计算机科学
COMPUTER SCIENCE

一种基于容器的Cisco IOS-XE系统入侵检测方法

杨鹏飞, 蔡瑞杰, 郭世臣, 刘胜利

引用本文

杨鹏飞, 蔡瑞杰, 郭世臣, 刘胜利.一种基于容器的Cisco IOS-XE系统入侵检测方法[J]. 计算机科学, 2023, 50(4): 298-307.

YANG Pengfei, CAI Ruijie, GUO Shichen, LIU Shengli. Container-based Intrusion Detection Method for Cisco IOS-XE [J]. Computer Science, 2023, 50(4): 298-307.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220300264

一种基于容器的 Cisco IOS-XE 系统入侵检测方法

杨鹏飞　蔡瑞杰　郭世臣　刘胜利
数学工程与先进计算国家重点实验室　郑州 450001
战略支援部队信息工程大学　郑州 450001
(graduated_learning@outlook.com)

摘　要　IOS-XE 网络操作系统被广泛地应用于 Cisco 核心路由交换节点中,其安全性非常重要。然而由于其设计时专注于数据的快速转发功能,缺少对自身的安全的防护,因而面临重大的风险。此外,现有的针对传统 IOS 系统的入侵检测方法移植到 IOS-XE 系统后存在实时性差、检测结果不准确、检测覆盖面不全等问题。为了加强 IOS-XE 系统自身的安全,提出了一种基于容器的 CiscoIOS-XE 系统入侵检测方法,通过在路由器上部署检测容器,实时监控路由器状态变化和用户访问请求,解决了配置隐藏攻击检测、路由器 https 管控流量解密以及路由器状态实时监控等问题,实现了对 IOS-XE 系统入侵行为的实时检测。实验结果表明,所提方法可有效检测针对 IOS-XE 路由器的常见攻击行为,包括口令猜解、Web 注入、CLI 注入、配置隐藏和后门植入等,与已有的检测方法相比具有较高的实时性和准确性,有效提升了 IOS-XE 路由设备的防护能力。

关键词:Cisco IOS-XE;容器;配置隐藏攻击;命令注入;入侵检测
中图法分类号　TP393

Container-based Intrusion Detection Method for Cisco IOS-XE

YANG Pengfei,CAI Ruijie,GUO Shichen and LIU Shengli
State Key Laboratory of Mathematical Engineering and Advanced Computing,Zhengzhou 450001,China
Information Engineering University,Zhengzhou 450001,China

Abstract　IOS-XE network operating system is widely used in Cisco core routing and switching nodes,and its security is very important. However,its design focuses on the traffic fast-forwarding function and ignores protection for its own security which makes it faces great risks. In addition,the existing intrusion detection methods for traditional IOS system have problems such as poor real-time performance,inaccurate detection results and incomplete detection coverage when transplanted to the IOS-XE system. In order to strengthen the security of the IOS-XE system,this paper proposes a container-based intrusion detection method for Cisco IOS-XE system which can monitor the router states and requests in real time by deploying a detection container on the router. It solves the problems of configuration hidden attack detection,router https control traffic decryption and router state real-time monitor,which helps to detect the intrusion behavior of IOS-XE in real time. Experimental results show that this method can effectively detect common attacks against IOS-XE routers,including password guessing,Web injection,CLI injection,configuration hidden and backdoor implantation. Compared with existing detection methods,the proposed method has higher real-time performance and accuracy,and effectively improves the defense capability of IOS -XE routing devices.

Keywords　Cisco IOS-XE,Container,Configuration hidden attack,Command injection,Intrusion detection

1　引言

Cisco 公司是路由器交换机市场最主要的设备提供商,位居市场首位[1]。随着主机端的网络攻击难度增大,攻击人员逐渐将攻击视角转向路由器,试图通过控制路由器实现数据获取、欺骗诱导等。德国电信公司 T-Mobile 事件[2]的起因就是边界路由器被黑客攻陷,导致大量用户信息被泄露。当前针对 Cisco 路由器的入侵检测成果集中于 IOS 操作系统,主要基于路由器信息提取进行离线检测,不能检测 IOS-XE(Internetwork Operating System-eXtended Edition)系统广泛存在的 Web 注入和命令行接口(Command Line Interface,CLI)注入等漏洞利用行为,检测实时性较差。

IOS-XE 是 IOS 的增强版,被广泛应用于聚合服务路由器、云服务路由器和集成服务路由器等设备,针对 IOS-XE 和 IOS 的攻击和检测方法部分是通用的。Lindner[3]开发了一个针对 CiscoIOS 系统的取证系统 Cisco 信息检索(Cisco Information Retrieval,CIR),其利用 IOS 核心转储文件和调试功能进行入侵行为的离线提取;Liu 等[4]提出了一种轻量级

到稿日期:2022-03-29　返修日期:2022-09-14
基金项目:科技委基础加强项目(2019-JCJQ-ZD-113)
This work was supported by the Foundation Strengthening Key Project of Science & Technology Commission(2019-JCJQ-ZD-113).
通信作者:刘胜利(dr_liushengli@163.com)

的针对路由设备的恶意行为检测系统，该系统利用加载于路由设备的轻量级程序监控路由器流量和配置方面的变化来识别恶意攻击行为并告警；Cisco 公司在 IOS-XE 系统上推出了统一威胁防御（Unified Threat Defense，UTD）服务配合 Snort 入侵检测系统（Snort Intrusion Prevention System，SnortIPS）容器[5]实现对过境数据的检测；Damiris[6]介绍了针对 Cisco-IOS-XE 路由器的攻击取证方法，从运行配置、启动配置等方面获取路由器运行信息，并利用路由器提供的核心转储功能获取核心转储文件并进行离线解析，提取入侵行为。

通过对当前 Cisco 设备入侵检测研究成果进行分析和总结，发现了以下问题：1）当前研究成果主要集中在 IOS 操作系统，虽然大部分方法能够移植到 IOS-XE 系统，但是移植后的实时检测能力不足；2）当前研究成果不能有效检测 IOS-XE 系统广泛存在的 Web 注入漏洞和 CLI 命令注入漏洞利用过程。

针对上述问题，本文学习并借鉴 Cisco SnortIPS 入侵检测解决方案提出的在容器中监测过境数据的思路，提出了一种基于容器的 IOS-XE 系统的入侵检测方法。通过分析当前针对 Cisco 路由器的攻击利用方法，提取攻击特征并设置检测策略实现实时检测。同时重点关注目的 IP 地址为路由器的流量，利用端口镜像技术将该类型流量实时镜像到容器中进行检测。

为了验证本文方法的有效性，本文根据 Cisco 路由器常见攻击方法设计了入侵行为检测实验，并与文献[4-6]所提方法进行对比。实验结果表明，本文方法在检测实时性和准确性方面效果较好，尤其是对检测 IOS-XE 系统广泛存在的 Web 注入类和 CLI 注入类漏洞的利用行为效果较好。

