基于虚拟蜜网的用电信息采集系统攻击检测方法

曹康华 董伟伟 汪锦量 周 林 王 勇
(上海电力大学计算机科学与技术学院 上海 200000)

摘 要 高级量测体系(AMI)是智能电网系统测量、接收、存储、分析和操作用户消耗数据的基础。消费者(智能电表)和公用事业之间的通信和数据传输需求使 AMI 的安全性显著下降。并且,随着大量新型智能采集终端的接入,以及多种通信方式、通信协议的应用,用电信息采集系统面临的网络攻击越来越频繁。系统目前侧重于采集终端的上线率和通信信道的连通性,缺乏相应的安全防护措施。针对以上问题,设计并实现了虚拟蜜网在用电信息采集系统上的部署方案,解决了传统蜜网硬件资源浪费的问题。同时设计数据控制算法对数据包进行检测,有效解决了攻击流量的控制问题。最后,进行了渗透攻击测试,并结合蜜网的三大核心功能对实验结果进行了分析,结果表明本方案可以有效检测到攻击。

关键词 用电信息采集系统,通信协议,网络攻击,安全防护,虚拟蜜网
中图法分类号 TP393.08 **文献标识码** A

Attack Detection Method for Electricity Information Collection System Based on Virtual Honeynet

CAO Kang-hua DONG Wei-wei WANG Jin-liang ZHOU Lin WANG Yong
(Shanghai University of Electric Power, College of Information and Technology, Shanghai 200000, China)

Abstract The Advanced Measurement System (AMI) is the basis for smart grid systems to measure, collect, store, analyze and manipulate user-consumed data. The communication and data transfer requirements between consumers (smart meters) and utilities significantly reduce the security of AMI. The electricity information collection system uses a variety of communication methods, communication protocols and new intelligent collection terminals. Therefore, the network attacks faced by the electricity information collection system are extremely frequent. Since the system currently focuses on the uplink rate of the acquisition terminal and the connectivity of the communication channel, there is a lack of corresponding security protection measures. Aiming at the above problems, the deployment scheme of the virtual honeynet on the power information collection system was designed and implemented, which solves the problem of waste of traditional honeynet hardware resources. At the same time, the data control algorithm is designed to detect the data packet, which effectively solves the control problem of attack traffic. Finally, the penetration attack test was carried out, and the experimental results are analyzed by combining the three core functions of the honeynet, which show that the scheme can effectively detect the attack.

Keywords Electricity information collection system, Communication protocol, Network attacks, Security protection, Virtual honeynet

1 引言

信息技术的快速发展使得智能电网这种崭新的能源管理模式应运而生,智能电网的建设是我国的重要战略部署,而高级量测体系(AMI)是实施智能电网的关键一步。利用安全、可靠的通信网络实现用户与供电方之间的双向互动是 AMI 的一个重要特征。

用电信息采集系统是 AMI 的关键组成部分。它的开放性和互动性给自身带来了很多威胁,如关键业务信息被非法窃取和破坏、设备被冒用、非法控制等安全隐患[1]。2009 年的美国黑帽安全会议上,有人演示并验证蠕虫病毒可以在 24 小时内感染智能电表,导致 1.5 万用户失去电力供应[2]。2014 年 10 月,研究人员发现了西班牙电表的安全漏洞,黑客可以利用这个漏洞攻击电表致使用电数据异常,甚至切断整个电路系统导致大面积停电;2015 年 12 月,黑客在乌克兰国家电网中植入了恶意软件,使多个区域的电网受到网络攻击,22.5 万民众失去电力供应[3]。大量攻击事件的发生,引发了安全专家对电力信息网络安全防护技术的研究。

本文将蜜网技术应用到真实的小型用电信息采集系统中,给出了虚拟蜜网在上面部署一个解决方案,这样既解决了

本文受国家自然科学基金资助项目(61772327),上海自然科学基金资助项目(16ZR14366300),浙江大学工业控制技术国家重点实验室开放式基金资助项目(ICT1800380),上海电力学院智能电网产学研开发中心基金资助项目(A-0009-17-002-05),上海市科委地方能力建设基金资助项目(15110500700)资助。

曹康华(1994—),女,硕士生,主要研究方向为用电信息采集系统安全防护,E-mail:akckh780823@163.com;**董伟伟**(1994—),女,硕士生,主要研究方向为智能电表通信安全。

