网络安全中渗透测试高效流程与方法

刘志滨

齐齐哈尔大学计算机与控制工程学院　黑龙江齐齐哈尔

【摘要】互联网离不开日常生活，网络安全关系到每一个网民，而渗透渗透测试被广泛用于网络的安全性。渗透测试人员通过模拟黑客的思维操作，对目标的攻击来发现漏洞。合理全面的渗透测试过程的方法，以解决当前技术的局限性。使用正确系统化的渗透测试流程真实模拟入侵者，从黑客的角度找出隐藏在网络中所有可能的攻击方式，将渗透测试的流程形成合理化高效的过程，引导渗透测试工作者选择最佳的响应行动，避免网络安全被非法入侵。优秀的渗透测试流程，从攻击者的角度，发现隐藏的攻击漏洞，改进现有的渗透测试技术，完善渗透测试流程，提高安全效率。

【关键词】漏洞；网络攻击；渗透测试；网络安全；自动化渗透

Efficient process and method of penetration test in network security

Zhibin Liu

School School of Computer and Control Engineering, Qiqihar University, Qiqihar, China

【**Abstract**】Internet is inseparable from daily life, network security concerns every netizen, and penetration penetration test is widely used in network security. Penetration testers find vulnerabilities by mimicking the thinking operations of hackers and attacking targets. A reasonable and comprehensive approach to the penetration testing process to address the limitations of current technology. The correct and systematic penetration test process is used to simulate the intruders, and all possible attack modes hidden in the network are found out from the hacker's point of view. The process of penetration test is formed into a reasonable and efficient process, and the penetration test workers are guided to choose the best response action, so as to avoid the network security being illegally invaded. Excellent penetration testing process, from the perspective of the attacker, find hidden attack vulnerabilities, improve the existing penetration testing technology, improve the penetration testing process, improve the security efficiency.

【**Keywords**】cyber attacks; penetration test; network security; automatic penetration

1 简介

渗透测试(Penetration Test，简称 PenTest)指通过试图利用漏洞来评估 IT 基础设施的安全性。这些漏洞可能存在于操作系统、服务和应用程序缺陷、配置不当或有风险的用户行为中。这种评估还有助于验证防御机制的有效性和最终用户对安全策略的遵从性[1]。渗透测试通常使用手动或自动化技术方式侵入目标设备，以及其他潜在的暴露点。测试目标的系统的漏洞被成功利用后，测试人员将继续尝试使用被破坏系统以外资源的攻击。通过渗透测试成功暴露的任何安全漏洞信息通常会被整合并提交给客户或上级，以帮助这些专业人员得出战略结论并确定修复工作。渗透测试的基本目的是测量系统或最终客户受损的可能性，并评估此类事件可能对相关资源或操作产生的后果。渗透测试人员（也称道德黑客）模拟黑客来评估 IT 基础设施的安全性。测试服务器、网络、网络应用程序、移动设备和其他潜在漏洞，以发现整个系统中的弱点。

良好的渗透测试流程和方法，是测试的核心影响因素，本文提出完整的渗透测试流程和方法，便于渗透测试安全人员对网络安全的探索，方便高效的进行工作和研究。

2 渗透测试的应用

测试目标的信息通常是机密的，如果被恶意攻击者获取，它的暴露会对消费者和公司造成重大损害[2]。渗透测试的成本不断上升，工程师一直在努力改进流程，以最大限度地减少漏洞。尽管有这些改进，由于程序及其部署配置的复杂性，漏洞仍继续发生。漏洞的持续流行增加了在部署的应用程序中识别漏洞技术的重要性。

