碳泽摇光安全深度测试平台

渗透测试、社交攻击、弱口令、漏洞验证、自动测试流程、综合报告的自动化平台

全功能自动化渗透测试平台（包含MetaSploit社区全部测试模块）

自动化渗透测试

- 涵盖所有MetaSploit渗透模块
- 支持批量渗透测试任务
- 支持渗透测试计划任务
- 测试自动向导，无干预模式
- 支持测试安全性设定

APT攻击测试

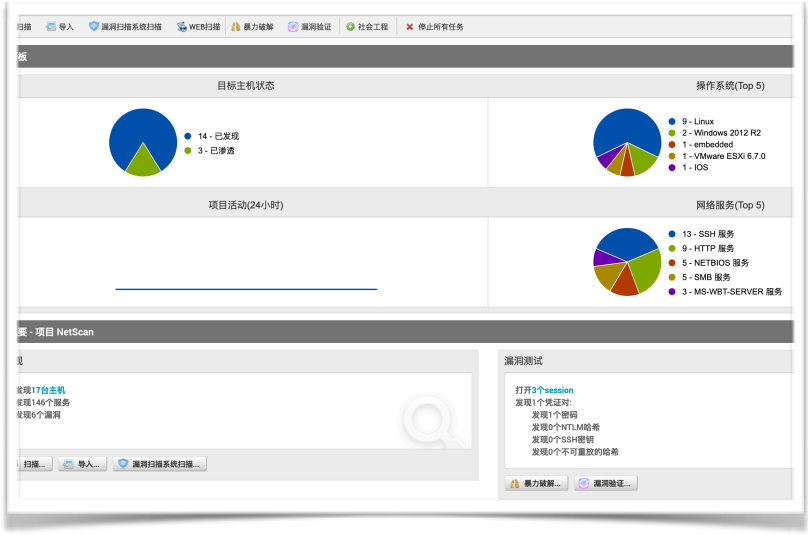
- 钓鱼邮件攻击测试
- USB后门测试
- 病毒、后门加壳测试
- VPN跳板攻击

暴力破解

- 多协议暴力破解
- 支持自定义密码字典
- 密码重复利用测试
- 支持设定测试频率

漏洞验证

- 第三方报告导入
- Nexpose/Nessus/Qualys
- AWVS/APPSCAN/BurpSuite
- 包含漏洞扫描模块及Web爬取



应对渗透测试难题：

在频发的安全事件催化下，网络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。

在安全检测评估技术中，渗透测试被广泛认为对系

防护方案有效性测试

- 载荷生成及加壳
- 攻击测试代码混淆
- 超过300种后攻击模块
- 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

全面的渗透后测试

- 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
- 超过300种后渗透测试模块

丰富多样的报告

- PDF、HTML、WORD
- 自定义报告

统安全性的最好检验，因为它最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。

在渗透测试领域，客户不妨问自己几个关键的问题：我能够找到具有良好技术能力的渗透测试人员吗？我能确保渗透测试人员的自身素养并符合保密要求吗？我有足够的预算维持渗透测试团队的稳定吗？

因此，使用软件自动化进行渗透测试有几个关键的好处。首先，当新漏洞出现时，自动化软件提供了更快速的检测速度。其次，自动化工具可以广泛测试大量系统中很多已知安全漏洞，而不需要繁琐的手动测试过程。最后，自动化工具减轻了高技能人员繁琐的工作，让他们可以集中精力来协调测试以及运用其专业知识在最重要的地方。

最真实的安全测试和漏洞验证：

销售联系邮箱：sales@tanze.io
联系电话：400-1788-258