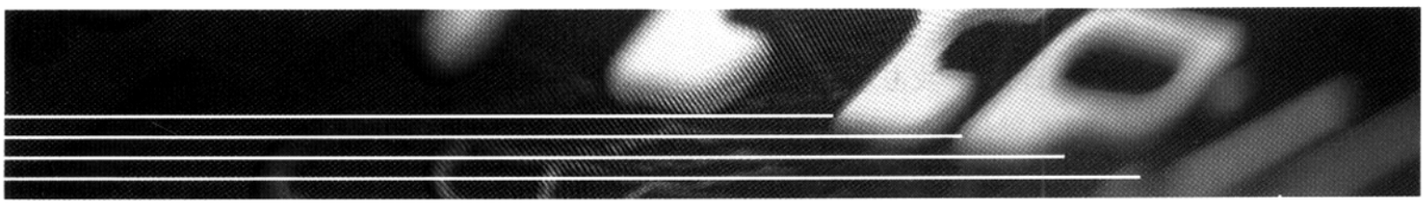

网络安全检测的理论和实践(二)

卿斯汉 (中科院信息安全技术工程研究中心 100080)

3 拒绝服务攻击

拒绝服务攻击-DoS (Denial of Service)是一种破坏性的攻击方法,其目的旨在使目标主机陷入停顿或无意义的繁忙,从而使合法用户无法使用资源,造成网络效率降低甚至瘫痪。

3.1 同步包风暴 (SYN Flooding)

同步包风暴是应用最广泛的一种DoS攻击方式,它的原理虽然简单,但使用起来却十分有效。

TCP连接时,根据3次握手协议连接的发起方C (Client) 先给连接对方S (Server) 发送一个SYN包,然后S发回一个SYN+ACK包,并等待C发送的第2个包。如果C的这个包到来,则TCP连接成功建立。S上的守护进程的accept调用返回"连接好的套接字描述符" (Connected Socket Descriptor),该连接则从S的等待队列中移出,给新的连接让出位置。每当一个SYN包从客户端到来,连接处于等待建立期间,TCP必须创建一些内存结构。例如,在BSD UNIX上,创建了下列结构:

套接字 (socket{}): 保存TCP连接本地端有关信息,如使用的协议、状态信息、地址信息、连接队列、缓冲区和标志等。

Internet协议控制块 (inpcb{}): 保存一些TCP需要的特定信息,如TCP状态信息、IP地址、端口号、IP头原型、IP选项、指向路由表中目标地址的指针等。当一个基于TCP的服务器程序调用listen()时创建PCB结构。

TCP控制块 (tcpcb{}): 包含TCP的具体信息,如计时器信息、序列号信息、流量控制信息、OOB数据等。

此外,还有所谓"Backlog Queue"的数据结构,对每个SYN包,必须分配一个。它必须保留所有"建立过程中"的TCP连接和"建立好了"的TCP连接的信息,直到守护进程调用accept()把它们取到进程自己的空间里。"Backlog"系指这两种连接的总数限制,当队列中等待服务器处理的连接数已经达到系统限制后,TCP就会抛弃新来的SYN包,直到队列中重新出现空缺,否则不能接受新的TCP连接请求。

同步包风暴攻击的机理是,它作为伪装的客户端,不会发出最后一个ACK包,甚至它发出的第一个SYN包中的源地址也是伪造的,造成被攻击主机的TCP栈中堆积大量不可能得到应答的半开连接。它们在等待队列中拥挤着,等待不可能来到的第3次握手信号,一直等到超过系统规定的时间限制才被抛弃。同时,正常的TCP连接请求反而因为Backlog Queue被占满而被拒绝。

3.2 PING风暴 (PING Flooding)

PING风暴也是一种常用的DoS攻击方法,只要多人约定在某个时刻同时对目标主机使用ping程序,就可能耗尽目标主机的网络带宽和处理能力,造成网络效率急剧降低或瘫痪。

