



渗透测试指南（更新版）

渗透测试指南（更新版）

渗透测试（penetration test）是为了证明网络防御按照预期计划正常运行而提供的一种机制。不妨假设，你的公司定期更新安全策略和程序，时时给系统打补丁，并采用了漏洞扫描器等工具，以确保所有补丁都已打上。如果你早已做到了这些，为什么还要请外方进行审查或渗透测试呢？因为，渗透测试能够独立地检查你的网络策略，换句话说，就是给你的系统安了一双眼睛。本技术手册将从渗透测试的理解、渗透测试具体实践和渗透测试行业解析三方面向大家详述渗透测试。

渗透测试初步理解

渗透测试并没有一个标准的定义，国外一些安全组织达成共识的通用说法是：渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

- ❖ **渗透测试的解释**
- ❖ **零了解渗透测试的赞成和反对理由是什么**
- ❖ **标准渗透测试的道德黑客技术**
- ❖ **保证企业网络安全必需渗透测试吗？**

渗透测试具体实践

在对网络渗透测试进行设计期间，需要设置许多界限来防止范围蔓延（scope creep），也就是哪些设备、服务以及网络需要测试，而哪些不用测试；这个范围依赖于测试的目标。一定要记录和保存这个计划，因为测试之后它就是你的测试框架，它能帮助你判断哪些测试结果应该分析，而哪些不用分析。

- ❖ 渗透测试方法：创建一个网络渗透协议测试
- ❖ 如何为渗透测试工作选取最佳 IT 安全认证
- ❖ 如何处理网络渗透测试结果
- ❖ 社会工程测试应该包含在渗透测试中吗？
- ❖ 渗透测试员解密企业系统评估

渗透测试行业解析

渗透测试的目标不仅是要评估电脑系统或者网络的安全性，还要决定成功攻击的可行性和商业影响。这样的测试模仿企图利用你的企业系统中的潜在的漏洞的攻击者。发现的任何安全问题随后都要报告，一起报告的还有对他们可能产生的影响的评估。

- ❖ 如何进入渗透测试行业
- ❖ 如何选择渗透测试人员
- ❖ 道德黑客如何转变为线路渗透测试人员？

渗透测试的解释

安全诊断主要有三种类型：渗透测试、审计和评估（被不同地描述为评估和风险评估）。单独使用任何一种测试都不可以很好的进行。在测量系统安全的时候，必须要在合适的时间执行合适的测试。还有一点非常重要，就是所选择的测试要基于企业的需要，而不是测试者（不管他们是内部员工还是外来的咨询人员）的技术（或者因为对技术的缺乏）。

渗透测试

渗透测试的名声最响，因为每个人都听说过，而且“知道”渗透测试是专家用于确保系统安全的。渗透测试目前很有吸引了，但是却是在大部分情况下使用最少得系统诊断方法。

先说重要的事情：正确执行的渗透测试是秘密的测试，其中由咨询人员或者内部人员扮演恶意攻击者，攻击系统的安全性。因为最终目的是渗透，这种测试不会发出警告，完全保密（当然，上层管理人员同意进行测试并且理解秘密的要求）。理想的是，应该没有来自企业的支持……或者，最大限度的指出哪些是渗透测试团队应该避免的。很显然，如果企业外包了渗透测试，客户应该让咨询者知道具体的目的是什么。测试就可以设计为模仿内部或者外部的攻击。它可以技术性的，也可以是非技术性的（例如，测试者可以使用社交工程师的方式进入网络）。在目标企业中，只能有一部分人知道测试。测试的关键的一方面是看企业是否能检测到渗透企图。处于这个原因，批准正式回应的人应该也被包括进去。

现在，为什么渗透测试不如它说明的那么有用？因为它唯一的目标是攻击安全。为了这么做，这个团队要鉴别可能的漏洞，重点是那些他们认为会产生结果，而不太可能被检测到的（从黑客的角度）。在这一点上，客户可以看到对这些漏洞的攻击可以产生什么样的破坏。但是，在运行测试的时候，测试员不会发现所有的漏洞，甚至不能确定测试可能检测到的所有漏洞的存在。渗透测试所能够证明的是系统可以被攻击。它不能对每一个漏洞进行记录，只能是那些在测试中被利用的漏洞。所以，虽软渗透测试可以推断出其他问题，但是任何渗透测试员都不能说已经鉴别到了客户的所有安全问题——或者甚至是大部分。

