文章编号:1673-095X(2014)02-0042-04

基于 Snort 的多视图网络流量可视化系统

韩 丹,王劲松,宋 密
(天津理工大学 计算机与通信工程学院,天津 300384)

摘 要: 现今网络恶意行为成爆炸性增长,而传统的基于文本的网络入侵检测系统在面对海量网络数据时存在认知负担过重、交互性不够等问题. 网络安全可视化技术则可以将海量数据以图形图像的方式表现出来,在人与数据之间实现图像通信,从而使人能够快速发现网络流量中潜在的安全威胁. 本文利用 Java 可视化工具包实现了一个基于 Snort 的多视图网络流量可视化系统,该系统能对从数据库中提取出的流量警报数据进行多视图动态展示和交互操作,在一定程度上减轻了网络分析员的负担,加快了查找网络问题的进度.

关键词: 入侵检测系统; 网络安全可视化; Snort; 多视图
中图分类号: TU352.110.4 **文献标识码:** **doi:10.3969/j.issn.1673-095X.2014.02.001**

Snort-based multi-view network traffic visualization system

HAN Dan, WANG Jin-song, SONG Mi
(School of Computer and Communication Engineering, Tianjin University of Technology, Tianjin 300384, China)

Abstract: Nowadays malicious behaviors are growing rapidly on the Internet, however, there are some limitations when handle the massive network data by the traditional text-based network intrusion detection system, such as heavy cognitive burden, lack of interaction and so on. Network security visualization techniques can convert massive data into graphic to achieve image communication between man and data communications, people can find the network traffic potential security threats quickly. This paper implements a Snort-based multi-view network traffic visualization system by java visualization toolkit, extracting traffic alerts in the database for multi-view dynamic display and interaction to help network administrators to understand network security posture easily.

Key words: intrusion detection systems; network security visualization; Snort; multi-view

近几年,互联网威胁造成的计算机感染数量呈稳步上升趋势. 2013 年的“棱镜门”事件显示,美国在全球进行了 6 万多次的渗透行动,据报道美国政府入侵中国网络至少有 4 年时间,中国已经成为该项计划中网络攻击最大的受害者,国家互联网应急中心表示,中国的网络安全形势日趋严峻,网络与信息安全应上升为国家战略.

然而目前网络研究人员只能依靠大量的日志文本信息来分析和处理网络异常. 这种传统的分析方式存在着认知负担过重、交互性不够、缺乏对网络全局信息的认识等缺陷[1]. 因此,面对网络安全所面临的种种新问题,必须寻求新的方法来帮助有关人员更快速有效地发现网络中的攻击和异常事件.

可视化技术作为一种强有力的联结,连接着人脑和计算机这两种最复杂的信息处理系统[2],它作为提取信息的关键技术,在网络安全领域的地位日趋突出[3]. 虽然在硬件要求和实时性上,网络可视化技术不如传统文本分析检测系统,但它对网络行为图解说明能帮助分析人员快速直观的掌握整个网络状况和安全态势[4-5].

本文设计了一个新型的多视图流量可视化系统,数据源采用 Snort 入侵检测系统的日志数据库,

收稿日期: 2013-10-24
基金项目: 国家自然科学基金(61272450);滨海新区科技小巨人成长基金(2011-XJR12005).
作者简介: 韩 丹(1990—),女,硕士研究生,E-mail: handan715@gmail.com.
通讯作者: 王劲松(1970—),男,教授,博士生导师,E-mail: jswang@tjut.edu.cn.

利用 Java 可视化工具包实现雷达图和 3D 模型图,对网络攻击进行统计和动态展示,并实现了旋转、放缩和数据过滤等交互性操作. 和已有的可视化检测系统相比,本系统具有交互性操作方便,网络特征行为图形表现丰富并易于识别的优势,有助于网络管理员直观掌握网络安全态势.

1　系统实现

1.1　系统结构

该系统主要包括两个模块: 数据提取分析模块和可视化分析模块. 如图 1 所示.

