渗透测试服务介绍

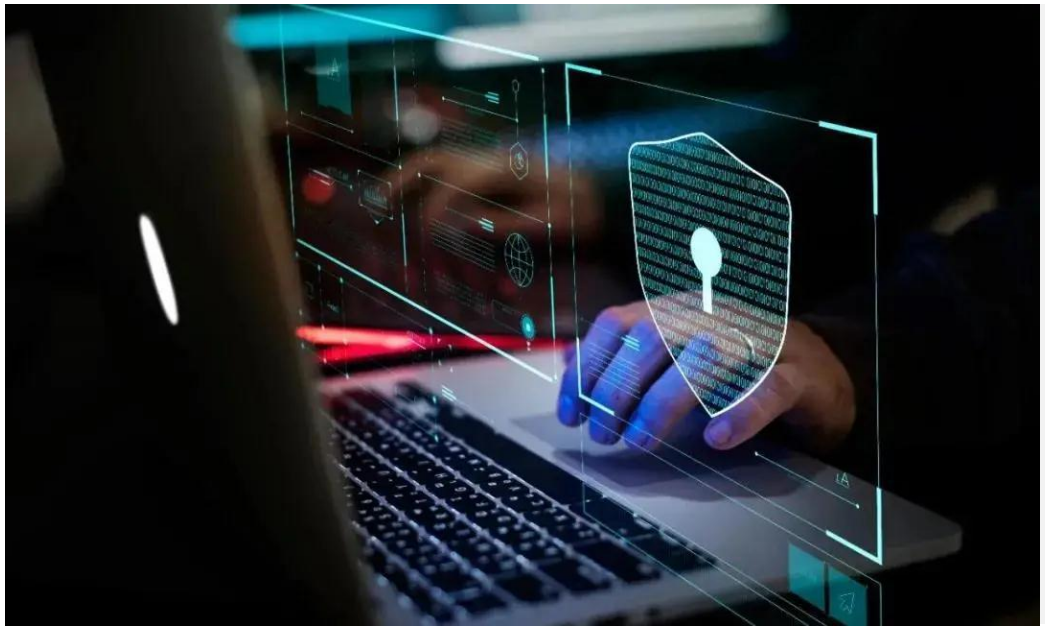
2023年6月

目录

01

背 景 介 绍

渗透测试背景介绍



“渗透测试”是完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全做深入的探测，发现系统最脆弱的环节。渗透测试和黑客入侵最大区别在于渗透测试是经过客户授权，采用可控制、非破坏性质的方法和手段发现目标和网络设备中存在弱点，帮助安全运营人员了解其网络或信息系统所面临的问题。

用户需求

合规场景

应对网络安全检查

业务场景

系统上线前安全检测

事件场景

避免被主管或监管单位通报

重保场景

提前发现系统弱点

渗透测试目的

验证风险	解决问题	规划依据	结果明显
针对客户重点业务系统渗透测试作为发现、验证系统风险重要手段	渗透测试模拟黑客事件能从中找出企业最急需解决的安全问题	渗透测试和工具扫描的结果一起为日后的安全加固安全规划等提供重要数据	渗透测试以非常明显直观的结果反映出系统的安全现状越来越受到国际/国内信息安全业界的认可和

02

服 务 介 绍

渗透测试服务流程


项目启动会
渗透测试调研
制定渗透测试方案
渗透测试授权
渗透测试实施
输出渗透测试报告
回归测试
输出回归测试报告

渗透测试分类方法

黑盒测试

渗透者完全处于对系统一无所知的状态。通常，这种类型的测试，最初的信息获取来自DNS、Web、Email及各种公开对外的服务器。

白盒测试

测试者可以通过正常渠道向被测单位取得各种资料，包括网络拓扑、员工资料甚至网站或其他程序的代码片段，也能与单位其他员工进行面对面的沟通，这类的测试目的是模拟企业内部雇员的越权操作

隐秘测试

隐秘是针对被测单位而言的。通常，接受渗透测试的单位网络管理部门会收到通知: 在某些时间段进行测试。因此能够检测网络中出现的变化。但在隐秘测试中，被测单位也仅有极少数人知晓测试的存在，因此能够有效地检验单位中的信息安全事件监控、响应、恢复做的是否到位。

