

SYN Flood 攻击防御系统的研究与实现

潘燕华 查春霞 张丙凡¹ 田宗洲

(江苏科技大学经济管理学院,电子信息学院¹,镇江 212003)

摘要 针对 SYN Flood 攻击常用的防御方法存在的一些弊端,从仿真模拟攻击测试的角度,设计了一种应对 SYN Flood 攻击的防御系统。首先介绍了 SYN Flood 的攻击原理,提出了防御系统的设计和实现方案;在此基础上,根据攻击防御测试的目标和内容,实施了仿真模拟攻击及防御;并详细介绍了攻击及防御实施的过程。实验结果表明此系统能够有效的防御 SYN Flood 攻击,具有一定的实用性。

关键词 SYN Flood 攻击 防御 入侵防御

中图法分类号 TP393.08; **文献标志码** A

SYN Flood 是当前最流行的 DOS 与 DDOS 攻击的方式之一,也是一种非常流行的利用协议漏洞的资源匮乏型攻击,它是用“合理”的服务请求来占用过多的服务资源,致使服务器超载,无法响应其它的请求。SYN Flood 攻击对网络破坏力惊人,广泛受到网络安全业界的关注^[1]。目前常用的一些防御手段,比如缩短应答等待时间,或者是对 TCP 协议做一些修改,但是这些应对方法在实现过程中均存在一定的问题。鉴于此,本文通过对 SYN Flood 仿真模拟攻击测试,提出了一种应对 SYN Flood 攻击的有效防御体系。

1 SYN Flood 攻击防御系统设计

1.1 SYN 通信及攻击原理

SYN 通信原理就是 TCP 三次握手:首先客户端发送一个包含 SYN 标志的 TCP 报文,同步报文会指明客户端使用的端口以及 TCP 连接的初始序号;服务器在收到客户端报文后,将返回一个 SYN + ACK 的应答报文,表示客户端的请求被接受,同时 TCP 序号被加一;最后客户端也返回一个确认报文 ACK

给服务器端,同样 TCP 序列号被加一,到此一个 TCP 连接完成^[1]。SYN Flood 攻击原理是利用 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的攻击方式。具体过程就是:客户端疯狂发送 SYN 报文,在服务器收到并发出应答报文后,客户端不返回确认报文,致使第三次握手无法完成。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服务器最终因占用过多资源,没有能力响应别的操作,此时从正常客户的角度来看,服务器失去响应,这种情况就称服务器端受到了 SYN Flood 攻击^[2-4]。

1.2 SYN Flood 攻击防御策略

从防御角度来说,目前常用的方法主要有:缩短 SYN Timeout 时间、设置 SYN Cookie,但是这两种方法只能对付比较原始的 SYN Flood 攻击,想有效地防御 SYN Flood 攻击,在服务器遭受攻击的同时,一方面要能检测出攻击行为,并及时响应;另一方面,还应该努力追踪出攻击源,为彻底遏制攻击提供帮助。为此,本文提出了一种应对攻击的防御体系:在服务器端分别设置 SYN Flood 攻击监听器、攻击分析器、攻击类型数据库、防御响应器。当遭遇 SYN Flood 攻击时,能通过监听器侦察到,再通过分析器触动防御响应器,及时地采取防御措施。

2009年10月12日收到

第一作者简介:潘燕华(1963—),女,汉族,江苏南通人,江苏科技大学教授,研究方向:管理信息系统,企业模型。

1.3 SYN Flood 攻击防御系统结构

1.3.1 系统设计的目标

(1) 对网络、系统的运行状况进行监视,通过人或者第三方软件,发现各种攻击企图、攻击行为,监测网络行为的合法性,以保证网络系统资源的机密性、完整性和可用性;

