# 锦行科技高交互蜜网欺骗防御方案

## 1）必要性

随着信息技术的发展，新时期下的网络安全形势更加严峻。一方面，**漏洞数量史无前例的增长，**根据中国国家漏洞库（CNNVD）的官方统计，2017年全年公布的漏洞总数达到14748个，同比去年增长70%；另一方面，**重大安全事件频发，网络攻击从最初的自发式、分散式的攻击转向专业化的有组织行为，呈现出攻击工具专业化、攻击目的商业化、行为组织化的特点。**APT攻击事件此起彼伏，并且以其无孔不入的触角延伸到了全世界各地，几乎所有的重要行业如政府、金融、电力、教育都受到了APT攻击的威胁。根据2017年4月黑客组织“影子经纪人”在网上公布的资料显示，**2000-2010年这十年间中国的一些重要基础设施、高校、大型企业等重点目标都曾遭到过入侵。**比较典型的，针对中国政府的海事机构、海域建设部门、科研院所和航运企业的APT攻击组织**“海莲花”当被曝光时已潜伏长达3年。**

目前，现有的传统的安全防御手段用来应对中低层次的普通网络威胁和非针对性网络攻击被证明能够发挥一定的作用，但在当前新的形式下，在面对一些高层次网络威胁、针对性网络攻击方面，则存在着不足，难以有效应对：

1. **难以及时发现和有效应对各种新型高级威胁。**高等级攻击隐蔽性很强，往往利用自定义工具、未知漏洞、模仿正常操作进行攻击，传统防御手段很难发现。
2. **缺乏有效的内网威胁感知手段。**不能正视漏洞的存在，导致大量重复的安全建设局限于边界防御，试图打造一个不可攻破的系统，而对于内部网络的安全威胁重视不足。
3. **一般只能在一定范围内发挥特定的作用，互相之间缺乏有效的数据融合和协同管理机制。**面对众多分散且海量的信息，无法全面直观地了解系统安全脆弱点、整体攻击状况以及安全防护效果，无法满足预判系统安全脆弱点并提前实施防御措施的需求。

面对新时期下的各类新型高级网络威胁，仍然仅仅沿袭和依赖现有的修补漏洞、识别阻断、事后审计等传统网络安全防御手段已经不够，必须转换思路，引入更为主动的、基于攻击者视角的网络安全防御新理念，作为对传统安全防御手段的必要补充。

欺骗防御是一种新兴的网络安全防御技术，**基于欺骗防御技术的安全产品可以实时、有效地检测、分析、防御0day攻击以及高级威胁。欺骗防御技术具有全自动化、高精准度的特点，能够深入洞察其他传统安全防御手段无法觉察的内网黑客活动。**全球最具权威的IT研究与顾问咨询公司高德纳(Gartner) 曾在2015、2016、2017年将欺骗防御技术列为**全球信息安全十大顶级技术之一。**

## 2）工作原理

根据洛克希德-马丁提出的著名“杀伤链”（Kill Chain）模型，虽然攻击的技术和手段在不断变化，然整个攻击的大致阶段是不变的，攻击者通过边界防御进入网络内部后，一般都要经过侦查、提权、横向移动等过程。



图2.1 Kill Chain模型

基于欺骗技术的高交互蜜罐系统的主要原理是**通过在黑客进行攻击和渗透的网络中的关键位置和关键环节中布置具有高度迷惑性的虚假资产和线索对攻击者进行欺骗，在攻击者进行侦查和横向移动等活动时，误导、干扰攻击者对目标网络环境的认知，并逐步将攻击者从用户的真实网络环境中引导至大型高交互蜜网系统中进行攻击，从而以达到保护用户真实网络环境和信息资产的目的。**

本定制化高交互蜜罐系统将**主要由中心和节点组成。**中心由虚拟化技术构建出的用于欺骗和诱捕攻击者的**仿真特定网络环境**（可包含网站、业务系统、数据库、中间件等）、**数据捕获及分析系统**、以及**管理展示平台**组成。节点是轻量级攻击流量转发探针，广泛分布在需要防护的真实网络中，通过欺骗技术，负责把攻击从真实网络诱导转移至高交互蜜网中进行攻击，并采集和分析攻击数据，获取威胁情报。

