软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(Suppl.(2)):301−308

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

UDP 反射 DDoS 攻击的 BAF 分析*

周文烽[1,2], 丁 伟[1,2], 李 刚[1,2]

[1](东南大学 计算机科学与技术学院,江苏 南京 211189)

[2](江苏省计算机网络技术重点实验室(东南大学),江苏 南京 211189)

通讯作者: 周文烽, E-mail: wfzhou@njnet.edu.cn

摘 要: UDP 反射 DDoS 攻击由于实现简单、效果显著,已成为当前网络攻击的主要手段之一.带宽放大因子 BAF(bandwidth amplification factor)是评价放射攻击放大能力的主要测度.在考虑了 IP 分片报文的条件下采用全报文负载修改了 BAF 的计算公式,使其能够更加准确地反映反射攻击的放大能力.利用 NBOS(network behavior observation system)提供的 CERNET(中国教育与科研计算机网)中有 19、123、161、1900 端口反射行为的主机信息,通过攻击实验获取 BAF 值.在此基础上,对获取的 BAF 数据进行了统计和稳定性方面的分析.分析结果表明,19 与 123 端口的 BAF 总体比较大,但稳定性较差.利用分析的结果对所有放大器的危险程度进行了评价,危险程度高的放大器是在攻击防范中应该重点关注的对象.

关键词: 反射攻击;带宽放大因子;放大器;分片报文;数据分析

中文引用格式: 周文烽,丁伟,李刚.UDP 反射 DDoS 攻击的 BAF 分析.软件学报,2016,27(Suppl.(2)):301−308. http://www.jos.org.cn/1000-9825/16044.htm

英文引用格式: Zhou WF, Ding W, Li G. BAF analysis of UDP reflection DDoS attacks. Ruan Jian Xue Bao/Journal of Software, 2016,27(Suppl.(2)):301−308 (in Chinese). http://www.jos.org.cn/1000-9825/16044.htm

BAF Analysis of UDP Reflection DDoS Attacks

ZHOU Wen-Feng[1,2], DING Wei[1,2], LI Gang[1,2]

[1](School of Computer Science and Engineering, Southeast University, Nanjing 211189, China)

[2](Jiangsu Provincial Key Laboratory of Computer Network Technology (Southest University), Nanjing 211189, China)

Abstract: UDP reflection DDoS attacks have become one of the primary means of network attack because of its simple realization and significant effect. BAF(bandwidth amplification factor) is the main measure to evaluate the ability of amplification. In this paper, considering the condition of IP slice message, the whole message load is used to modify the formula of BAF, so that it can more accurately reflect the amplification ability of reflection attacks. This paper obtains the hosts with 19, 161, 123, 1900 port reflection behavior in the CERNET (China Education and Research Computer Network) by NBOS (network behavior observation system) to implement the attack test to get the BAF data. On the basis of this, the BAF data are analyzed in terms of statistics and stability. Analysis results show that the BAF of 19 and 123 port is relatively large, but the stability is poor. The paper also uses the results of the analysis to evaluate the risk degree of all amplifiers. Amplifiers with high degree of risk are usually used by the attacker and should be the focus of attention in attack prevention.

Key words: reflection attack; bandwidth amplification factor; amplifier; slice message; data analysis

互联网上的 UDP 反射 DDoS 攻击(以下简称反射攻击)从 2013 年开始形成规模.2013 年 3 月,世界反垃圾邮件组织 Spamhaus 遭受了峰值达到 300Gbit/s 的反射型 DDoS 攻击[1].攻击者向互联网上开放的 DNS 服务器发

* 基金项目: 国家自然科学基金(61602114)
Foundation item: National Natural Science Foundation of China (61602114)
收稿时间: 2016-06-05; 采用时间: 2016-10-18

送了对 ripe.net 域名的 ANY 型解析请求,并将请求的源 IP 伪造成 Spamhaus 的 IP 地址.在这次攻击中,DNS 请求数据的长度为 36 字节,而响应数据的平均长度为 3 000 字节,攻击者轻松地将流量放大了近 100 倍.2014 年 2 月,美国 CDN 服务提供商 CloudFlare 遭受了峰值达到 400Gbit/s 的反射型 DDoS 攻击[2].攻击者利用 NTP 协议中的 Monlist 命令将攻击流量放大了近 200 倍.2016 年 4 月,国家计算机网络应急技术处理协调中心发布的《2015 年我国互联网网络安全态势综述》也提及利用互联网传输协议的缺陷发起的反射型 DDoS 攻击日趋频繁,增加了攻击防御和溯源的难度[3].

