文章编号：2095-2163(2020)05-0056-08 中图分类号：TP311.52 文献标志码：A

虚拟化工控网络靶场的设计与自动化部署

陈吉龙，翟健宏
（哈尔滨工业大学 计算机科学与技术学院，哈尔滨 150000）

摘 要：21 世纪互联网的高速发展带动了工业信息化的革新，越来越多的工业控制系统由原先的封闭网络转入开放互联网络，在资源利用率和工作效率不断提升的同时，工业控制系统的脆弱性也逐渐暴露在公众视角中。工控安全研究起步晚，现有能应对网络化、信息化工控安全问题的人才储备不足。同时，由于工业控制系统的复杂性、专业性和封闭性，市场上可用于工控安全研究及测试的软硬件平台不多，且都普遍存在成本投入大、操作复杂、灵活性不高等问题。本文给出了一种基于虚拟化技术的工控网络靶场解决方案，利用 OpenStack 和 Snort 等系统，以低投入、低消耗的代价实现了工业控制场景的虚拟化仿真，使工控安全教育研究能在虚拟化平台上开展。

关键词：工控安全；网络靶场；OpenStack；Snort

Design and automatic deployment of virtual industrial control network range

CHEN Jilong, ZHAI Jianhong
(College of computer science and technology, Harbin Institute of Technology, Harbin 15000, China)

【Abstract】 The rapid development of the Internet in the 21st century has led to the innovation of industrial informatization. More and more industrial control systems have been transferred from the original closed network to the open Internet. While the resource utilization rate and work efficiency have been continuously improved, the vulnerability of industrial control systems has been gradually exposed in the public perspective. The study of industrial control safety started late, and there are insufficient talents to deal with the problem of industrial control safety under network and informatization. At the same time, due to the complexity, professionalism and closure of the industrial control system, there are not many software and hardware platforms available for industrial control safety research and testing in the market, and there are widespread problems such as large cost input, complex operation and low flexibility. This paper presents an industrial control network range solution based on virtualization technology. OpenStack and Snort systems are used to realize the virtual simulation of industrial control scenarios at a low cost of investment and consumption, so that the research on industrial control safety education can be carried out on the virtualization platform.

【Key words】 Industrial Control Security; Cyber range; Docker; Snort

0 引 言

工业控制系统广泛应用于各个领域，包括基础设施（金融、能源、通信、电力、交通）、民生（水、电、燃气、医院、智慧城市、智能汽车）、工业生产（冶金、电力、石油化工、核能等）和军工等。超过 80%的涉及国计民生的关键基础设施依靠工业控制系统来实现自动化作业。2010 年的伊朗核电站攻击事件、2015 年的乌克兰电网攻击事件以及 2019 年的委内瑞拉电力系统攻击事件充分证实了工控安全问题对国家、社会和经济的重要影响[1]。

受限于历史原因，目前工业控制领域安全软硬件研发程度以及专业安全从业人员的数量还远远不能满足市场需求。尤其是在各类工控安全事件频发的今天，无论是工控产品制造方还是使用方均对工控安全予以高度重视，并在工业控制网络基础设施改善及相关人才培养方面逐年加大投入力度，搭建了适用于不同场景的工业控制实验模拟环境，用于工控安全技术的研究和人才培养，但是这些实验平台基本上采用全实物或半实物的方式，投入成本高，建设周期长，且往往只能针对某一种特定工业控制环境，一旦仿真对象变更就需要重新搭建一套平台，灵活性差。另外，以实物或半实物形式搭建的实验平台抗打击性差，进行研究测试时容易对现实设备造成不可逆的破坏，后期维护代价高。

鉴于上述存在的问题，本文提出了一种基于虚拟化技术的工业控制网络靶场[2]设计方案。该靶场依托于当前最新的虚拟化云平台 OpenStack，同时结合入侵检测系统 Snort，实现了在低投入、低消耗的条件下简单、便捷、高效地对各类现实工业控制环境进行模拟仿真，可有效支撑工业控制领域安全人