以图2.2简化的典型用户网络环境为例来说明，在未部署高交互蜜网之前，倘若攻击者一旦通过先进手段突破边界防御进入内网，则可顺利的实施后续的内网渗透行为，可能对用户的网络造成非常严重的危害（如盗取敏感数据、实施破坏行为等）。



图2.2 部署高交互蜜网系统前用户的网络环境

部署高交互蜜网过后，整体的用户网络环境可简单分为两部分（如图2.3），一部分是用户原有的网络，不会对其产生任何影响和改动。另一部分是蜜网（由高交互蜜罐构造的仿真虚拟网络环境），蜜网通过蜜罐节点映射到组织的真实网络环境中并与之融为一体。



图2.3 部署高交互蜜网后的网络环境

这种由高交互蜜罐构建出来的蜜网环境具有如下特点：

**1.极具迷惑性。**从攻击者的视角看来，蜜网与用户的真实网络不存在任何差异，这将成倍增加攻击者眼中用户网络的规模和复杂程度，指数级提高攻击者在内网渗透中对网络结构分析、攻击路径选取和目标判断的难度。

**2.极具诱惑性。**从攻击者的视角看来，相对于用户的真实网络，蜜网更具有吸引力，会主动诱引攻击者进行攻击，从而将攻击者从用户的真实网络环境中转移到蜜网中，同时对攻击者的所有攻击过程和操作进行监控和记录，并立即进行告警。

**3.与真实网络严格隔离。**蜜网是一个隔离可控的环境，即攻击者无法在蜜网中对用户真实网络或者任何外界环境发起攻击。

因此，在具备了高交互蜜网系统的防护后，即便攻击者成功利用先进手段和技术突破边界防御进入用户的网络当中，也极难甚至不可能顺利实施后续的内网渗透行为，难以对用户的真实网络环境产生实质性危害。

