# 聊聊弱口令的危害（二）——安全小课堂第十九期

京东安全应急响应中心 2016-07-22

安全小课堂第十九期

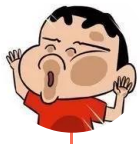
打个比方，你有一个保险柜,里面有几千万人民币现金,而口令则是进入保险柜的钥匙,当别人也有一把这样的钥匙...因为弱口令很容易被他人猜到或破解，所以如果你使用弱口令，就相当于把家门的锁是很老旧,拿个铁丝就可以打开，这是相当危险的。本期我们继续来聊一聊弱口令的危害。

本期邀请到
唯品会安全专家cookie
新浪安全专家吗啡
大家欢迎~

1

豌豆妹

白驹过隙，又见周五。本期我们继续来聊一聊弱口令的危害。 请问如何发现弱口令的存在呢？

小新 

内部方面，在系统上线前弱口令扫描；外部方面，应急响应接收。现在大多数公司都在这么做，现在网上的字典也是很强大的，企业在做安全的时候，主要是担心暴露在外网业务的弱口令。现在企业内外网隔离做的比较好的话，mysql、ssh、redis和mongodb的弱口令被扫到的话会少一点。

哆啦A梦 

扫描是一方面，别人扫，你能不能识别；识别之后做什么，这些都是要结合具体公司，具体业务来说的，有时候你在web日志上加了个监控，结果人家直接从pop或者imap上扫，所以监控取的点在哪里，从哪里监控；从哪几个点监控，也都是要综合考虑业务量，性能，机器处理能力，日志详细程度，受威胁程度来考虑的。

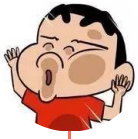
2

豌豆妹

如何防范弱口令呢？

葫芦娃 

比方说供应商的订单系统，这种由于供应商的用户没有相关安全意识，他们的密码设置通常不会复杂。 所以，经常会出现供应商的账户泄露，导致订单泄露这种情况。 防范弱口令的话，虽然说安全意识很重要，但是这种无法把控，我觉得防范弱口令主要还是得系统有强制的密码策略。不允许用户设置简单密码，这样以来，弱口令出现的概率就小了很多。

小新 

监控发现能力也很重要，另外为了防止暴力破解，还得定期修改密码。从技术层面考虑，可以开启认证。当然了，认证方式不能只局限在记住密码上，比如什么声纹鉴定、人脸识别、指纹识别，还可以双因子认证，完全可以把这些可用的多因素认证加进来。

豌豆妹

登陆SSH 能人脸指纹嘛？

小新

当然可以了，self path pam，又不是没做过。输入密码之后，pam会连接到我们的二次认证服务器，然后需要用户自己打开二次认证服务器的页面做二次识别，在web上做人脸、声纹虽然不流行，但是技术上是可行的，动态口令也是一个很典型的低成本的otp，otp和双因素不是一个维度上的概念，但是都可以用来缓解传统的密码问题。

3

豌豆妹

能甩一个被利用引发的惨案么~

小丸子

出现比较多的弱口令血案应该是在一些web应用上。

葫芦娃

我就截个图吧。（截图来自WooYun）


4

豌豆妹

如何方便记忆强口令呢？

葫芦娃

使用相对安全的口令，防止口令被穷举或字典法猜出，还应加强口令安全。主要措施如下：

(1)口令长度不小于8位，并应包含字母，数字和其他字符，并且不包含全部或部分的用户账号名；

(2)避免使用英文单词、生日、姓名、电话号码或这些信息的简单组合作为口令；

(3)不要在不同的系统上使用相同的口令；

(4)定期或不定期地修改口令；

(5)使用口令设置工具生成健壮的口令；

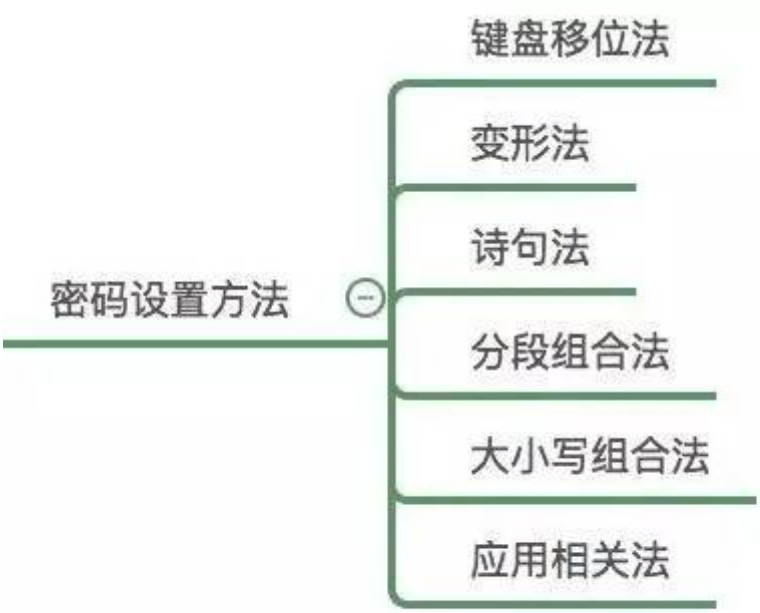
(6)对用户设置的口令进行检测，及时发现弱口令；

(7)限制某些网络服务的登录次数，防止远程猜测、字典法、穷举法等攻击。

另外还需加强员工安全意识培训，登陆口令，如系统/管理后台等最好升级为双因子认证方式。

哆啦A梦

以前学过一个联想记忆法，例如：fX1t$13Lx$$xY13y，解析：飞雪连天射白鹿，笑书神侠倚碧鸳；给你们一个，J1N9d0n9$eCg0od，解析：京东安全好；还可以用凯撒密码法(向右移动三位)，你可以键盘移一位，如:password，变形为P4$$w0rD，你再变一下 [5^^e-tf。




豌豆妹

好嘞~谢谢大家对这一话题的积极关注哟~下期见！

安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当；
7、XSS之攻击与防御；
8、电商和O2O行业诈骗那些事儿（上）；
9、电商和O2O行业诈骗那些事儿（下）；
10、CSRF的攻击与防御；
11、账户体系安全管理探讨；
12、远程代码执行漏洞的探讨；
13、服务器安全管控的探讨；
14、畅谈端口安全配置；
15、谈一谈github泄露；
16、撞库攻击是场持久战；
17、url重定向攻击的探讨；
18、聊聊弱口令的危害（一）。

jsrc_team

京东安全应急响应中心

动动手指~关注下呗~