

“护网 2019” 防守应对手册

一、边界安全

各单位应通过硬件防火墙设备对外部用户访问单位内部网络的数据，进行过滤或阻断，禁止外部用户访问单位内部未授权的网络或机器，保障外部用户只能够访问单位已授权访问的指定服务等资源，例如：网站、邮件等信息。

检查手段：

1、各单位安排安全运维人员，检查网络防火墙配置信息，确认对互联网用户开放的端口是否为业务所需端口，取消无需开放或不必要开放的业务端口。

2、使用 scanport 工具对单位的互联网访问地址进行端口扫描，确认互联网地址仅开放了单位所需的服务。（工具使用方法见附件一）

二、通信安全

各单位对外提供服务的网站、邮件等应用应采用安全的通信协议(例如网站配置 HTTPS 协议)，防止应用通信过程中的数据被窃听或篡改。

检查手段：

1、各单位安排安全运维人员，检查对外开放的网站、邮箱是否配置 HTTPS 协议，并将未配置 HTTPS 的网站或邮件

设置 HTTPS 协议，同时禁止 HTTP 协议访问或将 HTTP 访问自动跳转到 HTTPS 协议。（HTTPS 配置方法见附件二）

三、应用安全

各单位应自行或通过安全服务商对已开放互联网访问的应用进行漏洞扫描、渗透测试等安全检测，及时修复漏洞（中危及以上的漏洞必须修复），避免外部用户通过漏洞对单位应用进行攻击或破坏。

检查手段：

1、有签约网络安全服务商的单位可安排网络安全服务商对单位开放互联网的应用进行漏洞扫描、渗透测试等安全检测，并根据检测报告对漏洞进行修复。

2、无签约网络安全服务商的单位可先自主下载免费漏洞扫描软件对单位开放互联网的应用进行漏洞扫描，并根据漏洞扫描报告对漏洞进行修复。后续委托网络安全服务商开展渗透测试工作。（漏洞扫描工具推荐使用 OPENVAS 或 NESSUS，安装及使用方法见官方使用说明）

四、主机安全

各单位应通过在服务器上部署杀毒软件，关闭不必要的系统服务、删除或禁用不必要的系统用户、修改密码为 8 位以上符合复杂度要求的密码等手段加强主机服务器安全性，及时更新补丁，避免服务器被非法攻击利用。

检查手段：

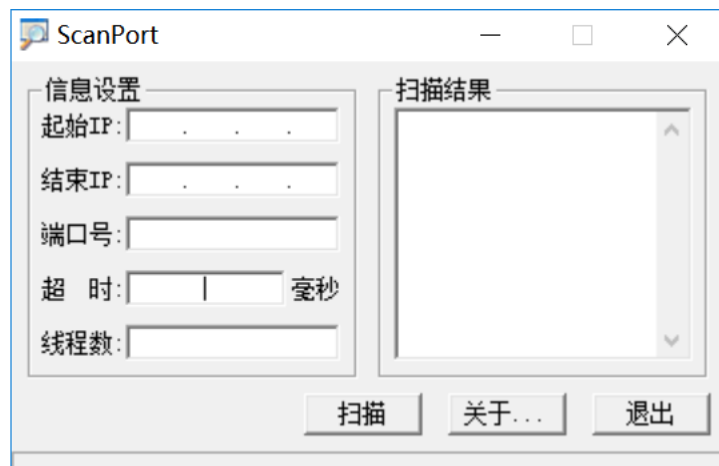
1、有签约网络安全服务商的单位可安排网络安全服务商对单位服务器进行安全检查和加固；

