安全宝渗透测试服务白皮书

公司介绍

星云融创（北京）科技有限公司成立于 2011 年，公司由具有超过 10 年安全产品研发运营经验的团队构成。安全宝是国内第一款真正基于云计算架构实现的网站在线保护和加速服务产品，是李开复先生创办的创新工场旗下第一家拿到 B 轮融资的公司，累计融资规模超 1 亿。

在未来，安全宝将继续专注于公共计算时代的互联网安全和速度问题，努力为用户提供最好的云安全服务。

1 渗透测试简介

安全宝聘请全职的安全专家，在用户的授权下，以模拟黑客攻击的方式，用黑客的思维进行渗透尝试，验证黑客可能利用的漏洞，测试网站的安全性，发现系统的脆弱点，帮助用户理解黑客是如何思考的，比黑客更早的发现漏洞。
渗透测试是一种专业的安全服务。

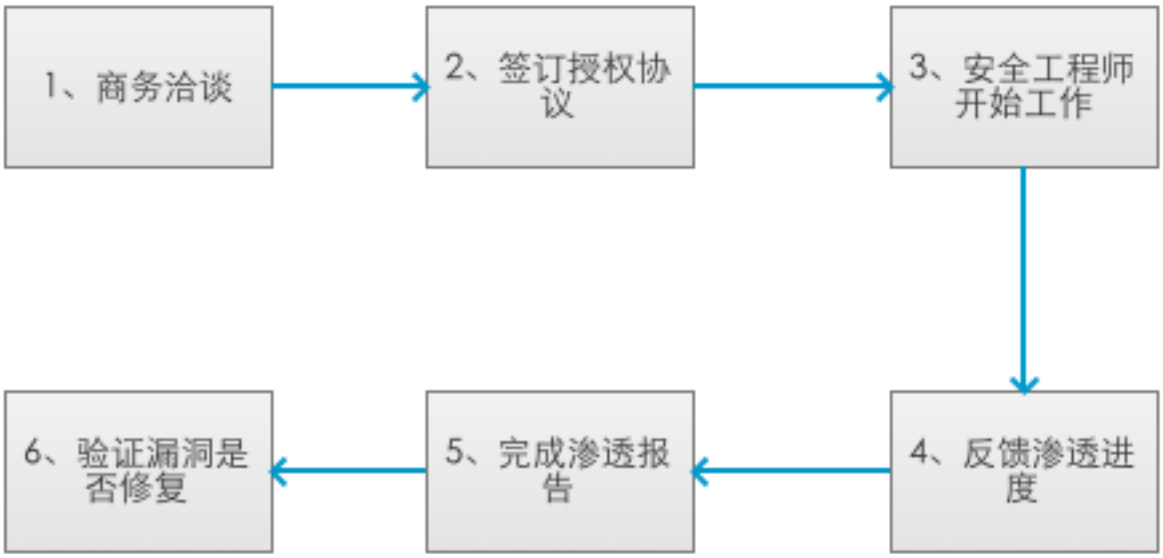
通过模拟黑客的渗透测试，评估目标系统是否存在可以被攻击者真实利用的漏洞以及由此引起的风险大小，为制定相应的安全措施与解决方案提供实际的依据