(2) 及时地判断或辨别出攻击行为,在发现攻击行为以后要能够对其作出分析并及时响应。

1.3.2 防御系统结构

根据 SYN Flood 攻击防御的策略以及攻击防御的系统结构设计的目标,系统结构图设置如图 1 所示。

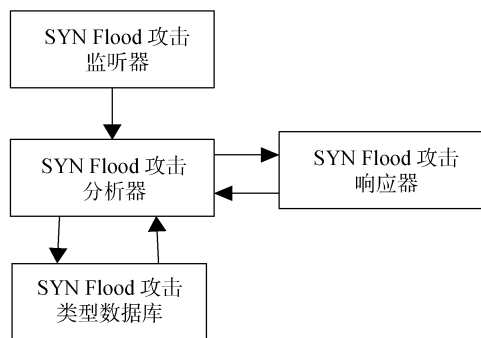


图 1 SYN Flood 攻击防御系统结构图

(1) SYN Flood 攻击监听器

监听器的工作原理就是接收、监视网段上的所有数据包。SYN Flood 攻击监听器应当挂接在所有所关注的流量都必须流经的链路上,此处“所关注流量”指的是来自高危网络区域的访问流量和需要进行统计、监视的网络报文,从中接收数据包,对网络系统进行实时监测,以发现来自系统外的入侵者,为计算机系统提供完整、可控、可信的主动保护;并将接收的数据包信息传送给 SYN Flood 攻击分析器^[5]。

(2) SYN Flood 攻击分析器

攻击分析器是整个防御体系的核心,其作用在于:一方面,对监听器传来的数据包进行分析,从而识别出是否存在攻击行为,并将结果反馈给响应器;另一方面将分析结果等信息储存于攻击类型数据库。数据包分析过程就是进行入侵检测规则的匹

配,匹配的过程就是对捕获的报文同构造的规则树进行比较的过程。如果发现存在一条规则匹配这个报文,就表示检测到一个攻击,并执行触动警报的操作。如果搜索完所有的规则都没有在这个数据包中找到匹配的内容,就说明报文正常。

(3) SYN Flood 攻击类型数据库^[6]

主要存储分析器所分析的数据包的相关有用信息,包括捕获到的数据包等,建立规则库文件记忆各种用户策略,方便系统的管理和使用;同时管理人员通过查看攻击类型数据中获取原始的数据信息,整理、归并到关系数据库中,并进行定期分析生成新的网络轮廓,一经确认可以更新分析器中的特征库。

(4) SYN Flood 防御响应器

响应器的功能就是在分析器检测到入侵行为并触动警报操作后,响应器要能够做出各种形式的反应,如通知管理员、拦截、反击或自行切断网络等。

2 SYN Flood 攻击防御仿真

实验仿真的环境是在同一局域网内进行的,由相互通信的不同主机甲、乙分别代表被攻击方和攻击方进行模拟仿真 SYN Flood 攻击实验,实验目的是为了验证上述防御体系的有效性。

2.1 SYN Flood 攻击的仿真

2.1.1 攻击目标和内容

乙对甲实施 SYN Flood 仿真模拟攻击主要包括两方面的内容:

(1) 对受保护系统实施 SYN Flood 攻击,检测攻击行为的有效性;

(2) 测试甲对 SYN Flood 攻击的响应能力。

2.1.2 攻击的实现

(1) 查找主机甲开放的端口

在乙上安装流光软件,利用流光软件查看局域网中指定主机甲的开放端口。查找结果甲开放了 80 端口。

(2) 利用 Hgod 对甲发动 SYN Flood 攻击

Hgod 具有 SYN/DrDos/UDP/ICMP/IGMP 拒绝服务测试功能,利用 Hgod 软件,启动 win - dos:运行

放在 d 盘下的 Hgod, 操作命令为: d: > hgod 192.168.6.183 80 -m: drdos -t: 10 -s: 192.168.6.2 -n: 200。其中: 192.168.6.183 为目标主机 IP; 80 为目标主机开放的端口; -m 为攻击方式, 在此向甲发动 DDOS 攻击; -t 发动攻击时间间隔的时间; -s 为攻击源主机 IP; -n 为动态分配源主机个数。

2.1.3 攻击结果

仿真攻击实施后, 在局域网中的其他主机上打开连接甲站点, 已经无法显示该网页, 表明攻击成功。

2.2 SYN Flood 防御仿真

2.2.1 防御的目标和内容

甲的防御工作主要包括两方面的内容:

(1) 能够检测 SYN Flood 攻击并作出反应;