UDP 反射 DDoS 攻击是利用有漏洞的应用层服务协议(以下简称服务协议)发起的 DDoS 攻击,这些服务均使用 UDP 作为传输协议.反射攻击用假冒源地址的服务请求报文发起.图 1 是这类攻击的一个场景.图中主机 1~*N* 开放了在 *X* 端口提供的存在漏洞的服务,这些主机也称为放大器.攻击者 A 向放大器的 *X* 端口发送以被攻击主机 O 为源地址的服务请求报文,所有放大器回复的报文被发送到被攻击主机 O,从而耗尽了被攻击主机 O 的带宽、达到拒绝服务目的.UDP 反射 DDoS 攻击因为无需组建僵尸网络、实现和控制过程更加简单、攻击源不易被跟踪等优势,使其迅速成为近来互联网上非常活跃的一类攻击手段[4].

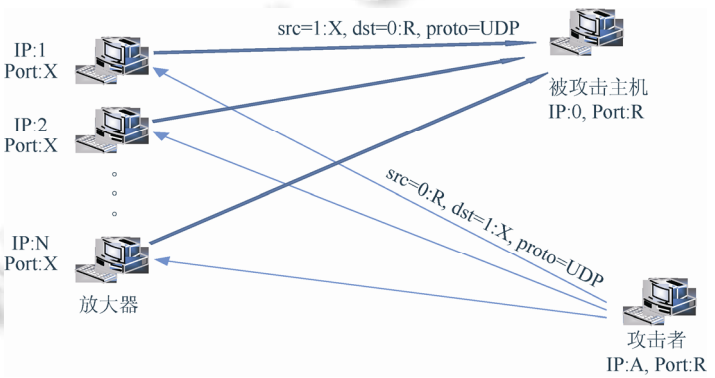

Fig.1 The scene of reflection attack[4]

图 1 反射攻击场景图[4]

为了评价反射攻击的效率,Rossow 提出了 BAF 的概念,并将其作为反射攻击放大系数的测量单位,同时给出了有关攻击实验的 BAF 结果[5].BAF 系数是评价放大器放大效率的主要依据.它具有随机性,同一台放大器在不同的攻击过程中的 BAF 也是会变化的,因此在可选择的条件下,攻击者更偏向于使用 BAF 系数大且稳定的放大器.

带宽放大因子 BAF 的相关研究不多,因为此类研究需要实测数据,具备完成相关的实验需要的环境和条件具有一定的难度.本文首先对文献[5]使用的 BAF 的计算公式进行了讨论和改进,在此基础上选择了 CHARGEN(19 端口)、NTP(123 端口)、SNMP(161 端口)、SSDP(1900 端口) 4 种可以产生反射攻击且在实际网络中有检测案例的协议,基于 CERNET 环境进行了获取 BAF 系数的攻击实验,随后对获取的 BAF 数据进行了统计分析和稳定性分析.在此基础上,综合考虑 BAF 数值大小和稳定性给出了一个放大器评价方法,可以将放大器分为轻微、关注、严重 3 种级别.关注和严重级别的放大器有较大的 BAF 系数并且 BAF 系数随着时间变化相对稳定,通常是攻击者偏向于利用的,也是在攻击防范中应该重点关注的对象.

1 服务协议与缺陷分析

UDP 反射 DDoS 攻击是利用有漏洞的服务协议发起的 DDoS 攻击.服务协议的漏洞是构建反射攻击命令的基础.本文研究的 4 种服务协议的漏洞产生的原因简单分析如下[6−11].

SNMPv2:该版本的 SNMP 协议引入了 snmpbulkget 功能支持用单个请求报文获得大量管理数据.攻击者向开启 SNMP 服务的网络设备发送 GetBulkRequest 请求.该服务使用 161 端口.

NTP:早期版本中的 monlist 请求功能支持客户端一次请求最多可获取 600 个与服务器同步的客户 IP 地址.攻击者向开放 NTP 服务的设备发送 get monlist 请求,该服务使用 123 端口.

SSDP:攻击者设置请求 SSDP 报头的 ST 字段为 all,即获得所有设备和服务的信息,该服务使用 1900 端口.

