ICS 35.030
CCS L80

DB3309

浙 江 省 舟 山 市 地 方 标 准

DB 3309/T 109—2024

网络攻击诱捕系统建设规范

2024－11－5 发布　　2024－12－5 实施

舟山市市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由舟山市公安局提出并归口。

本文件起草单位：舟山市公安局，北京元支点信息安全技术有限公司。

本文件主要起草人：张艳波，王翘楚，张通汉，何淼楹，施翔，丁峰，杨丁源，杨柯，任俊博，林建伟，史晨伟，黄林。

网络攻击诱捕系统建设规范

1 范围

本文件规定了网络攻击诱捕系统的系统架构、功能要求、系统部署和系统验收要求。

本文件适用于网络攻击诱捕系统的建设。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022　信息安全技术 术语

GB 50052　供配电系统设计规范

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

蜜罐

一种诱饵系统的通称，用于欺骗、分散、转移和鼓励攻击者，使其把时间花在看似很有价值但实际上是伪造的、合法用户不会感兴趣的信息上。

[来源：GB/T 25069—2022，定义3.420，有修改]

3.2

蜜网

蜜网是由多个蜜罐以及管理和分析这些蜜罐数据的组件组成的网络，用于监控和分析攻击者在网络中的行为。

3.3

诱饵

一种旨在通过放置伪造的信息或资源来迷惑和引导攻击者，从而保护真实的系统和数据的技术。诱饵可以是文档、网络服务或账户等，通常作为安全策略的一部分。

3.4

面包屑

一种诱骗技术，通过在系统中放置虚假的信息或痕迹来引导攻击者，从而达到保护真实目标或跟踪攻击者的目的。虚假信息包括伪造的文件路径、网络连接等。

3.5

诱捕探针

一种网络安全系统，该系统结合了诱捕技术和探针技术以发现、监控和转移网络活动或攻击行为，并试图将识别到的攻击行为重定向到蜜网。

3.6

网络攻击诱捕系统

一种网络安全系统，旨在通过创建虚假资源来吸引和误导潜在攻击者，从而检测、延缓和分析攻击行为。

4 系统架构

4.1 系统至少应包含欺骗防御管理、主机和终端威胁感知、威胁决策处置等模块。

4.2 网络攻击诱捕系统架构参考图见附录 A。

5 功能要求

5.1 主机威胁感知

应能够在真实业务主机（服务器）中部署多种类型诱饵、面包屑，用于发现入侵主机的恶意行为并将其诱骗至蜜网。

5.2 终端威胁感知

应能够在各类智能联网终端中部署多类型感知诱饵，用于发现入侵终端的恶意行为并进行预警，形成对攻击者的有效威慑。

5.3 威胁处置决策

应能收集相关威胁告警，并将汇聚的信息进行统一智能分析，输出可执行的处置动作建议，为安全人员做出快速应对安全威胁的关键决策提供有效信息支撑。

5.4 网络横向移动行为检测

应能够布设策略性虚假资源和服务，引诱并监测非授权的横向移动尝试，实时识别和记录此类攻击行为并生成威胁警报。应能进行流量牵引，将攻击行为引导至蜜网来进行深度分析，实现对攻击流量的转移。

6 系统部署

6.1 部署类型

6.1.1 诱捕探针部署

应在各业务区域部署高密度的诱捕探针，并构建复杂的内部网络拓扑结构，以实现对攻击者的干扰和迷惑，增加其对攻击目标识别的难度，形成一种主动诱捕的网络防御系统。

6.1.2 诱饵部署

应在各业务系统主机安装诱饵，用于失陷主机的检测和异常行为监控；应在计算机和其他联网泛终端中，投放多种类型威胁感知诱饵，用于发现被入侵的设备。

6.1.3 蜜网部署

应部署与实际业务环境相似的蜜网，用于对攻击行为的延缓，为分析攻击者的行为特征、技术、工具、意图等提供环境，为安全团队赢得更多时进行应对准备。在部署蜜网时，应确保其与组织的生产网络环境隔离，以防止潜在的攻击波及到实际的业务系统。

