网络安全

安全技巧（十一）

小未 主编

目　录

Win2000Server 入侵监测

入侵检测初步

上一章我们谈到了 Win2000Server 的安全配置，经过精心配置的 Win2000 服务器可以防御 90%以上的入侵和渗透，但是，就象上一章结束时我所提到的：系统安全是一个连续的过程，随着新漏洞的出现和服务器应用的变化，系统的安全状况也在不断变化着；同时由于攻防是矛盾的统一体，道消魔长和魔消道长也在不断的转换中，因此，再高明的系统管理员也不能保证一台正在提供服务的服务器长时间绝对不被入侵。

所以，安全配置服务器并不是安全工作的结束，相反却是漫长乏味的安全工作的开始，本文我们将初步探讨 Win2000 服务器入侵检测的初步技巧，希望能帮助您长期维护服务器的安全。

本文中所说的入侵检测指的是利用 Win2000Server 自身的功能及系统管理员自己编写的软件/脚本进行的检测，使用防火墙（Firewall）或入侵监测系统（IDS）的技巧并不在本文的讨论范围之内。

现在假定：我们有一台 Win2000Server 的服务器，并且经过了初步的安全配置（关于安全配置的详情可以参阅 Win2000Server 安全配置入门<一>），在这种情况下，大部分的入侵者将被拒之门外。（哈哈，我管理员可以回家睡大觉去了）慢着，我说的是大部分，不是全部，经过初步安全配置的服务器虽然可以防御绝大多数的 Scriptkid（脚本族-只会用别人写的程序入侵服务器的人），

遇到了真正的高手，还是不堪一击的。虽然说真正的高手不会随便进入别人的服务器，但是也难保有几个品行不端的邪派高手看上了你的服务器。（我真的这么衰么？）而且，在漏洞的发现与补丁的发布之间往往有一段时间的真空,任何知道漏洞资料的人都可以乘虚而入，这时，入侵检测技术就显得非常的重要。

入侵的检测主要还是根据应用来进行，提供了相应的服务就应该有相应的检测分析系统来进行保护，对于一般的主机来说，主要应该注意以下几个方面：

1、基于 80 端口入侵的检测

WWW 服务大概是最常见的服务之一了，而且由于这个服务面对广大用户，服务的流量和复杂度都很高，所以针对这个服务的漏洞和入侵技巧也最多。对于 NT 来说，IIS 一直是系统管理员比较头疼的一部分（恨不得关了 80 端口），不过好在 IIS 自带的日志功能从某种程度上可以成为入侵检测的得力帮手。IIS 自带的日志文件默认存放在 System32/LogFiles 目录下，一般是按 24 小时滚动的,在 IIS 管理器中可以对它进行详细的配置。(具体怎么配我不管你，不过你要是不详细记录，回头查不到入侵者的 IP 可不要哭)

现在我们再假设（怎么老是假设呀，烦不烦？）别急呀，我不能为了写这篇文章真的去黑掉一台主机，所以只好假设了，我们假设一台 WEB 服务器，开放了 WWW 服务，你是这台服务器的系统管理员，已经小心地配置了 IIS，使用 W3C 扩展的日志格式，并至少记录了时间（Time）、客户端 IP（ClientIP）、方法（Method）、URI 资源(URIStem)、URI 查询(URIQuery)，协议状态（ProtocolStatus)，我们用最近比较流行的 Unicode 漏洞来

进行分析：打开 IE 的窗口，在地址栏输入：127.0.0.1/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir 默认的情况下你可以看到目录列表（什么？你已经做过安全配置了，看不到？恢复默认安装，我们要做个实验），让我们来看看 IIS 的日志都记录了些什么，打开 Ex010318.log（Ex 代表 W3C 扩展格式，后面的一串数字代表日志的记录日期）：07:42:58127.0.0.1GET/scripts/..\../winnt/system32\cmd.exe/c+dir200 上面这行日志表示在格林威治时间 07:42:58（就是北京时间 23:42:58），有一个家伙（入侵者）从 127.0.0.1 的 IP 在你的机器上利用 Unicode 漏洞（%c1%1c 被解码为"\"，实际的情况会因为 Windows 语言版本的不同而有略微的差别）运行了 cmd.exe，参数是/cdir，运行结果成功（HTTP200 代表正确返回）。(哇，记录得可真够全的，以后不敢随便乱玩 Unicode 了)