作者简介：陈吉龙（1988-），男，硕士研究生，主要研究方向：工控安全；翟健宏（1968-），男，博士，副教授，硕士生导师，主要研究方向：内容安全、网络安全、云计算。

收稿日期：2020-03-01

才的教学培训、新产品新技术的研究测试、工业控制网络风险评估以及组织工控攻防演练或安全竞赛。

1　相关技术综述

1.1　工控知识介绍

工业控制网络相比于常规的小型局域网或企业办公网有其特殊的组织架构。现实的工业控制网络一般具有多层次结构，各层的业务属性和软硬件组成、配置均不尽相同。工业控制核心区域从上到下大致分为信息网（负责工控核心网的监控管理，以 ERP、MIS 等为主）、通信隔离区（以网络安全设备为主，在保障上下层合法数据通信的基础上防止非授权访问或意外的数据泄露）、调度网（以 SCADA、DCS、HMI、MES 等为主，实现对小型控制单元的监管）、控制网（以 PLC、RTU、IED 等设备为主，实现对实际生产设备的监控管理）、现场网（由实际生产设备组成，包括发电机、闸刀、开关等机械单元）。

现有的工控网络协议种类繁多，各自应用场景也不同。传统的工控协议基于现场总线，主要包括 CAN、DeviceNet、CCL-Link、Profibus-DP、Profius-PA 等。但随着两化的推进，衍生出许多基于工业以太网的工控协议，主要的有 Modbus、DNP3、Profinet、EtherNet/IP、S7 等。

目前工控网络中存在的不足和缺陷主要有以下方面：一是工业控制软件系统，如 SCADA、组态软件、PLC 编程软件等存在安全漏洞；二是通信协议，工控网络使用的协议众多，但基本上均是明文传输，无加密无认证无权限控制；三是小型控制单元，如 PLC、IED、RTU 等存在错误配置、业务逻辑漏洞、硬编码后门、缓冲区溢出等问题[3]。

1.2　虚拟化技术介绍

虚拟化是指通过虚拟化技术将一台计算机虚拟为多台逻辑计算机。在一台计算机上同时运行多个逻辑计算机，每个逻辑计算机可运行不同的操作系统，并且应用程序都可以在相互独立的空间内运行而互不影响，从而显著提高计算机的工作效率。虚拟化使用软件的方法，重新定义、划分 IT 资源，可以实现 IT 资源的动态分配、灵活调度、跨域共享，提高 IT 资源利用率，使 IT 资源能够真正成为社会基础设施，服务于各行各业中灵活多变的应用需求[4]。

OpenStack 是一个开源的云计算管理平台项目，它的主要任务是给用户提供 IaaS 服务。OpenStack 为私有云和公有云提供可扩展的弹性的云计算服务。项目目标是提供实施简单、可大规模扩展、丰富、标准统一的云计算管理平台。

1.3　入侵检测技术介绍

入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，观察网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

Snort IDS（入侵检测系统）是一个强大的网络入侵检测系统。它具有实时数据流量分析和记录 IP 网络数据包的能力，能够进行协议分析，对网络数据包内容进行搜索/匹配。它能够检测各种不同的攻击方式，对攻击进行实时报警。此外，Snort 是开源的入侵检测系统，具有很好的扩展性和可移植性。

2　靶场架构与核心功能

2.1　工控网络靶场架构描述

本文提出的方案中靶场的系统架构主要由用户区域、连接区域和虚拟区域构成[5]，系统组网架构如图 1 所示。

图 1　靶场架构图

Fig. 1　Range structure

用户区域。以工控安全研究人员或者学习者的个人电脑设备为主，使用者通过该区域接入虚拟网络平台，开展各类工控安全研究学习。

连接区域。以路由器和交换机为主，在用户区域和虚拟网络平台之间起到桥接作用，可通过设置各类访问规则来控制不同用户对工控虚拟网络的访问权限，或者对不同用户组进行访问隔离设置。