那么，渗透测试有什么作用呢？处于各种内部原因，有些企业需要有说服力的论据说明不充分的安全可能导致重大损失。执行情况良好的渗透测试当然可以证明。为了从业务的角度使渗透测试起作用，企业价值可能的损失必须要强有力的并生动的证明出来，要超出企业的电脑被攻击的事实。

有时，应该进行秘密渗透测试，看看安全策略是否被遵守了。虽然公开的测试也可以调查人们是否遵守了策略，但是在不知道被监视的时候人们就会有不同的表现，这是人类的天性。例如，XYZ 公司的安全策略禁止终端用户在电话中泄露密码，除非他们自己主动打电话到服务台。很明显，如果外部的咨询人员走到终端用户那里，并问：“你有没有把你的密码告诉过你不认识的人？”答案通常是没有。但是如果测试人员打电话给用户，情况就不同了，假扮成 IT 部门的同事，并向用户询问他或她的密码，这样测试人员就可以“确认”了。这样的社会工程渗透技术是确定是否遵守安全策略的更可靠的方法。

原文出处：http://www.searchsecurity.com.cn/showcontent_16856.htm

(作者: Ira Winkler 译者: Tina Guo 来源: TechTarget 中国)

零了解渗透测试的赞成和反对理由是什么

问：如果测试人员不了解要进行渗透测试网站，赞成和反对的理由是什么？在理想状态下，测试人员应该是什么也不知道吗（为了更好的模仿攻击者的思维模式）？

答：对网站的渗透测试环境的零了解意味着渗透测试人员被告知很少的目标信息，可能只有它的 URL，因此可以模仿真实的攻击者。

虽然对于预算和办公室政治的环境很有帮助，可以向老板提交报告证明即使不了解新网站的人也可以入侵进入，但是我对零了解的方法还有一些保留意见。我们知道一定百分比的攻击时来去网络边界内部的，或者来自有内部帮助的外部。如果你想要知道你的网站在所有现实情景中是否安全，零了解就不是必须的最好出发点。

零了解的方法也有潜在的缺点，它返回结果比较慢。如果预先对测试人员介绍了系统的某些基础，就会节省时间，而在产品生产的时候，时间通常是最紧张的。这里最重要的变数之一是目标的状态：是在生产还是在开发？当测试产品系统的时候，你可能想要测试人员让你尽快了解所发现的漏洞，而不是等最后的报告。假设和测试人员的合同写的很合适，你可能就可以给漏洞打补丁，并测试补丁。当然，有人会说把渗透测试人员作为安全的改进人员可以花最少钱得到最大的效果。

最后，不管你是否选择从零了解出发，记住在不触犯法律的情况下你不可能真正的复制现实世界。你必须假定你的攻击者准备好了犯法来完成他们的目标，但是很多企业可以给渗透测试人员免死金牌。所以，你想要你的渗透测试人员可以和犯罪黑客一样思考，并把非法渗透到系统的方法写下来给你。

底线是现实世界和渗透测试是两个不同的事情。如果有安全专家定期对产品中的潜在漏洞进行测试，而安全专家完全了解产品，而不是设置不现实的测试情景，你的安全资金可以以最好的方式支出。

原文出处：http://www.searchsecurity.com.cn/showcontent_17120.htm

(作者: Michael Cobb 译者: Tina Guo 来源: TechTarget 中国)

标准渗透测试的道德黑客技术

问：我最近为我们公司的合作伙伴作了一次渗透测试，发现管理层没有获得合作伙伴执行测试的书面许可。合作伙伴报告说他们被黑了，现在公司被卷入了诉讼！从现在开始我要确保我手里有书面许可，但是我要怎么做才能挽救我作为一名道德黑客的名誉呢？

答：没有什么能比得上把自己卷入诉讼中。好像你和你的公司都得到了很有价值的教训，知道在进行评估前首先要有合适的书面许可。你需要先做几件事情：一是和公司的管理层和律师谈谈，看看他们需要从你这里去的什么文件。这可能包括的文档有你被要求作什么事儿的，你做了什么测试，以及什么时候。要尽可能的合作，并快速建立一种观念，就是你是把公司利益放在第一位的员工。

