诱捕防御系统 TADS1.0

白皮书

杭州融至兴科技有限公司

二〇二二年九月

目录

【第 1 部分】 概述 1
1.1 背景介绍 1
1.1.1 网络安全现状 1
1.1.2 网络安全面临的挑战 1
1.1.3 传统防御方式不足之处 2
1.2 诱捕防御与传统防御技术 2
【第 2 部分】 诱捕防御系统 3
2.1 产品介绍 3
2.2 产品定位 3
2.3 技术原理 4
2.3.1 系统流量走向图 4
2.3.2 产品结构 4
2.3.3 系统应用架构 5
2.3.4 管理端要求 5
2.3.5 探针端要求 6
2.3.6 系统要求 6
2.4 系统特点 7
2.5 产品特点 9
2.6 产品功能 10
2.6.1 攻击捕捉 10
2.6.2 信息获取 10
2.6.3 黑盒测试 11
2.6.4 内建扫描 11
2.6.5 攻击源反制 13
2.6.6 集中分析 13

2.6.7 动态界面展示 13
2.6.8 账号资产 14
2.6.9 系统管理 14
2.7 应用场景 16
2.7.1 内网失陷场景 16
2.7.2 员工资产遗失场景 16
2.7.3 企业安全意识培训场景 16
2.8 界面展示 17
2.8.1 登录 17
2.8.2 首页 17
2.8.3 威胁感知 18
2.8.4 环境管理 21
2.8.5 威胁源管理 23
2.9 运维实施 25
2.9.1 系统测试 25
2.9.2 系统部署 25

【第 1 部分】 概述

1.1 背景介绍

互联网在给人类社会带来极大便利的同时，网络安全问题也逐渐成为网络空间亟须解决的核心问题。随着“震网""斯诺登""方程式"等事件的不断曝光，网络攻击复杂化、自动化、智能化的特点逐步显现，网络安全问题日益严峻。传统的网络防御技术大都是通过入侵检测、防火墙等方法来保护网络及系统的安全，属于被动防御手段，使得防御方在攻防过程中基本上处于劣势地位。

现在网络安全面临的一个大问题是缺乏对入侵者的了解。即谁正在攻击、攻击的目的是什么、如何攻击以及何时进行攻击等，而蜜罐为安全专家们提供一个研究各种攻击的平台。采取主动的方式，用定制好的特征吸引和诱骗攻击者，将攻击从网络中比较重要的机器上转移开，同时在黑客攻击蜜罐期间对其行为和过程进行深入的分析和研究，从而发现新型攻击，检索新型黑客工具，了解黑客和黑客团体的背景、目的、活动规律等。

1.1.1网络安全现状

近年来，计算机系统漏洞的发展速度加快，网络安全状况不容乐观。目前，网络攻击者技术精良，手段灵活，攻击对象范围扩大。尽管当前的网络安全技术与过去相比有了长足的进步，但总体形势不容乐观。同时，互联网的无政府、无组织状态是非常危险的，导致网络攻击快速增长，网络安全事件大量涌现，并从普通个人到上市公司，从军队到国家都受到不同程度的影响。网络安全在国家安全中的地位越来越重要，网络安全已被提升到国家安全的战略高度。

1.1.2网络安全面临的挑战

网络系统漏洞的存在是网络中的一个突出问题，其影响着网络的运行和发展。如果网络出现漏洞，就会为黑客入侵提供便利，造成信息和数据泄露，严重影响网络系统的安全。

互联网中的数据信息非常多，因此互联网环境具有一定的自由、开放的特点。正是由于互联网信息量大，病毒攻击等网络安全问题会加剧数据安全风险，从而出现信息破坏、泄露等问题。

在网络安全中，由恶意攻击或操作不当引起的安全问题较为常见。互联网在各个行业都发挥着重要作用，但是，由于部分用户操作水平有限或不了解网络规范，为不法分子对网络安全进行恶意攻击甚至给他人造成经济损失提供了机会。这种人为操作导致的安全问题，也是当前互联网安全问题中的突出问题。

1.1.3传统防御方式不足之处

1） 传统的被动安全防御思维具有一定的局限性

一个业务系统运行过程中，有可能会面临非法攻击的风险，也有可能不会遭遇非法攻击，正常运行。但由于安全风险的客观存在，我们无法预知业务系统何时会遭遇非法攻击，即：设想风险分析，被动防御未知风险。

2） 风险无法预知

由于安全风险的手段越来越多，比如：系统病毒、木马种类的增加，那对业务系统的防御手段或设备就也要增加，否则，之前的防御手段有可能就会被绕开，从而造成对业务系统的非法攻击。这就会给系统带来巨大风险，于是，传统的被动防御思维下，最大的问题还是不断增长的安全投入。

3） 成本大量投入

在人工智能、大数据信息化时代，各种商业应用都离不开网络、甚至很多都搬到了网络上，商业应用的安全变得越来越重要，如果还采用传统的被动安全防御的思维，商业应用的安全投入将变得越来越庞大。尤其对于物联网应用来讲，海量终端的管理，可能面临的更多安全风险，被动防御将无法保障他们的安全。

1.2 诱捕防御与传统防御技术

诱捕防御与传统防御技术的一个根本区别是：传统防御技术专注于攻击者的行为，目的是对它们进行检测和预防；而诱捕防御着眼于攻击者的认知，目的是干扰他们的认知并诱导攻击者采取有利于目标系统的决策。

诱捕防御与传统防御技术的另一个区别是：传统防御侧重于信息隐藏，而诱捕防御会采取隐藏真实信息和披露虚假信息相结合的方式来误导攻击者，使其在观察阶段产生认知偏差，从而保护关键目标。

【第 2 部分】 诱捕防御系统

2.1 产品介绍

诱捕防御系统（TADS）是由蜜罐演进而来的一种主动防御机制。防御者通过在己方网络信息系统中布设骗局，干扰、误导攻击者对己方网络信息系统的感知与判断，诱使攻击者做出对防御方有利的决策和动作，从而达到发现、延迟或阻断攻击者活动的目的。

诱捕防御系统是杭州融至兴科技有限公司开发的一款集蜜罐、扫描攻击源、自查漏洞为一体的软件产品。从内网失陷检测、外网威胁感知、威胁情报生产、扫描攻击源 IP、反制攻击源等场景出发，为用户提供可独立操作且实用的功能，通过安全、敏捷、可靠的中低交互蜜罐增加用户在失陷感知和威胁情报领域的能力。提供可高度自定义的蜜饵能力、一键部署、跨平台多架构、国产操作系统和 CPU 支持、极低的性能要求等多项特性，帮助用户降低运维成本，提升运营效率。