虚拟区域。即虚拟化工控网络靶场基础云平台，其中虚拟区域基于 OpenStack 设计，包括控制节点、计算节点和协议检测系统。OpenStack 平台用于生成部署虚拟网络，方便对工控网络拓扑及网络中节点单元的脆弱性开展研究测试，而基于 Snort 的协

议检测系统则用于对工业协议的安全性进行研究分析[6]。虚拟区域组网架构如图 2 所示。

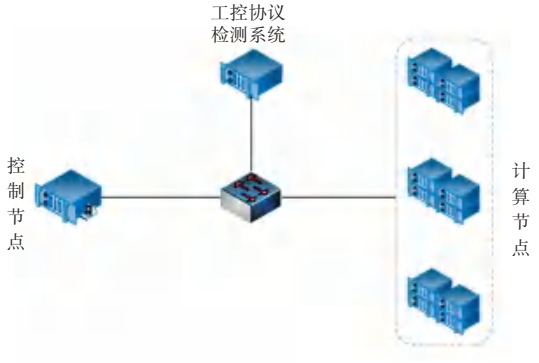

图 2 虚拟区域架构

Fig. 2 Virtual area architecture

一般情况下,行业内常讨论的工业控制网络的核心区域包括调度层和控制层。而 OpenStack 平台通过 Nova 组件和 Zun 组件分别实现了基于 KVM 的虚拟机和基于 LXC 的容器,结合其他相关技术,可虚拟工业控制网络中核心区域的服务器或设备。

2.2 工控知识镜像库

虚拟网络由多个虚拟节点组成,这些虚拟节点可能是虚拟服务器、主机、通信设备以及工控专属设备,系统涉及 Linux 和 Windows,系统之上运行着各类不同软件,而这些丰富多样的虚拟节点均生成于对应的虚拟镜像,一系列工控环境相关的虚拟镜像的集合构成了工控网络靶场的工控知识镜像库。

镜像是一种文件存储形式,与 ZIP 压缩包类似,它将特定的一系列文件按照一定的格式制作成单一的文件,以方便用户下载和使用。镜像文件是无法直接使用的,需要利用一些加载工具进行解压后才能使用。工控知识镜像库主要由各类系统镜像组成,每个系统镜像文件都包含特定的系统内核、系统设置、应用程序和资料文件。虚拟化平台利用镜像文件可直接生成虚拟系统,具备与真实 linux 或 windows 系统完全一样的功能,进入虚拟系统后,所有操作都是在这个全新的独立的虚拟系统里面进行。可以独立安装运行软件,保存数据,拥有自己的独立桌面,不会对真正的系统产生任何影响。

2.3 虚拟网络自动化部署

本文目标是实现各类型工控网络的自动化部署,除此之外还要保证部署过程尽可能简单易操作。根据以上要求,通过研究分析,设计了基于 XML 和 SDK 的协同工作模式,对网络配置与虚拟化部署进行切割分离,用户只需要对可读性强的 XML 配置文件进行编写,而不需要了解已封装部署工具的具体实现步骤和细节。