下一步，为将来的渗透测试创建可以遵守的程序。这应该要求有管理层的一些文件要求以及各方面的同意这么做的许可类型的通知。在测试后，还应该包括测试进行的时间和内容的文档。

如果你的公司可以很好地处理这种情况，管理层就会在这个过程中支持你。如果清楚了公司知道需要有许可并选择了忽略它，你还有一个选择，很不幸，就是你要辞职。有时，保护自己名誉的最好方法是完全和公司分开，并找一家尊重道德的新公司。这是很激烈的措施，但是最后对你最有利。任何称职的雇主都不会这么对待你。

原文出处：http://www.searchsecurity.com.cn/showcontent_16688.htm

(作者: David Mortman 译者: Tina Guo 来源: TechTarget 中国)

保证企业网络安全必需渗透测试吗？

问：在企业网络安全策略中，渗透测试的重要性有多大？

答：渗透测试可以提供安全防御的有价值的信息，但是成本很高。为了渗透测试的可信性，通常必须要有独立的外部公司进行。如果使用内部人员和测试揭开漏洞，你可能会听到这样的批评，测试人员一定在攻击中利用了他们的内部信息和架构的指示来扩大安全预算。另一方面，如果测试表明状况良好，你可能会受到测试不够彻底的批评。如果有的话，这就一定是第二十二条军规。

由于渗透测试的高成本，我通常推荐成熟的安全项目才能考虑使用。如果你正在构建安全架构，缺少几个主要的部分，那么首先就把预算花在这里吧。否则，渗透测试就只能揭示已经知道的漏洞。另一方面，如果采用了渗透测试来评估全面执行的架构，你可能会获得潜在漏洞有价值的信息。

原文出处：http://www.searchsecurity.com.cn/showcontent_16915.htm

(作者: Mike Chapple 译者: Tina Guo 来源: TechTarget 中国)

渗透测试方法：创建一个网络渗透协议测试

问：我是一个 IT 审计员，我想为我们公司的端口执行入侵渗透测试，但受到了 IT 小组的阻扰，因为他们担心这会导致系统停机。然而，根据我的研究，执行测试使系统停机的风险很低。你觉得我该怎么说服他们？

答：在给企业做任何网络渗透测试之前，采取一些基本的行动不仅是为了保护公司，也是为了保护你自己。我能给你的一个最好建议是，使用 NIST 特别出版物 800-115（信息安全测试和评估技术指南）中的一个模板，交战规则（Rules of Engagement, ROE）。交战规则模板将帮助您组织和准备渗透测试方法，同时也给 IT 部门一种印象，即你知道你在做什么，并且你对可能造成停机的问题比较关注。

例如，交战规则包括以下主要内容，您需要与 IT 和企业管理部门一起来完成：

介绍

- a. 目的
- b. 范围
- c. 假设和限制
- d. 风险
- e. 文档结构

物流

人员

- a. 测试进度表
- b. 测试场地
- c. 测试设备

沟通策略

一般沟通

a. 事件处理和反应

目标系统/网络

测试执行

非技术测试组件（如，面谈、社会工程）

- a. 技术测试组件（如网络扫描、发现、渗透测试）
- b. 数据处理

报告

签名页

测试小组组长和公司的高级管理人员（CSO、CISO、CIO 等）应签署交战规则，说明他们理解测试的范围、界限和风险。

另外，还有一些额外的东西需要添加到交战规则中，以帮助 IT 人员了解你是站在他们这一边的：

1. 允许的活动和不允许的活动内容。（例如，如果测试将导致系统中重要资产灾难性丢失，不允许对其进行渗透测试。此外，不允许在不能被中断的重大事件期间进行渗透测试。）
2. 确定那些未经授权测试的系统（如，制定一个“排除清单”）。
3. 有一个详细的事件处理和响应过程，以防在测试过程中网络发生事故。

通过完成 ROE，并与 IT 人员紧密合作，你可以证明你的意图和能力是可信的。

原文出处：http://www.searchsecurity.com.cn/showcontent_38517.htm

(作者: Ernest Hayden 译者: 曾芸芸 来源: TechTarget 中国)

