文章编号：2096-1472(2016)-09-01-03

基于Kali-Linux渗透测试方法的研究与设计

姚 莉， 林科辰，邓丹君
（湖北理工学院计算机学院，湖北 黄石 435003）

摘 要：渗透测试是一种在获得用户或甲方单位授权的情况下，对用户信息系统或目标系统实施漏洞攻击的方法。目前所有渗透测试的技术体系理论工作都处于不断完善和更新中。通过分析黑客攻击行为的完整流程，本文提出一种基于Kali-Linux进行渗透测试的方法，以提高渗透测试效率和能力。本文总结了当前业内被接受程度较高的几大标准技术测试体系理论，通过使用Kali-Linux系统作为平台载体，说明一套完整的渗透测试的思路、流程、步骤和结果输出等为网络管理者提供参考。

关键词：网络安全；安全测试；漏洞评估；Kali-Linux；渗透测试
中图分类号：TP399 **文献标识码**：A

Research and Design of the Penetration Test Method Based on Kali-Linux

YAO Li,LIN Kechen,DENG Danjun
(*School of Computer Science and Technology*,*Hubei Polytechnic University*,*Huangshi* 435003,*China*)

Abstract: The penetration test is a method to attack the user information system or the target system in the case of obtaining the authorization from the user or the first-party organization.At present,all the technical systems of the penetration test are constantly improving and updating.By analyzing the complete process of hacking,this paper puts forward a penetration test method based on Kali-Linux to improve the efficiency and capacity of penetration test.Several standardized technical test systems with high acceptance level in the industry are adopted in the research.Using the Kali-Linux system as the platform,the paper introduces the whole set of design,flow,procedures and result,providing some reference to network administrators.

Keywords:network security;security testing;vulnerability assessment;Kali-Linux;penetration test

1 引言(Introduction)

随着移动互联网的高速发展，计算机系统和数据的安全保障也将面临着日益严峻的考验。截止至2014年底，据《2014中国互联网网络安全报告》得知我国大约有22万余网站及系统被黑客入侵和篡改。其中商业机构网站占75%，政府类占4%，教育机构占1%，其他占20%。近年网站数据泄露事件频发，包括几十省几千万社保人员信息、运营商注册信息、网易邮箱注册用户信息、学信网等知名网站数据的泄露。在网上曝光的用户信息高达数十亿条，甚至有33%的组织不知道自身系统是否受到入侵[1]。网络安全面临着严峻的现实考验，如何保证网络安全已成为尤其重要的严峻课题。

2 渗透测试(Penetration testing)

渗透测试作为信息安全领域中的一种新型防护技术，是通过执行漏洞利用和概念证明(POC或EXP)攻击来证明系统确实存在安全隐患。在获得用户或甲方单位授权的情况下，由专业从事信息安全的相关人员发起攻击行为，同时进行高级安全风险评估，通过完全地真实地模拟黑客的攻击行为和过程，以达到评估计算机系统安全风险级别的目的[2]。渗透测试

基金项目：湖北理工学院科学研究青年项目，项目编号：15xjz03Q；湖北理工学院科学研究青年项目，项目编号：15xjz02Q；湖北理工学院科学研究青年项目，项目编号：14xjz06Q.

用于发现系统潜在的风险或漏洞，以达到加强计算机和网络系统的安全性。让其在使用中免遭攻击，最终目的就是使这些被测系统更加安全[3]。渗透测试因而成为检验一个网络是否安全的一个重要手段，渗透测试技术也成为保障系统和数据安全的一种重要途径。一个完整的渗透测试流程结束以后，后续输出的报告或文档会明确说明发现的系统漏洞及相关细节信息，并给出明确的修复意见。

2.1 渗透测试方法论

对信息系统进行一次安全风险评估是一项专业性极强的工作，评估到什么程度或级别困难指数将会成倍增长。选择使用一些开源的工具和测试方法论，则可大大降低这项工作的技术难度。目前已经有很多开源的安全工具和工具包镜像，Kali-Linux就是其中一个被广泛接受的工具集[4]。渗透测试方法理论当中，有偏向信息安全管理层面的，有偏向安全技术层面的，也有些偏向某些核心指标的。几种业内接受度相对较高的方法论，依次是：

