基于组合扫描的无状态工控设备资产探测方法

郑铁军[1],王　齐[2,3],张宏杰[1],贺建伟[1],雍少华[4],孙知信[5]
(1. 国网宁夏电力有限公司,宁夏 银川 750010;
2. 国网智能电网研究院有限公司,江苏 南京 210003;
3. 信息网络安全国网重点实验室,江苏 南京 210003;
4. 国网中卫供电公司,宁夏 中卫 755099;
5. 南京邮电大学 现代邮政学院,江苏 南京 210003)

摘　要:全面探测工控设备资产信息、了解资产状态是确保工业控制系统安全的重要前提。端口探活是进行资产探测的第一步,端口探活的准确率和效率将直接影响资产探测的性能。为提升端口探活的速度和准确性,提出了一种基于组合扫描的异步无状态端口扫描方法。通过构造组合扫描数据包,解决工控设备因禁 ping 导致主机探活准确率降低的问题,同时建立发送数据包线程和接收数据包线程,实现组合扫描数据包的异步处理,消除了传统无状态扫描的回复等待时间,缩短了端口探活时间。最后以 Modbus 协议为例,构造了资产请求数据包,并分析了数据包中主要字段和功能。测试结果表明,提出的资产探测方法在端口探活阶段单位时间内可以探测到更多的设备,同时能在较短的时间内完成完整资产信息的探测,在探测准确度和探测时间方面都得到了提升。

关键词:工业控制系统;资产探测;工控设备;端口扫描;异步处理
中图分类号:TP393　　**文献标识码**:A　　**文章编号**:1673-629X(2023)07-0098-06
doi:10.3969/j.issn.1673-629X.2023.07.015

Stateless Industrial Control Equipment Asset Detection Method Based on Combined Scanning

ZHENG Tie-jun[1],WANG Qi[2,3],ZHANG Hong-jie[1],HE Jian-wei[1],YONG Shao-hua[4],SUN Zhi-xin[5]
(1. State Grid Ningxia Electric Power Co.,Ltd.,Yinchuan 750010,China;
2. State Grid Smart Grid Research Institute Co.,Ltd.,Nanjing 210003,China;
3. State Grid Key Laboratory of Information & Network Security,Nanjing 210003,China;
4. State Grid Zhongwei Electric Power Supply Company,Zhongwei 755099,China;
5. School of Modern Posts,Nanjing University of Posts and Telecommunications,Nanjing 210003,China)

Abstract:Comprehensive detection of the asset information of industrial control equipment and understanding the asset status is an important prerequisite to ensure the safety of industrial control system. Port detection is the first step of asset detection. The accuracy and efficiency of port detection will directly affect the performance of asset detection. In order to improve the speed and accuracy of port detection,an asynchronous stateless port scanning method based on combined scanning is proposed. By constructing combined scanning data packets,the problem that the accuracy rate of host detection is reduced due to the prohibition of Ping in industrial control equipment is solved. At the same time,a sending packet thread and a receiving packet thread are established to realize asynchronous processing of combined scanning packets,which eliminates the reply waiting time of traditional stateless scanning and shortens the port detection time. Finally,taking Modbus protocol as an example,the asset request data packet is constructed,and the main fields and functions in the data packet are analyzed. The test results show that the proposed asset detection method can detect more equipment per unit time in the port detection stage,and complete the detection of complete asset information in a shorter time,which improves the detection accuracy and detection time.

Key words:industrial control system;asset detection;industrial control equipment;port scanning;asynchronous processing

收稿日期:2022-08-12　　**修回日期**:2022-12-14
基金项目:宁夏自然科学基金项目(2022AAC03613)
作者简介:郑铁军(1984-),男,硕士,高级工程师,研究方向为网络信息安全技术研究与应用;通信作者:王　齐(1983-),男,硕士,高级工程师,研究方向为网络安全。

0　引　言

工业控制系统(Industrial Control System,ICS)是电力、冶金、交通、能源等工业基础设施的核心组成部分,也是国民经济、社会运行和国家安全的重要基础。自 2019 年以来,受全球新冠疫情的影响,很多工作人员不得不在家里通过虚拟专用网络(Virtual Private Network,VPN)连接 ICS 实现居家办公,这加速了公共互联网与工业控制网络的融合,使工业控制网络与公共互联网的界限变得越来越模糊,打破了 ICS 的封闭性,导致 ICS 也将面临公共互联网中存在的各种安全问题[1-2]。