本文的贡献如下：

（1）提出了一种基于容器的 IOS-XE 系统的实时检测方法，结合当前针对 Cisco 路由器的攻击行为研究，能实现对口令破解、配置隐藏、后门植入等入侵行为的检测；

（2）弥补了 IOS-XE 系统 UTD 服务只能检测过境流量的不足，可以有效检测该系统广泛存在的 Web 注入类和 CLI 注入类攻击；

（3）提出了一种适用于 IOS 和 IOS-XE 系统的配置隐藏攻击检测方法，能抵御已知的配置隐藏攻击。

2 背景知识与相关工作分析

2.1 CiscoIOS-XE 系统的容器特性

IOS-XE 系统是 Cisco 公司推出的基于 Linux 的数据交换系统，其采用分层架构，实现了控制平面和数据平面的分离，控制平面由 IOS 守护进程（IOS daemon，IOSd）负责管理，该进程继承了 IOS 绝大部分的功能。

IOS-XE 路由器支持两种类型的容器：基于内核的虚拟机（Kernel-based Virtual Machine，KVM）和 Linux 容器（Linux Container，LXC）。其中，基于 KVM 的容器具备独立的内核和文件系统，基于 LXC 的容器与 IOS-XE 共享内核。IOS-XE 系统支持用户通过 CLI 接口和 Web 接口安装容器应用，容器与 IOSd 之间通过虚拟接口 VPG（VirtualPortGroup）进行网络通联。

Cisco IOS-XE 系统为了实现程序化管理，在系统中内嵌了 guestshell 容器，其中的 dohost 应用与 IOSd 进程中的 pnp_python_server 服务之间通过 unix 套接字建立连接，dohost 会发送 http 请求到 pnp_python_server，pnp_python_server 通过执行 cli-exec 任务，并将查询结果返回给 dohost，从而实现从 guestshell 对路由器的命令查询和配置修改。

2.2 Cisco SnortIPS 容器运行机理及缺陷分析

2.2.1 运行机理分析

Cisco 公司于 2014 年在 ISR 系列路由器中引入 UTD，并配合 SnortIPS 容器实现了对过境流量的检测。文献[7]介绍了网络数据在配置了 UTD 服务的 IOS-XE 路由器上的流转细节，包括在 SnortIPS 容器与路由器之间建立 GRE（Generic Routing Encapsulation）隧道，将过境数据转入 SnortIPS 容器。文献[8]详细介绍了 IOS-XE 系统中 Snort 入侵检测系统的详细部署方法，该方法通过配置 UTD 服务和安装 SnortIPS 容器，结合 Cisco 公司提供的检测规则对过境数据进行检测。

如图 1 所示，IOS-XE 路由器通过 VPG 接口与 SnortIPS 容器连接，从 G0 接口接收到网络数据包后会检测 UTD 配置状态，如果 G0 接口设置了 UTD 转发，则将数据包封装成 GRE 格式发送到 SnortIPS 容器中。容器中的 Snort 进程将结合检测规则对进入容器的数据进行检测，判断是转发还是丢弃。

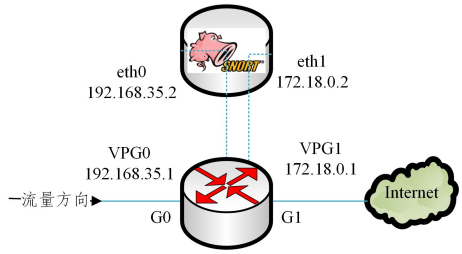


图 1 UTD 数据传输路径

Fig. 1 UTD data transmission path

2.2.2 缺陷分析

在使用 Cisco SnortIPS 容器的过程中，发现了以下问题：1）容器不允许用户操作的问题，网络管理员在发现入侵威胁时，期望能尽快修改入侵检测规则，以减小损失，然而可能是出于确保过境数据不被修改的原因，Cisco 官方网站提供的 SnortIPS 容器不允许用户进行登录、修改规则等操作；2）流量处理方面的问题，UTD 服务只转发路由器的过境流量，对于目的 IP 地址是路由器地址的流量，则不会将其转发到 SnortIPS 容器中进行检测；3）通用性问题，SnortIPS 容器只支持部分运行 Cisco IOS-XE 系统的路由器，不支持如 ASR1000 系列的路由器。

2.3 Cisco 路由器的攻击行为与检测现状分析

当前针对 Cisco 路由器的攻击和检测方法主要是针对 IOS 系统，但是对 IOS-XE 同样适用。网络攻击者在控制路由器后，为了进一步扩大影响范围，通常通过对路由器进行后门植入、数据获取，甚至是配置篡改来实现对重要网络的控制。为了提升检测效率，本文对当前存在的 Cisco 路由器攻击利用方法进行研究，总结如下。

2.3.1 Cisco 路由器的攻击方法分析

网络攻击者经常使用口令猜解、配置隐藏、权限提升、

持久化控制以及流量牵引等方法对路由器进行控制，并从中获取攻击者感兴趣的秘密信息，具体方法如表1所列。

首先，在不具备路由器控制权限的情况下，攻击者通常先搜集路由器管理员信息并用文献[9]中的方法制作字典，对路由器的口令进行猜解。口令猜解成功后利用文献[10-11]等介绍的配置隐藏方法添加隐蔽后门用户，同时隐藏修改过的路由器配置。

其次，在具备路由器权限提升漏洞的条件下，如文献[12-13]中所介绍的权限提升方法，获取IOS-XE路由器的更高权限。假如不具备权限提升漏洞，则使用文献[14-16]中的方法来布置持久化控制后门，实现对路由器的长期稳定控制。

最后，利用文献[17]中介绍的流量牵引方法，对路由器承载的网络数据进行嗅探，或者利用文献[18]中提出的方法进行恶意流量注入，实现对特定用户主机的突破和控制。

表1 路由器攻击方法

Table 1 Attack methods on router

攻击方法	实现方法	对应文献
口令猜解	利用社会工程学制作字典，利用hydra等工具进行自动化爆破	[9]
配置隐藏	①基于KRON计划任务的配置隐藏方法；②基于EEM事件管理器的配置隐藏方法；③基于autocommand的配置隐藏方法；④基于固件重构的命令劫持	[4][10-11][14]
权限提升	Web或CLI命令注入漏洞，获取操作系统权限	[12-13]
后门植入	①基于固件重构修改认证流程；②基于TCL脚本的后门植入；③基于配置隐藏的后门用户添加	[14-16]
流量牵引	GRE配合策略路由实现流量定向牵引，结合流量嗅探程序或其他攻击程序实现信息获取和渗透控制	[17-18]

2.3.2 入侵检测方法及存在的问题

针对Cisco路由器的入侵检测主要有以下3类方法：1)基于核心转储文件的信息提取方法，通过路由器自带的核心转储文件提取路由器状态信息，包括运行的TCL脚本、运行配置；2)基于TCL脚本的信息自动化提取方法，利用路由器支持的TCL脚本实时获取路由器的各种动态信息，包括日志、运行配置、端口开放、登录用户等，综合各类信息判定攻击行为；3)利用Cisco公司开发的SnortIPS容器对过境流量进行监控，结合检测规则判定入侵行为。