(2) 及时实施有效的防御手段, 采取相应的防护措施。

2.2.2 防御的具体实现过程

本文采用 OmniPeek 抓包软件来模拟防御实验。甲通过监听器监控来访信息, 并通过分析器分析来访包信息, 对甲实施相应的防护措施。

(1) 启动甲的安全防御系统, 本实验中启动 OmniPeek 抓包软件实时监控甲的通信信息, 并查看通信协议类型, 包大小, 持续时间长度。观察 Source 和 Protocol 及 Summary 信息如图 2 所示。

(2) 当乙向甲发动 SYN Flood 攻击时, 甲监听器立即监测到自身不断地接收 HTTP 协议请求, 而且每隔很短的时间发生一次。因此预测有攻击行为, 此时的通信信息如图 3 所示。

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
1322	WORKGROUP	IP-192.168.6.69		78	0:02:05.785137	PING Reply	Echo Reply: 192.168.6.69
1323	IP-192.168.6.233	IP-192.168.6.255		96	0:02:05.928172	NB Name Svc	C QUERY NAME=MAIL.FUCUZZY <00>
1324	IP-192.168.6.69	WORKGROUP		78	0:02:06.297712	PING Req	Echo: WORKGROUP
1325	WORKGROUP	IP-192.168.6.69		78	0:02:06.297752	PING Reply	Echo Reply: 192.168.6.69
1326	IP-192.168.6.69	WORKGROUP		78	0:02:06.465737	PING Req	Echo: WORKGROUP
1327	WORKGROUP	IP-192.168.6.69		78	0:02:06.465773	PING Reply	Echo Reply: 192.168.6.69
1328	IP-192.168.6.233	IP-192.168.6.255		96	0:02:06.679188	NB Name Svc	C QUERY NAME=MAIL.FUCUZZY <00>
1329	IP-192.168.6.69	WORKGROUP		78	0:02:06.788962	PING Req	Echo: WORKGROUP
1330	WORKGROUP	IP-192.168.6.69		78	0:02:06.789004	PING Reply	Echo Reply: 192.168.6.69
1331	IP-192.168.6.69	WORKGROUP		78	0:02:07.322243	PING Req	Echo: WORKGROUP
1332	WORKGROUP	IP-192.168.6.69		78	0:02:07.322287	PING Reply	Echo Reply: 192.168.6.69
1333	IP-192.168.6.69	WORKGROUP		78	0:02:07.469651	PING Req	Echo: WORKGROUP
1334	WORKGROUP	IP-192.168.6.69		78	0:02:07.469705	PING Reply	Echo Reply: 192.168.6.69
1335	IP-192.168.6.69	WORKGROUP		78	0:02:07.798902	PING Req	Echo: WORKGROUP
1336	WORKGROUP	IP-192.168.6.69		78	0:02:07.798946	PING Reply	Echo Reply: 192.168.6.69
1337	IP-192.168.6.69	WORKGROUP		78	0:02:08.323225	PING Req	Echo: WORKGROUP
1338	WORKGROUP	IP-192.168.6.69		78	0:02:08.323270	PING Reply	Echo Reply: 192.168.6.69

