企业渗透测试指南

企业渗透测试指南

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，最大限度的是指出哪些是渗透测试团队应该避免的。在本指南中将全面介绍渗透测试和道德黑客，以及渗透测试的作用和执行方式，此外，希望本指南也能为想要成为渗透测试人员，也就是道德黑客的技术人员提供帮助。

什么是渗透测试

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。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。本部分将介绍渗透测试的基本概念和道德黑客技术。

- 渗透测试的解释
- 标准渗透测试的道德黑客技术

渗透测试对企业的作用

渗透测试可以提供安全防御的有价值的信息。此外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就可以证明。本部分将介绍渗透测试对企业的作用，并涉及到企业建模的作用

- 保证企业网络安全必需渗透测试吗？
- 威胁建模对企业有帮助吗？

渗透测试的执行

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。那么如果选择合适的渗透测试人员呢？应该采用什么技术和工具呢？渗透测试应该包括哪些方面呢？本部分将对这些问题做出解释。

- 如何选择渗透测试人员
- 漏洞分析新工具：RE:trace
- 社会工程测试应该包含在渗透测试中吗？
- 零了解渗透测试的赞成和反对理由是什么

渗透测试和道德黑客

在互联网刚刚兴起的时候，我们经常可以听到渗透测试，但是最近几年这种狂热已经减轻了。这种信息风险评估方式——21 世纪中它的名字是道德黑客——正在复兴。人们开始看到以黑客的方式思考来防御黑客是全面信息风险管理项目的不可或缺的一部分。本部分将介绍如何成为道德黑客或者渗透测试人员，以及他们执行渗透测试的注意问题。

- 道德黑客十训（上）
- 道德黑客十训（下）
- 渗透测试员解密企业系统评估
- 如何进入渗透测试行业
- 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，最大限度的是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。

(作者：Ira Winkler 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。。

(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。

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

威胁建模对企业有帮助吗？

问：威胁建模是有用的防御机制吗？真的可以和黑客一样思考吗？

答：目前，威胁建模对安全专家来说是一种难以置信的有用的工具。进行威胁建模的训练，可以遵循一下的步骤。

首先，广泛考虑企业中最有价值的信息资产、重要的计算机资源以及他们的位置。

下一步，讨论一下细节，谁可能攻击你的企业，为什么。这些就是威胁。网络罪犯会攻击你吗？单一民族国家会吗？内部威胁呢？不要忘了考虑安装在环境内部的飘忽不定的蠕虫。目前的威胁不是全部都是人为的。

第三，基于你的威胁清单，开始考虑他们如何攻击你。最简单的方法是什么？取得详细的信息，不要马上列出你的同事也可以想到的各种怪异的想法。当威胁和漏洞重叠的时候，风险就出现了。

最后，考虑你已经采取的应对这些风险的对策。你的防御可以阻止你阐明的情景中的攻击吗如果不能，你可以在最低程度上快速删除不当之处并立即作出回应吗？

当然，你不能使用恶意人士和恶意软件攻击你的所有方法。攻击者都是创造性的，并在不断革新。还有一句老生常谈：你不能总是和攻击者想到的一样，但是你可以有时和他们想的存在某些相同之处。因此，确保你最少可以防御你的团队考虑到的最常见和破坏最大的攻击。不采用这些基本的威胁建模，你可能会受到可预测的、很明显的攻击，而这些攻击原本应该可以防御的。

OWASP（Open Web Application Security Project）的团队已经总结了各种威胁建模方法大纲，这是从微软自己的程序中获得的灵感。这份摘要描述了确定去也最大威胁和相关风险的不同方法。很多公司也正在开发自动威胁建模软件，包括 Skybox Security。

(作者：Ed Skoudis 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。

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

漏洞分析新工具：RE:trace

两名安全工程师在上周推出一种基于 Ruby 的新 framework，能够发现和攻击在 OS X、Unix 和其他操作系统上运行的常见应用软件存在的漏洞。

这个新的 framework 叫做“RE:trace”，它利用苹果公司 Leopard 操作系统中的 DTrace 性能监控工具，为安全专家和逆向工程师提供了同时在堆栈和堆发现漏洞的能力，然后运行各种有趣的测试。DTrace 是由 Sun Microsystems 开发的，最初是想帮助应用软件和操作系统进行疑难问题解决，但安全专家也将它运用在其他工作任务的用途上。

在华盛顿的黑帽大会上，高级安全工程师 Tiller Beauchamp 和安全工程师 David Weston 演示了如何使用 RE:trace。它基于 DTrace，不仅可以发现堆和堆栈溢出漏洞，还可以检测到缓冲区溢出，并在溢出对存在漏洞的软件造成真正的崩溃前，加以阻止。当数据在某给定应用软件中流通时，该 framework 还可以让用户对该数据进行追踪。

“花在漏洞分析的时间大大减少。”Weston 说。

DTrace 是在内核中运行的，这样就可以易于访问整个操作系统，Weston 说。由于它具有的特性广泛，本质上而言，它是一个“友好的、可编程的 rootkit”。但是 DTrace 不是特意作为逆向工程工具而编写的，所以它不包括逆向工程师可能需要的便利工具。所以 Weston 和 Beauchamp 通过使用 Ruby 语言，增加了特性，包括用面向对象的方式在内存和追踪应用软件中 dump 搜索的能力。

RE:trace 还为用户提供了所查看的应用软件正在发生什么的反馈信息。比如，framework 能够告诉用户谁分配了某字节的内存；谁使用了它；在一次攻击中，有多少的内存溢出；是否内存曾被释放。

Weston 和 Beauchamp 计划继续开发 RE:trace，并将在接下来的几个月内增加更多的特性和功能。

(作者：ennis Fisher 译者：Shirley 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工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对目标企业进行等级式的社会工程攻击，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。
- ✧ 记录测试中的所有的交互动作，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。