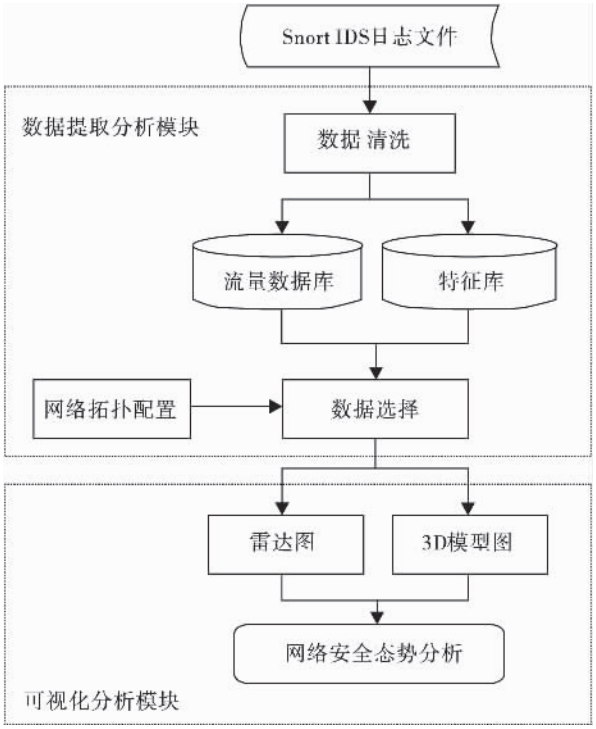

图 1　系统架构

Fig. 1　System architecture

1.2　数据提取分析模块

图 2 所示为 VastChallenge2011 年的 Snort 入侵检测系统日志文件[6]. 该系统中内置了约 20 种入侵的类型. 本次测试数据中出现了 8 种类型的攻击,它们分别是: TCP Portscan、TCP Portsweep、Fragmentation overlap、COMMUNITY SIP TCP/IP message flooding directed to SIP proxy、Tcp Window Scale Option found with length > 14、BARE BYTE UNICODE ENCODING、TCP Decoy Portscan 和 TCP Distributed Portscan.

```
[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**]
[Classification: Attempted Denial of Service] [Priority: 2]
01/27-14:07:55.230358 192.168.3.2:56760 -> 192.168.3.6:5900
TCP TTL:64 TOS:0x0 ID:2512 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xDE93EA5C  Ack: 0xA20AA6B2  Win: 0xAC0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 16772556 403107

[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**]
[Classification: Attempted Denial of Service] [Priority: 2]
01/27-14:08:15.493781 192.168.3.6:5900 -> 192.168.3.2:56760
TCP TTL:64 TOS:0x0 ID:61016 IpLen:20 DgmLen:1341 DF
***AP*** Seq: 0xA25BFD59  Ack: 0xDE93ED54  Win: 0x5B  TcpLen: 32
TCP Options (3) => NOP NOP TS: 408172 16774583

[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy [**]
[Classification: Attempted Denial of Service] [Priority: 2]
01/27-14:10:23.005903 192.168.3.2:56760 -> 192.168.3.6:5900
```

图 2　Snort IDS 日志文件

Fig. 2　Snort IDS log files

在数据提取分析模块中,利用 ETL 工具先对日志文件进行数据清洗,通过正则表达式提取出可视化所需要的流量数据和特征警报数据,并分别存入对应的数据库中,如图 3 所示. 然后读取网络拓扑数据,依照不同维度的可视化需求,从数据库中进行数据选择,生成雷达图和 3D 模型图.

