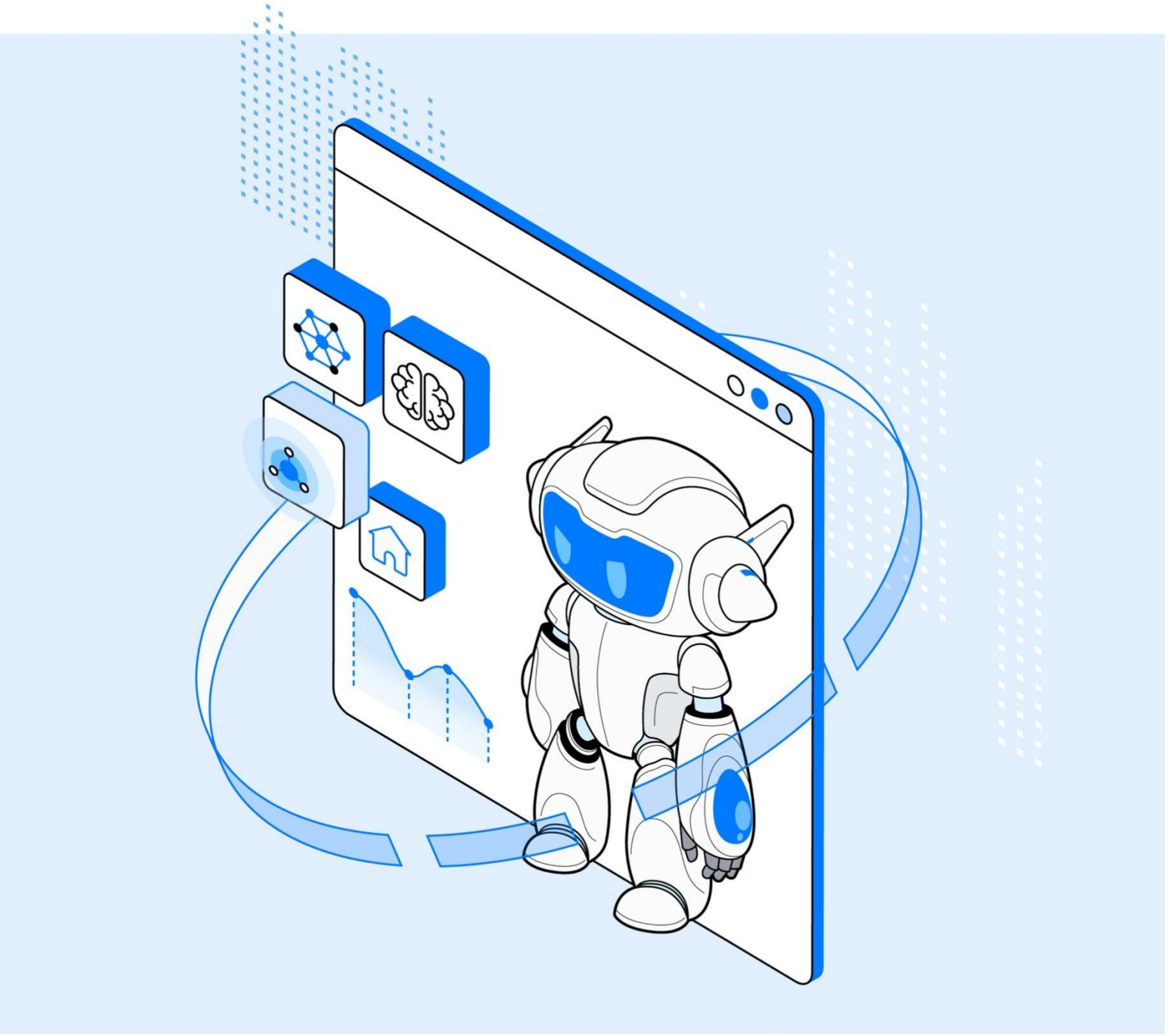
万径安全
MegaVector

小智—智能渗透测试机器人
产品白皮书



四维创智（北京）科技发展有限公司

目录

一、行业背景

近年互联网高速发展，给社会带来了极大的便利，同时也带来了大量的网络安全问题。据统计，2024 年全球网络安全事件造成的经济损失高达 1000 亿美元，平均每 20 秒钟就发生一起网络入侵事件。开放的网络环境为不法黑客提供了攻击目标，而网络的多样性、开放性、互联性等更为其提供了入侵的便利。

网络安全形势越来越严峻，国家对网络安全的重视程度越来越高。从 2016 年起，公安部每年举办护网行动，通过实际网络渗透攻击来检测国家重点单位的网络安全，同时促进重点单位对网络安全的重视。网络安全等级保护 2.0 的合规要求中明确指出要对系统进行渗透测试。

以攻代防的渗透测试安全方式越来越受到重视，但其存在的问题也越来越明显。渗透测试涉及到的知识面宽、专业性要求高，当前主要由专业的渗透测试人员通过手工进行，且过程中使用多种渗透测试工具才能够完成渗透测试。专业性要求高、基于人工、涉及工具多，导致渗透测试人员工作量大，造成渗透专业人才培养困难。

二、产品介绍

2.1 产品概要

“小智-智能渗透测试机器人”是国内率先实现“AI+网络安全检测”的智能渗透测试平台。它通过独创的 DPL 黑客语言把黑客渗透测试经验转化为机器可存储、识别、处理的结构化专家渗透经验，同时通过知识图谱技术将专家经验关联，形成决策“大脑”。通过决策“大脑”，“小智-智能渗透测试机器人”能够模拟黑客思维进行自动化渗透测试。

“小智-智能渗透测试机器人”能够自动化检测主机、web、视频监控、办公自动化设备的安全薄弱点，并且能够对相关漏洞进行自动验证、利用、取证。当前“小智-智能渗透测试机器人”主要应用于新系统上线前漏洞检测、业务系统漏洞日常检测、网络安全红蓝对抗等场景。能够协助人工进行渗透测试，一定程度上替代部分人工渗透测试，减少渗透测试人员工作量，提高渗透测试效率。

