DOI: 10.13245/j.hust.161107

面向网络安全事件的入侵检测与取证分析

龚 俭 王卓然 苏 琪 杨 望

(东南大学计算机与工程学院, 江苏 南京 211189)

摘要 为了提高安全事件应急响应的效率,设计并实现了一个入侵检测与取证分析自动化响应模型.该模型基于特定的安全事件信息,使用 OpenFlow 交换机实现报文的过滤和转发,利用 PF_RING ZC 零拷贝工具自动采集报文流量,使用开源入侵检测软件 Suricata 和多特征关联冗余消除算法完成对网络流量的入侵检测和警报冗余消除,同时结合 Bro 系统进行应用层协议分析以完成对网络流量的取证分析,可显著减少人工的干预.通过僵尸主机的检测实例对该模型进行了验证,结果表明了该模型对于提升安全事件应急响应效率的有效性.

关键词 安全事件; 应急响应; 入侵检测; 冗余消除; 取证分析

中图分类号 TP309 **文献标志码** A **文章编号** 1671-4512(2016)11-0030-04

Intrusion detection and forensic analysis for network security incidents

Gong Jian Wang Zhuoran Su Qi Yang Wang

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

Abstract To improve the efficiency of the security incident response, an intrusion detection and forensic analysis automation response model was designed and implemented. The model was based on the particular security event information, OpenFlow switches were used for packet filtering and forwarding, PF_RING ZC Zero-Copy tool was used to automatically collect packet traffic, and open source intrusion detection software Suricata and multi-feature associated redundancy elimination algorithm were used to complete network intrusion detection and redundance elimination of intrusion event. Bro system was combined with application layer protocol analysis to complete forensic analysis of network traffic, which could significantly reduce manual intervention. Various parts of the automated response model were analyzed in detail by bots detected experiment, the results show the effectiveness of the model for enhancing the efficiency of the security incident response.

Key words security incidents; emergency response; intrusion detection; redundancy elimination; forensic analysis

"十一五"期间 211 工程在 CERNET (China Education and Research Network)网络安全中心和 38 个核心节点上建设高性能网络管理与安全保障系统[1],功能包含监控网络的实时运行状态、检测网络安全的异常和隐患,及时响应网络安全事件等. CHAIRS(cooperative hybrid aided incidence response system)系统[2]是该项目的应急响应协同系统,为各节点的安全管理人员提供应急响应管理功能,提高了 CERNET 安全事件响应的效率.

然而随着大量安全事件的检出,在应急响应过程中原有的安全保障系统暴露出缺乏响应的入侵跟踪与取证分析的缺陷.本研究对原有的安全保障系统进行了功能上的增强(BIG-CHAIRS),

收稿日期 2016-08-01.

作者简介 龚 俭(1957-),男,教授,E-mail: jgong@njnet.edu.cn.

基金项目 国家自然科学基金资助项目(61602114).

使其可以满足网络安全事件应急响应的新需求. 改进包括：基于特定的安全事件信息，使用 OpenFlow 交换机实现报文的过滤和转发，利用 PF_RING ZC 零拷贝工具自动采集报文流量，使用开源入侵检测软件 Suricata 和多特征关联冗余消除算法完成对网络流量的入侵检测和警报冗余消除，同时结合 Bro 系统进行应用层协议分析以完成对网络流量的取证分析. 最后将分析结果回送给 CHAIRS 系统进行应急响应协同.

原始数据的收集、数据的过滤、元信息分析、取证分析以及结论表示是网络取证与分析流程的常见步骤[3]. 这里实现的取证分析流程主要包含：原始报文的收集，报文的过滤，应用层协议分析，结论表示. 取证分析流程的第 1 步为原始报文的收集，其来源为 CERNET 南京节点边界流量. 报文的过滤通过特定攻击对象信息对原始报文进行过滤，以达到数据精简的目的. 应用层协议分析通过应用层的语义分析来获取当前的网络行为特征，并根据网络行为特征信息进行网络行为频度分析. 结论表示针对取证分析流程进行总结，获取到相关结论，最终以证据的形式进行提交.

1　BIG-CHAIRS 自动化响应模型

图 1 为 BIG-CHAIRS 自动化响应模型，其中，HYDRA(hybrid detection respone agent)[4] 为基于 SDN 技术的入侵阻隔系统，该系统经过 OpenFlow 交换机[5] 控制网络报文的转发，可以在保证网络正常运行的同时，实现对恶意流量的阻断、对攻击流量的样本采集. CHAIRS 系统为应急响应管理系统，为安全管理人员提供了应急响应管理功能，提高了安全事件应急响应的效率. MONSTER(monitor on network security and tool for emergency response)[6] 为入侵检测和响应系统，功能包含网络报文采集及过滤、入侵检测协同及响应等.