本文主要设计了五种类型 XML 文件来分别描述网络架构、网段信息、节点信息和网络策略,即网络拓扑图中面、线、点以及相互间的关联。

不同类型的 XML 配置文件进行归拢整合后,构建出一个 XML 配置树结构,如下图 3 所示。

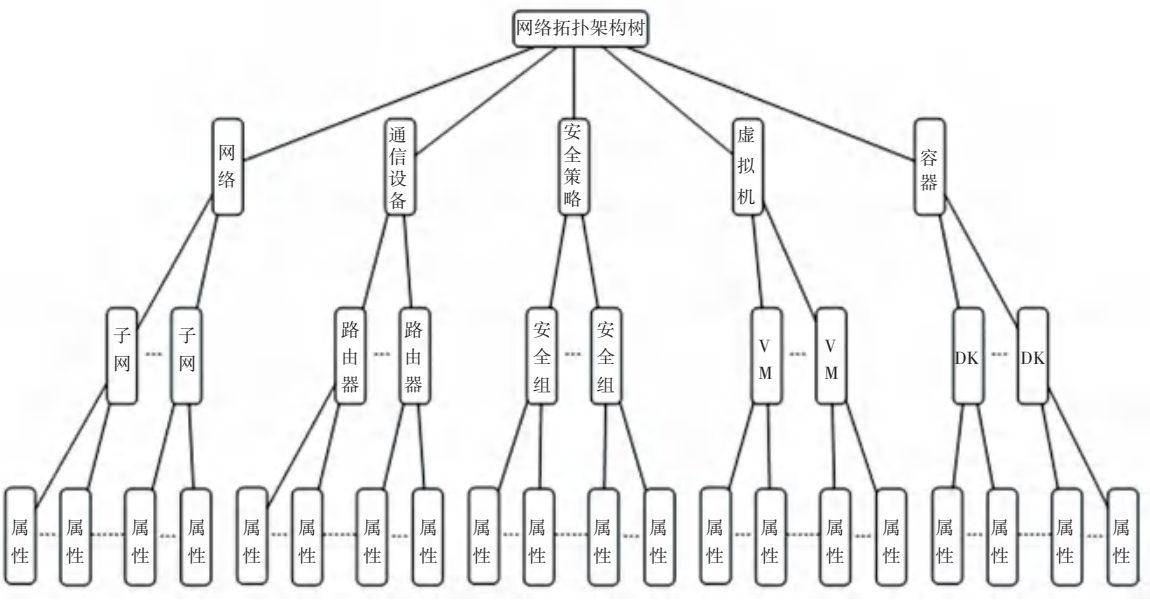

图 3 网络拓扑 XML 配置树结构

Fig. 3 Network topology XML configuration tree structure

XML 配置树从上到下分为 4 个层次,网络拓扑配置文件作为树根节点位于第一层次;第二层次包括五个分支节点,对应网络集合、路由器集合、安全策略集合、虚拟机集合以及容器集合;第三层次包含

父节点下属的特定配置文件，例如：父节点为虚拟机集合，则子节点为某些特定的虚拟机配置文件；第四层次即最后的叶节点（终端节点）主要对应各配置文件内的属性。

实现多层次工控虚拟网络自动化部署的首要条件是完成对 XML 配置树的遍历，本文根据靶场云平台的资源调度特性采用了深度优先遍历（DFS），算法核心思想是从某个节点一直往深处走，走到不能往下走之后，回退到上一步，直到找到解或把所有节点走完。DFS 前序遍历的算法如表 1 所示。

表 1　DFS 前序遍历算法

Tab. 1　DFS algorithm

算法步骤（递归或栈实现）
1、访问指定起始点。
2、找出与当前节点邻接的且尚未遍历的点访问，并将之放入队列中。
3、删除队列的队首节点。访问当前队列的队首，重复步骤 2，直到队列为空。
4、若途中还有顶点未被访问，则再选一个点作为起始顶点。重复步骤 2。（针对非连通图）。

通过分析研究，结合 OpenStack SDK 开发工具包，即可实现对虚拟化工控网络的自动化部署工具的设计与实现。

本文所研发的自动化部署工具主要分为前端和后端两个部分，前端是自动化部署模块，后端是基础调用包。基础调用包又细分为配置文件读取模块、虚拟资源部署模块和虚拟资源回收模块。各模块调用关系如图 4 所示。