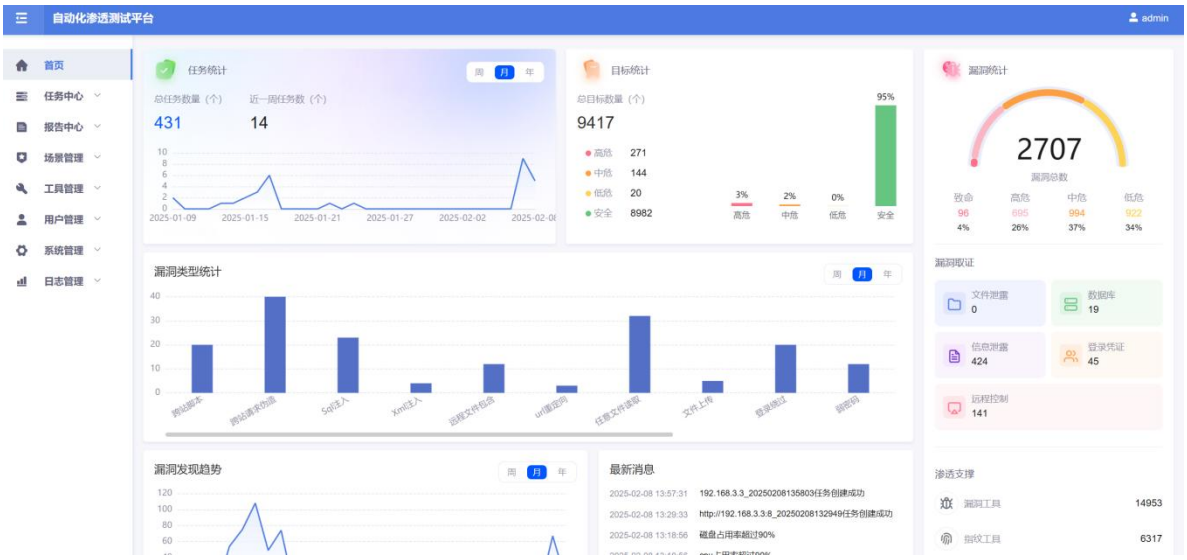


图 1：小智-智能渗透测试机器人界面

2.2 产品架构

“小智-智能渗透测试机器人”采用三层结构，分别为应用层、决策调度层、资源层。应用层是用户与平台交互的核心，集成了渗透测试全流程功能模块；决策调度层是平台的智能化中枢，依赖智能推理决策引擎动态制定渗透策略；资源层为上层提供基础能力支撑。

图 2：小智-智能渗透测试机器人架构图

（一）应用层

应用层是用户与平台交互的核心，集成了渗透测试全流程功能模块。任务管理负责统筹测试任务的生命周期；场景管理支持定制化场景配置；攻击面管理通过资产识别与风险评估动态监控目标暴露面；渗透可视化则实时展示攻击路径及效果；漏洞管理、报告管理模块实现漏洞跟踪与结果自动化输出；工具管理和用户管理确保资源权限可控；系统管理与日志管理提供平台运维支持，保障操作可追溯。应用层通过模块化设计，将复杂渗透流程简化为直观操作，提升任务执行效率。

（二）决策调度层

决策调度层是平台的智能化中枢，依赖智能推理决策引擎动态制定渗透策略。知识图谱库整合渗透经验与漏洞情报，构建多维关联关系，为决策提供语义化支持；渗透调度执行引擎基于推理结果，协调漏洞检测、横向渗透等能力模块，实现自动化任务编排。通过逻辑推理与资源调度，决策层将静态知识转化为动态执行方案，确保渗透测试的高效性与适应性。

（三）资源层

资源层为上层提供基础能力支撑。工具/平台三方接口实现外部工具集成与数据互通；资产指纹库涵盖服务器、Web 组件、网络设备、数据库等目标特征，支持精准资产识别；漏洞插件库内置 POC、EXP 及自定义脚本，覆盖多场景漏洞利用需求；测试

工具库集成信息收集、扫描探测等专用工具链，强化渗透执行能力；情报/信息资源与函数级安全能力形成底层技术底座，为漏洞验证、漏洞利用等提供原子化能力。

2.3 产品功能

“小智-智能渗透测试机器人”能够自动化完成渗透测试中信息收集、漏洞扫描、漏洞验证、漏洞利用、输出报告的全过程。下述功能模块是“小智-智能渗透测试机器人”进行渗透测试时会自动调用的功能模块和支持自动化渗透测试的功能模块。

（一）端口扫描

小智-智能渗透测试机器人通过和被测目标进行 TCP 全连接、半连接来获取被测目标的响应信息，通过响应信息判断被测目标端口开放和提供的服务。

端口扫描支持智能端口扫描、常用端口扫描、指定端口扫描、全端口扫描。其中智能端口扫描是在检测到目标存活的情况下，但未发现常用端口开放，系统将自动扫描其他未测试的端口，从而实现有效检测目标存活。

（二）WEB 路径猜测

WEB 路径猜测模块通过调用 web 路径字典中的敏感 URL 来探测被测目标是否存在对应的敏感 URL。系统通过分析被测目标响应敏感 URL 请求的报文来判断是否存在敏感 URL，从而实现获取网站的敏感目录和内容。

（三）口令猜测

口令猜测模块通过调用弱口令字典来尝试登录被测目标，从而实现验证被测目标是否存在弱口令漏洞。当前支持口令猜测的服务包括 telnet、mongodb、mssql、postgresql、redis、smb、ftp、ssh、mysql、http 等。

