智能配电系统入侵检测方法研究*

黄世泽[1]，王梦莹[2]，徐秋勇[3]，郭其一[3]，屠旭慰[4]
(1.同济大学 道路与交通工程教育部重点实验室，上海 201804;
2.同济大学 铁道与城市轨道交通研究院，上海 201804;
3.同济大学 电子与信息工程学院，上海 201804;
4.浙江中凯科技股份有限公司，浙江 温州 325604)

摘　要: 针对智能配电系统在运行过程中经常遇到的关键技术问题，从防入侵的角度出发，分析研究了 Snort 开源入侵检测系统，总结了现有 Modbus/TCP 协议异常报文入侵检测规则。在此基础上提出了基于白名单模型的 Modbus/TCP 异常报文入侵检测方法，给出了白名单入侵检测模型及其算法。在 Visual Studio 平台设计开发了白名单规则生成系统，并说明了白名单规则的生成过程及原理。搭建了测试系统，通过试验证明了基于白名单模型的 Modbus/TCP 异常报文入侵检测方法的可行性。

关键词: 智能配电系统; Snort 开源入侵检测系统; Modbus/TCP 异常报文; Visual Studio; 控制与保护开关

中图分类号: TM 76　**文献标志码:** A　**文章编号:** 2095-8188(2018)21-0036-07

DOI: 10.16628/j.cnki.2095-8188.2018.21.008

黄世泽(1983—)，男，副研究员，研究方向为信息安全、电磁兼容仿真与测试。

Research on the Method for Intrusion Detection of Intelligent Power Distribution System

HUANG Shize[1]，*WANG Mengying*[2]，*XU Qiuyong*[3]，*GUO Qiyi*[3]，*TU Xuwei*[4]
(1. Key Laboratory for Road and Transportation of the Ministry of Education, Tongji University, Shanghai 201804, China; 2. Institute of Rail Transit, Tongji University, Shanghai 201804, China;
3. College of Electronics & Information Engineering, Tongji University, Shanghai 201804, China;
4. Zhejiang Zhongkai Science Company Limited, Wenzhou 325604, China)

Abstract: From the point of view of intrusion prevention, the Snort open source intrusion detection system was analyzed and studied. This paper summarized the existing Modbus intrusion detection rules, put forward a Modbus intrusion detection method based on the white list model, and gave the Modbus white list intrusion detection model as well as its algorithm. The white list rule generation system was designed in Visual Studio, and the production process as well as the principle of white list rules were also introduced. An experiment based on the existing equipment and tools was carried out to prove the feasibility of the Modbus intrusion detection method based on the white list model.

Key words: intelligent power distribution system; Snort open source intrusion detection system; Modbus/TCP abnormal message; Visual Studio; control and protective switching devices

0　引　言

据匡恩网络《2015 工业控制网络安全态势报告》中对2015 年相关安全事件遭受攻击方式进行统计分析的结果，攻击方式呈现出多样化，其中基于网络的入侵现象最为严重，例如，2003 年美加

王梦莹(1996—)，女，研究方向为智能配电系统。
徐秋勇(1992—)，男，硕士研究生，研究方向为智能配电系统研究与设计。
* 基金项目: 国家自然科学基金(61703308); 中央高校基本科研业务

电网发生特大面积停电事故,造成事故的主要原因是蠕虫病毒阻碍了加拿大安大略省从停电事故中恢复正常供电的进程[1]。可见抵御恶意攻击、阻止病毒入侵系统以及检测入侵行为已经变得刻不容缓。但从整体上来说,对应用于工业控制系统的入侵检测系统的研究仍处于起步阶段,国内外只有少量针对工控系统入侵检测的研究。

已有研究者创新性地将 Snort 入侵检测系统移植到了工业以太网中去,并利用现有的条件构建了模拟测试环境验证了此方法的可行性,但 Snort 是一个开源系统,安全规则制定还不够完善,仍需改进[2]。伊朗核电站发生的"震网"事件也表明,现场总线网络可能遭受网络攻击,协议也绝非安全,需要应用入侵检测技术对现场总线网络上的设备进行保护。现有专门针对 Modbus/RTU 协议进行检测的 Snort 入侵检测系统,将 Modbus/RTU 的协议数据单元转换为 Modbus/TCP 的应用数据单元,再利用现有规则对 Modbus/TCP 数据包进行检测,从而保证 RTU 数据包的安全性[3-4]。又有研究在 Snort 系统的基础上增加了一种能处理 Modbus/RTU 报文的数据获取模块 DAQ,无需修改代码本身或增加其他硬件,即可实现对 Modbus/RTU 报文的检测[5]。此外,有学者设计了应对已知攻击方式的基于协议分析的入侵检测方法,并编写了相应的 Modbus 入侵检测规则,该文献为 Modbus 入侵检测规则设计提供了思路,但无法应对未知或新出现的攻击方式[6]。

