

利用 NetFlow 的被动服务发现方法

翟继强, 尹洪岩, 鲁颖新

(哈尔滨理工大学 计算机科学与技术学院, 黑龙江 哈尔滨 150080)

摘 要: 了解网络中布置了多少服务端和谁在扫描网络对于组织网络的安全管理员是非常重要的, 基于 NetFlow 技术提出一个新的服务发现方法. 该方法定义 6 个启发算法将单向的 NetFlow 流组装成面向连接的双向流, 整理输出 3 种类型的流, 进而提取 4 种类型的端点, 并在大型校园网里对这 6 个基于流数据集的启发式算法进行测试, 测试结果显示本方法可以简单有效地实现组织网络的可视化.

关键词: NetFlow; 服务发现; 被动探测; 双向流; 端点

中图分类号: TP393 **文献标志码:** A **文章编号:** 1007-2683(2014)05-0054-05

A Passive Services Discovery Method Using NetFlow

ZHAI Ji-qiang, YIN Hong-yan, LU Ying-xin

(School of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China)

Abstract: learn about which servers are deployed in the organization network and who is scanning the network. It network and security administrators. The novel service discovery method based on NetFlow is presented in this paper. The six heuristics are defined to reassemble unidirectional NetFlow flows into connection-oriented bidirectional flows, and then the three types of flow are analyzed to output, so the four types of endpoints are extracted from three types of flow. And these six heuristics on the flow dataset are evaluated on a large campus network, and the results of evaluation show that this approach provides a simple and efficient solution to gain visibility in organization networks.

Key words: NetFlow; service discovery; passive detection; bidirectional flows; endpoints

0 引 言

了解组织网络中布置了多少服务端和谁在扫描网络属于网络可视化的研究范畴, 现有的网络可视化技术可以分为两类: 主动探测和被动探测^[1]. 主动探测是通过主动扫描来检查监听服务的存在, 被动探测一般通过网络嗅探来提取服务端相关信息.

主动探测的优点是扫描快速和结果完整, 它的缺点是只能提供网络当前的快照, 而且主动扫描具有一定的入侵性, 大规模的并行高速扫描会对系统和网络造成的严重影响^[2]. 相对而言, 被动方法可以提供网络的联系视图, 探测结果不会受防火墙影响, 而且被动探测完全没有入侵性. 被动探测的缺点是不常用的服务可能要花几天甚至几周的时间才能发现^[3].

收稿日期: 2013-09-09

基金项目: 黑龙江省厅科学技术研究面上项目(12531121).

作者简介: 翟继强(1972—), 男, 博士, 教授, E-mail: zaijiqiang@126.com;

尹洪岩(1989—), 男, 硕士研究生;

鲁颖新(1980—), 女, 讲师.

在大型网络中,主动扫描的使用是受限的,因此更多采用被动探测. 现在已知的商用解决方案包括 Cisco 的安全监控分析和响应系统 MARS, Sourcefire 公司的 Real - Time Network Awareness (RNA) 和 Tenable 的 Passive Vulnerability Scanner (PVS). 这些方案的限制是必须使用流量负载信息,存储和分析大量的数据包负载是要消耗大量资源的,使得这些方法相对基于流的架构缺少伸缩性^[9]. 本文基于 NetFlow 技术提出一个简单有效的被动服务发现方法,实现连续准确检测给定网络的服务群,由此帮助网络安全管理员确定哪些是合法服务,哪些是可疑服务而报警.

1 NetFlow

NetFlow 是 Cisco 公司开发的一个网络协议,主要布置在路由器中使用数据包包头来收集流量信息^[9]. 本设计选择 NetFlow 原因如下: ①大部分网络已经布置 NetFlow 路由器,没有布置的也就可以简单实现扩充; ②相对于主动扫描,NetFlow 搜集的信息是连续更新的; ③NetFlow 技术是可伸缩和非入侵性的.