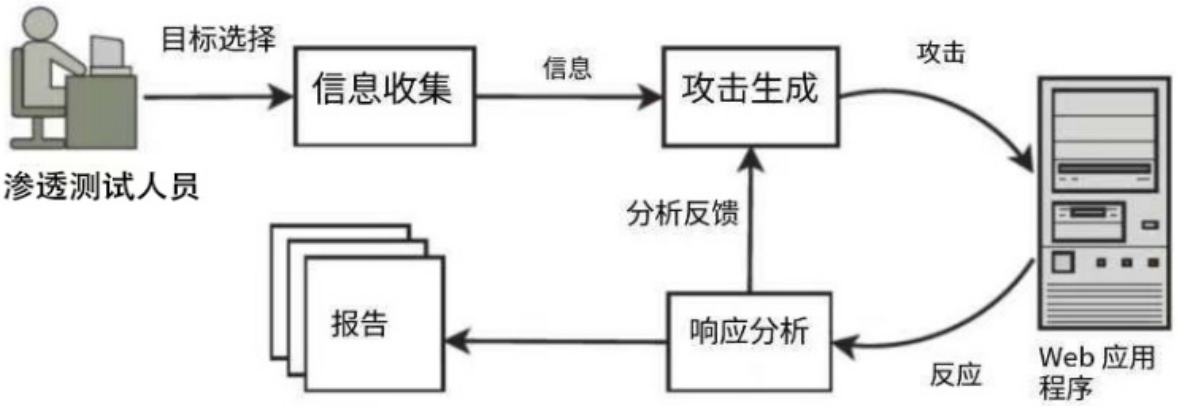

图 1 渗透测试过程

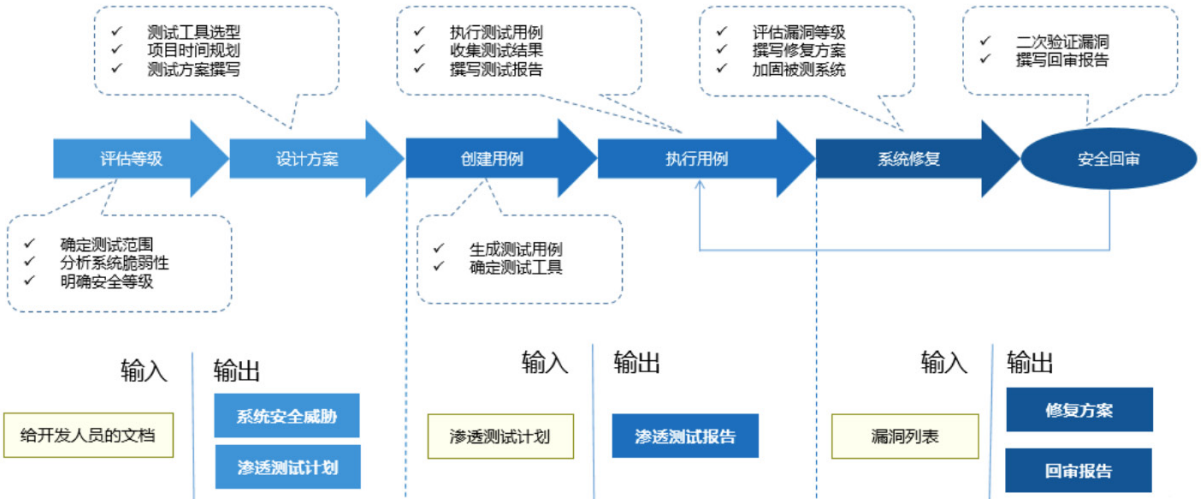

图 2 渗透测试过程

渗透测试的广泛使用促使标准化形成，加快认证渗透测试和建立标准化“最佳实践”渗透测试。尽管渗透测试人员需要执行各种各样的任务，但一般可以分为三个阶段：信息收集、攻击生成和响应分析[3]。“图 1”显示了渗透测试的攻击流程。在第一阶段，信息收集，渗透测试者选择目标应用程序，并使用各种技术获取关于它的信息。这个阶段的结果允许渗透测试人员执行第二个阶段，即开发对目标应用程序的攻击。这个阶段通常可以通过自定义众所周知的攻击或使用自动攻击脚本实现自动化。第三个阶段，一旦攻击被执行，渗透测试人员就会进行响应分析——他们分析应用程序的响应，以确定攻击是否成功，并就所发现的漏洞准备一份最终报告[4]。

3 基于知识图谱的自动化渗透测试

漏洞检测特性与漏洞库匹配漏洞扫描技术，自动化渗透测试通过构建攻击负载的方式验证漏洞，通过构建真实可控的内容请求，不仅兼容度更高，漏洞误报率低，合约数量少、检测速度快等特点，甚至可以绕过部分防御规则。