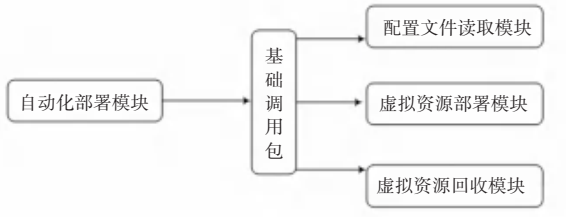

图 4　模块调用关系

Fig. 4　Module call relationship

详细的部署流程如表 2 所示。

表 2　自动化部署流程

Tab. 2　Automated deployment process

部署步骤
1、初始阶段调用部署程序，并传入项目配置文件全路径。
2、调用 read_project_xml 函数获取工控虚拟网络项目的各属性值。
3、加载项目基础信息，调用 create_project_and_user 函数创建项目空间及用户。
4、查询网络集（networks set），调用 read_network_xml 函数获取网络各属性值。
5、加载网络配置信息，调用 deploy_network 函数生成虚拟网络，重复步骤 4，直到网络集为空。
6、查询路由器集（routers set），调用 read_router_xml 函数获取路由器各属性值。
7、加载路由器配置信息，调用 deploy_router 函数生成虚拟路由器，重复步骤 6，直到路由器集为空。
8、查询安全组集（security groups set），调用 read_securitygroup_xml 函数获取安全组各属性值。
9、加载安全组配置信息，调用 deploy_sec_group 函数生成虚拟网络内的安全组，重复步骤 8，直到安全组集为空。
10、查询虚拟机集（vms set），调用 read_vm_xml 函数获取虚拟机各属性值。
11、加载虚拟机配置信息，调用 deploy_vm 函数生成虚拟机，重复步骤 10，直到虚拟机集为空。
12、查询容器集（dockers set），调用 read_docker_xml 函数获取容器各属性值。
13、加载容器配置信息，调用 deploy_docker 函数生成容器，重复步骤 12，直到虚拟机集为空。
14、查看已创建项目的个数是否达到要求，未到达要求则转跳到步骤 3 执行，已到达要求则执行下一步。
15、退出程序、完成部署、告知管理者。

相较于表 2 步骤，虚拟资源回收的操作流程可简单看做是部署流程的逆操作。

2.4　工控协议检测

工控协议研究是工控网络安全中至关重要的一环。本文针对 Snort 平台开展了研究分析，并在其基础上实现了工控协议检测系统的设计部署。系统主要应用有两个方面：一是为举办工控网络安全竞赛提供支持，系统可对参赛队伍的操作进度给予检测与评判；二是制作成工控知识镜像文件，在靶场的虚拟网络中部署，方便学生或相关研究人员开展工控协议的分析测试。

工业控制通信协议种类繁多，有的协议格式公开，如 modbus、dnp3 等，有的则是厂家的私用协议，协议规范不公开，如西门子的 s7 协议。公开的协议

可参照协议规范进行分析,过程相对简单,而私有协议则需要通过功能测试配合数据包分析技术研究分析,整个过程相对复杂、耗时。鉴于以上因素,Snort 入侵检测平台凭借开源性和兼容性,可以很好地拓展相关功能模块来实现对工控协议的分析检测。

靶场采用了两种模式对工控协议检测系统进行部署:

(1)在工控靶场的基础平台上部署。该部署模式目的是为组织工控安全竞赛提供支撑,核心是在靶场底层基础平台上对所有虚拟网络内的工业控制数据流进行监测,该需求的实现主要是依托于 OpenStack 虚拟网络通信的特性,即 OpenStack 默认部署模式下,计算节点通过 ml2 插件实现二层互通,所有三层流量都要经过网络节点。

(2)在工控靶场的虚拟网络中部署。除了将工控协议检测系统部署在基础云平台外,本文还将该系统制作成虚拟镜像文件,可在虚拟网络中使用,为工控协议学习、研究、测试提供服务。

3 实验与分析

3.1 实验环境

在 OpenStack 平台上,使用一台曙光服务器作为控制节点,控制节点用于控制虚拟机之间的通信和资源分配。另外使用两台曙光服务器作为计算节点,负责调度虚拟化资源。在计算节点上通过 Nova 组件和 Zun 组件分别虚拟出工控网络的监管层主机设备和现场层设备。

在工控协议检测平台上,使用一台曙光服务器搭建了 Snort+Base 的入侵检测系统,Snort 实现对检测数据的分析、识别、存储,Base 实现了对检测结果的可视化展示。四台曙光服务器的配置如表 3 所示。