国家计算机网络应急技术处理协调中心 CNCERT 发布的《2021 年上半年我国互联网网络安全监测数据分析报告》显示[3],大量暴露在互联网的工控设备类型有串口服务器、可编程逻辑控制器等;存在高危漏洞的系统涉及电力、石油、煤炭、城市轨道交通等重点行业,覆盖企业生产管理、企业经济管理、政府监管、工业云平台等。由于暴露在互联网中的工控设备类型越来越多,ICS 应用行业越来越丰富,运行环境越来越复杂,ICS 面临着前所未有的挑战。如果不能很好地防范 ICS 的安全,那么一旦被攻击带来的人力物力财力等各方面的损失将是不可估量的。思科的 Talos 安全研究团队在 2018 年发文指出美国罗克韦尔自动化公司的 Allen-Bradley MicroLogix 1400 系列可编程逻辑控制器中存在多项严重安全漏洞[4],一旦被黑客利用,很可能会发起拒绝服务攻击、篡改设备配置、修改内存模块上的数据等。因此,解决和强化 ICS 安全问题的关键是通过网络资产探测技术实时监测工控设备的资产信息,及时发现系统漏洞[5-6]。

工控设备资产探测的流程主要包括:端口探活、协议数据包构造、通信连接建立和数据收集。首先,对工控设备进行端口探活,获取运行指定工控协议的设备;然后,构造对应协议的探测数据包,与目标设备经过三次握手建立通信连接;最后,根据目标设备的响应数据包解析其资产信息。其中,端口探活需要首先确定被扫描的主机是否可达,然后扫描可达主机是否开启了指定的工控端口。对主机可达性的确认采用 ping 检测技术,通过构造特定的 ICMP 数据包,然后发送给目标主机,根据目标主机的响应判断是否存活。然而大多数的工控设备为了防止被扫描,通常会开启禁 ping 功能,将降低设备探活的准确性,从而影响资产探测的效率。此外,对可达主机端口的扫描最常采用的是全连接扫描和无状态扫描,但不管采用哪一种扫描方式都需要设置 timeout 参数,等待目标主机的响应。当进行大规模扫描时,等待时间将会成为提高扫描速度的瓶颈。

因此,该文旨在提高端口探活的准确性和速度,对端口探活过程中的主机存活扫描技术和端口扫描技术进行研究,提出一种基于组合扫描的异步无状态扫描方法,获取开放指定工控协议端口的设备,然后结合具体的工控协议构造请求数据包,从而收集设备的资产信息,为系统漏洞安全问题的发现提供依据。

1　相关研究

工控设备的资产信息是指可以标识设备的相关信息,包括设备的供应商、修订版本、产品代码等数据。目前,对工控设备进行资产探测的方法主要是基于传统互联网设备的探测技术。国外针对工控设备探测技术开展了一系列的研究,开发了很多功能强大的探测工具,其中使用较为广泛的是 Flody 公司发布的 Nmap 探测工具[7],并且很多其他探测工具都是由 Nmap 延伸开发出来的,比如 Shodan[8] 和 Zmap[9]。Nmap 是一种基于协议的网络探测工具,适用于快速扫描大型网络。除此之外,它还可以用来获取目标设备的操作系统类型、服务类型等。它的探测原理与 ping 检测技术类似,并且可以实现对多种协议的探测,但是由于很多工控设备通常会开启禁 ping 功能,所以使得 Nmap 对工控设备的探测准确率较低。

J. Matherly 通过长期对工控设备探测技术的研究,在 Nmap 探测工具的基础上发布了 Shodan 网络空间探测引擎[8,10]。Shodan 可以直接通过互联网查找物联网设备,然而由于 Shodan 对工控设备的扫描原理是基于 Nmap 的扫描方式,所以在探测性能方面并没有得到优化和提升,仍然面临着对工控设备探测准确率较低的问题。