我们已经介绍过,ping用来确认特定主机是否通过网络可达。ping使用ICMP的ECHO_REQUEST数据报,并期待从目标主　这样就会每秒给目标主机ercist.com发送一个ECHO_REQUEST包。当然,需要多人同时运行这个命令。如果一个网站每秒收到数万个垃圾ECHO_REQUEST包,就可能使它过度繁忙而无法提供正常服务了。实际上,我们可以通过一个程序,以最快的速度往目标主机发送ECHO_REQUEST包,并且通过修改源IP地址,可以使目标主机将ECHO_REPLY包回送到别的地方。

3.3 UDP回声风暴 (UDP Echo Storming)

UNIX系统通常开放一些用来测试的端口,如echo(7)、chargen(19)等。echo服务简单地把客户端送去的每个字符回送给客户端,并且在遇到回车符后把整个一行回送。于是,客户端发送的每行输入会产生两行输出。chargen服务则按ASCII顺序往客户端发送可打印字符。如果我们用某种方式把这两个服务对接起来,chargen向echo发送一个填满ASCII字符的包,则echo双倍返还。Chargen再次发送新的包,echo又将其加倍。UDP包的数目以2的幂指数的速度增长,很快目标主机就被淹没在

自己制造出的垃圾包里了。

这就是UDP回声风暴的原理，这种攻击方法只需要用一个包去触发，被攻击的主机就会陷入一种自杀性的死循环，所以效率很高。此外，攻击时需要伪造一个从目标主机的ECHO端口发出，发往目标主机的CHARGEN端口的UDP包。对于一些新的操作系统，已经对UDP回声风暴加以防范。

3.4 电子邮件炸弹（E-mail Bomb）

电子邮件炸弹的目的是通过不断往目标E-mail地址发送垃圾邮件，占满收信者的邮箱，使其无法正常工作。邮件炸弹的原理是，连接到邮件服务器的SMTP（25）端口，按照SMTP协议发送几行头信息加上一堆文字垃圾，即算发送了一封邮件。反复多次，就形成邮件炸弹。

例如，下面是一封垃圾邮件。为区别起见，我们将输入的句子加粗。

```
$ telnet smtp.ercist.net smtp
Trying 2.4.6.8 ...
Connected to smtp.ercist.net.
Escape character is ' ]'.
220 smtp.ercist.net ESMTP
hello yahoo.com
250 smtp.ercist.net
mail from:abc@ercist.net
250 Ok
rcpt to: def@university.net
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
垃圾邮件内容
.
250 Ok: queued as 96FE61C57EA7B
quit
$
```

实际上，黑客冒充yahoo.com，请求smtp.ercist.net把一封自称来自abc@ercist.net的电子邮件，发送给def@university.net。显然，能够成功发送匿名邮件，是因为发送邮件时服务器不进行身份验证。一般的邮件炸弹可以用这种方法实现匿名，但是，这种方法并不能作到真正的匿名。例如，在Netscape Messenger中，在菜单中选择View-->Headers-->All，就可以看到完整的邮件头，其中有如下信息：

Received: from yahoo.com (hotmail.mail.com [1.2.3.4]) by smtp.ercist.net
(Postfix) with SMTP id 1499B1C659233 for
<def@university.net>; Fri, 8 Dec 2000 10:19:20 +0800
(CST)

由此可知，伪造源地址yahoo.com后面就是真实地址hotmail.mail.com。

KaBoom！是一种较为先进的邮件炸弹程序，它实现了一种所谓邮件列表炸弹。邮件列表是一种用电子邮件实现的论坛，列表本身有一个电子邮件地址。向该列表对应的电子邮件地址发送电子邮件时，所有加入该列表的用户都会收到这封邮件。这样，不需要依靠攻击程序发送邮件炸弹，这些邮件列表会代替攻击程序作这件事。这种攻击有两个特点：一是作到了真正的匿名，发送邮件的的是邮件列表。其二是难以避免这种攻击，除非被攻击者更换电子邮件地址，或者向邮件列表服务器申请退出。

此外，有一类计算机病毒，通过病毒传播的方法发送电子邮件炸弹。

3.5 Winnuke攻击

Winnuke攻击针对Windows 95/NT系统上一般都开放的139端口，这个端口由NetBIOS使用。只要往该端口发送1字节TCP OOB数据，就可以使Win 95/NT系统出现“蓝屏”错误，并且网络功能完全瘫痪。除非重新启动，否则不能再用。

