黑客攻击技术和策略

黑客攻击技术和策略

黑客策略和技术一直都在进步。黑客还在继续开发新的攻击工具和黑客方法，来恶意访问系统并攻击你的网络，这样企业在开发和采取恰当的方法防御黑客的攻击就变得非常困难。《黑客攻击技术和策略》的技术指南将介绍黑客的内心想法，并帮助你理解恶意攻击者的动机，也提供了一些黑客攻击具体信息的方式，采用的方法以及企业应该采用的保护敏感数据的方法。 这里将会提供大量黑客技术和策路的信息，例如允许黑客获取网络系统或者文件访问的系统特征探测。你可以学到如何使用各种程序和防御措施阻挠黑客的策略和技术，包括入侵检测和入侵防御技术。本指南中还提供了保护网络端点重要性的一些建议，并将介入如何减轻黑客通过开放的网络端口连接到你的电脑的危险性。技巧还包括如何了解系统是否受到了攻击、如何保护无线网络安全以及针对终端用户在目前的威胁和防御措施培训的最佳实践。

防止黑客窃取信息

想想你们公司有的基础设施有多大可能正被不怀好意的黑客盯上。你的基础设施的信息具有多大的价值？是否知道你有多少敏感信息被黑客用小花招给公诸于众了？该怎样阻止黑客窃取你的信息呢？

- ❖ 如何防止黑客窃取信息：员工意识和风险评估策略

防御系统特征探测

真正的黑客在试图渗透一个系统时是不会像无头苍蝇一样盲目攻击的。相反，他们会利用黑客技术，如操作系统痕迹跟踪和探测技术系统地确定你公司使用的是什么系统和服务，以确定你最薄弱的环节。比如，你是否连接到一个合作伙伴网络，有一个千疮百孔的防火墙？你的

远程访问系统只需要简单的验证？你使用内部人员开发的没有检查安全漏洞的网站？这些都是黑客努力寻找的弱点。

❖ 黑客技术和攻击：防御系统特征探测

运用 IDS 和 IPS 阻止黑客

现在，每家安全厂商可能已经向你推销他们最新的网络入侵检测和防御工具或产品，声称可以做到从防止病毒到重新设置防火墙在内的各种功能。可惜的是，大多数这种商业系统都要让你花上一笔钱。在这种情况下，需要考虑预算的安全经理应该怎么办呢，尤其是在距离下一个财年还有几个月的时候。有几个免费的网络入侵检测工具可以让你在遭受黑客侵扰时敏锐察觉到危险。

❖ 运用免费网络 IDS 和 IPS 工具阻止黑客

避免物理安全威胁

墙上的小插孔连接着世界，从互联网到你公司的薪水系统。只要网线插入这个插座，他们就开始工作！谁开始工作？你可能会问。让我们从那个神秘的，在一个还不错的，安静的会议或是培训室找到一个网络插孔的人开始来看这个问题。这么做的真正的问题是什么，你怎么对付他们呢？在这里，你将学习怎样提高网络安全性以消除物理安全威胁。

❖ 网络安全：如何避免物理安全威胁

确定认证系统缺陷

好古老的登录界面。没有这个界面，安全系统还能算得上完善吗？不管是网站登录界面还是 Unix 登录提示符，大多数系统的安全都完全依靠一个有效的用户名和密码来证明用户的身

份。由于这通常是唯一的访问条件，所以很值得把你的身份验证安全系统放在放大镜下测试一下，看看能不能找出一些身份验证的弱点并看看他们如何拦截好奇的黑客。

❖ 确定认证系统缺陷 抵御黑客攻击

改善访问请求流程

许多公司都使用定义模糊、过时、繁琐、且效率低下或不安全的访问请求流程来处理公司内部的应用程序、数据以及系统的访问请求。通常，他们还会使用一份旧的，过时的，复制了不知多少次以至仅能勉强辨认的印刷表格。更糟的是，它往往并不要求有适当的签名或数据和系统的访问授权。如果你想要通过某项严格的审计并改善你所用的访问请求处理程序，那就继续读下去!

