<<局域网交换机安全>>

图书基本信息

书名：<<局域网交换机安全>>

13位ISBN编号：9787115229908

10位ISBN编号：7115229902

出版时间：2010-7

出版时间：人民邮电出版社

作者：（美）维恩克，（美）培根　著，孙余强，孙剑　译

页数：298

前言

人们常认为局域网和以太网交换机与管道系统很相似，易于安装、配置。
但恰恰是看似简单的东西，往往容易忽略对其安全性的关注。
以太网交换机存在着多个安全隐患。
利用这些隐患的攻击工具几年前就已经问世（例如著名的dsniff软件包）。
运用这些工具，黑客可以打破交换机的所谓安全神话：“不可能用嗅探和包截取技术来攻击交换机”。
的确，使用dsniff、Cain或者其他Windows、Linux系统下界面友好的工具，黑客可以轻而易举地将任何流量转向他的个人计算机，从而破坏了这些流量的保密性和完整性。
对于第二层协议，从生成树协议到IPv6邻居发现，这些隐患中的绝大部分都是与生俱来的。
一旦第二层被攻陷，再使用诸如“中间人”（MTTM）攻击之类的技术在更高层协议上构建攻击手段是轻而易举的事。
由于能够截取任意流量，黑客可以在明文通信（例如HTTP和Telnet）和加密通道（例如SSL或SSH）里做手脚。
要利用网络第二层的隐患，攻击者常常必须与攻击目标在第二层相邻。
尽管听起来有些不可思议，但实际上外部黑客是可以连接到一个公司的局域网的。
他可以运用社交工程出入公司场所，或是假扮成一名电话约来的工程师，来现场解决“机械故障”。
另外，很多攻击来自于公司内部员工，比如由一个在现场工作的雇员发起攻击。
传统上，企业一直存在着不成文的和在某些场合是书面的规则，即认定雇员是受信任的个体。
然而，过去数10年中无数的案件和统计数据证明，这一假设是错误的。
2006年CSI／FBI计算机犯罪与安全调查报告显示，受调查公司68%的损失都部分地或完全归结于内部员工的行为不端。
一旦进入大多数组织的场所内部，取得未经授权的网络连接相对来说就容易多了：找到一个墙上闲置的以太网插口，或者一部可以断开的网络设备（例如，一台网络打印机）。
考虑到DHCP的广泛部署，基于局域网的端口中仅有很低比例需要认证（例如IEEE 802.1x），用户的计算机可以获得一个IP地址，且在绝大多数情况下，拥有了和其他合法授权用户同样的网络访问级别。
获取网络中的一个IP地址后，恶意用户就可以尝试各种攻击手段。

<<局域网交换机安全>>

内容概要

本书是迄今为止国内引进的第一本专门介绍第二层交换环境安全技术的图书。
作者在书中通过一个个鲜活的第二层攻击场景，以及针对这些攻击的化解之策，来强调第二层安全的重要性。
这些针对第二层协议的攻击场景，囊括了读者所知的任何一种第二层协议(STP、VRRP/HSRP、LACP/PagP、ARP等)。
书中给出了针对上述攻击的各种反制措施。

除了攻击与对抗攻击之外，作者还高屋建瓴般地展望了未来以及正在流行的第二层安全体系结构及技术，这包括线速的ACL、IEEE 802.1AE、Cisco INBS以及结合IPSec与L2TPv3的安全伪线。
读完本书之后，读者将会加深对网络整体安全性的理解：网络安全并不能只靠防火墙、入侵检测系统甚至是内容过滤设备。
如果没有上述这些设备，在网络的第二层利用交换机同样可以实施网络安全。

本书适合从事计算机网络设计、管理和运维工作的工程技术人员阅读，可以帮助网络(安全)工程师、网络管理员快速、高效地掌握各种第二层网络安全技术。
本书同样可以作为高校计算机和通信专业本科生或研究生学习网络安全的参考资料。