大多数情况下，IIS 的日志会忠实地记录它接收到的任何请求（也有特殊的不被 IIS 记录的攻击，这个我们以后再讨论），所以，一个优秀的系统管理员应该擅长利用这点来发现入侵的企图，从而保护自己的系统。但是，IIS 的日志动辄数十兆、流量大的网站甚至数十 G，人工检查几乎没有可能，唯一的选择就是使用日志分析软件，用任何语言编写一个日志分析软件（其实就是文本过滤器）都非常简单，不过考虑到一些实际情况（比如管理员不会写程序，或者服务器上一时找不到日志分析软件），我可以告诉大家一个简单的方法，比方说你想知道有没有人从 80 端口上试图取得你的 Global.asa 文件，可以使用以下的 CMD 命令：find"Global.asa"ex010318.log /i 这个命令使用的是 NT 自带的 find.exe 工具（所以不怕紧急情况找不着），可以轻松的从文本文件中找到你想过

滤的字符串，"Global.asa"是需要查询的字符串，ex010318.log 是待过滤的文本文件，/i 代表忽略大小写。因为我无意把这篇文章写成微软的 Help 文档，所以关于这个命令的其他参数以及它的增强版 FindStr.exe 的用法请去查看 Win2000 的帮助文件。

无论是基于日志分析软件或者是 Find 命令，你都可以建立一张敏感字符串列表，包含已有的 IIS 漏洞（比如"+.htr"）以及未来将要出现的漏洞可能会调用的资源（比如 Global.asa 或者 cmd.exe），通过过滤这张不断更新的字符串表，一定可以尽早了解入侵者的行动。

需要提醒的是，使用任何日志分析软件都会占用一定的系统资源，因此，对于 IIS 日志分析这样低优先级的任务，放在夜里空闲时自动执行会比较合适，如果再写一段脚本把过滤后的可疑文本发送给系统管理员，那就更加完美了。同时，如果敏感字符串表较大，过滤策略复杂，我建议还是用 C 写一个专用程序会比较合算。

2、基于安全日志的检测

通过基于 IIS 日志的入侵监测，我们能提前知道窥伺者的行踪（如果你处理失当，窥伺者随时会变成入侵者），但是 IIS 日志不是万能的，它在某种情况下甚至不能记录来自 80 端口的入侵，根据我对 IIS 日志系统的分析，IIS 只有在一个请求完成后才会写入日志，换言之，如果一个请求中途失败，日志文件中是不会有它的踪影的（这里的中途失败并不是指发生 HTTP400 错误这样的情况，而是从 TCP 层上没有完成 HTTP 请求，例如在 POST 大量数据时异常中断），对于入侵者来说，就有可能绕过日志系统完成大量的活动。

而且，对于非 80Only 的主机，入侵者也可以从其它

的服务进入服务器，因此，建立一套完整的安全监测系统是非常必要的。

Win2000 自带了相当强大的安全日志系统，从用户登录到特权的使用都有非常详细的记录，可惜的是，默认安装下安全审核是关闭的，以至于一些主机被黑后根本没法追踪入侵者。所以，我们要做的第一步是在管理工具-本地安全策略-本地策略-审核策略中打开必要的审核，一般来说，登录事件与账户管理是我们最关心的事件，同时打开成功和失败审核非常必要，其他的审核也要打开失败审核，这样可以使得入侵者步步维艰，一不小心就会露出马脚。仅仅打开安全审核并没有完全解决问题，如果没有很好的配置安全日志的大小及覆盖方式，一个老练的入侵者就能够通过洪水般的伪造入侵请求覆盖掉他真正的行踪。通常情况下，将安全日志的大小指定为 50MB 并且只允许覆盖 7 天前的日志可以避免上述情况的出现。

