<<Cisco网络黑客大曝光>>

图书基本信息

书名：<<Cisco网络黑客大曝光>>

13位ISBN编号：9787302174363

10位ISBN编号：7302174369

出版时间：2008-6

出版时间：清华大学出版社

作者：安德鲁

页数：574

字数：824000

<<Cisco网络黑客大曝光>>

内容概要

这是国内第一本系统地介绍Cisco网络安全性的书籍。
本书从攻击者和防御者的不同角度阐述了Cisco网络的攻击手段及其防御措施，并提供了许多真实的案例研究。
　全书共分为4大部分14章。
第1部分从防御者和攻击者的角度概述了不同的网络拓扑、架构和设计会如何影响其安全性：第2部分是本书的核心部分，描述了攻击者首先如何列举整个网络，然后挑选特定的目标，精确地定位这些目标，发起适当的攻击，获得并保持超级用户级别的访问，然后通过或从被入侵的Cisco设备发起进一步的毁坏性攻击；第3部分描述了协议漏洞及其利用，入侵者利用协议漏洞可以完全控制网络流量；第4部分提供了极有价值的补充技术资料，能帮助读者理解、掌握本书描述的概念和技术。
　本书是负责安全保障的网络管理员和系统管理员的必备工具书，也可作为对网络安全感兴趣的研究人员的重要参考书。

作者简介

Andrew A.Vladimirov博士，通过了CCNP、CCDP、CISSP、CWNA、Linux+认证，是国际IT安全顾问公司Arhont公司的创始人之一。

Konstantin V.GavrilenkO，是Arhont公司的创始人之一，在Cisco PIX防火墙和Cisco VPN集中器方面具有极其丰富的经验。

Janis N.Vizulis，是专

<<Cisco网络黑客大曝光>>

书籍目录

章节摘录

第1部分　基础知识　　第1章　Cisco网络设计模型及其安全概述　　对于具有多台路由器、交换机、服务器、工作站和其他更奇特的主机的公司或团体网络而言，它的安全性不太容易实现。
在认真研究安全问题之前，你应该更全面地了解你的网络的运转。
你要详细地了解网络中采用的所有被路由协议和路由协议，还要清楚部署的所有网络设备的角色和功能。

与许多其他的网络安全书籍不同，本书没有详细地阐述网络和安全基础，包括OSI（开放式系统互联）模型及其与TCP／IP（传输控制协议／网际协议）之间的映射关系、CIA（机密性、完整性、可用性）三元组和安全策略的制定。
本书讲述如何黑（攻击）CiscO设备和围绕着CiscO设备组建的网络。
我们期望读者具有网络和信息安全基础，我们还希望能详细地提供反映了本书书名的实用信息。

熟练的专业黑客将目标网络当作一个完整的实体。
他／她不会错过侵入任何网络设备的机会，只要有可能，将来就利用它进一步对目标网络进行漏洞利用。
这类似于如果你获得了类UNIX系统上的一个用户账号，在进行本地访问之后就更容易获得根账号了。

作为网络安全维护人员，你应该彻底地评估并保护整个网络基础设施。
为了正确地提供深度防御，你所采取的安全措施必须涵盖整个OSl模型的7层，同时还要考虑部署的每台单机的安全性。
幸运的是，现有的CiscO网络安全解决方案涉及到了你所能想到的网络的每个方面，其范围从多协议标签交换虚拟专用网络（MPLS VPN）到用于用户台式机和笔记本的终端软件的安全措施。
不幸的是，只有少数系统管理员、网络集成和架构师、IT安全顾问了解这些解决方案的范围和能力。

此外，为了有效地利用许多CiscO网络安全装置并具有良好的投资回报率（RoI），需要将它们正确地部署在所要保护的网络中。
这意味着要从最初的设计阶段实现网络安全，因为在网络进入搭建阶段之后，即使添加最强大、昂贵的CiscO安全装置也可能毫无帮助，起不到应有的保护作用，造成巨大的资源浪费。
不过，CCDP（Cisco Certified DesignProfessional）学习教程通常没有将安全性列入互联网的设计目标中，或者没有将它作为最初的互联网设计步骤中的一部分。
从我们的角度来看，这是一个致命的错误。

