□□DOS攻击原理及Linux环境下的防御方案

□□

摘要:在系统上有许多类型的侵袭，我们一般把侵袭分为三种基本类型:入侵、拒绝服务(DOS)和盗窃信息。网络诞生以来遭受攻击事件不断发生，全球许多著名网站都遭到不名身份的黑客攻击，本文针对几种常见的DOS攻击提出在LINUX环境下的一些防御看法。

□□1、DOS攻击概念

□□DoS是Denial of
Service的简称，即拒绝服务，造成DoS的攻击行为被称为DoS攻击，其目的是使计算机或网络无法提供正常的服务。最常见的DoS攻击有计算机网络带宽攻击和连通性攻击。带宽攻

□□

击指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求就无法通过。连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。如:

□□(1)试图FLOOD服务器，阻止合法的网络通讯

□□(2)破坏两个机器间的连接，阻止访问服务

□□(3)阻止特殊用户访问服务

□□(4)破坏服务器的服务或者导致服务器死机

□□

随着电子商业在电子经济中扮演越来越重要的角色，随着信息战在军事领域应用的日益广泛，持续的

□□

DoS攻击既可能使某些机构破产，也可能使我们在信息战中不战而败。可以毫不夸张地说，电子恐怖活

□□动的时代已经来临。所以了解和防御网络攻击至关重要。

□□2、DOS的几种常见攻击及防御对策

□□下面我们看看几种常见的DONS攻击方式及在LINUX环境中我们如何采取防御措施。

□□2.1 LAND 攻击

□□概述:
LAND攻击是网络上流行的攻击方式。它的攻击方案是将TCP的请求连接数据包的IP源地址和目的地址指定成一样的。我们知道，TCP连接要经过“三次握手”，只有连接确认之后才能

进行数据的传输。它将源和目的地址指定成一样的以后，会将系统陷入一个死循环中，从而导致目标机陷入死锁状态。

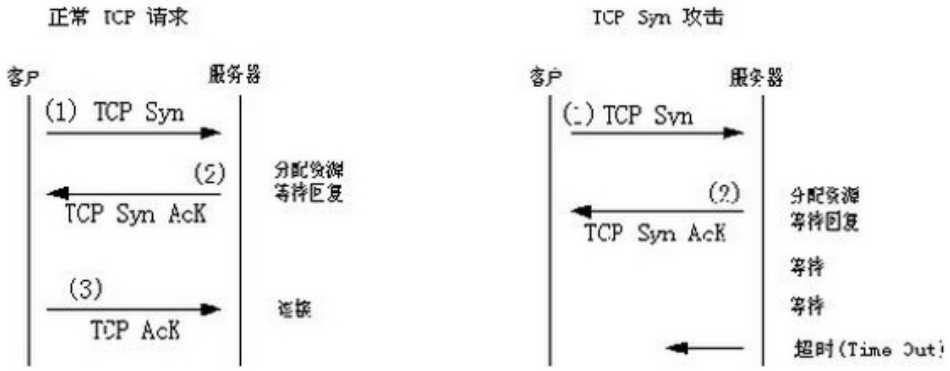
□□防御:
适当配置防火墙设备或过滤路由器的过滤规则就可以防止这种攻击行为(一般是丢弃该数据包)，并对这种攻击进行审计(记录事件发生的时间，源主机和目标主机的MAC地址和IP地址)。判断该项攻击的方法其实很简单，只需要判断IP的源与目的地址是否一致，以下是防御LAND攻语言:

□□if((tcph->syn)&&(sport==dport)&&(sip==dip))//判断源和目地地址是否相等{
printk("maybe land attack \n");//报警}

□□……//继续将包匹配下一条规则

□□2.2 SYN FLOOD攻击及防范

概述:SYN
Flood是当前最流行的DoS(拒绝服务攻击)与DDoS(分布式拒绝服务攻击)的方式之一，它是一种利用TCP协议缺陷，发送大量伪造的TCP连接请
求，从而使得被攻击方资源耗尽(CPU满负荷或内存不足)的攻击方式。漏洞在于TCP协议连接三次握手过程中，当每个TCP建立连接时，都要发送一个带
SYN标记的数据包，如果在服务器端发送应答包后，客户端不发出确认，服务器会等待到数据超时，如果大量的带SYN标记的数据包发到服务器端后都没有应
答，会使服务器端的TCP资源迅速枯竭，导致正常的连接不能进入，甚至会导致服务器的系统崩溃。



□□(图一 TCP Syn攻击示意图)

□□问题就出在TCP连接的三次握手
中，假设一个用户向服务器发送了SYN报文后突然死机或掉线，那么服务器在发出SYN+ACK应答报文后是无法收到客户端的ACK报文的(第三次握手无法
完成)，这种情况下服务器端一般会重试(再次发送SYN+ACK给客户端)并等待一段时间后丢弃这个未完成的连接，这段时间的长度我们称为SYN
Timeout，一般来说这个时间是分钟的数量级(大约为30秒-
2分钟);一个用户出现异常导致服务器的一个线程等待1分钟并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非 常多的资源----
数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的CPU时间和内存，何况还要不断对这个列表中的IP进行SYN+ACK的重
试。实际上如果服务器的TCP/IP栈不够强大，最后的结果往往是堆栈溢出崩溃---
即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的
TCP连接请求而无暇理睬客户的正常请求(毕竟客户端的正常请求比率非常之小)，此时从正常客户的角度看来，服务器失去响应。