因此,有必要设计一套完善的入侵检测方法,以便及时发现并处理入侵,给信息管理层提供安全保障,从根本上保障智能配电系统的安全运行。

本文从防入侵的角度出发,分析研究 Snort 开源入侵检测系统的原理,总结了现有 Modbus/TCP 协议异常报文入侵检测规则,并在此基础上设计基于白名单模型的 Modbus/TCP 异常报文入侵检测方法,给出白名单入侵检测模型及其算法,设计相应的白名单检测规则,利用现有设备及工具,搭建智能配电系统安全性测试平台,验证基于白名单模型的 Modbus/TCP 异常报文入侵检测方法的可行性。

1　入侵检测系统 Snort 技术分析

1.1　Snort 简介

Snort 是著名的开源入侵检测系统。它是一个基于规则检测的 NIDS[7],主要由包解码器、预处理器、检测引擎以及报警输出模块构成,协作完成特定攻击的检测,并生成相应的报警。Snort 体系结构图如图 1 所示[8]。

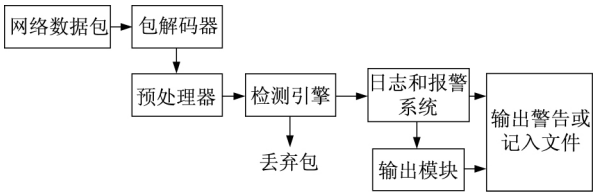

图 1　Snort 体系结构图

Snort 一般有 3 种工作模式:嗅探器模式、包记录器模式以及入侵检测模式。本文主要利用 Snort 的入侵检测模式对智能配电系统通信过程中的异常行为进行检测。通过对智能配电系统通信过程中的异常行为进行分类,并编写相应的入侵检测规则,使 Snort 能检测外界对系统的入侵。

1.2　Snort 规则

Snort 规则是 Snort 系统中最为关键的构成部分,有了完整的规则之后,系统才能对入侵行为进行匹配,从而产生报警[9]。Snort 规则由两部分组成:规则头以及规则选项,如图 2 所示。

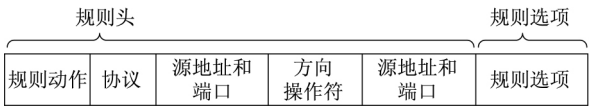

图 2　Snort 规则结构

(1) 规则头。规则中的重要构成部分,其定义了报文的源地址、目的地址、包含的协议等一些信息,以及规则被触发时应该做出的响应。通过这些对报文的限制,规则需要处理的数据量就会被大大减少,从而提高了效率。

(2) 规则选项。规则匹配的基础主要是为了供检测引擎在对规则头分析的基础之上作进一步分析匹配。规则选项在规则头后面的括号里,其内容可选,可以包含多个规则选项,每个选项之间用";"分开。选项之间的关系属于逻辑与,只有当所有条件都匹配时,规则动作才可能被触发。

1.3　已有 Modbus/TCP 异常报文检测规则分析

Snort 入侵检测系统从 2.9 版本开始加入 Modbus 等工业通信协议的预处理器,可对通信报文进行匹配分析;同时,第三方研究机构 Digital Bond 也发布了 Modbus/TCP 异常报文入侵检测

规则,根据工控系统中针对 Modbus 漏洞的攻击制定了相应的报警规则,有效地防护系统的安全。

(1) Modbus/TCP 协议请求报文分析。Modbus/TCP 协议报文应用数据单元包含报文头、功能码以及数据 3 个部分。假设主站向从站发送一个报文,如"00 01 00 00 00 06 08 03 00 A1 00 01"。该报文用来请求读取保持寄存器的内容,即读取设备的通信地址。