NetFlow 协议的一个流被定义为共享源 IP 地址、源端口、协议、目的 IP 地址、目的端口 5 个参数的单向顺序包组. NetFlow 网络接口每接收一个数据包,路由器将在缓冲区里查找是否存在共享以上 5 个参数的流,如果没有就创建一个新的流记录,否则更新现有流记录.

流记录分批由路由器使用 UDP 协议输出到 NetFlow 收集器,本方法使用 Nfsen/Nfdump 框架^[9]来接收和存储流记录. Nfsen 是设计用来配置和显示 NetFlow 数据的应用程序,可以启动和关闭 nfcapd 后台进程在给定时间间隔内存储流记录为压缩的二进制文件, Nfdump 则用来把这些二进制文件转换为可读的文本文件, Nfdump 同时可以使用 tcpdump 过滤语法分类、聚合和筛选流记录^[9].

NetFlow 目前为止主要用于流量统计与监控^[8-9]、网络安全态势分析^[10-11],而不是计算机端点类型的发现和识别,主要原因是 NetFlow 收集单向流,而仅仅依据单向流来是无法有效区分客户端和服务端的. 本文提出一个新的方法来重组单向流为面向连接的双向流,由此把 NetFlow 技术引入网络服务和扫描发现研究领域. 单向流是一组在给定时间窗口内由特定源到特定目的地址的数据包集

合,这样一个客户端和服务器的网络会话就包括两个单向流,第 1 个来自客户端,第 2 个来自服务器端,下面的例子说明了一个 10.0.0.1 客户端和一个 10.0.0.2 的 Web 服务器之间的网络会话.

timestamp	src IP:port	dest. IP:port	Proto	Pkts
2012-01-06 12:34:56.789	10.0.0.1:30323	10.0.0.2:80	TCP	12
2012-01-06 12:34:56.791	10.0.0.2:80	10.0.0.1:30323	TCP	11

第 1 个流为请求流,第 2 个流为应答流,通过比对源和目的地址信息可以将请求流和应答流合并为一个双向流:

timestamp	src IP:port	dest. IP:port	Proto	Pkts
2012-01-06 12:34:56.789	10.0.0.1:30323 - >	10.0.0.2:80	TCP	23

方向箭头指明了谁是客户端,谁是服务端. 在这个例子中,可以清晰看到请求流的第 1 个数据包早于应答流的第 1 个数据包 2ms 被路由器接收,由此依据时间戳确定方向相对容易. 但 NetFlow 记录的时间分辨率是毫秒级的,相对较低,请求流和应答流的时间戳会出现相等甚至滞后的情况,因此本文提出利用启发算法来解决这个问题.

2 启发算法

本文定义了 6 个启发算法来准确合并面向连接的流记录,对于处理过的每个双向流,依据流的读出顺序设置它的缺省方向,每个启发算法有 3 个可能的输出: 支持当前流向、支持反转流向、无法判定.

这 6 个启发算法是:

1) 流时序(H.0): 该启发算法依据流的时间戳判定谁是请求流,谁是应答流,如果请求和应答流具有相同的时间戳,则本启发算法无法判定.

2) 端口号(H.1): 该启发算法依据端口号来判断流向,服务端的端口号通常低于客户端,依据这个启发算法合并的双向流为高端端口到低端端口,如果源和目的端口相同,则无法判定

3) 端口阈值(H.2): 同 H.1 类似,服务端端口一般使用低于 1024 的公知端口,可以使用 1024 这个端口阈值帮助判断流向,如果源和目的端口同时大于或小于 1024 则无法判定.

4) 服务端口定义文件列表(H.3): 该启发算法依据系统文件/etc/service 来帮助判断流向,该文件定义了服务和端口的对应关系,其中的大部分公知服务端口是不能被客户端使用的. 如果源和目的端口都不在文件列表中,则无法判定.