但上述的入侵检测方法存在以下问题：1)核心转储文件提取信息方法需要离线分析，不能监控路由器实时状态变化；2)当前针对Cisco路由器的检测方法无法应对IOS-XE系统普遍存在的Web注入和CLI注入类漏洞利用行为和配置隐藏攻击；3)SnortIPS容器没有考虑目的地址为路由器的流量是否存在恶意流量。

2.4 解决思路

Cisco SnortIPS容器通过在容器中实现对路由器过境数据的监控方法，为我们研究IOS-XE系统的入侵检测提供了很好的思路。

1)通过在IOS-XE路由器上部署用户可控的入侵检测容器，在容器中实时监控路由器运行状态，重点关注用户在CLI中的输入，结合检测规则判定攻击行为，解决实时监控和CLI命令注入漏洞的检测问题；2)重点关注目的IP地址是路由器的网络流量，弥补UTD仅检测过境流量的不足，重点关注用户的Web请求，解决Web注入类漏洞的检测问题；3)重点分析配置隐藏的检测方法以及路由器内存中运行的TCL脚本的提取方法，解决以往无法实时判定配置隐藏和TCL后门植入的攻击行为。

3 基于容器的IOS-XE入侵检测方法

3.1 系统架构设计

3.1.1 系统设计

guestshell是Cisco IOS-XE路由器内嵌的基于LXC的容器应用，其自带的dohost功能可以直接查询路由器状态，非常适合用于入侵检测。然而由于guestshell容器安装包已经内嵌在路由器中，在guestshell中部署的入侵检测系统不易在别的IOS-XE路由器上进行移植部署，因此选择在自建容器中承载入侵检测系统，以便移植。

该系统分为以下两个模块：信息提取模块和入侵行为判定模块。信息提取模块解决了https加密流量的解密、配置隐藏攻击检测等问题，提取到了IOSd端口镜像过来的网络数据、实时查询路由器的状态信息以及IOSd发送的路由器日志信息。入侵行为判定模块通过读取信息提取模块提取到的流量、路由器状态和日志信息，结合入侵行为判定算法进行入侵行为判定，并将检测结果输出给Web服务器进行展示。

系统运行流程如图2所示。首先，在IOSd中配置ERSPAN(远程端口镜像)和日志服务，实现对路由器接口数据和路由器日志信息的获取；之后，在容器中实时接收路由器的网络数据、状态数据和日志数据，并保存到容器中部署的数据库中；最后，入侵行为判定模块从数据库中读取信息，并结合检测规则进行入侵行为判断。

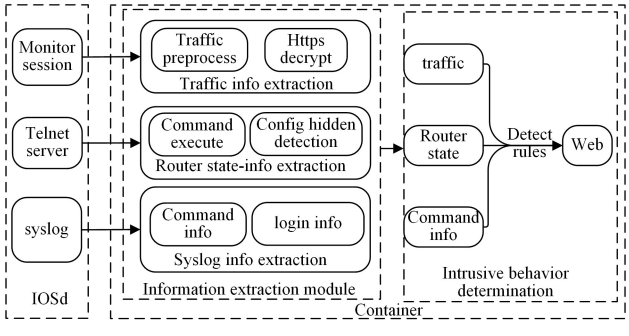


图2 系统架构

Fig. 2 System architecture

3.1.2 容器实现方法

本文在Cisco IOS-XE系统中基于自建容器实现入侵行为的检测，按文献[19]的方法制作了基于LXC的容器，容器

与 IOSd 进程通过 VPG 虚拟接口建立网络通联。自建容器与 guestshell 容器的最大区别在于 guestshell 容器的 dohost 功能可以查询路由器状态信息。dohost 功能依赖于该容器启动时映射到容器内的 unix 套接字，dohost 功能无法被移植到用户自建容器中，因此首先要解决如何从容器中查询路由器状态的问题。

本文研究了 IOS-XE 系统的模拟登录，实现了命令执行接口 router_command_execute，方便检测系统实时查询路由器状态，为检测系统实现路由器信息提取、TCL 脚本远程执行、配置隐藏检测提供了支撑。

3.2 信息提取

路由器自带的多个功能可以为攻击行为检测提供大量的原始检测数据，通过对当前路由器攻击方法进行研究，本文将重点从以下几个方面提取原始检测数据。

(1)Web 请求信息。通过对 Cisco 公司发布的 IOS-XE 路由器存在的漏洞信息进行统计，结果显示 IOS-XE 路由器存在大量的 Web 方面的漏洞，针对该类型漏洞的检测首先要获取所有的 Web 请求，然后结合漏洞的行为实现检测。Web 服务常用 http 和 https 两种协议，其中对 https 加密首先需要完成数据解密才能便于信息提取。

(2)状态信息。包括用户登录、网络连接、KRON 计划任务(Command Schedule)、嵌入式事件管理(Embedded Event Manager，EEM)、登录时间、开放端口、镜像安全等状态信息，结合管理员的操作习惯可以辅助判断攻击行为。状态信息获取的前提是要解决配置隐藏攻击的检测问题，防止获取到的状态信息被攻击者过滤和替换。

(3)日志信息。包括用户输入命令和系统产生的日志。路由器攻击者在获得路由器权限后通常会对路由器进行网络探测、跳板连接、后门用户添加、数据引流等操作，本文利用路由器的 archive 和 EEM 功能，结合在容器中部署的日志服务器，记录用户在 CLI 接口输入的所有信息。

通过对路由器各类信息的搜集，能够辅助判断口令猜解、CLI 命令注入、固件后门、Web 漏洞利用等常见的攻击手段。

3.2.1 流量处理方法

(1)流量预处理

由于本文主要定位于 Cisco 设备的自身防护，因此主要将目的 IP 为路由器地址的数据镜像到容器中。IOS-XE 不支持将数据以本地端口镜像的方式镜像数据到容器，因此本文使用 ERSPAN 的方式将数据镜像到容器中，带来的问题是镜像报文被封装成 GRE 格式。

因此，数据进入容器后需要对数据进行处理，剥离 ERSPAN 功能给数据包添加的 GRE 协议头部。GRE 头部剥离完成后得到原始数据格式，以便进行后续的信息提取。

(2)https 加密流量解密

https 协议是 Cisco 路由器 Web 管理常用的协议，Cisco 系统中默认安装了有 Cisco 签名的证书用于 https 加密传输，该证书不支持导出。为了实现对思科路由器 https 加密数据的解密，本文采用证书替换的方法，强制 Web 服务使用自签名证书进行数据的加密和解密。同时，配置 https 使用 RSA_WITH_AES_128_CBC_SHA256 加密算法，保证解密程序的解密效率。

https 解密模块实时接收预处理后的 https 加密数据，经过以下两个步骤实现加密数据的解密：1)提取客户端与服务器交互的 random 值，利用私钥解密 Client Key Exchange 中的 premaster 密钥；2)利用服务器和客户端交互的 random 和 premaster 计算 Master Secret，然后获取服务器和客户端两端的 AES 加密密钥，最后利用 AES 加密密钥解密数据。