口令猜测模块能够对带通用验证码登录入口进行弱口令检测，能够识别的验证码类型包括数字、字母、数字与字母组合等。

（四）信息收集检测

小智-智能渗透测试机器人在渗透测试过程中能够针对被测目标的服务、站点、URL和子域名等进行信息收集，包括但不限于收集被测目标的开放端口、协议信息、服务信息、组件信息、指纹信息、文件上传入口、URL、敏感路径、登录入口等。

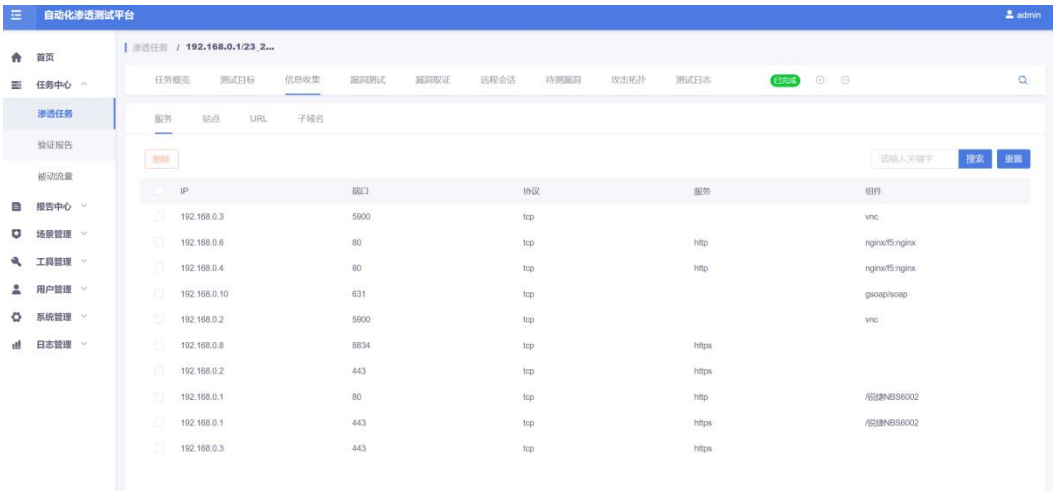


图 3：信息收集图

（五）登录检测

登录检测功能是在创建渗透测试任务时，通过提前预置被测目标的登录凭证，实现渗透测试过程中，系统通过预置的登录凭证登录被测目标进行登录后的渗透测试。目前支持对 http/https 进行登录检测，且支持的登录凭证包括用户名密码或 cookie。

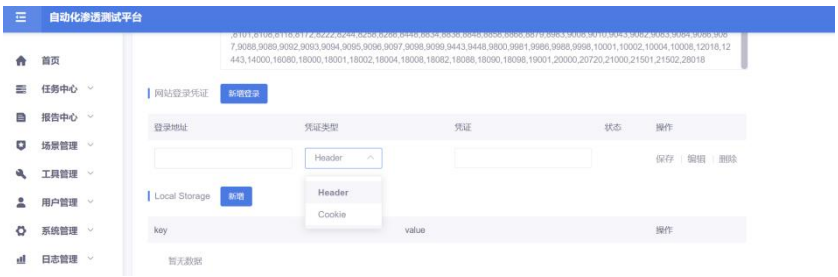


图 4：网站登录凭证图

（六）漏洞报文重放

渗透测试过程中，系统将检测漏洞的关键报文进行保存。用户通过查看编辑检测漏洞的关键报文，并且能够再次发送检测漏洞的关键报文，实现漏洞检测过程重放。

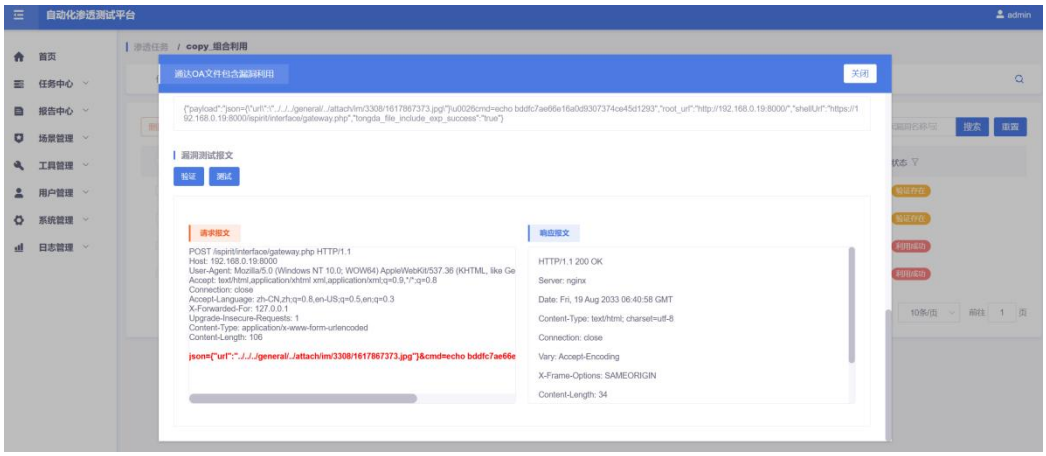


图 5：漏洞报文重放图

（七）操作系统渗透

能够识别的操作系统包括 windows、linux、unix、IOS、andriod 等。能够检测利用的操作系统自带或第三方组件的漏洞类型包括缓冲区溢出、命令执行、弱口令、未授权访问等。

（八）Web 系统渗透

能够识别的 web 组件包括 Apache、Tomcat、MicroSoft IIS、JBoss、Nginx、IBM WebSphere、WebLogic、litespeed、mongrel、axis2、IdeaWebServer、Sun ONE Web Server、ZendServe、Glassfish、Resin、Jetty、JBoss、Apache ActiveMQ、Lighttpd、Servlte、kangle、Varnish、Tengine、vWebserver 等。

