Introduction to Penetration Testing

渗透测试入门

徐孝忠　邬宏伟　裘建开　主编

湖南大学出版社

Introduction to Penetration Testing

渗透测试入门

徐孝忠 鄢宏伟 裘建开 主编

湖南大学出版社

内 容 简 介

渗透测试是从事网络安全工作的技术人员必须掌握的基础技术，也是目前检测系统网络安全的主要方法。本书为渗透测试学习的入门书籍，系统地阐述了渗透测试的基础知识和基础操作，主要包括信息安全和网络安全的概念、信息收集的方法、主机漏洞利用、Web 漏洞利用、权限维持及提升、痕迹清除与隐藏、防御安全及攻击溯源等，并详细介绍了渗透测试的经典案例。

本书是一本关于网络安全技术的通用工具书，操作性强、实用性强，可供渗透测试的初学人员、从事网络安全或信息安全的人员参考使用。

图书在版编目（CIP）数据

渗透测试入门/徐孝忠，邬宏伟，裘建开主编．—长沙：湖南大学出版社，2019.10

ISBN 978-7-5667-1798-6

Ⅰ.渗… Ⅱ.①徐… ②邬… ③裘… Ⅲ.①计算机网络—网络安全—基本知识 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2019）第 234352 号

渗透测试入门

SHENTOU CESHI RUMEN

主　　编：徐孝忠　邬宏伟　裘建开
责任编辑：汤彩云　金红艳　**责任校对：**尚楠欣
印　　装：长沙市昱华印务有限公司
开　　本：787mm×1092mm　16 开　**印张：**11　**字数：**234 千
版　　次：2019 年 10 月第 1 版　**印次：**2019 年 10 月第 1 次印刷
书　　号：ISBN 978-7-5667-1798-6
定　　价：36.00 元

出 版 人：雷　鸣
出版发行：湖南大学出版社
社　　址：湖南·长沙·岳麓山　　**邮　　编：**410082
电　　话：0731-88822559(发行部)，88821315(编辑室)，88821006(出版部)
传　　真：0731-88649312(发行部)，88822264(总编室)
网　　址：http://www.hnupress.com
电子邮箱：549334729@qq.com

编写组

主　编： 徐孝忠　邬宏伟　裘建开

副主编： 王志佳　李　琪　俞红生

编写组： 娄一艇　陈晓杰　叶明达　戚浩金　黄　智　张寒之

徐科兵　赵　萌　祝　婉　邹　翔　钱　幸　费　武

王　勇　严钰君　胡一慎　陈家宁　陈柏军　厉　进

张明达　葛志峰　王　刚　孙夷泽　管金胜　王敏佳

叶夏明　朱艳伟

前言 / Foreword

伴随着信息化时代的到来，网络安全的问题也逐渐走进大众视野。2017年6月，《中华人民共和国网络安全法》正式实施，其目的在于保障网络安全，维护网络空间主权和国家安全、社会公共利益，也意味着网络安全由个人或企业问题上升到国家层面。而渗透测试是检测网络安全的重要手段。

渗透测试是一种模拟真实黑客发起的网络攻击，用于证明网络防御是否按照预期计划正常运行的机制。即对某网站进行渗透，发现其中存在的漏洞和隐藏的风险，然后撰写一篇测试报告，提供给网络所有者，旨在检测目标网络安全性。对于从事网络安全工作的技术人员及热爱网络安全知识的人员而言，渗透测试是必备知识。

为此，本书根据渗透测试的流程展开，由浅到深详细阐述了渗透测试入门的基础知识和操作，全书共分为7章。第1章阐述了信息安全和渗透测试的基本概念及其重要性，并介绍了渗透测试的操作流程及方法。第2章主要介绍了渗透测试信息收集的目的及途径，并说明了信息收集的常见方法。第3章简单介绍了主机相关的渗透方法及过程，包括口令、缓冲区、中间件及其他网络服务。第4章重点介绍了Web相关的漏洞利用，并详细介绍了常见漏洞的基础知识、检测方法

及修复方法。第 5 章对权限维持及提升进行了说明，包括常见的后门渗透方式、提权技术及日志的清理。第 6 章介绍了防御安全及攻击溯源的途径，在防御方面主要采用加固基线的方法，在攻击溯源方面则采用日志分析和流量分析两种途径。第 7 章为融会贯通，介绍了可供渗透测试练习的两个案例网站，并对渗透测试的操作过程进行了详细介绍。读者通过扫描封底的百度网盘二维码，可以下载对应案例的镜像文件，进行渗透。