加密数据解密后，从中提取用户发送的 Web 请求参数信息，这对检测 IOS-XE 广泛存在的 Web 漏洞利用行为至关重要。

(3)其余流量处理

除 http 和 https 流量外，目的 IP 为路由器地址的数据还包括 cdp，bgp，ospf 等。针对上述协议的攻击检测，本文借鉴了 Cisco SnortIPS 的方法，在自建的容器中部署 Snort 入侵检测程序，检测规则来源于 Cisco 官方发布的 Snort 检测规则库[20]，能帮助捕获一些本文未掌握的攻击。

3.2.2 状态信息获取方法

IOS-XE 路由器提供的 CLI 命令行支持对路由器状态信息的获取，包括运行配置、用户信息、登录信息等。然而，CLI 经常遭受配置隐藏攻击，攻击者利用配置隐藏技术过滤配置查询结果，实现指定信息的隐藏，欺骗路由器管理员和检测人员。表 1 详细列举了该攻击方法常用的技术。文中为实现路由器状态实时获取而开发的 router_command_execute 接口最终调用的是 CLI 中的命令，同样无法阻挡当前的配置隐藏攻击，利用该方法不能保证获取到的信息是没有被篡改过的。因此，配置隐藏攻击行为是否能被正确检测，关系到获取的路由器状态信息是否准确。

(1)基于信息比对的配置隐藏攻击检测方法

配置隐藏攻击对用户输入的命令进行匹配，对要隐藏的信息进行过滤或者修改。

表 2 列出了获取路由器运行配置的 5 种公开的方法，方法 1—4 很容易遭到当前的配置隐藏方法攻击；方法 5 是攻击者常用的获取路由器配置的方法，该方法利用 snmp 服务的 RW 权限的 community 字串实现运行配置的远程获取，不受当前已知的配置隐藏攻击方法影响，能获取路由器的真实配置，然而如果数据回传没有使用安全协议，或者使用了安全协议但加密密钥提前被攻击者获取，回传数据就有遭受篡改的风险。

表 2 运行配置获取方法

Table 2 Running-configuration achieve method

编号	配置获取方法
1	Show running-config
2	copy running-config bootflash:1
3	write terminal
4	more system:running-config
5	snmp 远程读取 running-config

为了抵御当前已知的配置隐藏攻击，本文提出了一种配置隐藏攻击检测方法，该方法目前在公开的资料中并未有提及。

具体流程如算法 1 所示，TCL 脚本对路由器上虚拟目录 system 中的 running-config 文件进行读取，然后利用 RC4 加密算法对文件内容进行加密，最后将加密后的结果返回。这种配置文件获取方法能抵御当前的配置隐藏攻击的原因在于 TCL 脚本的执行依赖于 TCL 脚本解释器，调用 TCL 中的文件读写函数不会被当前的配置隐藏攻击拦截和过滤。

算法 1 基于 TCL 脚本的真实配置获取

```
输入:config_filepath/*运行配置路径*/
输出:encrypted_data/*加密后的配置*/
1. fp←open(config_filepath)
2. file_data←read(fp)
3. close(fp)
4. encrypted_data←RC4(file_data)
5. return encrypted_data
```

配置隐藏检测流程如算法 2 所示。首先,通过调用 router_command_execute 执行算法 1 所对应的真实配置获取脚本,得到路由器的真实运行配置;其次,模拟登录路由器,执行配置查看命令,获取到可疑的配置信息;最后,对两种方法获取到的配置进行比对,从而判定路由器是否遭受配置隐藏攻击。

算法 2 配置隐藏攻击判定算法

```
输入:tcl/*算法 1 中的代码*/
输出:TRUE or FALSE
1. encryped_config←router_command_execute(tcl)
2. decrypted_config←RC4(encryped_config)
3. tn←TelnetRoute(route_ip)
4. result←router_command_execute(tn,'show run')
5. compare←Compare(decrypted_config,result)
6. if isTrue(compare)then
7.    return TRUE/*there is no config_hide attack*/
8. else
9.    return FALSE/*  there exist config_hide attack*/
10. end if
```

配置隐藏检测效果如图 3 所示。图 3(a)是调用 IOS-XE 路由器 CLI 命令查看的运行配置结果,图 3(b)是执行算法 1 获得的真实运行配置结果。通过调用算法 2 对两个结果进行比对,可以实现对配置隐藏攻击的判定。

```
license udi pid CSR1000V sn 9AQFR28GNZG
license boot level ax
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
!
username cisco privilege 15 secret 5 $1$Lwne$BEVxrXtma102KsttG9gN50

!
redundancy
!
```

(a)

```
license udi pid CSR1000V sn 9AQFR28GNZG
license boot level ax
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
!
username cisco privilege 15 secret 5 $1$Lwne$BEVxrXtma102KsttG9gN50
username hacker privilege 15 password 0 hacker123
!
redundancy
!
```

(b)

图 3 配置隐藏检测效果

Fig. 3 Detection result of configuration hidden

至此,在解决路由器是否遭受配置隐藏攻击的问题的基础上,可以完全信任 router_command_execute 功能对路由器状态查询的结果的真实性。

(2)基于关键字匹配的 TCL 脚本实时提取

路由器状态信息获取中,TCL 脚本的提取也是非常重要的一环。TCL 脚本是路由器控制过程中常用的方法,攻击者常在 Cisco 路由器上利用 TCL 脚本实现反向代理、通道构建、后门预置等操作,通过内存执行 TCL 脚本实现对路由器的控制和利用。Cisco 路由器内存中运行的 TCL 脚本提取可以辅助检测人员判定攻击行为,而当前从 Cisco 设备内存中提取 TCL 脚本主要依赖于核心转储文件获取并离线分析提取。

TCL 支持明文运行和密文运行两种方式。其中加密运行指将明文的 TCL 脚本编译成路由器能够识别加载的 tbc 文件。加密运行可以有效提高脚本的保密性,tbc 文件有很明显的特征,其代码中存在"tbcload::bceval{}"字符串,只需完整提取花括号中的内容即可,并使用文献[21]中所介绍的 tbc 文件的解码方法实现解码;对于后缀为 tcl 的文件,选择特征字符串"proc{}"来匹配提取内存中的脚本内容。对于编写规范的 TCL 文件,该方法提取准确率较高,反之则要人工配合分析。

