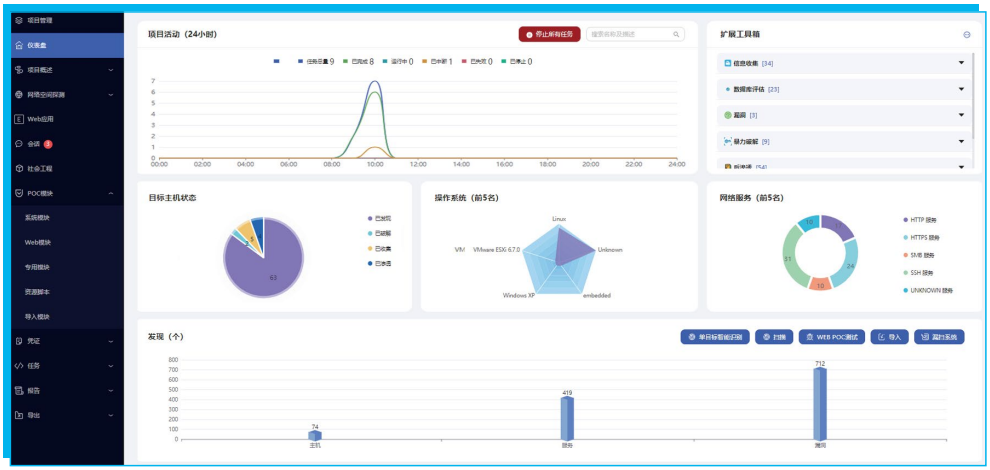
碳泽 TANZE

碳泽摇光自动化渗透测试系统

自动化渗透测试 | 网络空间探测 | 漏洞验证 | 社会工程学 | 弱口令 | 流程编排 | 综合报告

碳泽摇光自动化渗透测试平台能够提供快速自动化渗透测试能力，系统包含了丰富的模块，可以模拟真实的攻击过程，针对系统主机、网络设备等进行安全测试，帮助组织快速排查自身存在的风险。可导入第三方报告进行验证漏洞，并通过社会工程学功能提高员工安全意识。



碳泽摇光自动化渗透测试系统界面

01 产品功能特色

摇光自动化渗透测试平台，基于 B/S 架构，**能够让渗透测试人员快速开展大范围的渗透测试工作。**同时，综合了多种安全测试模块和组件，能够有效的帮助组织完成社工测试、暴力破解等多种工作:

自动化渗透测试
- 支持批量渗透测试
- 支持计划任务，可依据脚本完成自动化渗透测试
- 支持测试目标安全性设定
- 基于互联网的域名进行网络空间探测测绘，发现脆弱点风险辐射

APT攻击测试
- 钓鱼邮件攻击测试
- USB后门测试
- 病毒、后门加壳测试
- 跳板攻击

暴力破解
- 多协议暴力破解
- 支持自定义密码字典
- 支持密码变体
- 支持密码重用测试
- 支持设定测试频率

漏洞验证
- 支持远程调用"玉衡"发起扫描，导入扫描结果
- 验证结果回推"玉衡"
- 第三方报告导入
- 丰富的渗透测试模块

防护方案有效性测试
- 载荷生成及加壳
- 攻击测试代码混淆
- 多功能网络攻击模块
- 多种文件格式攻击模块
- 全开放全功能API

基于项目的测试协同
- 多用户协同工作
- 项目数据共享，多模块调用
- 自动构建攻击拓扑
- 计划任务，定时开启
- 详细的操作日志
- 测试状态实时查看
- 渗透测试链条设定固定工作流

丰富多样的报告
- PDF、HTML、WORD
- 自定义报告

后渗透测试
- 远程控制、获取信息
- 键盘记录、桌面截图
- 上传文件等多种动作
- 海量后渗透测试模块

02 应对渗透测试难题

在频发的安全事件催化下，信息安全已经上升至国家战略高度。信息安全保障措施中安全测试评估是必不可少的一环。国家网络安全法的第三十八条就规定了“关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估”。而从每年频繁暴露的重要安全漏洞及相关事件可以得知：**持续性的安全测试评估才能在达到有效的安全防御效果。**

在渗透测试领域普遍存在的关键问题：

Q1 是否能够找到具有良好技术能力的渗透测试人员？

Q2 是否能确保渗透测试人员的自身素养并符合保密要求？

Q3 是否拥有足够的预算维持渗透测试团队的稳定？

在安全检测评估技术中，渗透测试被广泛认为是对系统安全性的良好检验，因为它比较接近真实世界的攻击。执行这些测试通常需要技术娴熟的人员花费大量时间来执行，并且在理想情况下，执行这些测试的工程师需要达到或者超过潜在攻击者的技能水平。

因此，使用自动化渗透测试平台有几个关键的好处：

快速验证

当新漏洞出现时，自动化软件提供了较快速的渗透验证速度。

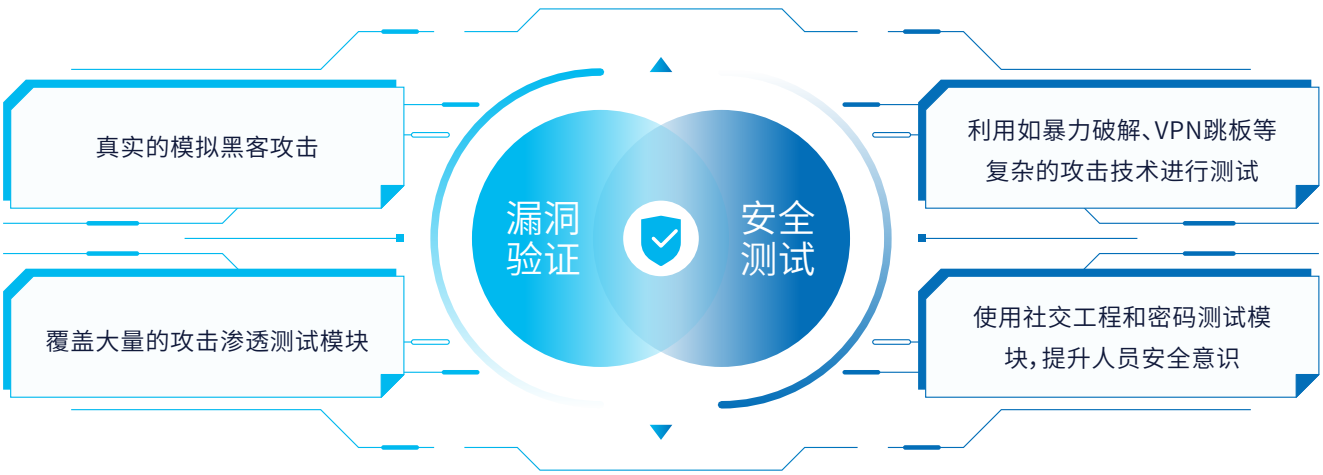
丰富准确

自动化工具可以广泛测试大量系统中很多已知的安全漏洞，而不需要繁琐的手动渗透过程。

节省人力

自动化工具减轻了高技能人员繁琐的工作，让他们可以运用其专业知识在较重要的工作上。

03 安全测试和漏洞验证



上海碳泽信息科技有限公司
Shanghai Tanze Info Tech Co., Ltd
电话：400-1788-258
网址：www.tanze.net.cn
销售咨询：sales@tanze.net.cn
技术支持：support@tanze.net.cn