NBOS的部署、运行和使用

CERNET华东北地区中心
东南大学 计算机学院
丁伟 wding@njnet.edu.cn

20131117

报告提纲

- 系统基本情况介绍
- NBOS驻地系统的安装和运行情况
- 使用NBOS发现网络中安全事件的实例
- NBOS当前版本的使用要点
- 其他有关问题

系统基本情况介绍

- Network Behavior Observation System
- NBOS的原型系统是在国家支撑计划项目支持下完成的以主干网流记录为数据源的网络安全监测系统。
- 目前在38个主节点所管理的网络边界部署的系统是在该原型基础上为211三期的主干网升级项目重新开发的配套系统。
- 目前的版本是NBOS-S2.0，可以支持的数据源是V5或V9格式的netflow或netstream，采用B/S结构工作

驻地系统的安装和运行情况

NBOS驻地系统的安装环境

- NBOS部署在曙光刀片服务器中的第 1个刀片上
- 该服务器配置2块网卡，各自使用不同的IP地址。 第一块使用主干网地址，由CERNOC统一分配并设置，用于系统的管理通道，不向主节点开放
- 主节点使用第二块网卡访问NBOS系统，该网卡接入主节点内部或校园网的交换机，因此这块网卡的资源由主节点提供，由项目组负责配置。主节点人员通过这个地址访问系统。

NBOS驻地系统的安装情况

- 所有38个主节点的安装已全部完成，并进行同步的升级维护
- 截止10月11日
  - 尚未完成本地环境配置的主节点：石家庄、银川、成都、昆明、拉萨、桂林、海口、郑州、杭州和哈尔滨
  - 获得局部数据源的主节点：成都、郑州和长沙
  - 没有获得数据源的主节点：银川、乌鲁木齐、海口、昆明、贵阳和拉萨

38个主节点的运行情况

- 项目组对19个最早进入正常运行（全部流量可见）的主节点进行了观测，并提供了试运行报告
- 根据运行中发现的问题，对系统进行的大小调整超过100次
- 除了流量最大的上海节点因内存问题调整了抽样比外，目前其他驻地系统均可以在较低的128抽样比下工作

NBOS应用实例

使用实例1-僵尸网络的发现

- *.195.161.27是江苏某大学地址，DDOS检测发现其经常出现在参与51类型攻击的源地址中，而且是唯一的参与攻击地址
- 将该地址放入局部流量后，发现其与电信地址114.80.119.131长时间交互
- 通过部署在江苏省网边界的采集器对*.195.161.27进行全报文采集和分析确认该地址的控制器就是114.80.119.131

2013年IP[redacted].195.161.27参与攻击的检测结果

序号	被攻击服务器	归属	类型	起始时间	结束时间	pps	最大pps	Kbps	最大Kbps	平均IP数	最大IP
1	180.186.16.133	联通	51	2013-10-15 14:22:28	2013-10-15 14:22:55	702	702	5,157	5,157	1	1
2	74.117.62.36	美国	51	2013-10-15 13:17:32	2013-10-15 13:18:43	1,214	1,214	8,917	8,917	1	1
3	74.117.62.37	美国	51	2013-10-15 13:05:36	2013-10-15 13:07:12	1,163	1,163	8,547	8,547	1	1
4	59.188.74.58	中国香港	51	2013-10-15 13:04:28	2013-10-15 13:04:46	3,000	3,000	3,043	3,043	1	1
5	162.212.34.117	美国	51	2013-10-15 09:15:28	2013-10-15 10:12:15	1,806	3,746	7,484	10,315	1	1
6	162.212.34.1	美国	51	2013-10-15 09:56:10	2013-10-15 09:59:21	1,152	1,152	8,460	8,460	1	1
7	70.39.80.94	美国	51	2013-10-15 09:20:16	2013-10-15 09:21:00	525	525	3,860	3,860	1	1
8	218.85.148.250	电信	51	2013-10-15 02:00:11	2013-10-15 02:00:57	511	511	3,753	3,753	1	1
9	162.211.182.197	未知	51	2013-10-15 01:50:06	2013-10-15 01:50:55	716	716	5,264	5,264	1	1
10	112.124.61.35	中国	51	2013-10-14 23:50:49	2013-10-15 00:00:57	1,893	3,558	1,893	3,785	1	2
11	162.221.13.68	加拿大	51	2013-10-14 20:44:03	2013-10-14 20:44:42	514	514	3,778	3,778	1	1
12	[illegible]	[illegible]	51	2013-10-14	2013-10-14	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

*.195.161.27与114.80.119.131长时间交互

【09-13 14:25到09-13 16:20】IP:*.*.195.161.27对端IP的TOP20

【09-13 16:20】

【09-13 16:15】

【09-13 16:10】

【09-13 15:55】

排名	对端IP	出流				入流				NO.1端口及其占用百分比和协议	NO.2端口及其占用百分比和协议	NO.3端口及其占用百分比和协议	NO.4端口及其占用百分比和协议	NO.5端口及其占用百分比和协议
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)					
1	114.80.119.131 电信	0	0	1	1	1	1	0	0	6009 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE

【09-13 10:30到09-13 12:25】IP:*.*.195.161.27对端IP的TOP20

【09-13 12:25】

排名	对端IP	出流				入流				NO.1端口及其占用百分比和协议	NO.2端口及其占用百分比和协议	NO.3端口及其占用百分比和协议	NO.4端口及其占用百分比和协议	NO.5端口及其占用百分比和协议
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)					
1	205.209.140.252 美国	0	0	278	1763	0	0	0	0	80 100% 17	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
2	205.209.140.251 美国	0	0	244	1527	0	0	0	0	80 100% 17	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
3	114.80.119.131 电信	0	0	1	1	2	1	0	0	6009 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE

在个别时间粒度有2个地址参与攻击

参与攻击的IP（随机选择五个）

IP	IP归属
[redacted].195.161.27	[redacted]大学
[redacted].119.208.236	[redacted]

注：参与攻击的IP存在伪造可能

2013年IP[redacted].119.208.236参与攻击的检测结果

序号	被攻击服务器	归属	类型	起始时间	结束时间	pps	最大pps	Kbps	最大Kbps	平均IP数	最大IP数
1	112.124.61.35	中国	51	2013-10-14 23:50:49	2013-10-15 00:00:57	1,893	3,558	1,893	3,785	1	2
2	112.175.69.115	韩国	51	2013-10-14 10:33:58	2013-10-14 10:34:24	506	506	3,715	3,715	2	2
3	14.17.74.102	电信	51	2013-10-11 20:00:35	2013-10-11 20:03:51	762	762	5,602	5,602	2	2
4	58.64.150.71	中国香港	51	2013-10-11 18:39:55	2013-10-11 18:44:39	4,504	7,223	2,111	3,386	1	2
5	112.175.234.232	韩国	51	2013-10-11 18:11:09	2013-10-11 18:14:48	2,954	2,954	3,050	3,050	2	2

点击上图* .119.208.236的页面，可见到5个攻击信息。经检查5个攻击中另外的一个地址均是*.195.161.27，这样可确定* .119.208.236与*.195.161.27具有相同问题的节点

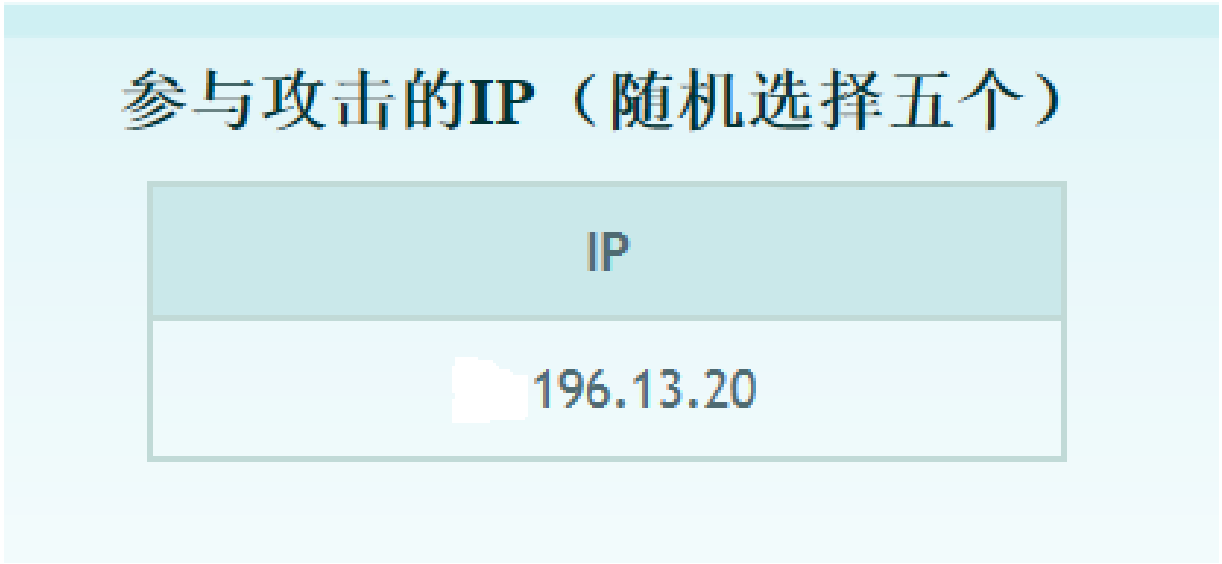
在其他主节点观测到的类似现象

EXCEL格式下载

SYN Flood | TCP/UDP Flood

序号	被攻击服务器	归属	类型	起始时间	结束时间	pps	最大pps	Kbps	最大Kbps	平均IP数	最大IP数
11	162.221.13.102	加拿大	51	2013-10-14 15:21:03	2013-10-14 15:22:03	802	802	5,640	5,640	1	1
12	162.221.13.68	加拿大	51	2013-10-14 15:18:50	2013-10-14 15:19:50	1,316	1,316	9,258	9,258	1	1
13	162.221.13.67	加拿大	51	2013-10-14 15:15:03	2013-10-14 15:16:02	1,948	1,948	13,698	13,698	1	1
14	162.221.13.103	加拿大	51	2013-10-14 15:11:50	2013-10-14 15:12:50	978	978	6,882	6,882	1	1
15	116.10.189.60	电信	51	2013-10-14 14:37:24	2013-10-14 14:54:55	2,261	3,537	18,918	29,601	2,646	4,141
16	162.221.13.102	加拿大	51	2013-10-14 14:37:29	2013-10-14 14:43:49	797	801	5,607	5,634	1	1
17	115.25.217.12	搜狐公司	52	2013-10-14 14:30:01	2013-10-14 14:39:59	566	595	290	305	564	586
18	199.36.73.20	美国	51	2013-10-14 13:41:40	2013-10-14 14:23:04	3,369	5,675	23,703	39,906	1	1