表 3 物理主机配置

Tab. 3 Server configuration

name	Type	Cpu	Memory	Storage	System
Controller	PhysicsMachine	8 核,2.13HZ	32G	500G	Ubuntu 18.04.5 LTS
Compute	PhysicsMachine	8 核,2.13HZ	32G	500G	Ubuntu 18.04.5 LTS
Compute	PhysicsMachine	8 核,2.13HZ	32G	500G	Ubuntu 18.04.5 LTS
Snort	PhysicsMachine	4 核,2.13HZ	8G	100G	Ubuntu 18.04.2 LTS

3.2 功能测试

(1)工控镜像。为验证工业控制系统软硬件在虚拟化平台上的运行状况,针对性收集了商用和开源两套工控软件系统,分别是西门子的 WinCC(软 SCADA)和 PLCSIM(软 PLC),以及开源软件 scadaBR(软 SCADA)和 OpenPLC(软 PLC),将以上软件分别安装在 Linux 和 Windows 系统上,制作成 OpenStack 云平台支持的系统镜像,然后进行虚拟化部署测试,结果显示各类镜像均能在虚拟化平台上有效运行,运行效果如图 5 所示。

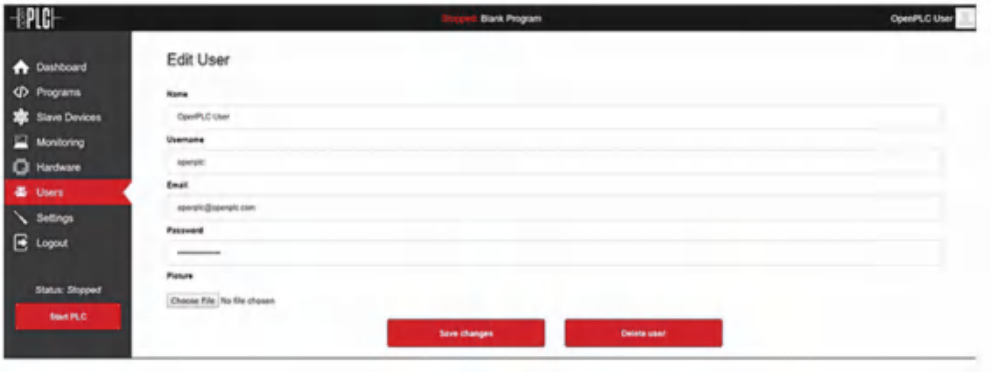

图 5 PLC 虚拟化运行效果

Fig. 5 OpenPLC operation screen

为进一步验证工控组态软件在虚拟平台上的协同运作状况,本文设计了一套火电厂输煤控制系统场景,在 SCADA 系统上构建了工控场景的示意模型,方便监控管理,如图 6 所示。同时,在 PLC 系统上植入了功能完备的梯形图程序,用于模拟操控工控设备工作。最后通过一定周期频率的测试,证实在虚拟化工控网络靶场平台上使用工控软件仿真模拟工控场景是合理有效的,且一切功能指标均显示正常。