(2) Modbus/TCP 协议响应报文分析。Modbus/TCP 协议的响应报文也包括 3 个部分:报文头、功能码以及数据。对应上面的报文请求,响应报文为"00 01 00 00 00 05 08 03 02 00 08"。该报文为返回保持寄存器的内容,即返回设备的通信地址。

从 Modbus/TCP 异常报文发起的攻击行为如表 1 所示。

表 1　从 Modbus/TCP 异常报文发起的攻击行为

类别	异常行为描述
诊断寄存器重置	通过发送功能码 08 及子功能码 0A 的指令来清空设备的诊断寄存器和计数器
远程重启	通过发送功能码 08 及子功能码 01 的指令来使现场设备重新启动
强制仅收听	通过发送功能码 08 及子功能码 01 的指令来使设备处于强制仅收听的状态,而不对请求的报文进行响应
从站攻击	通过发送功能码 17 的指令,获取设备状态信息
异常数据包长度	报文长度不合法

针对上述分类异常行为,Modbus/TCP 异常报文入侵检测规则已被编写并发表得到了具体应用[10]:

(1) 诊断寄存器重置入侵检测规则;

(2) 强制仅收听入侵检测规则;

(3) 远程重启入侵检测规则;

(4) 从站攻击入侵检测规则;

(5) 异常数据包长度入侵检测规则。

这些规则均适合于智能配电系统安全需求,但都只能应对一种具体的攻击形式,通过对攻击方式进行特征提取,再对报文进行分析匹配,从而发现攻击。如果出现新类型的 Modbus/TCP 异常报文攻击形式,那么已有规则就无法检测,从而给系统遗留遭受攻击的风险。因此有必要研究一种能检测新型攻击形式的入侵检测方法,通过建立白名单模型,将白名单以外的所有 Modbus/TCP 报文进行匹配,以及时发现入侵。

2　基于白名单模型的 Modbus/TCP 异常报文入侵检测方法设计

2.1　基于白名单的 Modbus/TCP 异常报文入侵检测模型

Modbus 在通信过程中最重要的 3 个要素分别为:设备地址、功能码以及寄存器或线圈起始地址。三者存在着一定的联系。智能配电系统中常用的设备种类相对比较固定,主要有可通信控制与保护开关(CPS)、可通信电表以及 PLC 等,且每一类设备都有固定的功能。由此可建立基于白名单的入侵检测模型。基于白名单的 Modbus/TCP 异常报文入侵检测模型如图 3 所示。

由图 3 可见,本模型中根据功能对设备进行分类,对每一类设备分配具体的地址范围,同时根据需要建立可信任功能码集合,并为每个功能码建立允许操作起始地址集合,就构建了地址码、功能码、起始地址三者之间的联系,从而建立了可靠的入侵检测模型。具体的入侵检测算法如下:

第一步:读取一条 Modbus/TCP 的数据报文,并分别提取其地址码、功能码以及起始地址字段。

第二步:判断地址码是否在已设定的可信范围内。若不在可信范围内,则说明为异常报文或入侵报文,系统报警显示;若在可信范围内,则继续第三步。

第三步:将从报文提取的功能码与该地址码所信任的功能码集合进行对比,判断该功能码是否属于该地址码可信任的功能码集合内。如果属于,则继续第四步;如果不属于,则视为异常报文或入侵报文。

第四步:将从报文中提取出的寄存器或线圈起始地址与该功能码允许操作的起始地址集合进行对比,判断该起始地址是否属于该功能码允许操作的起始地址集合内。若属于,则判定该报文正常;若不属于,则判定该报文异常或视为入侵报文,系统报警显示。

2.2　入侵检测规则编写

Snort 只能手动编写规则,没有相应的图形化界面,大大增加了规则编写的难度。因此,本文利用 Visual Studio 平台开发了一个具有图形化操作界面的Modbus/TCP异常报文入侵检测白名单规