传统的蜜网配置硬件利用率低、管理不方便等问题，又弥补了防火墙、身份认证等被动防御的不足。对进一步智能电网安全防御体系的建设起到了抛砖引玉的作用。

2 相关工作

目前，国内外信息网络的防御系统的设计和开发已经形成了一定的规模，包括提出入侵检测方法、安全网络协议的验证、信息安全评价体系的研究等[4]。但是，针对电力信息网络安全的主动式防御研究还比较少。例如，Faisal 等[5]提出了一种入侵检测系统(IDS)架构，通过分析智能电网中的 AMI 数据流和 IDS 数据集，证明了这种架构所利用的数据流挖掘算法的有效性。Wang 等[6]引入了用于评估 IDS 体系结构的成本模型框架。在加强智能电网安全的关键管理方面，Ye 等[7]提出了一种称为集成认证和机密性(IAC)的新型协议，以确保 AMI 通信的安全性。Liu 等[8]提出了一种适用于大量设备的新型管理模型。

但是，传统的被动网络防御技术如防火墙[9]、入侵检测[10]等存在着网络攻防不平衡的问题：1)因为攻击方处于隐蔽环境，存在未知的威胁和风险；2)因为现在的防御体系基本上都是依靠现有的、已知的一些漏洞、病毒等，需要一定的先验知识[11]。

蜜网是一种十分有效的主动式防御机制，它可以通过诱骗攻击者使攻击者误以为蜜罐主机就是真实服务主机，从而起到保护真实服务主机的作用[12]。在电力信息领域有许多致力于开发蜜罐的努力。其中，Conpot[13]是一种开源的低交互蜜罐，专为工业控制系统(ICS)而设计，并且得到了积极的维护。Conpot 支持多种 Internet 和 ICS 特定协议，如 Modbus。ShaPe[14]是专为智能电网设计的蜜罐系统。然而，以上研究的重点是设备级仿真，即智能电子设备(IED)，并且不提供物理系统仿真的任何支持。Fan 等针对存在限制其应用场景的功能缺陷问题，提出了一个通用的虚拟蜜网管理工具来解决这个问题[15]。但是其准确度并不高，并不能获取更复杂的网络拓扑信息。Ren 等制定和分析隔室模型以探索病毒流行与异构蜜网的效力之间的相互作用，并提出了一些限制病毒传播和改进蜜网设计的想法[16]。但是在部署蜜网时，由于有限的成本和潜在的风险，蜜罐很可能被用作跳板来攻击第三方，因此更多的蜜罐不一定更好。Sokol 等关注第一序列的 AR 模型和基于该模型的 bootstrap 来预测对蜜网的攻击[17]，但是该模型不适用于网络安全领域的其他时间序列。易秀双等通过对蜜网架构和主要技术的研究，分析了虚拟蜜网的工作流程，在此基础上给出了一种虚拟蜜网的部署方案[18]。但是该方案并没有应用于真实的系统中且缺乏具体数据控制策略，不能保证其有效性和攻击检测率。

3 用电信息采集系统的介绍

用电信息采集系统(以下简称“采集系统”)是构建智能电网的物理基础，采用先进的传感、通信、自动控制等技术，通过收集和掌握用户的用电数据，来及时发现异常情况，以便于数据统一管理、电能质量数据统计和线损统计分析[19]。通过监控、测量和控制不同用户的电力负荷，来更好地实现阶梯电价和智能费控等营销策略。

如图 1 所示，采集系统由主站层、通信信道层、采集设备层 3 部分构成。主站层包含各种服务器、工作站、全球定位系统(GPS)时钟、防火墙以及相关的网络设备，主要完成业务应用、收集所有采集设备存储的数据、下发控制指令、前置通信调度和数据库管理等功能。系统主站通过通信信道与采集终端进行数据的远程通信。通信信道包括光纤专网、230 MHz 无线专网、通用无线分组业务/码分多址(GPRS/CDMA)无线公用网络等[11]。采集设备是安装在现场的终端及计量设备，负责采集和存储整个系统的原始用电数据，包括专变采集终端、集中器、采集器以及智能电表等[20]。