2、无签约网络安全服务商的单位可自主进行服务器安全检查和加固。（主机安全要求及检查步骤见附件三）

附件一

端口扫描配置说明

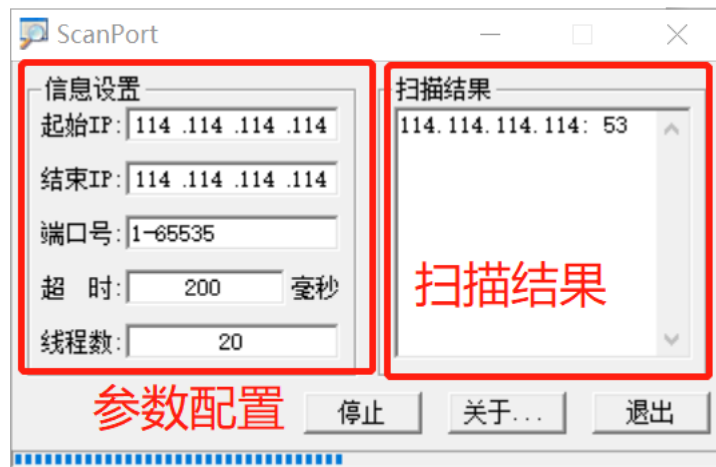
1: 打开 tools 中的 scanport.exe，启动后见下图：



2: 配置扫描参数

- 起始结束 IP 设置：单位的互联网 IP 地址，例如：
114.114.114.XXX，如单位仅有一个对外的 IP 地址，则起始、结束 IP 相同。如单位存在多个连续的互联网 IP 地址（例如：1.1.1.1 \ 1.1.1.2），则起始 IP 为：1.1.1.1，结束 IP 为：1.1.1.2
- 端口号设置：可设置为 1-65535
- 超时设置：200 毫秒
- 线程数设置：

3: 点击扫描，扫描结果见右侧



附件二：

HTTPS 配置方法

因各单位使用的软件不同，则配置方法也不相同，本手册仅提供常见 WEB 软件配置 HTTPS 的文件供参考：

1、apache 配置 HTTPS

<http://httpd.apache.org/docs/2.2/ssl/>

<https://www.cnblogs.com/liaojiafa/p/6028816.html>

<https://baijiahao.baidu.com/s?id=1612174952822431928&wfr=spider&for=pc>

2、nginx 配置 HTTPS

<https://www.cnblogs.com/bincoding/p/6118270.html>

<https://blog.csdn.net/duyusean/article/details/79348613>

3、IIS 配置 HTTPS

<https://jingyan.baidu.com/article/eb9f7b6d7f83b6869364e8a9.html>

附件三：

主机检查及配置

■ Windows 配置项清单

1、重命名管理员及来宾账号
2、禁用 guest 账号
3、更改默认远程桌面 3389 端口
4、禁用不必要的操作系统账号和服务
5、检查系统是否有未安装的安全补丁
6、删除系统默认的文件共享
7、安装杀毒软件并检查病毒库更新日期
8、开启密码复杂性要求及账号锁定策略
9、启用不显示最后登录用户名
10、开启操作系统审核策略