能够检测和利用的 web 服务漏洞包括 SQL 注入、XSS 跨站脚本漏洞、任意文件上传、任意文件下载、任意文件操作、信息泄露、弱口令、本地文件包含、目录遍历、远程命令执行、未授权访问、代码执行、反序列化漏洞、缓冲区溢出、会话劫持、拒绝服务、越权漏洞、认证绕过、远程文件包含、SSRF、XML 注入、其他逻辑漏洞、编辑器

漏洞、重放攻击、CSRF、CRLF 注入、Xpath 注入、命令注入、并发漏洞、主机头攻击、解析漏洞等类型 web 漏洞。

（九）**视频监控设备渗透**

能够识别的视频监控设备厂商包括大华、海康、天地伟业、金三立、海鑫格、云视通等。能够识别视频监控设备类型包括视频编码服务器（DVS）、数字视频录像机（DVR）、网络视频录像机（NVR）、网络存储服务器等视频监控设备，并且能够对视频监控设备进行渗透利用。

（十）**数据库系统渗透**

能够识别并利用的数据库类型包括 Oracle、Mysql、postgresql、SqlServer、达梦、Gbase、DB2、Informix。

（十一）**网络节点设备渗透**

能够识别和检测 Cisco、Juniper、Fortinet、HillStone、CheckPoint、天融信、PaloAlto、绿盟、华为、网神、启明星辰、网御星云、F5、Imperva SecureSphere、IBM、Symantec 等安全厂商设备；能够识别和检测 Cisco、Juniper、Netgear、H3C、HuaWei、中兴、TP-Link、D-Link、锐捷、MikroTik、JCG、Ruckus 等网络厂商设备。

（十二）**任务执行方式控制**

系统支持用户对被测目标的运行情况来自定义对被测目标进行即时检测、定时检测、周期性检测。

（十三）**渗透测试范围控制**

系统能够通过任务场景来控制渗透测试过程中运行的渗透测试工具，检测指定的安全漏洞，收集对应的目标信息等。

（十四）**漏洞组合利用**

系统在检测到多个漏洞时，会利用知识图谱的关联性，将多个漏洞的输出信息进行关联推理。当多个漏洞的信息在知识图谱上满足触发新漏洞条件时，系统就能够检测到新的漏洞，从而实现将多个低危漏洞组合成高危漏洞的效果。

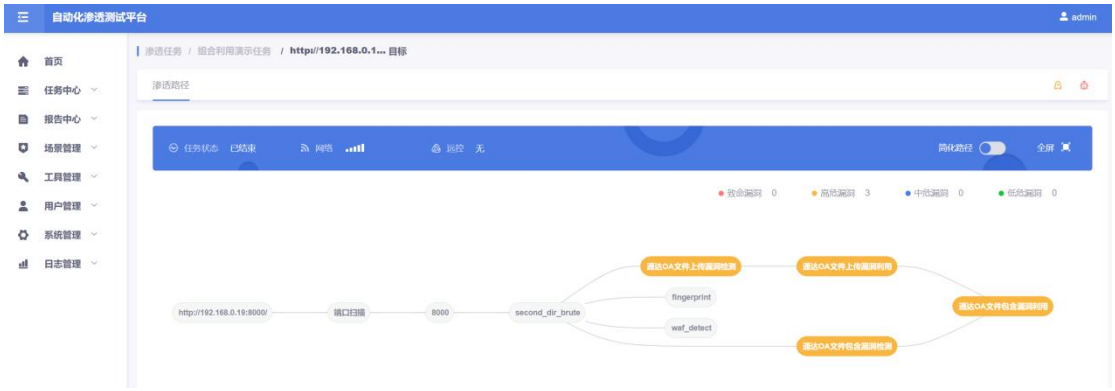


图 6：漏洞组合利用图

（十五）漏洞链式利用

系统在检测到某个漏洞时，会根据此漏洞的知识图谱连接特性，来发现此漏洞是否具备能够深入利用特性，从而实现对漏洞更深入全面的检测。

图 7：漏洞链式利用图

（十六）渗透痕迹追溯

系统能够详细记录渗透测试过程中调用的渗透工具、执行的渗透操作、检测的漏洞，并且能够记录发送相关的报文记录，从而实现对渗透测试溯源。

（十七）动态爬虫

动态爬虫采用本地无界面浏览器技术实现，系统通过访问本地无界面浏览器实现对被测目标的网页内容爬取和操作。通过无界面浏览器可以实现对被测目标进行页面预加载、网络空闲状态等待、网站内容劫持、模拟点击、页面加载过程的代码注入、请求拦截、函数劫持、事件监听、遍历节点及事件、填充表单等。

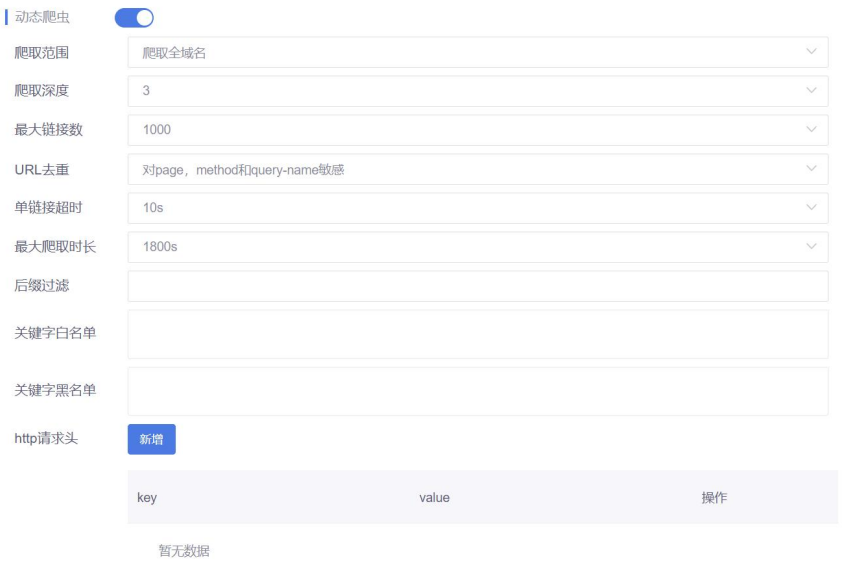


图 8：动态爬虫配置图

（十八）远程控制功能

测试任务中能够通过漏洞利用反弹 shell 到安全平台，用户能够通过平台的可视化界面对其进行操作，包括管理、断开和删除、远程控制被测目标，降低对被测目标的操作复杂程度。

