**安全测试之渗透测试成功的8个关键**

**1.知道为什么要[测试](javascript:;" \t "_self)**

　　执行[渗透测试](javascript:;" \t "_self)的目的是什么？是满足审计要求？是你需要知道某个新应用在现实世界中表现如何？你最近换了安全基础设施中某个重要组件而需要知道它是否有效？或者渗透测试根本就是作为你定期检查防御健康的一项例行公事？

　　当你清楚做测试的原因时，你也就知晓自己想从测试中得到什么了，而这可以让测试规划工作更有效率。知道做测试的缘由可以让人恰当地确立测试的范围，确定测试结果将会揭露什么问题。

　　或许这一步中最重要的一部分，是让团队提前架设好准备从测试结果中得出正确的结论的心理预期。如果测试是要审查IT基础设施的某个特定方面(比如说新的Web应用)，那就没必要着墨于公司整体安全。理解做测试的缘由可以让你问出正确的问题，得到能被恰当理解的结果。

**2.了解你的网络**

[漏洞](javascript:;" \t "_self)是安全的重点。企业网络上线之日直至如今必然经历种种变迁，只要攻击者比企业自己的IT员工更清楚其中存在的漏洞，企业网络就对攻击者门户洞开。

　　绘制公司网络地图的责任不落在渗透测试团队身上。如果渗透测试团队在做这项工作，就意味着你有可能错过他们的测试结果，因为你收到的网络架构消息都能把渗透测试结果淹没。

　　一张更新的网络地图(包括逻辑方面和拓扑方面)应成为渗透测试的强制性前提条件。如果渗透测试员在告诉你你所不知道的网络架构情况，那你就是在为网络地图买单——很贵的那种。

**3. 设置范围**

　　红队探测范围有多广，很大程度上取决于你为什么要做这个测试，因为太广或太窄可能都无甚大用。

　　测试范围过窄的问题很明显：如果想要找出的问题在测试范围外，那就没有任何数据能帮助确定该组件的安全。所以，必须确保测试参数包含事关公司当前安全状态的重要组件。最重要的是，你得确定自己要测试的是整体安全状况还是某特定系统的安全状态，以及人为因素(对网络钓鱼和其他社会工程攻击的敏感性)需不需要被包含进去。

　　如果测试范围过宽，有可能出现两个问题。第一个问题是经济上的：测试费用会随范围的扩大而增加，而测试价格与所需信息不相匹配的状况又会影响到公司高层对未来测试的热情。

　　第二个问题就更为致命了。测试范围过大时，测试本身容易返回太多信息，真正所需的数据很容易被淹没在巨量的测试结果中。教训很清楚：想要测试架构中特定部分的安全，就将渗透测试的范围限定在那个部分上。对整个系统的测试可以留待下次进行。

**4. 做好计划**

　　弄清测试目的并确定出测试范围后，就可以开始制定测试计划了。定出详细明确的测试条件和需求最为重要，任何松散或须经解释的测试要求都会削减渗透测试的效率。需做好详尽计划的原因有很多，其中最主要的原因与成本控制和提升测试结果可用性有关。

　　良好的测试计划应分为多个部分。一个部分帮助委托公司巩固其测试方案的要求。一个部分确认测试返回数据的类型。还要有一部分内容为向公司执行委员会解释测试开销做准备。

　　测试计划不是制定好后就固定不变的，测试过程中可能需作出修订。测试团队被聘用后，他们可能会针对某些测试元素提出一些能产生更好结果的建议。其中关键就在于，公司内部就该测试计划达成一致后 ，安全团队就能判断渗透测试员的建议是否能满足测试需求了，不用什么都依靠测试团队的力量。

**5. 雇正确的团队**

　　提供渗透测试服务的公司和顾问很多。这些公司都有各自的优势和弱点，他们的[技术](javascript:;" \t "_self)技巧各有千秋，呈现测试结果的方式也有好有坏。公司有必要确保所选测试团队的能力尽可能地符合测试需要。

　　要注意的是，测试需求应高于客户要求。确实，有些团队在导引征求建议书(RFP)过程或挤进获批供应商列表上颇有心得，但他们执行测试计划所需渗透测试动作的技术未必比得上这些在应付客户上的技巧。选择渗透测试团队时应将[测试技术](javascript:;" \t "_self)放在第一位，会计和行政管理方面的能力次之。

　　可以考察测试团队的老辣程度，看他们如何在不推翻原计划的条件下提出建议，改进客户的测试计划。这也是为什么前期要做好测试计划的一个重要原因。因为可以检查测试过程中的种种改动。

**6. 不要干预**

　　人都想得到别人的认同，这是人类天性。但渗透测试的目的就是要展现出公司企业安全状态的实际情况，所以，尽量别为了得到个看起来好看的结果而人为干扰渗透测试员，给防御方提供不公平的优势。

　　事实上，红队几乎总能某种程度上渗透进公司网络边界。我们当前的技术和操作就是这样的。很多情况下，真正的问题存在于蓝队到底什么时候才能发现已被攻破，会如何响应。

　　无论测试结果如何，都要让测试过程正常进行，以便结果真实、准确、有用。管理层的任何干预都会毁了渗透测试的有效性，请一定记得在测试完成前不要插手。

**7. 注意结果**

　　测试完成后，你会得到一份完整的报告，需仔细研读。渗透测试员应向你呈现出测试的结果，如果你有机会根据测试结果改进安全系统，别放过这种机会。

　　或许渗透测试是为了满足监管合规要求而做的。也有可能你就没想找任何理由来改变你的安全防御。这都没关系。你的安全防御如今已遭遇过敌军主力，而你可以看清安全计划的成功之处与失败的地方。

　　如果测试结果被用于做出有意义的改变，渗透测试就是划算的。而划算的渗透测试也更有可能在未来获得公司高层的安全预算。

**8. 沟通结果**

　　对大多数公司来说，渗透测试的结果不局限在安全团队范围内。至少，对整个IT部门都有影响，而很多情况下还有高管们需要看到的信息。

　　很多安全人员都觉得，向非安全专业的经理传达渗透测试结果是过程中最难的部分。不仅需要说明都做了什么，为什么要这么做，还要用他们能听懂的语言解释需要作出什么改动。这往往意味着要用商业术语沟通，而不是以技术语言阐述。

　　正如渗透测试可被视为真实攻击的预演，将其他部门的同事纳入结果阐述和操作展示的受众范围，也有助于确保被接收的信息确实是你想要传达的。