图 2 甲的通信信息

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
16124	IP-192.168.6.69	WORKGROUP		136	0:05:31.694872	HTTP	C PORT=2073 HEAD /scripts/tools HTTP/1.1
16125	IP-192.168.6.69	WORKGROUP		138	0:05:31.695104	HTTP	C PORT=2074 HEAD /scripts/samples HTTP/1.1
16126	WORKGROUP	IP-192.168.6.69		221	0:05:31.695259	HTTP	R PORT=2073 HTML Data
16127	WORKGROUP	IP-192.168.6.69		221	0:05:31.695476	HTTP	R PORT=2074 HTML Data
16128	WORKGROUP	IP-192.168.6.69		64	0:05:31.695593	HTTP	Src= 80, Dst= 2073, A...F, S=3773990086..
16129	WORKGROUP	IP-192.168.6.69		64	0:05:31.695742	HTTP	Src= 80, Dst= 2074, A...F, S=2622496363..
16130	IP-192.168.6.69	WORKGROUP		64	0:05:31.695774	HTTP	Src= 2073, Dst= 80, A..., S=2401596836..
16131	IP-192.168.6.69	WORKGROUP		64	0:05:31.695961	HTTP	Src= 2074, Dst= 80, A..., S=2423777536..
16132	IP-192.168.6.69	WORKGROUP		264	0:05:31.696908	CIFS	C Session setup and X
16133	WORKGROUP	IP-192.168.6.69		405	0:05:31.712700	CIFS	R Session setup and X Status=More proce..
16134	WORKGROUP	IP-222.79.101.169		75	0:05:31.757072	UDP	Src=19629, Dst=19503, L= 29
16135	IP-192.168.6.69	WORKGROUP		66	0:05:31.787049	HTTP	Src= 2076, Dst= 80, ..., S=1703960812..
16136	WORKGROUP	IP-192.168.6.69		66	0:05:31.787098	HTTP	Src= 80, Dst= 2076, A...S, S=3536818371..
16137	IP-192.168.6.69	WORKGROUP		64	0:05:31.787310	HTTP	Src= 2076, Dst= 80, A..., S=1703960813..
16138	IP-192.168.6.69	WORKGROUP		66	0:05:31.787554	HTTP	Src= 2077, Dst= 80, ..., S=1580243195..
16139	WORKGROUP	IP-192.168.6.69		66	0:05:31.787580	HTTP	Src= 80, Dst= 2077, A...S, S=3250739608..
16140	IP-192.168.6.69	WORKGROUP		64	0:05:31.787741	HTTP	Src= 2077, Dst= 80, A..., S=1580243196..
16141	IP-192.168.6.69	WORKGROUP		135	0:05:31.802422	HTTP	C PORT=2077 HEAD /scripts/perl HTTP/1.1
16142	IP-192.168.6.69	WORKGROUP		144	0:05:31.802514	HTTP	C PORT=2076 GET /scripts/...%25Sc../win...

图 3 受到攻击后甲的通信信息

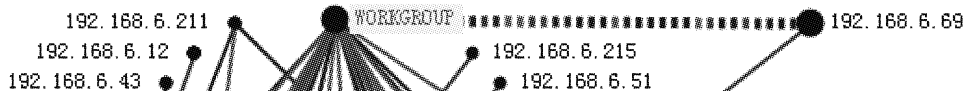


图4 甲受到攻击后 Peer Map 图

同时,在 Peer Map 图形中可以观察到如图 4 所示的信息。主机:192.168.6.69 频频和主机 WORKGROUP 建立通信。相断越多且越密,说明请求通信越频繁。

(3) 甲的响应措施:甲分析器在确定存在乙方的恶意攻击之后,并判断乙恶意向甲发动 HTTP 应答请求,此为 SYN Flood 攻击,触动响应器。采用 AnyView(网络警)软件,来阻断 Flood 攻击。AnyView 提供了许多限制方法,如图 5 所示。本文利用