算法 3 TCL 脚本提取算法

```
输入:command/*  copy system:memory/heap  */
输出:null
1. tftp←tftpserver()
2. router_command_execute(command)
3. while(TRUE)
4.    buffer←tftp.recvfrom(4096)
5.    if isHas(buffer,keystring)then/*关键字匹配*/
6.       tcl_script←extract_tcl(buffer)/*脚本提取*/
7.       writeTosql(tcl_script)/*结果写数据库*/
8.    if buffer.len<4096 then
9.       exit()
10. return
```

通过对 IOS-XE 运行 TCL 脚本的机理进行分析,可以确定运行中的 TCL 脚本保存在路由器 heap 区域。提取内存中运行的 TCL 脚本主要有两种方法:一是通过"showregion"命令确定 heap 区域的起始地址,然后利用"show memory"命令读取内存空间数据,该方法的缺点是速度慢;二是通过 copy 命令下载虚拟文件系统中的 heap 文件,该文件与 heap 空间内容是一致的,大小一般为 1 GB~3 GB 之间,下载完成后可利用二进制读取工具实现 TCL 脚本的快速定位,效率较高。

算法 3 描述了 TCL 脚本实时提取流程。通过 router_command_execute 远程回传路由器 system 目录下的 heap 文件,并循环接收 heap 文件,结合 tbc 文件的关键字和 TCL 脚本的特征,实现 IOS-XE 路由器内存中执行的 TCL 脚本的自动化定位和提取分析。

(3)系统完整性校验

系统完整性校验主要是检测 IOS-XE 路由器运行的系统是否被攻击者篡改。

文献[22]介绍了路由器镜像安全的检测方法,该方法是针对 IOS 系统检查镜像完整性,但仅检查固件和 text 代码段。IOS-XE 系统中的 IOSd 进程在执行的过程中加载了 500

多个动态链接库，攻击者有可能在加载的动态链接库中注入恶意代码，在动态链接库加载时执行恶意代码，因此仅检查固件和 text 代码段是不全面的。

本文借鉴并扩展了该方法，对路由器镜像的完整性进行检查。路由器镜像安全要考虑两个方面：一是启动的镜像文件是否完整性，与 Cisco 官方提供的信息是否一致；二是运行中的镜像可执行代码是否完整，是否有可能存在运行中的代码被恶意修改的情况。本文搜集了 432 个 Cisco 公司的 IOS-XE 系统固件，其中 ASR 系列固件 121 个，CSR 系列固件 211 个，ISR 系列固件 100 个，离线计算固件的 hash 值、IOSd 文件的 hash 值，以及加载的动态链接库的 hash 值，并建立初始索引文件。

同时，在容器中实时查询 IOSd 进程和其加载的所有动态链接库代码段的 hash 值，与索引文件中的 hash 值进行比对，从而确定系统镜像是否完整。

3.2.3 日志获取

路由器攻击者在获得路由器权限后通常会对路由器进行网络探测、跳板连接、后门用户添加、数据引流等操作，路由器日志信息中包含丰富的用户操作行为信息，包括用户命令、配置修改、用户登录等。本文利用路由器的 archive 和 EEM 功能，结合在容器中部署的日志服务器，记录用户在 CLI 接口输入的所有信息。

具体流程如下：1）开启路由器日志功能，设置远程日志服务器，使容器中的日志服务器实时接收日志信息；2）配置命令监控，包括用户命令和配置修改，实时获取用户在 CLI 中输入的所有命令信息；3）设置登录失败次数限制，并产生登录失败日志，用于防范口令猜解攻击。

3.3 攻击行为判定

本文使用误用检测和异常检测相结合的混合检测方式，实现对入侵行为的判定。误用检测指对已知攻击行为建立特征规则，当监测到的信息与特征规则相匹配，则判定为入侵行为；异常检测指分析正常操作的特征，当监测信息与正常操作特征的差异超过阈值，则产生入侵警告信息。

3.3.1 误用检测规则

误用检测对已知攻击的特征检测攻击行为依赖于准确的攻击行为规则。IOS-XE 系统已知的入侵行为主要包括 Web 注入、CLI 注入、固件后门植入等，通过对相关攻击方法的分析，构建的误用检测规则如表 3 所列。

表 3 误用检测规则

Table 3 Misuse detection rules

编号	特征	备注
1	Web 请求中包含 Linux 系统命令	Web 注入
2	CLI 命令中包含 Linux 系统命令	CLI 注入
3	运行配置所包含的用户以外的用户登录路由器	后门用户
4	show running-config 命令执行结果与真实配置有差异	配置隐藏
5	固件 hash 与官方提供的信息不一致	固件修改
6	TCL 脚本中包含 socket，exec，ios_config 等函数	TCL 后门
7	是否有连续多次(5 次以上)的登录失败日志	口令爆破攻击

例如，在检测到的 Web 访问请求中包含 CLI 命令，则可以判定有 Web 注入攻击，因为 Web 请求中不应该存在 CLI 命令。误用检测规则是从已知的攻击行为中提取得到，检测规则具备很强的针对性，在检测已知的入侵行为上，误报率和漏报率很低。随着越来越多的路由器攻击方法被揭露，可根据攻击方法提取攻击特征并对误用检测规则进行补充，使得系统检测能力不断提升。

3.3.2 异常检测规则

选择使用异常检测的目的是弥补误用检测在检测未知攻击行为能力上的不足，主要是基于攻击者操作和正常用户操作行为上的差异，实现入侵行为检测。

路由器攻击者常使用路由器提供的合法功能实现深层次入侵行为，很难通过单个行为来判定入侵行为。因此本文针对不同的行为特征设置不同的权重值用于综合判断，只有权重值超过阈值才会向用户输出告警，权重值的设定根据异常行为的可疑程度而设定不同的值。构建的异常检测规则如表 4 所列。

表 4 异常检测规则

Table 4 Anomaly detection rules

编号	异常特征	异常权重
1	日志操作	0.12
2	添加计划任务	0.11
3	修改 ACL 访问控制列表	0.11
4	使用 request，event，tcl，autocommand 等命令	0.10
5	账户操作	0.09
6	路由器开放非常规端口(22，23，80，443 以外的端口)	0.08
7	容器操作	0.06
8	路由器主动外联行为	0.06
9	存在策略路由和 GRE 隧道配置	0.06
10	使用 telnet，ssh 等远程管理命令	0.05
11	非工作时间段(08：00－17：00 以外)的操作	0.05
12	陌生的 IP 地址登录路由器	0.04
13	在路由器上进行抓包	0.04
14	存在端口镜像	0.03

基于异常行为的检测存在误报和漏报的情况，因此需要设定合理的阈值，实现误报率和准确率之间的平衡。

3.3.3 行为判定算法

行为判定算法运行流程如图 4 所示。首先从信息数据库中循环读取信息，并与误用规则进行模式匹配，如果有匹配项则直接判定有入侵行为；否则，将信息继续与异常规则进行模式匹配，对异常匹配项进行权重计算，当权重值超过阈值则向用户提出告警。