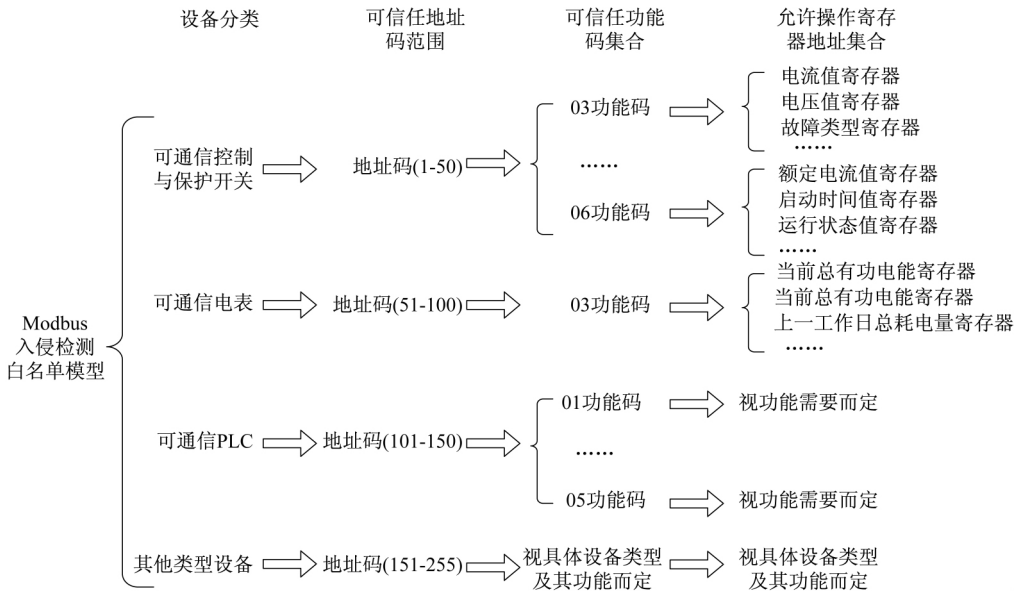

图3　基于白名单的Modbus/TCP异常报文入侵检测模型

则设计系统,可以在界面上进行操作快速生成规则,为规则编写提供了便利。本文设计的Modbus/TCP异常报文入侵检测白名单规则设计系统界面如图4所示。

图4　Modbus/TCP异常报文入侵检测白名单规则设计系统界面

Modbus/TCP异常报文入侵检测白名单规则分为两部分,一是功能码白名单规则,二是寄存器地址白名单规则,只有两者结合起来才能形成一套完整的入侵检测白名单规则。由图4可知,本规则设计系统用了两个规则生成按钮,分别生成功能码白名单规则以及寄存器地址白名单规则。

规则设计系统主要分为规则头设计与规则体设计两部分。规则头设计为公共部分,本文提出的基于白名单的Modbus/TCP异常报文入侵检测规则设计的重点在于规则体的设计,其中最重要的部分为对字符匹配内容(Content)的设计。通过对Content的设计,Snort可以对Modbus/TCP报文进行检测,从而判断该报文是否为合法报文。

在功能码白名单以及寄存器地址白名单的字符匹配内容设计中用到了逻辑非的概念,将不属于白名单中的功能码以及寄存器地址排除在外。

2.3　入侵检测实例分析

下面列举了具体实例来说明字符匹配内容的含义。

假设设备地址为2的可通信CPS只允许使用功能码03以及06,同时03功能码只允许操作地址为00 A1的寄存器以及地址为00 A2的寄存器,06功能码只允许操作地址为00 A3的寄存器,此时功能码白名单Content部分的内容为

content: "|00 00|"; offset: 2; depth: 2; content: "|02|"; offset: 6; depth: 1; content: !"|03|"; offset: 7; depth: 1; content: !"|06|"; offset: 7; depth: 1;

由上面对Modbus/TCP报文的分析以及Snort规则的分析可知,content: "|00 00|"; offset: 2; depth: 2;表示报文数据部分偏移2个字节后的2个连续字节,即Modbus协议标识符,用于确认该报文为Modbus报文。

content: "|02|"; offset: 6; depth: 1;用于检查设备地址,判断该报文是否发送给地址为2的

设备。

content:!"|03|"; offset:7; depth:1; content:!"|06|"; offset:7; depth:1;用于检测功能码是否为03或06,如果都不是,则正好匹配规则,产生报警。

寄存器地址白名单Content部分的内容为

content:"|00 00|"; offset:2; depth:2; content:"|02|"; offset:6; depth:1; content:"|03|"; offset:7; depth:1; content:!"|00 A1|"; offset:8; depth:2; content:!"|00 A2|"; offset:8; depth:2;

