链滴

渗透测试方法论

作者：zgzhang
原文链接：https://ld246.com/article/1495709349034
来源网站：链滴

一：

1　渗透测试的种类：

1.1　黑盒测试：在不清楚被测单位的内部技术构造的情况下，从外部评估网络基础设施的安全性。试的市场报价高于白盒测试。

1.2　白盒测试：可以获取被测单位内部资料甚至不公开资料，渗透视野更开阔，测试人员可以以最的工作量达到最高的评估精准度，测试时间/成本以及发现/

解决安全弱点的技术门槛都全面低于黑盒测试。

2　脆弱性评估与渗透测试：

2.1　脆弱性评估与渗透测试：通过分析企业面临的威胁程度，评估内外部的安全性，不仅要揭露有的风险，还要提出多重备选的补救措施，分为内部脆弱性评估

和外部脆弱性评估，但是不管内外，都要用各种攻击模式严格测试资产的安全性，确定应措施的有效性。

脆弱性评估和渗透测试的最大区别在于：渗透测试不仅要识别目标弱点，，还要利用这些点进行漏洞利用/权限提升/访问维护等，渗透测试可能会对生产

环境带来实际的破坏性影响，而脆弱性评估是以非入侵性方式，定性/定量的识别已知安全点。渗透测试的价格高于脆弱性评估。

3　安全测试方法论

3.1　开源安全测试方法论（OSSTMM）：http://www.isecom.org/research/osstmm.html　：际公认的安全测试和安全分析标准，这一方法论把安全

评估工作分为了4个组：范围（scope）/信道（channel）/索引（index）矢量（vector。

OSSTMM总结了多种形式的安全测试，并划分了6个标准种类：盲测（blind）/双盲测（double blind）/灰盒测试（grey box）/双灰盒测试（double

grey box）/串联测试（tandem）/逆向测试（reversal）　在这些种类的应用中，测试对被测目标的了解程度也不尽相同，被测单位也是如此。

3.2　信息系统安全评估框架（ISSAF）：http://www.oissg.org/issaf　:另一种开源的安全性测和安全分析框架，技术评估基准十分全面，可用于测试各种技术和不同流程，但是丰富的内容带来了大副作用，就是要跟上评估领域的技术变化速度，就要频繁更新，相反，OSSTMM受更新影响的幅就较小了许多。

3.3　开放式web应用安全项目(OWASP)：https://www.owasp.org　定期推出其top 10 projec（排名前10位的安全隐患防护守则），网站中还包括测试指南/开发人员指南/代码审计指南，同时OASP社区有大量安全工具。

3.4　web应用安全联合威胁分类（WASC-TC）：评估web应用程序安全性的开放标准，与OWAS标准相似，也从攻击和弱点两方面来讨论问题，但是更深入，划分了不同视图来帮助人们了解web应面临的安全威胁：　枚举视图/开发试图/交叉引用视图，无论何种web应用程序平台，都可使用kali linu的工具集验证/测试WASC-TC提出的常见攻击和常规弱点。

3.5　渗透测试执行标准（PTES）：这个标准由7个阶段的标准组成，事前互动/情报收集/威胁建模漏洞分析/漏洞利用/深度利用/书面报告

4　通用 渗透测试框架

41　范围界定：

42　信息收集：

43　目标识别：

44　服务枚举：

45　漏洞映射：

46　社会工程学：

47　漏洞利用：

48　提升权限：

原文链接：渗透测试方法论

49 访问维护：
50 文档报告：