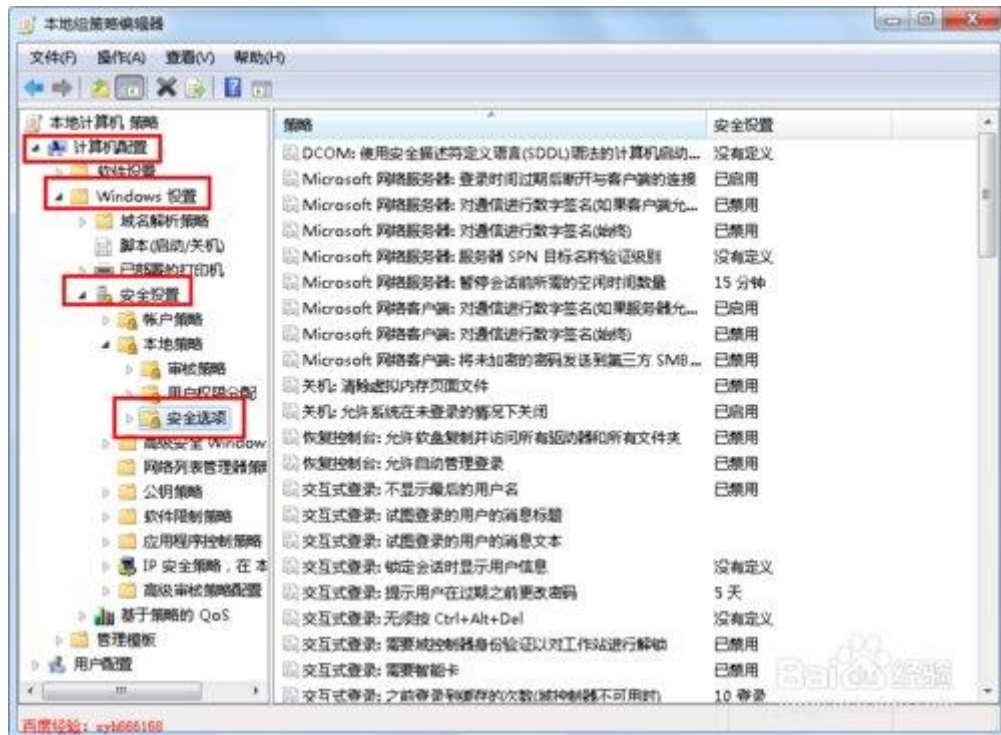
➤ 重命名管理员账号步骤

- 1、在程序中找到“运行”，打开运行窗口，或者键盘“windows”+“R”
- 2、输入 gpedit.msc, 之后回车或点击下面的确定打开 gpedit.msc（组策略工具）

3、点击本地计算机策略下面点击打开:计算机配置

-----windows 设置-----安全设置-----本地策略-----

安全选项



4、找到找到“账户:重命名系统管理员账户”，然后在上面点右键，之后在弹出菜单中选择属性

5、将输入框里面的 Administrator 修改为自己要改的用户名，然后点右下角的应用和确定按钮，就可以将系统默认的 Administrator 改为自己的用户名了。

6、找到找到“账户:重命名来宾账户”，然后在上面点右键，之后在弹出菜单中选择属性

7、将输入框里面的 Guest 修改为自己要改的用户名，然后点右下角的应用和确定按钮，就可以将系统默认的 Guest 改为自己的用户名了。

➤ 禁用来宾账号步骤

- 1、打开该系统的“开始”菜单，从中依次点选“程序”/“管理工具”命令，在弹出的系统管理工具列表中，双击“计算机管理”图标，打开对应系统的计算机管理窗口；
- 2、其次在该管理窗口的左侧显示区域，用鼠标依次展开“系统工具”/“本地用户和组”/“用户”分支选项，在对应“用户”分支选项的右侧显示区域，双击 guest 帐户图标。
- 3、勾选账号已禁用，并点击确定。



➤ 更改默认远程桌面 3389 端口

- 1、在程序中找到“运行”，打开运行窗口，或者键盘“windows”+“R”，输入 regedit 命令，打开注册表编辑器

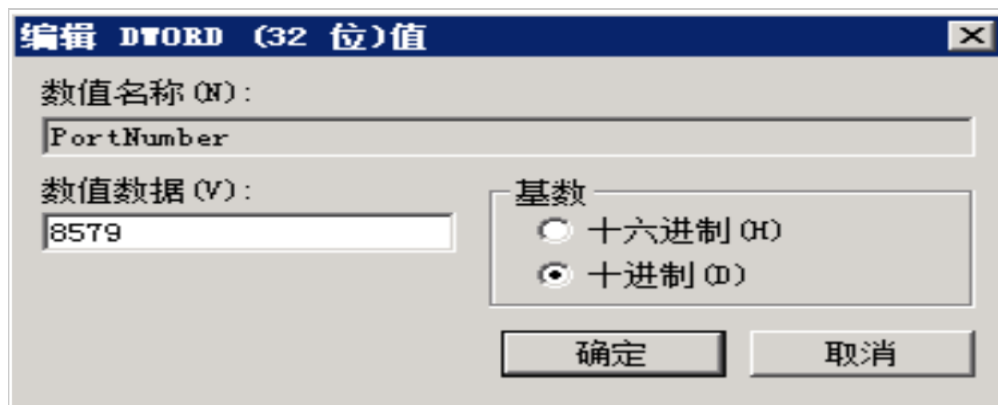
2、进入

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]，右侧找到 PortNumber，双击，默认显示的是十六进制数据 d3d，点击选择十进制后变为 3389。

3、修改 3389 为您需要的端口，例如：8579

4、再进入

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]，修改 PortNumber 的值为 8579，保存并关闭注册表。

