提高系统的可审计性，需要检查是否正确配置系统日志。 |
| **检测操作步骤** | 打开命令提示符，运行命令“eventvwr.msc”打开事件查看器，浏览到路径“事件查看器(\Windows日志)\ 系统(日志)”，右键点击“系统(日志)”，打开其属性对话框，切换到“常规”选项卡，配置“日志文件最大大小”为不小于标准值(注意：标准值为16进制表示)的值。  打开命令提示符，运行命令“eventvwr.msc”打开事件查看器，浏览到路径“事件查看器(\Windows日志)\ 系统(日志)”，右键点击“系统(日志)”，打开其属性对话框，切换到“常规”选项卡，配置“日志文件达到最大大小时”为“按需要改写(覆盖)事件”。 |
| **基线符合性判定依据** | >=0x800000  “按需要改写(覆盖)事件” |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置安全日志

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查安全日志文件最大大小  检查安全日志文件达到最大大小时的动作的序号 |
| **安全基线项说明** | 为了提高系统的可审计性，需要检查是否正确配置安全日志。 |
| **检测操作步骤** | 打开命令提示符，运行命令“eventvwr.msc”打开事件查看器，浏览到路径“事件查看器(\Windows日志)\安全(日志)”，右键点击“安全(日志)”，打开其属性对话框，切换到“常规”选项卡，配置“日志文件最大大小”为不小于标准值(注意：标准值为16进制表示)的值。  打开命令提示符，运行命令“eventvwr.msc”打开事件查看器，浏览到路径“事件查看器(\Windows日志)\安全(日志)”，右键点击“安全(日志)”，打开其属性对话框，切换到“常规”选项卡，配置“日志文件达到最大大小时”为“按需要改写(覆盖)事件”。 |
| **基线符合性判定依据** | >=0x800000  按需要改写(覆盖)事件 |
| **备注** | 等级：可选 / 评分：1 |

# 协议安全

## 检查是否已修改默认的远程桌面(RDP)服务端口

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查远程桌面(RDP)服务端口 |
| **安全基线项说明** | Windows系统RDP端口默认值为3389，容易猜测。所以为了提高系统的保密性，需要修改默认的RDP端口。 |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp”，修改名称为“PortNumber”的数值的数据，使其不等于标准值(注意：标准值为16进制表示)。此数据的有效值为1-65535。 |
| **基线符合性判定依据** | ！=0xd3d  依据系统的情况进行修改 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已启用并正确配置源路由攻击保护

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查源路由配置 |
| **安全基线项说明** | 源路由攻击有源地址欺骗、IP欺骗等，为了提高系统的可靠性，需要检查是否启用正确配置源路由攻击保护。 |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“DisableIPSourceRouting”、类型为DWORD、数据为标准值的数值，若已存在则修改其数据。此数据的有效值为0-2，其中0表示转发所有数据包，1表示不转发源路由的数据包，2表示丢弃所有传入源路由的数据包。 |
| **基线符合性判定依据** | =0x2 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已开启Windows防火墙

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查Windows防火墙状态 |
| **安全基线项说明** | 依据系统的情况检查是否需要开启windows防火墙，为了提高系统的可靠性，需要检查是否开启windows防火墙。 |
| **检测操作步骤** | 在Windows2000中，没有Windows防火墙，不检查此项；在WindowsXP及其SP1中，打开控制面板，找到“网络连接”，打开“本地连接”的“属性”对话框，切换到“高级”选项卡，勾选“通过限制或阻止来自Internet…”，并点击下方“设置”按钮设置例外端口；在其余版本的Windows中，打开控制面板，找到“Windows防火墙”，将当前网络位置的防火墙配置为“启用”，并根据实际需求设置例外。 |
| **基线符合性判定依据** | 开启防火墙 |
| **备注** | 等级：可选 / 评分：3 |