上图中所有针对美国和加拿大地址的攻击来源同一个地址



将该地址加入局部流量观测后发现其与三个网外地址长时间连接

【10-14 14:20到10-14 16:15】IP: .196.13.20对端IP的TOP20

【10-14 16:15】

【10-14 16:10】

【10-14 16:05】

【10-14 16:00】

排名	对端IP	出流				入流				NO.1端口及其占用百分比和协议	NO.2端口及其占用百分比和协议	NO.3端口及其占用百分比和协议	NO.4端口及其占用百分比和协议	NO.5端口及其占用百分比和协议
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)					
1	162.221.13.103 加拿大	0	0	13876	116869	0	0	0	0	80 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
2	64.62.184.187 美国	0	0	4	3	8	4	0	0	10991 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
3	114.80.119.131 电信	0	0	2	3	3	1	0	0	4130 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
4	118.244.215.23 联通	0	0	1	1	1	1	0	0	10991 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE

应用实例2-僵尸网络检测测

- NBOS热点监测显示江苏省网内某单位地址*.77.186.105经常会出现源地址的尖峰流量，使用UDP协议和30个以上端口
- 将该地址加入局部后发现这些尖峰流量每次发往单个国外地址，不同的尖峰发往不同的地址
- 通过辅助对上述地址的全报文采集，获得了该僵尸网络控制器的有关信息

检索IP：[redacted]77.186.105 其归属：江苏省[redacted]

序号	所在时间粒度	性质	流量(Mb/s)	流量TOP1端口及其占用百分比	流量TOP2端口及其占用百分比	流量TOP3端口及其占用百分比	流量TOP4端口及其占用百分比	流量TOP5端口及其占用百分比
1	09-17 08:35:00到09-17 08:39:59	源	1066.76	6193 1.36%	51237 1.36%	50859 1.35%	41316 1.35%	13772 1.35%
2	09-16 01:30:00到09-16 01:34:59	源	982.12	18249 1.54%	9883 1.52%	39651 1.51%	19310 1.5%	18659 1.5%
3	09-16 01:10:00到09-16 01:14:59	源	791.84	34390 3.01%	36840 2.97%	55642 2.93%	23943 2.92%	57263 2.89%
4	09-17 08:25:00到09-17 08:29:59	源	714.84	53196 1.31%	60346 1.3%	62904 1.3%	4270 1.28%	45620 1.28%
5	09-17 08:40:00到09-17 08:44:59	源	677.82	12120 1.39%	55889 1.36%	29749 1.35%	55245 1.35%	63426 1.34%
6	09-16 01:20:00到09-16 01:24:59	源	535.87	52918 36.49%	8239 1.13%	33608 1.07%	63384 1.02%	44187 1.01%
7	09-16 01:35:00到09-16 01:39:59	源	470.08	16924 1.28%	24678 1.27%	28193 1.26%	42708 1.25%	64809 1.24%
8	09-17 15:20:00到09-17 15:24:59	源	320.18	51638 2.99%	59984 2.95%	32187 2.88%	19180 2.84%	41284 2.78%
9	09-17 04:25:00到09-17 04:29:59	源	174.37	9941 1.02%	35586 0.94%	65224 0.94%	12358 0.94%	9936 0.94%
10	09-17 08:30:00到09-17 08:34:59	源	130.32	20711 0.08%	56069 0.05%	64562 0.05%	57536 0.04%	61768 0.04%

【09-17 15:40到09-17 17:35】IP·¹ 77.186.105对端IP的TOP20

【09-17 17:35】

【09-17 17:30】

排名	对端IP	出流				入流				NO.1端口及其占用百分比和协议	NO.2端口及其占用百分比和协议	NO.3端口及其占用百分比和协议	NO.4端口及其占用百分比和协议	NO.5端口及其占用百分比和协议
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)					
1	178.95.12.54 乌克兰	0	0	52148	566885	0	0	0	0	113 18.24% 17	18154 4.68% 17	59624 4.65% 17	44250 4.6% 17	10280 4.59% 17

【09-17 15:20】

排名	对端IP	出流				入流				NO.1端口及其占用百分比和协议	NO.2端口及其占用百分比和协议	NO.3端口及其占用百分比和协议	NO.4端口及其占用百分比和协议	NO.5端口及其占用百分比和协议
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)					
1	154.35.175.201 美国	0	0	30260	327794	0	0	0	0	61324 2.99% 17	33015 2.95% 17	34416 2.88% 17	38954 2.85% 17	8240 2.78% 17

对采集器1个小时的全报文分析结果

- *.77.186.105三次大量发送UDP报文现象
- 分析前后的其它报文，发现两个irc控制器：85.17.29.51和198.23.244.92，均使用6667端口
- 出现大量UDP报文前控制器向*.77.186.105发出开始攻击指令，三次的指令依次是：
  - Dilbar!Dilbar@test PRIVMSG #DDoS :.udpflood 74.117.173.147 113 180 65000
  - Forged!ddos@DDoS PRIVMSG #DDoS :.udpflood 91.212.150.172 80 150 65000
  - Forged!ddos@DDoS PRIVMSG #DDoS :.udpflood 192.184.11.134 80 120 65000
- 收到攻击指令之后依次出现针对74.117.173.147、91.212.150.172、和192.184.11.134的攻击，这些攻击流量在NBOS流量中检出
- 攻击结束*.77.186.105报告控制器本次攻击的强度，例如：
  - PRIVMSG #DDoS :[\002UdpFlood Finished!\002]: 8734 MB sent / Average: 58 MB/s
- 原始流量中能够看到大量的控制交互报文，大部分是通告botnet的各种状态信息，从中可以看到控制器在irc中的nickname是lelcomeatme