5) 给定端口关联的端口数(H.4): 该算法比较

一个双向流中与源和目的端口相关的端口数,一个服务端(固定端口)通常要面对应多个客户端(随机端口),因此一个和多个随机端口关联的固定端口判定为服务端,如果源和目的端口的相关端口数相同,则无法判定。

6) 给定端口关联端口数阈值(H.5):该启发算法是H.4的递进,定义了一个服务端关联端口的阈值5,该值是保守估计的,具体设置来自实验分析,如果源和目的端口的关联端口号都小于5则无法判定。

后端脚本从标准输入文件中读取流记录,依据协议、源和目的IP地址、源和目的端口,使用上述启发算法来合并单向流为双向流,最后输出客户端和服务端列表。

对于TCP流,每个流的包数和TCP标志位用来区分有效和无效连接。一个有效TCP连接至少要包含两个单向流,每个单向流至少两个包,每个流中SYN和ACK要置位,这样本算法要分析3个类型的流:无法配对的单向流、有效的双向流、无效的双向流。从这3个类型的流中,可以提取4种类型的端点:

- 1) 扫描端是指没有匹配成对的单向流的源端点,或者一个无效双向流的源端点。
- 2) 客户端是指有效双向流的源端点。
- 3) 服务端是指一个有效双向流的目的端点。
- 4) 无效端点是没有匹配成对的单向流的目的端点,或者一个无效双向流的目的端点。

因为一个连接的客户端侧的源端口一般是随机分配的,所以用三元组{source IP address; protocol; destination port}定义源端点,用{destination IP address; protocol; destination port}定义目的端点。

例如从下面5组流记录中,可以提取如下信息:

Id	timestamp	source IP: port	dest. IP: port	Proto	Pkts	Flags
#1	00:00:00.555	10.0.0.1:3006	10.0.0.2:445	TCP	1	.S...
#2	00:00:01.100	10.0.1.3:4000	10.0.1.4:22	TCP	64	.SAP..
#3	00:00:01.102	10.0.1.4:22	10.0.1.3:4000	TCP	65	.SAP..
#4	00:00:20.000	10.0.2.5:21560	10.0.2.6:8080	TCP	1	.S...
#5	00:00:20.001	10.0.2.6:8080	10.0.2.5:21560	TCP	1	...R.

1) Flow #1 是一个不能和其他任何单向流匹配成对的单向流。源端点{10.0.0.1; TCP; 445}标记为扫描端,目的端点{10.0.0.2; TCP; 445}标记为无效端。

2) Flow #2 和 Flow #3 组成一个有效的双向流。源端点{10.0.1.3; TCP; 22}标记为客户端,目的端

点{10.0.1.4; TCP; 22}标记为服务端。

3) Flow4 和 Flow#5 组成一个无效双向流。源端点{10.0.2.5; TCP; 8080}标记为扫描端,目的端点{10.0.2.6; TCP; 8080}标记为无效端点。

扫描端是指产生可疑流量的端点,请求连接不存在的或被过滤掉的服务,这样的可疑流量源自网络扫描或者网络和系统的配置失误。

后端PL脚本分析流处理记录的主要工作流程如图1所示:

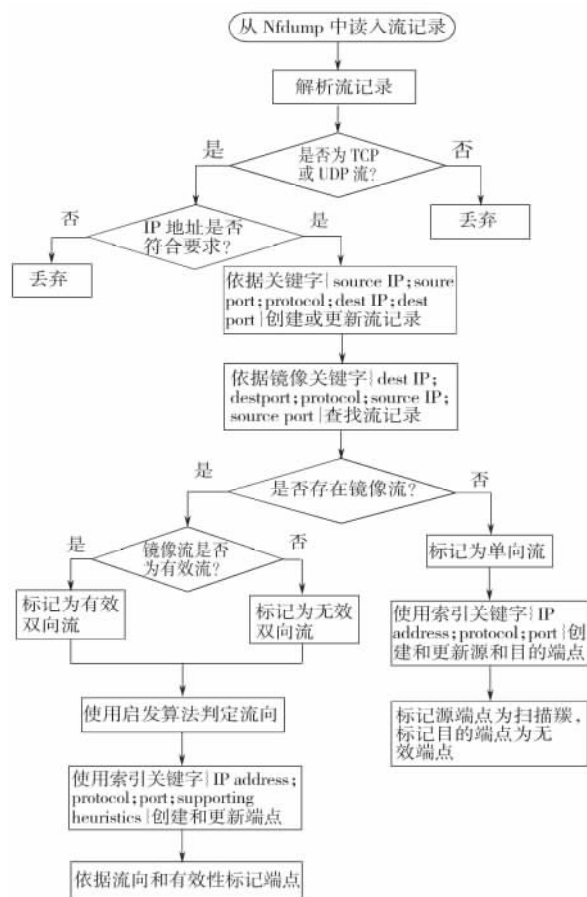


图1 流记录处理流程

3 测试和分析

通过和Nmap主动扫描^[2]发现的结果比对未来评估单个启发算法和多个启发算法组合的效率。

3.1 测试数据集

测试在哈尔滨理工大学校西区校园网内完成,包含两个C类网段(131 072个IP地址),在边界路由器进行48h持续数据采集,每5min由后台脚本生成一个输出文件,总计576个数据文件。表1显示了这些数据文件的平均统计值。

表 1 平均统计值

统计项	平均值	统计项	平均值
流记录数	442 356	合并双向流	191 315
输入流	226 831	提取的端点数	449 452
输出流	204 761	扫描端	20 269
TCP 流	271 608	客户端	157 441
UDP 流	159 985	服务端	99 226
ICMP 流	10 761	无效端	4 423
其他流	2	处理时间/s	170. 47
丢弃流	10 764		

Nfsen 框架和后台数据处理脚本运行在一台 2G 内存的 3. 8G 的双核 CPU 主机上, 每个文件的平均处理时间为 170. 47 s, 最小时间 76 s, 处理 203 522 个流, 最大时间为 296 s, 处理 877 801 个流. 后端脚本配置使用所有启发算法的组合来分析检测端点, 这就是说对于给定的双向流, 如果启发算法 H. 0 和 H. 1 支持反转流向, 而 H. 2 和 H. 5 支持当前流向, 则后端脚本接受这两种输出, 记录两个端点类型. 校园网内总计 404 615 个服务端在 48 h 内被发现, 这些服务端作为测试的基准.

3. 2 Nmap 结果分类

为了评测启发算法的准确性, 使用 Nmap 主动扫描工具检查每个 TCP 服务端的状态. 扫描发起自校园网内部, 因此不会被基于 NetFlow 边界路由器记录. Nmap 端口和服务扫描有 3 种输出:

- 1) Open: 被扫描端返回有效回应;
- 2) Closed: 被扫描端返回无效回应;
- 3) Unknown: 被扫描端没有回应.

Unknown 状态的发生, 可能因为被扫描端不是一个服务器, 或者被防火墙保护, 也可能服务是瞬变的, 不再连入网络. 为了深入了解该端点的信息, 对每一个没有回应的服务端, 要检查它是否和其他端点通信, 如果只有一个端点与之通信, 则对该端点发送主动扫描, 产生另外 3 种输出:

- 1) Source open: 该端点对主动扫描回应;
- 2) Source closed: 该端点返回无效回应;
- 3) Source unknown: 该端点没有回应.

配置主动扫描脚本在一小时内不会对同一目标做 2 次扫描, 48h 内不断有端点被发现, 每次测试结果变化不超过 0. 99%. 为判定检测的准确性, 对 Nmap 输出做如下排序: Open > Closed > Source closed > Source open > Unknown > Source unknown. 表 2 对 48h 的主动扫描结果做了总结.