## 检查是否已启用并正确配置SYN攻击保护

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已启用SYN攻击保护  检查TCP连接请求阈值  检查取消尝试响应 SYN 请求之前要重新传输 SYN-ACK 的次数  检查处于SYN\_RCVD 状态下的 TCP 连接阈值  检查处于SYN\_RCVD 状态下，且至少已经进行了一次重新传输的TCP连接阈值 |
| **安全基线项说明** | SYN 攻击利用了 TCP/IP 连接建立机制中的安全漏洞。要实施 SYN 洪水攻击，攻击者会使用程序发送大量 TCP SYN 请求来填满服务器上的挂起连接队列。这会禁止其他用户建立网络连接  说明：使 TCP 调整 SYN-ACK 的重传。配置此值后，在遇到 SYN 攻击时，对连接超时的响应将更快速。在超过 TcpMaxHalfOpen 或TcpMaxHalfOpenRetried 的值后，将触发 SYN 攻击保护。  所以为了提高系统的可用性，需要检查是否正确配置SYN的攻击保护 |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“SynAttackProtect”、类型为DWORD、数据为标准值(注意：标准值为16进制表示)的数值，若已存在则修改其数据。此数据的有效值为0-1。  打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“TcpMaxPortsExhausted”、类型为DWORD、数据为标准值(注意：标准值为16进制表示)的数值，若已存在则修改其数据。此数据的有效值为在0-ffff(16进制)。  打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“TcpMaxConnectResponseRetransmissions”、类型为DWORD、数据为标准值的数值，若已存在则修改其数据。此数据的有效值为0-255。  打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“TcpMaxHalfOpen”、类型为DWORD、数据为标准值(注意：标准值为16进制表示)的数值，若已存在则修改其数据。此数据的有效值为在64-ffff(16进制)。  打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“TcpMaxHalfOpenRetried”、类型为DWORD、数据为标准值(注意：标准值为16进制表示)的数值，若已存在则修改其数据。此数据的有效值为在50-ffff(16进制)。 |
| **基线符合性判定依据** | =0x1  =0x5  =0x2  =0x01f4  =0x0190 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已启用并正确配置ICMP攻击保护

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已禁用ICMP重定向 |
| **安全基线项说明** | 通过将此注册表值修改为 0，能够在收到 ICMP 重定向数据包时禁止创建高成本的主机路由  是否响应ICMP重定向报文。ICMP重定向报文有可能被用以攻击，所以系统应该拒绝接受此类报文，用以抵御ICMP攻击。  为了提高系统的可用性，需要检查是否正确配置ICMP攻击保护。 |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“EnableICMPRedirect”、类型为DWORD、数据为标准值的数值，若已存在则修改其数据。此数据的有效值为0-1。 |
| **基线符合性判定依据** | =0x0 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已禁用失效网关检测

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已禁用失效网关检测 |
| **安全基线项说明** | 当服务器设置了多个网关，在网络不通畅的时候系统会尝试连接第二个网关。允许自动探测失效网关可导致 DoS，关闭它可以抵御SNMP攻击，优化网络  为了提高系统的可用性，需要检查是否禁用失效网关检测 |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“EnableDeadGWDetect”、类型为DWORD、数据为标准值的数值，若已存在则修改其数据。此数据的有效值为0-1。如果不将该值设置为 0，攻击可能会强制服务器切换网关，而切换到的新网关可能并不是您打算使用的网关。 |
| **基线符合性判定依据** | =0x0 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置重传单独数据片段的次数

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查重传单独数据片段的次数 |
| **安全基线项说明** | 频繁的重传会加剧网络拥塞程度，所以为了提高系统的可用性，需要检查是否已正确配置重传单独数据片段次数。 |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“TcpMaxDataRetransmissions”、类型为DWORD、数据为标准值的数值，若已存在则修改其数据。此数据的有效值为0-65535。 |
| **基线符合性判定依据** | =0x2 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已禁用路由发现功能

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已禁用路由发现功能 |
| **安全基线项说明** | ICMP路由通告报文可以被用来增加路由表纪录，可能导致DOS攻击，所以为了提高系统的可用性，需要禁止路由发现 |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“PerformRouterDiscovery”、类型为DWORD、数据为标准值的数值，若已存在则修改其数据。此数据的有效值为0-1。0表示禁用此功能，1表示开启。“路由发现”请求路由信息以构建整个网络，如果开启此功能，系统会将此信息添加到路由表中。 |
| **基线符合性判定依据** | =0x0 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置TCP“连接存活时间”

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查TCP“连接存活时间” |
| **安全基线项说明** | 连接存活时间过长，会加剧网络拥塞程度，所以为了提高系统的可用性，需要检查是否已正确配置TCP“连接存活时间” |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“KeepAliveTime”、类型为DWORD、数据为标准值(注意：标准值是以毫秒为单位的)以内的数值，若已存在则修改其数据。此数据的有效值为1-0xFFFFFFFF。该值控制 TCP 通过发送“保持活动”的数据包来验证空闲连接仍然完好无损的频率。如果仍能连接到远程计算机，该计算机就会对“保持活动”的数据包作出应答。默认情况下，不发送“保持活动”的数据包。建议将该值设置为 300,000（5 分钟）。 |
| **基线符合性判定依据** | <=0x300000 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已启用并正确配置TCP碎片攻击保护