此对应功能码为03的情况:content:"|03|"; offset:7; depth:1;用于匹配03功能码;content:!"|00 A1|"; offset:8; depth:2; content:!"|00 A2|"; offset:8; depth:2;用于检测寄存器地址是否为00 A1以及00 A2,如果都不是,则正好匹配规则,产生报警。

content:"|00 00|"; offset:2; depth:2; content:"|02|"; offset:6; depth:1; content:"|06|"; offset:7; depth:1; content:!"|00 A3|"; offset:8; depth:2;

此对应功能码为06的情况:content:"|06|"; offset:7; depth:1;用于匹配06功能码;content:!"|00 A3|"; offset:8; depth:2;用于检测寄存器地址是否为00 A3,如果不是,则正好匹配规则,产生报警。

通过这几条规则的组合就可建立地址码为02,允许功能码为03、06,以及03功能码允许操作寄存器地址00 A1、00 A2,06功能码允许操作寄存器地址00 A3的入侵检测白名单规则集合。利用此集合就可检测到其他格式的报文并产生报警,从而保证了地址码为02的设备的通信安全。

在利用Modbus/TCP异常报文入侵检测白名单规则设计系统进行规则设计时,只需要在相应的位置填写内容,按规则生成按钮生成相应的规则,并可同步将规则保存到White_list规则文件中去,生成的规则在系统最下面的显示框内即可查看,白名单规则实例如图5所示。

当Snort检测引擎检测到报文与规则中规定的内容匹配时,就会产生报警,提醒工作人员发现入侵报文或可疑报文,从而增加了系统通信过程的安全。上面列举了设备地址码为02,允许功能码为03、06,以及03功能码允许操作寄存器地址00 A1、00 A2,06功能码允许操作寄存器地址00 A3的规则编写原理及具体的生成过程,对于

```
alert tcp $MODBUS_CLIENT  any -> $MODBUS_SERVER  502
(flow:from_client,established; msg:"Suspicious or unauthentic
message!!!"; sid:10001; rev:1; priority:1; content:"|00 00|"; offset:2;
depth:2; content:"|02|"; offset:6; depth:1; content:!"|03|"; offset:7;
depth:1; content:!"|06|"; offset:7; depth:1;)

alert tcp $MODBUS_CLIENT  any -> $MODBUS_SERVER  502
(flow:from_client,established; msg:"Suspicious or unauthentic
message!!!"; sid:10002; rev:1; priority:1; content:"|00 00|"; offset:2;
depth:2; content:"|02|"; offset:6; depth:1; content:"|03|"; offset:7;
depth:1; content:!"|00 A1|"; offset:8; depth:2; content:!"|00 A2|";
offset:8; depth:2; )

alert tcp $MODBUS_CLIENT  any -> $MODBUS_SERVER  502
(flow:from_client,established; msg:"Suspicious or unauthentic
message!!!"; sid:10003; rev:1; priority:1; content:"|00 00|"; offset:2;
depth:2; content:"|02|"; offset:6; depth:1; content:"|06|"; offset:7;
depth:1; content:!"|00 A3|"; offset:8; depth:2;)
```

图5　白名单规则实例

系统中用到的其他一些设备,都可以通过上述方法编写与其对应的白名单规则,从而构建整个系统的白名单检测规则集合。

3　测试与验证

3.1　试验系统搭建

本文利用现有通信CPS设备搭建了一套测试系统,用以测试上文提出的基于白名单的Modbus/TCP异常报文入侵检测方法的正确性。测试系统架构图如图6所示,具体的实物测试环境如图7所示。