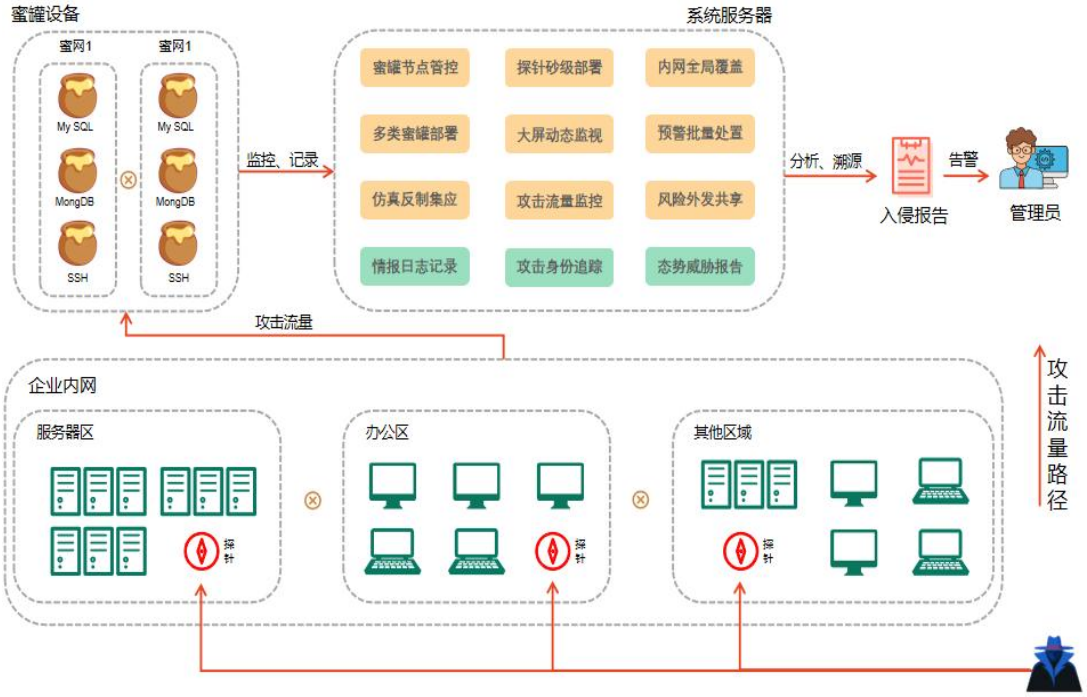
2.2 产品定位

【诱捕防御系统】

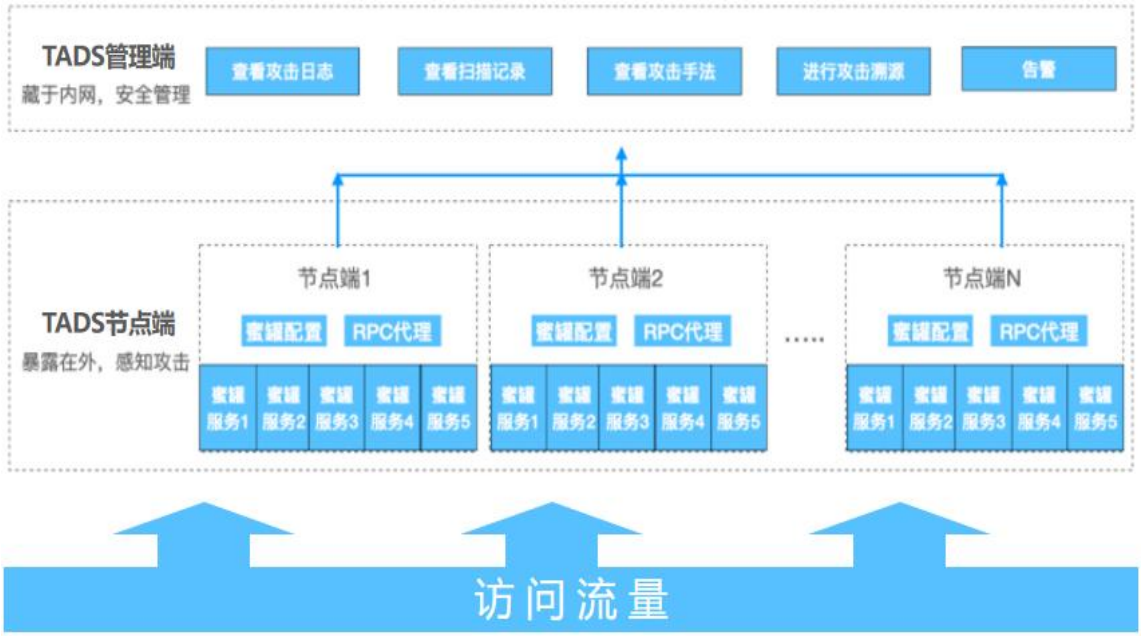
1) 采用主动监听方式，通过模拟多种虚假主机和服务来主动引诱攻击者现身，记录所有对虚假 IT 资产的访问和入侵行为，实现检测能力的前置和延伸。
2) “主动威胁引流、业务仿真、攻击者画像”，帮助用户解决攻易守难的困境，化被动防御为主动防御。
3) 本系统为一个组织的网络安全提供保护，包括攻击检测，预警，联动处理及取证。

2.3 技术原理

2.3.1系统流量走向图

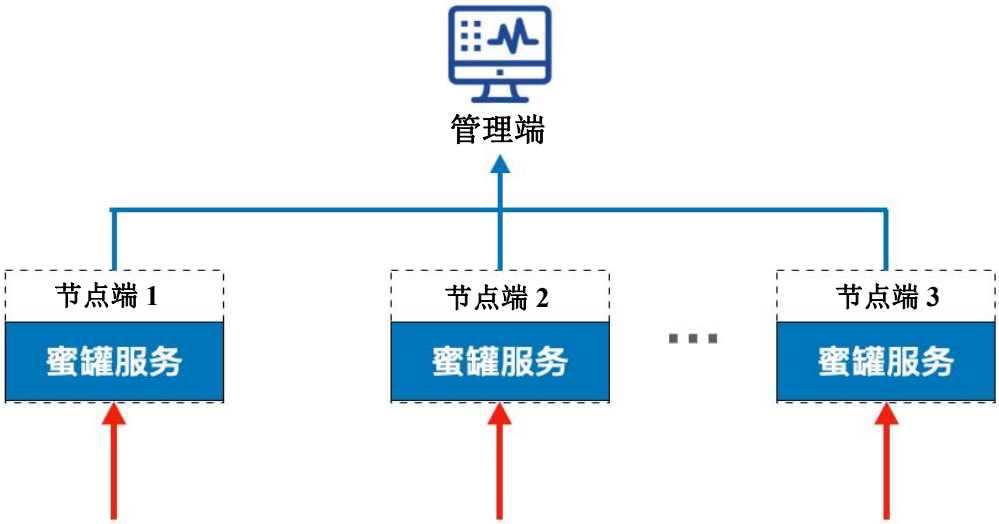


2.3.2产品结构



2.3.3 系统应用架构

诱捕防御系统采用B/S架构，系统由管理端和节点端组成，管理端用来生成和管理节点端，并接收、分析和展示节点端回传的数据，节点端接受管理端的控制并负责构建蜜罐服务。管理端只用于数据的分析和展示，节点端建设虚拟沙箱，最后由管理端来承受攻击。



TADS 系统由管理端（server）和节点端（client）组成：

1） **管理端：**

生成和管理节点端，并接收、分析和展示节点端回传的数据，管理端必须部署在安全区。

2） **节点端：**

接受管理端的控制并负责构建蜜罐服务。

2.3.4 管理端要求

a. 软硬件一体机；
b. 配置≥2 颗 Intel 处理器，每颗核数≥8 核，线程数≥16，主频≥2.1GHz；
c. 配置≥1 块 4T 企业级 SATA 硬盘；
d. 配置≥64G 内存；
e. 配置≥2 个万兆网口，含多模光模块；
f. 配置蜜罐数量≥32 个；

2.3.5探针端要求

a. 蜜网攻防一体机探针部署方式支持软硬件一体机和安装在现有服务器上两种模式；
b. 每台蜜网攻防一体机配置软件探针≥100 个；
c. 每台蜜网攻防一体机配置硬件探针 2 个，硬件配置为：硬盘≥64G，业务口≥1 个；
d. 探针支持自定义监听 1-65535 的任意端口；
e. 探针支持同时感知到 TCP 协议和和 UDP 协议的探测；
f. 探针感知探测后，支持查询完整的端口探测过程和探测中发送的数据；
g. 支持感知 Ping 扫描，被 Ping 后能够记录下 Ping 扫描源；
h. 可在物理机、虚拟机、甚至 docker 容器内部署探针；

2.3.6系统要求

a. 配置仿真沙箱种类 40≥种；
b. 支持伪装 SSH、Telnet、FTP、TFTP、VNC 等服务。收到攻击后，SSH 和 Telnet 可以查询完整的连接建立与断开记录、用户密码登录记录、命令执行记录、文件遗留记录等；
c. 支持伪装 WordPress 仿真登录、通用 OA 仿真登录、Mysql、Redis、ESXi 系统、IIS 服务器、群晖 NAS 等页面。当诱捕防御系统数据沙箱受到攻击时，记录完整 Web 攻击事件，包括攻击源使用的账号密码、请求头等信息；
d. 对接精准的云端的威胁情报，可对攻击行为进行更准的研判，帮助用户更科学的进行处置；

2.4 系统特点

1） 数据价值

IDS和防火墙等网络安全工具的价值在于保护主机安全，对于保护的效果来说，这些工具是高效的。然而，他们的保护措施本身对数据的使用率实际是很低的，因为无论是IDS、防火墙还是其他网络安全工具，都需要对大量的网络数据包进行监控，而这些数据包中绝大多数都是安全包，只有少量的包含有攻击信息。而蜜罐则不同，由于蜜罐不提供真实的网络服务，因此对蜜罐的访问本身就可以认为是一种攻击行为，所以，从原理上说，蜜罐收到的所有数据都是攻击数据，蜜罐的数据价值显然比其他网络安全工具高得多。

2） 资源占用率低

目前，大多数安全设备提供的安全性能都是以高昂的成本作为代价换来的。IDS（入侵检测系统）需要强大的主机性能以实时监控网络的每个时间并对其中的各种数据包进行匹配，而防火墙则以其固有硬件为基础对通过网关的包进行过滤以达到防护效果。蜜罐没有那么多的限制，特别对于产品型蜜罐，由于其虚拟性并不需要硬件基础，因此仅需要很少的资源就能搭建，并且由于蜜罐本身并不提供实际服务，蜜罐的数据量与IDS防火墙等安全工具相比也少很多。

3） 简捷性

蜜罐的核心思想在于虚拟主机并诱骗黑客攻击，对于大多数蜜罐，特别是产品型蜜罐而言，是没有特殊算法要求的，蜜罐所涉及到的算法通常都是TCP/IP等实际的协议算法，在RFC文档中都有详细的规定，无需重新设计，而蜜罐的部署也非常简单，只要将蜜罐部署在网络的某个区域，定期检查蜜罐产生的数据即可。

4） 回报率高

蜜罐并非真实系统，对外界不提供任何有价值的服务，因此对蜜罐的访问总是“不合法”的，访问蜜罐的行为本身就可以被认为攻击行为，而事实上，由于攻击的步骤中大多都有扫描、系统探测等基本步骤，因此只要存在攻击，蜜罐主

机大部分情况都能产生相关记录，因此蜜罐主机的回报率相较其他安全工具要高很多。

5） 主动防御

在每个企业，几乎每分钟都在发生这样的场景：潜伏在互联网角落中的攻击者发起一次攻击探测，防守方业务不存在安全漏洞，IDS 告警后事情就不了了之。应用诱捕型产品后，转换为主动防御思路： 探针响应了攻击探测，诱骗攻击者认为存在漏洞，进而发送了更多指令，包括从远端地址下载木马程序，而这一切不仅被完整记录下来，还可以转化为威胁情报供给传统检测设备，用于在未来的某个时刻，准确检测主机失陷。