基于知识图谱的自动化渗透测试打破了模型的固化过程，将渗透测试相关经验和工具结构抽象为

实体节点的知识映射，通过节点之间的关联，形成渗透性知识图谱，每条路径的知识图谱就是一个渗透测试思路，通过扩展知识图谱的规模，可以提高渗透测试的能力。在实际的渗透测试过程中，将已有的渗透知识图谱与采集到的数据相结合，绘制动态的渗透知识图谱，并根据已有的渗透数据和当前的渗透状态进行渗透路径规划，从而提高渗透测试的效率。而且由于知识图谱的相关性，可以对各个阶段采集的数据进行综合分析，从而实现渗透后期采集的数据可以带动前期的渗透测试步骤，从而实现更全面、更全面的渗透测试。深入渗透，最终接近人形渗透的效果。在渗透测试过程中，系统可以根据收集到的信息和历史渗透测试状态分析判断当前渗透测试状态，通过知识图谱和专家系统联合推理决策，选择最优渗透测试路径进行渗透测试，从而提高渗透测试的效率。并且系统能够以渗透图的方式展示渗透过程的思路、步骤和操作，实现渗透测试过程的思路和步骤的重复，为渗透测试人员提供渗透思路。

4 渗透测试范围和内容

网站安全渗透包括 SQL 注入、cookie 注入、文件上传和包含、敏感目录暴露、URL 跳转漏洞、在线编辑器漏洞、网站认证过滤漏洞、远程代码执行漏洞、数据库漏洞、网站路径漏洞、XSS 跨站漏洞、弱口令、文件下载漏洞、程序功能逻辑漏洞、发送任意数量的短信、泛洪攻击、注册任意数量的手机号码或电子邮件安全渗透测试漏洞、api 接口安全认证绕过以及防火墙绕过等漏洞。

服务器安全渗透包括，内网渗透、FTP 特权升级漏洞、SQL Server 数据库特权升级漏洞、Mysql 特权升级漏洞、linux 本地溢出漏洞、替换系统服务漏洞、远程桌面认证绕过漏洞、端口映射漏洞、CC 压力测试、DDOS 压力测试、arp 欺骗篡改页面测试、DNS 欺骗漏洞、会话劫持漏洞、对许多应用系统(如虚拟主机)进行漏洞测试。采用国际标准的攻击前、攻击和攻击后三个阶段，见“图 2”：攻击前主要是指一些信息收集和漏洞扫描的过程；攻击过程主要利用第一阶段发现的漏洞或弱密码等待漏洞入侵；攻击后是指在获得攻击目标的某些权限后，进行权限升级、安装后门、删除跟踪等后续工作[5]。同时结合社工、密码库等先进方法进行攻击测试。

渗透测试是为了让测试目标更安全，让测试目标预期效果。web 应用的渗透测试大致可以分为三个阶段：信息收集阶段、漏洞发现阶段和漏洞利用阶段[6]。在实际测试实践中，测试过程需要进一步细化。下面细致的介绍了 9 个阶段的渗透测试的整个系统过程（注：测试过程中使用的工具、漏洞以及可利用收集的信息不局限据文章所提）：

（1）明确目标

①确定安全测试范围：如：IP、域名、内外网、整站、部分页面 or 部分模块；②确定安全测试规则：渗透的程度，是否可以进一步渗透、时间限制、能否修改上传文件、能否提权、是否允许阻断业务正常运行、接入方式等等；③确定需求：根据用户需求以及自己所掌握的技术能力来确定接下来可以完成的任务。

（2）测试过程分析风险，获得授权

分析渗透测试过程中可能涉及的风险问题，如大量测试数据的处理、对正常服务使用的影响、服务器异常事件的应急响应、软件和数据损坏、数据备份与恢复、以及测试过程中所消耗的人力和物力成本。把实施计划由测试人员准备并提交给客户审查。在获得客户的书面授权后，授权测试人员才可对授权目标进行渗透测试。

（3）信息收集

在信息收集阶段，测试人员需要尽可能多地收集有关授权目标的信息，以便测试人员更好地分析和利用。收集的信息包括：开放的端口、使用的相关协议、使用的编程语言版本类型、服务器信息、使用的应用软件和硬件信息、目录结构、数据库类型版本、所有链接页面、应用框架等。可使用 NAMP 或者 GOBY，AWVS 等安全扫描工具来扫描网站，使用 WHOIS 查看域名，域名注册信息，Web 应用中发布人员 ID ,网站管理员名称、未经授权使用搜索引擎获取页面、敏感站点、P 地址、域名、端口、协议、网段、操作系统版本，所有检测到的应用程序版本信息类型和版本、服务器、防火墙等。

（4）漏洞探测（手动&自动）

针对不同漏洞问题，利用相关信息进行不同的方案，可使用相应的漏洞检测 AWVS、Nessus、AppScan、w3af 等漏扫工具，结合漏洞去 exploit-db 等位置找利用，在网上寻找验证 POC。