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已启用TCP最大传输单元(MTU)大小自动探测 |
| **安全基线项说明** | 如果有意发送总长度超过65535的IP碎片，一些老的系统内核在处理的时候就会出现问题，导致崩溃或者拒绝服务，所以为了提高系统的可用性，需要检查是否已正确配置TCP碎片攻击保护。 |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，添加名称为“EnablePMTUDiscovery”、类型为DWORD、数据为标准值的数值，若已存在则修改其数据。此数据的有效值为0-1，其中0表示不自动探测MTU大小，都使用576字节的MTU，1表示自动探测MTU大小。如果不将该值设置为 0，攻击者可能会强制 MTU 值变得非常小，从而导致堆栈的负荷过大。 |
| **基线符合性判定依据** | =0x0 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已删除SNMP服务的默认public团体

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已删除SNMP服务的默认public团体 |
| **安全基线项说明** | Snmp服务的默认public团体，黑客可以利用此默认团体进行信息收集。所以为了提高系统的保密性、可靠性，需要减产是否删除snmp服务的默认public团体。 |
| **检测操作步骤** | 打开命令提示符，运行命令“services.msc”打开服务管理器，在右边窗格中找到名称为“SNMP Service”的服务(若未找到则表示未安装SNMP服务，即合规)，停止此服务，或打开其属性对话框，切换到“安全”选项卡，删除public团体，或修改其名字。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

# 其他配置操作

## 检查是否已安装防病毒软件

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已安装防病毒软件 |
| **安全基线项说明** | 根据系统自身的情况决定是否安装防病毒软件，为了提高系统的可靠性，建议安装防病毒软件。 |
| **检测操作步骤** | 安装防病毒软件，并及时更新病毒库 |
| **基线符合性判定依据** | 安装防病毒软件，并及时更新病毒库 |
| **备注** | 等级：一般 / 评分：5 |

## 检查是否已启用并正确配置Windows自动更新

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查Windows自动更新设置级别 |
| **安全基线项说明** | 及时的安装系统补丁，可以提高系统的可靠性。 |
| **检测操作步骤** | 打开控制面板，找到“自动更新(Windows Update)”，配置为自动下载更新并安装。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已启用“不显示最后的用户名”策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已启用“不显示最后的用户名”策略 |
| **安全基线项说明** | 为了提高系统的保密性，需要减产是否已启用“不显示最后的用户名”策略。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“登录屏幕上不要显示上次登录的用户名”(适用于Windows2000)或“交互式登录: 不显示最后的用户名”，配置为“已启用”。。 |
| **基线符合性判定依据** | 已启用 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置“提示用户在密码过期之前进行更改”策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查“提示用户在密码过期之前进行更改”策略中配置的天数 |
| **安全基线项说明** | 为了提高系统的可靠性，需要检查是否已正确配置“提示用户在密码过期之后进行更改”策略 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“交互式登录: 提示用户在密码过期之前进行更改”或“交互式登录: 在密码到期前提示用户更改密码”，配置为不小于标准值(注意：标准值为16进制表示)的值。Windows2000中无此设置，不检查此项 |
| **基线符合性判定依据** | >=0xe |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已正确配置“锁定会话时显示用户信息”策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查“锁定会话时显示用户信息”级别 |
| **安全基线项说明** | 为了提高系统的保密性，在锁定会话时，系统不显示用户信息。 |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System”，添加名称为“DontDisplayLockedUserId”、类型为DWORD、数据为标准值的数值，若已存在则修改其数据。此数据的有效值为1-3，其中1表示显示名称、域名、用户名，2表示仅显示用户名称，3表示不显示用户信息。WindowsXP需要安装207399补丁才能生效；Windows2000没有此设置，不检查此项。 |
| **基线符合性判定依据** | =0x3。 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已禁用Windows硬盘默认共享