2.5 产品特点

1） 使用简单

不需要改变现有的网络部署方式，用户只需要将诱捕系统合理放置在网络中并监测沙箱告警信息；

2） 占用资源少

系统仅记录和响应尝试与自己建立连接的行为，不会被庞大的网络流量淹没，同时，它对硬件要求较低，不需要昂贵的专用硬件设备；

3） 数据价值高

只收集异常访问行为信息，收集到的数据具有较高的研究价值，通过研究分析，可以较完整地还原攻击者的攻击方法、意图和工具。

4） 告警准确

诱捕防御系统作为正常业务的 "影子" 混淆在网络中，每次触碰都可以视为威胁行为。对于本产品来说，几乎不存在正常请求，即使有也是探测行为。

5） 检测信息丰富

不同于其它检测型安全产品，本产品可以模拟业务服务甚至对攻击的响应，完整获取整个交互的所有内容，最大深度的获得攻击者探测行为之后的 N 个步骤，可检测点更多，信息量更大。

6） 降低成本

本产品具备系统内部扫描任务，无需额外请团队对企业内网进行渗透测试，可以直观获取内部资产薄弱面。降低企业运维成本的同时又能提升企业效益。

7） 路径溯源

产品可以实现主机侧 Checklist 的自动全面化检测，根据检测结果自动数据聚合，进行黑客攻击路径溯源。扫描结果会告知风险级别、风险时间、风险事件、文件位置、事件详情等。

2.6 产品功能

2.6.1攻击捕捉

1） 攻击源 IP 画像

对于本系统而言，当用户的情报全部开放给所有的情报，系统会自动生成生成攻击源的 IP 画像，用于做更多的 IP 画像分析，完成诱捕防御系统的生产和使用。除了通过整合情报，提供失陷情报以外，我们还提供本地威胁检测模块的攻击行为检测出次数综合检测标签与 IP 相关信息。

2） 捕捉系统沙箱信息

观察本地部署的诱饵、沙箱、节点情况，是否出现失陷状态，实时掌握主动权，主动防御周围黑暗信息面，支持查看部署数量世界，内容及存在情况等信息。

2.6.2信息获取

攻击者入侵后，随时了解针对服务器发动的最新的攻击和漏洞。通过窃听黑客之间的联系，收集黑客所用的种种工具，并且掌握他们的社交网络信息。

1） 失陷感知

当本地部署的资产信息被攻击源攻陷够，系统自动获取相关信息，包括被攻击后的沙箱情况。

a. 被攻击沙箱/蜜饵名称
b. 被攻击数量
c. 被攻击节点名称
d. 攻击来源 IP 和地理位置
e. 威胁情报
f. 最后一次攻击时间
g. 攻击时间
h. 攻击数据长度
i. 攻击详情

2） 动态告警

为保证能够及时的发现核心指标是否存在异常，需要对核心指标进行检测监控，运维人员依托自己运维的经验，配置一定的指标阈值。每一类指标的阈值，首先运维专家需要根据对应的业务情况去配置自认为合理的阈值。不同运维人员配置的阈值存在着差别。

a. 支持短信
b. 支持邮件
c. 支持系统界面告警
d. 支持大屏轮播

2.6.3 黑盒测试

1） 资产自查测试

企业网络管理者对企业内部的网络脆弱性不了解，一些安全产品仅可以抵御外部攻击，无法对内部资产的安全性做一些测试，企业会花钱去找安全团队进行渗透测试。设定模拟黑盒测试功能，根据客户需求定期使用可以对企业内部的安全环境进行直观的分析，什么服务器存在什么漏洞，了解企业自身存在的部分设备资产问题。

根据客户需求定期对企业内部资产进行模拟黑盒测试，发现企业内部资产存在漏洞后可通过 syslog、邮件、Webhook 进行信息告警

2） 攻击源 Web 扫描

当蜜罐受到攻击后，无法得知攻击源的信息，造成被动防御的状况。使用模拟黑盒测试功能，能及时获取的攻击源信息进行模拟渗透测试，收集到黑客方的漏洞并进行利用。通过信息收集平台获取攻击源关联的互联网资产，构建基础资产信息库。协助甲方安全团队或者渗透人员有效侦查和检索资产，发现存在的薄弱点和面。

2.6.4 内建扫描

诱捕防御系统其中涵盖了“系统内建扫描任务”功能。可以帮助用户方的安全应急响应人员对Linux主机排查时提供便利。

企业内部资产被攻破或是运维人员误操作导致文件信息被修改，可下发系统内扫描任务，可获取主机信息、alias、文件类安全检测、各用户历史操作类、进程类安全检测、网络类安全检测、后门类检测、账户类安全检测、日志类安全检测、安全配置类安全检测、Rootkit分析、WebShell类文件扫描等信息，实现主机侧Checklist的自动全面化检测，根据检测结果自动数据聚合，进行黑客攻击路径溯源。扫描结果会告知风险级别、风险时间、风险事件、文件位置、事件详情等，及时准确恢复数据信息。

在攻击防御中，挖掘攻击者身份，通过资产面，回溯等判断用于攻击者身份，提供适时的防卫需求。当攻击者扫描、攻击或被退回正常对沙箱攻击时，本系统提供的攻击包括但不限于：通过现有工具，在合理范围内攻击者进行信息提取、溯源等必要的攻击防御信息采集源手段。

1） web 型蜜罐溯源

系统内部所有的网页诱饵、沙箱，包括自定义沙箱，都可以在这种情况下进行追踪源。对扫描器、webshell 管理器、java 反序列化显示信息。

a. 获取架构
b. 获取微信账号
c. 获取 QQ 账号
d. 获取 QQ 音乐账号
e. 获取百度云账号
f. 获取浏览器记录
g. 获取 history
h. 获取 whoami 等信息

2） Java 远程调用蜜罐溯源

Java 调用假据点沙箱是本系统远程保存的一种服务。当攻击者使用 java 反序列化工具对用户 Java 远程调用该据点进行攻击时，由于系统内部设定构建了 Java 反序列化工具的漏洞利用方式。

a. 获取架构
b. 获取微信账号
c. 获取 QQ 账号

d. 获取 QQ 音乐账号
e. 获取百度云账号
f. 获取浏览器记录
g. 获取 history
h. 获取 whoami 等信息

2.6.5攻击源反制

在网络世界中存在攻防不对等的情况，防守方对隐藏在暗的攻击者的信息是一无所知的，通过信息收集平台可最大化的收集攻击者的信息，再对接反制平台对攻击者进行定向打击。支持通过反制平台对攻击源进行反制，主要包括：黑客地址分析、子域名收集、系统漏洞以及 Web 漏洞的扫描。

2.6.6集中分析

1） 系统运行

针对系统的运行，提供节点状态和蜜罐状态可视化查看能力。针对管理端的运行情况，提供了状态栏进行查看。

2） 攻击情况

从扫描/测试/高试测试的链接测试结果，在攻击者的测试中进行的测试，进行更好的威胁发现。从攻击源 IP 的部署趋势、服务的趋势攻击以及部署的趋势，进行可视化展示，更好地了解威胁的来源，迅速制定对策和反应。

3） 部署信息

观察本地部署的诱饵、沙箱、节点情况，是否出现失陷状态，实时掌握主动权，主动防御周围黑暗信息面，支持查看部署数量世界，内容及存在情况等信息。

2.6.7动态界面展示

多源适配，可视化建模，配合强大灵活的数据分析能力，轻松实现秒级数据响应，实时发现异常。数据监控，安全预警，异常发现，多种实时场景，灵活适配。

2.6.8账号资产

收集所有被用来攻击的账号密码，通过配置可跟踪企业丢失进行有效监控。通过高级设置监控策略，协助企业进行失账监控，随时建议输入企业邮箱、企业域名、员工姓名等信息，监控泄露日志。

a. 收集账号、密码

b. 获取攻击源登录信息

c. 分析整理，数据整合

d. 依据使用频繁程度进行排名

2.6.9系统管理

1） 诱饵

诱饵一般是一个文件或数据形式，也是诱使攻击者打开或下载。当攻击者看到各类数据文件时，往往难以忍住下载的欲望，这样就落入了本系统部署的的陷阱。当本系统发现这里的文件有被打开过的痕迹或攻击者跟随诱饵文件内容进行某种操作时，就可以追溯来源，发现被攻陷的设备。

支持进一步改造，在 Word 文档、PDF 文档中植入一个隐蔽的链接，当攻击者打开这个文件时，链接可以被自动触发，系统借机获取攻击者的真实网络地址、浏览器指纹等信息，从而直接溯源定位攻击者真实身份。

2） 沙箱

在使用又不防御系统的时候，往往会在一个网络里放很多诱饵，以增加攻击者踩中的几率。简单的说：“沙箱就是多个诱饵存放在一个小型的箱子中，形成了这种沙箱的说法”。沙箱需要和业务强相关，攻击者在试图攻破我们的系统时，为了拿到自己想要的东西（业务数据、文件等），往往会重点攻击和业务相关的节点。因此，我们可以参照真实的业务环境，在攻击者的必经之路上放罐，给攻击者提供横向移动的空间和更丰富的入侵接口。这样，当攻击者踩过一连串诱饵或节点的时候，我们就能轻松地看到攻击者的手法和习性。

3） 节点

监测未使用的端口和 IP 段的情况，并对试图进行交互的流量重定向。节点支持快速部署，并且对业务不产生影响。

4） 告警

在完成系统安全状况分析并确定系统所存在的问题之外。在某些情况下还要采取一些行动。诱饵、沙箱被攻陷时，系统自定义告警信息，支持随时随地告警处理，设定相关阈值，系统自动识别入侵信息，检测到对系统的闯入。