应用实例3-信息泄露事件

- NBOS热点监测发现江苏省网内某单位地址*.192.176.67作为流量源热点，向大量国外地址发送数据
- 这个服务器是该学校的数字化校园的短信平台

【09-13 09:30到09-13 11:25】IP:[redacted].192.176.67对端IP的TOP20

【09-13 10:40】

排名	对端IP	出流				入流				NO.1端口及其占用百分比和协议	NO.2端口及其占用百分比和协议	NO.3端口及其占用百分比和协议	NO.4端口及其占用百分比和协议	NO.5端口及其占用百分比和协议
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)					
1	24.20.42.116 美国	0	0	515	5024	207	74	0	0	1050 37.59% 17	30584 27.74% 17	11566 19.86% 17	16706 12.05% 17	21846 2.77% 17
2	192.227.140.105 澳大利亚	0	0	122	1263	46	16	0	0	1050 38.41% 17	11566 24.41% 17	30584 19.8% 17	16706 16.24% 17	21846 1.14% 17
3	71.196.122.164 美国	0	0	19	187	5	2	0	0	2001 59.67% 17	30584 25.32% 17	11566 8.78% 17	16706 6.23% 17	0 0% NONE
4	70.72.57.138 加拿大	0	0	17	185	7	2	0	0	1026 49.29% 17	30584 23.46% 17	16706 15.53% 17	11566 11.72% 17	0 0% NONE
5	204.188.236.96 美国	0	0	16	167	3	1	0	0	11566 26.7% 17	1050 24.41% 17	30584 22.4% 17	16706 15.65% 17	1026 10.84% 17
6	84.251.186.201 芬兰	0	0	14	155	5	1	0	0	30584 51.93% 17	1026 20.36% 17	11566 19.26% 17	16706 6.42% 17	21846 2.03% 17
7	151.118.161.59 美国	0	0	11	128	7	2	0	0	30584 40.49% 17	16706 26.63% 17	1026 17.43% 17	11566 15.45% 17	0 0% NONE

*.192.176.67服务器首页

其他主节点发现的类似情况

【07-30 13:40到07-30 15:35】IP:[redacted].120.84.197对端IP的TOP20

【07-30 15:35】

排名	对端IP	出流				入流				NO.1端口及其占用百分比和协议	NO.2端口及其占用百分比和协议	NO.3端口及其占用百分比和协议	NO.4端口及其占用百分比和协议	NO.5端口及其占用百分比和协议
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)					
1	108.242.243.14 美国	0	0	456	4614	166	67	0	0	2001 39.19% 17	30584 28.51% 17	11566 18.6% 17	16706 13.18% 17	21846 0.52% 17
2	66.91.2.120 美国	0	0	391	3866	58	27	0	0	2001 36.68% 17	30584 28.44% 17	11566 20% 17	16706 12.71% 17	21846 2.17% 17
3	190.210.177.210 阿根廷	0	0	366	3655	118	55	0	0	2001 39.76% 17	30584 29.08% 17	11566 20.33% 17	16706 10.08% 17	21846 0.74% 17
4	24.163.85.161 美国	0	0	352	3527	133	62	0	0	2001 42.35% 17	30584 26.09% 17	11566 20.93% 17	16706 10.17% 17	21846 0.47% 17
5	208.115.206.181 美国	0	0	319	3160	112	45	0	0	2070 41.3% 17	30584 26.95% 17	11566 19.72% 17	16706 9.95% 17	21846 2.07% 17
6	68.196.147.164 美国	0	0	235	2263	91	36	0	0	2001 38.86% 17	30584 29.37% 17	11566 16.71% 17	16706 12.4% 17	21846 2.66% 17

应用实例4-信息泄露

- NBOS通过某主节点的流量宿热点功能发现，台湾地址121.254.120.218以6.5Mbps左右的速度从网内下载信息
- 将该节点加入局部流量后发现，下载信息全部来自网内地址*.218.18.79
- *.218.18.79所在服务器是该单位某校区的学团工作网站

网外宿热点检索发现下载活动始于7月26日16点25分左右（第4行），连接数量在50个以上

检索IP：121.254.120.218 其归属：中国台湾

序号	所在时间粒度	性质	流量(Mb/s)	流量TOP1端口及其占用百分比	流量TOP2端口及其占用百分比	流量TOP3端口及其占用百分比	流量TOP4端口及其占用百分比	流量TOP5端口及其占用百分比
1	07-26 16:35:00到07-26 16:39:59	宿	7.03	58487 2.08%	58494 2.02%	58757 2.01%	58618 2.01%	58868 2%
2	07-26 17:15:00到07-26 17:19:59	宿	6.95	63554 2.12%	63661 2.09%	63922 2.08%	63542 2.07%	63921 2.05%
3	07-26 16:45:00到07-26 16:49:59	宿	6.87	59783 2.16%	59690 2.09%	59956 2.05%	59771 2.03%	59629 2.03%
4	07-26 16:25:00到07-26 16:29:59	宿	6.78	57047 2.27%	57406 2.11%	57278 2.11%	57076 2.1%	57451 2.09%
5	07-26 16:55:00到07-26 16:59:59	宿	6.71	61207 2.15%	61187 2.14%	61367 2.13%	61129 2.11%	60793 2.09%
6	07-26 16:40:00到07-26 16:44:59	宿	6.71	59062 2.11%	59445 2.07%	59050 2.07%	59250 2.07%	59105 2.07%
7	07-26 16:30:00到07-26 16:34:59	宿	6.46	58269 2.36%	58270 2.35%	58298 2.35%	58267 2.26%	58393 2.18%
8	07-26 17:10:00到07-26 17:14:59	宿	5.93	63259 2.59%	63297 2.36%	63312 2.35%	62882 2.34%	63319 2.32%
9	07-26 17:00:00到07-26 17:04:59	宿	5.76	61739 2.54%	61813 2.47%	61506 2.41%	61608 2.39%	61712 2.39%