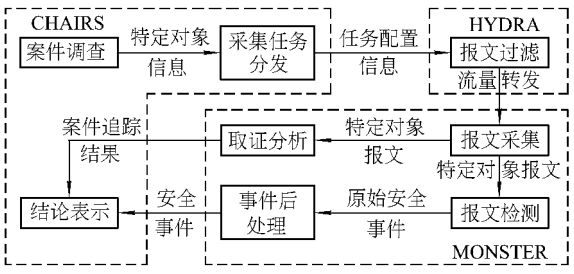

图 1　BIG-CHAIRS 自动化响应流程

当安全调查员进行案件调查时，CHAIRS 系统将产生待跟踪和取证的特定对象信息(以 IP 及其相关特征来表示)，并以此对象信息自动生成任务配置信息发送给 HYDRA 系统，HYDRA 系统自动将含有特定对象的流量转发给 MONSTER 系统，MONSTER 系统将以攻击报文流为输入，自动地进行入侵检测和取证分析.

在入侵检测流程中，报文检测模块将依据攻击报文流自动产生原始安全事件，接着在事件后处理模块中进行冗余消除生成安全事件发送给 CHAIRS 系统. 而在取证分析流程中，取证分析模块将对攻击报文流进行语义分析，以此来对攻击对象的后续行为进行持续性的观察(攻击追踪)，最后将攻击追踪结果回送给 CHAIRS 系统进行应急响应协同.

2　BIG-CHAIRS 自动化响应模型的实现

BIG-CHAIRS 自动化响应模型系统结构图如图 2 所示，设计重点在于 MONSTER 系统中入侵检测和取证分析功能的实现，CHAIRS 系统和 HYDRA 作为其协同系统共同完成自动化的响应流程. MONSTER 系统的设计分为报文采集、入侵检测和取证分析三个部分.

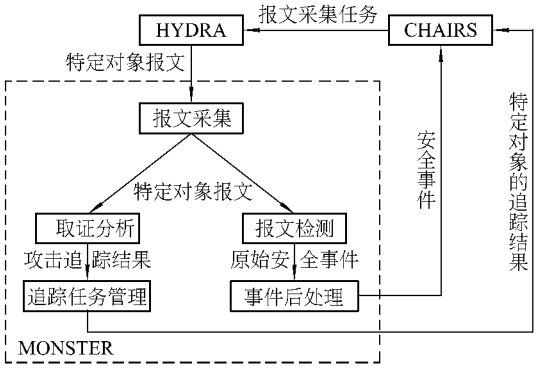

图 2　MONSTER 系统详细设计

2.1　报文采集

当接收到 HYDRA 系统发送过来的采集任务配置任务(含有案件编号和采集时间范围信息)后，报文采集模块自动配置 PF_RING ZC[7] 零拷贝工具，将 HYDRA 转发过来的特定对象报文收集并保存为 pcap 文件，文件保存在以案件编号，采集时间范围作为唯一标志的文件中. 而当当前报文采集任务正常结束后，报文采集模块将给报文检测和取证分析模块发送处理通知信息.

2.2　入侵检测

入侵检测功能由报文检测模块和事件后处理模块共同完成. 报文检测模块基于开源入侵检测软件 Suricata[8] 完成，当接收到报文采集模块的

通知信息后,Suricata 对报文采集阶段存储的特定对象的报文进行基于规则的离线检测,检测完成后会生成警报日志文件 eve.json.接着,报文检测模块自动调用脚本对 eve.json 进行处理,提取其中的 signature 和四元组信息生成原始安全事件.原始安全事件自动发往事件后处理模块,利用多特征关联冗余消除算法[9]进行冗余消除,生成简单攻击事件,最后发送给 CHAIRS 系统.

2.3 取证分析

取证分析实现基于开源入侵软件 Bro[10]完成,当接收到报文采集模块的通知信息后,Bro 将自动进行离线检测产生日志文件.接着,取证分析模块将抽取日志文件中的数据(主要是 bro 报警内容字段信息)生成当前的网络行为特征,若发现异常的网络行为特征,则根据不同 IP 发生各种网络行为的频度进行统计,进而发现哪些机器正在发起攻击或者已经感染网络病毒.接着,取证分析模块将网络行为特征信息和频度分析结果进行自动汇总生成追踪任务结果,发送给 CHAIRS 系统进行应急响应协同.