❖ 使用系统认证改善访问请求流程

社会工程攻击策略和威胁

你已经安装了两个防火墙，一个入侵防御系统（IPS）并配置了杀毒软件，因此对企业整个的网络安全状况感觉良好。服务器打过补丁了、信息数据包也处理过了，而且当网络流量出现异常的时候你会收到警报，并当场杀毒。耶！生活太美好了。那么问题出在哪儿呢？

❖ 了解社会工程黑客攻击策略和威胁

远程访问点保护

黑客喜欢配置不良的远程访问点，为什么呢？很多时候，这些访问点都代表了进入网络的开放的大门，而不需要考虑互联网边界的防火墙以及入侵检测/防御系统。考虑到这些配置不良的设备带来的威胁，所有公司都应该保护远程访问点，并配置远程连接来防御攻击。实际

上，大部分的网络都有远程访问点，而这些访问点大部分都没有采用恰当的安全策略。远程访问点大部分都是拨号猫或者 VPN 集中器，找到电话号码或者 IP 地址也不费多大劲。

- 远程访问点保护及防御攻击的连接配置

保护 Web 服务器

在操作系统不定发布并在你的环境中测试的时候，Web 服务器应该第一批打补丁，防御 Web 服务器的攻击。在发现漏洞的几天内，任何人都可以获得攻击代码。在黑客获取到之后的几天内，准备好的攻击可能已经发生了，可以成功攻击你没有配置补丁的 Web 服务器。几乎没有时间给这些漏洞测试和安装补丁，所以在补丁发布前设计配置计划非常重要

- 保护 Web 服务器 防御黑客攻击

访问点的认证和加密

随便穿过一个本地的商业公园，我就筏县乐大约 15 个向公公开发的无线接入点，而其中几个不需要认证就可以访问公司的网络。如果你用无线网络接口打开你的笔迹本，并在城市里面走动，也没有什么太奇怪的。为了保住你的无线网络不受那些查找接入点的 war-driver 的影响，利用认证和加密等基础方法提高无线访问点的安全性非常重要。副标题简介

- 无线安全基础：访问点的认证和加密

如何判断是否被黑

最坏的情况是：你有已经被黑的奇怪感觉，但是你不确定下一步应该怎么做。如果你和大部分的 IT 人士一样，你就不需要知道在哪儿查找系统被攻击的证据，那么你要如何判断你是否被攻击了呢？让我们看看在系统泄露后可以找到的更常见的证据吧。

❖ 如何判断是否被黑：系统被攻击的特征

如何防止黑客窃取信息：员工意识和风险评估策略

想想你们公司有的基础设施有多大可能正被不怀好意的黑客盯上。你的基础设施的信息具有多大的价值？是否知道你有多少敏感信息被黑客用小花招给公诸于众了？该怎样阻止黑客窃取你的信息呢？

任何一个真正的黑客的攻击总是从侦察目标开始的。让我们来看看几个比较常见的技术同时也学学如何制止黑客窃取信息。

往往网上散布着的关于你公司的敏感信息会多得让你惊讶——它们就那样等着被人发现。你是否曾经上 IT 论坛搜索你的域名？试试看！公司技术人员很可能会在公共论坛上发布问题和解答，其间会提及公司正在使用的具体设备，也许他们使用的还是他们的工作电子邮件的地址！哎哟！很显然，他们没有意识到危险：那些黑客可能不需要接触你的网络就了解了你在使用哪种类型的防火墙或服务器。

为了避免这种情况，可以开展一个员工意识和公司风险评估政策的培训，从而要求企业用户在公共论坛发布任何信息时使用非工作电子邮件地址。确保你的员工知道公司的名称不应该出现在这些贴子中。这样做并不会影响他们的问题得到解答，然而公司的基础设施的细节却不会让全世界都看到了。

为了了解你的技术人员的信息，另一个黑客会去的地方是在线 IP 地址数据库和网站登记库。 实际上，全球的这类信息被分别保存在四个数据库中。检查 ARIN.net 上的 Whois 数据库，看看在你的公司的域名列表下是否有你公司的技术人员的名字、邮箱、或是电话号码。理想的情况是，你应该只提供了公共的信息，以防止黑客猜测这些人员的身份信息，从而诱使你的员工泄露他们的密码或其他敏感信息。