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已禁用Windows硬盘默认共享 |
| **安全基线项说明** | Windows 2000/XP/2003版本的操作系统提供了默认共享功能，如果服务器联网，那么网络上的任何人都可以通过共享盘，随意进入你的电脑。所以为了提高系统的保密性、可靠性，需要检查此项。 |
| **检测操作步骤** | 此项仅适用于非域环境。首先，打开命令提示符，运行命令“compmgmt.msc”打开计算机管理面板，浏览到路径“计算机管理(本地)\系统工具\共享文件夹\共享”，删除所有硬盘默认共享；然后，在命令提示符中运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\ Services\LanmanServer\Parameters\”，添加名称为“AutoShareServer”和“AutoShareWks”、类型为DWORD、数据为0的两个数值，若已存在则修改其数据。注意：若关闭C盘默认共享(C$)，将不能使用BVS的SMB扫描。 |
| **基线符合性判定依据** | 不包含$ |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已启用并正确配置屏幕保护程序

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已启用屏幕保护程序  检查屏幕保护程序等待时间  检查是否已启用“在恢复时显示登录界面 |
| **安全基线项说明** | 在无操作的一段时间内，系统开启屏幕保护程序。为了提高系统的保密性，需要检查此项。 |
| **检测操作步骤** | 在桌面空白处点击右键，打开属性(个性化)对话框(面板)，切换到“屏幕保护程序”选项卡(面板)，选择一个屏保程序，将等待时间配置为不大于标准值(注意：标准值是以秒为单位的)的值，且勾选“在恢复时需要密码保护(显示登录屏幕)”。 |
| **基线符合性判定依据** | 已启用  <=300  =1 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已启用并正确配置Windows网络时间同步服务(NTP)

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查Windows Time(W32Time)服务状态  检查时间服务器地址  检查Windows Time(W32Time)服务的启动类型 |
| **安全基线项说明** | 为了保证windows系统的时间同步，提高系统的可审计性，需要检查此项。 |
| **检测操作步骤** | 打开命令提示符，运行命令“services.msc”打开服务面板，在右边窗格中找到名称为“Windows Time”的服务，点击右键，“启动”此服务。  打开命令提示符，运行命令“timedate.cpl”打开“时间和日期属性”对话框，切换到“Internet时间”选项卡，勾选“与Internet时间服务器同步”，配置服务器地址为标准值之一。  打开命令提示符，运行命令“services.msc”打开服务面板，在右边窗格中找到名称为“Windows Time”的服务，点击右键，打开其属性对话框，配置“启动类型”为“自动”。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已关闭Windows自动播放

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已对所有驱动器关闭Windows自动播放 |
| **安全基线项说明** | 极客中通过把恶意代码写在U盘上，如果系统开启了自动播放功能，那么只要这些U盘插入在服务器上，该服务器就会感染到U盘上的病毒。所以为了提高系统的可靠性，需要检查此项。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\管理模板\Windows组件\自动播放策略”(适用于Windows2008、WindowsVista、Windows2008R2、Windows7)或“本地计算机策略\计算机配置\管理模板\系统”(适用于Windows2000、WindowsXP、Windows2003、Windows2003R2)，在右边窗格中找到“关闭/停用自动播放”，配置为“启用”，且选为对“所有驱动器”生效。 |
| **基线符合性判定依据** | 启用，对所有驱动器生效 |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已关闭不必要的服务-DHCP Client

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查DHCP Client服务状态 |
| **安全基线项说明** | DHCP Client服务如果没有必要使用的话，建议关闭该服务。攻击者可以伪造DHCP服务器，提供错误的信息给客户端的网卡。也可以伪造MAC地址，持续发送Discovery包，耗尽IP地址池。所以为了提高系统的可用性，需要检查此项。 |
| **检测操作步骤** | 打开命令提示符，运行命令“services.msc”打开服务管理器，停止显示名称为“DHCP Client”的服务。并禁用重启 |
| **基线符合性判定依据** | 关闭服务 |
| **备注** | 等级：可选 / 评分：1 |

## 检查系统是否已安装最新补丁包和补丁

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查系统是否已安装最新高危补丁  检查补丁包版本和系统版本 |
| **安全基线项说明** | 为了提高系统可靠性，需要安装最新补丁。 |
| **检测操作步骤** | 访问网页http://update.microsoft.com，按照提示安装补丁。  从微软官方下载最新补丁包安装，或开启自动更新安装最新补丁包。WindowsXP最新补丁包为SP3，Windows2003和Windows2003R2最新补丁包为SP2，WindowsVista和Windows2008为SP2，Windows7和Windows2008R2为SP1 |
| **基线符合性判定依据** |  |
| **备注** | 等级：一般 / 评分：5 |