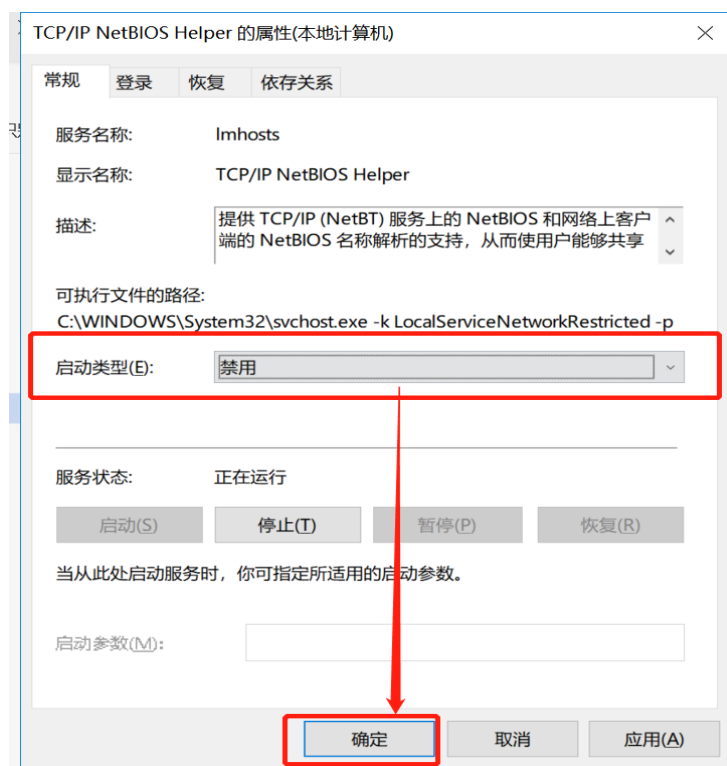


注：如果系统自带防火墙处于开启状态，则需把修改后的远程端口设置允许入站，否则将无法连接远程桌面。

➤ 禁用不必要的操作系统账号和服务

因不同业务依赖的系统服务不同，禁用服务前需确认系统或业务应用是否依赖该服务，本文不提供需要关闭的服务列表，请各单位根据实际情况而定。

- 1、在程序中找到“运行”，打开运行窗口，或者键盘“windows”+“R”，输入 services.msc 命令，打开系统服务管理器
- 2、找到需要禁用的服务，点击右键/属性，在弹出的属性框中，将启动类型设置为“禁用”。



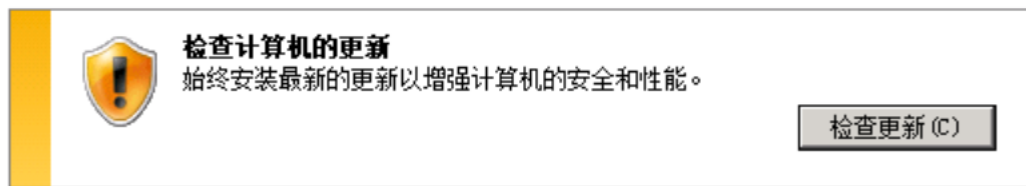
- 3、打开该系统的“开始”菜单，从中依次点选“程序”/“管理工具”命令，在弹出的系统管理工具列表中，双击“计算机管理”图标，打开对应系统的计算机管理窗口；
- 4、禁用不需要的账号操作参考禁用来宾账号操作。

➤ 检查系统是否有未安装的安全补丁

1、打开 windows 控制面板, 双击 windows update, 打开系统补丁更新管理器。

2、点击“检查更新”，查看是否存在未安装的安全补丁。

Windows Update



最近检查更新的时间: 昨天 19:47
安装更新的时间: 2016/5/9 14:56。 [查看更新历史记录](#)
接收更新: 适用于 Windows 产品和其他来自 Microsoft Update 的产品