(1)开源安全测试方法OSSTMM。

(2)渗透测试执行标准(PTES)。

(3)开放式Web应用程序安全项目(OWASP)。

(4)Web应用安全联合威胁分类(WASC-TC)。

其中开源安全测试方法(OSSTMM)和渗透测试执行标准(PTES)这两种测试方法更偏向信息评估需求，而开放式Web应用程序安全项目(OWASP)十大Web应用风险和Web应用安全联合威胁分类(WASC-TC)更偏向于Web应用安全方面的测试。由于信息系统微小的变化都可能导致出现意想不到的严重后果，直接影响整个安全测试工作的结果。因此在使用上述方法论的过程中，都必须保证目标环境的完整性。

2.2 Kali-Linux测试方法论

Kali-Linux是一套开源的功能大的操作系统级的工具集，集成了目前众多主流的安全测试、评估和渗透工具。由于各类的工具非常多，在没有合适的方法理论支撑的情况下，扩展或直接使用这些工具进行测试时常出现测试失败或不太令人满意的结果[5]。因此，无论是从管理层面还是技术角度出发，使用一套规范化的、标准化、结构化的测试方法来支撑安全测试过程，是非常重的。Kali-Linux方法论体系中所有的测试过程都可以被切分成若干步骤，具体包括：目标界定、信息收集、发现目标、枚举目标、映射漏洞、社会工程学、漏洞执行、系统提权、持续控制及输出报告归档。Kali-Linux测试流程的示意图如1所示。

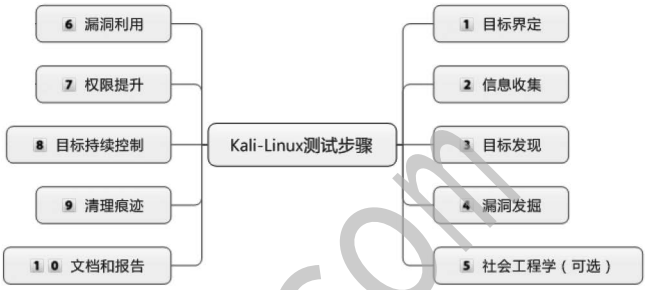

图1 Kali-Linux渗透测试流程

Fig.1 Penetration testing process

3 案例分析(Case analysis)

3.1 执行摘要

测试团队接受客户要求进行渗透测试，测试团队的所有活动都在模拟恶意黑客对客户目标进行针对性攻击，确定其是否存在安全威胁。

(1)确定一个远程攻击者可以穿透用户的安全防御。

(2)确定安全漏洞的影响。

(3)对用户私人数据保密处理。

(4)确定内部可用基础设施和信息系统。

所有测试和行动都根据NIST SP 800-1151标准下进行。主要识别和利用安全漏洞，发现允许远程攻击者对组织数据未授权访问。

3.2 测试过程

(1)对远程系统漏洞挖掘

为了尽可能模拟所有资产在没有确定之前尽可能避免遭到网络攻击，客户提供一个对外信息特别少的组织域名。本次测试首先对域名服务器传送进行测试，发现主机ns2很容易出现DNS区域传送记录。这为测试提供了与主机名和相关联的IP地址和列表，可用于进一步定位客户目标。区域传送可提供有关的详细信息，也可以泄露所有者组织网络范围信息，如图2所示。

