如何搞垮他的数据库谈Oracle安全 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__E5_A6_82_E4_BD_95_E6_90_9E_E5_c102_143413.htm 人们经常听到Windows的安全漏洞，频繁的遭受病毒攻击等，我们的传统观念是 Windows太不安全了；实际上Unix/Linux如果配置不当，其危险性远远高出人们的想象，大部分人非常重视操作系统的安全，但作为其最重要的数据库应用，你注意它了么？本文旨在介绍数据库级的安全，当然操作系统被攻破的话，那一切免谈。 让我带你去试着攻击一台装有Oracle的机器 1、首先确定被攻击Oracle的IP地址（无目的，那就去全网扫描吧，发现1521端口打开的就挑出来，不要说连扫描都不会，F..t） 2、猜测它的SID号；好象很困难，事实上安装Oracle时有缺省值，80%的人安装时都不会去修改，或改为很容易猜测的值，比如：ORCL、ORA、ORA8、ORA9、ORACLE、ORACLE8、ORACLE9、ORACLE8I、ORACLE817、ORACLE92... 3、连接后，猜测用户名和口令；好象更困难，事实上安装 Oracle时，SYS、SYSTEM等系统用户有缺省口令，可惜在9i中，终于改为需用户自己确定口令(不过大部分用户还是沿用以前的口令或使用oracle)，而且还有被人们遗忘的用户，比如SCOTT，缺省安装时他会被建立起来的。 4、sqlplus scott/tiger@ora_sid 终于登陆进来，可是这个小用户只是用来做测试学习的，我们用他来干什么呢？ 键入： SQL> 0select USERNAME,DEFAULT_TABLESPACE from USER_USERS.USERNAME DEFAULT_TABLESPACE----------

----------SCOTT USERSSQL> 0select * from session_privs.PRIVILEGE----------CREATE SESSIONALTER SESSIONUNLIMITED TABLESPACECREATE TABLECREATE CLUSTERCREATE SYNONYMCREATE VIEWCREATE SEQUENCECREATE DATABASE LINKCREATE PROCEDURECREATE TRIGGERCREATE TYPECREATE OPERATORCREATE INDEXTYPESQL> 0select * from user_ts_quotas.TABLESPACE_NAME BYTES MAX_BYTES BLOCKS MAX_BLOCKS---------- ---------- SYSTEM 524288 0 64 0USERS 65536 0 8 0什么意思呢？ 意思是我们的这个用户是数据缺省是建在USERS表空间上的，拥有建表等权限，而USERS表空间的磁盘使用是无限制的，聪明的读者应该明白我们可以在这里写入很多数据直到占满它的磁盘，造成数据库无法使用..... 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