3、如存在未安装的安全补丁，则点击安全更新

Windows Update



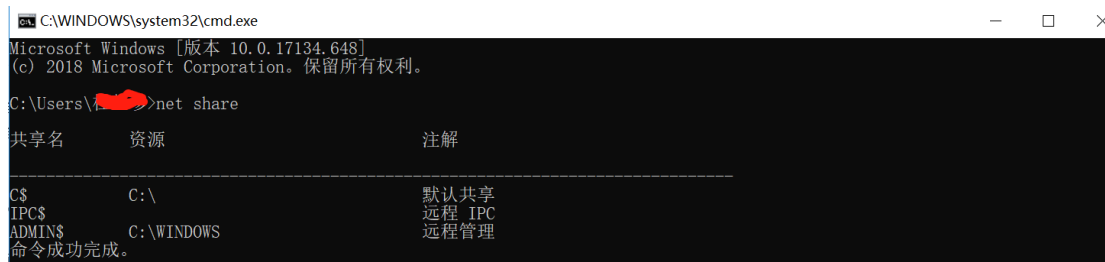
最近检查更新的时间: 今天 0:38
安装更新的时间: 2016/5/9 14:56。 [查看更新历史记录](#)
接收更新: 适用于 Windows 产品和其他来自 Microsoft Update 的产品

4、安装完成后，根据系统要求，重启系统。

➤ 删除系统默认的文件共享

1、在程序中找到“运行”，打开运行窗口，或者键盘“windows”+“R”，输入 cmd 命令。

2、在 cmd 窗口中输入 net share 命令，查看存在的默认共享



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.17134.648]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\<redacted>>net share

共享名      资源      注解
-----
C$          C:\       默认共享
IPC$        C:\       远程 IPC
ADMIN$      C:\WINDOWS 远程管理
命令成功完成。
```

3、在 cmd 窗口中输入 net share “共享名” /del 删除默认共享，例如：