（十九）自定义报告

系统能够导出对多个目标进行分析的综合任务报告和单个的漏洞目标报告。用户能够根据报告模板自定义报告内容，自定义报告封面，支持导出 word、pdf、html、excel 和 CSV 类型的报告。

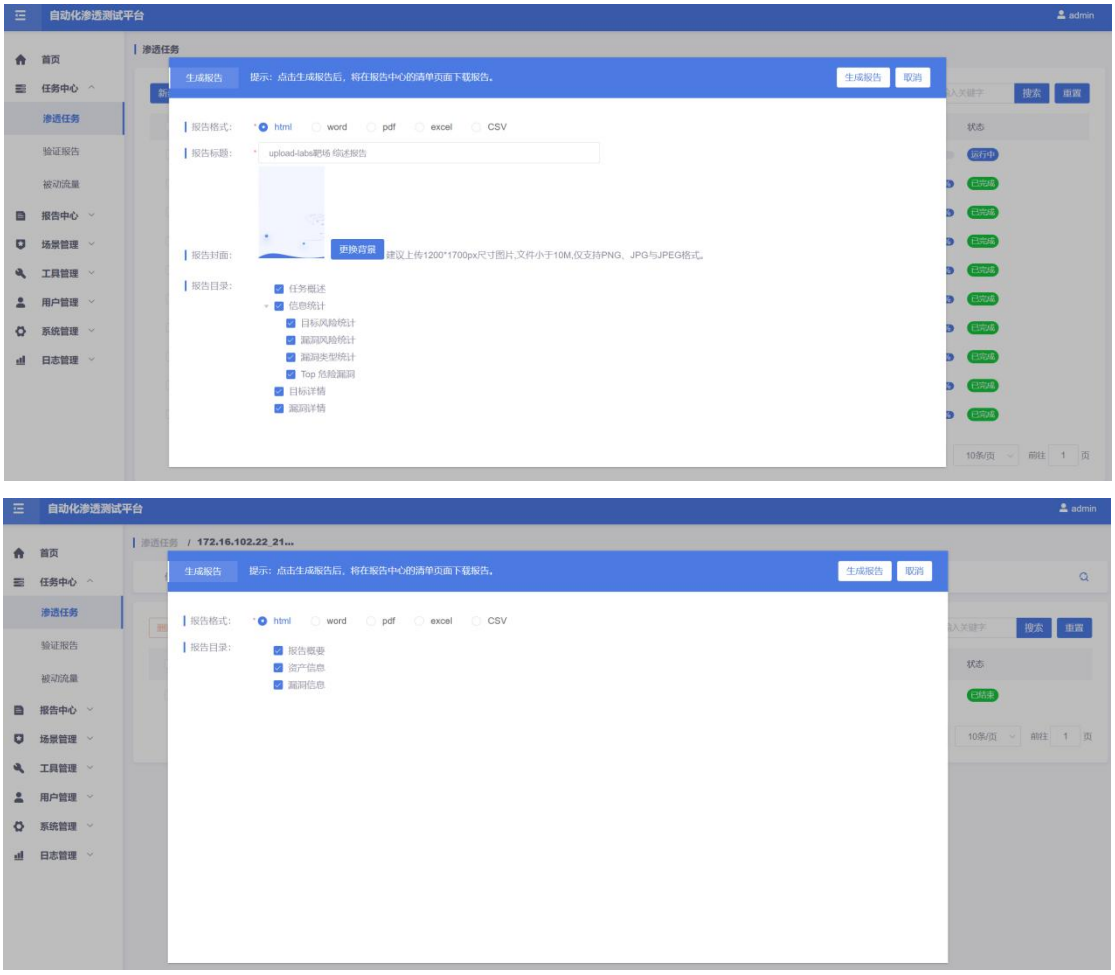


图 9：生成报告配置图

（二十）渗透路径规划

渗透测试过程中，系统能够基于知识图谱和专家系统对收集回来的信息和当前渗透状态进行综合推理决策，分析出当前存在的渗透测试路径，并选择最优渗透测试路径进行渗透测试，提高渗透测试效率。

（二十一）分布式

系统支持分布式部署，可以管理多个渗透节点。创建渗透任务时，可以选择多个渗透节点进行渗透攻击，提高任务执行效率，同时也可以选择指定的渗透节点对特定网段的目标进行渗透测试。

（二十二）半自动化渗透

半自动化渗透是指在用户可参与到运行的渗透任务中，可手动添加目标、漏洞、攻击面等攻击知识，同时系统将根据增加的知识自动进行测试。

（二十三）内网横向移动

系统支持通过获取到系统权限的测试目标能够上传远控工具，抓取用户信息、网卡信息、系统版本、进程信息、端口信息、环境变量等，并且可以通过远控目标为代理跳板实现内网进行横向移动。