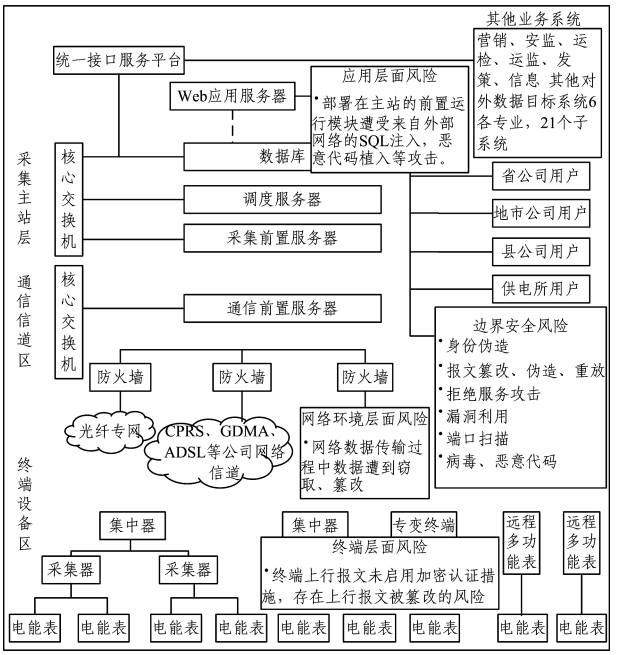

图 1 采集系统结构及安全威胁[21]

由于业务涉及用电控制指令，在产生、传送、执行等多个环节可能发生对指令进行篡改、伪造和重放的危险。因此，采集系统面临内网边界、业务应用、通信信道和采集设备等多个层面的安全威胁[21]。

4 蜜网的核心功能分析与配置

一种用于检测和分析未知攻击媒介的网络安全措施是蜜罐。蜜罐通常是一个“诱饵”系统，旨在吸引网络攻击者，以便及早发现攻击企图，减缓和减轻攻击，收集攻击痕迹有利于学习攻击媒介和设计网络安全系统。而蜜网由多个蜜罐组成，实际上它是一种研究型、高交互型蜜罐。

蜜网技术从第一代的概念性证明，到第二代的改进，目前已经进入到完整、易部署、易维护的第三代[18]。本文在 Windows 操作系统下，采用 Honeywall Roo 和 VMware 软件在用电信息采集系统上部署虚拟蜜网。该方案最主要的部分是 Honeywall(蜜墙)，这个蜜网网关是第三代蜜网的心脏，因为它能够完成蜜网的三大核心功能：数据捕获、数据控制和数据分析。

为了便于分析蜜网的三大核心功能，先给出本文所用到的用电信息采集系统上的虚拟蜜网部署方案，如图 2 所示。蜜网网关有 3 个接口：Eth0，Eth1 和 Eth2。其中，Eth0 采用桥接模式与主机的一块物理网卡相连，并通过该网卡与外部网络通信；Eth1 与虚拟蜜罐相连，采用仅主机模式；Eth2 采用桥接模式与主机的另一块网卡相连，并通过该网卡与内部管理网络通信。

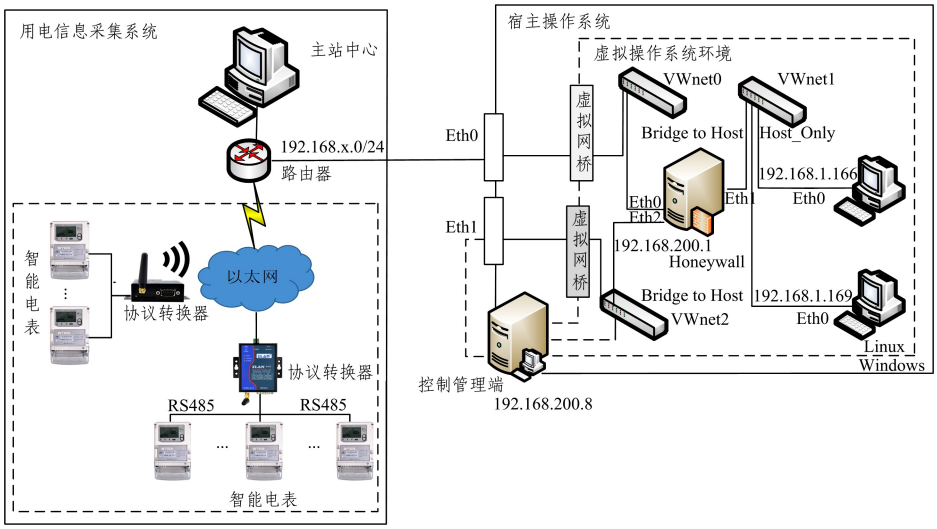

图 2　虚拟蜜网在采集系统上的网络拓扑

本文先搭建了真实的小型用电采集系统，然后选择虚拟机的最佳网络连接方式，来实现更高效率的工作方式。其次进行蜜网的相关配置，蜜网正常工作后，进行相应的端口扫描、数据捕获、数据控制和数据分析等工作。其主要的过程如图 3 所示。