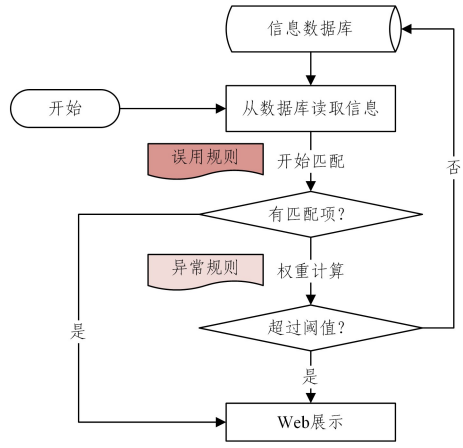


图 4 行为判定流程

Fig. 4 Behavior determination process

误用检测计算方法如式(1)所示：

$$f_i(x)=\begin{cases}1, & x\in X\\ 0, & x\notin X\end{cases} \tag{1}$$

其中，i 表示对路由器进行操作的用户固定 id 值，该值由 IP 地址和源端口组成的二元组共同确定；x 表示从数据库中获取的原始检测信息，X 表示误用规则集合，$f_i(x)$ 表示误用检测结果。

异常检测计算方法如式(2)所示：

$$g_i=\begin{cases}g_i+Y(x), & x\in Y\\ g_i, & x\notin Y\end{cases} \tag{2}$$

其中，i 和 x 的含义同上，Y 表示异常规则集合，$Y(x)$ 代表匹配异常规则表得到的权重值，g_i 代表用户 i 的异常程度值，初始值为 0，该值的计算是一个多次累加的过程，每次匹配完成后该值都会被临时保存到数据库中。比如 id 值为〈172.16.1.2,23665〉的用户对路由器的操作记录有 3 条，分别匹配异常规则表中的第 2,6 和 7 条，则该用户的最终异常度 g_i 为 0.25。

综上，入侵行为判定方法如式(3)所示：

$$F_i(x)=\begin{cases}2, & f_i(x)+g_i\geqslant 1\\ 1, & 0.25\leqslant f_i(x)+g_i<1\\ 0, & f_i(x)+g_i<0.25\end{cases} \tag{3}$$

为了平衡漏报和误报，本文根据实验(见 4.2.3 节)设置阈值为 0.25。当 $F_i(x)=0$ 时，不告警；当 $F_i(x)=1$ 时，发出中危告警，提醒管理员可能存在入侵；当 $F_i(x)=2$ 发出高危告警。

4 实验评估

4.1 实验设置

4.1.1 实验环境以及对比方法

为了验证本文方法的性能，在 ISR4300，ASR1000 实体路由器和 CSR1000v 虚拟路由器上搭建了测试环境，重点对 Web 命令注入和 CLI 命令注入进行检测。在检测前对相关漏洞进行了复现，具体测试环境如表 5 所列。

表 5 测试漏洞列表

Table 5 Vulnerability for test

设备	版本	漏洞编号	备注
ISR4300 ASR1000 CSR1000v	16.3.9	CVE-2021-1435	Web
	16.3.9	CVE-2020-3211	Web
	16.6.4	CVE-2019-1862	Web
	16.9.3	CVE-2019-12650	Web
	16.11.1a	CVE-2020-3224	Web
	16.6.3	CVE-2019-1753	Web
	16.8.1	CVE-2019-1754	Web
	16.6.3	CVE-2019-1755	Web
	16.8.2	CVE-2019-12666	CLI
	16.9.5	CNVD-2022-14605	CLI

搭建测试拓扑如图 5 所示，其中 A 为管理员主机，用于查看行为判定模块的监控结果；R 为运行 IOS-XE 系统的路由器；B 为攻击者主机，用于对路由器 R 进行口令猜解、配置修改、后门植入和漏洞利用。

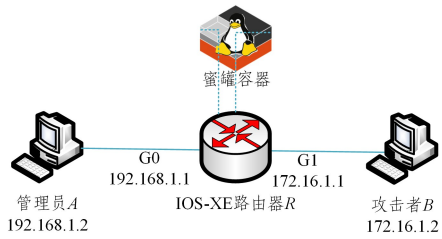


图 5 测试拓扑

Fig. 5 Test topology

同时，对以往的 Cisco 路由器入侵检测成果在 IOS-XE 路由器上进行复现，并进行实验对比，选择的对比方法如表 6 所列。

表 6 实验对比方法

Table 6 Comparative methods of experiment

对比方法	提出时间	对应文献
方法 1	2018	[5]
方法 2	2020	[4]
方法 3	2020	[6]

4.1.2 测试方法

具体步骤如下：首先，在路由器上准备日志记录、数据镜像等功能，启动容器中的入侵检测系统，准备捕获各类信息；其次，根据测试内容，对路由器进行相应的行为检测；最后，访问检测系统的 Web 功能，对检测结果进行分析。

4.2 测试结果

4.2.1 数据采集能力对比测试

为了验证本文方法在数据采集方面的优势，从表 7 中提取 29 种攻击特征(19 种普通攻击特征和 10 个漏洞利用行为)用于测试，并与表 6 中的 3 种方法进行数据捕获能力的对比，具体测试结果如图 6 所示。

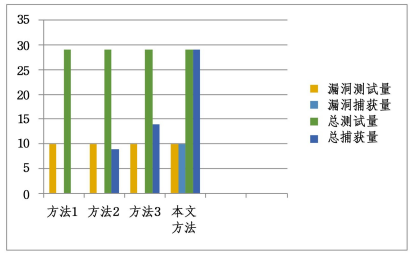


图 6 数据采集能力对比

Fig. 6 Data acquisition capability comparison

实验结果表明，本文方法在路由器信息采集方面能力较强，信息捕获更加全面，尤其是在注入类漏洞行为捕获上优于对比方法。其原因在于，方法 1 只捕获路由器收到的网络数据，没能关注路由器状态变化和用户请求；方法 2 专注于监控路由器状态变化，没能解决配置隐藏攻击检测问题，且没能实时提取和分析路由器日志；方法 3 主要使用离线分析方法，不能实时监控路由器命令输入，且无法解决路由器自身 https 流量的解密问题。

4.2.2 测试数据集的构建

路由器入侵检测领域没有成熟的测试数据集，本文通过抽取常见的攻击特征和正常管控特征组成测试数据集。

攻击行为从表 7 的 21 种攻击特征中随机选取。攻击者

攻击过程常包含多个特征，测试时最少选取 4 种，从每一组中抽取的特征共同组成一次攻击行为，用于模拟攻击者对路由器进行攻击；正常管控行为从表 8 中随机抽取（编号 1 与编号 2、编号 3 与编号 4 为互斥特征，对于互斥特征每次只能抽取其中一个）。正常情况下管理员对路由器管理的行为较少，为了更好地模拟用户正常管控行为，特征抽取时最多选取 8 种，从每一组中抽取的特征共同组成一次正常管控行为，模拟管理员的正常管控行为。