“带外数据”OOB（Out of Band），系指TCP连接中发送的一种特殊数据，它的优先级高于一般的数据。带外数据在报头中设置了URG标志，可以不按照通常的次序进入TCP缓冲区，而是进入另外一个缓冲区，立刻可被进程读取；或者可以根据进程的设置，直接用SIGURG信号通知进程有带外数据到来。

进行这种攻击时，先创建套接字sock，然后连接到目标主机的139端口，最后，执行下述程序：

```
char c = 'X';
send (sock , &c, 1, MSG_OOB);
```

在send最后一个参数flags中设置成MSG_OOB，就能发送带外数据。

3.6 Land攻击

Land攻击的机理是，向目标主机的某开放端口（如113、139）发送一个TCP包，并伪造TCP/IP源地址，使源IP等于目的IP，源端口等于目的端口。这样，就可以使包括Windows 95在内的许多平台上的主机死锁。这些平台包括：

BSDI 2.1	FreeBSD 2.2.2-RELEASE
FreeBSD 2.2.5-RELEASE	FreeBSD 2.2.5-STABLE
FreeBSD 3.0-CURRENT	HP-UX 10.20

MacOS 8.0	NetBSD 1.2
NeXTSTEP 3.0	NeXTSTEp 3.1
OpenBSD 2.1	Solaris 2.5.1
SunOS 4.1.4	Windows 95

3.7 分布式拒绝服务(DDoS：Distributed Denial of Service)

分布式拒绝服务系指，同时从多个不同的地点向某一特定目标发起拒绝服务攻击。 DDoS是DoS的最新形式，约在1999年下半年出现。1999年6－7月间，黑客组织攻击了一个由2000台以上分布在世界各地的主机组成的网络。同年8月，又攻击了美国明尼苏达大学的服务器，造成瘫痪。2000年2月初，黑客集中攻击了Yahoo、eBay、Amazon、Buy、CNN等一系列世界著名网站，造成损失达12亿美元。

DDoS引入分布式攻击和Client/Server结构，使DoS的威力以数十倍的程度激增。同时，DDoS囊括了已经出现的各种重要的DoS攻击方法。因此，DDoS比DoS的危害性更大。

现有的DDoS工具一般采用三级结构，如图1所示。

其中，Client（客户端）运行在黑客的主机上，用来发起和控制DDoS攻击。Handler（主控端）运行在已被黑客侵入并获得控制的主机上，用来控制代理端。Agent（代理端）运行在已被黑客侵入并获得控制的主机上，从主控端接收命令，负责对目标实施实际的攻击。

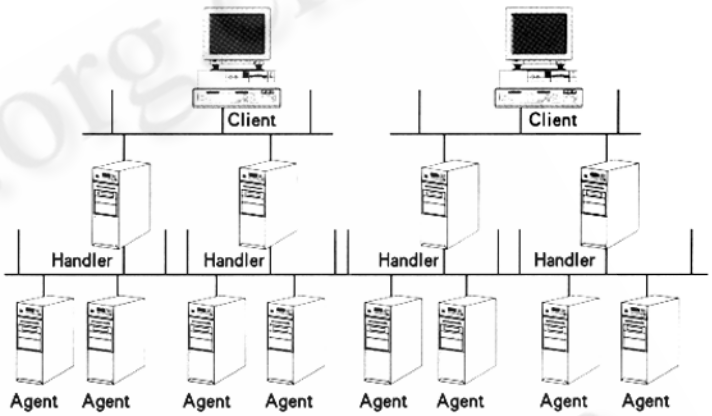

图 1 DDoS的三级控制结构

DDoS要获得成功，需要进行长期的准备工作。首先，黑客必须侵入并控制分布在世界各地的大量主机，在它们上面编译安装Handler和Agent，并使它们持续地活动。这一步骤称之为，“构造攻击网络”。其次，黑客在自己的机器上操纵客户端，将控制命令发往各个主控端。最后，再由主控端间接地控制代理端，发起DDoS攻击。

目前，主要的DDoS工具有：Trinoo、TFN（Tribe Flooding Network）、Staecheldraht等。其中，Trinoo的DDoS攻击程序已经在全世界构造了主机数大于2000台的攻击网络。■

（未完待续）