渗透测试服务内容


信息收集
爬虫、搜索引擎
DNS及域名信息
github信息泄露
域名安全问题
人员敏感信息泄露
用户敏感信息泄露
网络安全
漏洞扫描
暴力破解
网络设计缺陷
安全策略缺陷
配置缺陷
系统安全
账户安全
端口安全
进程安全
软件漏洞
木马病毒
应用安全
SQL注入
命令执行
XSS/CSRF深度利用
设计/配置缺陷
未授权访问
文件任意上传
任意文件读取
文件包含
后台弱口令
接口暴力破解
越权漏洞
插件漏洞
数据安全
资产泄露
信息泄露
未经授权访问
越权访问
API安全
登录认证
认证授权
接口调用安全
访问控制
中间件安全
未授权认证
反序列化漏洞
数据库安全
SQL注入
命令执行
版本较低
补丁未及时修复
配置不当

渗透测试目标分类

主机操作系统渗透

对Windows、Solaris、AIX、Linux、SCO、SGI等操作系统进行渗透测试。

数据库系统渗透

对MS-SQL、Oracle、MySQL、Informix、Sybase、DB2等数据库应用系统进行渗透测试。

内网测试

内网测试指的是测试人员从内部网络发起测试，这类测试能够模拟内部违规操作者的行为。主要的“优势”是绕过了防火墙的保护。内部主要可能采用的渗透方式：远程缓冲区溢出，口令猜测，以及B/S或C/S应用程序测试（如果涉及C/S程序测试，需要提前准备相关客户端软件供测试使用）。

外网测试

外网测试指的是测试人员完全处于外部网络（例如拨号、ADSL或外部光纤），模拟对内部状态一无所知的外部攻击者的行为。包括对网络设备的远程攻击，口令管理安全性测试，防火墙规则试探、规避，Web及其它开放应用服务的安全性测试。

网络设备渗透

对各种防火墙、入侵检测系统、网络设备进行渗透测试。

应用系统渗透

对渗透目标提供的各种应用，如ASP、CGI、JSP、PHP等组成的WWW应用进行渗透测试。

渗透测试风险规避

01 在渗透测试中不使用含有拒绝服务的测试策略

02 渗透测试时间尽量安排在业务量不大的时段，避开业务高峰期

03 在渗透测试过程中如果出现被评估系统没有响应的情况，应当立即停止测试工作，与用户相关人员一起分析情况，在确定原因后，并待正确恢复系统，采取必要的预防措施（比如调整测试策略等）之后，才可以继续进行

04 测试人员会与用户网站系统和安全管理人员保持良好沟通，随时协商解决出现的各种难题

05 由渗透测试方对本次测透测试过程中的三方面数据进行完整记录：操作、响应、分析，并形成完整有效的渗透测试报告提交给用户

服务价值

发现安全隐患

渗透测试是一个从空间到面再到点的过程，测试人员模拟黑客的入侵，从外部整体切入最终落至某个威胁点并加以利用，最终对整个网络产生威胁，以此发现整个系统中的安全隐患点。

提高安全意识

任何的隐患在网络安全中都可能造成"千里之堤溃于蚁穴"的效果，渗透测试的结果可作为内部安全意识培养的案例，在对相关的管理人员进行安全教育时使用这些案例，可有效督促管理人员提高安全意识，从而降低整体风险。

明晰安全现状

渗透测试报告有助于用户以案例的形式说明组织目前的安全现状，协助用户发现组织中的安全最短板，从而提升组织信息建设的步伐。

服务优势

知识沉淀

高端网络攻防专家的经验固化到半自动化渗透工具中，形成标准化的渗透流程规范，让大量渗透人员具有高水平的服务效果。

深度检测

深度测试在用户授权允许下尝试利用漏洞，直观体现漏洞破坏力，更多考虑多点之间联动互相影响产生的漏洞以及业务功能的逻辑漏洞。

指导建设

根据实践总结的常见暴露点进行全面测试，以尽可能全面的发现暴露点，全面识别安全隐患，指导组织后期补全业务系统漏洞，提升安全健壮度。

03

服 务 案 例

服务案例

石 油

- 中石油集团
- 昆仑数智
- 新疆油田
- 大庆油田
- CNODC
- 昆仑能源
- 中石油尼日尔
- 西南油气田
- 西南管道

石化

- 中石化集团
- 石化盈科
- 普光油气田
- 江汉油田
- 胜利油田
- 中原油田
- 中科炼化

海油

- 中海油
- 海油信科
- 海油伊拉克
- 中海油湛江
- 中海油天津

其他

- 五矿/中冶
- 中电建
- 中储粮
- 中航工业
- 钢研科技集团
- 国家管网


谢谢聆听
THANKS LISTENING