□□一般来说，如果一个系统(或主机)负荷突然升高甚至失去响应，使用Netstat
命令能看到大量

□□
SYN_RCVD的半连接(数量>500或占总连接数的10%以上)，可以认定，这个系统(或主机)遭到了SYN Flood攻击。

□□防御:

□□第一种是缩短SYN Timeout时间。由于SYN
Flood攻击的效果取决于服务器上保持的SYN半连接数，这个值=SYN攻击的频度 x SYN
Timeout，所以通过缩短从接收到SYN报文到确定这个报文无效并丢弃改连接的时间。

□□第二种方法是设置SYN
Cookie，就是给每一个请求连接的IP地址分配一个Cookie，如果短时间内连续受到某个IP的重复SYN报文，就认定是受到了攻击，以后从这个IP地址来的包会被丢弃。

□□可是上述的两种方法只能对付比较原始的SYN Flood攻击，缩短SYN
Timeout时间仅在对方攻击频度不高的情况下生效，SYN
Cookie更依赖于对方使用真实的IP地址，如果攻击者以数万/秒的速度发送SYN报文，同时利用SOCK_RAW随机改写IP报文中的源地址，以上的 方法将毫无用武之地。

□□2.3 Smurf攻击及防范

□□概览:Smurf攻击并不十分可怕;它仅仅是利用IP路由漏洞的攻击方法。攻击者向网络广播地址发送ICMP包，并将回复地址设置成受害网络的广播地址，通过使用ICMP应答请求数据包来淹没受害主机的方式进行，最终导致该网络的所有主机都对
次ICMP应答请求作出答复，导致网络阻塞。更加复杂的

□□Smurf攻击攻击将源地址改为第三方受害者，最终导致第三方崩溃。

□□

防御：为了防止黑客利用你的网络攻击他人，关闭外部路由器或防火墙的广播地址特性。为防止被攻击，在防火墙上设置规则，丢弃掉ICMP包。

□□(1)配置路由器禁止IP广播包进网，命令为：no ip directed-broadcast

□□

(2)配置网络上所有计算机的操作系统，禁止对目标地址为广播地址的ICMP包响应。我们可以在

□□LINUX的IPTABLE模块加入利用下面命令实现：

□□iptables –A –I eth0 -s 172.30.4.0/16–P icmp –j DROP

□□

(3)通过在路由器上使用输出过滤，你就可以滤掉这样的包，从而阻止从你的网络中发起的Smurf攻击。

□□在路由器上增加这类过滤规则的命令是：

□□Access-list 100 permit IP {你的网络号} {你的网络子网掩码} anyAccess-list 100 deny IP any any

□□(4)被攻击目标与ISP协商，有ISP暂时阻止这些流量。

□□2.4 IP欺骗原理和防范

IP欺骗也是针对TCP/IP协议的缺陷。我们先来看看IP欺骗的过程

□□(图二:IP伪装示意图)

□□

我们先做以下假定：首先，目标主机已经选定。其次，信任模式已被发现，并找到了一个被目标主机信任的主机。

□□黑客为了进行IP欺
骗，进行以下工作：使得被信任的主机丧失工作能力，同时采样目标主机发出的

□□TCP
序列号，猜测出它的数据序列号。然后，伪装成被信任的主机，同时建立起与目标主机基于地址验证的应用连接。如果成功，黑客可以使用一种简单的命令放置一个
系统后门，以进行非授权操作。

□□
要通过包过滤防火墙的过滤规则来阻挡IP欺骗的攻击，几乎是不可能的，因而我们设计了强大的身份验证来抵御这种攻击。

□□有一种设计方案：当一个IP数据包从一个网络内
部机器到另一内部机器，但这个数据包却通过外部网络通向内部网络的入口进入，同时，我们通过包过滤和分析IP报头，可以知道该数据包有两个源地址。其中一
个是伪IP源地址。这样我们就毫不犹豫地断定我们受到了IP欺骗的攻击。在处理时，我们立即丢弃该数据包，并把记录写入日志文件中。

□□关于这一点，请看类C语言：

□□If (IP 数据包入站){

□□If (iphdr->SrcAddr 属于本地网络&&

□□Iphdr->DstAddr属于本地网络){

□□丢弃IP数据包;

□□作日志纪录;

□□}

□□else{使用出站或转发规则过滤数据包;}

□□事实上LINUX内核本身支持防范IP欺骗得功能，我们可以用下面的命令：

□□ech0 1>/proc/sys/net/ipv4/conf/eth0/rp_filter

□□3、结束语

□□
当网络中应用新的安全技术后，恶意用户的攻击技术也深入改造，变异。此时就需要网络管理人员或用户的细心发现计算机是否有异常情况，如反应变慢、非
法连接数据、莫名程序及莫名用户等。为了能自动化防守计算机，相关人氏建议在安全策略上要做到精、细、准，在软件应用上要调节安全度，并提写相关日志文
件，安装必备的防火墙，做好前置工作，才能以逸待劳!