本书共 7 章，第 1 章、第 2 章由徐孝忠、祝婉、张寒之、厉进负责编写；第 3 章由邬宏伟、黄智、徐科兵、赵萌、葛志峰负责编写；第 4 章由裘建开、邹翔、娄一艇、孙夷泽、王刚、王敏佳、叶夏明负责编写；第 5 章由王志佳、叶明达、胡一嗔、陈家宁、朱艳伟负责编写；第 6 章由李琪、钱幸、费武、陈柏军负责编写；第 7 章由俞红生、戚浩金、陈晓杰、张明达负责编写；全书由王勇、严钰君、管金胜统稿。

本书是一本关于网络安全技术的通用工具书，操作性强、实用性强，可供渗透测试的初学人员、从事网络安全或信息安全的人员参考使用。

目次 / Contents

第 1 章

概　述

信息时代已然到来，网络已经走入千家万户，我国已经成为网络大国，人们对于网络的依赖性和信息安全的关注度也日益增长。信息化和信息产业发展水平已成为衡量一个国家综合国力的重要标准。谈及网络，人们首先想到的就是信息安全问题，信息安全涉及的范围大到一个国家，小到个人财产。本章作为本书的入门章节，对信息安全的基本概念及重要性、渗透测试基本概念及流程进行介绍。

1.1 信息安全概述

在日常生活中，谈到安全问题，我们可能会想到锁、保险柜、安全帽、密码、安检仪等一些实体性的物品。但是生活中还有很多是看不见、摸不着的安全问题，比如网络攻击、个人信息泄露、密码被盗、手机信息泄露、银行卡信息泄露、身份证信息泄露等信息安全问题。随着社会的快速发展及科学技术的不断进步，信息安全方面的问题也是花样百出，造成的后果及损失令人措手不及。为了提高读者的信息安全意识、保护个人隐私及财产安全，本节将从信息安全基本概念、重要性和意义几个方面进行阐述。

1.1.1 信息安全基本概念

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的因素而遭受破坏、更改或泄露，信息系统连续可靠正常地运行、信息服务不中断。其实质就是要保护信息系统或者信息网络中的信息资源免受各种类型的威胁、干扰和破坏。

信息安全具有三个特性，即完整性、机密性、可用性。完整性要求做到被保护的数据内容不被篡改；机密性要求做到被保护的数据内容不被泄漏；可用性要求被保护的资源“随需而得”。

信息安全中，人们接触最多的是计算机安全领域。黑客普遍被认为是破坏者，但在计算机安全领域，往往用帽子颜色来比喻黑客的好坏，一般有“黑帽子”和“白帽子”之分。白帽子是指那些精通安全技术旨在保护互联网安全，并与破坏网络安全的破坏者斗争的专家们；而黑帽子是指那些利用黑客技术破坏互联网规则，通过寻找系统漏洞以获得规则之外权利的群体，旨在破坏网络安全，攫取利益。可见“安全”这一概念是相对的，“不安全”是绝对的。

1.1.2 信息安全重要性及意义

2016 年 11 月 7 日，中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过了《中华人民共和国网络安全法》，并于 2017 年 6 月 1 日正式颁布实施。习近平指出，没有网络安全就没有国家安全。网络安全已经由个人或企业问题上升到了国家安全问题，可谓牵一发而动全身，无论从国家还是社会发展的角度来说，网络信息安全已经成为了不可忽略的重要组成部分。无论是计算机病毒，还是黑客攻击，或是网络监管力度不足，其影响都极为严重。国家和网络安全相关组织需要针对相关的网络信息漏洞做出针对性的方案措施，保证能够最大限度地维护信息安全。

计算机是信息网络的载体，随着社会的发展，计算机的使用率和普及率逐年上升。计算机的使用提高了各个领域人员的工作效率，并且在政治、军事、科技、经济、文化、社

会等领域产生了深刻影响，网络已经融入到社会生活的方方面面，深刻改变了人们的生产方式和生活。网络信息安全受到的威胁也越来越大，世界范围之内不断出现因信息被盗或黑客攻击而引起的安全事故，人们对于信息安全也越来越担忧。信息安全问题已引起了各国政府的高度重视。

近5年，我国发生了多起影响重大的网络攻击事件，如驱动人生供应链事件、数据泄漏事件、勒索病毒、虚拟货币交易所被攻击事件、WebLogic组件多个远程命令执行漏洞、应用克隆攻击、ZipperDown通用漏洞、智能门锁漏洞、Web应用程序0day攻击事件、雄迈摄像头漏洞，Cisco路由器被攻击事件、供应链攻击、GPON远程命令执行漏洞、Java反序列化漏洞、Drupal远程代码执行漏洞、EOS平台远程命令执行漏洞、多个区块链项目RPC接口安全问题、区块链智能合约相关漏洞等。

