快速通道

文档分类
软件作品
文档作品
<=
代码作品

推荐作品
对 RPC DCOM worm 的设想
[vulnwatch] Serv-U MDTM Command Buffer Overflow Vulnerab...

对 RPC DCOM worm 的设想

提交作品： lion
提交日期： 2003-08-08
作品属性： 推荐
文档类别： 文档作品
浏览次数： 今4次/总11244次

名称: 对 RPC DCOM 蠕虫的设想
作者: lion <lion@cnhonker.net>
主页: http://www.cnhonker.com
日期: 2003/08/08

最近好象几乎每一个大的漏洞公布出来，接着都会有一个针对这个漏洞的蠕虫(worm) 流行，最近闹得很凶的 RPC DCOM 漏洞估计也即将成为 worm 的新传播载体。好象写 worm 是一个热门，很多人也觉得好奇，觉得 worm 是很深的一种技术，其实这个是很简单的编程游戏而已。我一直有个想法就是想写一篇关于 worm 的技术分析(---为了不教坏小孩子:)，只是一直懒得提笔，本人对蠕虫的编写已经失去了兴趣，现在在新的 worm 风暴即将到来之前，我这里很简单分析一下蠕虫的相关技术，并对 RPC DCOM 蠕虫进行一些设想。大家当我是助“ 纣 ”为虐也好，故意卖弄也好，我觉得还是要写这篇文章，一年多没写过文章了，同时也了却了自己的一个心愿。你现在可以选择不继续往下看，但看完后不要对我吐口水。:)

一 什么叫蠕虫

首先从 spark <spark.bbs@bbs.nankai.edu.cn>的 《Internet蠕虫的定义和历史》文章中摘抄一段关于worm的解释: 蠕虫这个生物学名词在1982年由Xerox PARC 的John F. Shoch等人最早引入计算机领域[30]，并给出了计算机蠕虫的两个最基本特征："可以从一台计算机移动到另一台计算机"和"可以自我复制"。他们编写蠕虫的目的是做分布式计算的模型试验，在他们的文章中，蠕虫的破坏性和不易控制已经初露端倪。1988年Morris蠕虫爆发后，Eugene H. Spafford 为了区分蠕虫和病毒，给出了蠕虫的技术角度的定义，"计算机蠕虫可以独立运行，并能把自身的一个包含所有功能的版本传播到另外的计算机上。" （worm is a program that can run by itself and can propagate a fully working version of itself to other machines. ）。

由于这里不是向大家介绍蠕虫的定义和历史就不多说了，大家如果对这些感兴趣，可以到这里读 spark 的文章。http://www.nsfocus.net/index.php?act=magazine&do=view&mid=1851

二 蠕虫的组成部分

一个蠕虫的组成其实很简单，由于我不是在这里教你们写蠕虫，也由于时间限制，我这里只简单的说一些。
我们可以把它看做一个工程，我们把这个工程分成 4 个模块:

1. 攻击模块

首先得需要有一个大量系统受影响的能被简单利用的严重漏洞，以便能够远程控制机器。比如猜测薄弱口令啊，远程溢出啊等。

2. 感染模块
考虑怎么让对方被攻击后，执行你想要实现的功能，完成对一个主机的感染。对远程溢出来说也就是完善shellcode了。这中间得考虑一个感染传播(繁殖)途径的问题。

3. 传播模块
比如，扫描一个网段有相关弱点的机器，存成一个文件，然后对这些IP进行攻击，或者随机生成IP然后对这些IP进行攻击等。
简单的说就是扫描薄弱的机器。

4. 功能模块
功能模块其实是一个可要可不要的模块，但如果你想对方感染蠕虫后还在对方加上后门/DDoS等其他功能时，就必须得要有这个啦。

其实，一个蠕虫成功的关键是一个攻击模块和感染模块。:)

三 常见的蠕虫的传播(繁殖)途经

具体就不深入了, 只简单列举一下:

1. email

2. ftp

3. http

4. netbios

5. tftp

6. rcp

7. 其他

四 RPC DCOM 漏洞介绍

RPC DCOM 漏洞是最近出的一个Windows系统的严重漏洞，也是有史以来最严重影响最广泛的Windows漏洞。

Remote Procedure Call (RPC)是运用于Windows操作系统上的一种协议。RPC提供相互处理通信机制，允许运行该程序的计算机在一个远程系统上执行代码。RPC协议本身源于OSF (Open Software Foundation) RPC协议，后来又另外增加了一些Microsoft专用扩展功能。RPC中处理TCP/IP信息交换的模块由于错误的处理畸形信息，远程攻击者可利用此缺陷以本地系统权限在系统上执行任意指令。该缺陷影响使用RPC的DCOM接口，此接口处理由客户端机器发送给服务器的DCOM对象激活请求(如UNC路径)。攻击者成功利用此缺陷可以以本地系统权限执行任意指令。攻击者可以在系统上执行任意操作，如安装程序、查看或更改、删除数据或建立系统管理员权限的帐户。
这个漏洞影响如下Windows版本：
Microsoft Windows XP SP1a
Microsoft Windows XP SP1
Microsoft Windows XP
Microsoft Windows NT 4.0SP6a
Microsoft Windows NT 4.0SP6
Microsoft Windows NT 4.0SP5
Microsoft Windows NT 4.0SP4
Microsoft Windows NT 4.0SP3
Microsoft Windows NT 4.0SP2
Microsoft Windows NT 4.0SP1
Microsoft Windows NT 4.0
Microsoft Windows 2003
Microsoft Windows 2000SP4
Microsoft Windows 2000SP3
Microsoft Windows 2000SP2
Microsoft Windows 2000SP1
Microsoft Windows 2000

可以看到, 此漏洞影响除了WinME以下版本的Windows系统之外的所有其他Windows系统。同时，此漏洞能够被攻击者远程利用，
在没有修补该漏洞的机器上可以远程执行任意代码，导致攻击者能够完全控制有漏洞的机器。

五 RPC DCOM 蠕虫的设想

1. 由于RPC COM已经有攻击未打补丁的Win2000/WinXP的通用攻击代码发布出来，因此该漏洞更有可能被利用制作成为能够感染具有RPC DCOM漏洞的Win2000/WinXP机器的蠕虫。

如PacketStorm上公布的这个对Win2000和WinXP通用的Exploit:

```
/* Windows 2003 <= remote RPC DCOM exploit
* Coded by .:[oc192.us]:. Security
*
* Features:
*
* -d destination host to attack.
*
* -p for port selection as exploit works on ports other than 135
(139,445,539 etc)
*
* -r for using a custom return address.
*
* -t to select target type (Offset) , this includes universal offsets for -
*    win2k and winXP (Regardless of service pack)
*
* -l to select bindshell port on remote machine (Default: 666)
*
* - Shellcode has been modified to call ExitThread, rather than ExitProcess,
thus
*   preventing crash of RPC service on remote machine.
*
*   This is provided as proof-of-concept code only for educational
*   purposes and testing by authorized individuals with permission to
*   do so.
*/
```

在测试过这个exploit后发现，其实研究后我们可以发现可以在所有Win2000和WinXP上的RET地址，这就解决了判断目标系统版本的问题，直接可以使用一种数据包成功攻击所有Win2000/WinXP。
我们只要简单的修改一下该exploit, 使之能自动产生随机IP地址，然后对这个IP进行攻击尝试，就可以完成worm的攻击模块。或者你可以先生成一个随机的C类地址，然后扫描这个C段里有多少机器是开放135端口的，然后从扫描结果里取数据，并对这个IP实行攻击尝试，可以加快传播的速度。这些其实修改起来其实非常的容易。

2. 通过过替换攻击代码的shellcode部分，爱好者很容易能够在目标机器上执行任意命令和功能。比如简单的在主机上添加一个管理员用户，开一个shell端口，反连一个shell或者使计算机自动从某一个FTP或者HTTP服务器自动下载程序并执行等。然后想要进一步深入，就可以在采用合适完美的shellcode上来做文章，达到最大的传播效果。如exec command shellcode, bind port shellcode, connect back shellcode, down file and exec shellcode, down url file and exec shellcode等，你容易在网上找到它，如hsj的ida溢出exploit里就有一个down file and exec shellcode等。这个有汇编基础的攻击者很容易实现。这里对上面谈到的shellcode类型分别做一个简单的比较，以找出RPC DCOM最可能利用的传播途径。

a. 通过添加一个管理员用户，可以很容易的用Netbios共享来远程共享传播文件。但有对防火墙过滤了Netbios或者主机上不存在共享的情况下，不大好利用，而且，RPC DCOM的攻击代码溢出后获得的是system权限，想直接通过shellcode或者下载的程序来远程用Netbios拷贝文件比较困难，需要有一个system to user的权限转换模块，所以为了更高效的利用这个漏洞，达到传播快和速度大的 RPC DCOM 蠕虫不大可能利用这种技术。

b. 直接把命令写进shellcode里的话，简单快捷。甚至可以把所有需要用到的功能全写进

shellcode里去，如年初扫荡全球的sql worm， 把攻击，感染，传播三个模块写到短短的200多个16进制代码里实现。同样可以在里面加上下载程序并执行等功能。

c. 简单的开一个bind port shell, 你可以执行系统命令，比如echo写入一个脚本下载FTP站点里的程序并执行，甚至直接用TFTP下载程序等。这种方法执行命令，很简单，但每次攻击需要有两个连接，对系统开销比较大，而且可能受防火墙的影响也比较大，不宜采取。