表 2 Nmap 主动扫描结果分类

扫描结果	情况分析	端点数
Open	服务端存在	14 242
Closed	服务端不存在	137 407
Unknown	服务端存在但被过滤	12
	服务端不存在	
	服务端是瞬时的	
Source open	客户端实际是服务端	103 555
Source closed	客户端不是服务端	34 728
Source unknown	客户端是服务端但被过滤	8 899
	客户端是服务端但是瞬时的	
	客户端不是服务端	
Timeout	没有任何扫描回馈	105 772
总计		404 615

可以看到, 去除 105 772 个没有任何回馈的扫描超时端点, 测试中成功报告了 298 843 个扫描端点. 下面分析哪一个启发算法或启发算法的组合导致准确的检测或误报.

3. 3 单个启发算法的检测结果

表 3 给出了每个启发算法的检测结果, 第二列和第三列显示启发算法正确和错误识别的端点数, 可见 H. 2、H. 3 和 H. 5 有近乎完美的检测比率, 端点检测正确率都在 97. 71% 以上. H. 4 是 66. 92% 相对不错, 而 H. 1 只有 17. 91% 的正确检测率, 这么低的正确率说明仅仅依靠客户端端口高于服务端端口的推论是不准确的.

表 3 单启发算法正确率

启发算法	正确识别端点	错误识别端点	正确率 / %
H. 0	15 907	55 449	22. 29
H. 1	43 595	199 874	17. 91
H. 2	9 035	66	99. 27
H. 3	8 844	55	99. 38
H. 4	5 522	2 730	66. 92
H. 5	2 693	63	97. 71

H. 0 依据流向准确判定的端点类型比率是 22. 29%. 为了分析 H. 1 到 H. 5 对 H. 0 的支持, 依据请求和应答流的时序戳, 把实验结果中的端点分成 3 部分: 请求和应答流具有相同的时间戳、请求流早于应答流被记录、请求流晚于应答流被记录.

表 4 给出了针对这三组类型的端点, H. 1 至 H. 5 的检测结果. 结果显示当时间戳相同时, H. 2 至 H. 5 具有非常高的检测率. H. 2、H. 3、H. 5 在时序相

反时,推论结果也是可信的,因为最低也有 94.86% 的正确率.而 H.1 在时序相反时只有 15.66% 的对服务端的识别率.

表4 依据时序的正确率

启发算法	正确率	时间戳相同	请求先于应答	应答先于请求
H.1	正确	6 983	10 741	31 782
	错误	13 787	15 967	171 170
	比例	33.62%	40.22%	15.66%
H.2	正确	5 113	8 217	818
	错误	21	19	30
	比例	99.59%	99.77%	96.46%
H.3	正确	4 960	8 043	804
	错误	18	17	23
	比例	99.64%	99.79%	97.22%
H.4	正确	3 815	3 811	886
	错误	420	268	2 047
	比例	90.08%	93.43%	30.21%
H.5	正确	2 391	1 229	702
	错误	12	15	38
	比例	99.50%	98.79%	94.86%

3.4 启发算法组合的检测结果

对于每个双向流,每个启发算法有 3 种可能输出:

- 1) 启发算法支持反转流向,用 + 号标示;
- 2) 启发算法支持原流向,用 - 号标示;
- 3) 启发算法无法决断,用 = 号标示.

这样 6 个启发算法总计 216 种组合,经过 48 h 的测试,83 种组合记录在数据集中,依据准确率对这些组合进行排序,以消除那些导致误报的组合.在采集的 83 种组合里,39 种组合的判断存在二义性,同时输出两种流向.一些组合非常清晰的指明流向而带了更准确的判定.例如组合 (H.0 -) (H.1 +) (H.2 =) (H.3 =) (H.4 -) (H.5 -) 就有如下结果:

- 1) 流向保持: 占正确分类的服务器的 97.22%;
- 2) 流向反转: 占正确分类的服务器的 0.18%.

这个结果和上面单独分析启发算法的结果是一致的. (H.0 -) (H.1 +) (H.2 =) (H.3 =) (H.4 -) (H.5 -) 组合中,H.1 支持反转流向 (0.18%) 的准确率,而 H.0、H.4 和 H.5 支持保持原流向 (97.22% 的准确率).