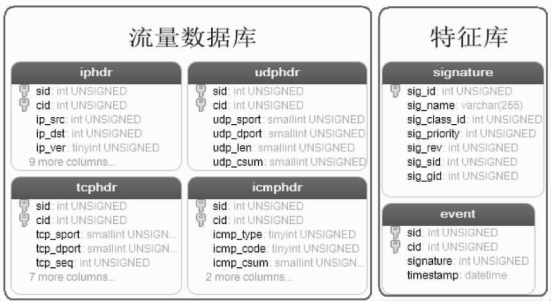

图 3　数据库表

Fig. 3　Database tables

1.3　多视图可视化模块

1.3.1　雷达图

该视图采用 processing 数据可视化工具实现. 雷达图界面分为 3 部分: 左边显示的是时间控制和颜

色对照面板，中间显示的是动态雷达图，右边显示的是历史风险直方图. 系统根据用户设置的时间段，从数据库中查找出对应的时间数据，显示在雷达图中. 如图4所示，此雷达图可视化了VastChallenge2013年Snort入侵检测系统日志. 从图4可以看出，雷达图最外层8段不同颜色的风险弧对应着8种不同的事件，里层不同大小的圆代表不同的主机类型. 雷达图中可视化了每个事件的源地址到目的地址，再到风险弧的连线. 右边的历史风险直方图可以将本次扫描的所有事件做一次统计，使管理人员能够很直观地看出一段时间内不同攻击的总数.

图4 雷达图

Fig. 4 Radar map

1.3.2 3D模型图

该模型图利用Java3D图形接口开发，如图5所示，在3D模型图的中央，形象的用一堵墙来代表网关，将内外网隔离开，不同网段的主机采取按照网络拓扑配置采用网格布局算法进行整齐排列，不同网段的主机用不同颜色的球体表示，每个球体之间粗细不同的连线代表主机间的通信，通信量越大则连接线越粗. 按照时间顺序，动态地展示主机间通信的过程，视图下方明确地显示出当前系统时间和数据包的产生时间.

如图6所示，该三维视图支持多种交互操作，比如视图放缩，旋转移动、显示通信端口，球体下方带有数字标号的立方体代表主机的通信端口，其中绿色的立方体表示此次事件中连接的发起方端口，红色的立方体表示此次事件中连接的目的方端口；点击位于球体下方的圆锥体，可以显示报警与本主机相关的事件统计信息.

如果网络拓扑复杂，主机过多导致产生的三维视图画面复杂的情况，则可以对视图进行选择性过滤. 过滤对象不仅针对主机，更细分到了主机下的每个通信端口. 过滤方法有两种：一是通过直接点击表示主机的球体或表示端口的立方体，配合勾选视图下方的主机过滤或端口过滤复选项来进行过滤；二是通过定义过滤规则，过滤规则间还可选择不同逻辑连接词：与或非. 如图7所示，过滤内容包括：源IP地址、目的IP地址、源端口、目的端口、协议类型、警报优先级、数据包时间.

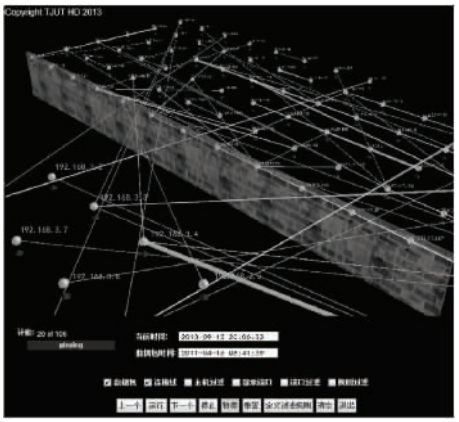

图5 网络3D模型图

Fig. 5 Network 3D model diagram

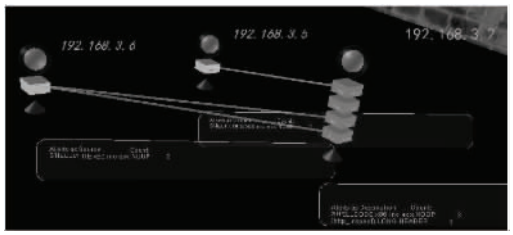

图6 3D模型图的交互操作展示

Fig. 6 Interoperability showcase of 3D model diagram

图7 规则过滤窗口

Fig. 7 Rule of filtering window

2 讨 论

H. Koik和K. Ohno研发的SnortView[7]系统采

用二维图形显示 Snort 报警信息. 该系统使用不同的图标区分报警类型，并且采用垂直的红线表示报警数量，以防止由于在一段连续的时间内产生大量同种类型的报警而发生重叠. 该系统可以实时地对 Snort 报警进行分等级显示，但与本系统相比，可视化视图单一并缺乏交互性操作.