（二十四）盲测平台

系统支持 HTTP/TCP、DNS 盲测平台，能够对无法回显的漏洞进行测试。系统支持配置自定义盲测平台。

（二十五）代理功能

系统可以通过代理服务器对测试目标进行渗透测试，支持的代理类型包括 HTTP、HTTPS 和 Socks5。

（二十六）OpenVPN

系统支持基于 OpenVPN 的远程接入检测，通过 OpenVPN 可以对内外网隔离环境的系统进行渗透测试。

（二十七）被动流量

被动流量模块主要用于监控和分析网络流量，通过代理用户流量的方式，有效地监听和采集网络通信数据，以便于进行深入安全分析与评估。

三、产品特色

3.1 关键技术

“小智-智能渗透测试机器人”基于模块化设计方案，采用先进的专家系统、知识图谱等技术，保障了小智-智能渗透测试机器人的先进性。

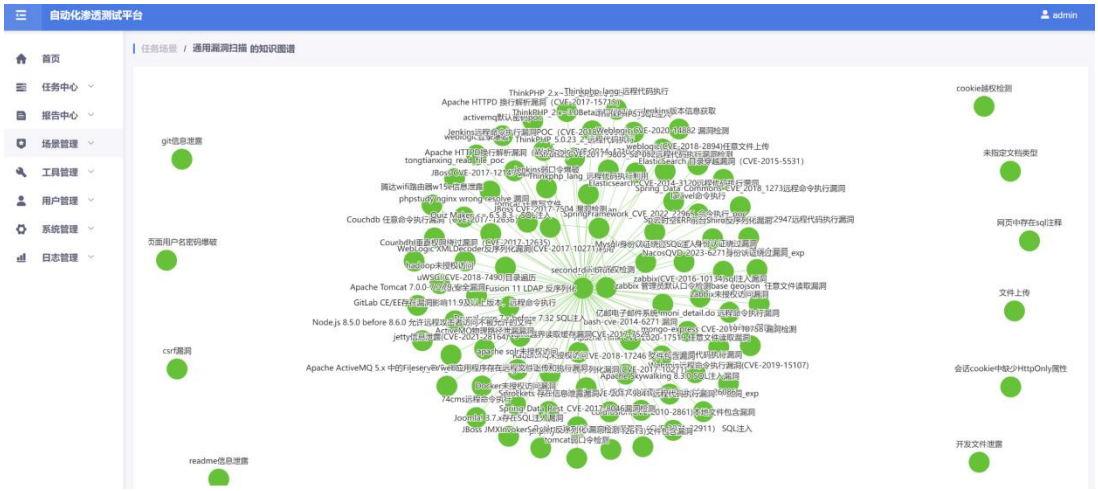
（一）专家系统

专家系统是一种模拟人类专家解决领域问题的计算机程序系统，其内部含有大量的特定领域专家知识与经验。它能够利用特定领域一个或多个专家提供的知识和经验，进行推理和判断，模拟人类专家的决策过程，以便解决那些需要人类专家处理的复杂问题。渗透专家经验是把黑客在渗透测试过程中的思路和方法转化成计算机能够识别、存储、执行渗透测试规则。渗透测试时，系统通过渗透专家经验分析推理收集到的渗透数据，实现渗透过程的决策规划。

（二）知识图谱

知识图谱是揭示实体之间关系的语义网络，它通过把所有不同种类的信息连接在一起得到一个关系网络，从而揭示知识领域的动态发展规律，提供了从“关系”的角度去分析问题的能力。知识图谱的关联性能够重构渗透测试流程，它将“信息收集”、“漏洞探测”、“漏洞利用”、“后渗透”等渗透测试过程产生的信息进行再次组合，从而重复驱动其他渗透测试步骤，能够有效提高渗透测试的全面性。

知识图谱的关联性也可以将专家经验进行关联，使专家经验成为知识图谱中的渗透节点，通过渗透节点的关联性，系统能够产生出多条渗透路径，通过节点间权重关系，能找到最快的渗透路径实现渗透路径规划。



渗透知识图谱

3.2 产品价值

基于专家系统和知识图谱技术的“小智-智能渗透测试机器人”实现自动化渗透测试、渗透路径规划，同时提高了漏洞检出率高、误报率低等。

自动化渗透测试

“小智-智能渗透测试机器人”能够自动化完成从信息收集、漏洞验证、漏洞利用、输出报告的渗透测试全过程。基于知识图谱的关联性，渗透测试各阶段能够将渗透测试过程产生的数据重用，实现渗透测试流程重构，提高渗透测试全面性。另系统支持定时和周期执行，可实现对不同类型的目标进行持续性、常态化资产漏洞渗透测试，能够减少渗透测试人员工作量，提高渗透测试效率。

漏洞检测更全面

“小智-智能渗透测试机器人”通过知识图谱能够对漏洞进行组合利用和链式利用。通过漏洞组合利用，能够实现将多个低危漏洞组合成高危漏洞，达到 1+1>2 的渗透测试效果。通过漏洞链式利用方式实现对漏洞深入探测和利用，实现在单漏洞上再发现漏洞。通过漏洞组合利用和漏洞链式利用能够有效提高渗透测试的全面性。

漏洞误报率低

“小智-智能渗透测试机器人”采用专家系统进行漏洞检测，能够有效降低漏洞误报率。专家系统通过专家经验对检测到的漏洞进行多维度多角度的推理分析，可有效降低传统工具因版本匹配和渗透测试人员经验不足导致的漏洞误报率高的问题，实现精准、快速、低误报的漏洞检测。

渗透路径规划

“小智-智能渗透测试机器人”在渗透测试过程中，系统能够根据收集回来的信息和历史渗透测试的状态来分析判断当前的渗透测试状态，并通过知识图谱和专家系统进行联合推理决策，选择最优渗透测试路径进行渗透测试，提高渗透测试效率。并且系统能够将渗透过程的思路、步骤、执行的操作以渗透图的方式展示，从而实现渗透测试过程的思路和步骤重现，为渗透测试人员提供渗透思路。

四、产品部署方式

产品能够固部署在机房的传统服务器上，也可部署在云平台上。

4.1 固定部署

固定部署方式是将产品部署在机房，主要用于测试检测单位内部网络的部署，且对并发渗透测试数量不大的情况。部署时将设备固定在服务器机架上，同时将设备的网络接口连接到交换机端口上，只要被测目标和系统网络可达，即可实现对被测目标进行检测。