一个人的垃圾是另一个人的宝藏...是有这么个谚语！“捡垃圾”是一个古老的，肮脏的，但仍效果显著的信息收集技术。攻击者通过分析你不要的信息，寻找社会安全号

码，电话号码，用户 ID，IP 地址和密码。鉴于此，员工意识培训计划应得到认真地执行，以教会员工如何妥善销毁任何可能被利用的信息。您可能认为这是不必要的，但我仍然鼓励你们，特别是 IT 领域的公司，检查每一台网络打印机旁废弃文件的内容。想想如果你发现的东西到黑客手里，你会觉得放心吗？

（作者：Vernon Habersetzer　译者：Sean　来源：TechTarget 中国）

黑客技术和攻击：防御系统特征探测

真正的黑客在试图渗透一个系统时是不会像无头苍蝇一样盲目攻击的。相反，他们会利用黑客技术，如操作系统痕迹跟踪和探测技术系统地确定你公司使用的是什么系统和服务，以确定你最薄弱的环节。比如，你是否连接到一个合作伙伴网络，有一个千疮百孔的防火墙？你的远程访问系统只需要简单的验证？你使用内部人员开发的没有检查安全漏洞的网站？这些都是黑客努力寻找的弱点。

在每一个黑客工具包都有中有各种各样的免费的系统探测和痕迹跟踪的工具，用来确定你的硬件和软件的具体配置。毫无疑问，这些工具中有些能检查可能泄露的路由器和防火墙上开放的端口以及系统服务。要了解黑客怎么做，你只需下载并运行这些工具对你自己的网络演练一下。请务必让您的工作人员学会发现什么时候这些工具正在运行，以便在性能出现问题时，知道是由黑客的扫描引起的。记住始终提前对一些非关键的设备试验一下。

阻止那些旨在访问你的系统的黑客技术的第一步是关闭不必要的防火墙输入端口。开放的端口应该让应用该端口的服务打好补丁保护起来，如 Web 服务，电子邮件和 FTP。你的软件供应商应能提供最新的补丁。CERT 列出了那些你可能在运行的服务所具有的漏洞信息。此外，Cassandra 是一个很好的免费的网上漏洞数据库。它能协助你发现正在运行的服务有哪些漏洞，其中有许多在是在别的地方没有列出的应用。

要确定是否有人使用这类工具探测和跟踪你的操作系统的网上痕迹，您需要至少用到一种能记录端口扫描，痕迹跟踪，失败的登录等行为的登录工具。理想的情况下，任何开放端口都应被入侵防御系统（IPS）监测。这个系统能在你的操作系统被入侵前检测并阻止大多数攻击。Snort 是一个常用的且开源的入侵检测系统（ IDS ）——即只侦测攻击但并不阻止他们—— 同时也是 IPS。简单地用谷歌一搜索就会发现很多 Snort 免费支持和附加组件。

无论你用什么系统检测那些对你的操作系统进行的痕迹跟踪和探测，你需要留意日志文件，以便发现哪些机器可能在探测你的系统。当检测到攻击时，许多防火墙和入侵检测/阻止系统可以通过电子邮件或是弹出一个程序来提醒你，但没有一个系统能穿过网络控制住黑客的监视器并拍开他们的手。

（作者：Vernon Habersetzer　译者：Sean　来源：TechTarget 中国）

运用免费网络 IDS 和 IPS 工具阻止黑客

现在，每家安全厂商可能已经向你推销他们最新的网络入侵检测和防御工具或产品，声称可以做到从防止病毒到重新设置防火墙在内的各种功能。可惜的是，大多数这种商业系统都要让你花上一笔钱。在这种情况下，需要考虑预算的安全经理应该怎么办呢，尤其是在距离下一个财年还有几个月的时候。有几个免费的网络入侵检测工具可以让你在遭受黑客侵扰时敏锐察觉到危险。

首先，一定要有一个用来分析网络流量的工具，特别是在网络边界附近。Snort 的 是目前最好的免费 IDS 软件，它也有商业版的可供购买。Snort 可以配置用于监测所有网络流量。通常情况下，你需要复制你的互联网入站流量到一个或多个与安有 Snort 的计算机相连接的交换机端口（用思科的话来说，这叫做把流量扩展到端口）。你唯一的成本是这台电脑本身，它可以运行在 Linux 或 Windows 上 。通常情况下，只要一台有合适硬盘空间的空余电脑就可以很好地满足要求。Snort 的可以把可疑流量转储到日志文件，在此之后，你可以随便选用几个免费告警工具，在监测到这种流量的时候，监控日志文件、邮件和页面。