Chargen:Chargen 协议的设计中规定每当服务器收到一个 UDP 数据包后向客户端返回一个数据包,其中包含长度为 0~512 字节之间随机值的任意字符.虽然 RFC 864 对 Chargen 协议标准做出了说明,但许多系统的 UDP 回复报文超过了 512 字节的字符.该服务使用 19 端口.

基于上述原理,我们利用实验室本地主机的真实地址,向 CERNET 内的放大器发送了请求报文,获取回复报文.其中在 161 端口的 SNMP 和在 19 端口的 Chargen 的回复报文产生了分片.

2 BAF 相关工作与测度定义

BAF 和 PAF(packet amplification factor)的定义最早出现在文献[5]中,其计算方法如下(为区别于本文的计算方法,此处带宽放大系数符号表示为 *BAF*′):

$$BAF' = \frac{\text{len(UDP payload) amplifier to victim}}{\text{len(UDP payload) attacker to amplifier}} \tag{1}$$

$$PAF = \frac{\text{number of packets amplifier to victim}}{\text{number of packets attacker to amplifier}} \tag{2}$$

BAF 和 PAF 都是用来描述放大器主机放大效果的测度.Rossow 按照公式(1)和公式(2)的计算方法,给出了 14 种可能会导致反射攻击的协议的 BAF 和 PAF 值,其中由于 BAF 存在变化性,文献只给出了平均强度(all)和两类极限强度(50%和 10%)下的 BAF,见表 1.

Table 1 BAF value of the fourteen protocols[5]

表 1 14 种协议的 BAF 值[5]

Protocol	BAF			PAF
	all	50%	10%	all
SNMP v2	6.3	8.6	11.3	1
NTP	556.9	1 083.2	4 670	10.61
DNSNS	54.6	76.7	98.3	2.08
DNSOR	28.7	41.2	64.1	1.32
NetBios	3.8	4.5	4.9	1
SSDP	30.8	40.4	75.9	9.92
CharGen	358.8	n/a	n/a	1
QOTD	140.3	n/a	n/a	1
BitTorrent	3.8	5.3	10.3	1.58
Kad	16.3	21.5	22.7	1
Quake 3	63.9	74.9	82.8	1.01
Steam	5.5	6.9	14.7	1.12
ZAv2	36	36.6	41.1	1.02
Sality	37.3	37.9	38.4	1
Gmaeover	45.4	45.9	46.2	5.39

本文认为公式(1)和表 1 中给出的部分 BAF 值得商榷.首先,表 1 中 SNMP 和 CharGen 的 PAF 均为 1.00,这意味着每个请求报文仅仅产生了一个回复报文,这与本文实验获取的结果明显不符.本文认为导致问题的原因是实验过程中使用了全局端口匹配而忽略了分片报文,也就是说,产生 IP 分片的报文没有被算作回复报文参与计算,因此得到的 PAF 值为 1.00,这也会直接导致 BAF 值偏小.另一方面,公式(1)使用负载长度作为 BAF 计算基准.作者考虑的是在将来实验中 IPv6 地址首部的影响,所以未将以太网首部、IP 报头以及 UDP 报头部分算入负载长度的计算中.这样的计算方式存在一定的不合理性,因为大部分的反射攻击请求命令的报文负载都比较小,CharGen 请求的负载甚至是 1 字节,这容易造成 BAF 的波动,不利于对各种协议的 BAF 系数做出公平的比较分析.

对此,出于合理性考虑,同时也希望能真正反映反射攻击中带宽放大的实际情况,本文将使用全报文负载计算 BAF,并且在计算中考虑对应的分片报文.下面是本文使用的 BAF 计算公式.

定义一次请求中,请求报文长度为 $len(Rq)$,回复 n 个报文($n \geqslant 1$),每个回复报文长度为 $len(Rp_i)$,i 表示第 i 个

报文,则 BAF 计算表达式:

$$BAF = \frac{\sum_{i=1}^{n} len(Rp_i)}{len(Rq)} \tag{3}$$

3 BAF 分析样本的获取

3.1 放大器的获取

一定规模的放大器主机数量是开展反射攻击实验和获取大量实测 BAF 系数的基础.这些放大器应该是真实存在且有过反射攻击行为.本文实验使用的放大器由 NBOS 系统提供.

NBOS 是基于流记录数据实现对网络流量行为的观测与精细化管理系统[12].它安装在网络的边界,采用基于端口匹配和流量强度阈值的检测算法来检测 CERNET 网内的反射攻击行为.