本章试图通过讲述针对CiscO推荐的网络设计模型和层次的安全措施，来纠正这种错误和其他潜在的CiscO互联网设计错误。
第2章继续讨论这个主题，概述了层次化网络的各个层上对应的各种CiscO安全措施。
从攻击者的角度来看，这两章阐述了攻击可能会被阻止的地方、会被记录的可疑活动，以及启动的事件响应过程。
攻击者可以清晰地获得以下信息：如果基于CiscO的网络被正确地设计并维护着，而且管理者具有安全意识，那就最好别动它，否则就要承担后果。

1.1 CiscO网络设计模型：安全观点　　CiscO推荐了几种实用的设计模型，选择哪种取决于网络规模和目的。
每种模型在安全性方面都有其优缺点，各种方案在安全措施的可用性、配置和维护方面都存在很大差别——这些方面有些类似于军队所采用的命令、地点部署和战术，它们取决于即将打响的战斗所处的地形。

1.1.1　平地模型　　平地模型（flat earth model）是一种基于Layer 2的网络设计。
过去，网络包括集线器、中继器和网桥。
随着以各种802.11 LAN和8O2.15（如蓝牙）用户访问设备为代表的无线网络的不断增长，现在主要是基于交换的设计了。
理论上，平地设计模型应该只应用于规模有限的小型办公室／家庭办公室（SOHO）的局域网

，CCDP指南建议如果网络中部署的节点超过50就不要采用这种模型。
实际上，每个广播域中有数十个用户是很平常的，无线的扩展使得这种状况更糟糕，因为普通的12个端口的交换机可能会接入几个访问点，而每个访问点具有30-40个用户。
此外，许多Cisco Catalyst交换机是可堆叠的，它们本身就具有很多端口。
如果TCP／IP允许每个LAN最多具有500个用户，而不会使得广播流量严重影响性能，那么网络搭建者就会部署这种LAN，根本不会对管理和安全问题加以考虑。
对他们而言，这种冒险仅仅是“充分利用Catalyst交换机的容量”以及“充分利用花出去的每一分钱”。
平地模型被认为很不安全，只能采取很少的措施来对抗使用Ettercap、Hunt、Taranis和类似工具的黑客。
传统的平地模型安全措施包括媒质访问控制（MAC）地址过滤和利用虚拟LAN（VLAN）划分网段。
基于MAC地址的设备认证是旁路的基础。
尽管比较费力，但为交换机端口分配MAC地址（数量是预先设定好的）以及手工分配所有允许的MAC可以有效地防止交换机CAM表由于遭受洪流攻击而变得无效。
IOS类型和Set／Clear CLI（Command Line Interface，命令行接口）Catalyst交换机都支持任意选项的MAC地址过滤——务必要实施MAC地址过滤。
如果方式正确的话，管理大型MAC地址过滤表并不是那么麻烦。
可以抽取并保存交换机配置文件（或只抽取CAM表），然后在工作站上进行编辑（也许可以使用一点Perl脚本），产生要上传到交换机上的新配置文件。
你甚至不需要登录进去；正如http：//www.ciscO.com／warp／public／477／SNMP／cam-Snmp.xhtml上面所解释的那样，通过SNMP（Simple Network management Protocol，简单网络管理协议）可以方便地从Catalyst交换机获得MAC地址信息。
VLAN网段的好处是显而易见的；CiscO设备通过专有的VLAN（PVLAN）和VLAN访问列表（VACL）额外地增强了VLAN。
运行CatOS 5.4或更新版本的Catalyst 6000交换机以及运行CatOS 6.2或更新版本的Catalyst 4000、2980G、2980G—A、2948G和4912G型号都支持专有VLAN。
采用CatOS 5.3或更新版本的Catalyst 6000支持VACL；如果安装了PFC（Policy FeatureCard，策略功能卡），就可以不需要路由器在Catalyst 6500的Layer 2实现VACL。
由于VACL条目的查找和执行是在硬件中实现的，所以不会造成性能下降，转发率始终不变。
第12章详细讨论了PVLAN、VACL和Cisc0针对各种VLAN跳跃攻击（jumping attack）的对应措施，第2章则概述了它们在基于Catalyst 6500的入侵检测中的角色。
目前请记住，PVLAN和VACL可能是你的网络安全设计计划的有益补充；请明智地选择Catalyst交换机和软件以免今后不得不进行升级。
平地网络模型安全方面的重大变化发生在2001年6月l4日，当时IEEE标准委员会通过了802.1x，这是一种基于Layer 2端口的网络访问控制标准。
802.1x为连接到交换机、路由器或无线访问点的设备提供了一种认证和授权机制。
实际的认证和授权是通过代表认证方设备的RADIUS（Remote Authentication Dial—In User Service，远程认证拨号用户服务）或TACACS（Terminal Access ControllerAccess Control System，终端访问控制器访问控制系统）服务器和请求方（认证主机）提供的凭证实现的。
图l.1描述了通过802.1x保护的平地网络模型。
两台RADIUS服务器为终端用户机器提供认证和授权，一台交换机作为认证设备。
RADIUS服务器之间的一条额外的链路提供了弹性，它们必须使用故障切换协议，如CiscoHSRP（Hot Standby Router Protocol，热备份路由器协议）或IETF VRRP（Virtual RouterResilience Protocol，虚拟路由器恢复协议），以便在一台认证服务器失效时仍然可以提供服务。
请记住，HSRP涵盖了在采用这种协议时必须要考虑的安全问题（参看第13章），VRRP也是如此，但涵盖的稍微少一些。
图1—1中的交换机可以是支持基于802.1x的Cisco IBNS（Identity.Based NetworkingServices，网络身