作者简介

作者：（美国）维恩克（Eric vyncke） （美国）培根（Christopher paggen） 译者：孙余强 孙剑维恩克（Eric Vymcke），获得比利时列日大学计算机科学工程系硕士学位后在该校任助理研究员。
随后进入比利时网络研究院，出任研发部门的领导。
之后加盟西门子出任多个安全项目（包括-个代理防火墙项目）的项目经理。
自1997年起，他被Cisco公司委以杰出咨询工程师一职，担当公司欧洲地区的安全技术顾问。
20年来，Eric从事的专业领域一直在从第二层到应用层的网络安全方面。
Eric还是几所比利时大学安全研讨班的客座教授，经常参加各种安全活动.（如Cisco Live的Networkers、RSA大会）并发言。
培根（Christopher Paggen），于1996年加入Cisco，一直从事以局域网交换和安全方面为主的工作。
之后，转而负责公司当前和未来高端防火墙的产品需求定义。
Christopher持有几项美国专利，其中一项与动态ARP检测（Dynamic ARP Inspection，DAI）有关。
除CCIE证书（CCIE#2659）外，Christopher还曾获得HEMES大学（比利时）计算机科学学士学位，并继续在I.IMS大学（比利时）学习了两年经济学。

<<局域网交换机安全>>

书籍目录

章节摘录

插图：17.2.2 认证认证是为请求服务的客户端确立和证实身份的过程。
在建立相关授权时，认证是必需的，其强度由所采取的核实方法决定。
17.2.3 授权授权是指在一个域中获得服务的权利，它可以发生在OSI参考模型的任意-层。
未经认证的授权毫无意义。
IBNS和802.1X一起提供了对用户和／或设备进行认证的基本概念，并提供了与I.AN介质的无关性。
从技术角度来看，当用户通过传统的点到点介质连入交换机或通过无线网络访问LAN时，必须对用户进行认证。
通常，应仅允许已经一个组织批准的机器或用户进行访问。
此外，当用户或设备通过有区别的访问控制获得对网络的访问时，IBNS还有助于为这些用户和设备制定行为规范。
认证还针对网络提供了立即记账的能力，除了能够知晓何时、何处以及如何获得服务以外，还可以了解“谁”获得了网络访问。
17.3 探索扩展认证协议基于端口的网络访问控制使用IEEE 802 I.AN基础设施的物理访问特性。
这些基础设施能够充分利用扩展认证协议（EAP）承载任意的认证信息，而非认证方法本身。

<<局域网交换机安全>>

编辑推荐

《局域网交换机安全》：与普遍观点相反，以太网交换机并不具备天然的安全性。
以太网交换机中的安全隐患多种多样：从交换机的实现，到控制平面协议（生成树协议（STP）、Cisco发现协议等）和数据平面协议，例如，地址解析协议（ARP）或动态主机配置协议（DHCP）。
《局域网交换机安全》阐述了网络基础设施中与以太网交换机相关的所有安全隐患，而且还展示了如何配置交换机以防止或缓解基于这些安全隐患的攻击。
《局域网交换机安全》还以专门章节描述了如何利用交换机以增强整个网络的安全性，并防范未来的攻击。
《局域网交换机安全》为4个部分，为读者提供了实施的具体步骤，以确保在第二层设备上穿梭往来的语音及数据流量的完整性。
第1部分讲述了第二层协议中的缺陷，以及如何配置交换机阻止针对这些缺陷的攻击。
第2部分介绍了与以太网交换机有关的拒绝服务攻击（DoS），并演示了如何遏制这些攻击。
第3部分详述了通过在交换机上利用线速访问控制列表（ACL）的处理，以及通过IEEE80 2.1X执行用户的认证和授权，从而切实增强网络整体安全性的方法。
第4部分研究了IEEE LinkSec工作组的未来发展。
《局域网交换机安全》通篇的绝大部分内容与硬件供应商无关，并对所有部署以太网交换机的网络架构师都有极高的实用性。
阅读完《局域网交换机安全》后，读者一定会对加深对LAN安全的理解，并有能力堵住存在于诸多园区网络中的安全漏洞。
利用端口安全防范CAM攻击防范生成树攻击运用正确的配置手段隔离VLAN防范流氓DHCP服务器阻止ARP欺骗防范IPv6邻居发现和路由器恳求攻击识别PoE隐患缓解HSRP阳VRRP的风险遏制利用CDP、PaGP、CGMPI以及其他Cisco辅助协议的信息泄露理解并防范针对交换机的DoS攻击利用ACI一执行简单的线速安全策略以端口为基础利用802.1X实施用户认证使用IEEE的新协议以线速加密所有以太网帧《局域网交换机安全》为Cisco Press出版的网络技术系列丛书之一。
Cisco Press出版的安全类别的图书可以帮助网络从业人员保护重要的数据和资源。
防范和缓解网络攻击。
以及构建端到端的自防御网络。

<<局域网交换机安全>>

版权说明