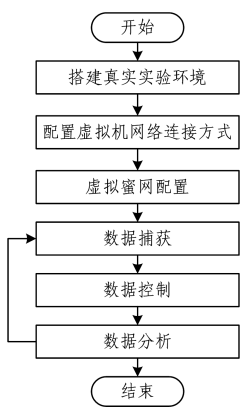

图 3　用电信息采集系统攻击检测流程图

4.1　数据捕获

蜜网内的所有活动和进出蜜网的信息都经过蜜网网关，在攻击者不知道被监视的情况下实现数据捕获，为进一步分析入侵提供素材。数据捕获的实现流程如图 4 所示。

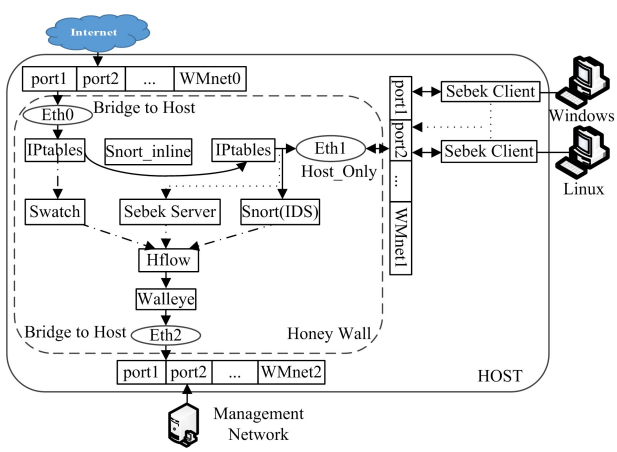

图 4　数据捕获流程图

蜜网通过基于防火墙日志、snort 记录的网络流和 sebek 捕获的系统活动 3 个层次来捕获数据。

(1)基于防火墙日志

入侵者的数据包首先经过虚拟交换机 VMnet0，从 Eth0 流入 Honeywall 后将通过 IPtables 防火墙，防火墙会根据设置好的规则将进入的连接记录到/ var/ log/ messeges。此时对流入的攻击不进行过滤，可跳过 Snort_inline。

(2)Snort 记录的网络流

Snort 进程会在链路层捕获所有的数据流量和内部接口 Eth1 的数据包信息，用于后续的攻击数据分析。

(3)Sebek 捕获的系统活动

蜜罐在对于攻击者是隐形状态的前提下，还要能够捕获产生在其上的全部数据。Sebek 是一个在数据加密情况下进行数据捕获的强大工具，它由客户端和服务端两部分组成。因此每个蜜罐上都必须装有 Sebek 客户端，用于记录蜜罐上的所有数据包，并且可以通过隐秘通道传送到位于 Honeywall 的 Sebek 服务器上。

4.2　数据控制

数据控制机制可以控制通过蜜网的数据流量，这主要是为了确保一旦蜜网中的蜜罐被攻陷，所有的恶意活动就必须限制在蜜网内。数据控制功能的实现主要通过两种手段：1)限制对外连接数；2)对攻击包进行抑制。具体的数据控制实现如图 5 所示。

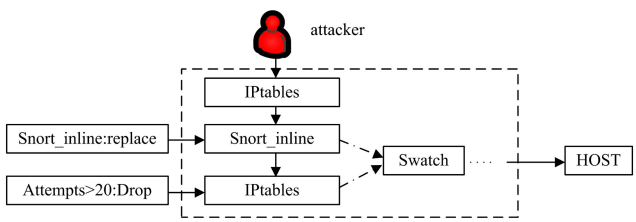

图 5　数据控制实现

根据图 4 所示的结构，数据控制的第一个策略是预先在 IPtables 中设置特定的规则。当源自蜜罐的连接数超过每分钟 20 个时，IPtables 会将它们记录到日志中并断开后续连接。同时，防火墙将数据包发送到 Snort_inline，Snort_inline 将已知的攻击数据包设置为 Replace。如果传出数据包超过每分钟 20 或发现已知攻击，系统将通过 Swatch 向主机(管理机)发送警报邮件。这可以避免网络嗅探或对第三方的攻击。