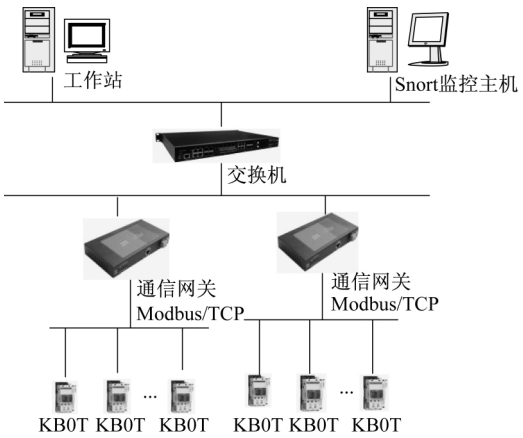

图6　测试系统架构图

Snort入侵检测系统安装于Snort监控主机中,用于检测系统通信链路中的报文。一旦发现与规则匹配的报文就发出警告。它的安装与配置

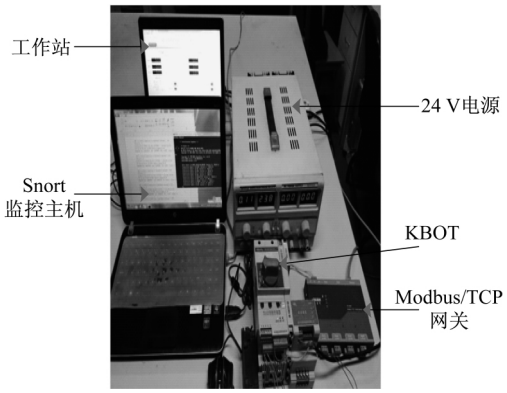

图7　测试系统实物图

是整个系统的核心,通常采用“传感器+数据库+分析平台”的3层体系架构,其中传感器采用WinPcap作为系统底层接口驱动,Snort作为数据包获取、筛选以及转储程序;数据库采用MySQL作为数据库存储相关信息;分析平台采用BASE作为能够查询数据库的分析平台,BASE的优势体现在对报警信息的图形化展示上,能以图形化的界面代替文本的显示。但Snort在2.9版本之后就不再支持直接将报警信息记录到MySQL数据库中,不能在BASE分析平台上对报警信息进行查看与分析。如果需要,可以在UNIX或者Linux平台下,利用Barnyard插件实现相关信息到MySQL数据库的转存,从而实现在BASE平台上对报警信息的查询。在没有安装BASE分析平台的情况下,可以在alert.ids文件中查看具体的报警信息。

Snort入侵检测系统安装完成后需要对Snort.conf文件进行修改,配置主站、从站的IP地址以及添加自定义的规则等。这里需要将上文编写的白名单规则添加进来,并禁用已有的规则,只需在Snort.conf文件的“Customize your rule set”部分添加自定义规则文件名即可。

3.2　试验结果与分析

首先启动Snort入侵检测系统,在命令行cmd中输入c:\snort\bin\snort -c “c:\snort\etc\snort.conf” -l “c:\snort\log”,其中,-c “c:\snort\etc\snort.conf”用于指定Snort配置文件的路径,-l “c:\snort\log”用于将报警信息记录到日志中。

本文首先用Wireshark抓包软件抓取主站发送给从站的Modbus/TCP报文,对抓取的报文进行分析,再与设定的规则进行比较,最后分析得到的试验结果,看是否与预期的结果一致。Wireshark抓包软件抓取到的Modbus/TCP请求报文如图8所示。

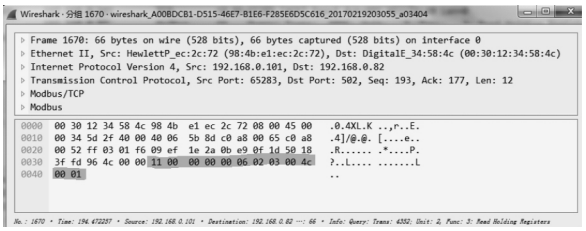

图8　Modbus主站发送的请求报文

由图8可知,主站发送的Modbus/TCP请求报文为11 00 00 00 00 06 02 03 00 4c 00 01,用于读取设备地址为02的KB0T的启动时间值,功能码为03,寄存器起始地址为00 4c。

本文编写的白名单入侵检测规则规定地址码为02的设备允许使用的功能码为03、06,同时03功能码允许操作的寄存器起始地址为00 A1、00 A2。而上面发送的请求报文寄存器起始地址00 4c不属于允许操作寄存器地址,不在规定的白名单内,因此匹配了相应的规则,具体为

alert tcp 192.168.0.15/24 any -> 192.168.0.82/24 502 (flow: from_client, established; msg:" Suspicious or unauthentic message!!!"; sid: 10002; rev: 1; priority: 1; content:"|00 00|"; offset: 2; depth: 2; content:"|02|"; offset: 6; depth: 1; content:"|03|"; offset: 7; depth: 1; content:!"|00 A1|"; offset: 8; depth: 2; content:!"|00 A2|"; offset: 8; depth: 2;)。