6.2 部署步骤

6.2.1 现场勘查

应勘查现场，编写现场勘查报告，内容应包括网络的相关设置。

6.2.2 方案设计

应根据现场勘查报告，进行设备的部署设计，编写部署方案，部署方案应至少包括IP地址规划、路由策略规范、设备口令规划。

6.2.3 安装调试

6.2.3.1 应按照安装设计方案将所有硬件设备安装到位，并对已安装的所有产品进行外表标识，记录每个模块的产品序列号。

6.2.3.2 硬件设备安装完成之后，应对所提供的电力供应进行检查，电力供应应符合 GB50052 和硬件设备的要求。

6.2.3.3 对硬件设备进行加电启动，对软硬件设备进行安装、调试。

6.2.3.4 有多个节点时，应从中心到边缘的所有节点逐个进行设备安装及加电调测。

6.2.3.5 在完成所有软硬件设备安装及调测之后，应对整个系统进行调测，并编写系统整体调测报告。

6.3 部署验证

6.3.1 诱捕探针部署验证

诱捕探针数量应不低于业务主机数量的2倍，或能够覆盖所有主机，且应覆盖全部业务系统所在网络区域，并能将各网络隔离区域的攻击流量转发至蜜网。

6.3.2 诱饵部署验证

应在计算机和泛终端关键位置部署异常行为感知诱饵,用于对外部攻击者或内部人员的异常行为检测，迷惑攻击者并将其引导至蜜网。

6.3.3 蜜网部署验证

6.3.3.1 蜜网应支持常见的系统服务的伪装，根据不同业务场景配置符合场景相似度的蜜罐。

6.3.3.2 蜜网支持的系统服务应至少包含以下服务。

a) 操作系统层服务：
   - 文件服务；
   - 网络服务；

b) 应用层服务：
   - 数据库服务；
   - Web服务；
   - 邮件服务。

7 系统验收

7.1 系统初验

实施验收前应制定验收计划，对整个系统进行单点初验测试与系统初验测试，并形成相应测试报告。

7.1.1 验收计划

应制定系统初验计划，组织有关部门和人员对系统的功能、性能、使用等进行初验测试，依据测试结果判定是否通过系统初验，并形成系统初验报告。

7.1.2 系统试运行

应制定系统试运行计划，审批通过后开始系统试运行工作，试运行期间应解决初验时的问题。试运行结束前，形成系统试运行报告。

7.1.3 系统终验

应制定系统终验计划，组织有关部门和人员对系统的功能、性能、使用等进行终验测试，对终验过程中出现的问题应进行记录，形成问题缺陷管理报告与系统终验报告。

7.2 验收档案

验收相关文档应妥善保存，以备查验。

附 录 A
（资料性）
攻击诱捕系统架构图

网络攻击诱捕系统架构参考图见图A.1。

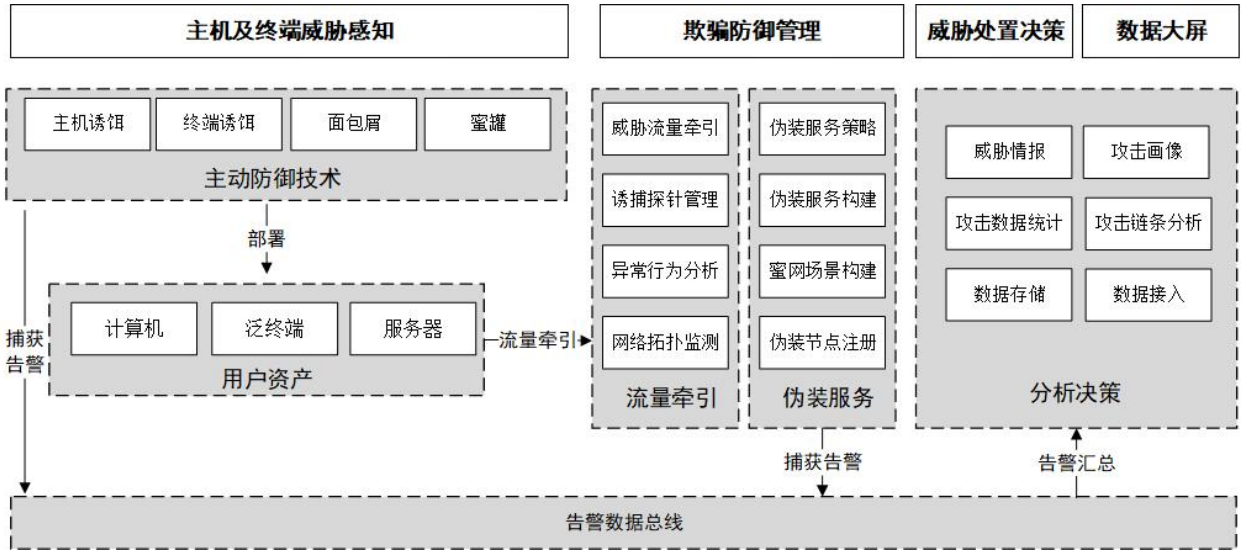

图 A.1 网络攻击诱捕系统架构图