一个容易忽视的Oracle数据安全问题 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/143/2021_2022__E4_B8_80_E4_B8_AA_E5_AE_B9_E6_c102_143739.htm 数据库安全问题一直是人们关注的焦点之一，我们知道一个企业或者机构的数据库如果遭到黑客的攻击，而这些数据库又保存着非常重要的数据，象银行、通信等数据库，后果将不堪设想。Oracle数据库使用了多种手段来保证数据库的安全性，如密码，角色，权限等等。 作为Oracle的数据库管理员都知道，数据库系统典型安装后，一般sys和system以及internal这三个用户具有默认的口令，数据库安装成功后，系统管理员作的第一件工作就是修改这些用户的口令，保证数据库的安全性。然而，众多管理员往往忽视了其中的一个安全问题，下面我们就将详细讨论这个问题。 Oracle数据库系统如果采用典型安装后，除了创建前面介绍的几个用户外，另外还自动创建了一个叫做DBSNMP的用户，该用户负责运行Oracle系统的智能代理（Intelligent Agent），该用户的缺省密码也是“ DBSNMP ”。如果忘记修改该用户的口令，任何人都可以通过该用户存取数据库系统。现在我们来看一下该用户具有哪些权限和角色，然后来分析一下该用户对数据库系统可能造成的损失。 启动SQL/PLUS程序，使用该用户登录进入： SQL> 0select * from session_privs.CREATE SESSIONALTER SESSIONUNLIMITED TABLESPACECREATE TABLECREATE CLUSTERCREATE SYNONYMCREATE PUBLIC SYNONYMCREATE VIEWCREATE SEQUENCECREATE DATABASE LINKCREATE PROCEDURECREATE TRIGGERANALYZE

ANYCREATE TYPECREATE OPERATORCREATE INDEXTYPE可以看到该用户不是SYS或SYSTEM管理用户，然而，它却具有两个系统级权限：UNLIMITED TABLESPACE和CREATE PUBLIC SYNONYM。 看到这两个权限你应该马上想到，这些都是安全隐患，尤其是UNLIMITED TABLESPACE，它是破坏数据库系统的攻击点之一。如果这时候你还依然认为，即使有人利用这个没有修改的口令登录进数据库也造成不了什么损失的话，我就不得不提醒你：该用户具有UNLIMITED TABLESPACE的系统权限，它可以写一个小的脚本，然后恶意将系统用垃圾数据填满，这样数据库系统也就无法运行，并将直接导致最终的瘫痪。目前很多数据库系统都要求7X24的工作，如果出现了系统用垃圾数据填满的情况，那么，等数据库系统恢复时，恐怕不可挽回的损失已经造成了。 为了保证Oracle数据库系统运行的绝对安全，强烈建议数据库管理员修改该用户的默认口令，不要为不怀好意的人留下“ 方便之门 ”。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com