为了进一步提升探测速度,密歇根大学在 Nmap 工具的基础上设计开发了 Zmap 设备扫描器,该扫描器主要功能是发现开放端口[9,11]。因为 Zmap 使用了无状态连接的扫描方式进行端口扫描,所以它的扫描速度比 Nmap 快了 1 300 倍,在 1 GB 带宽的网络环境下,扫描全部 IPV4 地址空间只需要 45 分钟。然而,由于其追求探测速度,等待与目标设备建立连接的时间很短,所以探测到的资产信息量比较少,使得其探测准确率较低。

国内在工控设备资产探测方面也取得了一些成果,文献[12]设计了一种工业控制系统扫描平台(ICSMap),该平台将 Nmap 和 Zmap 进行了结合,优化了探测的效率,并且支持扫描多种工控协议,但是探测的准确率并没有得到优化。文献[13-14]针对西门子工控设备提出了一种基于 Profinet 协议的扫描方法,该方法利用 Profinet 协议获取西门子工控设备的资产信息,但是该方法仅适用于对西门子厂商生产出来的

工控设备进行探测,不支持其他工控协议。文献[15]提出了一种基于 NSE 脚本的工业互联网设备探测方法,可支持多种工控协议。但是该方法只是增加了支持的工控协议种类,并没有优化探测性能。文献[5,16]专门提出了一种针对工控设备的通用资产探测方法,可同时支持 Modbus、S7、DNP3 和 BACnet 四种工控协议,并且在端口探活阶段通过增加数据包的发送,以解决工控设备中的禁 ping 问题。然而由于对工控设备的探测通常集中在某个网段,涉及的设备数量比较多,如果端口探活阶段增加数据包的数量很有可能引起网络拥塞,另外等待目标设备响应而设置的 timeout 参数也会成为提升扫描速度的瓶颈。因此,基于上述研究,该文旨在提高工控设备资产探测的速度和准确性。

2 基于组合扫描的异步无状态工控设备资产探测方法

对传统互联网的探测往往是对一台或者几台设备进行一些常用端口或者全部端口的探测,目的是全面收集这些探测设备端口的开启和关闭情况、设备信息和安全漏洞等,通常情况,对一台设备的探测时间会比较久。与传统互联网不同,对工控设备的探测通常集中在某个网段,涉及的设备数量比较多,如果对大量没有开启的端口或者不运行的设备发送大量探测数据包,将会造成系统资源的不必要浪费,导致探测效率的降低。因此,该文首先对端口进行探活,初步发现探测的网段中有哪些设备正在运行。

端口探活技术包括主机扫描技术和端口扫描技术两种类型。主机扫描是收集探测信息的第一步,以确定扫描的目标主机是否可达。主机存活扫描利用的最基本手段是 ping 命令,通过 ping 命令来探测能否与目标主机建立通信连接。然而大多数的工控设备为了防止被扫描,通常会开启禁 ping 功能。此时就无法通过 ping 命令判断设备的状态,从而降低了探测的准确性。当通过主机扫描技术确认了目标主机的连接状态后,接下来就利用端口扫描技术对处于运行状态的设备进行端口开放情况的探测。传统的端口扫描方式主要是通过 TCP 三次握手去连接,而建立连接过程中存在的连接状态是由操作系统在底层实现存储的,需要消耗大量的系统资源,从而限制了端口扫描的速度,延长了探测周期。

为了解决工控设备因开启禁 ping 命令而引起探测准确性降低的问题,目前常用的方法是构造多个不同的数据包,在对目标主机进行探活时依次将多个报文发送给目标设备,只要能收到其中一个报文的回复,就说明目标设备是处于开启状态的[5,16]。这种方式虽然能避免禁 ping 和丢包造成的错误判断,但是主机探活过程将产生大量数据包,不仅浪费系统资源,而且容易引起网络拥塞。在端口扫描阶段,为了提高端口扫描速度和节约系统资源,产生了一种无状态的连接方式,无状态连接是指主机不需要关心 TCP 连接的状态。无状态连接的通信过程如图 1 所示。首先扫描主机向目标主机发送一个 SYN 数据包,然后等待目标主机回复 SYN+ACK 包,之后发送 RST 取消建立连接。因整个过程没有完成 TCP 的三次握手连接,所以不会占用操作系统的 TCP/IP 协议栈资源,也不需要操作系统对连接状态进行会话组包。这种方式可以极大地提高端口扫描的速度,但是,TCP SYN 扫描很容易被对方的入侵检测系统或防火墙检测到,并且需要设置 timeout 参数等待目标主机的回复。