3 BIG-CHAIRS 自动化响应总体流程

BIG-CHAIRS 自动化响应总体流程如图 3 所示,CHAIRS 系统完成最初的案件调查和最终的结论表示,HYDRA 系统完成报文过滤,MONSTER 系统完成报文采集、入侵检测和取证分析流程.

在此自动化响应流程中,大部分步骤都是自动衔接的,而须要人工干预的地方主要有:初始的案件调查阶段,冗余消除规则的编写和提前置入,判断网络行为特征是否存在异常.

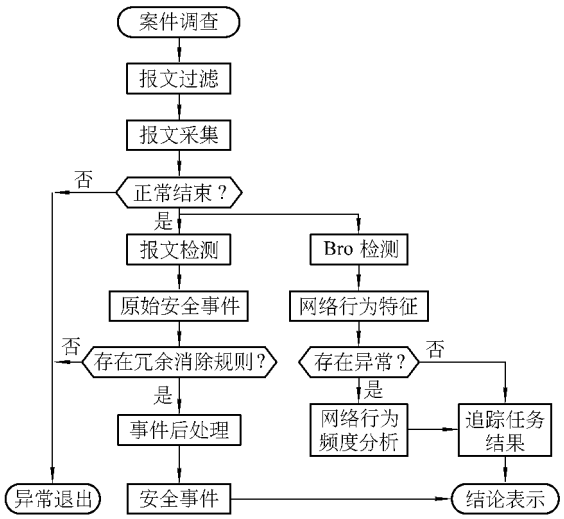

图 3 BIG-CHAIRS 总体流程图

4 实验与分析

4.1 实验过程

为了测试 BIG-CHAIRS 自动化应急响应流程的有效性,本研究以僵尸网络主机的自动化响应作为说明.僵尸网络的检测判定主要分为僵尸网络的 C&C 域名的检测判定和僵尸网络的僵尸主机的检测判定.安全事件调查员从 CHAIRS 中获取案件进行调查,CHAIRS 系统将根据案件中包含的疑似僵尸网络控制器的信息以及调查员设置的报文采集起始和结束时间配置采集任务,并将其自动发送给 HYDRA 进行流量的过滤转发.MONSTER 系统将在此流量信息基础上自动进行入侵检测和取证分析,以期获得对僵尸网络主机的检测判定,进而对僵尸网络进行定性.

如图 4 所示,MONSTER 系统对 HYDRA 转发过来的流量进行自动的采集和存储,存储格式为:案件编号_采集起始时间_采集结束时间.

```
-rw-r--r-- 1 '          users 1.1M Jun  7 09:58 1888_2016-05-30
T10:00:00_2016-06-07T10:00:00.pcap
-rw-r--r-- 1 '          users 621K Jul  7 18:17 1888_2016-06-25
T07:30:00_2016-07-02T07:30:00.pcap
```

图 4 自动报文采集结果

报文采集结束后将自动进入入侵检测和取证分析流程:如图 5 所示,入侵检测完成后,从 Suricata日志记录中得到原始安全事件共 68 条,根据攻击类型的名称自动选取冗余消除规则"eventname= bot and samefield = {SRCIP,DSTIP,DSTPORT} and timeout=3600"进行多特征关联的冗余消除,处理后得到安全事件 39 条.

取证分析主要基于 Bro 进行应用层协议分析.如图 6 所示,Bro 检测完成后,取证分析模块得到 3 条网络行为特征(dns_unmatched_msg,2838)、(DNS_Conn_count_too_large,213)及(dns_unmatched_reply,128),由于发现大量的异常网络行为特征,因此随后自动进入网络行为频度分析,以获得僵尸主机的列表.

4.2 实验结果分析

采用实例(僵尸主机的检测)来验证入侵检测与取证分析自动化流程的有效性.在案件调查员调查案件后,CHAIRS 系统将含有疑似僵尸主机控制器的信息配置成采集任务自动发往 HYDRA 系统,HYDRA 系统自动完成配置任务中既定时间的报文过滤和转发,并将其自动发往 MONSTER 系统,以进入报文采集、入侵检测和取证分