目前正式运行的 NBOS 系统可以检测 CHARGEN、DNS、NTP、SNMP 和 SSDP 这 5 种协议的反射 DDoS 攻击.具体的检测结果如图 2 所示.以第 1 条攻击事件为例,主机 23*.147.3 被网内的 1 个放大器攻击,从 2016-05-16 01:37:58 起到 2016-05-16 01:42:11 共产生了 148.59MB 的攻击流量.NBOS 还同时可以给出参与攻击的主机,就是放大器.图 3 是这次攻击中放大器的信息,它使用的是 19 端口.

ip	归属	类型	起始时间	结束时间	持续时间	活跃粒...	Kpps	最大Kp...	MBps	最大M...	总流量(...	对端IP数
23[redacted].147.3	北美洲-美国	0x41	2016-05-16 01:37:58	2016-05-16 01:42:11	253	1	0.44	0.44	0.495	0.495	148.59	1
23[redacted].16.215	北美洲-美国	0x41	2016-05-16 01:25:50	2016-05-16 01:39:59	849	2	0.395	0.408	0.534	0.55	802.13	18
104[redacted].188.207	北美洲-美国	0x41	2016-05-16 01:21:07	2016-05-16 01:34:58	831	1	0.429	0.429	0.543	0.543	488.94	14
24[redacted].137.173	北美洲-美国	0x41	2016-05-16 01:25:38	2016-05-16 01:30:35	297	1	0.586	0.586	0.778	0.778	233.55	11

Fig.2 UDP reflection attacks detected by NBOS

图 2 NBOS 检测到的 UDP 反射攻击

攻击对象：23[redacted].147.3 攻击类型：0x41 开始时间：2016-05-16 01:37:58 结束时间：2016-05-16 01:42:11

ip	归属	总流量(MB)	总报文数	开始时间	结束时间	端口
222.[redacted].166.112	[redacted]学院	148.59	135424	2016-05-16 01:37:58	2016-05-16 01:42:11	19

Fig.3 The information of amplifier which attacked 23.*.147.3

图 3 攻击 23.*.147.3 的放大器信息

NBOS 系统部署在 CERNET 全网,本文实验使用的放大器均是由 NBOS 系统提供的.虽然 NBOS 可以检测 5 个应用协议的反射攻击,但由于具有 DNS 反射攻击的请求报文中需要提供域名参数,情况比较复杂,作为研究工作的起点,本文仅讨论其余 4 种简单协议的 BAF.

3.2 实验过程

本文选择一台可以访问 CERNET 内所有地址的主机作为请求代理,用于向所有放大器发送反射攻击的请求命令,代理安装 TCPDUMP(dump the traffic on a network),用以记录请求和回复过程中全部的往返报文.实验中,代理主机的 IP 地址是:*.*.110.154.实验开始于 2015 年 11 月 24 日.代理在每天的 1 点和 13 点从 NBOS 获取放大器列表,在随后的 3 点和 15 点向放大器列表中的所有主机发送请求,TCPDUMP 记录全部交互过程.实验

持续了 15 天,共进行了 30 次.每次实验后,BAF 统计程序会读取 TCPDUMP 记录的报文,计算 BAF 等信息.

SNMP 协议和 CHARGEN 协议的回复报文中会出现 IP 分片报文,而 IP 分片报文中没有端口信息,如果报文采集的条件设置为 IP+端口,IP 分片报文就不会被 TCPDUMP 抓取到,为了保证能够抓取到分片报文,TCPDUMP 的报文过滤条件不对端口进行设定,而采用 IP 地址+UDP 协议.采用 IP 地址+UDP 协议的过滤条件可以保证抓取到 IP 分片报文,但由于没有设定端口,TCPDUMP 会抓取到许多无用端口的 UDP 报文,为了解决上述问题,实验阶段,代理主机只开放了本文讨论的 4 种端口.

3.3 获取的 BAF 数据

实验中获取的部分放大器的 BAF 等信息如图 4 所示.