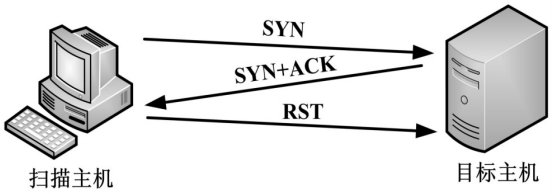

图 1 无状态链接通信过程

因此,该文提出一种基于组合扫描的异步无状态端口扫描方法,通过建立发送数据包线程和接收数据包线程,来消除等待目标服务端回复的时间,以进一步提升扫描速度,并且发送数据包线程采用组合扫描的方式,同时实现对主机存活状态和端口开关状态的判断。组合扫描的过程如图 2 所示。

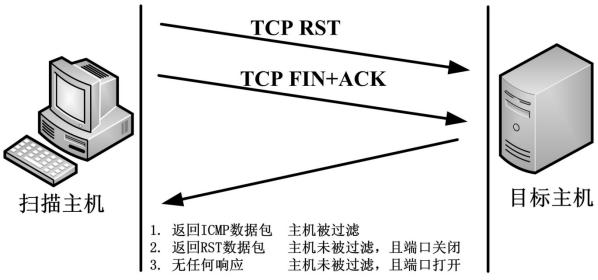

图 2 组合扫描过程

组合扫描是同时发送 TCP RST 数据包和 TCP FIN+ACK 数据包到目标主机。根据 RFC 793 协议规定,当主机收到 TCP RST 数据包时,尽管 TCP 堆栈不会响应这个类型的数据包,但如果无法访问目标计算机,路由器将发送 ICMP 数据包。因此,如果没有返回 ICMP 数据包,则表示目标存在;否则,目标不存在。这个操作可以用来判断目标主机是否被过滤,能更多地获取工控设备的存活信息,避免因为禁 ping 问题而做出错误判断,大大提高端口探测的准确率。当向目标主机发送 TCP FIN+ACK 数据包时,若未收到响应,则表示目标端口打开或者目标主机被过滤;若收到

RST 数据包,则表示目标端口关闭。这个操作可以有效降低被对方的防火墙或入侵检测系统监测到的概率,因为该方法没有完成完整的连接操作,所以对方不会认为是一种扫描或攻击,而只会认为是一次网络错误的发生,从而不会被记录下来。

扫描过程启动后,扫描主机会对网卡建立一对异步处理线程,分别是发送数据包线程和接收数据包线程[17]。发送数据包线程将构造好的组合扫描数据包发送给目标主机,如果目标主机返回响应数据包,响应数据包由接收数据包线程接收,并解析收到的数据包。整个过程中,发送数据包线程只负责发送构造好的探测数据包,接收数据包线程只负责接收目标主机的响应数据包,两者之间没有交互,从而消除了传统无状态连接的回复等待时间,具体工作流程如图 3 所示。