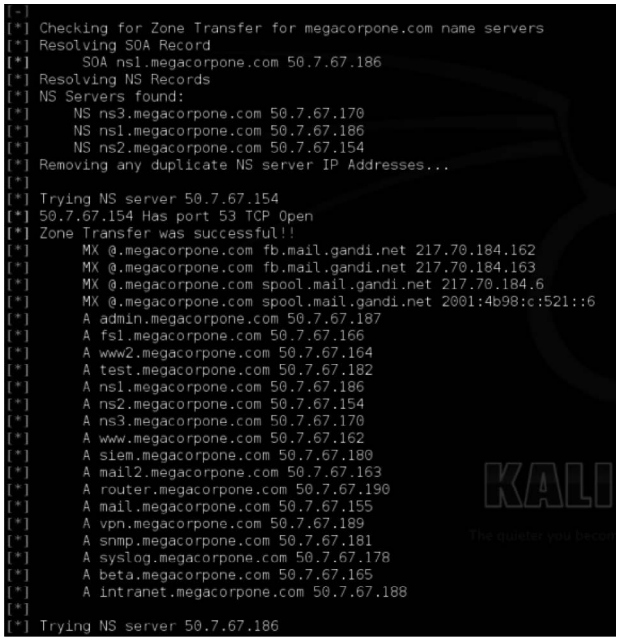

图2 查询DNS服务器传送信

Fig.2 Query DNS server transfer letter

以上主机列表已得到客户验证，由此整个50.7.67.X都纳入渗透测试范围。通过扫描探测这些系统允许服务进行详细审查确定运行的服务，由此确定可能面临的针对性的攻击。通过DNS遍历和网络扫描相结合，能够建立一个探测出客户的网络。该admin二级域名WEB服务器发现在81端口运行Apache服务器。通过访问URL网址显示空白页。接下来进行一次快速枚举扫描系统存在目录和文件，如图3所示。

扫描结果显示与普通的Apache默认文件一起确定一个“/admin”目录后可以开始验证访问。基于用户网站内容，准备针对性的密码破解，整理了自定义字典。经过几轮排列和替换最终筛出为有16201密码的字典。该字典将用于密码破解，用户名使用“admin”尝试进行猜解测试。最终破解出密码为“nanotechnology”。利用这些凭据成功获得对保护部分的未授权访问，如图4所示。

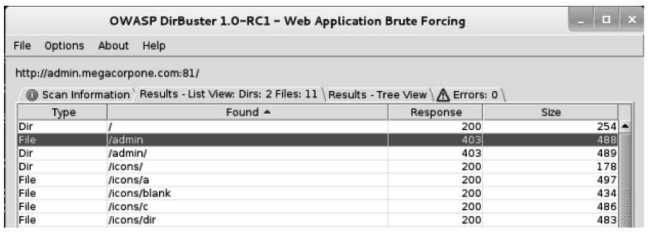

图3 枚举Web服务器文件结构

Fig.3 Enumeration Web server file structure

图4 发现管理员登录入口密码

Fig.4 Found administrator login password

网站管理部分包含SQLite Manager Web，这里是不需要任何其他验证即可访问。利用这个接口，发现是支持管理他网站实际内容的数据库，如图5所示。

图5 SQLite manager web管理SQL数据库

Fig.5 SQLite manager web manage SQL database

通过接口对数据库执行访问获取了用户列表中密码hash值。经检测发现hash值不是常见hash加密，通过下载“phpsqlitecms”程序直接对源代码分析获得系统的密码hash生成方法。方法是利用一个十位字符散列的hash值，再拼接原始的散列与字符串一起存入到数据库中。根据上述方法，采用同样的hash值散列来暴力破解密码并尝试破解其他账户。使用相同的用户账号和密码信息，可以登录用户不同的其他应用系统(如email、OA、ERP、CRM等)，有效提高了进入目标系统的可能性，可以轻松的进入了其他内部系统。

(2)获取Admin服务器shell

客户使用“SQLite Manager”软件版本偏低，存在一个注入漏洞。可以利用此漏洞导致Webshell访问。基于网络公共资源搜索并修改利用exploit，就能获取对admin服务器的shell访问。

(3)权限提升

通过Webshell操作获取网络服务器管理员，继续寻找升级权限的方法。通过信息收集，发现使用该版本系统的服务存在本地权限提升漏洞。该漏洞利用不一定都是系统，包括

开发工具上都可能成为漏洞攻击的对象。在目前的渗透过程中，Webserver代表的内部攻击平台是恶意攻击的一方。随着获取到完整的管理权限，恶意攻击者可以利用该漏洞进行更深入的攻击，从对客户本身攻击扩散到客户的用户面。这可能就是未来攻击者利用这个系统的目的。