日期	放大器	端口	请求字节数	回复字节数	BAF值
2015/11/24_03	110.[redacted].96.24	19	43	5540	128.8372
2015/11/25_03	110.[redacted].96.24	19	43	1491	34.67442
2015/11/27_13	210.[redacted].232.183	1900	136	0	0
2015/11/27_13	58.[redacted].189.210	1900	136	7440	54.70588
2015/11/24_03	221.[redacted]204.110	123	234	0	0
2015/11/24_03	221.[redacted]161.219	123	234	48200	205.9829
2015/12/03_03	121.[redacted].0.51	161	81	1513	18.67901

Fig.4 BAF information of some amplifiers

图 4 部分放大器 BAF 信息

图 4 给出了部分放大器的 BAF 信息.图中有 1 个细节值得关注,图中第 1 条和第 2 条 BAF 信息均来自于 19 端口放大器 110.*.96.24,是在不同的实验中获取的,两次实验的请求报文是一样的,但 BAF 分别是 128.837 1 和 34.674 42.由此可见,同一台放大器在不同的攻击过程中的 BAF 也是会变化的,BAF 具有随机性.

4 BAF 特征分析

4.1 分析样本筛选

图 4 中的第 3 和第 5 条记录中的 BAF 为 0,导致这个现象的原因是多方面的,但 BAF 为 0 的记录没有研究价值,应当去除.本文在去除 BAF=0 的记录的基础上作如下定义:

- 有效放大器和无效放大器:在实验持续的时间 t 内,若某台放大器主机 H 的所有 BAF 的平均值小于 20,则称 H 为无效放大器,否则称 H 为有效放大器;BAF 均值小于 20 的放大器放大效果不明显,被攻击者选用的概率较低,因此本文在进行 BAF 特征分析时去除了这些样本.
- 有效 BAF 样本:在实验持续的时间 t 内,请求有效放大器获取的 BAF 样本称为有效 BAF 样本.

实验中筛选的有效放大器与有效 BAF 样本信息统计见表 2.

Table 2 Summary of effective BAF samples and effective amplifiers

表 2 有效 BAF 样本与有效放大器汇总

端口	有效 BAF 样本	有效放大器
19(CharGen)	9533	654
123(NTP)	6019	377
161(SNMP)	243	9
1900(SSDP)	10945	613

4.2 统计特征分析

为了研究不同协议中放大器 BAF 的统计性规律,对于有效放大器的 BAF,分不同协议统计各自的均值和极值结果见表 3.

Table 3 BAF statistics of valid amplifier

表 3 有效放大器 BAF 统计信息

端口	均值	最大值	最小值
19(CharGen)	67.35	165.91	1.40
123(NTP)	126.37	205.98	2.06
161(SNMP)	48.31	58.70	21.31
1900(SSDP)	52.34	241.79	2.61

由表 3 可知,NTP 与 CharGen 反射攻击仍是放大效果最好、攻击强度最强的反射攻击.NTP 协议的 BAF 均值达到了 126.75,远远超过其他 3 种协议.实验中,SSDP 协议的 BAF 均值达到了 52.34,最大 BAF 甚至达到 241.79,超过了 NTP 与 CharGen 反射攻击的最大 BAF.这些数据表明,SSDP 反射攻击应该引起人们足够的重视.Akamai 发布的 2015 年第一季度网络安全现状报告指出 SSDP 反射攻击已经成为 TOP1 的 DDoS 攻击方式,占到了 20.78%[13].图 5 是 4 种协议中部分放大器按 BAF 均值由小到大的分布.

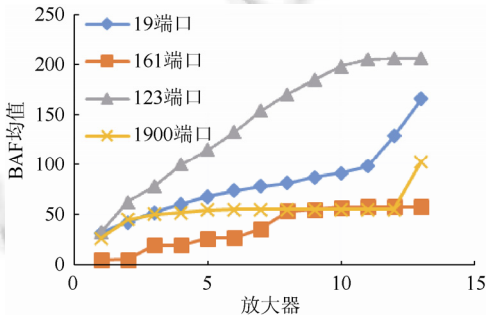

Fig.5 Average value of effective amplifier from the four ports

图 5 4 种端口部分有效放大器均值

为了方便显示,图 5 按 BAF 均值均匀选择了 4 种协议中 13 台放大器.不同协议中放大器是不同的,横轴中的值 x 只是表示 4 种协议中第 x 台放大器.图 5 可以发现,4 种协议中不同放大器主机之间的 BAF 以及变化规律均存在明显的差异.4 种协议中放大器的 BAF 均在有界区间分布.