d. 反连的shellcode跟bind port shell差不多，不过这个可以把反连的这个监听端口做成一个server形式，以便于接受多个连接，然后自动对每一个连接发送一些指令，使机器能完成传播。这个其实也是不错的，能突破不少防火墙，唯一的就是对禁止任何反连的防火墙没什么好办法。

e. 还记得hsj的ida溢出的exploit吧，该exploit监听一个端口，对目标溢出攻击成功后，目标系统反连攻击机的这个端口接受一个指定的文件并保存在本机硬盘上，然后执行，这其实跟反连shellcode差不多，只是一个是反连一个shell，另一个是反连回来取文件。这应该是蠕虫作者考虑中的传播途径。

f. 把程序放在某一个域名或者IP的FTP/HTTP站点里，所有感染的机器从这里取程序，下载到本地后执行。这种方法的好处是实现简单，而且可以很好的绕过防火墙，因为大多数的网络还是允许往外访问21/80端口的，而且可以很好的控制worm的版本和传播，把文件删掉就不会感染其他机器了，一般用于小规模感染。因为大规模感染的情况下，第一个倒下的是你的FTP/HTTP服务器。:)

g. Redcode/nimda的tftp下载程序方法，可以用在防火墙没有屏蔽udp的网络情况下，缺点是tftp传送文件太慢。居于Redcode/nimda的成功先例，这应该是蠕虫作者考虑中的传播途径。

h. 你自己自由发挥想象力．．．

3. 如果RPC DCOM蠕虫，采用结合以上各种方法的优势，就可以完善一个能突破大多数防火墙的繁殖方式来，以使蠕虫能更好更快的得到传播，通过结合利用Redcode和nimda的相关技术，利用Redcode和nimda相同的tftp传播方法，尝试从攻击IP里tftp里下载一个程序，如果下载成功的话就执行，如果不成功，可以反连至该攻击IP的某一个端口接受文件，如果再不成功，可以开一个端口接收文件，再不成功，可以从FTP/HTTP站点下载文件．．．不过也得考虑你的shellcode的长度哦，呵呵。更多的，你自己自由发挥想象力．．．

4. 加大蠕虫传播的途径，还可以考虑nimda的email, html, netbios共享等方法来进行繁殖和传播，做到这一点就可以把RPC DCOM做成一个继nimda后的第二个超级蠕虫。

5. 甚至可以结合病毒技术，感染exe文件，加大传播途径，做到这一点，RPC DCOM worm肯定是一个超过nimda的超级蠕虫。

6. 功能模块中，还可以加上木马功能或者DDoS功能，比如所有感染的机器同时向whitehouse，microsoft或者其他网站网站进行DDoS攻击，以完成更大的杀伤力。

7. 如果RPC DCOM worm通过UDP/135进行传播, 估计网络又会一片阻塞。

十 RPC DCOM 蠕虫爆发前的防治工作

1. 为自己的主机打上微软发布的相关修补补丁。下面为补丁的相关下栽地址 ：

Windows NT 4.0 Server：
http://microsoft.com/downloads/details.aspx?FamilyId=2CC66F4E-217E-4FA7-BDBF-DF77A0B9303F&displaylang=en

Windows NT 4.0 Terminal Server Edition ：
http://microsoft.com/downloads/details.aspx?FamilyId=6C0F0160-64FA-424C-A3C1-C9FAD2DC65CA&displaylang=en

Windows 2000：
http://microsoft.com/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=en

Windows XP 32 bit Edition：
http://microsoft.com/downloads/details.aspx?FamilyId=2354406C-C5B6-44AC-9532-3DE40F69C074&displaylang=en

Windows XP 64 bit Edition：
http://microsoft.com/downloads/details.aspx?FamilyId=1B00F5DF-4A85-488F-80E3-C347ADCC4DF1&displaylang=en

Windows Server 2003 32 bit Edition：
http://microsoft.com/downloads/details.aspx?FamilyId=F8E0FF3A-9F4C-4061-9009-3A212458E92E&displaylang=en

Windows Server 2003 64 bit Edition：
http://microsoft.com/downloads/details.aspx?FamilyId=2B566973-C3F0-4EC1-995F-017E35692BC7&displaylang=en

2. 向用户宣传此漏洞的严重性和被蠕虫利用的危害性，促使用户修补该漏洞。

3. 在自己的路由器上封掉 TCP/135，UDP/135，甚至 TCP/139，UDP/139，TCP/445，UDP/445等RPC DCOM能利用的相关端口， 以阻断蠕虫的攻击和传播。

*** 花了两小时来写这篇文章, 此文仅用于表达我对 RPC DCOM 蠕虫的设想! :) ***

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net