Snort入侵检测系统在检测过程中就会根据匹配到的规则发出相应的警告,可以在c:\snort\log\alert.ids文件中查看具体的报警信息,如图9所示。

```
[**] [1:10002:1] Suspicious or unauthentic message!!! [**]
[Priority: 1]
02/24-15:29:16.794640 192.168.0.15:50381 -> 192.168.0.82:502
TCP TTL:64 TOS:0x0 ID:25263 IpLen:20 DgmLen:52 DF
***AP*** Seq: 0xAE898304  Ack: 0x6D7EA07  Win: 0x3F39  TcpLen: 20

[**] [1:10002:1] Suspicious or unauthentic message!!! [**]
[Priority: 1]
02/24-15:29:17.095692 192.168.0.15:50381 -> 192.168.0.82:502
TCP TTL:64 TOS:0x0 ID:25266 IpLen:20 DgmLen:52 DF
***AP*** Seq: 0xAE898310  Ack: 0x6D7EA12  Win: 0x3F37  TcpLen: 20

[**] [1:10002:1] Suspicious or unauthentic message!!! [**]
[Priority: 1]
02/24-15:29:17.385765 192.168.0.15:50381 -> 192.168.0.82:502
TCP TTL:64 TOS:0x0 ID:25267 IpLen:20 DgmLen:52 DF
***AP*** Seq: 0xAE89831C  Ack: 0x6D7EA1D  Win: 0x3F34  TcpLen: 20
```

图9　入侵检测结果

由图9可知,Snort在运行过程中检测到了Modbus/TCP异常报文,并根据设定的规则记录了相应的报警信息,与预期的结果一致,能够很好地证明所设计的基于白名单模型的Modbus/TCP异常报文入侵检测方法的可行性。

4 结　语

在互联网中,入侵检测系统通过抓取数据链路层报文,根据已有规则进行匹配,从而检测报文是否为可疑或入侵报文,能很好的防范黑客从网络对主机进行攻击。本文将其应用于智能配电系统中,通过检测Modbus/TCP报文,匹配自定义规则,从而保证主站发送指令的安全性,能有效的防止入侵。

提出了基于白名单模型的Modbus/TCP异常报文入侵检测方法。通过建立地址码、功能码以及寄存器或线圈起始地址之间的关系,给出了白名单入侵检测模型,并设计了相应的白名单检测规则,能对通过Modbus/TCP协议发起的攻击进行有效的检测,从而能够及时发现攻击并进行处理,有效保障了智能配电系统的安全性。

本试验主要是为了验证文中设计的基于白名单模型的Modbus/TCP异常报文入侵检测方法的可行性,通过对alert.ids文件中报警信息的分析可以很直观地说明该方法的可行性以及正确性,无需再用BASE平台对报警信息进行分析。在UNIX或者Linux平台下利用Barnyard插件实现在BASE平台上对报警信息进行查询是本文需要完善的地方。

【参 考 文 献】

[1] 李帅,王先培,王泉德,等.基于SMDP强化学习的电力信息网络入侵检测研究[J].电力自动化设备,2006,26(12):75-78.

[2] 任恺.入侵检测系统在工业以太网中的应用[D].武汉:中南民族大学,2008.

[3] MORRIS T, PAVURAPU K. A retrofit network transaction data logger and intrusion detection system for transmission and distribution substations [C] // Power and Energy (PECon),2010 IEEE International Conference on. IEEE,2010:958-963.

[4] MORRIS T, VAUGHN R, DANDASS Y. A retrofit network intrusion detection system for Modbus RTU and ASCII industrial control systems [C] // System Science (HICSS),2012 45th Hawaii International Conference on. IEEE,2012:2338-2345.

[5] TYLMAN W. Native support for Modbus RTU protocol in Snort intrusion detection system [M]. New Results in Dependability and Computer Systems. Springer International Publishing,2013:479-487.

[6] 罗耀锋.面向工业控制系统的入侵检测方法的研究与设计[D].杭州:浙江大学,2013.

[7] 李坊标.基于snort的网络入侵检测系统NIDS的研究和应用[D].上海:上海交通大学,2008.

[8] 谢少春.Snort入侵检测系统的研究及其性能改进[D].西安:西安理工大学,2008.

[9] 王建忠.基于Snort的分布式入侵检测系统的研究与设计[D].兰州:兰州理工大学,2007.

[10] PETERSON D. Quickdraw: Generating security log events for legacy SCADA and control system devices [C] // Conference For Homeland Security, 2009. CATCH09. Cybersecurity Applications & Technology. IEEE,2009:227-229.

收稿日期:2018-10-10