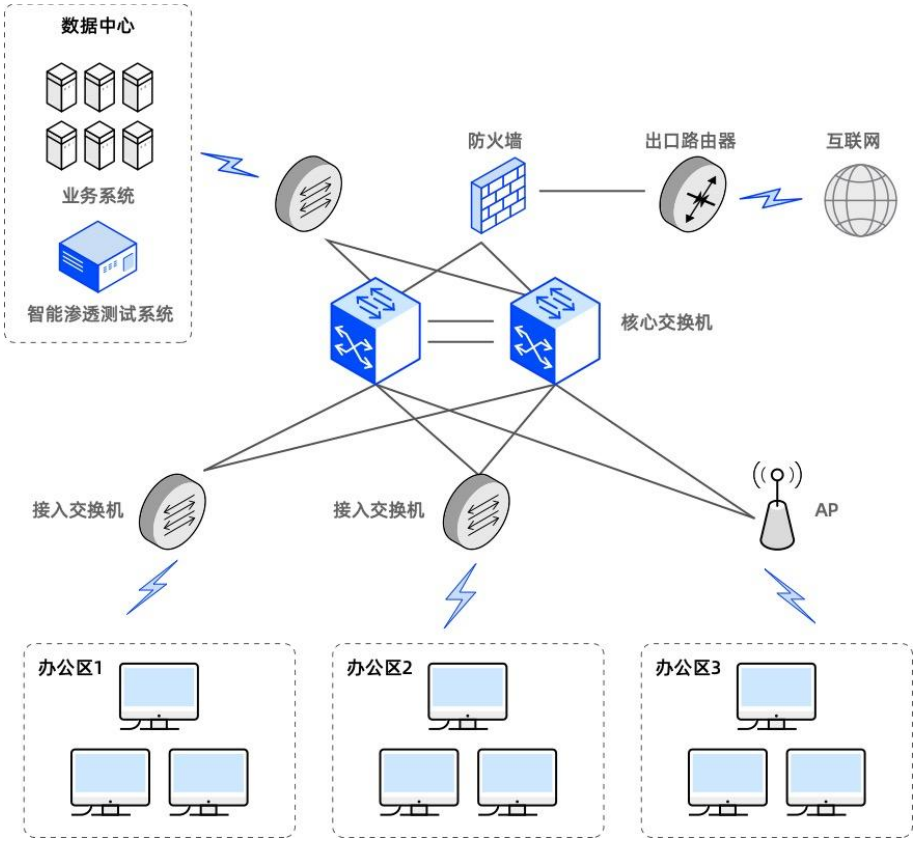


图 10：小智-智能渗透测试机器人-固定部署图

4.2 云端部署

云部署是将系统部署在云服务器上，主要用于客户对于并发量需求较大，且对并发需求有扩展的情况。部署时将系统安装在云主机上，配置好系统的 IP，确保云主机能够连接到网络上，只要被测目标和系统网络可达，即可实现对被测目标进行检测。

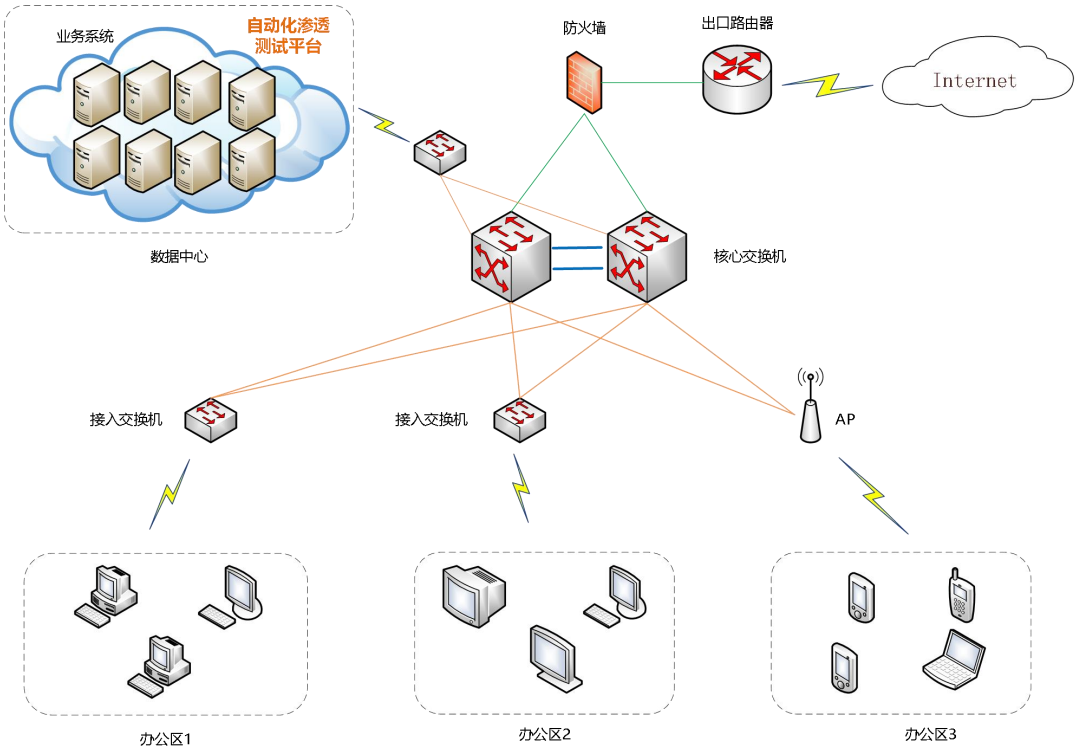


图 11：小智-智能渗透测试机器人-云端部署图

五、典型应用场景

（一）新系统上线前检测

运营商/能源/税务/金融等单位的新系统上线前需要通过渗透测试来发现系统上存在的安全隐患。每年上线的新系统多，而小版本更新的系统更多，但因为安全人员有限，仅能够对核心业务系统上线前渗透测试，普通和更新的系统几乎没有资源进行检测，导致很多系统本身带漏洞上线。通过"小智-智能渗透测试机器人"的自动化渗透测试，能够少量渗透测试人员介入的情况下，就能对其他系统进行渗透测试，从而实现快速高效的发现系统薄弱点后，及时进行薄弱点修复，实现新上线系统的安全性可靠性。