如何为渗透测试工作选取最佳 IT 安全认证

问：你认为如今安全行业中最受认可的黑客或渗透测试认证是什么？

答：依我看来，受认可的程度并不是选取认证的最佳度量方式。最好换个思路来考虑：哪一个认证能证明最高的技术水平？或，哪一个认证最能满足我的需求？

经常光顾我的专栏的读者可能还记得，我并不热衷于认证，也不属于那种将认证当成工作聘用捷径的人。重返你的问题，我的建议是不要在认证上费心思，而应当接受更多的培训并积累经验。名字之后的认证头衔并不重要，重要的是你知道什么、你应用该知识的实际工作经验有多少。履历和面试的目的就是设置来获取这方面信息的。

原文出处：http://www.searchsecurity.com.cn/showcontent_32869.htm

(作者：David Mortman 译者：唐波 来源：TechTarget 中国)

如何处理网络渗透测试结果

你的第一个企业网络渗透测试现在完成了，恭喜你！而如今你将面临数目众多的漏洞信息，但是你不仅不知道怎样通过分析它们来辨别企业的脆弱之处，也不知道怎样使用这些信息对网络加强防护。

虽然采用网络渗透测试分析的做法可能会让你头晕，但这篇文章里我们还是要详细阐述如何对渗透测试的结果数据进行分析和处理。

在对网络渗透测试进行设计期间，需要设置许多界限来防止范围蔓延（scope creep），也就是哪些设备、服务以及网络需要测试，而哪些不用测试；这个范围依赖于测试的目标。一定要记录和保存这个计划，因为测试之后它就是你的测试框架，它能帮助你判断哪些测试结果应该分析，而哪些不用分析。

举个例子，如果你的测试范围是企业中所有的路由器和交换机，那么测试任务就是检查所有跟这些设备有联系的漏洞。而在扫描过程中，数据显示一台运行着 Windows 操作系统的机器其实是一台易受攻击的 FTP 服务器。虽然这个易受攻击的服务会带来一定风险，但是花费时间去评估这个任务范围之外的设备却会影响渗透测试分析的时间安排。出现这种情况可能是一个较小的特权访问管理问题，也可能是更严重的安全破坏，但不管怎样，简单地报告这个问题并存储相关信息就可以了。

如果时间和要求允许，你可以把这个额外的数据写进报告的附录，作为测试范围外漏洞概述（需要更深入的调查）。无论如何，不要毁坏相关的测试结果，即使这些结果不属于目前需要交付的信息。

一旦你已经辨识出测试范围之内的那些漏洞测试结果，那么就要使用多种资源来验证它们的有效性。这是个重要的工作，因为不存在一种工具总是能够根据你的测试范围提供准确的信息。这些资源一般应该包括像 Nmap 这样的工具所提供的网络测试结果。另外，还可以把数据跟 Nessus 之类的漏洞评估工具所提供的结果进行比较。

在最初的渗透测试结果分析中，其关键是去除那些可能跟特定设备相关、但跟平台无关的漏洞。Windows 的 SMB 漏洞利用程序就是一个很好的例子，虽然是针对 Windows 的漏洞利用程序，但是其运行平台实际上是一个运行 Samba 软件的 Linux 主机，它可以几种

非 Windows 的平台通过 TCP/IP 跟 Windows 系统相互联系。尽管新型的扫描器总是能更好的识别平台信息，但是由于专用安全设备，比如防火墙、IPS 以及负载均衡器等的使用，得到的实际平台结果往往并不准确。

从现在开始，把渗透测试结果数据跟所有的网络文档进行比较。今天，越来越多的渗透测试是在内部进行的白盒测试，用以验证网络设计是否反映了操作执行的情况，可以对数据的相关性进行深入剖析。从这个角度看，白盒测试一般而言会更正确一些，因为实际漏洞可能会跟网络结构图、IP 子网分配、服务列表以及其他的网络记录方面有联系。如果你正在运行一个内部测试并且可以访问这些信息的话，使用这些信息将帮助你避免浪费宝贵的时间去做出针对关键漏洞的错误肯定（false-positives）。

一旦你感觉测试结果已经减少到了能够处理的数量，那么就要使用标准把识别出来的风险进行分级。这个工作应该根据安全标准进行，这些标准是一般性的，但是也可以针对自己的环境进行细微的修改。这方面有许多深入的、免费的以及易于实现的标准框架。一个是开源安全测试方法手册（OSSTMM），另外一个开放式软件保证成熟度模型（OpenSAMM）。虽然 OSSTMM 是直接面向安全测试的，但是两个标准都有很好的例子可以为你的企业建立一套标准体系。