数据控制的第二个策略是通过 Eth0 将所有流向 192.168.x.0/24 字段的数据都定向到 Honeywall 宿主主机上。

在 IPtables 模块完成数据流量导向，设置如下：

[root@hnroot]# Iptables-P INPUT DROP

[root@hnroot]# Iptables-P FORWARD DROP

[root@hnroot]# Iptables-P OUTPUT ACCEPT

[root@hnroot]# Iptables-A FORWARD-I eth0-d

由于数据控制直接影响了用电采集系统的安全性，因此本文结合以上介绍的两种策略实施数据控制。首先当数据包被检测到是已知的攻击时，直接断开后续连接并报警。如果数据包不满足第一个条件时，判断 IP 地址是否在白名单中，如果在白名单中则数据均通过 Eth0 导向 Honeywall 宿主主机上。当数据包从 Honeypots 向外发起的连接数每分钟如果超过 20 个，则断开此 IP 后续连接，并通过 Swatch 产生 Email 报警邮件发给宿主主机(管理机)。其中，数据用 B 表示；数据包是否满足黑名单用 A 表示；子网 IP 用 X 表示；数据包从 Honeypots 向外发起的连接数每分钟为 i 个。数据控制算法如算法 1 所示。

算法 1 数据控制算法

If A=1 then

系统将通过 Swatch 向主机(管理机)发送警报邮件；

end

Else if 0<X<120

数据均通过 Eth0 导向 Honeywall 宿主主机上；

If i>20

系统断开此 IP 后续连接，并通过 Swatch 向主机(管理机)发送警报邮件；

end

end

4.3 数据分析

数据分析是数据捕获后的一项重要任务。利用蜜网中的安全软件，例如将入侵防御系统(Snort_inline)和入侵检测系统(Snort)组合在一起，可以全面分析流入和流出蜜网的数据，并可以显示分析结果。从图 3 和图 4 的数据捕获和数据流中可以看出，数据分析主要使用两种机制：自动报警机制和辅助分析。

本文从 3 个层面进行数据分析。首先，Swatch 工具为蜜网中的 Snort_inline 日志文件和 IPtables 提供可视化功能，并在受到攻击时根据相应特征的配置文件进行匹配，并通过 Eth2 向管理网络发出报警邮件。Sebek 服务器收集并处理 Sebek 客户端发送的信息，Snort 记录并统计流入蜜网的流量。其次，Hflow 软件接收经过 Swatch、Sebek 服务器和 Snort 的预处理数据，将这些信息整合以后输出到辅助分析工具 Walleye。最后，辅助分析工具使用 Walleye，这是一个安装在 Honeynet 网关上功能强大的基于浏览器的数据分析工具。在该控制界面中，可以监控、配置和管理整个蜜网系统，有利于直观地了解攻击过程，管理员还可以实时掌握蜜网网络的最新动向。

5 虚拟蜜网配置与实验分析

5.1 蜜网的配置

为了方便分析，在图 1 中已经给出在用电信息采集系统中的蜜网部署架构图，将数据中心的主机作为宿主主机。攻击机的 ip 地址为 192.168.1.180。VWnet0，VWnet1 和 VWnet2 是虚拟机软件提供的虚拟交换机，网桥也是虚拟机提供的服务。这些虚拟设备经过配置后可以直接使用，具体设备信息如表 1 所列。

表 1 虚拟蜜网配置列表

设备	系统/软件	型号/版本
宿主主机 操作系统	Windows XP SP3	型号：DELL Inspiron 14R 5437 RAM：4G
虚拟机 1 (Honeywall)	Honeywall-Roo-1.4.hw-2008	处理器：1 RAM：256
虚拟机 2 (Linux 系统)	Ubuntu 7.10	处理器：1 RAM：512
虚拟机 3 (Windows 系统)	Windows 7 旗舰版	处理器：1 RAM：512
虚拟机软件	VMware Workstation	Vmware-workstation-full-14.1.3
内核级 捕获工具	Sebek	Sebek-win32-3.0.5 Sebek-linux26-3.2.0b

