简译版

渗透测试的八种常见错误以及如何避免

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	8 common pen testing mistakes and how to avoid them		
原文作者	Michelle Drolet	**原文发布日期**	2019 年 12 月 6 日
作者简介	Michelle Drolet 是一位经验丰富的安全专家。https://www.csoonline.com/author/Michelle-Drolet/		
原文发布单位	CSO Online		
原文出处	https://www.csoonline.com/article/3487557/8-common-pen-testing-mistakes-and-how-to-avoid-them.html		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

渗透测试的八种常见错误以及如何避免

Michelle Drolet

2019 年 12 月 6 日

渗透测试至关重要，但是企业的做法正确吗？本文将介绍渗透测试的一些常见错误，并给出避免这些错误的建议。

揭示企业安全缺陷和弱点的最有效方法之一是 :聘请第三方对系统进行有计划的渗透测试。渗透测试就是要找到防御系统中的漏洞 ,并在真正的攻击者利用这些漏洞之前将其消除。针对企业的不同方面，有不同类型的渗透测试。

这些方面包括 :网络基础设施到应用程序再到设备和员工，它们成为犯罪分子的潜在攻击途径。优秀的渗透测试合作伙伴将不限定针对以上的哪一个方面执行渗透测试，他们模拟恶意攻击者，探查企业漏洞，试图采用各种技术和工具来破坏企业网络。

尽管渗透测试已被广泛接受，但是企业必须进行妥善的计划和执行。缺乏专业知识或经验会导致渗透测试适得其反，不仅无法发现企业的漏洞，还会让企业暴露无遗。

接下来，我们将介绍一些常见的错误以及如何避免这些错误。

未确定风险优先级

在尝试改善企业安全状况时，企业要做的第一件事就是建立风险基线。在此基础上，确定最大的风险是什么。这些信息有助于确定渗透测试的目标——渗透测试应具备明确的目标，无论是客户数据、知识产权还是公司财务数据。确定风险优先级，有助于企业将安全工作重点放在价值最大的地方。

想象一下公司最糟糕的场景，并以此为基础确定渗透测试目标。容易发现较小的潜在问题，这可能会使企业偏离真正重要的问题。

使用错误的工具

目前有大量的渗透测试工具，但是要想知道使用哪些工具，在哪里使用这些工具以及如何正确配置这些工具，需要大量的专业知识。如果你认为可以购买现成的渗透测试工具，然后让内部 IT 团队运行这些工具，结果可能会让你失望。除非企业内部有一支经验丰富的红

队，否则企业需要聘请具有渗透测试专业知识的第三方。

聘请渗透测试人员的成本很高，企业很可能会选择短期聘用，因此可以考虑采用自动化工具。自动化渗透测试平台是验证防御系统并提供持续保护的好方法。请谨慎选择，并咨询第三方渗透测试合作伙伴。

无法落地的扫描报告

如果第三方渗透测试人员提供的报告无法落地，则企业很难了解已发现的任何漏洞及其对业务的潜在影响。获取易于理解的信息（包括企业存在什么问题、如果不解决该问题会造成什么后果，以及如何进行补救等）至关重要。

如果渗透测试没有明确的目标，则其扫描报告也不会容易落地。因为报告中没有重点和方向，导致企业不知道哪些是关键威胁。好的报告将过滤掉噪音和误报，凸显对企业至关重要的威胁。企业应避免使用指出数千个漏洞，却不能确定重点漏洞的第三方或自动工具。不要好高骛远，制定具有可操作性的优先级计划，确定重点漏洞并进行修复。

合规测试

如果企业要求渗透测试人员进行合规测试，那么企业会错过很多问题。虽然合规性很重要，但这并不是进行渗透测试的唯一原因。采用这种方法可能会使企业陷入一种虚假的安全感，因为网络犯罪分子并不会按照合规测试的那些项目来执行攻击。

干扰业务

企业应妥善计划，并考虑渗透测试对关键业务系统的潜在影响。成功的攻击者在利用漏洞时通常不会导致服务中断，企业雇用的渗透测试人员也应如此。确保他们了解是否在生产环境中进行测试。在黑盒场景中，渗透测试人员不了解企业的基础架构，导致服务中断的风险会更大。

使用过时的技术

随着新技术、新工具和新漏洞不断出现，任何未能演进的渗透测试计划都将很快变得一文不值。企业需要及时了解最新情况，并不断更新测试方法。优秀的渗透测试合作伙伴会把最新的黑客技术纳入其测试战略中。

渗透测试频率低

每年进行一次渗透测试的情况可能很普遍，但这并不能让企业放心。偶尔进行测试，只能了解企业在运行测试时的防御情况。企业应不断地验证防御系统并进行重新测试，以确保已经修复了发现的漏洞。这是自动化渗透测试平台获得青睐的另一个原因。

未能针对渗透测试的结果进行修复

对渗透测试合作伙伴和自动化工具生成的报告，确定采取行动的负责人。企业必须给这些发现的问题确定优先级，并及时解决排名靠前的问题。如果企业未能修复已知漏洞，就很可能会发生数据泄露事件，给企业造成重大经济损失。因此，企业应针对已确定的漏洞进行测试，确保其已被修复。

计划和执行不良的渗透测试是很危险的。如果企业想要保持强大的安全态势，就不能好高骛远。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com