```
net share c$ /del
```

```
net share ipc$ /del
```

```
net share admin$ /del
```

注：上述方法为临时删除默认共享，如想每次开机后自动删除默认共享，只需把上面的命令保存为.bat 文件，开机自动运行就可以了。

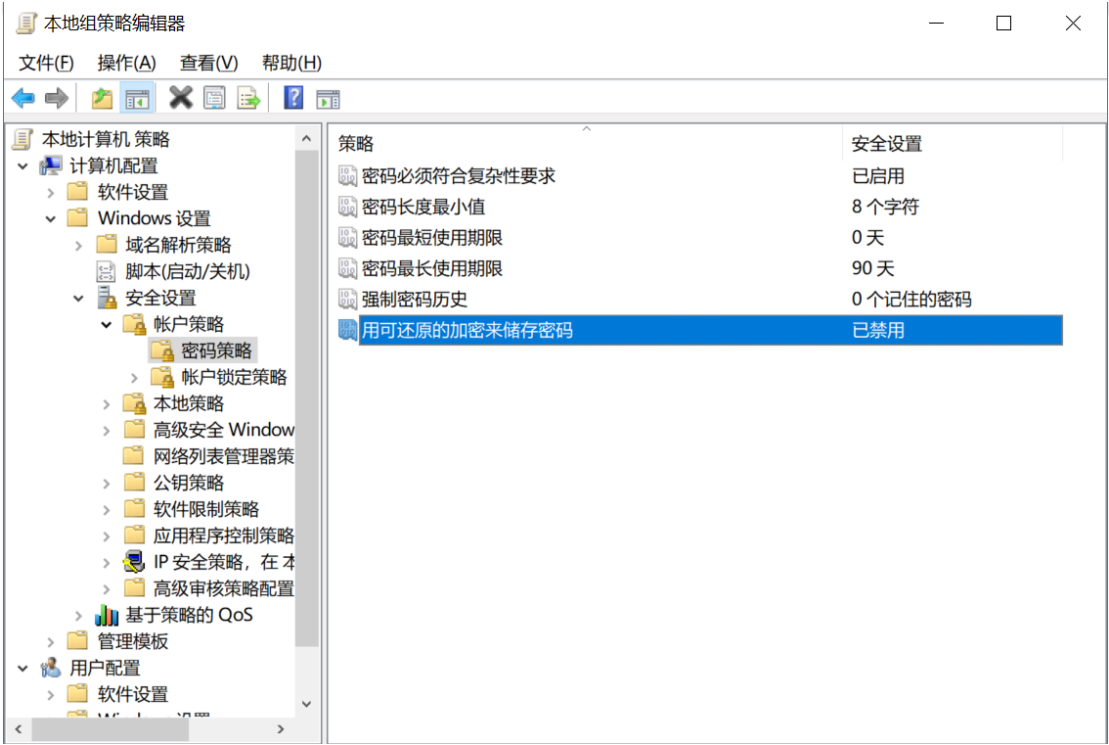
➤ 开启密码复杂性要求及账号锁定策略

1、在程序中找到“运行”，打开运行窗口，或者键盘“windows”+“R”

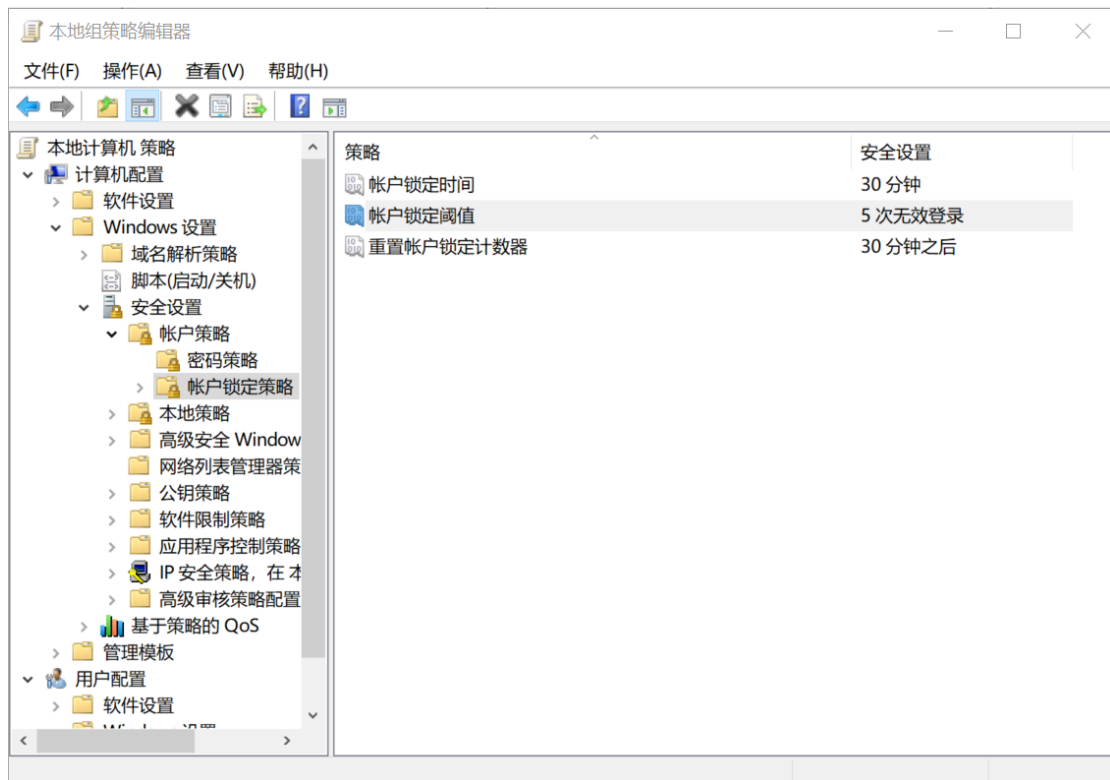
2、输入 gpedit.msc, 之后回车或点击下面的确定打开 gpedit.msc（组策略工具）

3、点击本地计算机策略下面点击打开：计算机配置
\\windows 设置\\安全设置\\账户策略\\密码策略

4、设置复杂度要求为已启用、密码最小长度 8、密码最长使用期限 90

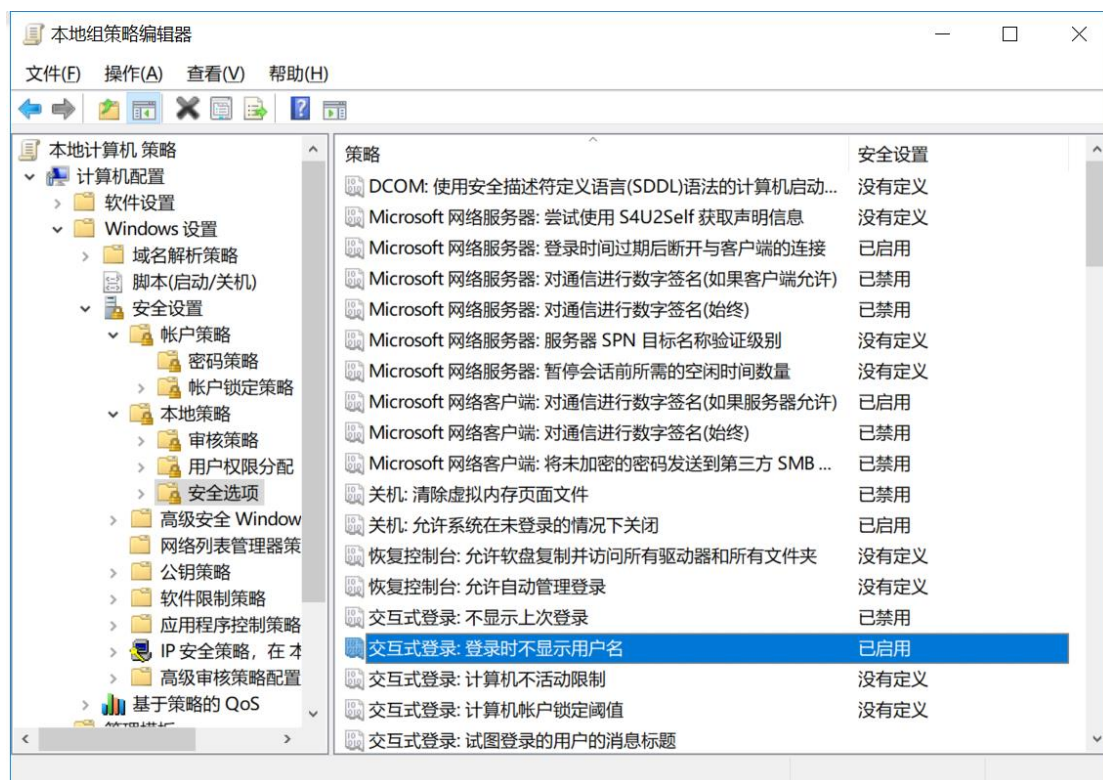


5、点击本地计算机策略下面点击打开:计算机配置
\\windows 设置\\安全设置\\账户策略\\账户锁定策略，设置
账户锁定时间为 30 分钟，锁定阈值为 5 次，重置账户锁定
计数器为 30 分钟