端口限制来拦截来自乙方的攻击。在端口限制中增加类型为 TCP,端口号为 80,且主机范围为乙的 IP 地址,即填写攻击方主机地址。

(4) 其他拦截措施,在甲上启动防火墙,过滤攻击源主机,使得在短暂时间内甲隔离攻击源。

2.2.3 防御结果

经过防御处理,查看进程状况,发现进程又恢复正常,说明甲的防御手段是行之有效的。

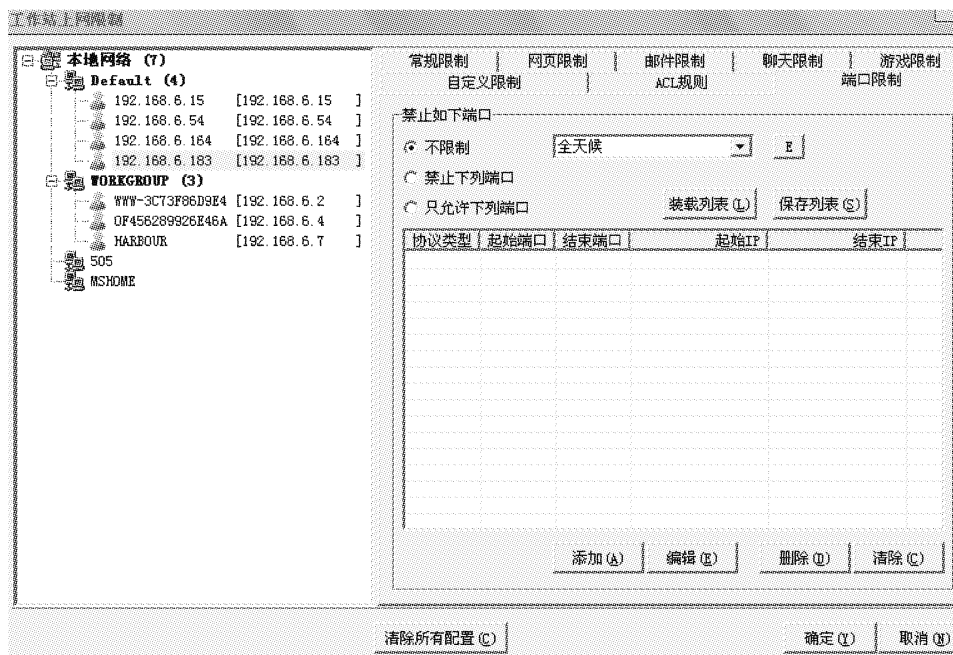


图5 防御攻击行为

3 小结

通过实验仿真模拟 SYN Flood 攻击,提出了一种 SYN Flood 攻击的防御系统,在实验中取得了较好的防御效果,希望有助于网络提高自身保护。仿真模拟的攻击及防御,对于企业保护自身免受攻击,具有一定的指导意义;这些研究内容对于防御其他

的 DOS 攻击也有一定的借鉴意义。

参 考 文 献

- 1 吴宏波. 关于 DDOS 中 SYN Flood 攻击的防御算法研究. 内蒙古科技与经济, 2007; (11): 287—288
- 2 (美) Kao M. 网络安全设计 (第二版). 吴中福, 译. 北京: 人民邮电出版社, 2005

(下转第 129 页)

The Analysis of Zero Inventory Drift Variant Based on DE-APVIOBPCS Model

HE Jia-ning, JIN Wen-zhou¹

(School of Business Administration and College of Traffic and Communications¹,
South China University of Technology, Guangzhou, 510641, P. R. China)

[Abstract] The DE-APVIOBPCS model with MMSE forecast for AR(1) demand in a single-echelon supply chain has first been described in control engineering perspective. By applying the Final Value Theorem, a final value offset (*i. e.* inventory drift) can be measured and does exist even though the actual lead-time is known. Thus to eliminate the inherent offset and keep the system variances acceptable, a new policy with zero inventory drift based on DE-APVIOBPCS model is presented. The analysis of the variance amplification suggests the lead-times conservatively in new policy should be always estimated. The general stability conditions for zero inventory drift variant are evaluated in succession and some valuable attributes of new policy are illustrated via simulation under the assumption that misidentification of lead-time is inevitable.

[Key words] lead-time estimation inventory drift variance amplification replenishment rule z -transform

(上接第 107 页)

- | | |
|---|--|
| <p>3 黄贻望, 万 良, 李 祥. 基于 IP 欺骗的 SYN 泛洪攻击. 计算机技术与发展, 2008;18(12):159—163</p> <p>4 (美) McClure S, Scambray J, Karty G. 黑客大曝光: 网络安全机密与解决方案(第五版). 王吉军, 张玉亭, 周维续, 译. 北京: 清华大学出版社, 2006</p> | <p>5 苏 明, 颜世峰. IPv6 校园网入侵检测系统设计. 小型微型计算机系统, 2009;(3):481—482</p> <p>6 沈 超. 分布式协同入侵检测系统模型的设计. 科技信息, 2008;(36):86—87</p> |
|---|--|

Research and Implementation of SYN Flood Attack Defense System

PAN Yan-hua, ZHA Chun-xia, ZHANG Bing-fan¹, TIAN Zong-zhou

(School of Economics and Management, School of Electronic Information¹,
Jiangsu University of Science and Technology, Zhenjiang Jiangsu 212003, P. R. China)

[Abstract] There are some shortcomings of the methods commonly used in defense of SYN Flood attack. In terms of attack simulation test, I designed a defense system to SYN Flood attack. Firstly, the principle of SYN Flood attack is introduced, and then put forward the design and realization of the defense system, on this basis, according to the objectives and content of the defense attacks test, carried out the simulation attack and defense. At last the implementation of the attack and defense is introduced in detail. The experimental results showed that this system can be an effective defense to SYN Flood attack, and had certain practical value.

[Key words] SYN Flood attack defence intrusion prevention