其次，你得有办法分析系统安全日志。从你的网络边界开始，确保你的边界路由器通过配置了可以把 syslog 消息发送到网络内可访问的服务器上。有些防火墙也可以发送 Syslog 消息，你可以把这些消息转到同样的的内部服务器上去。有些防火前那个野可以发送系统日志信息，也可以把它转向到内部服务器上。此外，确保 DMZ 内的服务器可以从内部访问到，或者是把它们的事件日志设置指向到内部的服务器上去。在路由器、防火墙和服务器上做这些配置其实并不困难，通常只需要几个命令或几次点击就可以了。

所有的日志文件都可以访问到之后，下面要做的就是安装一个免费的告警工具或者自己开发一个。如果你有兴趣编写自己的告警工具，Batch、Perl 或其他免费脚本工具可以用来执行解析命令，如 Windows 的“查找”命令或 Unix 的“grep”命令。这可以帮助你

从 Snort 和你的服务器、路由器还有防火墙安全日志里找到可疑活动。接下来就可以使用免费的电子邮件程序，如 Blat，发送日志条目给传呼，手机或电子邮件地址。

这当然还只是开发低预算告警系统的速成教程，但你会惊讶于这样一个系统所能提供的对潜在恶意活动，如端口扫描和失败的登录尝试的报警功能，而且成本极低。

（作者：Vernon Habersetzer　译者：Sean　来源：TechTarget 中国）

网络安全：如何避免物理安全威胁

在那儿...墙上的小插孔连接着世界，从互联网到你公司的薪水系统。只要网线插入这个插座，他们就开始工作！谁开始工作？你可能会问。让我们从那个神秘的，在一个还不错的，安静的会议或是培训室找到一个网络插孔的人开始来看这个问题。这么做的真正的问题是什么，你怎么对付他们呢？在这里，你将学习怎样提高网络安全性以消除物理安全威胁。

私人设施相较于公共设施一直拥有更高的安全性，因为它们更容易达到物理上的安全。公共场所——如医院，大学和图书馆——的安全保护可能是一项挑战，因为很难在物理上做到安全。不管公共或私人的场所，网络插座频繁使用的地方总是会有某种程度的安全风险。教室，座谈室和会议室都是通常不会锁门以及任何好奇的人都能进入一探究竟的问题区域。

让我们用实例来说明这些风险。假设黑客用笔记本电脑连上你所在大楼的网络插孔。大多数网络插孔是频繁使用，也就是说它们可以连接到网络设备功能区域上。假如你运行的是 DHCP 服务器，——它会为每一个连接到网络的设备分配一个 IP 地址——同样也会为黑客的笔记本电脑分配一个。如果没有使用 DHCP，黑客可以很容易地使用嗅探器为他的笔记本电脑找到一个未使用的 IP 地址。一旦连接上网络，几个简单的命令就可以定位你的关键服务器，然后列举出用户帐户，服务就开始了。于是几分钟内，密码可能就泄露了，一两个服务器就可能被攻击了，游戏也就此结束；黑客已经赢了。摆在你面前的是一个真正的混乱情况。

幸运的是，总有办法避免物理安全威胁并阻止黑客——甚至能阻止供应商和承包商之类找到网络插孔来连接到你的网络。第一件你可以做的事是禁用会议室和教室的网络插孔，直到需要时才启用。另一个最佳实践是在任何可能的时候都把房间锁起来。第三个防御的办法是让你的网络交换机只允许特定 MAC 地址的网卡连接到网络。每一个网卡都有一

个独一无二的 MAC 地址，虽然这个地址可以通过欺骗软件改变。更严格的方案是，配置你的网络服务器，要求在每个用户登录前先认证计算机。请记住，如果你想防止未经授权的人使用已经连接到你的网络电脑，如教室的电脑，除了要求用户认证，你应该在用户端和网络端都设置电脑开机锁和屏幕保护程序密码锁。欲了解更多有关证书的问题，请联系公钥基础设施（PKI）和数字证书系统的供应商。

大多数上述建议需要服务器和网络管理员的配合。如果你不向他们解释这些真实存在的安全风险，他们未必意识到这些改变能带来的价值。可用的网络插孔是黑客入侵的通道，一旦忽视，可能导致的重大安全事件。