## 检查是否已正确配置服务器在暂停会话前所需的空闲时间量

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查服务器在暂停会话前所需的空闲时间量 |
| **安全基线项说明** | 每个 SMB 会话会占用服务器资源，并且许多空会话会减慢服务器速度，或可能导致服务器失败。 攻击者可能会反复建立 SMB 会话，直到服务器的 SMB 服务变得缓慢或无响应。所以为了提高系统的可用性，需要检查此项。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“(Microsoft 网络服务器: )暂停(挂起、断开)会话前所需的空闲时间量”，配置为标准值(注意：标准值为16进制表示)。 |
| **基线符合性判定依据** | =0xf |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已启用“当登录时间用完时自动注销用户”策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已启用“当登录时间用完时自动注销用户”策略 |
| **安全基线项说明** | 为了提高系统的可靠性，在登录时间完成时自动注销用户。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“(Microsoft 网络服务器: ) 当登录时间用完时自动注销用户”(适用于Windows2000、WindowsXP、Windows2003、Windows2003R2)或“Microsoft 网络服务器: 登录时间过期后断开与客户端的连接”，配置为“已启用”。 |
| **基线符合性判定依据** | =0x1 |
| **备注** | 等级：可选 / 评分：1 |

## 域环境：检查是否已启用“需要域控制器身份验证以解锁工作站”策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已启用“需要域控制器身份验证以解锁工作站”策略 |
| **安全基线项说明** | 为了提高系统的可靠性，需要检查此项。 |
| **检测操作步骤** | 此项仅适用于域环境。打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“交互式登录: 需要(要求)域控制器身份验证以解锁(脱离)工作站”，配置为“已启用”。Windows2000中无此设置，不检查此项。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已禁用“登录时无须按 Ctrl+Alt+Del”策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已禁用“登录时无须按 Ctrl+Alt+Del”策略 |
| **安全基线项说明** | 为了提高系统的可用性，需要检查此项。 |
| **检测操作步骤** | 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“禁用按CTRL+ALT+DEL进行登录的设置”(适用于Windows2000)或“交互式登录: 无须(不需要)按 Ctrl+Alt+Del”，配置为“已禁用(停用)”。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

## 域环境：检查是否已正确配置“可被缓存保存的登录的个数”策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 域环境：检查是否已正确配置“可被缓存保存的登录的个数”策略 |
| **安全基线项说明** | 为了提高系统的可靠性，需要检查此项。 |
| **检测操作步骤** | 此项仅适用于域成员。打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“(交互式登录：)可被缓存保存的前次登录个数（在域控制器不可用的情况下）”或“交互式登录: 之前登录到缓存的次数(域控制器不可用时)”，配置为不大于标准值的值。非域成员主机的实际值将显示为0。 |
| **基线符合性判定依据** | <=5。 |
| **备注** | 等级：可选 / 评分：1 |

## 域环境：检查是否已正确配置域环境下安全通道数据的安全设置

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已启用“域环境下对安全通道数据进行数字加密或数字签名”策略  检查是否已启用“域环境下对安全通道数据进行数字签名”策略  检查是否已启用“域环境下对安全通道数据进行数字加密”策略 |
| **安全基线项说明** | 为了提高系统的保密性，需要检查此项。 |
| **检测操作步骤** | 此项仅适用于域成员。打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“域成员(安全通道):对安全通道数据进行数字加密或数字签名(始终)”，配置为“已启用”。  此项仅适用于域成员。打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“域成员(安全通道):对安全通道数据进行数字签名(如果可能)”，配置为“已启用”。  此项仅适用于域成员。打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“域成员(安全通道):对安全通道数据进行数字加密(如果可能)”，配置为“已启用”。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

## 域环境：检查是否已启用“域环境下需要强会话密钥”策略

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查是否已启用“域环境下需要强会话密钥”策略 |
| **安全基线项说明** | 为了提高系统的保密性，需要检查此项。 |
| **检测操作步骤** | 此项仅适用于域成员。打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows设置\安全设置\本地策略\安全选项”，在右边窗格中找到“域成员(安全通道): 需要使用强(Windows 2000 或更高版本)会话密钥”，配置为“已启用”。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