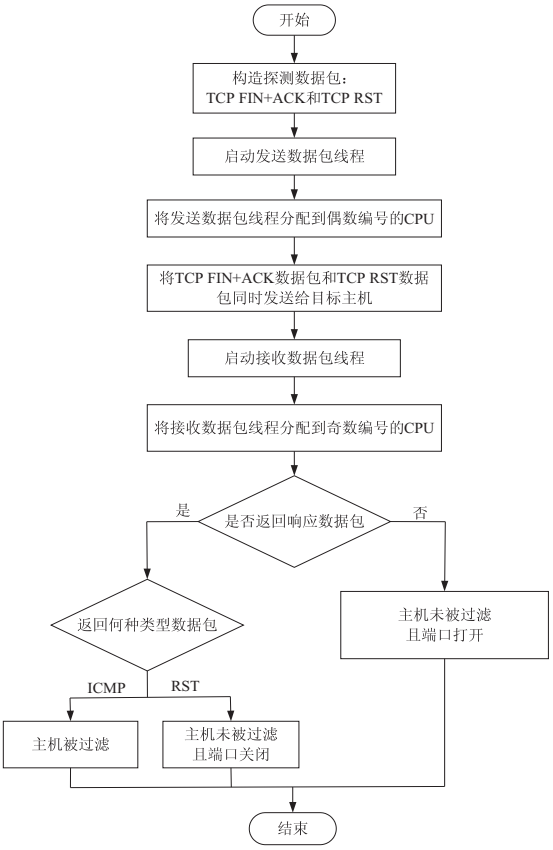

图 3　基于组合扫描的异步无状态端口扫描工作流程

为了更好地实现异步操作,在启动发送数据包线程和接收数据包线程后,将发送数据包线程分配到偶数编号的 CPU,接收数据包线程分配到奇数编号的 CPU。发送和接收数据包线程的具体执行流程如下:发送线程首先创建一个指向外部变量的指针,用于通知线程内发送数据包的数量以及当前的发送速度等信息,然后发送数据包线程初始化被扫描网段的 IP 和端口,设置数据包的初始发送速度,接着根据被扫描网段的 IP 数和每个 IP 端口数的乘积来确定需要执行的扫描数量,最后循环发送组合扫描数据包,直到完成指定扫描数量,进入下一网段的扫描。接收线程同样首先创建一个指向外部变量的指针,用于通知线程内接收数据包的数量以及当前的接收速度等信息,然后创建接收表记录响应数据包的信息,并根据响应数据包输出端口开放情况。

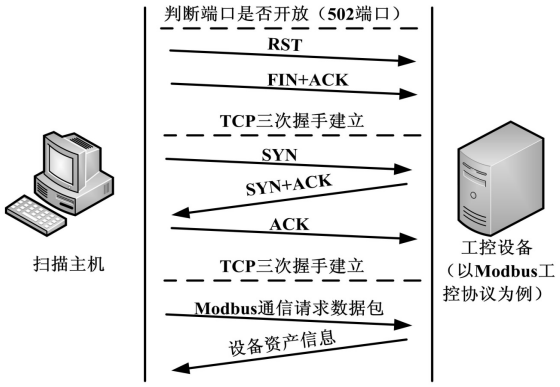

图 4　Modbus 工控设备资产探测通信流程

以 Modbus 工控协议[18]为例,它是一种基于以太网 TCP/IP 的应用层通信传输协议,广泛应用在分散控制方面。运行 Modbus 协议的设备资产探测通信流程如图 4 所示。Modbus 协议常用的端口号是 502,通过上述端口探活流程,获取开启了 502 端口的工控设备,然后扫描主机向目标工控设备的目标端口发起 TCP 三次握手连接。通信连接建立后,扫描主机首先构造 Modbus 通信请求数据包,构造的 Modbus 通信请求数据包如表 1 所示。Modbus 数据包中的字段是由十六进制编码构成的,前两个字节 00 00 为此次通信事务处理标识符,通常每次通信之后会加 1 以区别不同的通信数据报文。接下来的两个字节 00 00 表示 Modbus 的协议标识符,00 06 为数据长度,单位是字节,这里表示的是请求 6 个字节的数据信息。09 是设备地址,即这台设备中包含资产信息的寄存器编号,以上 7 个字节称为 Modbus 的报文头。03 为功能码,表示读取保持寄存器。00 00 为起始地址;00 01 为读取的寄存器数,即从 00 00 开始读取 6 个字节,并且只读 1 个资产信息寄存器。然后将此数据包发送给目标设备,之后目标设备返回 6 个字节数据的资产信息,通常包含有工控设备供应商、产品型号、版本号等[19]。

表 1　构造的 Modbus 通信请求数据包

构造字段码	字段码说明
0x00 0x00	通信事务处理标识符
0x00 0x00	协议标识符,0000 标识为 Modbus 协议
0x00 0x06	数据长度,指示接下来的数据长度,单位字节
0x09	设备地址
0x03	功能码,读取保持寄存器
0x00 0x00	起始地址
0x00 0x01	读取的寄存器数