网络攻击事件在电网安全生产方面也造成了严重的损失，给人们敲响了网络安全的警钟，其中影响较为深远的是2015年乌克兰电网事件和2019年委内瑞拉电网事件。

2015年12月23日，负责乌克兰当地电力供应的当值人员在整理桌上文件时，突然发现计算机屏幕上的光标指向负责当地变电站断路器的导航按钮，并点击对话框选择了断开断路器的操作指令。最终导致当地23万名居民陷入无电可用的困境，损失惨重。

2019年3月7日，委内瑞拉发生了全国性的大面积停电事故，影响人群接近3 000万人；3月8日，全国范围大面积停电逐步开始恢复；但是到3月9日，再次出现大范围停电情况，速度之快，令人措手不及。该事件成为了继“乌克兰电网事件”后的又一“网络战”的典型案例。

作为现代战争的一个重要作战手段，通过网络攻击对手国家的基础设施，从而造成生产停止、通信中断、交通瘫痪、能源供给不足等重大损失，其破坏性远胜于常规炮火攻击。就我国而言，电力系统体系庞大复杂，应加强电力系统安全建设，做到从点到面、从被动到主动、从安全防御到态势感知、从技术手段到安全管理，只有这样，才能应对瞬息万变的安全局面，也唯有这样，才能打赢这场“没有硝烟的网络战争”。

综上所述，信息安全不仅涉及个人的财产安全，更影响着一个国家的安全稳定。而在信息安全中最常见的问题则是由漏洞引起的，针对漏洞我们需要做的是发现并及时解决，即下一小节讲述的渗透测试。

1.2 渗透测试概述

渗透测试就是渗透人员利用所掌握的渗透知识，对某个网站进行一步一步地渗透，发现其中存在的漏洞和隐藏的风险，然后撰写一篇渗透测试报告，提交给网络所有者。

1.2.1 渗透测试基本概念

渗透测试是一种模拟真实黑客发起的网络攻击，用于证明网络防御是否按照预期计划正常运行的一种机制，其目的是以一种安全和受控的方式向人们展示渗透人员如何对网站进行破坏的一种方法，旨在检测目标网络安全性。渗透测试一般具有专业性强和覆盖领域广的特点。

渗透测试常见的攻击技术包括 Web、DB、系统层、网络层。Web 攻击包括 XSS、CSRF、越权、逻辑错误、目录遍历、远程代码执行、网页挂马、文件包含、漏洞利用(Struts2 远程命令执行)等；DB 攻击包括 SQL 注入、漏洞利用、弱口令等；系统层包括 DDOS、远程溢出、本地溢出提权等；网络层包括 DDOS、ARP 欺骗等。

1.2.2 渗透测试的流程

渗透测试是由网络所有者确定其测试目标后，渗透人员开始信息收集，经过漏洞探测、漏洞验证、信息分析、后续渗透、信息整理等，最终形成测试报告。网络所有者根据渗透人员提供的测试报告，可以清晰地知道系统中存在的安全隐患和问题并对其进行修补，以防止黑客的入侵。

因此，一般渗透测试包含明确目标、信息收集、漏洞探测、漏洞验证、信息分析、后续渗透、信息整理、形成报告 8 个步骤，流程图如图 1-1 所示。

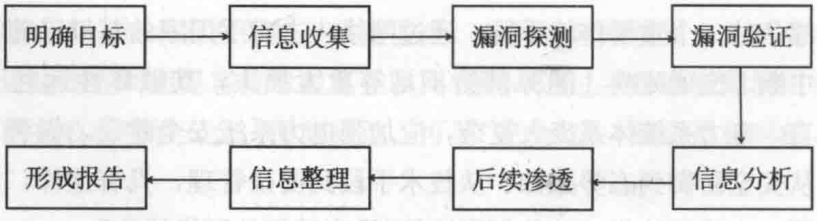

图 1-1 渗透测试流程图

(1)明确目标。

明确目标是整个渗透测试过程有效性的保证。渗透测试之前，渗透人员应先明确测试目标，如测试范围、IP、域名；接入方式(内、外网)；整站或者部分模块、是否允许阻断业务正常运行等；渗透规则，如渗透的程度(发现漏洞为止还是继续利用漏洞)、时间限制、能否修改上传、能否提权等；渗透需求，如 Web 应用漏洞、业务逻辑漏洞、人员权限管理漏洞等。

(2)信息收集。

信息收集是渗透测试工作中不可缺少的阶段。在明确目标之后，渗透人员要做好信息收集工作，对目标系统的信息收集能力是渗透人员一项非常重要的技能，信息收集是否充

分在很大程度上决定了渗透测试的成败，若遗漏掉关键的情报信息，将可能在后面的阶段里一无所获。

例如通过搜索引擎、广告介绍、社会工程学、网络工具的探测等方式，可以得知目标网站的一些基础信息，如 IP 地址、网段、域名、端口、操作系统版本、脚本语言、在该服务器上是否还有其他防护设备等。

