Linux 账户口令安全加固

为了响应等保三级。需要在 Linux 服务器上启用账号密码安全策略。更好的加强服务器的安全性。

具体做法如下：

一、准备工作

安装 PAM 的 cracklib 模块，cracklib 能提供额外的密码检查能力。

Debian、Ubuntu 或 Linux Mint 系统上：

```
$ sudo apt-get install libpam-cracklib
```

CentOS、Fedora、RHEL 系统已经默认安装了 cracklib PAM 模块，所以在这些系统上无需执行上面的操作。

为了强制实施密码策略，我们需要修改 /etc/pam.d 目录下的 PAM 配置文件。一旦修改，策略会马上生效。

注意：此教程中的密码策略只对非 root 用户有效，对 root 用户无效。

二、禁止使用旧密码

找到同时有 “password” 和 “pam_unix.so” 字段并且附加有 “remember=5” 的那行，它表示禁止使用最近用过的 5 个密码(已使用过的密码会被保存在 /etc/security/opasswd 下面)。

Debian、Ubuntu 或 Linux Mint 系统上：

```
$ sudo vi /etc/pam.d/common-password
```

```
password [success=1 default=ignore] pam_unix.so obscure sha512 remember=5
```

CentOS、Fedora、RHEL 系统上：

$ sudo vi /etc/pam.d/system-auth

password sufficient pamunix.so sha512 shadow nullok tryfirstpass useauthtok remember=5

三、设置最短密码长度

找到同时有 “password” 和 “pam_cracklib.so” 字段并且附加有 “minlen=10” 的那行，它表示最小密码长度为（10 - 类型数量）。这里的 “类型数量” 表示不同的字符类型数量。PAM 提供 4 种类型符号作为密码（大写字母、小写字母、数字和标点符号）。如果你的密码同时用上了这 4 种类型的符号，并且你的 minlen 设为 10，那么最短的密码长度允许是 6 个字符。

Debian、Ubuntu 或 Linux Mint 系统上：

$ sudo vi /etc/pam.d/common-password

password requisite pam_cracklib.so retry=3 minlen=10 difok=3

CentOS、Fedora、RHEL 系统上：

$ sudo vi /etc/pam.d/system-auth

password requisite pam_cracklib.so retry=3 difok=3 minlen=10

四、设置密码复杂度

找到同时有 “password” 和 “pam_cracklib.so” 字段并且附加有 “ucredit=-1 lcredit=-2 dcredit=-1 ocredit=-1” 的那行，它表示密码必须至少包含一个大写字母（ucredit），两个小写字母（lcredit），一个数字（dcredit）和一个标点符号（ocredit）。

Debian、Ubuntu 或 Linux Mint 系统上：

$ sudo vi /etc/pam.d/common-password

password requisite pam_cracklib.so retry=3 minlen=10 difok=3 ucredit=-1 lcredit=-2 dcredit=-1 ocredit=-1

CentOS、Fedora、RHEL 系统上：

$ sudo vi /etc/pam.d/system-auth

password requisite pam_cracklib.so retry=3 difok=3 minlen=10 ucredit=-1 lcredit=-2 dcredit=-1 ocredit=-1

五、设置密码过期期限

编辑 /etc/login.defs 文件，可以设置当前密码的有效期限，具体变量如下所示：

$ sudo vi /etc/login.defs

PASSMAXDAYS 150 PASSMINDAYS 0 PASSWARNAGE 7

这些设置要求用户每 6 个月改变他们的密码，并且会提前 7 天提醒用户密码快到期了。

如果你想为每个用户设置不同的密码期限，使用 chage 命令。下面的命令可以查看某个用户的密码限期：

$ sudo chage -l xmodulo

Last password change : Dec 30, 2013 Password expires : never Password inactive : never Account expires : never Minimum number of days between password change : 0 Maximum number of days between password change : 99999 Number of days of warning before password expires : 7

默认情况下，用户的密码永不过期。

下面的命令用于修改 xmodulo 用户的密码期限：