蜜罐攻击防护系统项目需求

**项目概述**

随着网络与信息技术的发展，社会信息化进程的不断加速,尤其是互联网的广泛普及和应用，包括云计算，大数据，移动互联网，物联网，区块链等在内的新兴技术的兴起，安全威胁形势愈加严峻，网络安全事件层出不穷。

近年来，APT攻击、勒索攻击、工控设备攻击、供应链攻击、数据窃取等呈爆发态势，攻击者通过多种技术手段和社会工程等方法侵入企业内部网络，进而进行数据窃取、勒索，挖矿等行为，成为了威胁企业、社会甚至国家安全的重大问题。

建立基于欺骗防御理念，由散布在多个业务网段中的诱捕节点和集中部署的实体蜜罐，并由统一的管理平台进行管理的分布式蜜罐攻击防护系统系统。引诱攻击者对蜜罐仿真服务进行攻击，及时发现潜藏在其网络中的安全威胁，对威胁网络的恶意行为实现早期的快速发现，对攻击源头进行精准定位，掌握安全事件的主动权，并能迅速进行应急响应，控制和降低企业安全风险。

1. **系统功能需求**
	1. **蜜罐仿真能力**
		1. 蜜网创建能力

支持在一台蜜罐主机上通过管理界面创建2个以上的蜜网, 蜜网IP网段具有自动填充功能不和已有的蜜网冲突，创建的蜜网至少包括名称，网段，状态，是否允许外联等信息。

* + 1. 系统服务类蜜罐仿真

支持ssh服务、ftp服务、telnet服务、rsync服务、samba服务、rdp服务、ssh-centos服务、vnc服务等多种系统服务的仿真蜜罐。

* + 1. 数据库类蜜罐仿真

支持mysql数据库、redis数据库、mongodb数据库、memcached数据库postgresql数据库等多种数据库的仿真蜜罐。

* + 1. Web应用类蜜罐仿真

支持OA应用、mail应用等多种Web应用的仿真蜜罐。

* + 1. 漏洞类蜜罐仿真

 支持struts2漏洞、smb漏洞、Tomcat ajp漏洞、shiro漏洞、PHPmyadmin漏洞、shellshock漏洞、log4j漏洞等多种漏洞的仿真蜜罐。

* + 1. 溯源反制类蜜罐仿真

 支持Web溯源、反制蜜罐等多种类型的仿真蜜罐。

* + 1. 蜜罐自定义能力

·Web蜜罐内容自定义，支持蜜罐自定义登录用户名、口令、Title、logo等。

·支持蜜罐自定义https证书。

* + 1. 蜜罐仿真制作能力

刻录仿真蜜罐，支持对现有系统的刻录仿真

* 1. **攻击诱导能力**
		1. 节点伪装能力

支持在管理界面配置诱捕节点暴露不同的服务端口，伪装成不同的诱捕服务形态。

* + 1. 节点扩展能力

支持通过管理界面在一台虚机上批量创建多个具有独立IP地址的诱捕节点，并且为每个节点配置不同的开放端口和对应的蜜罐服务。

* + 1. 攻击转移能力

支持对诱捕节点暴露的服务的访问，转向后端仿真蜜罐，形成攻击转移和隔离。

* 1. **攻击监测能力**
		1. **节点类**

·节点触碰捕获，支持捕获利基于TCP, UDP, ICMP协议对诱捕节点的触碰行为。

·ARP欺骗捕获，支持感知ARP欺骗行为，支持记录攻击日志，至少包含被伪装的IP、IP 伪装前的MAC地址和伪装后MAC地址。

·IPV4，支持捕获对诱捕节点ipv4的访问。

* + 1. **蜜罐交互类**

·支持系统及系统服务交互行为捕获。

·支持数据库类交互行为捕获。

·支持web类交互行为捕获，捕获内容至少包括请求头，请求体，响应的状态码，响应体等字段信息。

* + 1. **蜜罐内监控能力**

·支持对在蜜罐中执行的命令的捕获。

·支持蜜罐中文件变动的捕获。

* + 1. **攻击行为检测**

·支持恶意行为识别，如sql注入等攻击行为。

·支持CVE漏洞识别。

·支持工具识别。

* + 1. **取证**

·支持捕获流经蜜罐的流量，保存并下载。

·支持攻击回放。

* 1. **威胁分析能力**
		1. **威胁展示**

支持以列表的形式展现节点触碰类告警、蜜罐交互类告警等，并提供检索功，告警详情支持以时间线的方式展示攻击行为。

* + 1. **高级分析能力**

·支持攻击源IP，目的IP，URL，User agent，referer，cookie，事件类别，事件行为，事件IOC, 属性标签，状态码等字段作为条件去检索捕获的蜜罐交互行为；筛选条件支持“AND、OR”，“等于、不等于”这样的筛选关系。

·分析展示支持同时展示事件的汇总信息和详情信息，汇总信息包括热力图，属性标签，数据量图，区域分布等统计图表。显示详情信息字段并且支持动态选择字段进行显示点击汇总信息的图表的内容，支持汇总信息和详情相应筛选变动。

* + 1. **统计报表**

支持创建报表任务并生成统计报表，包括单次任务和周期性任务，报表内容包括告警事件统计信息、节点运行状况等信息。

* 1. **溯源反制能力**
		1. **黑客溯源**

支持web溯源。

* + 1. **攻击反制**

蜜罐系统部署完毕，包括相应的网络设置和系统设置。

* 1. **联动处置能力**
		1. **白名单配置**

支持根据源，目标，目标端口，协议等多维度的白名单配置。

* + 1. **数据上报**

·支持通过kafka进行信息上报，支持分别按事件类型和事件等级进行上报，同时支持上报到多个kafka目标。

·支持通过syslog进行信息上报，支持分别按事件类型和事件等级进行上报，同时支持上报到多个syslog目标。

* + 1. **告警通知配置**

·支持界面实时弹框告警，支持分别按事件类型和事件等级进行，支持通过开关来进行配置。

·支持声音告警，支持通过开关来进行配置，支持分别按事件类型和事件等级进行配置，支持提示声音替换。

·支持通过邮箱进行邮件告警，支持分别按事件类型和事件等级进行告警，同时支持不同的策略，发送到不同的收件箱。

* 1. **符合安全等保要求**

·支持双因子认证，三权分立

·数据传输加密，支持https证书部署

·数据备份，支持本地备份和异地备份，备份周期符合等保要求

1. **配置要求**

·支持虚拟机部署或服务器硬件部署，硬件部署需配置冗余电源

·支持灾备机制，在系统出现故障时能快速恢复

1. **交付要求**

·合同签订后1个月内完成系统的部署和调试；

·6个月内完成系统上线使用和项目验收。

·从设备交付当日起提供三年售后技术支持。