(3)漏洞探测。

当渗透人员收集到足够的信息之后，即可以开展网络漏洞探测。漏洞探测是基于漏洞数据库或基于渗透人员的经验，通过扫描和手工测试等手段，对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测行为。它和防火墙、入侵检测系统互相配合，能够有效地提高网络的安全性。通过对网络的扫描或渗透，网络管理员能了解网络的安全设置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员能根据扫描或渗透的结果更正网络安全漏洞和系统中的错误设置，在黑客攻击前进行防范，从而有效避免黑客攻击行为，做到防患于未然。

(4)漏洞验证。

漏洞主要分为主机型漏洞与 Web 型漏洞。主机型漏洞包括口令安全、缓冲区溢出、中间件等，Web 型漏洞包括目录遍历、暴力破解、SQL 注入、跨站脚本、文件上传、文件包含、反序列化等。在渗透测试过程中，渗透人员发现漏洞并征得系统管理人员同意后，对目标系统进行漏洞验证。部分主机型漏洞验证过程中可能会造成系统宕机，应做好沟通与应急措施，并在漏洞验证环节中做好记录，为后续的漏洞报告做准备。

(5)信息分析。

渗透人员发现目标漏洞后，应记录漏洞的位置点和利用过程，并对可能造成的危害进行分析。在提取数据库信息时，应做到适可而止，只提取对后续渗透有用的信息，不能对目标系统进行脱库操作。即将数据库内所有信息进行备份，但不能私下备份目标系统的网页源码，且这些操作在渗透测试前应签好保密协议进行约束。

(6)后续渗透。

若渗透测试客户需要进一步测试目标网站安全，在验证漏洞并分析可用数据后，可对目标网站做后续渗透，包括后门植入及权限提升，用以验证目标网站的风险程度。并对目标网站的日志文件、系统进程进行查看，检查目标网站日志文件权限设置情况、系统补丁更新情况，进而对目标系统的安全性做进一步的评估。

(7)信息整理。

将渗透测试中使用的渗透工具、收集的信息、验证的漏洞信息、漏洞利用的过程进行记录及整理，包括整理渗透过程中用到的利用代码、渗透过程中遇到的各种漏洞，各种脆弱位置信息等。

(8)形成报告。

在网络渗透测试结束后，应当根据收集到的信息进行分析并生成报告，为整个网络渗透测试实施总结。对收集到的数据信息进行进一步的分析，识别被测网络系统可能受到的威胁，了解被测网络系统的脆弱性，并结合已有的控制措施，在分析与研究中得到总结性的结论，为生成报告奠定基础。生成报告的过程也是对整个网络系统的安全性进行评估的过程，确定被测网络系统的风险程度，并给出较为明确的结论，让被测方明白网络系统出现风险的原因从而对所有产生的问题提出合理高效安全的解决办法。

但由于没有严格的测试标准，测试结果存在差异性，其结果主要取决于渗透人员的技术能力和经验等。

1.2.3 渗透测试的方法

渗透测试的方法一般分为黑盒测试和白盒测试。黑盒测试又被称为“Zero-Knowledge Testing”，渗透人员完全处于对系统一无所知的状态；白盒测试与黑盒测试恰恰相反，渗透人员可以通过正常渠道向被测单位获取各种资料，包括网络拓扑、员工资料甚至网站或其他程序的代码片段，也能够与单位的其他员工进行面对面的沟通。

(1)黑盒测试。

黑盒测试可以模拟外部攻击，因为外部人员通常不知道所攻击网络或系统的内部情况。渗透人员必须收集关于目标的各种信息，然后才能确定优缺点。黑盒测试的优点在于系统管理员无需提供任何信息，所有的渗透信息均需渗透人员进行信息收集或漏洞探测获取。这种测试广泛应用于系统上线测试阶段，在安全平台网站进行发布，面向全社会的渗透人员，通过挖掘到的漏洞数量并有效提交，来向渗透人员支付报酬。

(2)白盒测试。

白盒测试则采用与黑盒测试完全相反的方法。这种安全测试的前提是渗透人员完全了解网络、系统和基础架构。这种信息允许渗透人员采用一种更规范的方法，他不仅能够查看所提供的信息，还能够验证它的准确性。

所以，黑盒测试在收集信息方面花费的时间更多，白盒测试则在漏洞检测方面花费较多时间。白盒测试多用在系统上线前，由专业的安全测试机构对目标网站进行测试，发现可能存在的漏洞点。白盒测试相对黑盒测试而言效率更高。

综上所述，无论采用哪一种方法，都旨在对目标网络的安全性进行系统检查，以保证目标网络的安全。

本章作为入门章节，首先介绍了信息安全的基本概念及重要性，从理论和实例两个层面向读者展示信息安全的重要性及意义，然后介绍了渗透测试的基本概念和流程，为后续章节的展开做了基础的铺垫工作。