（作者：Vernon Habersetzer　译者：Sean 来源：TechTarget 中国）

确定认证系统缺陷 抵御黑客攻击

创】啊，好古老的登录界面。没有这个界面，安全系统还能算得上完善吗？不管是网站登录界面还是 Unix 登录提示符，大多数系统的安全都完全依靠一个有效的用户名和密码来证明用户的身份。由于这通常是唯一的访问条件，所以很值得把你的身份验证安全系统放在放大镜下测试一下，看看能不能找出一些身份验证的弱点并看看他们如何拦截好奇的黑客。

黑客通过猜测常用的用户名和密码的方法来暴力进入一个系统是非常普遍做法。最好避免使用"admin"、"test"、"user"和任何默认的用户名。需要避免的常用密码有用户 ID、"password"、"pass"和任何预设的密码。有些系统在登录失败时显示的信息让用户更容易发现一个有效的用户名。这些信息可能会说， “无效的用户 ID”。这告诉黑客，他或她应继续猜测用户名。当一个有效的用户名被发现，恶意黑客就可以看到另一个提示信息，如，“密码无效。”理想的情况下，无论失败的原因，系统的登录失败的信息应该是通用的，如“无效的用户名和密码”。否则，黑客可以列举出有效的用户 ID，并开始猜测密码，寻找到薄弱的一个。我们在下面要讲到的正是密码。

弱密码是认证系统的一个重要的安全弱点。如果可能的话，强制网络上的每一个系统，特别是网络边界上的系统遵循密码规则。密码和帐户的规则应至少需要混合字母和数字，并应指定最小密码长度，提供密码历史，帐户锁定和密码到期。如果可能的话，设置密码规则，不允许密码和用户名或者用户的名或姓相同，因为这些都容易猜到。我目标是迫使用户选择强密码。

要真正加强你的认证机制，你应该建立双因素或三因素认证系统。多因素验证意味着，用户身份验证必须提交至少两种不同类型的证书。有三类验证因素：“你拥有的”，“你知道的”，“你是什么”。认证机制的每个因素应来自不同的类别。换句话说，用户 ID 和密码仍只是单因素认证，因为这两个件事情都属于"你知道的"。一些有效的组合应是

这样的：一个电子密钥和个人身份号码（PIN）配合，指纹识别和密码配合或者视网膜扫描仪和你的声音配合。

通过改善你的认证机制，黑客想暴力进入你的系统变得更加困难。除了多因素认证系统，上述建议的采用并不会让你增加太多成本，如果有的话。

（作者：Vernon Habersetzer 译者：Sean 来源：TechTarget 中国）

使用系统认证改善访问请求流程

许多公司都使用定义模糊、过时、繁琐、且效率低下或不安全的访问请求流程来处理公司内部的应用程序、数据以及系统的访问请求。通常，他们还会使用一份旧的，过时的，复制了不知多少次以至仅能勉强辨认的印刷表格。更糟的是，它往往并不要求有适当的签名或数据和系统的访问授权。如果你想要通过某项严格的审计并改善你所用的访问请求处理程序，那就继续读下去!

建立良好的系统访问请求流程的第一步是明确本组织的应用程序和数据的归属。这就要求对应用程序和数据进行分类存储，并指定一个负责人。例如，财务总监负责会计和工资数据，销售总监负责销售数据。一旦这些应用和数据的属主已经确定，就需要创建一个更新的表格。

最好是创建一个基于 Web 的表格或定制电邮表格，以便在网上操作并且能限制仅某些员工可以获得访问权限。如果你不允许提交纸质的表格的话，那就就可以确保只有经过授权的人使用的才是最新的表格。使用基于 Web 的形式的另一个好处是，你可能会捕捉到用户的用户名和 IP 地址以便进一步证明请求来自授权的雇员。表格应该要求每一处用户需要访问的地方报请应用程序和数据的所有者批准。根据申请应用的复杂性等级，应用程序或数据的拥有者的批准可以是电子形式，或印刷形式，必要时还可以用签名的形式。通常情况下，在 IT 部门可以很容易找到一些有创建基于 Web 或电子邮件表格的经验的人。