表 7 常见攻击特征

Table 7 Common attack characteristics

编号	特征	编号	特征	编号	特征
1	CLI 注入	8	口令爆破	15	非法用户登录
2	Web 注入利用	9	日志操作	16	存在流量牵引
3	TCL 后门脚本	10	路由器开放非常规端口	17	计划任务
4	使用 request，event，tcl，autocommand 等危险命令	11	主动外联	18	利用路由器横向渗透（ssh，ip nat 等）
5	IOSd 代码修改	12	ACL 修改	19	账户操作
6	配置隐藏	13	异常 IP 登录	20	路由器流量嗅探
7	容器操作	14	工作时间段以外操作	21	存在端口镜像

表 8 正常管控特征

Table 8 Normal management characteristics

编号	管控行为	编号	管控行为
1	非工作时间登录	9	容器自动化管理
2	工作时间登录	10	查看运行配置
3	非工作 IP 登录	11	端口镜像分析
4	工作 IP 登录	12	上传下载文件
5	账户操作	13	测试联通性
6	ACL 操作	14	抓包排错
7	查看接口状态	15	修改路由表
8	修改接口属性	16	查看日志

每次测试抽取一组攻击行为和一组正常管控行为，经过多次重复抽取得到一个测试数据集，可以用于测试本文方法在检测入侵行为中的检测率和误报率。

4.2.3 阈值设置

3.3.3 节在判断入侵行为时结合了误用检测和异常检测，异常检测需要测定一个阈值用于判定入侵行为，可以通过设置不同的阈值，并测试该阈值下本文提出的检测方法的检测率和误报率，来得到合理的阈值。测试结果如表 9 所列。由实验结果可知，阈值越小，误报率越高；阈值越大，入侵检测率越低。当阈值为 0.2 时，检测率较好，但是误报率较高；当阈值为 0.25 时，检测率和误报率相对平衡，误报率在可接受范围内；当阈值为 0.3 时，在检测入侵行为较少的情况下检测率不高。因此，本文中阈值选取 0.25。

表 9 阈值测定

Table 9 Threshold determination

阈值	随机抽取攻击行为	随机抽取正常行为	重复次数	检测成功次数	误报次数	误报率/%	检测率/%
0.20	4	4	8	5	0	0.0	62.5
	6	6	8	8	2	25.0	100.0
0.25	4	4	8	7	1	12.5	87.5
	6	6	8	8	2	25.0	100.0
0.30	4	4	8	4	0	0.0	50.0
	6	6	8	7	0	0.0	87.5

4.2.4 通用性测试和性能测试

为了测试本文方法的通用性和检测性能，在 ISR4300，ASR1000，CSR1000v 这 3 个系列路由器（IOS-XE 版本为 16.9.3，该版本既存在 Web 注入和 CLI 注入漏洞，方便测试）上进行实验对比测试。

检测结果如表 10 所列，在 ASR，ISR 和 CSR 这 3 种系列路由器上进行测试，随机选取不同数量的攻击行为和正常行为组成测试用例，并将正常行为和攻击行为分开测试。

表 10 性能测试结果

Table 10 Performance test results

测试环境	随机抽取攻击行为	随机抽取正常行为	重复次数	方法 2					方法 3					本文方法				
				行为捕获数量	检测成功次数	误报次数	误报率/%	检测率/%	行为捕获数量	检测成功次数	误报次数	误报率/%	检测率/%	行为捕获数量	检测成功次数	误报次数	误报率/%	检测率/%
ISR4300 16.9.3	4	4	8	24	5	3	37.5	62.5	43	4	0	0	50.0	64	6	1	12.5	75.0
	5	5	8	36	5	3	37.5	62.5	55	5	0	0	62.5	80	7	2	25.0	87.5
	6	6	8	40	6	4	50.0	75.0	61	6	0	0	75.0	96	8	2	25.0	100.0
	7	7	8	48	7	5	62.5	87.5	69	7	0	0	87.5	112	8	1	12.5	100.0
ASR1000 16.9.3	4	4	9	31	5	2	22.2	55.6	49	6	0	0	66.7	72	5	0	0.0	55.6
	5	5	9	39	6	3	33.3	66.7	60	6	0	0	66.7	90	6	1	11.1	66.7
	6	6	9	51	8	4	44.4	88.9	76	7	0	0	77.8	108	9	2	22.2	100.0
	7	7	9	55	8	4	44.4	88.9	91	8	0	0	88.9	126	9	2	22.2	100.0
CSR1000v 16.9.3	4	4	10	33	6	2	20.0	60.0	55	5	0	0	50.0	80	5	1	10.0	50.0
	5	5	10	47	7	3	30.0	70.0	71	4	0	0	40.0	100	7	2	20.0	70.0
	6	6	10	56	9	3	30.0	90.0	85	5	0	0	50.0	120	10	2	20.0	100.0
	7	7	10	63	9	4	40.0	90.0	101	6	0	0	60.0	140	10	3	30.0	100.0

测试结果表明，方法 2 使用运行效率较低的 TCL 脚本实现检测，重点关注路由器配置的修改行为，缺乏对加密请求流量的解密能力，该方法在入侵行为判定上根据单条规则触发即判断入侵行为，误报率较高；方法 3 需要利用 Cisco 核心

转储功能获取核心转储文件进行离线分析，由于该方法是通过检测信息的语义判断是否存在入侵行为，误报率很低。但是该方法在路由器实时状态获取方面能力较差，缺乏对加密请求流量的解密能力，无法检测 IOS-XE 普遍存在的注入类漏洞检测能力。相比之下，本文提出的检测方法在掌握的攻击者攻击行为越多的情况下，检测率越高，在测试过程中平均检测率为 83.3%，平均误报率为 17.5%，检测率高于两种对比方法，且误报率在可接受范围内。

此外，为了测试本文方法的运行性能，对方法 2、方法 3 和本文方法的运行时间（检测完成时间与测试数据输入完成时间差）、存储消耗（占用的运行内存）做记录。随机选取 5 种正常特征、7 种异常特征，重复测试 10 次。

开销对比实验结果如表 11 所列，可以看出，本文方法的时间开销最少。原因在于，本文方法在自建的 LXC 容器中开发了入侵检测系统，系统运行环境优于方法 2 的运行环境；而方法 2 在路由器上部署了基于 TCL 脚本的检测系统，运行效率低；方法 3 通过离线分析检测，导致消耗时间和存储消耗都最多。

表 11 开销对比

Table 11 Overhead comparison

测试环境	对比方法	时间消耗/ms	存储消耗/byte
CSR1000v 16.9.3	方法 2	13418	377520
	方法 3	785668	≥5242880
	本文方法	9685	1048576

4.3 实验结果总结

通过和已有的路由器入侵检测与取证方面的研究成果进行对比分析，实验结果表明本文提出的方法对 IOS-XE 路由器攻击利用具备相对较好的检测能力。

（1）实时检测能力

由于本文解决了 IOS-XE 路由器上 https 流量的解密问题，并具备在容器中查询路由器配置和状态信息的能力，能够实时监控用户的 Web 请求、CLI 命令输入和其余日志信息，因此在检测实时性方面比以往的研究成果更好。