4.3 稳定特征分析

攻击者更偏好使用 BAF 稳定性好的放大器,这需要进行重点防范.本节将进行 BAF 的稳定特征分析,从整体角度比较各个协议的 BAF 的稳定性以及考察各个协议中放大器主机的 BAF 随时间变化是否稳定.同样,稳定性的分析也只对有效 BAF 样本进行.

4.3.1 协议间的稳定特征分析

信息熵可用来衡量一个随机变量的稳定性,一个变量的信息熵越大,那么它的离散程度越大,稳定性就越差[14].本文用信息熵来比较各个协议间的 BAF 的稳定性.信息熵的具体的定义是:假设离散型随机变量 X 的取值范围 $R=\{x1,x2,...\}$ 是有限可数的.设 $pi=P\{X=xi\}$ 为随机变量 X 取 xi 的概率,X 的熵定义为 $H(x)=-\sum_{I\geqslant 1}Pi\cdot\log pi$.本文将各个协议中的 BAF 样本值看作一个离散随机变量的取值.根据上述公式计算出的各个协议的有效 BAF 的信息熵统计见表 4.

Table 4 Information entropy of BAF in each protocol

表 4 各个协议中 BAF 的信息熵

端口	信息熵
19(CharGen)	10.83
123(NTP)	6.51
161(SNMP)	5.49
1900(SSDP)	2.87

由表 4 可以发现,1900 端口和 161 端口 BAF 的信息熵相对较小,分别为 2.87 与 5.49;19 端口和 123 端口 BAF 的信息熵相对较大,分别为 10.83 与 6.51.从信息熵大小来看,SSDP 协议中 BAF 最稳定,CharGen 协议中的 BAF 最不稳定.

4.3.2 放大器间的稳定特征分析

变异系数可以作为衡量一组数据的离散程度的度量,而且变异系数($C\cdot V$)可以消除单位和平均数不同对两个或多个资料变异程度比较的影响[15].变异系数有评价的临界值,一般认为 $C\cdot V\leqslant 15\%$,数据间变异较小,比较稳定.本文用变异系数来考察放大器 BAF 相对于时间变化的稳定性,即同一放大器在不同的攻击实验中 BAF 的变化情况.变异系数的具体定义是:标准差与平均数的比值称为变异系数,其计算公式为 $C\cdot V$=(标准偏差 SD/平均值 $Mean$)×100%.本文首先根据放大器 BAF 的变异系数给出了稳定放大器的定义,然后根据这个定义统计出各个协议中稳定放大器的数目.相关统计结果见表 5.

● 稳定放大器:在实验持续的时间 t 内,若放大器 H 主机 BAF 的变异系数小于或等于 15%,则称 H 为稳定放大器.

Table 5 Stable amplifier statistics for each port

表 5 各个端口的稳定放大器统计

端口	有效放大器	稳定放大器	比例(%)
19(CharGen)	654	181	27.7
123(NTP)	377	144	38.2
161(SNMP)	9	9	100
1900(SSDP)	613	493	80.4

由表 5 可以发现,SSDP 协议中的稳定放大器最多,达到 493 台,SNMP 协议中 9 台有效放大器都是稳定放大器,比例高达 100%.19 端口与 123 端口中放大器的 BAF 值虽然较大,但稳定放大器的比例较小.

4.3.2 放大器评价

BAF 在较小数值范围内上下波动的放大器,即使是稳定放大器,但放大效果不明显,攻击者往往也不倾向于使用.本文在综合考虑 BAF 大小和稳定性的基础上,对各个放大器进行评价,并按照危险程度将放大器分为轻微、关注、严重 3 种级别.各个协议中不同级别放大器的数目见表 6.

● 轻微、关注、严重级别:在实验持续的时间 t 内,如果稳定放大器 H 的所有 BAF 的均值大于 20 且小于等于 50,则 H 为轻微级别;如果大于 50 且小于等于 100,则 H 为关注级别;如果大于 100,则放大器 H 为严重级别.

Table 6 Amplifier statistics by level for each port

表 6 各个端口中放大器按级别统计

端口	轻微	关注	严重
19(CharGen)	42	74	65
123(NTP)	10	6	128
161(SNMP)	4	5	0
1900(SSDP)	35	458	0

从表 6 中可以发现,只有 19 与 123 端口中存在严重级别的放大器,分别为 65 台与 128 台.161 端口与 1900 端口中稳定放大器集中在轻微和关注两种级别.1900 端口中绝大数稳定放大器为关注级别,达到 458 台.

