链滴

服务器安全检查

作者：sumoonyoko
原文链接：https://ld246.com/article/1569292920056
来源网站：链滴

<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/bing/20180523.jpg?imageView2/1/w/960/h/540/interlace/1/q/100">
对您的服务器进行排查，如果您不知道排查方法的话，建议您按照下面的说明进行相关排查：</
>
1、（1） 检查服务器内是否有异常的账户，查看下服务器内是否有非系统和用户本身创建的账
，一般黑客创建的账户账户名 后会有 $ 这个字符，有此类账户存在，请立即禁用或者删除掉；
（2） 黑客也可能在您服务器内创建隐藏用户，隐藏账户在本地用户内是查看不到的，您可以在
务器内点击开始-运行-输入 regedt32.exe，依次选择 HKEY_LOCAL_MACHINE/SAM/SAM，默认
看不到里面的内容，这个时候点到 SAM，鼠标右键选择 权限，选择 administrator，将权限勾选为
全控制，确定。然后点开始-运行，输入 regedit，选择 HKEY_LOCAL_MACHINE/SAM/SAM/Doma
ns/Account，打开显示的就是你的机子的所有用户名，如出现本地账户中没有的账 户，即为隐藏账
，可以删除下，这样就可以删除隐藏用户了（建议您在操作修改注册表前先备份下，以免操作出错）<
p>
2、登录服务器点击开始-运行-输入 cmd-输入 netstat –nao 查看下服务器是否有未被授权的端
被监听，查看下对应的 pid 进程号，然后服务器点击开始--> 运行--> 输入“msinfo32”软件
境--> 正在运行的任务，通过 pid 号查看下运行文件的路 径，删除对应路径文件
3、检查下您服务器内部是否有异常的启动项，首先在服务器内点击开始-所有程序-启动，此目
在默认情况下是一个空 目录，但是如果有启动程序或者.bat 后缀的文件，核实下是否为您技术人员
加的，如果不是请删除下；然后再次点击 开始-运行，输入 msconfig，打开系统启动项，在启动菜
栏中查看是否存在命名异常的启动项目，例如 A.EXE XXXXI1SU2.EXE 等，有的话您将启动项目的勾
去掉，并到命令中显示的路径删除下文件，最后点击开始-运行，输入 regedit，依次点击 HKEY_CUR
ENT_USER/software/micorsoft/windows/currentversion/run 看下右侧是否有启动异常的项目，
的话也删除下 并建议在服务器内安装杀毒软件对判断做下病毒查杀，清除下病毒木马。
4.Windows 系统用户展开任务管理器会看到异常进程，这类进程的进程名一般不符合英语语法
惯、计算机命名习惯，或者有随机字符串的特征。
1 进程名不合符英语语法习惯，如 eeosec.exe
2 进程名全为数字，如 117466363.exe
3 进程名具有一定意义上的随机性，如 lkdhpec.exe
4 进程名具有明显的中文特征，如 SB360.exe、 caonima.exe
优化建议：修改远程端口点击开始-运行-输入 regedit，打开注册表，进入如下路径：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd
Tds\tcp
HKEY_LOCAL_MACHINE\SYSTEM\CurrentContro1Set\Control\Tenninal Server\WinStation
\RDP-Tcp
修改下右侧的 PortNamber 值
限制远程登录 IP：
windows 2003:打开防火墙点击例外，选择下远程桌面-点击编辑-更改范围，在自定义列表中填
上需要远程的 IP
windows 2008/2012:依次打开控制面板-系统安全-Windows 防火墙-高级设置-入站规则-远程
面（TCP-In）-作用域，在远程 IP 处填写需要远程连接的服务器 IP