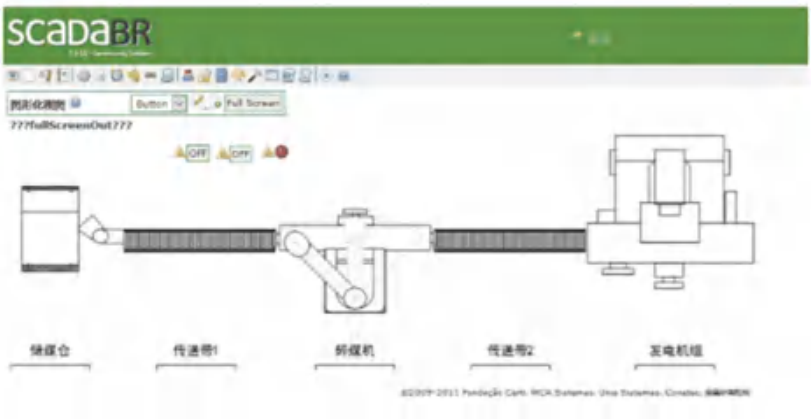

图 6　工控场景示意架构

Fig. 6　Schematic architecture of industrial control scene

（2）自动化部署。本文设计了一种复杂工控网络架构，以验证自动化部署工具的有效性和稳定性，如图 7 所示。复杂工控网络是在常规工控网络的基础上根据工业互联的发展趋势，添加了企业办公网和 DMZ 区，同时依据业务属性在企业 OA 网和工控调度网间添加了一台双网卡数据库服务器，便于 OA 网内的业务管理系统获取生产线的各类参数。

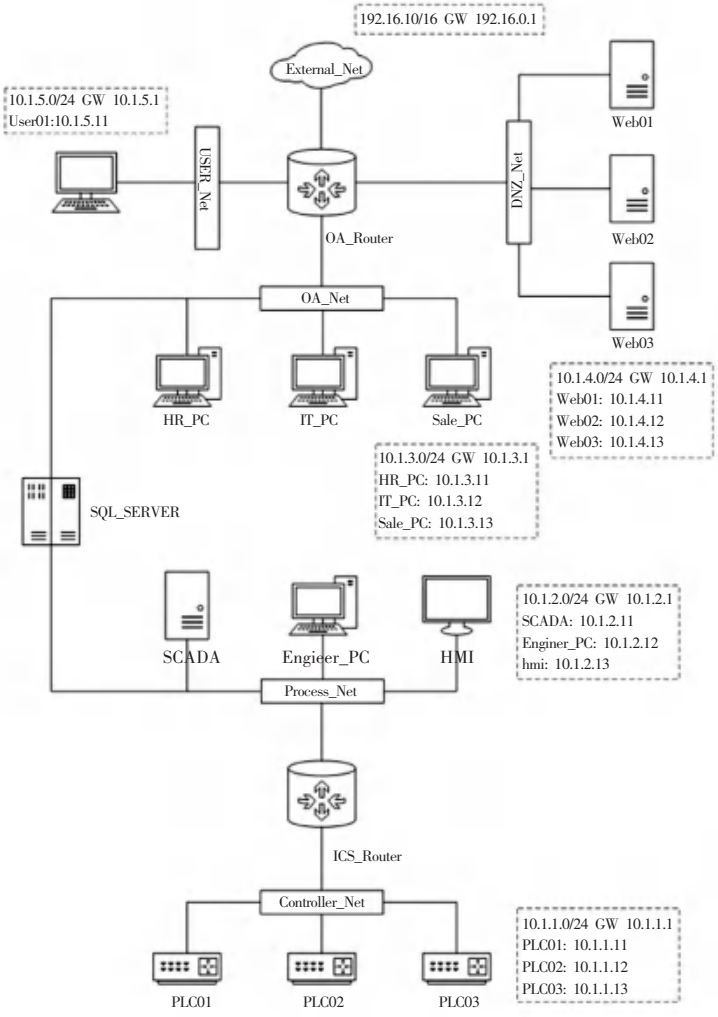

图 7　复杂工控网络拓扑

Fig. 7　Complex ICS Network topology

使用自动部署工具 automation 对上述网络进行自动化部署,经过多次测试,部署和回收工具均能稳定,有效地完成多套虚拟工控网络的部署与回收任务。除初始阶段对工具的调用外,后续过程均无需用户参与,符合自动化设计的初衷和要求。

(3)协议检测。为验证工控协议检测系统的功能效果,本文在工控网络靶场平台上部署了虚拟化工控网络,在虚拟网络内配置并运行工控生态系统,让软 SCADA 系统和软 PLC 通过 Modbus 进行不间断通信,并提前开启工控协议检测系统的网络数据嗅探功能。