121.254.120.218的下载信息全部来自*.218.18.79

【07-26 15:25到07-26 17:20】IP:121.254.120.218对端IP的TOP20

【07-26 17:20】

排名	对端IP	出流				入流				NO.1端口及其占用百分比和协议	NO.2端口及其占用百分比和协议	NO.3端口及其占用百分比和协议	NO.4端口及其占用百分比和协议	NO.5端口及其占用百分比和协议
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)					
1	[redacted].218.18.79 [redacted]学院	392	4465	0	0	0	0	200	79	80 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE

隐藏该日数据项

【07-26 17:15】

排名	对端IP	出流				入流				NO.1端口及其占用百分比和协议	NO.2端口及其占用百分比和协议	NO.3端口及其占用百分比和协议	NO.4端口及其占用百分比和协议	NO.5端口及其占用百分比和协议
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)					
1	[redacted].218.18.79 [redacted]学院	623	7117	0	0	0	0	351	132	80 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE

*.218.18.79所在服务器首页

应用实例5-恶意代码的发现

- NBOS某主节点首页的端口流数分布饼图出方向总有一个高端端口比例明显偏高，且10分钟左右变化一次，这些高端端口的流量全部来自同一个地址*.87.176.89
- 经主节点与该校园网沟通后确认该地址是在虚拟服务器上为一位老师做测试用的建的一台 虚拟机，在完成实验测试后没有及时做关机处理，也没有登陆进行管理。校园网随后立刻将虚拟 机关闭。

应用实例6-DDOS检测

- NBOS的DDOS检测显示中山大学旅游学院的WEb服务器stm.sysu.edu.cn所在主机211.66.128.162，从8月19日的19：50开始被高强度的 TCP-SYN-Flood DDOS攻击
- 攻击导致本被管网边界的流数在瞬间激增3倍
- 由于这个攻击是面向80端口的，所以在攻击持续期间首页的流数占比饼图80端口流数占比超过95%
- 这个攻击在20日上午11点左右终止，并在21日上午11:20-13:15被再次以超过这次接近一倍的强度实施
- 在相近的时间内，江苏南通大学的某服务器也受到类似行为的攻击

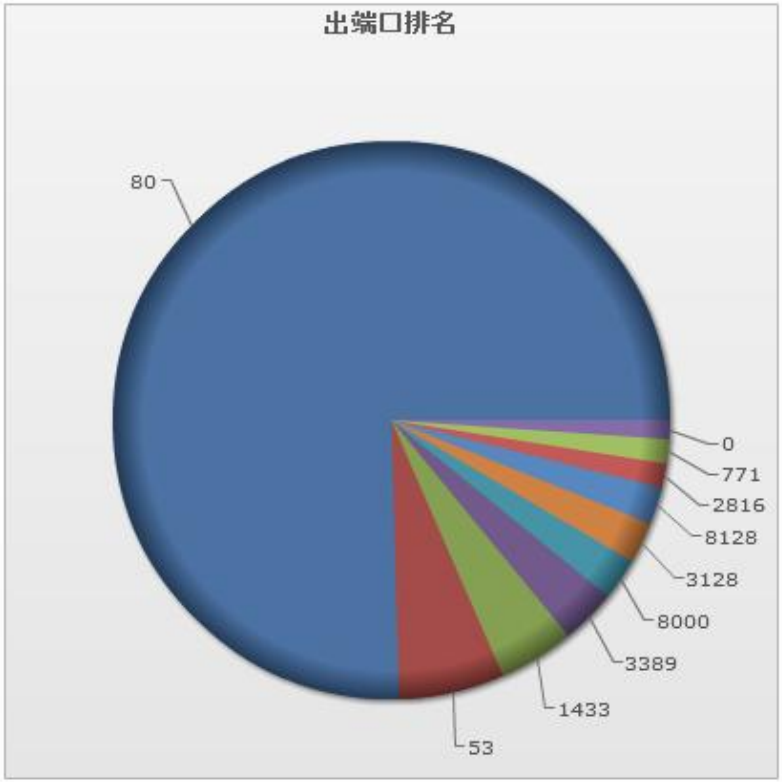
DDOS页面和测度进程页面的显示

7	222.201.134.38	华南理工大学(大学城校区)	2	2013-08-20 07:30:00	未终止	1,328	1,369	670	692
8	211.66.128.162	中山大学(大学城校区)	3	2013-08-19 17:50:13	未终止	574,808	604,106	260,459	273,735
9	182.99.143.39	电信	4	2013-08-15 20:00:41	未终止	1,545	1,748	724	819