对于其他一些组合,结果并不是特别清晰,如组合 (H.0 -) (H.1 -) (H.2 =) (H.3 =) (H.4 +)

(H.5 =) 就有如下的准确率:

- 1) 流向保持: 占正确分类的服务器的 7.50%;
- 2) 流向反转: 占正确分类的服务器的 2.56%.

这样的结果表明这个算法组合并不足以判定双向流的流向.

总体来看,相对于单个启发算法,使用算法的合理组合可以有效增加检测的准确率.单个启发算法实验中 H.2 和 H.3 的正确识别率是最高的,分别为 99.27% 和 99.38%,而部分算法组合的正确识别率可以达到 99.8% 以上.表 5 给出了测试中最好的 5 种组合,字母 R 标示反转流向,字母 K 标示保持流向.

表5 准确率最高的 5 种组合

方向	算法组合	正确率/%
K	H.0 = H.1 - H.2 - H.3 - H.4 = H.5 =	99.93
K	H.0 - H.1 - H.2 - H.3 - H.4 = H.5 =	99.89
R	H.0 + H.1 + H.2 + H.3 + H.4 = H.5 =	99.89
R	H.0 + H.1 + H.2 + H.3 + H.4 + H.5 =	99.85
R	H.0 = H.1 + H.2 + H.3 + H.4 + H.5 =	99.83

4 结 语

本文提出了一个简单而有效的基于 NetFlow 被动服务发现方法,定义和编写了 6 个启发算法重组单向流为面向连接的双向流,整理输出 3 种类型的流,进而提取 4 种类型的端点.通过对单个算法和算法组合的测试和比较,证明合理的选择算法和算法组合可以连续准确检测给定的服务群,帮助网络安全管理员确定网络中多少有效服务端,同时也可以了解有多少个客户端和扫描端连接本网络,进而有助于掌握系统的整体安全状态.

参 考 文 献:

- [1] 孙扬,蒋远翔,赵翔,肖卫东.网络可视化研究综述[J].计算机科学,2010,37(02):12-19.
- [2] BARTLETT G, HEIDEMANN J, PAPADOPOULOS. Understanding passive and active service discovery [C] //Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement, ACM New York, NY, USA, 2007:57-70.
- [3] WEBSTER S, LIPPMANN R, ZISSMAN M. Experience Using Active and Passive Mapping for Network Situational awareness [C] //The Fifth IEEE International Symposium on Network Computing and Applications, 2006:19-26.
- [4] LI Bingdong, SPRINGER Jeff, BEBIS George, et al. A Survey of Network Flow Applications [J]. Journal of Network and Computer Applications, 36(02):567-581.

(下转第 64 页)