设置了安全日志却不去检查跟没有设置安全日志几乎一样糟糕（唯一的优点是被黑了以后可以追查入侵者），所以，制定一个安全日志的检查机制也是非常重要的，作为安全日志，推荐的检查时间是每天上午，这是因为，入侵者喜欢夜间行动（速度快呀，要不你入侵到一半的时候连不上了，那可是哭都哭不出来）上午上班第一件事正好看看日志有没有异常，然后就可以放心去做其他的事了。如果你喜欢，也可以编写脚本每天把安全日志作为邮件发送给你（别太相信这个了，要是哪个高手上去改了你的脚本，每天发送"平安无事"……）

除了安全日志，系统日志和应用程序日志也是非常好的辅助监测工具，一般来说，入侵者除了在安全日志

中留下痕迹（如果他拿到了 Admin 权限，那么他一定会去清除痕迹的),在系统和应用程序日志中也会留下蛛丝马迹，作为系统管理员，要有不放过任何异常的态度，这样入侵者就很难隐藏他们的行踪。

3、文件访问日志与关键文件保护

除了系统默认的安全审核外，对于关键的文件，我们还要加设文件访问日志，记录对他们的访问。

文件访问有很多的选项：访问、修改、执行、新建、属性更改.....一般来说，关注访问和修改就能起到很大的监视作用。

例如，如果我们监视了系统目录的修改、创建，甚至部分重要文件的访问（例如 cmd.exe,net.exe，system32 目录)，那么，入侵者就很难安放后门而不引起我们的注意，要注意的是，监视的关键文件和项目不能太多，否则不仅增加系统负担，还会扰乱日常的日志监测工作（哪个系统管理员有耐心每天看四、五千条垃圾日志？）

关键文件不仅仅指的是系统文件，还包括有可能对系统管理员/其他用户构成危害的任何文件，例如系统管理员的配置、桌面文件等等，这些都是有可能用来窃取系统管理员资料/密码的。

4、进程监控

进程监控技术是追踪木马后门的另一个有力武器，90%以上的木马和后门是以进程的形式存在的（也有以其他形式存在的木马，参见《揭开木马的神秘面纱三》)，作为系统管理员，了解服务器上运行的每个进程是职责之一（否则不要说安全，连系统优化都没有办法做)，做一份每台服务器运行进程的列表非常必要，能帮助管理

员一眼就发现入侵进程，异常的用户进程或者异常的资源占用都有可能是非法进程。除了进程外，DLL 也是危险的东西，例如把原本是 exe 类型的木马改写为 dll 后，使用 rundll32 运行就比较具有迷惑性。

5、注册表校验

一般来说，木马或者后门都会利用注册表来再次运行自己，所以，校验注册表来发现入侵也是常用的手法之一。一般来说，如果一个入侵者只懂得使用流行的木马，那么由于普通木马只能写入特定的几个键值（比如 Run、Runonce 等等），查找起来是相对容易的，但是对于可以自己编写/改写木马的人来说，注册表的任何地方都可以藏身，靠手工查找就没有可能了。（注册表藏身千变万化，例如需要特别提出来的 FakeGina 技术，这种利用 WINNT 外嵌登录 DLL（Ginadll）来获得用户密码的方法最近比较流行，一旦中招，登录用户的密码就会被记录无遗，具体的预防方法我这里就不介绍了。）应对的方法是监控注册表的任何改动，这样改写注册表的木马就没有办法遁形了。监控注册表的软件非常多，很多追查木马的软件都带有这样的功能，一个监控软件加上定期对注册表进行备份，万一注册表被非授权修改，系统管理员也能在最短的时间内恢复。

6、端口监控

虽然说不使用端口的木马已经出现，但是大部分的后门和木马还是使用 TCP 连接的，监控端口的状况对于由于种种原因不能封锁端口的主机来说就是非常重要的了，我们这里不谈使用 NDIS 网卡高级编程的 IDS 系统，对于系统管理员来说，了解自己服务器上开放的端口甚至比对进程的监控更加重要，常常使用 netstat 查看服务