漏洞主要包括：信息泄露漏洞、逻辑漏洞、XSS 跨站和 SQL 注入漏洞、CSRF、SSRF、文件上传漏洞、系统漏洞[7]、Web Sever 漏洞、Web 应用程序漏洞、中间件漏洞、服务器配置不正确、端口服务漏洞、数据库服务器问题、数据库设计问题、数据库弱密码、通信安全、明文传输、cookie 传输中的 token、网络协议漏洞等。

（5）漏洞验证

验证所有可以成功利用的漏洞，结合实际情况搭建模拟真实环境进行测试攻击，结合自动扫描工具提供的结果，可以根据已知的漏洞资源进行人工验证。

（6）信息分析

经验证的安全漏洞可用于攻击目标程序。不同的安全漏洞具有不同的攻击机制。针对不同的安全漏洞，进一步分析制定详细的攻击计划，以保证测试稳定全面。

（7）利用漏洞，实施攻击

执行攻击获取内部信息：基础设施（网络设备信息、网络连接、VPN、路由、网络拓扑等）、进一步渗透、内网入侵、敏感目标。进行持久化，但是一般不需要进行持久化。痕迹清除：清除相关日志（访问、操作）和上传文件。

（8）整理数据

整理渗透过程中用到的渗透工具、代码、POC、EXP、适应的方式。整理渗透过程中获得的所有信息。渗透过程中遇到的各种漏洞和漏洞位置信息[8]，以便于形成报告。

（9）书写报告，提出解决方法，提交报告

编写渗透测试报告，记录渗透测试的过程，描述项目安全测试目标、信息收集方法、漏洞扫描工具及漏洞情况、攻击计划、实际攻击结果等，根据与客户确定的范围组织数据，形成报表。分析漏洞产生的原因、验证过程和危害。结合成本等诸多因素提出解决方案，针对所有问题提出合理、高效、安全的解决方案，并提交测试报告。

5 结束语

合理的渗透测试方法和步骤可以有效地评估系统的安全性并提出合理的改进方案。渗透测试模拟黑客对系统的入侵，获取机密信息，形成入侵过程和详细信息的报告，向用户提供报告以识别系统安全威胁并提示安全管理员改进安全策略以降低安全风险[9]。经过专业系统化渗透测试，可以让渗透测试速度更快、思路更加清晰高效，让测试更加全面。就算系统没有被攻破，也能证明测试系统的安全稳定性。渗透测试是一种广泛使用的安全保护技术，有助于提高 web 应用程序的安全性[10]。渗透测试是网络安全的一道重要防线。一个好的渗透测试方法可以有效地提高渗透测试的工作效率，让渗透工程师有一个明确的流程来进一步探索目标，保护安全环境，维护国家、民族以及个人利益。

参考文献

[1] 唐成华,余顺争.基于安全保障能力的网络安全策略评估[J].武汉大学学报(理学版),2009,55(01):109-112.

[2] 石淑华,池瑞楠. 计算机网络安全技术[M].人民邮电出版社:, 201608.312.

[3] 徐飞龙. 基于上下文无关文法的 SQL 注入漏洞测试用例生成研究[D].哈尔滨工程大学,2017.

[4] William G. J. Halfond, Shauvik Roy Choudhary, Alessandro Orso, et al. Improving penetration testing through static and dynamic analysis[J]. Software Testing, Verification and Reliability, 2011, 21(3):195-214.

[5] 吕俊霖. 基于 VirtualBox 的网络渗透测试平台的设计与实现[D].华南农业大学,2016.

[6] 李玲. 列控系统信息安全渗透测试技术研究[D].北京交通大学,2018.

[7] .2009 年安全漏洞态势分析与展望[J].信息网络安全,2010(02):76-79.

[8] 曾佩璇,汤艳君,钱丽纳.基于 Web 渗透测试的 SQL 注入研究[J].网络安全技术与应用,2018(12):16-18.

[9] 李鑫.基于 Web 渗透测试的 SQL 注入研究[J].信息与电脑(理论版),2020,32(03):164-166.

收稿日期：2022 年 8 月 18 日
出刊日期：2022 年 9 月 6 日
引用本文：刘志滨，网络安全中渗透测试高效流程与方法[J]. 国际计算机科学进展, 2022, 2(2) : 5-8. DOI: 10.12208/j. aics.20220013
检索信息：RCCSE 权威核心学术期刊数据库、中国知网（CNKI Scholar）、万方数据 （WANFANG DATA）、Google Scholar 等数据库收录期刊