VisFlowConnect[8] 和 Visalert[9] 系统采用平行轴坐标技术表现连接信息，该方法有利于检测来自内部的攻击. 单纯分析大量网络日志信息，虽然能分析出针对某台主机的扫描事件，但不能同时发现某一网段的扫描事件，而且当信息量过大时，视图过于混乱，不易辨识出有效信息. 相比之下，本文设计的系统采用的多重过滤操作可以在大数据环境下屏蔽掉大量非敏感信息，而且 3D 模型图的旋转操作方便管理员从多个角度对网络进行观察.

CMV[10] 系统采用交互式的多视图可视化方法，对无线网络中常见的 Sybil 攻击进行识别和分析. 该系统由三个视图组成：时间直方图、结点连接图、散点图. 多视图的表现方法能够从多个角度对攻击进行分析，但是和本文设计的系统相比，CMV 所能表现得网络攻击不够丰富，仅能对特定的攻击进行有效分析.

3　结　论

本系统采用多视图对 Snort 日志文件进行了可视化分析. 雷达图能够依据事件顺序，再现 Snort 安全事件，从图上能够直接读出事件的源地址，目的地址和事件的类型，具有相对实时性. 风险历史直方图对风险事件次数做了一次统计，方便网络管理人员做出相应的判断. 由于雷达图可视化的安全事固定，只对 8 种常见的安全事件做了可视化，如果有其他的安全事件，则要手动添加另外的颜色表示，扩展性不强. 但是 3D 模型图弥补了雷达图的缺陷，能够自动表示出所有的安全事件，而且对端口信息也进行了可视化，方便管理员辨别事件的发起方和目的方，以及每个主机对应的安全事件，而视图的放缩和数据过滤等交互性操作也在很大程度上有助于管理员了解整个网络安全态势，快速发现网络中存在的问题.

参　考　文　献：

[1] 吕良福，张加万，孙济洲，等. 网络安全可视化研究综述[J]. 计算机应用，2008，28(8)：1924-1927.

[2] Foresti S，Agutter J. VisAlert：From idea to product [C] // Goodall J R，Conti G，Ma K L. Proceedings of the VizSEC 2007 workshop on visualization for computer security. Berlin Heidelberg：Springer，2008：159-174.

[3] 周　宁. 信息可视化技术在端口扫描检测中的应用研究[D]. 天津：天津大学，2007.

[4] Le Malécot E，Kohara M，Hori Y，et al. Interactively combining 2D and 3D visualization for network traffic monitoring [C] //Proceedings of the 3rd international workshop on Visualization for computer security. New York：ACM，2006：123-127.

[5] Fu Lu L，Wan Zhang J，Lin Huang M，et al. A new concentric-circle visualization of multi-dimensional data and its application in network security [J]. Journal of Visual Languages & Computing，2010，21(4)：194-208.

[6] Visual Analytics Community. VAST challenge 2013：Mini - Challenge3 [EB/OL] (2013 - 08 - 15) [2013 - 10 - 23] http：//www. vacommunity. org/VAST + Challenge + 2013%3A + Mini - Challenge + 3.

[7] Koike H，Ohno K. SnortView：visualization system of snort logs [C] //Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. New York：ACM，2004：143-147.

[8] Yin X，Yurcik W，Slagell A. The design of VisFlowConnect - IP：A link analysis system for IP security situational awareness [C] // Third IEEE International Workshop on Information Assurance. Los Alamitos，CA：IEEE Computer Society，2005：141-153.

[9] Foresti S，Agutter J. VisAlert：from idea to product [C]. //VizSEC 2007. Proceedings o f the Workshop on Visualization for Compater Security. Springer Berlin Heidelberg，2008：159-174.

[10] Harrison L，Hu X，Ying X，et al. Interactive detection of network anomalies via coordinated multiple views [C] // Proceedings of the Seventh International Symposium on Visualization for Cyber Security. New York：ACM，2010：91-101.