器的端口状况是一个良好的习惯,但是并不能 24 小时这样做，而且 NT 的安全日志有一个坏习惯，喜欢记录机器名而不是 IP（不知道比尔盖子怎么想的），如果你既没有防火墙又没有入侵检测软件，倒是可以用脚本来进行 IP 日志记录的，看着这个命令：

netstat-n-ptcp10>>Netstat.log,这个命令每 10 秒钟自动查看一次 TCP 的连接状况，基于这个命令我们做一个 Netlog.bat 文件:

time/t>>Netstat.log

Netstat-n-ptcp10>>Netstat.log

这个脚本将会自动记录时间和 TCP 连接状态，需要注意的是：如果网站访问量比较大，这样的操作是需要消耗一定的 CPU 时间的，而且日志文件将越来越大，所以请慎之又慎。(要是做个脚本就完美无缺，谁去买防火墙？:)

一旦发现异常的端口，可以使用特殊的程序来关联端口、可执行文件和进程(如 inzider 就有这样的功能，它可以发现服务器监听的端口并找出与该端口关联的文件，inzider 可以从 http://www.nttoolbox.com 下载到)，这样无论是使用 TCP 还是 UDP 的木马都无处藏身。

7、终端服务的日志监控

单独将终端服务（TerminalService）的日志监控分列出来是有原因的，微软 Win2000 服务器版中自带的终端服务 TerminalService 是一个基于远程桌面协议(RDP)的工具，它的速度非常快，也很稳定，可以成为一个很好的远程管理软件，但是因为这个软件功能强大而且只受到密码的保护，所以也非常的危险，一旦入侵者拥有了管理员密码，就能够象本机一样操作远程服务器（不

需要高深的 NT 命令行技巧，不需要编写特殊的脚本和程序，只要会用鼠标就能进行一切系统管理操作，实在是太方便、也实在是太可怕了）。虽然很多人都在使用终端服务来进行远程管理，但是，并不是人人都知道如何对终端服务进行审核，大多数的终端服务器上并没有打开终端登录的日志，其实打开日志审核是很容易的，在管理工具中打开远程控制服务配置（TerminalServiceConfigration），点击"连接"，右击你想配置的 RDP 服务（比如 RDP-TCP(MicrosoftRDP5.0)，选中书签"权限"，点击左下角的"高级"，看见上面那个"审核"了么？我们来加入一个 Everyone 组，这代表所有的用户，然后审核他的"连接"、"断开"、"注销"的成功和"登录"的成功和失败就足够了，审核太多了反而不好，这个审核是记录在安全日志中的，可以从"管理工具"->"日志查看器"中查看。现在什么人什么时候登录我都一清二楚了，可是美中不足的是：这个破烂玩艺居然不记录客户端的 IP（只能查看在线用户的 IP），而是华而不实的记录什么机器名，倒！要是别人起个 PIG 的机器名你只好受他的嘲弄了，不知道微软是怎么想的，看来还是不能完全依赖微软呀，我们自己来吧？写个程序，一切搞定，你会 C 么？不会？VB 呢？也不会？Delphi？……什么？你什么编程语言都不会？我倒，毕竟系统管理员不是程序员呀，别急别急，我给你想办法，我们来建立一个 bat 文件，叫做 TSLog.bat，这个文件用来记录登录者的 IP，内容如下：

```
time/t>>TSLog.log
netstat-n-ptcp|find":3389">>TSLog.log
startExplorer
```

我来解释一下这个文件的含义：

第一行是记录用户登录的时间，time/t 的意思是直接返回系统时间（如果不加/t，系统会等待你输入新的时间），然后我们用追加符号">>"把这个时间记入 TSLog.log 作为日志的时间字段；

第二行是记录用户的 IP 地址，netstat 是用来显示当前网络连接状况的命令，-n 表示显示 IP 和端口而不是域名、协议，-ptcp 是只显示 tcp 协议，然后我们用管道符号"|"把这个命令的结果输出给 find 命令，从输出结果中查找包含":3389"的行（这就是我们要的客户的 IP 所在的行，如果你更改了终端服务的端口，这个数值也要作相应的更改），最后我们同样把这个结果重定向到日志文件 TSLog.log 中去，于是在 SLog.log 文件中，记录格式如下：