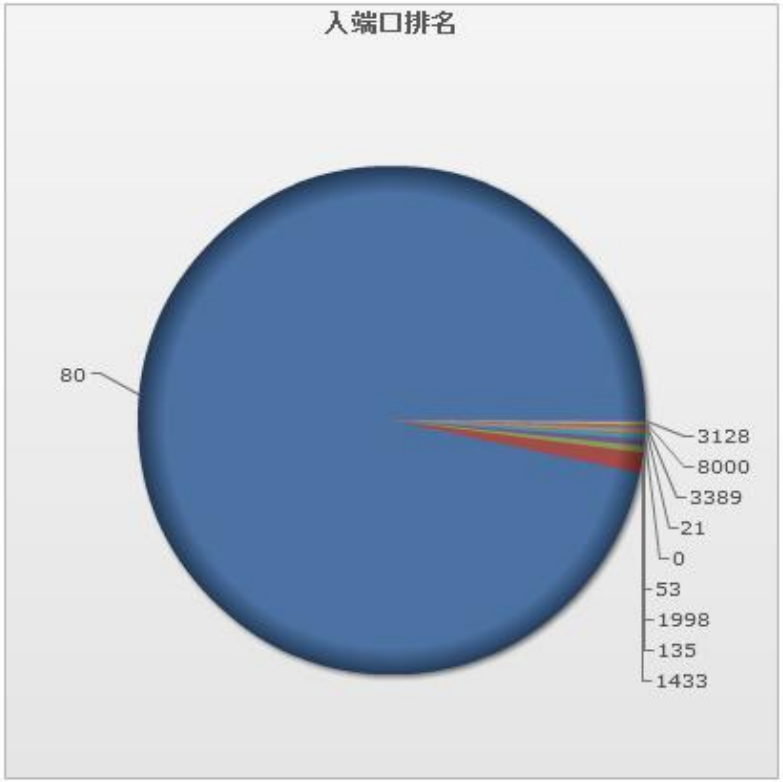
211	776,428	613,450	0	0	1 正常	2 正常	3 正常	6 正常	3 正常	4 正常	2 正常	1 正常	1 正常	15 正常
212	850,605	617,125	0	0	1 正常	3 正常	4 正常	8 正常	3 正常	3 正常	2 正常	1 正常	1 正常	15 正常
213	875,777	689,557	0	0	1 正常	2 正常	4 正常	9 正常	3 正常	3 正常	3 正常	1 正常	1 正常	17 正常
214	2,480,741	1,449,352	0	0	1 正常	4 正常	6 正常	17 正常	6 正常	6 正常	2 正常	2 正常	1 正常	30 正常
215	2,532,458	2,111,357	0	0	1 正常	4 正常	8 正常	26 正常	8 正常	7 正常	3 正常	2 正常	1 正常	47 正常

攻击持续期间某时候广州主节点首页流数比饼图显示的情况

端口占用排名 Top20



出方向流数按源端口排名



入方向流数按宿端口排名

NBOS当前版本的使用要点

NBOS驻地系统用户管理

- 超级用户：由总体掌控，可以进入所有系统，具有全部的功能
- 管理员用户：驻地系统自行管理
  - 用户名-NBOS
  - 原始口令
  - 管理管理员用户口令
  - 配置局部流量
  - 管理普通用户
- 普通用户：浏览驻地系统所有网页

发现可能存在的配置方面的问题

- 对上行接口间的流量观测
  - 通过导航条中基本流量行为二级菜单进入接口间流量
  - 选定数据源，路由器1或2
  - 指定接口显示的是上行接口，选择对端接口为指定接口
- 对局部流量中的非正常地址观测