（二）日常安全检测

运营商/能源/税务/金融等单位需要定期对内部业务系统进行渗透检测，以便发现系统中存在的漏洞。目前此类单位面临着安全人员少，且专业水平不均衡等问题，导致安全人员渗透测试工作量，且很多系统检测不到，检测效果一般。通过"小智-智能渗透测试机器人"的周期性渗透测试的特性，能够实现对资源漏洞的周期性监控与检测，达到提高渗透测试效率和全面性，同时某种程度上减少安全人员的工作量。

（三）突发漏洞检测

市面上爆发风险高、影响普通漏洞时，一般需要渗透测试人员手动排查当前系统是否存在爆发的漏洞。通过手工排查漏洞工作量大，且对安全人员的水平要求较高。通过"小智-智能渗透测试机器人"的自动化漏洞检测功能和持续更新的漏洞库，能够快速检测出系统中哪些资产存在新爆发的高风险漏洞，能够有效提高排查资产漏洞的效率。

（四）重大活动前检测

政府、金融、大型央企一般会在重大活动前进行安全检测，从而实现所有的业务系统在重大活动期间不被外界入侵。因为重大保障时间紧，要检测的系统多，而自有的安全人员少，不得不外包安全公司进行渗透测试，因此面临着安全检测的成本高。通过"小智-智能渗透测试机器人"自动化检测能力，能够对内部业务系统进行批量渗透检测，从而提高渗透测试效率，降低对外包安全公司的依赖，降低安全检测的成本。

（五）执法检测

公安/网信办需要对所辖区域内的网络进行安全性检测。当前执行网络安全检测的主要依靠基层民警，但基层民警的网络渗透专业性较弱，且缺乏有效的安全检测手段，因此执法效果差，较难体现出安全执法检测的权威性。通过"小智-智能渗透测试机器人"对辖区内的网络进行大规模的渗透检测，能够有效检测到网络安全漏洞。同时也可使用便携式版本，到被测单位进行检测，实现现场安全执法检测。

六、产品案例

小智-智能渗透测试机器人已服务于公安、军队、银行、能源等多个行业。根据客户反馈信息，其能够降低渗透测试人员工作量，提高渗透测试效率，降低漏洞检测的误报率。

案例一：国家电网

某国网公司业务系统多，具备渗透测试能力的安全人员较少，因此为完成系统的渗透安全检测，除自己的安全人员加紧检测外，不得不外包安全公司进行检测，极大的增加了安全检测的成本。

为降低渗透测试的成本，减轻渗透测试人员工作压力，公司 2024 年通过采购小智-智能渗透测试机器人。

当前"小智-智能渗透测试机器人"的应用场景主要在新上线的系统测试和日常业务系统测试。通过"小智-智能渗透测试机器人"的自动化渗透测试，实现了对新上线系统和版本更新系统的上线前渗透测试。通过自动化渗透测试能够有效发现系统的薄弱点；通过定时任务和周期任务实现了对业务系统的日常安全检测。自动化渗透测试减少了安全人员的工作量，同时提高了渗透测试效率，降低了渗透测试成本。

案例二：工信部研究所

工信部研究所面临着保障 Web 应用系统安全的严峻挑战。传统的渗透测试方式存在工具零散、漏洞检测深度不足、过程不可控以及专业人才短缺等问题，导致网络安全维护成本高、效率低。在此背景下，工信部研究所亟需一套全面、高效的安全检测系统，以保护 Web 应用系统的安全稳定运行。

小智在该项目中的应用场景主要是对在运行的信息系统进行风险探测。它能自动建模业务逻辑、生成定制化攻击载荷，并在多轮交互中优化检测策略，适用于 Web 应用系统的安全检测。

在实际应用中，小智全面覆盖了 Web 应用系统的安全检测需求，涵盖从信息收集、漏洞探测、验证利用到后渗透再到完成报告输出的全渗透测试流程，用户只需输入目标即可一键完成测试，避免了多工具协同带来的困扰。小智基于知识图谱和智能决策引擎，显著提升了逻辑漏洞与零日漏洞的发现能力，降低了系统被攻击的风险。全方位提升了研究所 Web 应用的安全防护水平，通过可视化路径和节点详细信息，提升了安全团队整体能力。

案例三：联通某省公司

联通某省公司现有的安全防护体系面临着诸多挑战。随着网络攻击手段的持续升级和产业化，传统的被动防御手段已难以满足日益增长的威胁检测与响应需求。攻击面不断扩大，防护成本逐年增加，攻防不平衡的现状亟需变革。

公司内部已经部署了众多网络安全厂商的设备，也开发了一些管理平台，但网络安全厂商较多，相关系统没有统一的调度管理，无法满足公司内部在重大活动保障期间对众多资产的漏洞快速排查和漏洞安全预警工作。

引入小智 AI 智能渗透测试机器人后，深入解决多种复杂场景，漏洞覆盖率提升至 95% 以上，有效杜绝了“已知漏洞未整改”和系统“带病上线”的情况。检测时间减少了 70% 以上，测试准确率高达 98%，提升了联通某省公司网络安全防护的效率和深度，实现了从被动防御到主动检测和响应的转变，安全运维的效率提升了 3 倍。

万径安全
MegaVector

万径安全公众号

010-5945 6626（北京）
北京市海淀区 上地街道 金隅嘉华大厦 F座804
market@4dogs.cn
http://megavector.cn