2.7 应用场景

2.7.1 内网失陷场景

由于设备外带、USB 设备接入、员工下载非法软件、客户端漏洞、VPN 账号失窃、恶意员工等众多原因导致内部办公或内部服务器失陷，攻击者和蠕虫木马在内网肆无忌惮的横向移动。

1） **解决方案：**

该场景是蜜罐在企业环境最常见的使用方法，用来捕捉内网已经实现、勒索软件和恶意行为，重点在于敏捷准确，具体可细分为内部办公场景和内部服务器场景，

a. 内部办公场景：蜜罐被部署在企业内部服务器区，用于感知内网失陷主机、勒索软件扫描或恶意员工内网刺探行为，常见模版可设置为监听 tcp/135、139、445 和 3389 等端口。
b. 内部服务器场景：蜜罐被部署在企业内部服务器区，用于感知内网失陷和横向移动，常见模版可以设置为模拟 Web、MySQL、Redis、Elasticsearch、SSH、Telnet 等服务。

2.7.2 员工资产遗失场景

员工账号密码资产遗失对于企业来说都是致命隐患，安全团队如何感知是当下一个空白。

1） **解决方案：**

企业可将常见的对外服务器例如：vpn.company.com.cn 或 oa.company.com.cn 替换成蜜罐，通过监控试图登录的账号判断是否为内部员工账号，并实时通知安全团队和该员工，敦促其尽快修改密码。