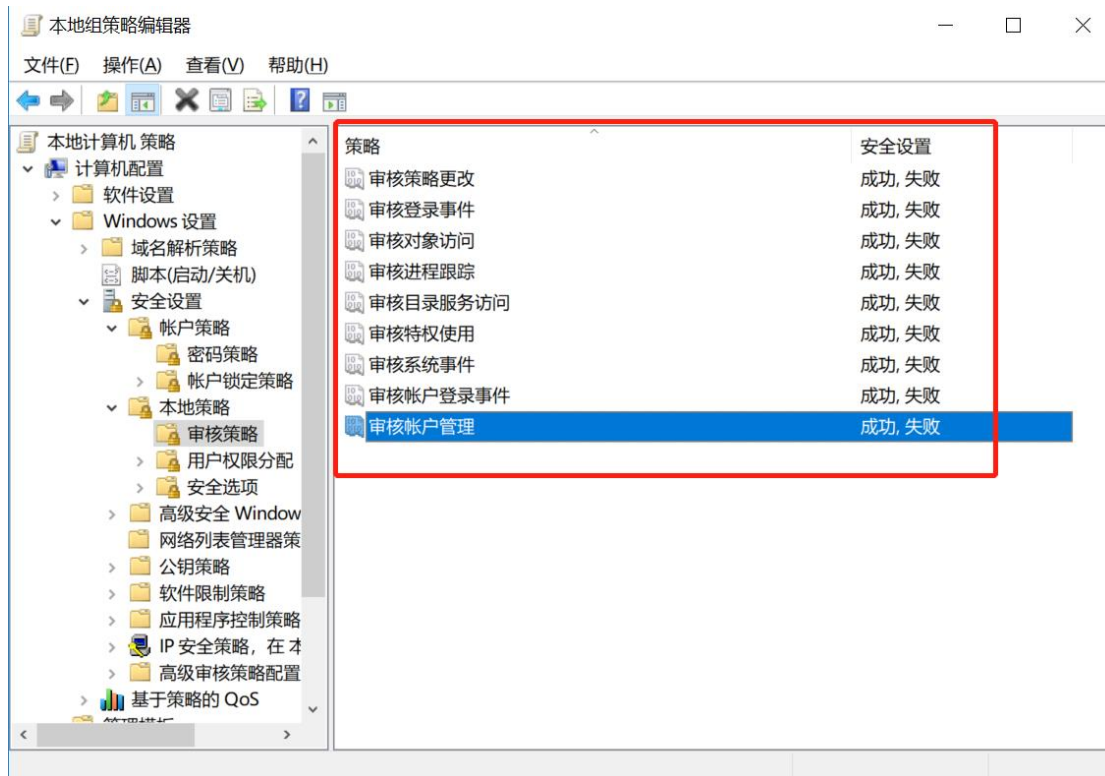
➤ 启用不显示最后登录用户名

- 1、在程序中找到“运行”，打开运行窗口，或者键盘“windows”+“R”
- 2、输入 gpedit.msc, 之后回车或点击下面的确定打开 gpedit.msc（组策略工具）
- 3、点击本地计算机策略下面点击打开:计算机配置
\\windows 设置\\安全设置\\本地策略\\安全选项
- 4、找到交互式登录: 登录时不显示用户名, 并设置为启用。



➤ 开启操作系统审核策略

- 1、在程序中找到“运行”，打开运行窗口，或者键盘“windows”+“R”
- 2、输入 gpedit.msc, 之后回车或点击下面的确定打开 gpedit.msc（组策略工具）
- 3、点击本地计算机策略下面点击打开: 计算机配置
\windows 设置\安全设置\本地策略\审核策略
- 4、将右侧审计项全部设置为审核成功和失败。



■ Linux 配置项清单

- 1、更改 SSH 服务默认端口
- 2、禁止 ROOT 用户远程登录
- 3、禁用不必要的服务或账号
- 4、设置账号密码安全策略
- 5、设置系统会话超时时间

➤ 更改 SSH 服务默认端口

- 1、打开 SSH 配置文件 (vi /etc/ssh/sshd_config) ,
- 2、修改 PORT 的值为您需要的端口，例如：22222