2 渗透测试的必要性

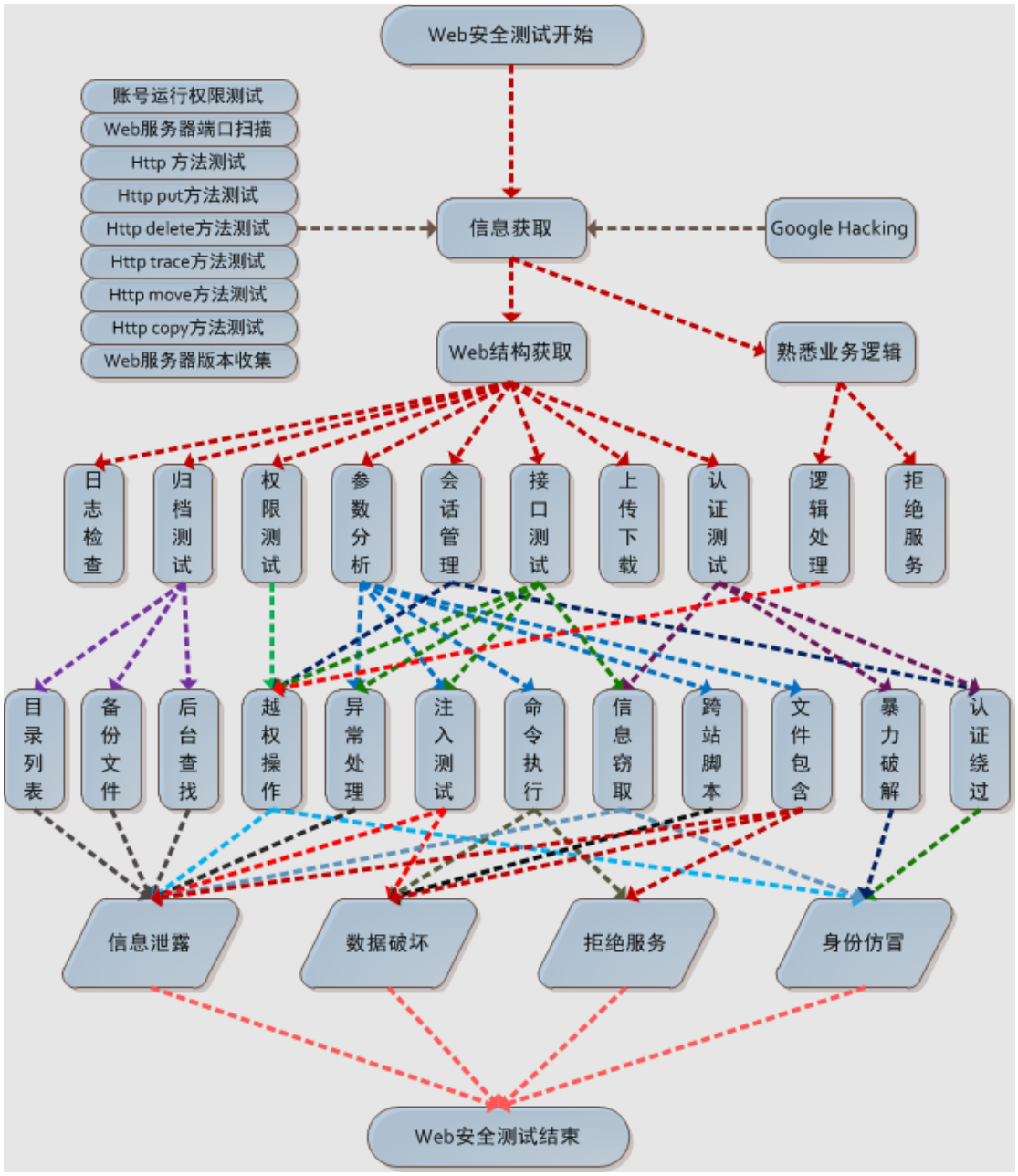
渗透测试是具有丰富经验的安全工程师对服务器、网络设备、防火墙、应用等进行非破坏性质的模拟黑客攻击，目的是侵入系统并获取机密信息并将入侵的过程和细节产生报告给用户。

渗透测试和工具扫描可以很好的互相补充。工具扫描具有很好的效率和速度，但是存在一定的误报率和漏报率，并且不能发现高层次、复杂、并且相互关联的安全问题；渗透测试需要投入的人力资源较大、对测试者的专业技能要求很高（渗透测试报告的价值直接依赖于测试者的专业技能），但是非常准确，可以发现逻辑性更强、更深层次的安全风险点。

3 渗透测试服务流程



4 渗透测试的基本过程


Web安全测试开始
账号运行权限测试
Web服务器端口扫描
Http 方法测试
Http put方法测试
Http delete方法测试
Http trace方法测试
Http move方法测试
Http copy方法测试
Web服务器版本收集
信息获取
Google Hacking
Web结构获取
熟悉业务逻辑
日志检查
归档测试
权限测试
参数分析
会话管理
接口测试
上传下载
认证测试
逻辑处理
拒绝服务
目录列表
备份文件
后台查找
越权操作
异常处理
注入测试
命令执行
信息窃取
跨站脚本
文件包含
暴力破解
认证绕过
信息泄露
数据破坏
拒绝服务
身份仿冒
Web安全测试结束

5 渗透测试的工作范围

5.1 主机操作系统渗透

对 WINDOWS、SOLARIS、AIX、LINUX、SCO、SGI 等操作系统本身进行渗透测试。
Windows 系列操作系统漏洞包括:

1) 端口扫描
2) NetBIOS name service 测试
3) RFC 漏洞攻击
4) SMB 漏洞攻击
5) Windows DNS 测试
6) Snmp 漏洞测试
7) 活动目录测试
8) Sql Server 弱口令测试
9) 系统弱口令测试
10) 终端服务弱口令测试
11) IIS 权限及溢出测试
12) Exchange server 漏洞测试
13) ftp 弱口令测试

*nix 系列渗透测试包括:

1) 端口扫描
2) ssh 弱口令测试
3) telnet 弱口令测试
4) Ftp 弱口令测试
5) Samba 弱口令测试
6) RPc 枚举和漏洞测试
7) NFS 漏洞测试
8) Snmp 漏洞测试
9) DNS 漏洞测试
10) rlogin,rsh 漏洞测试

5.2 数据库系统的测试

对 MS-SQL、ORACLE、MYSQL、DB2 等数据库应用系统进行渗透测试。 包括:

1) 默认账号及弱口令攻击
2) 存储过程漏洞攻击
3) 数据库运行权限探测
4) 提权漏洞攻击
5) 低版本溢出漏洞攻击

5.3 WEB应用系统渗透

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

Web 脚本及应用测试专门针对 Web 及数据库服务器进行。在 Web 脚本及应用测试中，可能需要检查的部份包括：

1）检查应用系统架构、防止用户绕过系统直接修改数据库
2）检查身份认证模块，防止非法用户绕过身份认证
3）检查数据库接口模块，防止用户获取系统权限
4）检查文件接口模块，防止用户获取系统文件
5） 检查其他安全威胁

5.4 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。包括:

1) Tftp 获取配置攻击
2) 管理界面默认账号密码
3) snmp 读写权限攻击
4) telnet,ssh 默认账号弱口令攻击
5) 低版本溢出漏洞攻击

5.5 对系统业务进行渗透

对系统的核心业务进行安全风险挖掘，包括:

1) 用户安全、恶意注册、盗号风险
2) 支付安全，交易安全
3) 秒杀、排名作弊
4) 垃圾消息

5.6 口令猜解

口令猜测也是一种出现概率很高的风险，几乎不需要任何攻击工具，利用一个简单的暴力攻击程序和一个比较完善的字典，就可以猜测口令。

对一个系统账号的猜测通常包括两个方面：首先是对用户名的猜测，其次是对密码的猜测。

5.7 其它

除了上述的测试手段外，还有一些可能会在渗透测试过程中使用的技术，包括：

1) 社会工程学
2) 客户端攻击

3) 拒绝服务攻击
4) 中间人攻击

6 风险规避与管理

为了尽量规避渗透测试过程中对客户系统的影响，我们将提供以下多种方式来进行风险规避。

6.1 时间选择

为减轻渗透测试对网络和主机的影响，渗透测试时间尽量安排在业务量不大的时段或晚上。 测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

6.2 策略选择

为防止渗透测试造成网络和主机的业务中断，在渗透测试中不使用含有拒绝服务的测试策略。 安全宝工程师都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

6.3 信息控制

安全宝公司内部员工对客户信息通过严格的保密协议进行信息控制，保证客户的敏感信息的安全性。

7. 客户收益

渗透测试是以第三方角度对客户产品的安全性进行检查，可以让用户了解从外部网络漏洞可以被利用的情况。渗透测试是可以帮助用户对目前自己的网络、系统、应用的缺陷有相对直观的认识和了解。

因此，从渗透测试中，客户能够得到的收益至少有：

1) 协助用户发现系统中的安全最短板，协助企业有效的了解目前存在的安全风险；

2) 一份文档齐全有效的渗透测试报告有助于组织 IT 管理者以案例说明目前安全现状，从而增强信息安全的认知程度，甚至提高组织在安全方面的预算；

3) 信息安全是一个整体工程，渗透测试有助于组织中的所有成员意识到自己的岗位同样可能提高或降低风险，有助于提升内部员工的安全意识；

8. 安全宝渗透测试服务的特点

我们确信安全专家的经验是扫描器所不可能替代的。因此为了保证效果，我们的每一次渗透测试都是由安全专家手动实施。

我们的专家团队拥有丰富的安全行业经验。在渗透测试完成后，还会提出可实施性强的专业修复建议，帮助用户真正解决安全问题。

9. 联系我们

服务热线:400-805-4999
传真:010-57525300
邮箱:inquire@anquanbao.com
邮编:100080
地址:北京市海淀区海淀大街 3 号鼎好电子商城 A 座 10 层