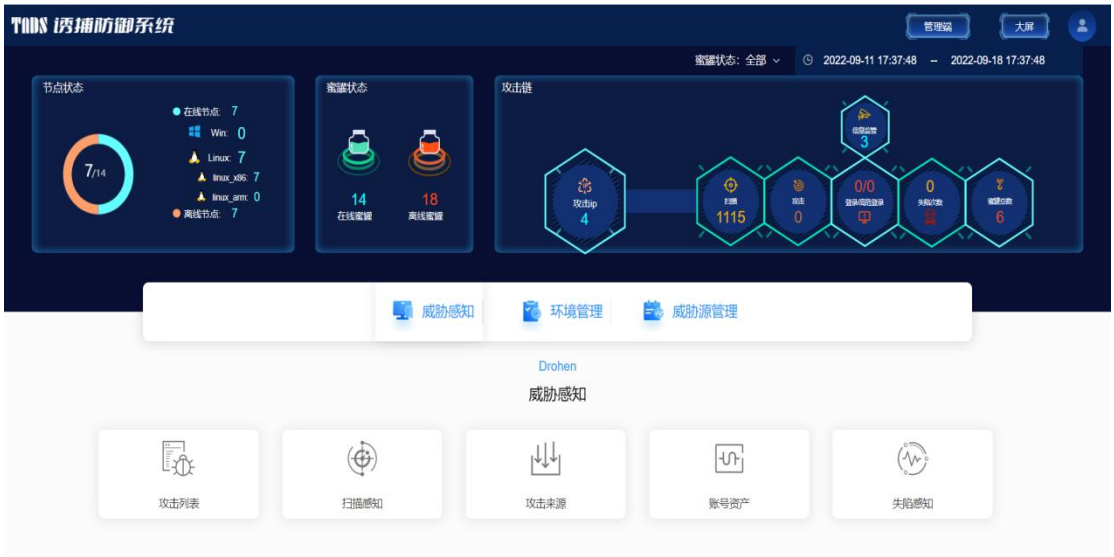
2.7.3 企业安全意识培训场景

在企业安全工作中，员工安全意识问题常常被忽略。使用开源的钓鱼邮件工具和 Web 蜜罐自定义能力，可以快速、低成本的组装企业安全意识培训平台。

2.8 界面展示

2.8.1登录

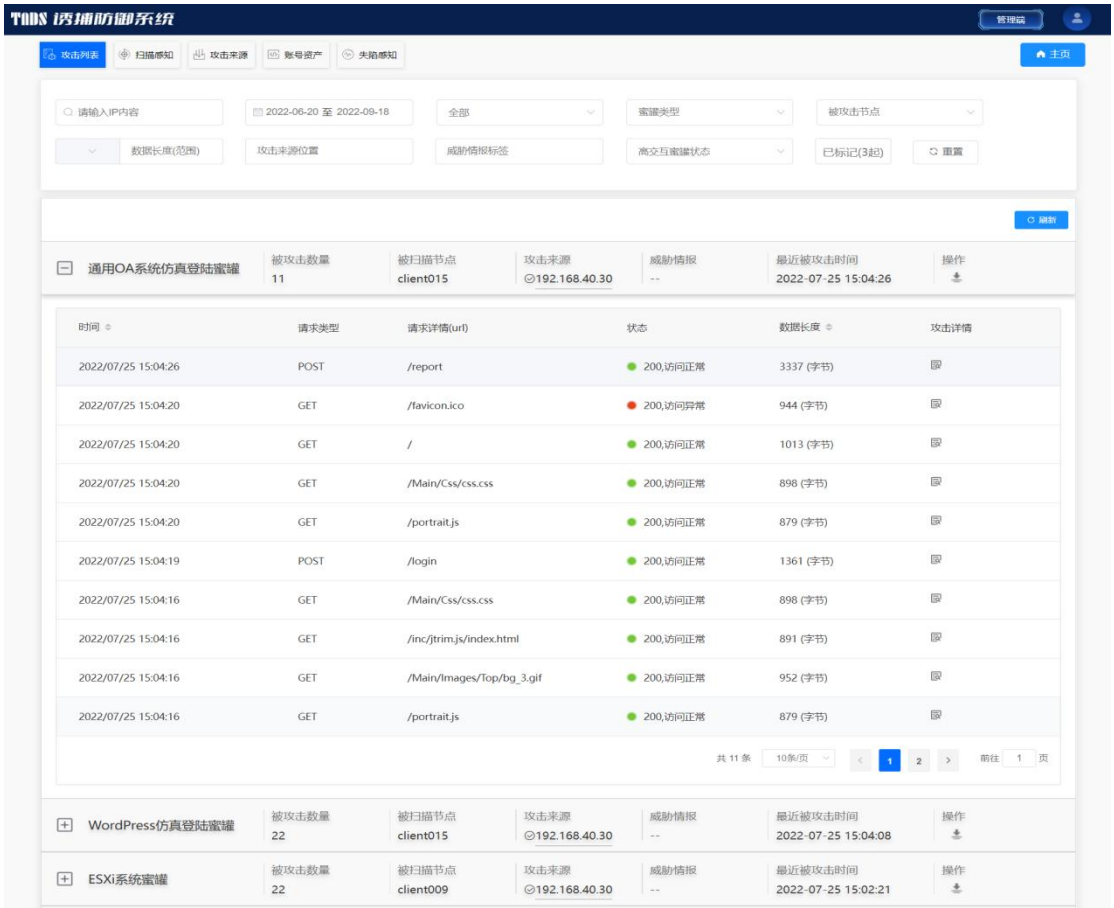
2.8.2首页



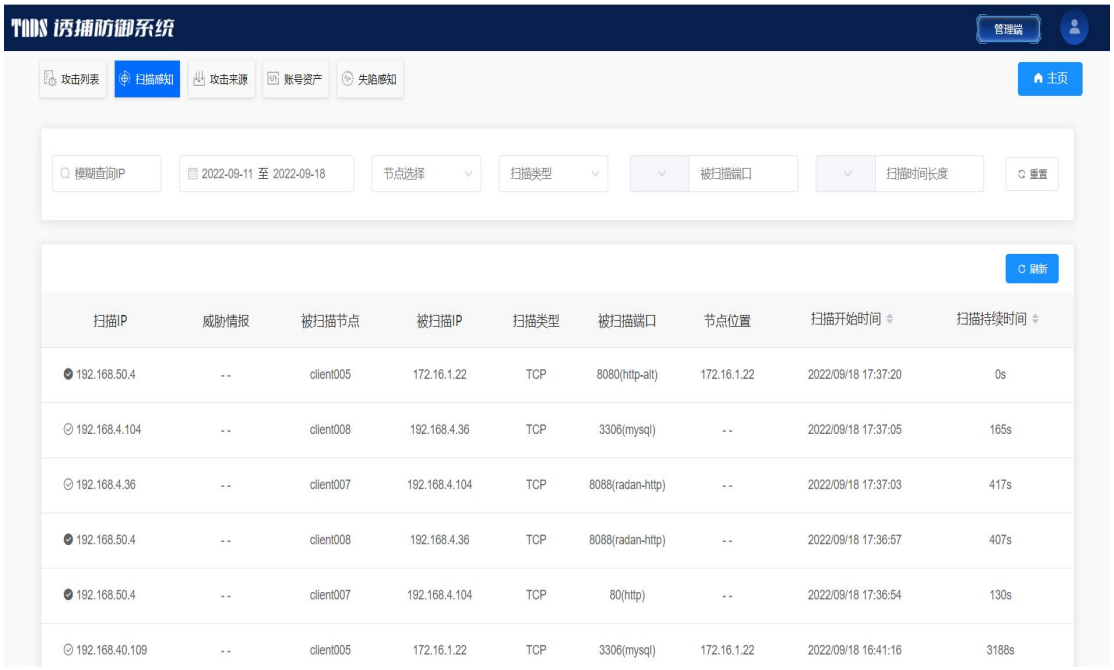
2.8.3威胁感知

1） 大屏

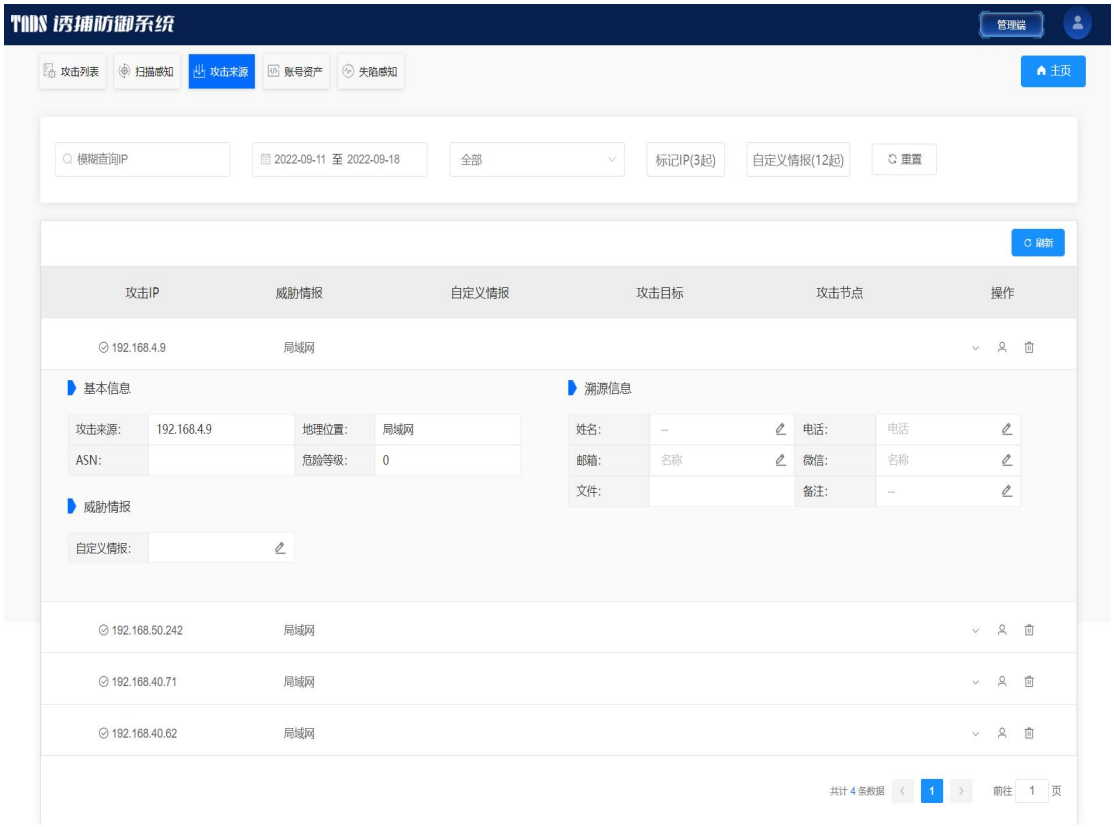
2） 攻击列表



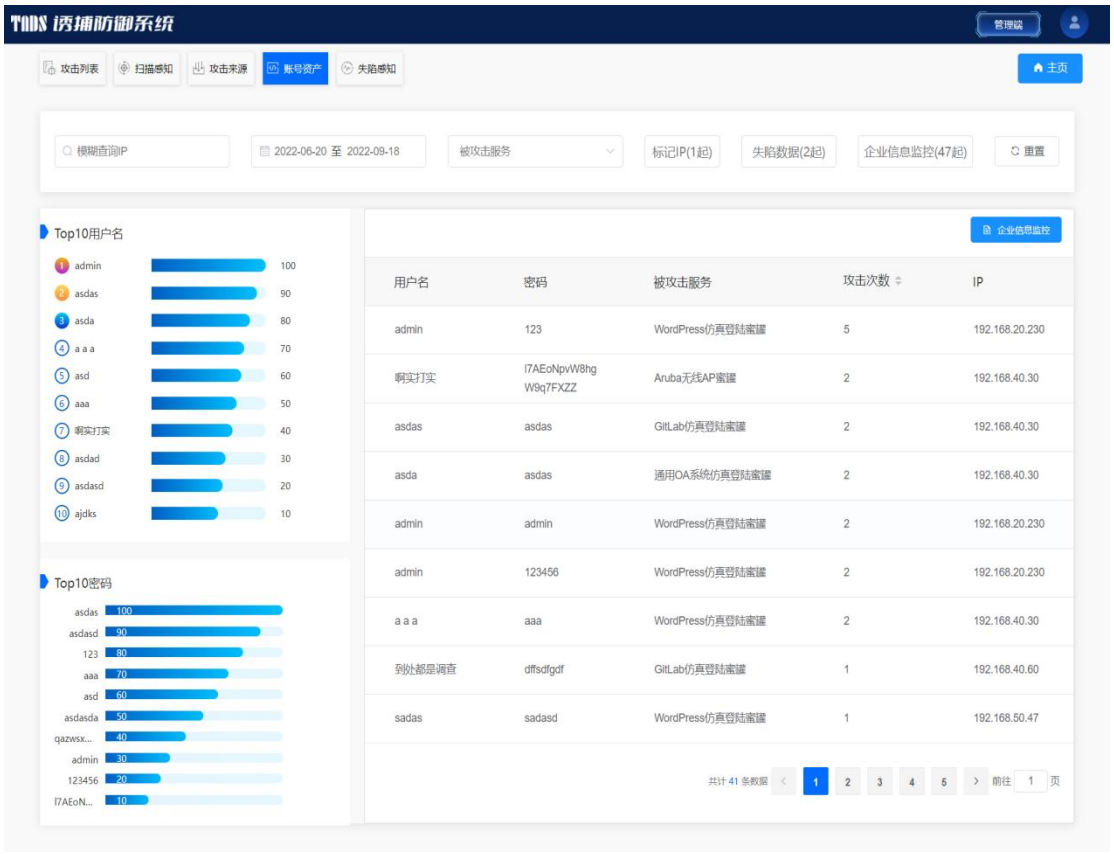
3） 扫描感知


TADS 诱捕防御系统
管理端
攻击列表
扫描感知
攻击来源
账号资产
失陷感知
主页
模糊查询IP
2022-09-11 至 2022-09-18
节点选择
扫描类型
被扫描端口
扫描时间长度
重置
刷新
扫描IP 威胁情报 被扫描节点 被扫描IP 扫描类型 被扫描端口 节点位置 扫描开始时间 扫描持续时间
192.168.50.4 -- client005 172.16.1.22 TCP 8080(http-alt) 172.16.1.22 2022/09/18 17:37:20 0s
192.168.4.104 -- client008 192.168.4.36 TCP 3306(mysql) -- 2022/09/18 17:37:05 165s
192.168.4.36 -- client007 192.168.4.104 TCP 8088(radan-http) -- 2022/09/18 17:37:03 417s
192.168.50.4 -- client008 192.168.4.36 TCP 8088(radan-http) -- 2022/09/18 17:36:57 407s
192.168.50.4 -- client007 192.168.4.104 TCP 80(http) -- 2022/09/18 17:36:54 130s
192.168.40.109 -- client005 172.16.1.22 TCP 3306(mysql) 172.16.1.22 2022/09/18 16:41:16 3188s

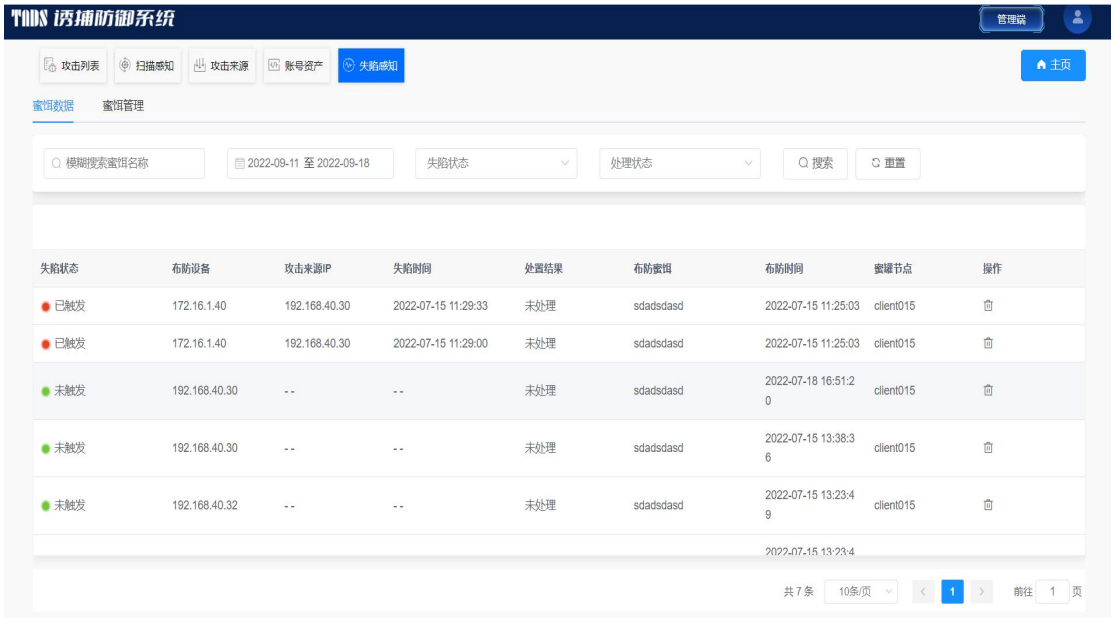
4） 攻击来源


TADS 诱捕防御系统
管理端
攻击列表
扫描感知
攻击来源
账号资产
失陷感知
主页
模糊查询IP
2022-09-11 至 2022-09-18
全部
标记IP(3起)
自定义情报(12起)
重置
刷新
攻击IP 威胁情报 自定义情报 攻击目标 攻击节点 操作
192.168.4.9 局域网
基本信息
攻击来源: 192.168.4.9
地理位置: 局域网
ASN:
危险等级: 0
溯源信息
姓名: --
电话: 电话
邮箱: 名称
微信: 名称
文件:
备注: --
威胁情报
自定义情报:
192.168.50.242 局域网
192.168.40.71 局域网
192.168.40.62 局域网
共计 4 条数据
1
前往 1 页