(作者：Ed Skoudis 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，你可能就可以个给漏洞打补丁，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。

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

道德黑客十训（上）

在互联网刚刚兴起的时候，我们经常可以听到渗透测试，但是最近几年这种狂热已经减轻了。这种信息风险评估方式——21 世纪中它的名字是道德黑客——正在复兴。人们开始看到以黑客的方式思考来防御黑客是全面信息风险管理项目的不可或缺的一部分。

在过去几年中，我们看到了很多道德黑客的正面和反面的意见，但是我想要和 TechTarget 中国的读者们分享我以自己的经验和其他人的成败中总结出的 10 条经验。希望其中一两条可以对你的道德黑客工作有所帮助。

1.必须有书面资料

你已经听到一千遍了，但是不管你信不信，我曾看到过在没有任何书面材料的情况下，安全专家就在关键的业务系统上进行——而且安全经历也同意——道德黑客活动。你可能已经涵盖了你的资产，而且不仅需要参与各方的基本的结束信息，而且还要考虑和记录谁要（谁不要）在测试中出错的时候负责任。在道德黑客活动中也会有不好事情的发生——服务器可能崩溃，数据可能丢失。从业务的角度考虑这个问题。你的律师和保险商会以你为傲的。

2.必须要有目标

和成功的商业投资一样，你需要确定经过道德黑客活动，想要取得什么样的具体结果。你期待什么样的救国？是为了证明你需要迁移到 Novell 或者 Unix 的平台吗？想要在安全方面获得更多的资金吗？是为了遵守政府法规或者满足安全标准吗？还有问问自己想要保护那些信息，哪些系统需要测试。

3. 不要一次性测试所有系统

这一条不适用于小型网络，但是谁还再使用“小型”网络呢？排列需要测试的系统，并首先测试最重要的系统。这些可能是 Web、邮件或者数据库服务器，甚至是路由器和防火墙等边界设备。查找失败的单独的节点或者业务不能缺少的系统。很多安全专家都只关注可以公共访问的主机。记住，黑客活动可能发生在网络内部，所以不要完即内部威胁以及可能受到影响的系统。

4.不要忘记测试“不重要”的系统

这一点和第三条有冲突。这么说不准确。你不需要测试所有的系统，但是这对于思考攻击的发生以及对其他不太重要的系统产生的影响有所帮助。没有机密数据的工作站、远距离工作的家用电脑或者只提供基础邮件访问的 Web 服务器都会被用于攻击其他更重要的系统的跳板。不要排除流氓“小人物”。

5.以敌人的方式思考很有帮助

紧跟第四条经验的是经过证明的好经验“了解你的敌人”。这可能是老调重弹，但却是正确的。如果系统的测试只使用了最新的自动化工具，而没有考虑所有的其他可能发生的各种手动攻击的方式，就不能看到全景。对每一种可能的黑客活动从每个角度都进行测试是不可能的。关键是要确保确实进行了研究，而且理解了黑客的动机和方式，并以此构成了道德测试项目的一部分。

（作者： Kevin Beaver 译者：Tina Guo 来源：TechTarget 中国）

道德黑客十训（下）

6. 使用合适的工具

这是我每一次进行道德黑客测试的时候，我都会被这样提醒。我不知道没有了我在这几年里收集的工具（有免费的，也有商业化的），我还能做什么。就好像成功的住宅设计师所讲的：为了完成工作，你需要有合适的工具。否则，这就是没用的演习，也得不到结果。最为安全经历，要确保你的团队或者你所雇用的第三方道德黑客拥有合适的工具。很多都不容易使用，而且不便宜，但是他们一定有必要。

7. 要有时间计划

每一次都听说有人在一分钟内把一百万个信息包砸向系统，查看 TCP/IP 是否稳定。这种测试可能可以，但是就像老人家告诉我们的，做事情要有合适的时间的地点。确保道德黑客测试不是在网络或者主机的使用高峰期进行的。你也不想要网络运行速度变慢或者引起系统崩溃。如果在测试正在进行时，系统不稳定或者存在其他请求的超载，也有很多安全工具可以完成。安排时间表，并写下来。

8. 不要认为没有渗透就安全了

一个常见的误解是如果没有可能的渗透，那么系统就一定是安全的。不是的！可能是没有使用合适的工具或者没有测试合适的系统。还可能是在测试系统的时候，漏洞还没有被发现。道德黑客是一些特定系统的快照。应有有欺诈路由器（或者用户）在没有注意到的或者不是初始范围内的其他位置渗透一个安全问题。你永远看不到。

9. 维持这项优秀的工作

第八条的原因使第九条更重要。我知道你听到过一次次的测试系统。这是真的，事情总是在变化。新的威胁和漏洞突然出现。确保你的系统进行了定期测试，检查新问题和过去错过的漏洞。确保你的系统。循环是关键。

10. 关注重要和紧急漏洞

我曾见看到很多安全经理觉得有义务修复在道德黑客过程中所发现的每一个漏洞。这实际是不能的。给自己或自己的团队增加压力保障每一处的安全是不合理也不公平的。当区分每日工作的优先顺序的时候，可以根据管理专家推荐的时间：查找重要（如果被利用会产生很大的影响）和紧急的（被利用的可能性很高）漏洞。其他的漏洞可以根据时间、资源和资金的允许以后解决。

如果你可以把我在这几年了总结的 10 条经验中的一部分应用到你的道德黑客工作中，作为一名安全经理，你的工作就会简单一些，毕竟，积少成多阿。

（作者：Kevin Beaver　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很多钱。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！

（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北京，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。

（作者：Mike Rothman　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。

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