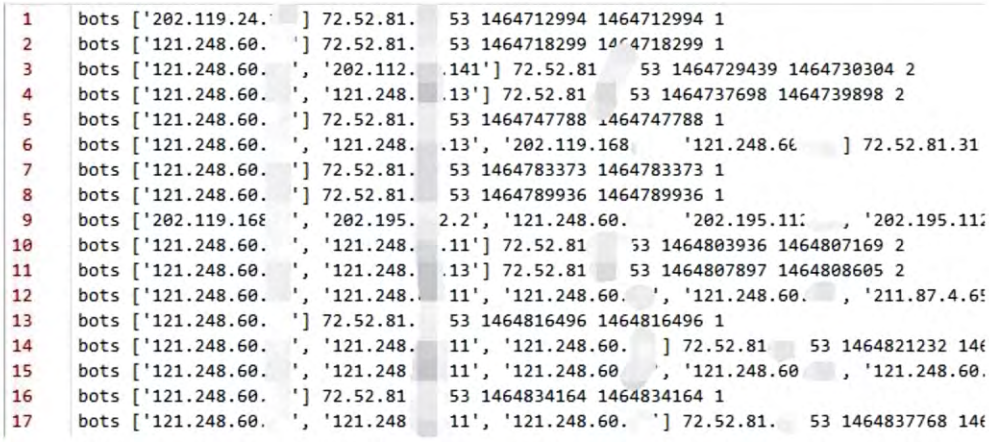

图 5　特定对象的安全事件

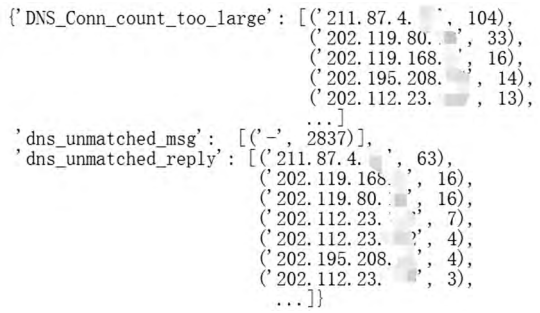

图 6　网络行为分析结果

析流程.

相比于传统的手动采集报文，在报文采集流程中，MONSTER 系统依旧对 Hydra 发送过来的采集任务信息自动进行报文采集，并将其以案件编号_采集起始时间_采集结束时间.pcap 的格式进行了存储.

入侵检测流程中，报文检测模块依据报文采集流程中保存的报文进行自动检测，生成原始安全事件 68 条，接着原始安全事件经过自动的事件后处理得到安全事件 39 条，然后这些信息被自动发送给 CHAIRS 系统进行入侵响应协同. 在入侵检测流程中，系统自动完成了报文检测和警报冗余消除(须要提前置入冗余消除规则)，一方面，减少了人工的干预；另一方面，事件的后处理(冗余消除)也有效的减少了警报数量，进一步提升了安全事件响应的效率.

取证分析流程中，取证分析模块依据报文采集流程中保存的报文自动进行应用层的协议分析，并从检测日志中提取网络行为特征 3 条，由于网络行为特征中出现异常类型，然后进行网络行为频度分析，得到僵尸主机列表. 最后，这些信息将自动汇总形成追踪任务摘要信息，发送给 CHAIRS 系统进行应急响应协同. 在取证分析流程中唯一须要人工干预的地方在于从网络行为中判断是否存在异常，考虑到网络攻击行为的广泛性，要建立统一的自动化判断标准是比较困难的. 除此之外，取证分析流程都是自动完成的，这在很大程度上提升了安全事件应急响应的效率.

参　考　文　献

[1] 马亚洲，龚俭，杨望. 面向应急响应的高速网络流量采集设计与实现[J]. 通信学报，2014，11：46-51.

[2] 朱礼智，龚俭. 分布式网络应急响应管理系统 CHAIRS 的设计与实现[D]. 南京：东南大学计算机科学与工程学院，2015.

[3] 杨泽明，许榕生，曹爱娟. 网络取证与分析系统的设计与实现[J]. 计算机工程，2004，30(13)：72-74.

[4] 金磊，龚俭. 基于 SDN 技术的网络入侵阻断系统 HYDRA 的设计与实现[D]. 南京：东南大学计算机科学与工程学院，2016.

[5] ONF. The OpenFlow switch specification[EB/OL]. [2016-06-10]. http://ONF.org.

[6] 孙成峰，龚俭. 面向万兆网络的滥用入侵检测系统改进[D]. 南京：东南大学计算机科学与工程学院，2013.

[7] Ntop. PF_RING ZC (zero copy)[EB/OL]. [2016-06-10]. http://www.ntop.org/products/packet-capture/pf_ring/pf_ring-zc-zero-copy/.

[8] Suricata. Suricata open source IDS/IPS/NSM engine [EB/OL]. [2016-06-10]. https://suricata-ids.org/.

[9] 龚俭，梅海彬，丁勇，等. 多特征关联的入侵事件冗余消除[J]. 东南大学学报：自然科学版，2005，35(3)：366-371.

[10] Nick Buraglio. Overview of the Bro intrusion detection system[EB/OL]. [2016-06-10]. http://faster-data.es.net/assets/20150522-Buraglio-Bro.pptx.