一旦建立了表格，你应该把这些表格限制只给授权的人员，并制定让用户遵循的说明。这些说明应存放在和表格相同的位置。还应该制定一份流程图，记录 IT 部门填写申请的内部程序。

最好指定一个人维护这些表格。这样就更容易使表格的设制和修改保持一致性。稍作变动，这些表格还可以用于处理员工的离职过程。一旦你建立了健全的流程，以及易于使

用的表格，员工们就会觉得更舒服，审计人员也会觉得更轻松。只要确保你为每一个获准访问某一应用程序和数据集的人员都提供了访问申请表格。

（作者：Vernon Habersetzer 译者：Sean 来源：TechTarget 中国）

了解社会工程黑客攻击策略和威胁

你已经安装了两个防火墙，一个入侵防御系统（IPS）并配置了杀毒软件，因此对企业整个的网络安全状况感觉良好。服务器打过补丁了、信息数据包也处理过了，而且当网络流量出现异常的时候你会收到警报，并当场杀毒。耶！生活太美好了。那么问题出在哪儿呢？

黑客很聪明，而且在从毫不怀疑的员工身上获取信息的时候通常都很狡猾。你的服务台、IT 员工和普通的用户关心的是对需要帮助的人伸出援手并安抚他们。不管你的员工付出了多大的代价，它们都不能想防火墙处理数据包一样处理电话。实际上，大部分人都想在看似无辜的人需要帮助的时候伸出援助之手。

社会工程是黑客可以取得更多成绩的策略，这样必识别或者绕过防火墙和 IPS 用的时间要少很多。幸运还是不幸都依赖于你问的人是谁，安全管理员不可能屏蔽每个人的电话或者询问进入公司的每个人的 ID。你的员工，特别是那些非结构化的员工应过滤恶意请求，阻止它们通过大门和电话线进入。他们可以做这些昂工作吗？让他们做好准备的最好方式是对他们进行他们上下班时间可能遇到的社会工程黑客攻击策略的培训。

很简单，社会工程攻击包括采用明智的方式回答问题，然后使用这些问题还获取限制区域或者信息的访问。它可以是黑客假扮成服务台的技术人员询问用户的密码，或者假扮成其他人例如网络管理员、难过的用户或者需要访问通讯设备的电工、需要进入机房的消防人员、看门人或者其他可信人员。这些类型的人想要访问电脑或者机房的难度有多大呢？你向那些不期而遇的电工询问 ID 的次数有多少呢？如果你在布线室发现了一位“电工”，你会问他问题吗？如果你和大部分人一样，你就会认为一切正常，并继续做你的工作。这种行为试验模式正是黑客预计的行为。

除了员工培训，这些类型的攻击最好可以通过制定社会工程防御策略来阻止。这些策略要禁止在电话和邮件中泄露敏感信息，禁止通过大门，并要求访问者佩戴标志。我还高度推荐你读一下 Kevin Mitnick 关于社会工程的书，叫作《欺骗的艺术》（The Art of Deception）。通过查看安全的人为因素，你就可以防御对公司顶级机密的非授权访问。

（作者：Vernon Habersetzer　译者：Tina Guo 来源：TechTarget 中国）

远程访问点保护及防御攻击的连接配置

黑客喜欢配置不良的远程访问点，为什么呢？很多时候，这些访问点都代表了进入网络的开放的大门，而不需要考虑互联网边界的防火墙以及入侵检测/防御系统。考虑到这些配置不良的设备带来的威胁，所有公司都应该保护远程访问点，并配置远程连接来防御攻击。实际上，大部分的网络都有远程访问点，而这些访问点大部分都没有采用恰当的安全策略。远程访问点大部分都是拨号猫或者 VPN 集中器，找到电话号码或者 IP 地址也不费多大劲。

大部分的远程访问点只要求静态的用户 ID 和密码就可以登录网络。如果你的远程访问点不要求强大的认证，你可能就应该考虑在某个地方，你的员工或者厂商已经用保存的用户 ID 和密码建立到你网络的远程访问连接。这也就是说打开连接的任何人都可以访问你的网络，包括你员工的邻居，他们的电脑可能在一个月前用于查收邮件了，也包括你厂商的员工，他可能上周离职了，并带走了他所有客户的远程访问密码。