有些渗透测试工具会提供有限范围内的相对的风险级别，即不考虑其他任何控制的实际漏洞的分级。这样做既有好处又有坏处——好处是因为它能够快速的查看高风险、能被远程利用的漏洞（这些漏洞可以让攻击者利用，进而完全控制终端设备）；但坏处是识别出的某种低风险漏洞有可能处于网络中受其他保护所控制的某台隐蔽的主机上，以至于这种漏洞才似乎更令人担心。

最终，测试背后的动机将决定最终测试报告的形式。比如，测试报告可能描述了渗透测试的目标以及范围、分级别的渗透测试结果、带有修正建议的结论以及一个可选附录（为了更深入的调查或者描述测试范围之外的发现等）。请记住，真正的危险等级是根据你自己定义的标准得来的，现成的高级、中级以及低级标准一般不会真实的反映出实际存在的风险。

渗透测试仍然是发现网络安全薄弱环节的重要方法，这需要花费大量的时间和努力，如果没有指定出如何使用测试结果的策略，那么进行测试是没有意义的。只有通过确认测试范围、验证结果、运用指标对它们的严重性进行分类、清楚简明地报告发现结果，才能真正反映出公司当前的网络安全风险状况。

原文出处: http://www.searchsecurity.com.cn/showcontent_31990.htm

(作者: David Meier 译者: Sean 来源: TechTarget 中国)

社会工程测试应该包含在渗透测试中吗？

问：社会工程应该是渗透测试的一部分吗？这样做是道德的吗？

答：这个问题的答案还在争论之中。以下尽量不偏颇地列出对这个尴尬问题的双方的观点。然后，我会谈一下我的意见。

有些安全专家坚决认为社会工厂测试不应该成为渗透测试的一部分。原因是安全人员需要对企业的所有员工都非常信任。如果没有这种信任，这些员工可能会忽视在渗透测试中的社会工程演习一部分的欺骗他们的人提出的建议。更糟的是，在这种测试中发现的缺乏良好的安全实践的员可能会被动或者主动地破坏他们的安全主动性，并对整个企业的安全状况的改善带来不利影响。

在这个问题的另一个方面，有些人认为确保员工理解并遵守安全实践至关重要，不必企业的技术结构和配置的重要性低。即使有完美的安全技术（而这是不存在的），不遵守可靠的安全实践的用户可能会破坏整个企业。而且如果员工的做法没有标准，如何决定他们是不是合适呢？最好的安全测量的方法之一就是目标企业进行等级式社会工程攻击，来看看他们如何反应。这样的测试对员工的行为必调查或者测验有了更好的实际的了解，在调查或者测验中，员工的反应总是像他们是模范市民。

虽然我对双方的观点都很尊重，但是我更赞同第二种观点。社会工程测试具有很高的启迪作用，可以揭示目标企业的安全意识中的不足。具体的发现可以帮助企业以更快捷更划算的方式建立更好的安全意识。但是，这样的测试的进行必须要极端关注和专业精神。在开始任何社会工程测试之前，都要确定：

- 列出测试的内容，并创建具体的测试假象脚本。
- 确定管理层预先同意在最后的报告中不提及具体的员工姓名，测试应该关注确定企业中的漏洞，以及对员工整体改善的建议，而不是查找有问题的个人。
- 记录测试中的所有交互动作，但是不再最后的报告中包括员工姓名。
- 考虑企业是否具有管理这种测试的专业技术，或者还是应该雇佣第三方。

原文出处：http://www.searchsecurity.com.cn/showcontent_16926.htm

(作者: Ed Skoudis 译者: Tina Guo 来源: TechTarget 中国)

渗透测试员解密企业系统评估

Chris Nickerson 是你最怕的噩梦，你看不到他的进入，他可以潜入你的数据中心。在他选择的任何服务器上安装恶意软件，并在不对安全产生影响的情况下从容退出。