5 总结与展望

本文对基于 UDP 的 CHARGEN、NTP、SNMP、SSDP 4 种协议的反射攻击进行了讨论,在此基础上提出了对带宽放大因子(BAF)计算公式的改进方法.随后利用 NBOS 平台提供的 CERNET 全网 38 个主节点内具有上述 4 种反射行为的放大器进行了 BAF 的获取实验,并对于获取的数据从统计特征、稳定特征两个方面进行了比较与分析.获得的结论有:NTP 与 CharGen 反射攻击的 BAF 稳定性较差,但仍然是放大效果最好、强度最大的反射攻击.SSDP 与 SNMP 反射攻击的 BAF 有较好的稳定性,但放大效果比不上 NTP 与 CharGen 反射攻击.

同时需要说明的是,SSDP 反射攻击的 BAF 均值达到了 52.34,最大 BAF 甚至达到 241.79,超过了 NTP 与 CharGen 反射攻击的最大 BAF,虽然没有处于严重级别的放大器,但 90%以上的放大器处于关注级别,达到 458 台.这些都说明 SSDP 反射攻击足以产生高强度的反射攻击行为,应该引起人们足够的重视.后继的工作将从两个角度展开:从请求响应延迟、总吞吐量、CPU 消耗量等多个方面来测验和评估各种协议的反射攻击;对于攻击命令中含有参数的反射攻击,如 DNS 反射攻击,分析参数对 BAF 等用来评价反射攻击强度指标的影响.

References:

[1] The DDoS That Knocked Spamhaus Offline (And How We Mitigated It). 2013. https://blog.cloudflare.com/
[2] Technical Details Behind a 400Gbs NTP Amplification DDoS Attack. 2014. https://blog.cloudflare.com/
[3] Summary of China's Internet security situation in 2015. 2016. http://www.cert.org.cn/publish/main/17/index.html/
[4] Li G, Ding W. The principle and prevention of UDP reflection DDoS attacks. China Education Network, 2015(4):43 (in Chinese with English abstract).
[5] Rossow C. Amplification hell: Revisiting network protocols for DDoS abuse. In: Proc. of the 2014 Network and Distributed Systems Security Symposium (NDSS 2014). 2014. 23–26.
[6] Postel J. Character generator protocol, IETF RFC 864, 1983.
[7] Mills DL. Network time protocol, IETF RFC 958, 1985.
[8] Case J, McCloghrie K. Protocol Operations for SNMPv2, IETF RFC 1905, 1996.
[9] Goland YY, Cai T, Leach P, Gu Y. Simple service discovery protocol, IETF INTERNET-DRAFT, 2000.
[10] An Analysis of DrDoS SNMP/NTP/CHARGEN Reflection Attacks: Part II of the DrDoS White Paper Series, 2013. https://news.asis.io/sites/default/files/An_Analysis_of_DrDoS_SNMP.pdf
[11] SSDP Reflection DDoS Attacks: The DrDoS White Paper Series. 2013. https://www.akamai.com/us/en/multimedia/documents/
[12] Zhang WW, Gong J, Ding W, Zhang XG. NBOS: A fine-grained network management system. Journal of Taiyuan University of Technology, 2012,43(10):41–46 (in Chinese with English abstract).
[13] Network security status report for the first quarter of 2015. 2015. http://www.stateoftheinternet.com/security-report
[14] Zhang SS. The properties and applications of information entropy. Technology Information, 2011,(14):14 (in Chinese with English abstract).
[15] Wang WS. Coefficient of variation: A simple and useful statistical indicator to measure the degree of dispersion. China Statistics, 2007,(6):41–42 (in Chinese with English abstract).

附中文参考文献:

[4] 李刚,丁伟.UDP 反射 DDoS 攻击原理和防范.中国教育网络,2015(4):43.
[12] 张维维,龚俭,丁伟,张孝国.NBOS:一个基于流技术的精细化网管系统.太原理工大学学报,2012,43(10):41–46.
[14] 张姗姗.信息熵的性质及应用.科技信息,2011(14):14.
[15] 王文森.变异系数——一个衡量离散程度简单而有用的统计指标.中国统计,2007,(6):41–42.

周文烽(1992－),男,江苏东台人,硕士,主要研究领域为网络安全.

丁伟(1962－),女,博士,教授,博士生导师,主要研究领域为网络测量,网络安全,网络行为学.

李刚(1990－),男,硕士,主要研究领域为网络行为学.