5） 账号资产

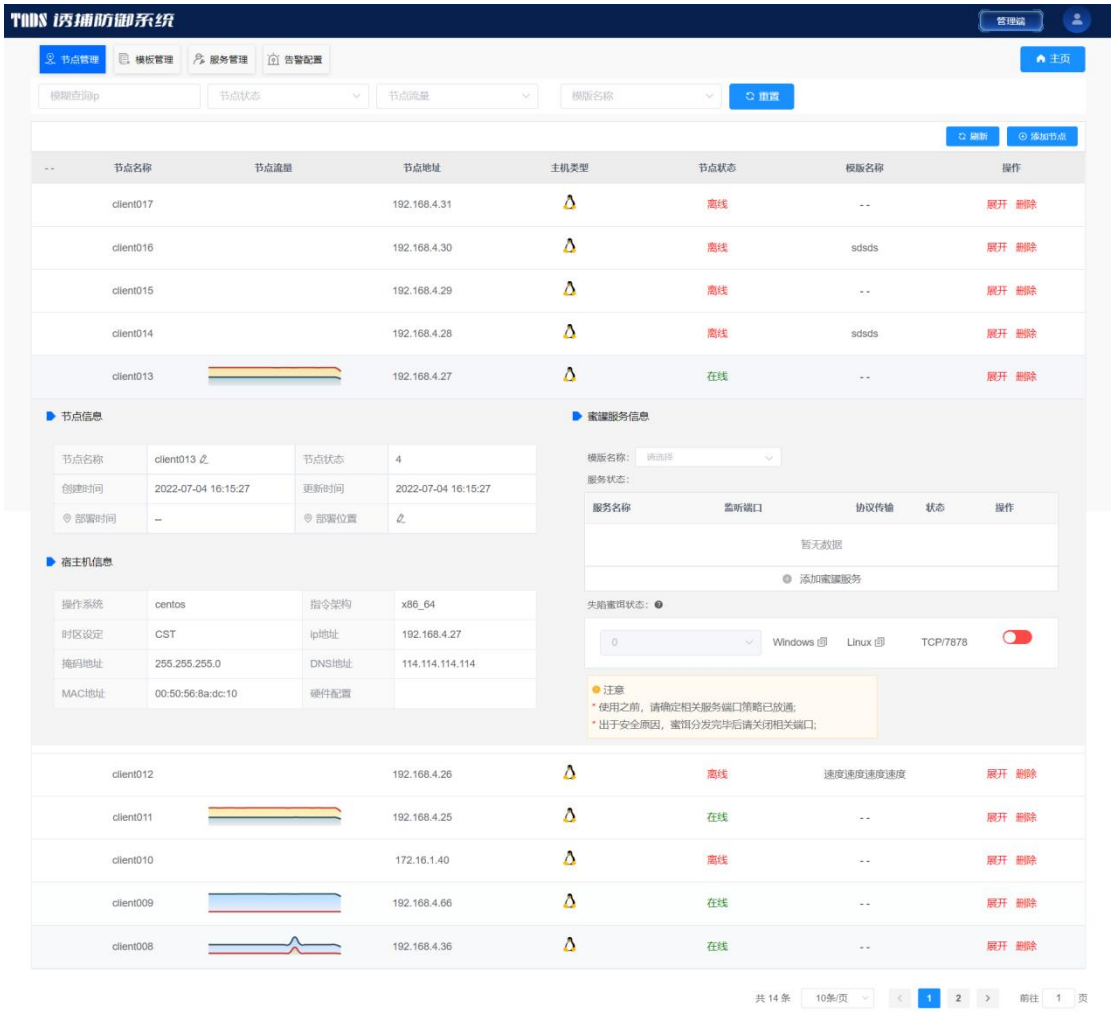

TADS 诱捕防御系统
管理端
攻击列表
扫描感知
攻击来源
账号资产
失陷感知
主页
模糊查询IP
2022-06-20 至 2022-09-18
被攻击服务
标记IP(1起)
失陷数据(2起)
企业信息监控(47起)
重置
Top10用户名
admin 100
asdas 90
asda 80
a a a 70
asd 60
aaa 50
啊实打实 40
asdad 30
asdasd 20
ajdks 10
Top10密码
asdas 100
asdasd 90
123 80
aaa 70
asd 60
asdasda 50
qazwsx... 40
admin 30
123456 20
I7AEoN... 10
企业信息监控
用户名 密码 被攻击服务 攻击次数 IP
admin 123 WordPress仿真登陆蜜罐 5 192.168.20.230
啊实打实 I7AEoNpvW8hg W9q7FXZZ Aruba无线AP蜜罐 2 192.168.40.30
asdas asdas GitLab仿真登陆蜜罐 2 192.168.40.30
asda asdas 通用OA系统仿真登陆蜜罐 2 192.168.40.30
admin admin WordPress仿真登陆蜜罐 2 192.168.20.230
admin 123456 WordPress仿真登陆蜜罐 2 192.168.20.230
a a a aaa WordPress仿真登陆蜜罐 2 192.168.40.30
到处都是调查 dffsdfgdf GitLab仿真登陆蜜罐 1 192.168.40.60
sadas sadasd WordPress仿真登陆蜜罐 1 192.168.50.47
共计 41 条数据
前往 1 页

6） 失陷感知

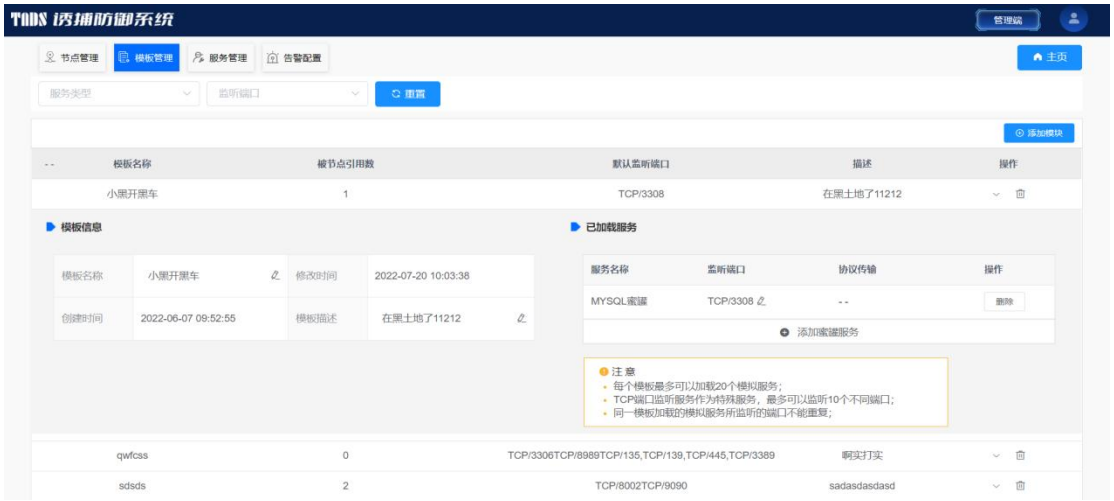

TADS 诱捕防御系统
管理端
攻击列表
扫描感知
攻击来源
账号资产
失陷感知
主页
蜜饵数据
蜜饵管理
模糊搜索蜜饵名称
2022-09-11 至 2022-09-18
失陷状态
处理状态
搜索
重置
失陷状态 布防设备 攻击来源IP 失陷时间 处置结果 布防蜜饵 布防时间 蜜罐节点 操作
已触发 172.16.1.40 192.168.40.30 2022-07-15 11:29:33 未处理 sdadsdasd 2022-07-15 11:25:03 client015
已触发 172.16.1.40 192.168.40.30 2022-07-15 11:29:00 未处理 sdadsdasd 2022-07-15 11:25:03 client015
未触发 192.168.40.30 -- -- 未处理 sdadsdasd 2022-07-18 16:51:20 client015
未触发 192.168.40.30 -- -- 未处理 sdadsdasd 2022-07-15 13:38:36 client015
未触发 192.168.40.32 -- -- 未处理 sdadsdasd 2022-07-15 13:23:49 client015
共 7 条
10条/页
前往 1 页