- [] . IEEE Transactions on Consumer Electronics, 2008, 54(4) : 1962 – 1968.
- [6] 胡琼, 汪荣贵, 胡韦伟, 等. 基于直方图分割的彩色图像增强算法 [J]. 中国图象图形学报, 2009, 14(9) : 1777 – 1784.
- [7] STARCK Jean-Luc, MURTAGH Fionn, J EMMANUEL, et al. Gray and Color Image Contrast Enhancement by the Curvelet Transform [J]. IEEE Transactions of Image processing, 2003, 12(6) : 706 – 717.
- [8] JAYANTA Mukherjee, SANJIT K Mitra. Enhancement of Color Images by Scaling the DCT Coefficients [J]. IEEE IEEE Transactions of Image Processing, 2008, 17(10) : 1783 – 1794.
- [9] GONZALEZ R C, WOODS E. Digital Image Processing (2nd) [M]. Beijing: Publishing House of Electronics Industry, 2005: 59 – 112.
- [10] CHA Youngjoon, KIM Seongjai. The Error-Amended Sharp Edge (EASE) Scheme for Image Zooming [J]. IEEE Transactions of Image Processing, 2007, 16(6) : 1496 – 1505.
- [11] PAN Chen, PARK Dong Sun, LU Huijuan, et al. Color Image Segmentation by Fixation-based Active Learning with ELM [J]. Soft Comput, 2012, 16: 1569 – 1584.
- [12] LETICIA Rittner, JENNIFER S W C, PEDRO F et al. Analysis of Scalar Maps for the Segmentation of the Corpus Callosum in Diffusion Tensor Fields [J]. J Math Imaging Vis, 2013, 45: 214 – 226.
- [13] CHEN Xuming, YANG Simion. A Practical Solution For Ripe Tomato Recognition and Localization [J]. J Real-Time Image Proc, 2013, 8: 35 – 51.
- [14] 龚薇, 斯科, 叶秀清, 等. 一种强鲁棒性的实时图像增强算法 [J]. 传感技术学报, 2007, 20(9) : 2024 – 2028.
- [15] NAIK Sarif Kumar, MURTHY C A. Hue-Preserving Color Image Enhancement Without Gamut Problem [J]. IEEE Transactions of Image processing, 2003, 12(12) : 1591 – 1598.
- [16] YOU Ju-Yeon, CHIEN Sung-Il. Saturation Enhancement of Blue Sky for Increasing Preference of Scenery Images [J]. IEEE Transactions on Consumer Electronics, 2008, 54(2) : 762 – 768.
- [17] 于天河, 贾丽娟, 张殿龙. 红外监控系统图像增强技术的应用 [J]. 哈尔滨理工大学学报, 2012, 17(3) : 23 – 26.
- [18] GULO Jesus An. Geometric Algebra Colour Image Representations and Derived Total Orderings for Morphological Operators – Part I: Colour Quaternions [J]. J. Vis. Commun. Image R., 2010, 21: 33 – 48.
- [19] 刘松涛, 王维, 殷福亮. 基于动态广义直方图均衡的红外图像增强方法 [J]. 系统工程与电子技术, 2010, 32(7) : 1410 – 1420.
- [20] O Jr AVALDO Severino, GONZAGA Adilson. A New Approach for Color Image Segmentation Based on Color Mixture [J]. Machine Vision and Applications, 2013, 24: 607 – 618.

(编辑: 温泽宇)

(上接第 58 页)

- [5] 陈亮, 龚俭. 基于 NetFlow 记录的高速应用流量分类方法 [J]. 通信学报, 2012, 33(03) : 145 – 152.
- [6] HOQUE N, BHUYAN H M, BAISHYA R C. Network attacks: Taxonomy, Tools and Systems [J]. Journal of Network and Computer Applications, 2013, 32(9) : 34 – 48.
- [7] PILLI EMMANUEL S, JOSHI R C. NIYOGI Rajdeep. Network Forensic Frameworks: Survey and Research Challenges [J]. Digital Investigation, 2010, 7(1 – 2) : 14 – 27.
- [8] LIU Bin, LIN Chuang, QIAO Jian, et al. A NetFlow Based Flow Analysis and Monitoring System in Enterprise Networks [J]. Computer Networks, 2008, 52(5) : 1074 – 1092.
- [9] 徐兵, 胡宁, 方红琴. 基于 NetFlow 的网络流量监测系统研究 [J]. 计算机测量与控制, 2012, 20(1) : 44 – 46.
- [10] 赖积保, 王慧强, 金爽. 基于 NetFlow 的网络安全态势感知系统研究 [J]. 计算机应用研究, 2007, 24(8) : 167 – 172.
- [11] 李涛, 李飞, 张刚. 基于 NetFlow 技术的网络安全态势评估研究 [J]. 现代电子技术, 2011, 34(5) : 117 – 120.
- [12] Angela Orebaugh, Becky Pinkard. Nmap in the Enterprise [M]. Chapter 4 Using Nmap, 2008: 87 – 136.

(编辑: 温泽宇)