Nickerson 是 Lares Consulting 的 CEO，他在 TechTarget 的这次采访中谈到了渗透测试的乐趣和外包的风险。

TechTarget: 有人付钱请你入侵到公司的建筑和网络中。为什么需要这种等级的评估？

Chris Nickerson: 原因是，在有我的安全项目的我工作过的每个地方，最大的问题就是取得正确渗透测试的基金。我发现你表示和证明的你可以做得越多，你在人造造成的心理影响就越大。当我在他们面前拿到了他们密码，并且证明我可以在夜里两点进入他们的数据中心。当在他们的安全快照中什么也没有的时候，它就起作用了。这个很有用，而且已经在政府部门使用了一百多年了。对于安全人员来说，他们要说他们已经准备好战斗了。那么好，证明一下吧。

TechTarget: 海外各国写了这么多的代码，如果公司没有对使用的人足够的注意，那么商业间谍的危险会有多大？

Nickerson: 这一点儿非常现实。这些公司在很多地方花了了多少钱。在软件行业这是个大问题。我认识一些人，而且我自己也曾经作过事故响应，在这里你会发现，正是守门人窃取了源代码。这种情况越来越糟。有些资金雄厚的公司雇用黑客团队进入他们对手的公司，并且取下一季度的设计稿。看看社会诱捕行动这样的事情吧。紧跟在后面的人们可以帮助桌面工程师，建立管理，然后开始向他们支付没有信息的费用。然后他们就依靠这些钱，很快我就可以让他们为他们没想过的事情付钱。我就以你的公司为基地，然后把你付款要我保护的信息出售一百次。这是很漂亮的黑客的方式。我们把这种商业间谍作为美国公司中的严重威胁，而这些公司都会把他们的研究开发（R&D）向其他国家外包，然后再回到本国进行产品分类。

TechTarget: 平常的公司如果防御商业间谍呢？

Nickerso: 他们需要少发些牢骚，少猜测。我在 Sprint 运行了一个项目，但是却很不安全。我们做了社会工程培训项目，想要把一些人们常用的诡计教给用户。在一个星期后，我们打了电话，对他们进行了社会工程测试。成功率很低。这很不安全。他们所知道的唯一的事情是了解了测试有多糟糕。

TechTarget: 你所看到的企业的信息安全项目中最大的错误是什么？

Nickerson: 了解业务是我认为的最正常的，但是我的大部分客户都被我的观点震惊了。全面检查并决定什么是最重要的需要保留的，并把信息安全项目建立在这些之外是最关键的，而不仅仅是遵守法规。你可能遵守了法规，但是如果你的系统受到了工具，你就会被辞退，而没有薪水。人们会在法规和安全的方面犯错误。

TechTarget: 你见过有些公司把重点放在了法规上，而没有作足安全？

Nickerson: 是的。我曾经为一家遭受过数据泄露攻击的公司的母公司做过评估，我向他们展示了漏洞，他们说：“这不是法规的要求，我们不在乎。”这是敞开数据中心的大门，而他们所说的只是“法规、法规”。我喜欢向人们表示我可以接近公司的关键资源，不管多近。我喜欢告诉客户任何东西都可以通过 Windows 控制。你不认为这是问题吗？好吧，我可以对你的硬盘加密而不告诉你密钥。你就完了！

原文出处: http://www.searchsecurity.com.cn/showcontent_17099.htm

(作者: Dennis Fisher 译者: Tina Guo 来源: TechTarget 中国)

如何进入渗透测试行业

问：我做了四年的质量工程师，并在 IAM 安全和漏洞产品测试中有两年的工作经验。我想要进入渗透测试领域，我应该做什么呢？我是否应该去考取一些 CEH（EC 理事会的鉴定道德黑客）一类的证书呢？

答：在渗透测试中有一些纪律，我会从几个方面来回答这个问题。首先，决定你想要做哪方面的渗透测试。可能是针对网络的、针对应用的、甚至是针对人的。对于广义的渗透测试来说，也有一些具体的规矩。既然你有质量工程师的背景，那么做应用测试应该很有利。作为应用测试人员要学习的最难得是应用到底是怎么工作的。由于你已经在应用的功能性和特征的测试方面有了多年经验了（我假设的），那么确定如何测试安全问题就不是个大挑战了。

还有，对于理解如何进入应用以及如何对已发现的问题提出建议等的人来说，有很多要求。White Hat Security 的 Jeremiah Grossman 去年多了一些研究，表明我们需要 10 倍的人员，来对最重要的 Web 应用的 2% 进行应用测试。随着 Web 2.0 应用的增值，这个问题不可能在短时间内获得解决。