2.8.4环境管理

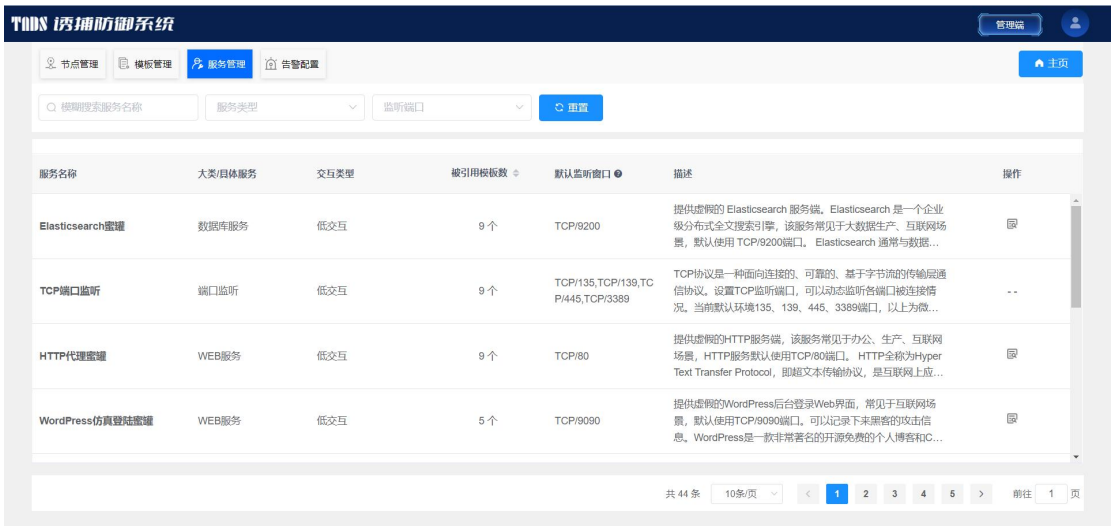
1） 节点管理



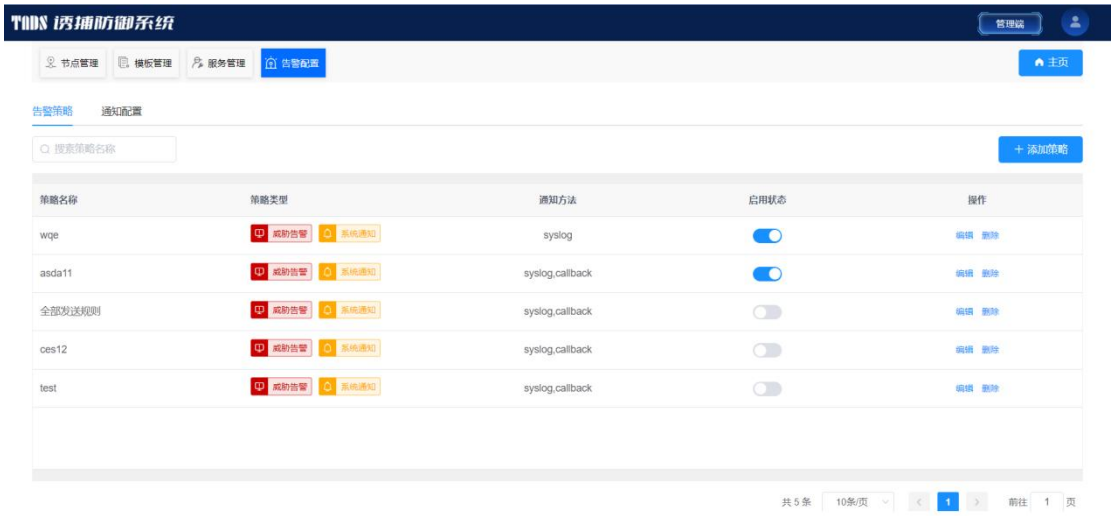
2） 模板管理

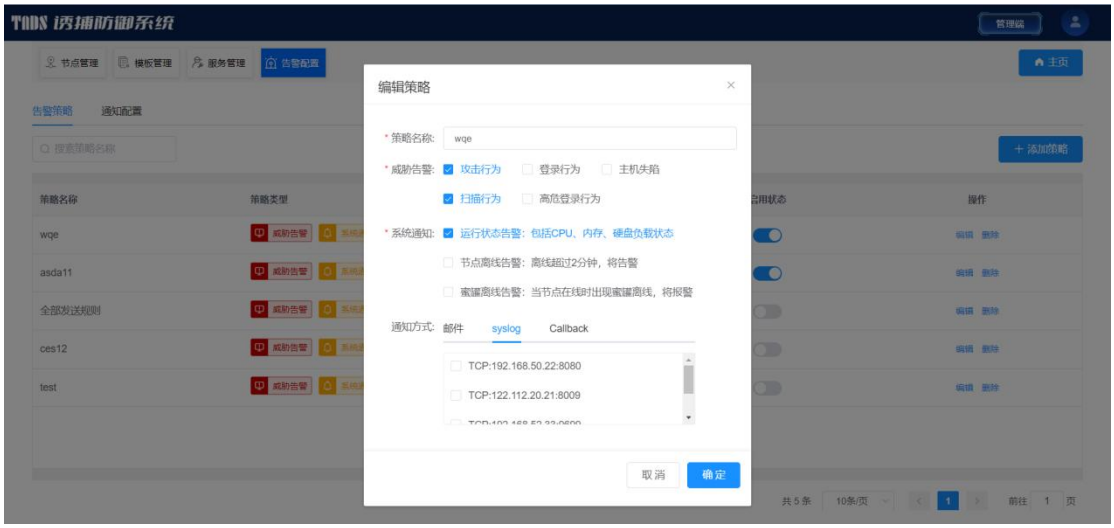


3） 服务管理


TADS 诱捕防御系统
管理端
节点管理
模板管理
服务管理
告警配置
主页
模糊搜索服务名称
服务类型
监听端口
重置
服务名称
大类/具体服务
交互类型
被引用模板数
默认监听窗口
描述
操作
Elasticsearch蜜罐
数据库服务
低交互
9 个
TCP/9200
提供虚假的 Elasticsearch 服务端。Elasticsearch 是一个企业级分布式全文搜索引擎，该服务常见于大数据生产、互联网场景，默认使用 TCP/9200端口。 Elasticsearch 通常与数据…
TCP端口监听
端口监听
低交互
9 个
TCP/135,TCP/139,TCP/445,TCP/3389
TCP协议是一种面向连接的、可靠的、基于字节流的传输层通信协议。设置TCP监听端口，可以动态监听各端口被连接情况。当前默认环境135、139、445、3389端口，以上为微…
HTTP代理蜜罐
WEB服务
低交互
9 个
TCP/80
提供虚假的HTTP服务端，该服务常见于办公、生产、互联网场景，HTTP服务默认使用TCP/80端口。 HTTP全称为Hyper Text Transfer Protocol，即超文本传输协议，是互联网上应…
WordPress仿真登陆蜜罐
WEB服务
低交互
5 个
TCP/9090
提供虚假的WordPress后台登录Web界面，常见于互联网场景，默认使用TCP/9090端口。可以记录下来黑客的攻击信息。WordPress是一款非常著名的开源免费的个人博客和C…
共 44 条
10条/页
前往
页

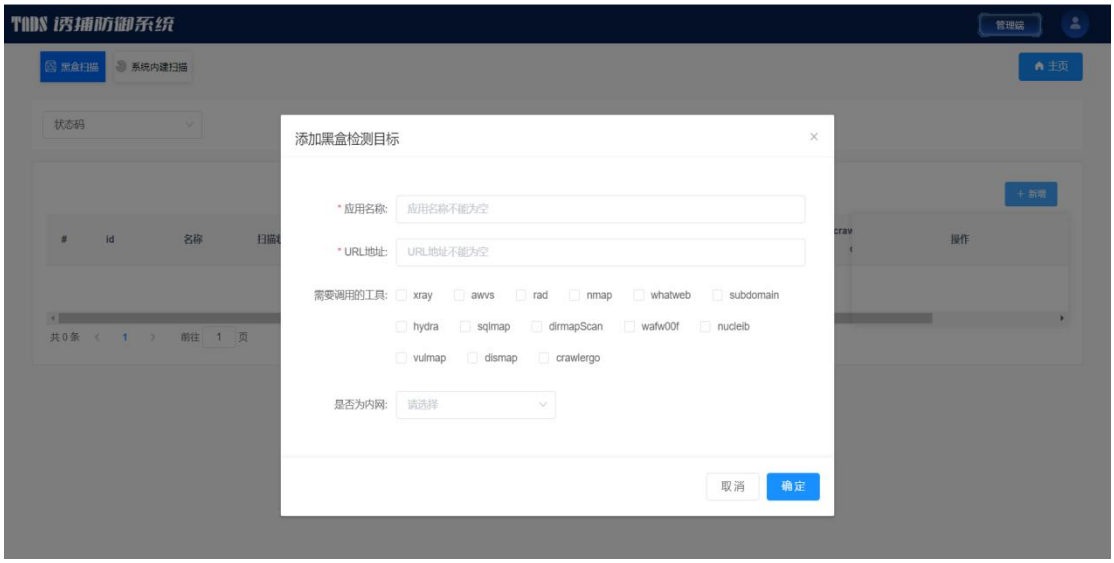
4） 告警配置


TADS 诱捕防御系统
管理端
节点管理
模板管理
服务管理
告警配置
主页
告警策略
通知配置
搜索策略名称
添加策略
策略名称
策略类型
通知方法
启用状态
操作
wqe
威胁告警
系统通知
syslog
asda11
syslog,callback
全部发送规则
ces12
test
编辑
删除
共 5 条
10条/页
前往
页


TADS 诱捕防御系统
编辑策略
策略名称:
wqe
威胁告警:
攻击行为
登录行为
主机失陷
扫描行为
高危登录行为
系统通知:
运行状态告警: 包括CPU、内存、硬盘负载状态
节点离线告警: 离线超过2分钟，将告警
蜜罐离线告警: 当节点在线时出现蜜罐离线，将报警
通知方式:
邮件
syslog
Callback
TCP:192.168.50.22:8080
TCP:122.112.20.21:8009
取消
确定