## 检查共享文件夹的权限设置是否安全

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查共享文件夹的共享权限 |
| **安全基线项说明** | 为了提高系统的保密性，需要检查此项。共享文件夹权限不应该是everyone权限。 |
| **检测操作步骤** | 此项不适用于域控服务器。打开命令提示符，运行命令“compmgmt.msc”打开计算机管理面板，浏览到路径“计算机管理(本地)\系统工具\共享文件夹\共享”，查看每个自定义共享文件夹的共享权限，若其中包含“Everyone(任何人)”，则将其删除。 |
| **基线符合性判定依据** | 不等于everyone |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已启用Windows数据执行保护(DEP)-需重启

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查当前Windows数据执行保护(DEP)等级 |
| **安全基线项说明** | 数据执行保护，可以防止代码在未经授权的特定内存区域中运行。所以为了提高系统的可靠性，需要检查此项。 |
| **检测操作步骤** | 打开控制面板，找到“系统”，打开“系统属性(高级系统设置)”，切换到“高级”选项卡下，点击“性能”中的“设置”按钮弹出“性能选项”对话框，切换到“数据执行保护”选项卡，勾选“仅为基本Windows程序和服务启用DEP”。更改此配置需要重启系统才能生效。在Windows2000、WindowsXP及其SP1上无此设置，不检查此项。 |
| **基线符合性判定依据** |  |
| **备注** | 等级：可选 / 评分：1 |

## 检查是否已禁止Windows自动登陆

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查Windows自动登录设置 |
| **安全基线项说明** | 为了提高系统的保密性、可靠性，需要检查此项。Windows不可自动登陆 |
| **检测操作步骤** | 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon”，将名称为“AutoAdminLogon”的数值修改为0。 |
| **基线符合性判定依据** | =0 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否已关闭不必要的服务-Simple TCP/IP Services

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查Simple TCP/IP Services服务状态 |
| **安全基线项说明** | 建议关闭不必要的服务，Simple TCP/IP内包含chargen(字节生成器协议)  该协议具有拒绝服务漏洞。所以为了提高系统的可用性，需要检查此项。 |
| **检测操作步骤** | 打开命令提示符，运行命令“services.msc”打开服务管理器，停止显示名称为“Simple TCP/IP Services”或“简单 TCP/IP 服务”的服务。 |
| **基线符合性判定依据** | 关闭服务 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否已关闭不必要的服务-Simple Mail Transport Protocol (SMTP)

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查Simple Mail Transport Protocol (SMTP)服务状态 |
| **安全基线项说明** | Smtp为邮件协议，默认端口25。经常被用来邮箱伪造、钓鱼攻击等。所以为了提高系统的可靠性，需要检查此项。 |
| **检测操作步骤** | 打开命令提示符，运行命令“services.msc”打开服务管理器，停止显示名称为“Simple Mail Transport Protocol (SMTP)”的服务。 |
| **基线符合性判定依据** | 关闭服务 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否已关闭不必要的服务-Windows Internet Name Service (WINS)

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查Windows Internet Name Service (WINS)服务状态 |
| **安全基线项说明** | Wins服务中的漏洞可能存在允许远程执行代码漏洞，所以为了提高系统的可靠性，需要检查此项。 |
| **检测操作步骤** | 打开命令提示符，运行命令“services.msc”打开服务管理器，停止显示名称为“Windows Internet Name Service (WINS)”或“WINS”的服务。 |
| **基线符合性判定依据** | 关闭服务 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否已关闭不必要的服务-DHCP Server

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查DHCP Server服务状态 |
| **安全基线项说明** | 具有一些安全问题，如DHCP服务欺骗攻击等。所以为了提高系统的可靠性，需要检查此项。 |
| **检测操作步骤** | 打开命令提示符，运行命令“services.msc”打开服务管理器，停止显示名称为“DHCP Server”的服务。 |
| **基线符合性判定依据** | 服务关闭 |
| **备注** | 等级：重要 / 评分：7 |

## 检查是否已关闭不必要的服务-Message Queuing

|  |  |
| --- | --- |
| **安全基线项目名称** | 检查Message Queuing服务状态 |
| **安全基线项说明** | Windows消息队列服务MSMQ中存在过权限提升的漏洞，所以为了提高系统的可靠性，需要检查此项。 |
| **检测操作步骤** | 打开命令提示符，运行命令“services.msc”打开服务管理器，停止显示名称为“Message Queuing”的服务。 |
| **基线符合性判定依据** | 服务关闭 |
| **备注** | 等级：重要 / 评分：7 |