3 性能测试

为了验证提出的资产探测方法在探测准确度和探测时间上的优势,选取传统资产探测工具 Nmap 和文献[16]提出的资产探测方法作为对比进行实验验证。探测准确度和探测时间的定义如下:

探测准确度:在端口探活阶段,单位时间内探测到的开放指定端口的 IP 数量。IP 数量越多,说明探活的准确度越高,能够获得资产信息的设备数越多。

探测时间:在指定网段内完成完整资产探测所需的时间,包括端口探活时间和获取设备资产信息的时间,探测时间越短,说明探测速度越快。

端口探活阶段是扫描主机与目标工控设备建立初步通信的阶段,这个阶段的准确性将对后面探测具体资产信息的工作产生直接影响。为了保证探测准确度不受网络环境的影响,实验选定的探测范围为同一 IP 范围段,并且是三台主机在同一时间段内并行运行不同资产探测方法。此外,用 Python 编写脚本以实时记录探活数量和探活时间,统计一段时间内探活到的开放指定端口的 IP 数量。实验如无特殊说明,均以 Modbus 的 502 端口为探测的目标端口,这是因为 Modbus 协议在工控设备中的应用较多,能够进行探测的 IP 范围较为广泛,测试结果如图 5 所示。

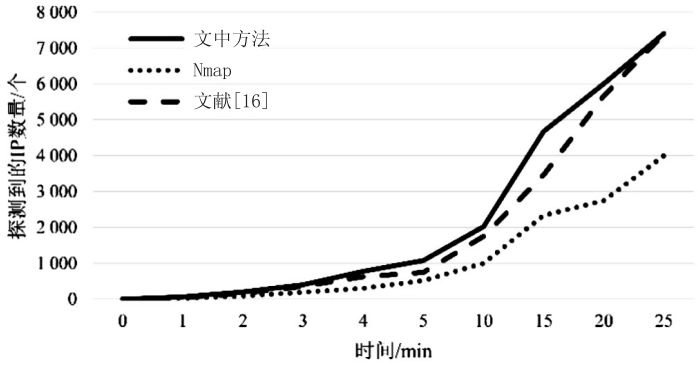

图 5 Modbus 端口探活结果

由图 5 可以看出,提出的基于组合扫描的异步无状态端口扫描方法在单位时间上探测到的 IP 数量明显增多,这说明在同一 IP 范围段,提出的方法能够获取更多设备的资产信息。从具体数据上来看,在实验呈现的时间段内,所提方法的探测准确度与 Nmap 相比提高了 2 倍左右。这是因为采用的组合扫描方式可以有效降低被对方防火墙或入侵检测系统监测到的概率,并避免了因工控设备开启禁 ping 导致主机探活失败的问题。虽然文献[16]在探活阶段通过向目标设备依次发送 5 个探测报文来应对工控设备禁 ping 的问题,但是探活过程产生的大量数据包将增加网络的传输和处理时延,使得其在单位时间内探活到的 IP 数量少于所提方法。

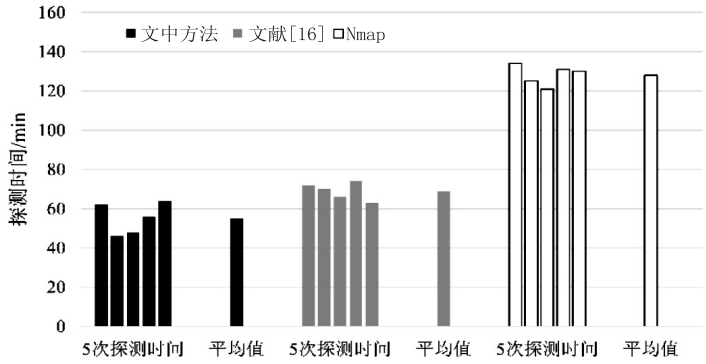

图 6 探测时间对比结果

接下来对资产探测时间进行对比分析,统计采用所提方法、文献[16]方法和 Nmap 探测工具完成指定网段内完整资产探测所需的时间,并进行多次重复探测,分别记录每次探测的时间,然后计算平均值,图 6 所示柱状图记录了每次完成探测的时间及其平均值。由图可以看出,所提方法完成完整资产探测所花费的时间最短。这是因为所提方法在端口探活阶段对探活数据包的处理采用异步方式,消除了全连接扫描和传统无状态连接扫描的连接建立时间和回复等待时间,提升了端口探活的效率。从具体数据上来看,所提方法与传统探测工具 Nmap 相比,在探测时间上缩短了约 50%;与文献[16]提出的方法相比,探测时间缩短