选择数据源： 路由器1 指定接口： ALL 对端接口： ALL

历史周选择： 2013/10/14-2013/10/15 当前周

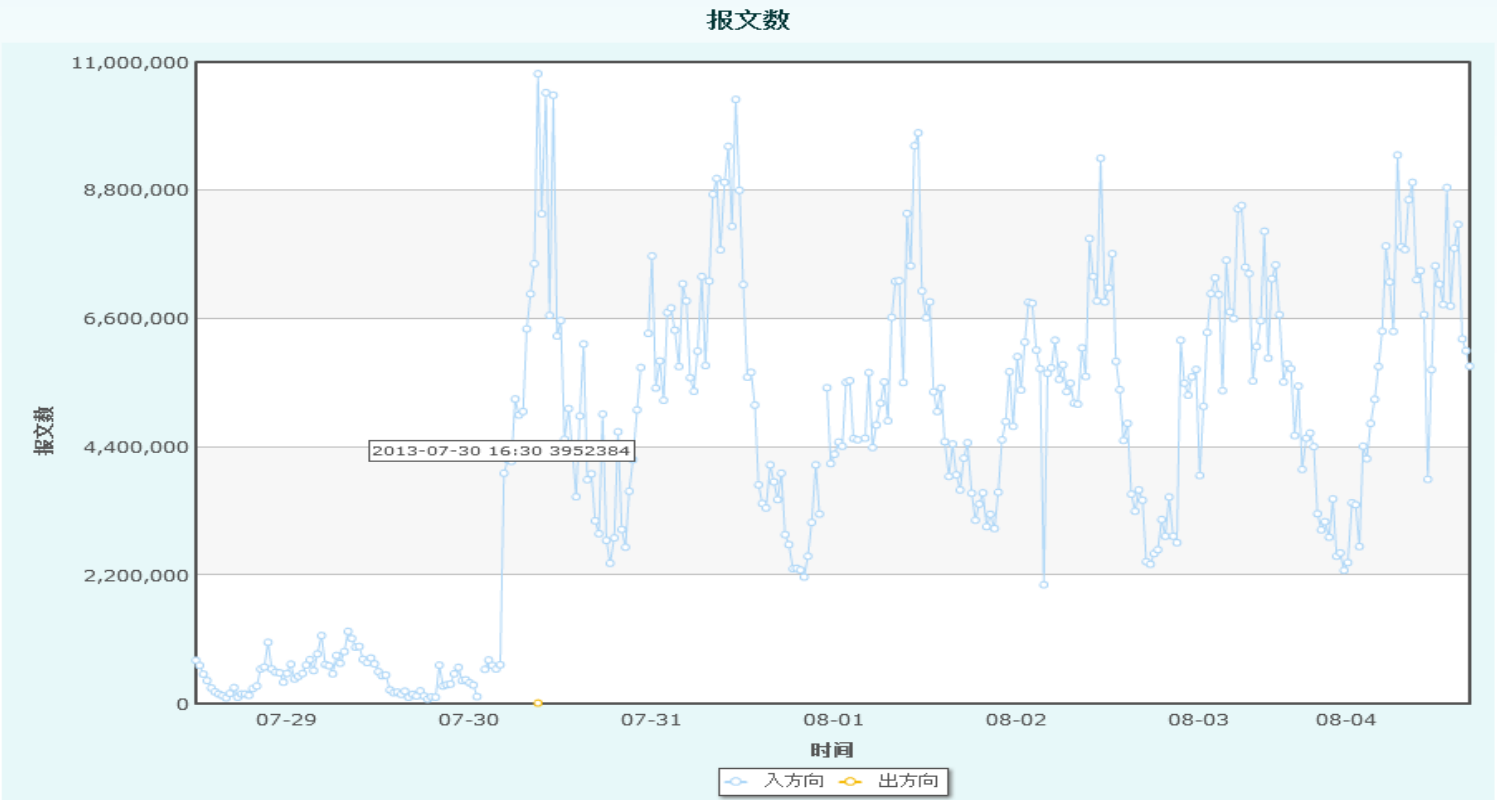
68
66

当前周路由器1接口ALL到ALL间流量行为

历史周选择： 2013/07/29-2013/08/04 查询 当前周

2013/07/29-2013/08/04路由器1接口67到67间流量行为

流数 报文数 字节数



广州主节点某时间粒度局部流量功能提供的非正常地址情况

最近24小时被管单位非正常地址IP流量的TOP50

【09-03 19:00】

排名	IP	出流				入流			
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)
1	183.60.202.246	0	0	0	0	0	0	2480	18797
2	183.60.201.195	0	0	0	0	0	0	2111	16003
3	183.57.57.15	0	0	0	0	0	0	588	4456
4	121.10.125.211	0	0	0	0	0	0	587	4451
5	121.10.125.100	0	0	0	0	0	0	581	4410
6	199.175.49.88	0	0	48	71	341	3868	0	0
7	121.10.125.81	0	0	0	0	0	0	505	3833
8	202.116.192.86	0	0	1327	814	1340	2144	0	0
9	162.212.131.14	0	0	184	1789	69	23	0	0

用局部流量功能定位异常行为

- 基于热点的观测
  - 网内源流量热点：参见实例2
  - 网外宿流量热点：参见实例4
- 基于特定端口
  - 3389、19、0
  - 根据局部流量中这些端口对端地址的观测获得
- 基于DDOS提供的信息
  - 用局部流量观测可能存在的真实地址：实例1和6
- 基于总体流量行为
  - 热连接信息：热点与异常-聚合分析-当前周或历史周提供的热连接和热地址对信息获取有关IP并将其放入局部流量观测更详细的流量情况
  - 热端口信息：基本流量行为-总体流量行为-端口占用排名选项卡，从中发现异常端口

局部流量行为页面


Network Behavior Observation System
首页
基本流量行为
服务质量
热点与异常
安全威胁分析
其他
总体流量行为
被管单位流量行为
分类流量行为
局部流量行为
接口间流量行为
局部流量行为
局部流量数据导出
局部流量参数配置
放大
端口流量行为
时的端口绑定IP的TOP50
时的端口对端IP的TOP50
被管单位局部放大
最近24小时每小时被管单位IP流量Top50
最近24小时每小时被管单位IP流数Top50
最近24小时每小时被管单位IP报文数Top50
最近24小时每小时被管单位IP字节数Top50
IP局部放大
最近48小时IP流量行为
最近36个小时IP绑定端口流量TOP10
最近36个小时IP对端IP流量TOP20

局部流配置页面


局部流量参数配置
【导出数据】
配置观测端口
配置观测被管单位
配置观测IP
配置首页参数
【配置观测端口】
端口1：53
端口2：80
端口3：135
端口4：445
端口5：1433
端口6：3389
端口7：6601
端口8：18089
端口9：18090
端口10：50001
提交
重置

【08-01 08:10到08-01 10:05】IP:111.74.239.151对端IP的TOP20

【08-01 10:05】

排名	对端IP	出流				入流				NO.1端口及其占用百分比和协议	NO.2端口及其占用百分比和协议	NO.3端口及其占用百分比和协议	NO.4端口及其占用百分比和协议	NO.5端口及其占用百分比和协议
		源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)	源报文数(pps)	源字节数(kbps)	宿报文数(pps)	宿字节数(kbps)					
1	.105.248.29 学新园区校园网	46	423	0	0	0	0	31	22	3389 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
2	.105.30.69 大学新园区校园网	35	317	0	0	0	0	18	14	3389 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
3	.105.245.44 校园网	34	311	0	0	0	0	24	18	3389 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
4	.105.193.219 校园网	32	287	0	0	0	0	21	15	3389 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
5	.105.67.123 校园网	32	268	0	0	0	0	28	22	3389 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
6	.105.247.13 校园网	31	270	0	0	0	0	24	16	3389 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
7	.105.71.186 校园网	26	234	0	0	0	0	25	14	3389 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE
8	.105.130.180 校园网	26	228	0	0	0	0	12	7	3389 100% 6	0 0% NONE	0 0% NONE	0 0% NONE	0 0% NONE