如何保护远程访问并配置远程连接

为了解决这个问题，最好采用某种强大的认证，要求用户 ID 和单次使用的密码或者生物认证。有些厂商销售远程访问密钥连令牌，这些产品可以没几秒产生一个新的单次密码。另外，你的供应商和厂商可能需要给你的操作部门打电话要一个远程访问密码，那么在处理外部的访问者的时候要多增加一些安全措施。通过采用强大的认证系统，保留远程连接的密码就不会存在信息安全风险了。

另外，大部分的远程访问点都不检测远程计算机的病毒或黑客软件，而且他们通过不会观测从这些计算机来的网络流量。如果使用带病毒的电脑的用户或者黑客使用这样的软件远程登录你的网络，网络就可能处于服务器攻击或者病毒爆发的接收端。为了帮助防御远程连接攻击，最好在远程连接点和内部网络之间使用 IDS 或者 IPS。这样的系统就可以

捕获黑客基于网络的攻击或者杂生病毒。有些系统甚至可以防止杀毒软件没有更新的用户连接到你的网络。另外最好可以限制访问内部网络的端口数量。

通过留意认证过程以及来自远程用户的流量，你就可以大大减少远程访问点变成不受欢迎的公司的风险。

(作者：Vernon Habersetzer 译者：Tina Guo 来源：TechTarget 中国)

保护 Web 服务器 防御黑客攻击

在操作系统不定发布并在你的环境中测试的时候，Web 服务器应该第一批打补丁，防御 Web 服务器的攻击。在发现漏洞的几天内，任何人都可以获得攻击代码。在黑客获取到之后的几天内，准备好的攻击可能已经发生了，可以成功攻击你没有配置补丁的 Web 服务器。几乎没有时间给这些漏洞测试和安装补丁，所以在补丁发布前设计配置计划非常重要。

看一下 Web 代码，黑客有几种操控网站 URL 执行 SQL 注入、目录移动和缓冲器一处等的方法。防御这三种类型的漏洞又两种常见的方法。其一是让一个人或者工具检查你的 Web 代码，识别并修正漏洞。或者你可以安装应用防火墙，检查 yon 过户的输入，在它进入后门应用前确定它不是恶意或者格式错误的。Blue Coat Systems Inc.和 Sanctum Inc.都有这种的产品，值得看看，特别是在你认为不能给程序员再次作编写安全代码的培训的时候。

如果你是用网站销售产品或者提供金融服务，检查提交到服务器处理在线订单的数据就具有极大的重要性，如果你的安全性只是依赖于网页上显示给用户的价格或者帐户信息，使用在黑客的电脑上运行的代理工具就可以进行简单的操作。这样的工具允许攻击者改变提交到你的服务器上的数据，移除网页本身执行的所有限制。一本价格是 50 块的书可以改到 1 块钱，而银行账号可以在资金转账或者显示其他张户的帐户平衡时改成其他人的。

根据你处理终端用户提交的信息的方式，你可以采取以下验证终端用户的方式。例如，大多数程序可以编写为在处理提交的数据前，检查数据中的不恰当的字符和长度。这种验证应该放在后端执行，而不是限制网页上的输入区域，因为网页上的限制可以使用上面提到的代理工具绕过。

Web 服务器是从外部进入公司网络的第一个方法。通过采用恰当的 Web 服务器防护措施保护 Web 服务器，你就可以解决网络上风险最大的问题，并防御潜在的极端危险的攻击。

(作者：Vernon Habersetzer　译者：Tina Guo 来源：TechTarget 中国)

无线安全基础：访问点的认证和加密

随便穿过一个本地的商业公园，我就筏县乐大约 15 个向公公开发的无线接入点，而其中几个不需要认证就可以访问公司的网络。如果你用无线网络接口打开你的笔迹本，并在城市里面走动，也没有什么太奇怪的。为了保住你的无线网络不受那些查找接入点的 war-driver（译者注：War Driver 就是携带着一台标准的手提电脑、无线 NIC 卡驾车在城市商业区四处游逛。这样就可以准确地确定所在地区内所有 802.11 网络的位置及它们是否使用 WEP。）的影响，利用认证和加密等基础方法提高无线访问点的安全性非常重要。