了约 20% 。通过对上述两组实验结果的分析,所提方法与文献[16]和传统资产探测工具 Nmap 相比,可以有效提升资产探测的速度和准确性。

4　结束语

为了提升工控设备资产探测的速度和准确性,提出了一种基于组合扫描的异步无状态工控设备资产探测方法。该方法主要对资产探测过程中的端口探活过程进行改进,通过异步处理方式提升端口探活的效率,以缩短资产探测时间,并采用组合扫描降低被对方入侵检测系统监测到的概率,确保端口探测的准确率。最后的测试实验结果证明了该方法的有效性。

参考文献:

[1] 杨　婷,张嘉元,黄在起,等. 工业控制系统安全综述[J]. 计算机研究与发展,2022,59(5):1035-1053.

[2] 刘蔚棣,郭乔进,产院东,等. 工业控制系统安全发展综述[J]. 信息化研究,2021,47(1):1-9.

[3] 国家计算机网络应急技术处理协调中心. 2021 年上半年我国互联网网络安全监测数据分析报告[R]. 北京:国家互联网应急中心,2021.

[4] 谛听安全分析团队. 2018 年工业控制网络安全态势白皮书[R/OL]. 2019. https://www. freebuf. com/articales/ics-articles/196647. html.

[5] 于新铭. 基于协议分析的工业互联网资产探测系统的设计与实现[D]. 北京:北京邮电大学,2020.

[6] 刘红星,杨红平,王民涛,等. 基于实物 ID 的资产普查与隐患排查系统研究[J]. 计算机技术与发展,2021,31(2):209-215.

[7] LYON G F. Nmap network scanning:the official Nmap project guide to network discovery and security scanning[M]. Sunnyvale:Nmap Project,2009.

[8] SIMON K,MOUCHA C,KELLER J. Contactless vulnerability analysis using Google and Shodan[J]. Journal of Universal Computer Science,2017,23(4):404-430.

[9] DURUMERIC Z, WUSTROW E, HALDERMAN J A. ZMap:fast internet-wide scanning and its security applications[C]//USENIX conference on security. San Jose:USENIX Association,2013:605-620.

[10] AL-ALAMI H,HADI A,BAHADILI H A. Vulnerability scanning of IoT devices in Jordan using Shodan[C]//International conference on the applications of information technology in developing renewable energy processes and systems. Amman:IEEE,2017:1-6.

[11] DURUMERIC Z,BAILEY M,HALDERMAN J A. An internet-wide view of internet-wide scanning[C]//USENIX security symposium. [s. l.]:USENIX Association,2014:65-78.

[12] 陈　卓. 基于无状态连接的工控系统扫描平台的设计与实现[D]. 北京:北京邮电大学,2018.

[13] 王欢欢,张冬梅,于　亮. 一种针对工控系统的网络探测方法[C]//中国通信学会青年工作委员会. 第十九届全国青年通信学术年会论文集. 北京:国防工业出版社,2014:26-30.

[14] 邓正宇. 基于 ERTEC 200P 的 PROFINET 工控网关的研制[D]. 绵阳:西南科技大学,2013.

[15] 周光凯. 联网工控设备巡查系统的设计与实现[D]. 哈尔滨:哈尔滨工业大学,2017.

[16] 于新铭,郭燕慧. 一种针对工控设备的资产探测方法[J]. 计算机工程与应用,2019,55(20):65-72.

[17] 侯美静. 基于智能爬行算法的网络扫描技术研究及实现[D]. 西安:西安电子科技大学,2018.

[18] COROTINSCHI G. Enabling IoT connectivity for Modbus networks by using IoT edge gateways[C]//2018 international conference on development and application systems. Romania:IEEE,2018:175-179.

[19] SI Qinghua,XU Haibo,XU Jun,et al. Application of Modbus protocol in the automatic safety device[J]. Advanced Materials Research,2015,1070-1072:765-769.