进入新的行业有两种方法——证书或者背景。培训和证书可能不是从 A 点进入 B 点的方法。如果你的背景不能对你想要做的工作带来任何可信性，那么你就需要某种程度的教育和/或证书来证明你的价值。

但是，如果你有技术背景，而且有兴趣和能力使用现有的工具（例如，Web 应用扫描器、Metasploit 以及其他的渗透测试技术），那么不用正式的证书，你就可以进入这一领域。我不是说 CEH 没有用，但是在花钱、花时间获取证明前，你需要决定是否需要它来完成你的目标。

原文出处：http://www.searchsecurity.com.cn/showcontent_17090.htm

(作者: Mike Rothman 译者: Tina Guo 来源: TechTarget 中国)

如何选择渗透测试人员

问：选择渗透测试员有什么标准？

答：渗透测试的目标不仅是要评估电脑系统或者网络的安全性，还要决定成功攻击的可行性和商业影响。这样的测试模仿企图利用你的企业系统中的潜在的漏洞的攻击者。发现的任何安全问题随后都要报告，一起报告的还有对他们可能产生的影响的评估。建议还要指出如果减轻这些问题。通常这些测试都是在系统或者应用使用之前进行的。然后测试会定期进行。

在选择渗透测试员之前，需要正确地确定你想要测试哪些系统。例如，测试 Unix 系统的专家可能不是测试 Windows 系统的专家。一旦决定了要测试的系统，就向其他公司的同事询问做过类似工作的人的资料。相比较渗透测试证书而言，我更喜欢这种方法，因为在这个领域还没有真正的行业标准。

我也不会总是关注著名的咨询人员。这些咨询人员通常都是通才，而渗透测试是专业工作。不管你会用谁，都要保证当签订合同时，来的人不是生手。

还应该了解渗透潜在的测试人员喜欢使用的方法。执行渗透测试的最好方法是进行一系列系统的可以重复的测试，可以对很多不同种类的漏洞进行测试，避免使用效率较低的分散的方式。但是还是要谨慎对待检查清单的方法，并且不能过度依赖自动化工具。这种类型的结果更像是漏洞扫描而不是全面的渗透测试。渗透测试并不是精密科学，所以测试人员要在探究关注的领域时非常灵活，并对最新的阻力进行追踪。这样，测试就可以关注你的环境中的攻击携带者。

如果决定了让谁进行测试，要确保他们有时间进行彻底的评估。紧迫的时间限制会迫使测试人员跳过某些涉及到的问题。有一点很重要，他们要不断把发现的结果、测试完成后的最终报告细节、关键的发现和建议通知你。记住这些报告是你付了钱所购买的，而且你需要找时间何测试人员进行讨论。如果你在选择测试人员的时候很着急，那么不仅会造成资金的浪费，而且你收到的报告会让企业造成误解，对安全做出错误判断。

原文出处：http://www.searchsecurity.com.cn/showcontent_17037.htm

(作者: Michael Cobb 译者: Tina Guo 来源: TechTarget 中国)

道德黑客如何转变为线路渗透测试人员？

问：经过认证的道德黑客如果成为线路测试人员呢？

答：作为一名渗透测试人员找一份工作（或者在现在的工作上增加责任）确实是个问题。道德黑客认证提供了确认渗透测试资格的测试。

道德黑客认证和其他大多数认证的不同之处在于它可能是善意的，也可能是恶意的。通过对黑客使用的工具和技术的培训，经过认证的道德黑客应该不仅测试企业对这些技术的防御程度，还要更有效的防御这些攻击。

当然，这些都是理论。实际上，我发现安全专家需要能够像黑客一样思考。他们需要谨慎的查看系统，并指出漏洞在哪里。虽然不能完全消除这些漏洞，大部分明显的问题完全可以通过使用道德黑客技术和攻击工具来解决。

我非常喜欢测试网络、系统和应用。我为什么这么说呢？可以参看我最近在安全博客中的写的文章，为什么企业渗透测试很重要。

原文出处：http://www.searchsecurity.com.cn/showcontent_14579.htm

(作者: Mike Rothman 译者: Tina Guo 来源: TechTarget 中国)