份认证服务）技术的任何Catalyst交换机，例如Cisco Catalyst 4000、4500或6500系列。
此外，也可以用固件支持WPA（Wireless ProtectedAccess，无线保护访问）业界认证需求的CiscoAironet无线访问点来取代交换机。
在本书成稿之时，只有WPA第1版，但802.Lli无线安全标准（WPA就基于这种标准）最终被通过了，而wPA第2版正在开发之中。
访问点使用何种版本的WPA都是无所谓的，因为它们都利用802.1x分发、管理所有的设备或所有的会话安全密钥以及认证无线用户。
因此，可以安全地（有时没有这么安全，请参看我们的书籍Wi-foo:The Secrets of Wireless Hacking）分隔开平地无线LAN中的设备。
正如你所了解的，“简单的”平地网络模型安全并不只是通常看起来的那样简单。
请耐心点，本书的第3部分将揭示针对“普通的”基于CiscO的LAN的许多Layer 2攻击及其对应措施。
1.1.2 星形模型 星形模型（star model）是一种非常经济的网络设计方式，用单个路由器作为中心点，为整个网络提供连接。
图1.2说明了用一个VPN集中器（concentrator）代替临时路由器。

<<Cisco网络黑客大曝光>>

编辑推荐

以久经考验的“黑客大曝光”方法学，为你的Cixco网络部署防御堡。

通过从入侵者的角度探查Cisco网络和设备，来抵御最隐秘的攻击。

本书逐步骤地展示了黑客如何定位暴露在外的系统，如何获得访问权限，以及如何控制受害网络。书中涉及了所有的特定于设备以及与网络密切相关的安全问题，同时辅以真实的例子、深入的案例分析以及详细的应对措施。

本书包罗万象，从交换机、路由器、防火墙、无线网络以及VPN漏洞到Layer 2中间人、VLAN iul33P、BGP、DoS和DDoS攻击。

通过了解如何发现以CiSCO为中心的网络中的新漏洞以及它们是怎样被计算机罪犯滥用，能让你防患于未然。

此外，你还可以从WWW.hackingexposedciscO.com获得未公开的CiscO命令、安全评估模板和重要的安全工具。

<<Cisco网络黑客大曝光>>

版权说明