## 3）功能性能指标

|  |  |  |
| --- | --- | --- |
| **模块** | **指标** | **参数/描述** |
| **诱捕引流模块** | 蜜罐代理 | 支持通过代理节点将攻击转移到远端蜜罐和蜜网中 |
| 占用资源 | 内存256M/CPU800MHz单核/硬盘100M |
| 操作系统环境 | 支持Ubuntu 14.04、CentOS 6.5、EulerOS2.0以上环境 |
| 自定义端口转发 | 支持自定义端口转发 |
| 节点动态绑定 | 支持代理节点和蜜罐的转发关系重新解绑并重新绑定 |
| 最大并发节点数量 | 200个节点 |
| 欺骗诱饵数量 | 8种  |
| 欺骗诱饵类型 | Linux : hosts、history、SSH登录凭证Windows : hosts、3389登录日志、工具登录痕迹(xshell)、工具登录痕迹(secureCRT)、账号密码记录(txt) |
| 实时节点状态监控 | 支持节点状态监控 |
| **蜜网仿真模块** | 蜜罐模版管理 | 支持蜜罐模版的创建、重置、删除 |
| 蜜罐管理 | 支持对蜜罐的主机名管理、用户及用户组管理、文件管理、命令执行、服务配置 |
| 蜜罐状态监控 | 支持蜜罐状态的监控 |
| 主机蜜罐操作系统支持 | Windows 、Centos、Ubuntu |
| 模拟的协议数量 | 27种 |
| 欺骗环境数量 | 60余种  |
| 模拟的服务 | 支持如下服务：telnet、mysql、ssh、ftp、http、smtp、imap、https、remote\_login、rsync、socks、oracle\_database、oracle\_database\_default\_listener、svn、redis weblogic d\_s\_n、simplify\_media、radan\_http wap\_wsp、git、mongod、mssql、rdp、snmp、vnc、ntp、kerberos、sip、tftp |
| 模拟的内网场景 | 支持如下内网场景模拟：DMZ区、普通办公区、管理员区、开发区核心数据区 |
| 复杂蜜网场景 | 支持将所有蜜罐组成一个大型复杂网络场景 |
| 自定义场景 | 支持对蜜网场景进行自定义修改和订制 |
| 按照被保护资产类别分组管理 | 支持 |
| **数据捕捉模块** | 捕捉的数据种类 | 网络行为，包括：网络连接 |
| 文件操作行为，包括：创建文件、读文件、写文件、删除文件、文件重命名、创建目录、删除目录、目录重命名 |
| 命令行行为，包括：Linux指令输入输出、windows cmd输入输出、windows powershell输入输出 |
| 进程行为，包括：进程创建 |
| 注册表行为，包括：修改注册表值项、删除注册表值项、创建注册表键、删除注册表键 |
| 登录行为，包括：用户登录 |
| 会话行为，包括：远程会话登录 |
| **数据存储模块** | 单机支持存储的数据量 | 大于1T，小于4.8T |
| 单机支持备份的数据量 | 大于1T，小于4.8T |
| 数据检索 | 支持 |
| 外部不可删除 | 具备 |
| **数据还原分析模块** | 攻击事件分析 | 支持如下攻击事件分析：扫描事件分析、HTTP攻击事件分析、HTTP高危攻击事件分析、SSH攻击事件分析、菜刀攻击事件分析、Mysql攻击事件分析、Mongodb攻击事件分析、RDP攻击事件分析、SQLServer攻击事件分析、SVN攻击事件分析、勒索病毒事件分析、ORACLE攻击事件分析 |
| 攻击回放 | 支持如下回放方式：指令回放、Windows远程桌面屏幕录像回放 |
| **威胁情报模块** | 威胁情报分析 | 支持威胁情报中多种数据的关联分析：攻击源IP、攻击事件、攻击样本名、攻击样本HASH、攻击字典 |
| 威胁情报输出 | 支持如下威胁情报数据输出：攻击来源IP、攻击工具样本、攻击字典 |
| **取证溯源模块** | 溯源数据捕获 | 支持如下溯源数据的捕获：攻击来源IP、攻击工具样本、攻击字典 |
| 帐号密码风险评估 | 支持依据捕获攻击者使用的字典对特定密码进行风险评估 |
| **攻击报警模块** | 报警渠道 | 支持如下报警方式：邮箱报警、页面报警、syslog报警方式 |
| 报警等级分级 | 高危、低危 |
| 报警事件合并 | 支持攻击数据按事件自动归类合并报警 |
| 报警策略 | 支持按ip过滤、类型过滤、报警等级进行订制 |
| **安全控制模块** | 数据保护 | 具备核心数据加密存储 |
| 蜜罐程序自保护 | 所有蜜罐程序相关的进程、文件、网络数据及网络连接均具备深度隐藏特性，通过常规手段及工具无法检测出。 |
| 攻击隔离 | 不能以蜜罐为跳板攻击外网不能以蜜罐为跳板攻击客户真实网络 |
| 鉴权失败处理 | 多次失败限制IP登录 |
| 角色及权限管理 | 可以设置不同等级用户具备不同等级权限 |
| 管理员操作审计  | 管理员日志对管理员的所有操作进行日志记录 |
| **设备性能指标** | 支持欺骗环境数量 | 单台支持最多2000个报警蜜罐或者50个主机蜜罐 |
| 数据监控程序 | cpu占用2-3%左右，内存150M左右 |
| 视频还原 | 视频还原每秒20M |
| 最大流量 | 流量最大峰值100M（千M网卡） |