22:40

TCP192.168.12.28:3389192.168.10.123:4903ESTABLISHED

22:54

TCP192.168.12.28:3389192.168.12.29:1039ESTABLISHED

也就是说只要这个 TSLog.bat 文件一运行，所有连在 3389 端口上的 IP 都会被记录，那么如何让这个批处理文件自动运行呢？我们知道，终端服务允许我们为用户自定义起始的程序，在终端服务配置中，我们覆盖用户的登录脚本设置并指定 TSLog.bat 为用户登录时需要打开的脚本，这样每个用户登录后都必须执行这个脚本，因为默认的脚本（相当于 shell 环境）是 Explorer（资源管理器），所以我在 TSLog.bat 的最后一行加上了启动 Explorer 的命令 startExplorer，如果不加这一行命令，用

户是没有办法进入桌面的！当然，如果你只需要给用户特定的 Shell：

例如 cmd.exe 或者 word.exe 你也可以把 startExplorer 替换成任意的 shell。这个脚本也可以有其他的写法，作为系统管理员，你完全可以自由发挥你的想象力、自由利用自己的资源，例如写一个脚本把每个登录用户的 IP 发送到自己的信箱对于重要的服务器也是一个很好的方法。正常情况下一般的用户没有查看终端服务设置的权限，所以他不会知道你对登录进行了 IP 审核，只要把 TSLog.bat 文件和 TSLog.log 文件放在比较隐蔽的目录里就足够了，不过需要注意的是这只是一个简单的终端服务日志策略，并没有太多的安全保障措施和权限机制，如果服务器有更高的安全要求，那还是需要通过编程或购买入侵监测软件来完成的。

8、陷阱技术

早期的陷阱技术只是一个伪装的端口服务用来监测扫描，随着矛和盾的不断升级，现在的陷阱服务或者陷阱主机已经越来越完善，越来越象真正的服务，不仅能截获半开式扫描，还能伪装服务的回应并记录入侵者的行为，从而帮助判断入侵者的身份。

我本人对于陷阱技术并不是非常感兴趣，一来从技术人员角度来说，低调行事更符合安全的原则；二来陷阱主机反而成为入侵者跳板的情况并不仅仅出现在小说中，在现实生活中也屡见不鲜，如果架设了陷阱反而被用来入侵，那真是偷鸡不成了。

记得 CoolFire 说过一句话，可以用来作为对陷阱技术介绍的一个结束：在不了解情况时，不要随便进入别人的系统，因为你永远不能事先知道系统管理员是真的

白痴或者伪装成白痴的天才……

入侵监测的初步介绍就到这里，在实际运用中，系统管理员对基础知识掌握的情况直接关系到他的安全敏感度，只有身经百战而又知识丰富、仔细小心的系统管理员才能从一点点的蛛丝马迹中发现入侵者的影子，未雨绸缪，扼杀入侵的行动。

网上防黑秘籍

对于在网上冲浪的微机，其系统的安全性能将会受到严格的考验。如果不加防范，其上的重要数据、文件等信息将会完全暴露。在上网时你将面对的是有很高计算机水平的黑客的攻击。只要你稍不留神，他便会悄悄地侵入你的系统。

防 IP 地址的攻击

现在常见的这类攻击工具有：Nuke、Winnuke、Teardrop、。它们主要利用 Win98/NT 下微软网络协议 NetBIOS 的例行处理程序 OOB 的漏洞，将一个包以 OOB 方式放在某个 IP 地址的某个开放的端口上（一般为 136、139、135、113），就可能使你的电脑突然死机。遭受此类攻击的对象主要是 Win95，而 Win98 系统在这方面的防御能力要强一些，使其受攻击的概率减少。对于 Win95 我们可以通过在注册表/HKEY—LOCAL—MACHINE/System/CurrentControlSet/Services/VxD/中新建字符串“BSDUr”，键值为“1./”，并将

\Windows\tem 中的 Vnbt.386 更名为 Vnbt.bak 来防范攻击。另外，我们还可以使用 Nocrash、Antinuke、N

ukenab 等程序来防范攻击。

手工检查和清除木马

上面的措施有些对一般用户来说似乎并不容易办到，但我建议你至少应养成定时检查微机系统的习惯。我们已经介绍了 Cleaner、Sudo99 等软件，下面介绍一些“特洛伊木马”的手动检查及清除方法：