5.2 渗透攻击测试

在进行实验之前，先测试一下 Host 主机与 Honeypot 主机之间的连通性，用 Host 主机 ping 一下 Honeypot 主机，再用 Honeypot 主机 ping 一下 Host 主机。测试成功以后再测试一下远程连接，我们把管理口的 ip 加入到 Honeywall 的允许远程登录列表中，通过主机进行连接：

ssh root@192.168.200.8

su-

输入以上命令加入远程连接后，可以登录管理界面，然后使用 roo 帐户和设置的密码登录 Walleye 主页。

本次攻击实验使用 Kali Linux，它是基于 Debian 的 Linux 发行版，主要用于数字取证、渗透测试和黑客攻防。其中预装了很多渗透测试软件，Metasploit 就是其中的一款开源的安全漏洞检测工具。我们在 kali linux 中启动 Mataploit。攻击过程为：

root@kali:~# msfconsole

msf>search ms17_010

msf>use exploit/windows/smb/ms17_010_

eternalblue

msfexploit(ms17_010_eternalblue)>show options

msf exploit(ms17_010_eternalblue)>set RHOST 192.168.1.166

msfexploit(ms17_010_eternalblue)>exploit

攻击结果如图 6 所示。攻击结束后，蜜网管理界面 Walleye 的主页视图如图 7 所示。

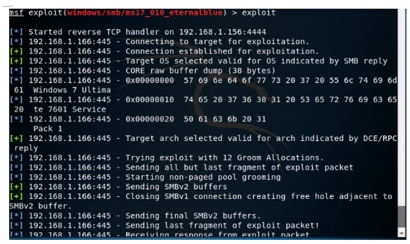

图 6 渗透攻击结果

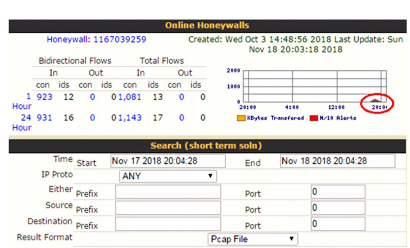

图 7 Walleye 主页视图

5.3　实验结果分析

渗透攻击成功以后，蜜网网关捕获的数据可以通过 Walleye 分析工具来查看。对攻击数据进行分析来验证蜜网的数据捕获、数据控制和数据分析三大核心功能。

5.3.1　数据控制功能

在攻击实验完成以后，我们查看蜜网网关中的 Iptables 文件，摘取其中一条信息如下：

Nov 18 19:45:42 roo-test kernel:Drop udp>20 attempts IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.166 DST=192.168.1.180 LEN=161 TOS=0x00 PREC=0x00 TTL=1 ID=1298 PROTO=UDP SPT=59986 DPT=1900 LEN=141

可以看到，在 19:45:42 时丢弃了一个连接，这个连接触发的是我们预先设置的防火墙规则。从这条信息中可以看到，UDP 的连接数因为大于每分钟 20 个而被丢弃。该条连接企图从 eth1 进，从 eth0 出；源端口 ip 地址为 192.168.1.166，目的 ip 地址为：192.168.1.180，源端口和目的端口分别为 59986 和 1900，使用的协议是 UDP。

5.3.2　数据捕获和分析

图 8 显示的是 Honeynet 网关捕获的攻击机发起的向内连接视图和获得的反向 shell 连接。连接记录显示了攻击的 ip 地址是 192.168.1.180，攻击机的操作系统是 Windows，目的 ip 地址是 192.168.1.166。此外还包括连接持续的时间、发送的数据包数、字节数等详细信息。

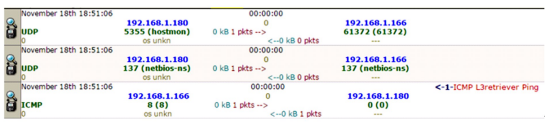

图 8　捕获的数据连接视图

Snort 软件记录了流经蜜网网关的数据包，Snort 发送的报警信息如图 9 所示，攻击机先对靶机进行监听，然后尝试共享访问，最后获得反向 shell 建立起与靶机的连接。

图 9　snort 报警信息

5.4　小结

本节详细介绍了蜜网的三大核心功能，并进行了渗透攻击测试，结果证明本次部署能够达到预期效果，表明蜜网在用电信息采集系统上的工作状态良好，能够有效检测到对数据中心的恶意活动。如果再进行进一步的调整和设置，便可应用于大规模的用电信息采集系统，以检测未知的攻击行为和特征，保障用电信息采集系统的安全。