```
# If you want to change the port on a
# SELinux about this change.
# semanage port -a -t ssh_port_t -p t
#
Port 22222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

➤ 禁止 ROOT 用户远程登录

- 1、打开 SSH 配置文件（vi /etc/ssh/sshd_config），
- 2、修改 PermitRootLogin 的值为 no

```
# Authentication:
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

- 3、重启 SSH 服务（service sshd restart）

➤ 禁用不必要的服务或账号

因不同业务依赖的系统服务不同，禁用服务前需确认系统或业务应用是否依赖该服务，本文不提供需要关闭的服务列表，请各单位根据实际情况而定。

- 1、查看系统服务列表（chkconfig --list）
- 2、停止不必要的服务（例如：service telnet stop）

- 3、禁止不必要的服务开启启动（例如：`chkconfig telnet off`）
- 4、查看系统账号列表（`cat /etc/passwd`）
- 5、删除或锁定不必要的账号（例如：`userdel telnet` 或 `usermod -L telnet`）

➤ 设置账号密码安全策略

- 1、修改系统配置文件（`vi /etc/login.defs`）
- 2、将 `PASS_MIN_LEN` 的值修改为 8（密码最小长度 8 位）
- 3、将 `PASS_MAX_DAYS` 的值修改为 90,（密码最长使用期限）
- 4、将 `PASS_WARN_AGE` 的值修改为 7,（设置过期提前警告天数）
- 5、保存并退出编辑
- 6、设置账户登录错误锁定策略（`vi /etc/pam.d/system-auth`），加入：
`auth required pam_tally.so onerr=fail deny=6
unlock_time=300`
- 7、保存并退出编辑

➤ 设置系统会话超时自动断开

- 1、修改系统配置文件（`vi /etc/profile`）

2、修改会增加 TMOUT=180 配置项（3 分钟无操作自动退出）

3、保存并退出编辑

4、重新加载 profile 文件（source /etc/profile）