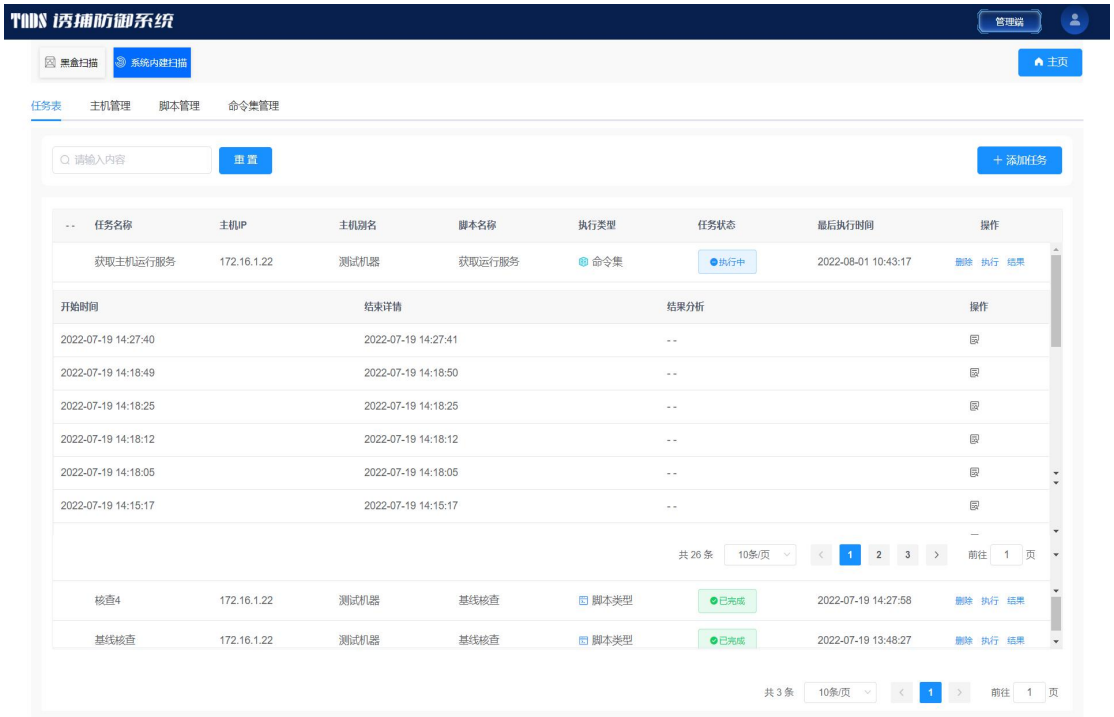
2.8.5威胁源管理

1） 黑盒扫描

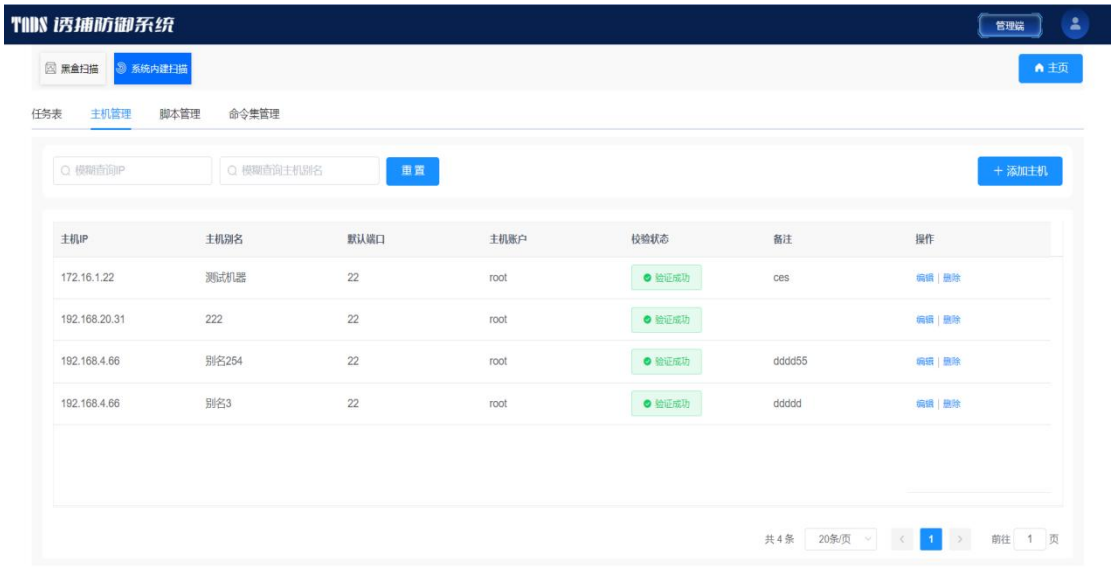


2） 系统内建扫描

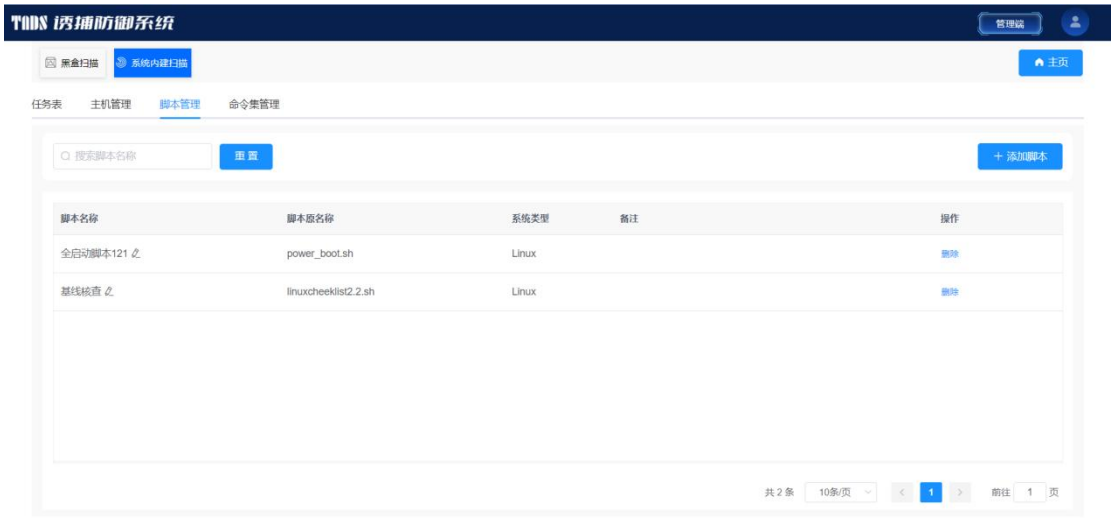
a. 任务表



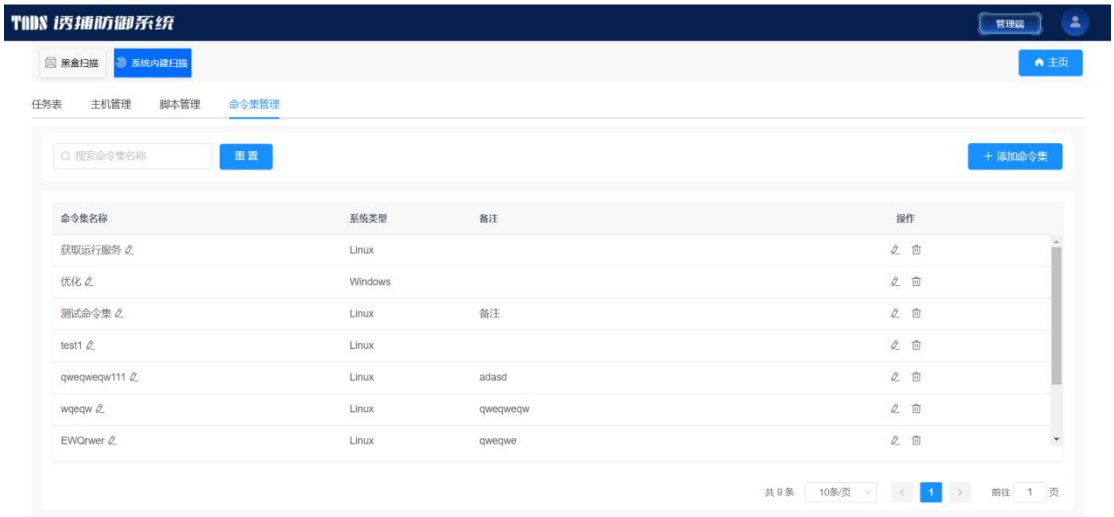
b. 主机管理



c. 脚本管理



d. 命令集管理



2.9 运维实施

2.9.1 系统测试

杭州融至兴科技有限公司安全服务团队根据现有开源蜜罐中使用量最多的两款蜜罐进行测评。蜜罐测评通过以下六个步骤进行：

编号	测试步骤
1	收集目前使用量最多的两款开源蜜罐
2	本地部署蜜罐
3	制作符合现在主流业务的沙箱
4	对蜜罐实施网络攻击，测试其攻击识别能力
5	测试两款蜜罐的可用性
6	总结两款蜜罐的优缺点

2.9.2 系统部署

测试大类	系统环境	参数
TADS	系统版本	Ubuntu 20.04.1 LTS
	容器环境	Docker version 20.10.14, build a224086
	地址（内网）	https://192.168.20.89:4433/web/login
	账号密码	admin/Favor@123