网管必读：防溢出提升权限攻击解决办法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/140/2021_2022__E7_BD_91_E7_AE_A1_E5_BF_85_E8_c100_140104.htm 在骇客频频攻击、在系统漏洞层出不穷的今天，作为网络管理员、系统管理员的我们虽然在服务器的安全上都下了不少功夫：诸如，及时的打上系统安全补丁、进行一些常规的安全配置,但是仍然不太可能每台服务器都会在第一时间内给系统打上全新补丁。因此我们必需要在还未被入侵之前，通过一些系列安全设置，来将入侵者们挡在“ 安全门 ”之外.下面就以本人一直以来所用到的最简单、最有效的防(Overflow)溢出、本地提供权限攻击类的解决办法给大家讲讲。 1、如何可以防止溢出类的骇客攻击呢? ① 尽最大的可能性将系统的漏洞补丁都打完.最好是比如Microsoft Windows Server系列的系统可以将自动更新服务打开，然后让服务器在您指定的某个时间段内自动连接到Microsoft Update网站进行补丁的更新。如果您的服务器为了安全起见 禁止了对公网外部的连接的话，可以用Microsoft WSUS服务在内网进行升级。 ② 停掉一切不需要的系统服务以及应用程序，最大限能的降底服务器的被攻击系数。比如前阵子的MSDTC溢出，就导致很多服务器挂掉了。其实如果WEB类服务器根本没有用到MSDTC服务时，您大可以把MSDTC服务停掉，这样MSDTC溢出就对您的服务器不构成任何威胁了。 ③ 启动TCP/IP端口的过滤:仅打开常用的TCP如21、80、25、110、3389等端口.如果安全要求级别高一点可以将UDP端口关闭，当然如果这样之后缺陷就是如在服务器上连外部就不方便连接了，这里建议大家用IPSec来封UDP。

在协议筛选中"只允许"TCP协议(协议号为:6)、UDP协议(协议号为:17)以及RDP协议(协议号为:27)等必需用协议即可其它无用均不开放。 ④ 启用IPSec策略:为服务器的连接进行安全认证，给服务器加上双保险。如③所说，可以在这里封掉一些危险的端品诸如:135 145 139 445 以及UDP对外连接之类、以及对通读进行加密与只与有信任关系的IP或者网络进行通讯等等。(注:其实防反弹类木马用IPSec简单的禁止UDP或者不常用TCP端口的对外访问就成了,关于IPSec的如何应用这里就不再敖续，你可以到服安讨论Search "IPSec"，就 会有N多关于IPSec的应用资料..)。 ⑤ 删除、移动、更名或者用访问控制表列Access Control Lists (ACLs)控制关键系统文件、命令及文件夹: a.黑客通常在溢出得到shell后，来用诸如net.exe net1.exe ipconfig.exe user.exe query.exe regedit.exe regsvr32.exe 来达到进一步控制服务器的目的如:加账号了，克隆管理员了等等.这里我们可以将这些命令程序删除或者改名。(注意:在删除与改名时先停掉文件复制服务(FRS)或者先将%windir%\system32\dllcache\下的对应文件删除或改名。) b.也或者将这些.exe文件移动到你指定的文件夹,这样也方便以后管理员自己使用。 c.访问控制表列ACLS控制:找到%windir%\system32下找到cmd.exe、cmd32.exe net.exe net1.exe ipconfig.exe tftp.exe ftp.exe user.exe reg.exe regedit.exe regedt32.exe regsvr32.exe 这些黑客常用的文件，在“ 属性 ”→“ 安全 ”中对他们进行访问的ACLs用户进 行定义，诸如只给administrator有权访问，如果需要防范一些溢出攻击、以及溢出成功后对这些文件的非法利用.那么我们只需要将system用户 在ACLs中进行拒绝访问即可。 d.如果你觉得在GUI下面

太麻烦的话，你也可以用系统命令的CACLS.EXE来对这些.exe文件的Acls进行编辑与修改，或者说将他写成一个.bat批处理文件来执行以及对这些命令进行修改。(具体用户自己参见cacls /? 帮助进行，由于这里的命令太多我就不一一列举写成批处理代码给各位了!!) e.对磁盘如C/D/E/F等进行安全的ACLS设置从整体安全上考虑的话也是很有必要的，另外特别是win2k，对Winnt、Winnt\System、Document and Setting等文件夹。 ⑥ 进行注册表的修改禁用命令解释器: (如果您觉得用⑤的方法太烦琐的话，那么您不防试试下面一劳永逸的办法来禁止CMD的运行) 通过修改注册表，可以禁止用户使用命令解释器(CMD.exe)和运行批处理文件(.bat文件)。具体方法:新建一个双字节(REG_DWORD)执行 HKEY_CURRENT_USER\Software\Policies\ Microsoft\Windows\System\DisableCMD，修改其值为1，命令解释器和批处理文件都不能被运行。修改其值为2，则只是禁止命令解释器的运行,反之将值改为0，则是打开CMS命令解释器。如果您赚手动太麻烦的话,请将下面的代码保存为*.reg文件，然后导入。 Windows Registry Editor Version 5.00 [HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System] "DisableCMD"=dword:00000001 ⑦ 对一些以System权限运行的系统服务进行降级处理。(诸如:将Serv-U、Imail、IIS、Php、Mssql、Mysql等一系列以System权限运行的服务或者应用程序换成其它administrators成员甚至users权限运行，这样就会安全得多了...但前提是需要对这些基本运行状态、调用API等相关情况较为了解. ) 其实，关于防止如Overflow溢出类攻击的办法除了用上述的几点以外，还有N多种办法:诸如

用组策略进行限制，写防护过滤程序用DLL方式加载windows到相关的SHell以及动态链接程序之中这类。当然自己写代码来进行验证加密就需要有相关深厚的Win32编程基础了，以及对Shellcode较有研究.由于此文仅仅是讨论简单的解决办法，因此其它办法就不在这里详述了。 2、如何在防止被骇客溢出得到Shell后对系统的而进一步入侵呢? ① 在做好1中上述的工作之后，基本上可以防目骇客在溢出之后得到shell了.因为即使Overflow溢出成功，但在调用CMDSHELL、以及对外联接时就卡了。 (为什么呢，因为:1.溢出后程序无法再调用到CMDSHLL我们已经禁止system访问CMD.exe了。2.溢出之后在进行反弹时已经无法对外部IP进行连接了。所以，基本上要能过system权限来反弹shell就较困难的了...)。 ② 当然世界上是不存在绝对的安全的，假设入侵者在得到了我们的shell之后，做些什么呢?一般入侵者在在得到shell之后，就会诸如利用系统命令加账号了 通过tftp、ftp、vbs等方式传文件了等等来达到进一步控制服务器。这里我们通过1上述的办法对命令进行了限制，入侵者是没有办法通过tftp、ftp来传文件了，但他们仍然可以能过echo写批处理，用批处理通过脚本BAT/VBS/VBA等从WEB上下载文件，以及修改其它盘类的文件等潜在破坏行为。所以我们需要 将echo命令也限制以及将其它盘的System写、修改文件的权限进行处理。以及将VBS/VBA类脚本以及XMLhttp等组件进行禁用或者限制system的运行权。这样的话别人得到Shell也无法对服务器上的文件进行删除以及进行步的控制系统了.以及本地提权反弹Shell了。 后记:其它服务器、系统的安全是个整体的概念.有可能你其它一小点的疏忽就可以让你的网站、甚至服务器沦

陷。因此安全策略必需走防患未然的道路，任何一个小地方都不能马虎。