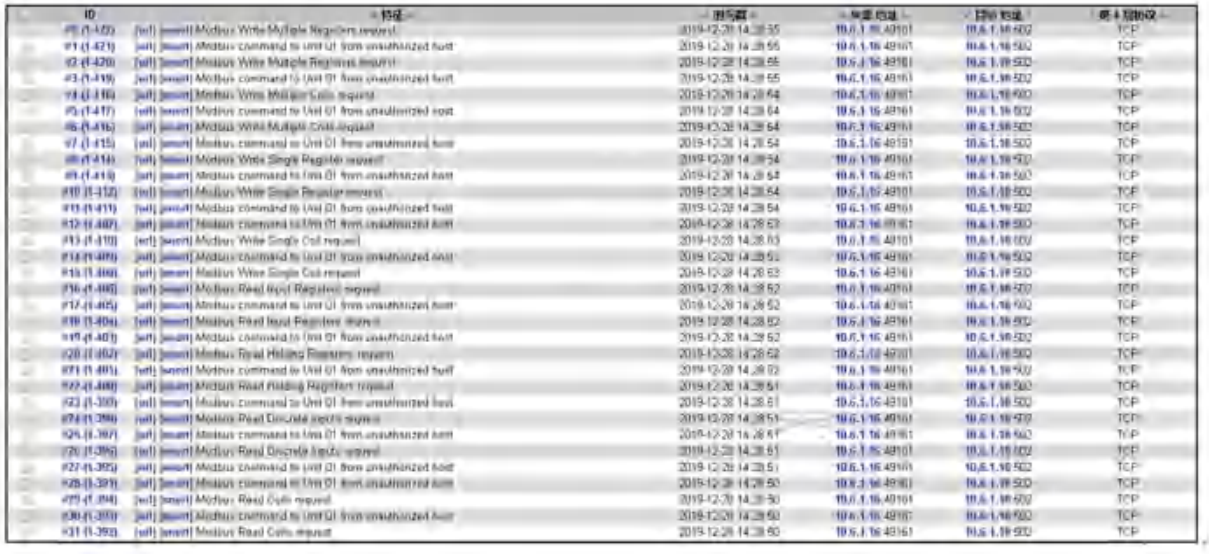

图 8 Modbus TCP 检测识别效果

Fig. 8 Modbus TCP detection effect

通过实验测试发现工控协议检测系统可以实时、准确地对 Modbus 通信协议指令进行监控告警,告警内容会实时显示在 Snort Base 管理界面,如图 8 所示,告警信息涉及 Modbus 通信的源 IP 地址、目的 IP 地址、源端口、目的端口、通信时间以及 Modbus 执行的具体指令。

3.3 性能测试

(1)时耗性能。主要对虚拟工控网络的各组成单元进行部署周期测量,通过多次测量取平均值的方式来分析节点单元的时耗性能,测试结果如表 4 所示。

表 4 虚拟资源部署测试结果

Tab. 4 Virtual resource deployment test results

内容	Cirros 虚拟机	Cirros 容器	子网	路由器	安全组
平均时耗/s	70.56	4.61	1.71	0.16	1.13

测试结果显示各类虚拟资源的部署时间代价在预期的可控访问内。

(2)网络性能。网络性能是判断一个网络优劣的关键要素,本文采用了目前主流的两款网络性能检测工具(iperf3 和 ixChariot)对部署的虚拟工控网络进行测试,研判靶场所生成的虚拟网络是否满足应用需求,检测结果如表 5、表 6 所示。

表 5 iperf3 检测结果

Tab. 5 iperf3 detection result

端点	带宽
接收端	656 Mbits/sec
发送端	656 Mbits/sec

表 6 ixChariot 检测结果

Tab. 6 ixChariot detection result

最高	最低	平均带宽
839.983 Mbits/sec	524.106 Mbits/sec	645.422 Mbits/sec

综合分析两种工具的测试结果,可以判断工控网络靶场所生产的虚拟网络符合原有预期,其网络性能足以支持各类工控学习、研究与实验。

4 结束语

本文研究的目的在于设计一种仿真度高、简单易操作、推广性强的工控网络靶场,可用于工控安全技术的研究与相关人才的培养。通过上述实验测试

(下转第 66 页)