## 4）设备选型

## 6）部署方案

**6.1 部署网络情况**

**6.2 部署分析及建议
6.2.1部署网络区域的选择**

除了蜜罐本身诱饵质量的因素外，蜜罐的攻击捕获存在一定的概率问题，我公司的幻云产品所采用的蜜罐节点技术为轻量级转发节点，几乎不会对部署企业的真实网络环境产生任何影响，因此理论上来讲，节点当然尽可能多的好，但是在综合考量成本等因素的情况下，在节点数量有限或者不足的情况下，是存在区域的侧重点的。由于攻击者主要有两种入侵途径进行攻击，一种是通过利用对外提供的服务器存在的漏洞，通过外部入侵，另一种是通过内网办公区，利用病毒、木马以及钓鱼等手段借助内部员工的电脑实现内部入侵，**因此部署的重点区域主要有2种，一种是用户网络区域中能够直接被外网访问的区域，另一种是用户网络中能够直接访问外网的区域。**因此在部署建议上在XXX区域、XXX区及XXXX区域部署蜜罐节点，对攻击者进行诱捕。

针对蜜罐节点的部署侧重，针对特定的网络区域，还可以做进一步细化。比如办公网，可以针对能够接触到开发或者测试区域核心代码、业务数据等的开发人员和运维人员区域周围做重点针对性部署。

**6.2.2 部署节点数量选择**

为确保诱捕的有效性，我们建议的节点的数量与真实服务器的比例为1：4~1：2之间，也就是说蜜罐节点的数量占该网络区域已用IP数的20%~50%之间。

理由是:这主要是基于我公司的安全团队十余年来的应急响应服务和APT案例过程的分析研究得出的结论：平均一次局部网络区域的成功入侵行为，会触碰该区域内80%的主机。

**6.2.3 蜜罐类型选择**

针对蜜罐类型的分配和选择，可以进行有针对性的选择部署，以达到最佳的效果和性价比，按交互程度和作用划分，幻云的蜜罐主要分为报警蜜罐和主机蜜罐，报警蜜罐主要用于攻击发现，成本较低，可大规模扩容，实现广泛覆盖，主机蜜罐主要用于深度攻击行为数据的捕获，可以提取有价值的威胁情报，但成本较高，可以进行有针对性的部署，如部署在核心资产周围，关键路径点等。蜜罐的操作系统和服务类型也可以根据周围业务和网络环境进行有针对性的选择，比如数据区、生产服务区等可多部署一些数据库、中间件类型蜜罐，WINDOWS服务器居多的区域可部署WINDOWS系统蜜罐、linux系统居多的区域可部署linux蜜罐、外围区域及非核心区域以报警蜜罐部署为主，主要起早期预警作用。

**6.2.4 部署建议**

结合上述分析及客户网络环境实际情况，我们建议：

1. 在XXX 网段、XXX网段、XXXX网段进行蜜罐节点部署。
2. 部署的蜜罐节点总数为X个（部署网络真实主机数量的20%，其中高交互主机蜜罐X个，报警蜜罐X个）
3. 部署蜜罐类型主要有WINDOWS蜜罐、CentOS蜜罐、数据库蜜罐、以及中间件蜜罐、XXX蜜罐。。。。

**6.3 部署拓扑**

****

## 7）方案报价

预计费用如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 产品 | 型号 | 参数 | 数量 | 单价(万元) | 小计(万元) |
| **锦行幻云欺骗防御与本地威胁情报平台** | JES-HYU-XXXX/V2.6 | 可支持部署X个高交互主机蜜罐、X个低交互报警蜜罐、X个软件节点。功能指标：（详见3.功能性能指标）硬件参数：2\*Xeon/E5-2603V4/128G/8\*2T/Raid10/独立电源电源接口 | 1 |  |  |
| **总计** |  |

备注：
A：本方案为满足该项目安全防护需求所需的最低蜜罐数量及规格，为了达到更好的推荐防护效果，也可对蜜罐节点进行扩容。

B:主机蜜罐与报警蜜罐均可进行扩容，如需进行扩容，主机蜜罐按照X万/个；报警蜜罐按照0.X万/个收取费用。如报警蜜罐或主机蜜罐超过单台中心设备性能最大值，需增加新的中心硬件设备，需另外收取硬件成本费用。

C:产品自带3年免费售后维保服务，此后按照合同总额的X%收取费用。

D:产品售后维保服务仅限解决产品自身使用及故障解决等问题。