历史周选择： 2013/10/14-2013/10/15 查询 当前周

当前周聚合分析

活跃源前缀 活跃宿前缀 **活跃连接** 活跃IP地址前缀对

活跃连接

序号	源前缀	宿前缀	源端口	宿端口	协议	最大流量（Kb/s）	平均流量（Kb/s）	出现时间比
1	[redacted]121.199.209	美国 173.245.59.133	50918	53	17 - UDP	581,436	568,154.74	16.43%

端口占用排名TOP20

按报文数统计 **按字节数统计**

序号	出端口	流数比(%)	报文数(pps)	字节数(Kbps)
1	80	9.79	35,893	325,940
2	0	0.32	53,562	236,326
3	29555	<0.01	11,510	114,409
4	50918	<0.01	8,039	94,972
5	8090	0.75	7,132	73,398

序号	入端口	流数比(%)	报文数(pps)	字节数(Kbps)
1	5001	0.01	6,154	72,574
2	80	7.97	27,901	26,413
3	0	2.2	8,682	17,271
4	5041	0.53	3,238	16,789
5	4466	0.67	3,874	13,936

4002事件

- 4002事件是宿地址是私有地址的事件
- 该事件在绝大部分主节点普遍存在
- 造成该事件的原因主要是边界设备性能
- 4002直接导致丢包率上升

NBOS最新增加的一个功能

- 用参与攻击的地址，对DDOS攻击行为分类
  - 进入DDOS页面
  - 查看参与攻击的地址
  - 点击其中的一个，可以获得该地址参与的所有攻击的信息
- 某主节点的一个实例

查询被攻击服务器: All 攻击检测年选择: 2013 查询 当前年

当前年全网DDoS攻击检测

EXCEL格式下载

SYN Flood | TCP/UDP Flood

序号	被攻击服务器	归属	类型	起始时间	结束时间	pps	最大pps	Kbps	最大Kbps	平均IP数	最大IP数
1	59.66.142.132	清华大学	8	2013-10-15 06:02:15	未终止	305	578	3,511	6,625	1	1
2	219.228.111.52				0-15 :57	627	627	4,252	4,252	1	1
3	202.120.79.111	复旦大学	7	12:48:52	0-15 13:19:24	1,388	1,388	11,780	11,780	2	2
4	59.42.37.226	电信	10	2013-10-15 12:07:12	2013-10-15 13:07:25	839	846	9,805	9,880	1	1
5	219.74.134.45	新加坡	10	2013-10-15 11:16:11	2013-10-15 12:46:26	488	509	5,567	5,794	1	1

类型意义

类型=8：伪造源地址UDP Flood攻击，被攻击服务器在被管网外，攻击源在网内

参与攻击的IP（随机选择五个）

IP	IP归属
8.8.8.8	美国

2013年IP8.8.8.8参与攻击的检测结果

序号	被攻击服务器	归属	类型	起始时间	结束时间	pps	最大pps	Kbps	最大Kbps	平均IP数	最大IP数
1	59.66.142.132	清华大学	8	2013-10-15 06:02:15	2013-10-15 15:19:59	305	578	3,496	6,625	1	1
2	202.112.51.11	CERNET华北地区网络中心（OFFICE）	8	2013-10-15 10:13:58	2013-10-15 11:02:27	684	2,202	5,444	9,151	1	1
3	59.66.142.132	清华大学	8	2013-10-14 12:50:07	2013-10-15 01:09:59	311	568	3,596	6,441	1	1
4	59.66.142.132	清华大学	8	2013-10-14 12:17:08	2013-10-14 12:49:54	446	446	5,090	5,090	1	1
5	59.66.142.132	清华大学	8	2013-10-14 [illegible]	2013-10-14 [illegible]:59	290	494	3,245	5,589	1	1
6	59.66.142.132	清华大学	8	2013-10-13 19:52:05	2013-10-13 20:14:56	194	194	2,099	2,099	1	1
7	59.66.142.132	清华大学	8	2013-10-13 18:28:03	2013-10-13 19:24:59	191	197	2,119	2,180	1	1
8	202.112.51.11	CERNET华北地区网络中心（OFFICE）	8	2013-10-13 18:54:38	2013-10-13 19:07:16	347	599	2,756	3,118	1	1
9	202.112.51.11	CERNET华北地区网络中心（OFFICE）	8	2013-10-13 18:55:00	2013-10-13 19:04:57	221	263	2,628	3,118	1	1
10	59.66.142.132	清华大学	8	2013-10-13 17:34:12	2013-10-13 17:54:58	197	203	2,065	2,125	1	1
11	59.66.142.132	清华大学	8	2013-10-13 15:09:55	2013-10-13 15:24:59	193	193	2,079	2,079	1	1
12	59.66.142.132	清华大学	8	2013-10-13 12:36:01	2013-10-13 13:24:58	304	405	3,423	4,619	1	1
13	59.66.142.132	清华大学	8	2013-10-13 04:18:00	2013-10-13 04:39:51	184	184	2,009	2,009	1	1

类型意义

类型=8：伪造源地址UDP Flood攻击，被攻击服务器在被管网外，攻击源在网内

其他有关问题

驻地系统后继升级功能

- 增加面向DNS服务器的DDOS攻击检测功能
- 增加近期热点的检索功能

- 增强活跃连接和活跃地址对相关信息的提供
- 将异常事件改为非授权事件

其他需要说明的问题

- NBOS只能“看见”网络中的问题，但不具备任何解决问题的能力
- NBOS追求的目标功能不是带宽计算的准确，而是安全态势感知
- NBOS系统与Chairs系统
- 当以下事件发生时，请联系我们
  - NE40路由器的重启
  - 被管网地址范围变化

THE END

Thanks & Questions