1.BackOrifice（BO）

检查注册表\HEKY—LOCAL—MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 中有无.exe 键值。如有则将其删除，并进入 MSDOS 状态，将\Windows\System 中的.exe 文件删除。

检查注册表\HEKY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 中有无键值 Spynotify.exe 和 Netspy.exe。如有将其删除，重启计算机后将\Windows\System 中对应文件删除。

2.Netbus

用 Netstat－an 查看 12345 端口是否开放，在注册表对应位置中是否有可疑文件，首先清除注册表中的 Netbus 的主键，然后重新启动计算机，删除掉其运行文件即可。

特洛伊木马的防范

“特洛伊木马”技术是黑客常用的攻击方法。它通过在你的电脑系统中隐藏一个会在 Windows 启动时悄悄执行的程序，用服务器/客户的手段，而达到在你上网时控制你电脑的目的。黑客可以利用它窃取你的密码，浏览你的硬盘，修改你的文件、注册表等等。对于它我们可以采用 LockDown 等在线黑客监视程序加以防范。

在网络流量分析方面，“SessionWall－3”更是具有

独到之处———以响应方式监督“交通”。这意味着无需经过“SessionWall－3”，用户就可以分析网络交通状况并采取行动了。因为它提供用户一个实时的信息流量图形来监测网络数据流量（或者还可按要求显示指定时期的信息流量），具备了智能特性。而且由于是按照“Session”级检测，它可以检测到一般的网络防火墙（按“包”来检测）检测不到的非法入侵，防止诸如“拒绝服务”之类的新的攻击手段。

为了高效地抵御大面积“拒绝服务”攻击工具的进攻，冠群金辰正在加强对 TFN2K 工具各种变种的侦测能力。网络安全防护软件“InternetPro tector”和“SessionWall－3”将与 KILL 系列其他反病毒产品一起为企业网络系统提供全面安全保护。

E-mail 的防犯

网时最扫兴的事莫过于遇到邮件炸弹了。如果某一天收邮件的时候发现邮箱里面有上万封信，这就是邮箱被恶作剧者炸掉了。假如是相当重要的邮箱，里面又恰好有一些紧急信件待取，那给被炸者带来的损失就非同小可。因此有效防范邮件炸弹成了一种必要的上网措施。虽然目前有好多工具能利用远程管理邮箱的功能来清除这些垃圾邮件，例如 FoxMail，TheBat！，Eudora 等，但如果你的电脑上刚好没有安装这些软件，那怎么办呢？别忙，如果你的机子上安装了 OICQ，那还有另外一个解决办法。

选取 OICQ 主菜单里面“系统参数/E-mail 设置”，弹出控制面板，在“邮件检查（POP 设置）”栏的“用户名”中填入被炸信箱的帐号，“密码”中填入该帐号的密码。再下面是相应的 POP3 和 SMTP 服务器地址，正

确填写后可以在右边设置检测邮箱的时间间隔。出于防范目的,当然要设置一个尽量短的时间间隔(如 5 分钟),设置完后按确定，重新上线就行了。

在此我要提醒各位网友注意以下几点：

1.不要轻易运行来历不明和从网上下载的软件。即使通过了一般杀毒软件的程序也不要轻易运行，对于此类软件，要用如 Cleaner、Sudo99 等专门的黑客程序清除软件检查。

2.保持警惕性。不要轻易相信好友发来的 E－mail 就一定没有黑客程序，如 Happy99 就会自动加在附件当中。

3.不要在聊天室内公布你的 Email 地址。对来历不明的 E－mail 应及时清除。

4.不要随便下载软件（特别是不可靠的 FTP 站点)。

5.不要将重要密码存放在计算机上,这样才可以达到防黑的效果!

网络安全技术-透析网络过载攻击

在过载攻击中，一个共享的资源或者服务由于需要处理大量的请求，以至于无法满足从其他用户到来的请求。例如一个用户生成了大量的进程，那么其他用户就无法运行自己的进程。如果一个用户使用了大量的磁盘空间，其他蝴户就无法生成新的文件。有效保护系统免遭过载攻击的办法是划分计算机中的资源，将每个用户的使用量限制在自己的那一份中。另外，还可以让系统自动检查是否过载或者重新启动系统。