结束语　蜜网技术作为一种主动防御机制，是应对攻击的一种有效方法，虽然企业型的蜜罐和蜜网技术已经发展得较为成熟，但是它在电力领域中的应用还处于探索之中。本文给出了虚拟蜜网在用电信息采集系统中的具体实现，并详细分析了蜜网的三大核心功能。最终的实验结果表明，蜜网能够实现数据捕获、数据控制和数据分析的功能。今后的工作应进一步地分析和研究虚拟蜜网与现有的安全技术的结合，探究在大型用电信息采集系统中部署蜜网的硬件配置问题，在结构更复杂的情况下进行测试，降低用电信息采集系统被攻击的风险。

参 考 文 献

[1] 赵兵，翟峰，李涛永，等. 适用于智能电表双向互动系统的安全通信协议[J]. 电力系统自动化，2016，40(17)：93-98.

[2] 李敏，王刚，石磊，等. 智能电网信息安全风险分析[J]. 华北电力技术，2017(1)：62-65.

[3] 李中伟，佟为明，金显吉. 智能电网信息安全防御体系与信息安全测试系统构建乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J]. 电力系统自动化，2016，40(8)：147-151.

[4] 任天成. 电力信息网络主动式风险预警系统开发研究[D]. 北京：华北电力大学，2015.

[5] FAISAL M A，AUNG Z，WILLIAMS J R，et al. Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid：A feasibility study[J]. IEEESystems Journal，2015，9(1)：31-44.

[6] WANG K，OUYANG Z，KRISHNAN R，et al. A game theory-based energy management system using price elasticity for smart grids[J]. IEEE Transactions on Industrial Informatics，2015，11(6)：1607-1616.

[7] YE F，QIAN Y，HU R Q. A security protocol for advanced metering infrastructure in smart grid[C]// 2014 IEEE Global Communications Conference. Austin，TX，USA：IEEE，2014：649-654.

[8] LIU N，ZHU C L，ZHANG J，et al. A key management scheme for secure communications of advanced metering infrastructure in smart grid[J]. IEEE Transactions on Instrumentationand Measurement，2013，60(10)：4746-4756.

[9] 张恩超. 智能电网信息安全防御体系架构与关键技术研究[D]. 北京：华北电力大学，2016.

[10] 周晟，赵君翊，葛元鹏. 主被动防御结合的智能电网信息安全防护体系[J]. 电子科技，2015，28(6)：213-215.

[11] 陈飞. 智能电网信息安全交互模型及关键技术研究[D]. 北京华北电力大学，2014.

[12] 诸葛建伟，唐勇，韩心慧，等. 蜜罐技术研究与应用进展[J]. 软件学报，2013，24(4)：825-842.

[13] CONPOT ICS/SCADA honeypot[EB/OL]. https://www.conpot.org.

[14] KOLTYS K，GAJEWSKI R. Shape：A honeypot for electric power substation[J]. Journal of Telecommunications and Information Technology，2015(4)：37-43.

[15] FAN W，FERNÁNDEZ D，DU Z. Versatile virtual honeynet management framework[J]. IET Information Security，2017，11(1)：38-45.

[16] REN J，XU Y. A compartmental model to explore the interplay between virus epidemics and honeynet potency[J]. Applied Mathematical Modelling，2018，59：86-99.

[17] SOKOL P，GAJDOŠ A. Prediction of Attacks Against Honeynet Based on Time Series Modeling[J]. Applied Computational Intelligence and Mathematical Methods，2018，662：360-371.

[18] 易秀双，马世伟，王卫东. 虚拟蜜网核心功能剖析与实例部署[J]. 计算机科学，2012，39(3)：101-103，109.

[19] 胡江溢，祝恩国，杜新纲，等. 用电信息采集系统应用现状及发展趋势[J]. 电力系统自动化，2014，38(2)：131-135.

[20] 祝恩国，刘宣，葛磊蛟. 用电信息采集系统非结构化数据管理设计[J]. 电力系统及其自动化学报，2016，28(10)：123-128.

[21] 翟峰，冯云，李保丰. 电力采集系统安全防护和密码管理体系[J]. 网络空间安全，2018，9(2)：79-84，89.