Windows 账户管理和认证授权

1、账户

1.1 默认账户安全

a. 禁用 Guest 账户。

b. 禁用或删除其他无用账户（建议先禁用账户三个月，待确认没有问题后删除。）

思考：

a、为什么要禁用 Guest 用户?

Guest 账户为临时账户，但是该账户允许用户登录到网络、浏览 internet 以及关闭计算机。黑客可以通过 guest 用户提权到 administrator 组得到管理员权限，进行后渗透。

b、为什么禁用或删除其他无用账户?

防止提权

c、为什么建议先禁用账户三个月，待确认没有问题后删除?

因为直接删除，有些正常用户就无法使用了，为了避免影响业务所以先禁用三个月，在三个月之内需要使用的用户发现异常会联系你，也就知道哪些是正常用户哪些该用户该删除。

操作步骤

打开 控制面板 > 管理工具 > 计算机管理，在 系统工具 > 本地用户和组 > 用户 中，双击 Guest 帐户，在属性中选中 帐户已禁用，单击 确定。

1.2 按照用户分配帐户

按照用户分配帐户。根据业务要求，设定不同的用户和用户组。例如，管理员用户，数据库用户，审计用户，来宾用户等。

思考：

主要是为了最小权限分配，防止用户的权限过大，查看了不属于自己权限的内容。

操作步骤

打开 控制面板 > 管理工具 > 计算机管理，在 系统工具 > 本地用户和组 中，根据您的业务要求设定不同的用户和用户组，包括管理员用户、数据库用户、审计用户、来宾用户等。

1.3 定期检查并删除与无关帐户

定期删除或锁定与设备运行、维护等与工作无关的帐户。

操作步骤

打开 控制面板 > 管理工具 > 计算机管理，在 系统工具 > 本地用户和组 中，删除或锁定与设备运行、维护等与工作无关的帐户。

1.4 不显示最后的用户名

配置登录登出后，不显示用户名称。

思考:

因为如果显示登录名，就让别人知道了你账户，可以尝试进行暴力破解。

操作步骤:

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 安全选项 中，双击 交互式登录:不显示最后的用户名，选择 已启用 并单击 确定。

2、口令

2.1 密码复杂度

思考:

理论上来说，任何密码都是可以被破解的，但是密码越复杂，破解的时间长度等攻击成本是黑客所承受不了的，所以越复杂越安全。

密码复杂度要求必须满足以下策略:

a. 最短密码长度要求八个字符。

b. 启用本机组策略中密码必须符合复杂性要求的策略。

即密码至少包含以下四种类别的字符中的两种:

- ✓ 英语大写字母 A, B, C, … Z
- ✓ 英语小写字母 a, b, c, … z
- ✓ 西方阿拉伯数字 0, 1, 2, … 9
- ✓ 非字母数字字符，如标点符号，@, #, $, %, &, *等

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 帐户策略 > 密码策略 中，确认 密码必须符合复杂性要求 策略已启用。

2.2 密码最长留存期

对于采用静态口令认证技术的设备，帐户口令的留存期不应长于 90 天。

思考：

静态口令认证技术，也就是说你的账户密码一直不变，那么如果你在某一个时间不小心泄露了密码，在 90 天之内也会更改密码，所以在一定程度上来说使你的账户密码更安全。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 帐户策略 > 密码策略 中，配置 密码最长使用期限 不大于 90 天。

2.3 帐户锁定策略

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 10 次后，锁定该用户使用的帐户。

思考：

用户连续认证失败次数超过 5 次，很可能就是别人使用暴力破解，所以锁定账户就禁止了别人继续对该账户进行暴力破解。

操作步骤

打开 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 中，配置 帐户锁定阈值 不大于 10 次。

3、授权

3.1 远程关机

在本地安全设置中，从远端系统强制关机权限只分配给 Administrators 组。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 用户权限分配 中，配置 从远端系统强制关机 权限只分配给 Administrators 组。

3.2 本地关机

在本地安全设置中关闭系统权限只分配给 Administrators 组。

思考：

主要是为了防范一些客户误操作，或者说黑客进行攻击以后拿到临时账号，进行关闭系统影响业务正常。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 用户权限分配 中，配置 关闭系统 权限只分配给 Administrators 组。

3.3 用户权限指派

在本地安全设置中，取得文件或其它对象的所有权权限只分配给 Administrators 组。

思考：

这个目的是为了防止别的用户组进行越权获得其他对象的权限。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 用户权限分配 中，配置 取得文件或其它对象的所有权 权限只分配给 Administrators 组。

3.4 授权帐户登录

在本地安全设置中，配置指定授权用户允许本地登录此计算机。

思考：

对能进行本地登录此计算机的用户进行限制

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 用户权限分配 中，配置 允许本地登录 权限给指定授权用户。

3.5 授权帐户从网络访问

在本地安全设置中，只允许授权帐号从网络访问（包括网络共享等，但不包括终端服务）此计算机。

思考：

和上一步应该一起使用，一个是限制本地登录账户一个是限制只能从网络访问，配合起来就限制了什么账户只能以什么样的方式进行登录，如果黑客通过获取了你的 user 账户进行提权到管理员，那么得从本地才能登录，在一定程度上限制了攻击得难度。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 用户权限分配 中，配置 从网络访问此计算机 权限给指定授权用户。