3.3 渗透测试执行标准

渗透测试执行标准(Penetration Testing Execution Standard)是目前一个正在开发中的新标准，其核心宗旨是在渗透测试技术领域对渗透测试进行重新诠释。定义一个完整的渗透测试流程的所有步骤和相关操作规范，将渗透测试工作规范化、流程化和标准化。一切的测试都必须在不影响用户正常环境使用的前提下进行。因此必须要双方明确自己的义务和责任，并在整个测试过程中双方都遵循标准的操作方法和流程。

4 结论(Conclusion)

综上所述，为了满足安全风险评估的日益复杂的需求，在有限的时间内对庞大的目标系统进行一次完整的安全风险评估是非常重要的。使用何种测试方法以及技术体系作为理论指导非常重要，因此本文提出的渗透测试方法是基于目前安全行业内主流的渗透测试方法和技术体系，例如：OSSTMM、PTES、OWASP和WASC-TC等作为理论指导。本文提出了基于Kali-Linux的网络安全渗透测试技术方法，并在结合具体案例的情况下全面讲述了该方法的使用过程与测试效果。Kali-Linux方法论体系中所有的测试过程都可以被切分成若干步骤，要完成整个评估项目，必须在整个测试过程当中严格遵循这些步骤。在本次案例渗透测试过程中还需注意发现安全基础设施，同时在网络边界和主机安全管理未设置足够的访问控制时应采取网络分段来加强保障客户网络安全。

参考文献(References)

[1] Babincev I,Vuletic D.Web Application Security Analysis Using the Kali Linux Operating System[J].Military Technical Courier,2016,64(2):513-531.

[2] Heriyanto T,Allen L,Ali S.Kali Linux:Assuring Security By Penetration Testing[C].Packt Publishing,2014:4.

[3] Ramachandran V,Buchanan C.Kali Linux Wireless Penetration Testing:Master Wireless Testing Techniques to Survey and Attack Wireless Networks with Kali Linux[J].Packt Publishing 2015:3.

[4] 张明舵,张卷美.渗透测试之信息搜集的研究与漏洞防范[J].信息安全研究,2016(03):211-219.

[5] 雷惊鹏,沙有闯.利用Kali Linux开展渗透测试[J].长春大学学报,2015(06):49-52.

作者简介：

姚 莉(1982-)，女，硕士，讲师.研究领域：计算机应用技术，嵌入式系统设计及应用.

林科辰(1993-)，男，本科生.研究领域：软件工程，网络安全.

邓丹君(1981-)，女，硕士，讲师.研究领域：计算机应用技术.

(上接第13页)

by Nanofiltration:Operational Optimization and Membrane Fouling Analysis[J].Journal of Environmental Sciences,2016(05):106-117.

[3] Hui Gong,et al.Membrane Fouling Controlled by Coagulation/Adsorption during Direct Sewage Membrane Filtration(DSMF) for Organic Matter Concentration[J].Journal of Environmental Sciences,2015(06):1-7.

[4] 韩永萍,等.MBR膜污染的形成及其影响因素研究进展[J].膜科学与技术,2013(01):102-110.

[5] 刘海萍.神经网络在CPI预测中的应用[A].中国管理现代化研究会.第五届(2010)中国管理学年会——市场营销分会场论文集[C].中国管理现代化研究会,2010:7.

[6] Guo ShengPeng,et al.Task Space Control of Free-floating Space Robots Using Constrained Adaptive RBF-NTSM[J].Science China(Technological Sciences),2014(04):828-837.

[7] 王芹芹,雷晓云,高凡.基于主成分分析和RBF神经网络的融雪期积雪深度模拟[J].干旱区资源与环境,2014(02):175-179.

作者简介：

汤 佳(1991-)，女，硕士生.研究领域：MBR计算机模拟仿真，大数据与云计算.

李春青(1962-)，男，博士，教授.研究领域：MBR计算机模拟仿真，大数据与云计算.