（2）注入类漏洞检测能力

本文方法在解决路由器 https 加密流量的解密问题后，分析了 IOS-XE 路由器的 Web 注入利用方法和 CLI 命令注入方法，实现了对该型号路由器的注入类漏洞利用检测，弥补了当前针对该型号路由器注入类漏洞检测的空白。

（3）路由器攻击利用检测能力

通过对现有路由器攻击利用方法进行分析研究，结合以往在路由器取证方面的研究成果，形成攻击检测策略，能有效检测路由器攻击中的口令猜解、后门植入、配置隐藏、流量牵引等利用方法，提升对路由器攻击的检测能力。

结束语 本文提出了基于容器的 IOS-XE 系统的入侵检测方法，在路由器的内嵌容器中实时搜集路由器的状态信息和路由器收到的网络流量，结合对现有 Cisco 路由器的攻击方法的深入研究，总结入侵行为检测规则，实现对口令爆破、配置隐藏、Web 注入攻击等入侵行为的检测。实验结果表明，本文提出的方法实时性和通用性较好，且能解决 IOS-XE 路由器所面临的 Web 注入攻击和 CLI 命令注入攻击问题，检测效果较好。

不足之处在于文中所提的流量检测仅针对 Web 流量进行检测，未能扩展到其他协议流量。下一步将探索从路由器进程信息、堆栈信息、内存信息中还原更多的底层操作系统变化信息，弥补所提方法的不足。

参 考 文 献

[1] IDC. IDC's Worldwide Trackers Show Growth in the Ethernet Switch and Router Markets in Q3 2021[EB/OL]. (2021-12-08)[2022-03-05]. https://www.idc.com/getdoc.jsp?containerId=prUS48502421.

[2] DANIEL Z. Hacker broke into T-Mobile via vulnerable router[EB/OL]. (2021-09-02)[2022-03-05]. https://adware.guru/hacker-broke-into-t-mobile/.

[3] LINDNER F. Developments in Cisco IOS forensics[EB/OL]. (2009-08-14)[2022-03-05]. http://www.blackhat.com/presentions/bn-usa-08/Linder/BH_US_08_Linder_Developments_in_IOS_Froensics.pdf/.

[4] LIU B N, CAI R J, YIN X K, et al. A Method for Detecting Malicious Behavior of Weakly Supervised Routing Equipment[J]. Journal of Information Engineering University, 2020, 21(3): 361-368.

[5] Cisco. Snort IPS[EB/OL]. (2017-08-07)[2022-03-05]. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16-12/sec-data-utd-xe-16-12-book/snort-ips.pdf.

[6] DAMIRIS G P. Router Forensics[D]. Piraeus: University of Piraeus, 2020.

[7] Cisco Systems, Inc. Troubleshoot Datapath Handling by UTD and URL-Filtering[EB/OL]. (2020-01-10)[2022-01-22]. https://www.cisco.com/c/en/us/support/docs/routers/xe-sd-wan-routers/215107-troubleshoot-datapath-handling-by-utd-an.html.

[8] KURELI S. Snort IPS on ISR, ISRv and CSR-Step-By-Step Configuration[EB/OL]. (2018-04-19)[2022-03-09]. https://community.cisco.com/t5/security-documents/snort-ips-on-isr-isrv-and-csr-step-by-step-configuration/ta-p/3369186.

[9] YAO K L, WANG R X, LUO C J, et al. SSH Password Brute Force Cracking and Defense Based on Kali Linux[J]. Network Security Technology & Application, 2022(7): 27-28.

[10] NATHAN A. Best Practices and Useful Scripts for EEM[EB/OL]. (2020-10-12)[2022-02-26]. https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-16/216091-best-practices-and-useful-scripts-for-ee.html.

[11] MANUEL H S P. IOSTrojan: Who really owns your router?[EB/OL]. (2009-08-04)[2022-02-26]. https://sansorg.egnyte.com/dl/MTDsf9Y5xu.

[12] MIKE P. IOS-XE: request system shell vulnerability[EB/OL]. (2014-11-12)[2022-03-05]. https://networkengineering.stackexchange.com/questions/12790/ios-xe-request-system-shell-vulnerability.

[13] Trend Micro Research Team. CVE-2019-12643: CISCO IOS XE

AUTHENTICATION BYPASS VULNERABILITY[EB/OL]. (2019-10-18)[2022-03-05]. https://www.zerodayinitiative.com/blog/2019/10/17/cve-2019-12643-cisco-ios-xe-authentication-bypass-vulnerability.

[14] MUNIZ S. Killing the myth of Cisco IOSrootkits [EB/OL]. (2008-05-01)[2022-03-05]. https://drwho.virtadpt.net/images/killing_the_myth_of_cisco_ios_rootkits.pdf.

[15] ANDY D. Creating Backdoors in Cisco IOS using Tcl[EB/OL]. (2007-11-28)[2022-03-05]. http://www.irmplc.com/content/pdfs/Creating_Backdoors_in_Cisco_IOS_using_Tcl.pdf.

[16] KYLER M. Penetration Testing: How to Hide an Admin User on Cisco IOS(Router/Switch) Platform[EB/OL]. (2015-04-03)[2022-03-05]. https://www.kylermiddleton.com/2015/04/penetration-testing-how-to-hide-admin.html.

[17] Gauis. Things To Do in Ciscoland When You're Dead[EB/OL]. (2000-01-05)[2022-01-24]. http://www.phrack.org/issues/56/10.html.

[18] NAKIBLY G, SCHCOLNIK J, RUBIN Y. {Website-Targeted} False Content Injection by Network Operators[C]// 25th USENIXSecurity Symposium(USENIX Security 16). 2016:227-244.

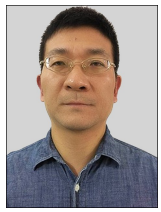
[19] RADOVAN B. Hosting KVM Apps Inside IOS XE Virtual Service Container [EB/OL]. (2020-08-02)[2022-03-14]. https://brezular.com/2020/08/02/hosting-kvm-apps-inside-ios-xe-virtual-service-container/.

[20] Cisco. UTD Snort Signature[EB/OL]. (2022-03-12)[2022-03-15]. https://software.cisco.com/download/home/284364978/type/286285292/release/29130.383.

[21] Corbamico. TBC(TclByteCode) decoder[EB/OL]. (2018-07-31)[2022-01-22]. https://github.com/corbamico/tbcload.

[22] CERT-EU. CISCO IOS/IOS XE Risk Mitigation [EB/OL]. (2014-10)[2022-03-15]. https://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_08_CISCO-Risk-Mitigation_1_5.pdf.

YANG Pengfei, born in 1990, postgraduate. His main research interests include network device security and network attack detection.



LIU Shengli, born in 1973, Ph.D, professor. His main research interests include network device security and network attack detection.

(责任编辑:何杨)