无线访问点可以通过配置实现访问点 SSID 和域名的广播，而通常这是不需要的。通过关闭广播，你可以在很大程度上停止对外界公开你的网络。是的，SSID 是在无线节点连接到无线网络的时候传输的，但是相比较之先它还是不常见的。SSID 应该设置为不能描述企业信息，从而使黑客了解无线网络的所有者更加困难。

无线安全加密可以防御有人在数据传播的时候读取到，而且可以和有线等效保密（Wired Equivalent Privacy，WEP）、WPA、EAP-TLS 或者虚拟专用网软件一起使用。WEP 缺少真正的认证，而是使用静态加密密钥。而静态加密密钥只需要用免费软件在很短的时间内就可以获取到，对不断地窃听者提供的防护也很少。WPA 要求认证，并使用较长的动态加密密钥，而它被攻击的可能也降低了。但是 WPA 确实要求兼容的客户端硬件和软件。EAP-TLS 使用数字证书验证和加密使用 SSL 的无线流量，但是要求某种程度的复杂的 PKI 架构。

无线天线通常有电力设置，可以允许调整信号的传输强度。最好把天线调整为他们正好可以覆盖需要无线访问的范围，而不要进入可能潜伏了黑客的地方。

大多数的无线访问点还允许限制媒体存取控制（MAC）地址的访问。MAC 地址是只 用于识别每个网络节点的硬件地址。但是要警惕，它也可以被攻击，使用的是可以捕获网络

上允许的设备的 MAC 地址的被动无线嗅探器攻击。一旦获取到了，黑客就可以伪装他的 MAC 地址，而且也不会只限制在那一层了。限制 MAC 地址可以增加必须攻破的层，值得考虑使用。

这是对无线安全基础和风险的简要介绍，但是它可以让你全面地查看管理无线网络和无线访问点安全策略的时候肯定会面对的一些真实问题。

(作者：Vernon Habersetzer 译者：Tina Guo 来源：TechTarget 中国)

如何判断是否被黑：系统被攻击的特征

最坏的情况是：你有已经被黑的奇怪感觉，但是你不确定下一步应该怎么做。如果你和大部分的 IT 人士一样，你就不需要知道在哪儿查找系统被攻击的证据，那么你要如何判断你是否被攻击了呢？让我们看看在系统泄露后可以找到的更常见的证据吧。

开始，可疑的用户帐户（那些不符合特征或者习惯的账户应该在大部分的有效用户账户中禁止）应该禁用，研究一下并决定谁设置了账户以及设置的原因。如果开启了恰当的审计，审计日志可以显示谁创建这些账户。如果有可能确认账户创建的日期和时间，而且账户最终显示是黑客攻击的结果，你就可以在时间表中查看其它可能相符的审计日志事件。

为了确定可疑应用是否正在监听可以作为攻击的后门端口的入站连接，可以使用 Microsoft Windows Sysinternals 或者 Fpipe from McAfee Inc. Foundstone 部门的的 TCPView 等工具。这些 Windows 功能可以显示那些应用使用了系统上的开放端口。对于 Unix 系统，使用植入到操作系统中的 netstat 或者 lsof。因为机敏的黑客可以使用木马（不会显示黑客打开的端口）替换 netstat 或 lsof 程序，最好可以从另一台计算机上使用 Nmap 端口扫描器扫描受攻击的系统。这样可以提供系统开放端口的不同角度的看法。攻击 Windows 服务器的黑客可能增加或者替换从以下区域通过注册表启动的程序：

- HKLM > Software > Microsoft > Windows > CurrentVersion> Run
- HKCU > Software > Microsoft > Windows > CurrentVersion> Run

恶意软件业可以从操作系统的工作表中启动。要查看 Windows 系统上计划运行那些工作，可以打开命令提示符，并键入 AT。在 Unix 体统上，使用 cron 或者 crontab 命令查看计划运行的工作表。

攻击 Unix 系统的黑客可能使用了 rootkit。它可以帮助黑客通过攻击操作系统的漏洞或者安装应用或者根访问。因为黑客可以使用大量的 rootkit,确定那些文件被修改了非常困难。有些程序可以帮助进行这项工作，例如 chrootkit。黑客可以使用很多方法掩盖他的踪迹，但是查看上面提到的项目是确定你是否被黑的很好的开始。

(作者：Vernon Habersetzer　译者：Tina Guo 来源：TechTarget 中国)