

<<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

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<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，然后通过或被入侵的Cisco设备发起进一步的破坏性攻击；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。

<<Cisco网络黑客大曝光>>

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

序言案例研究：黑帽子论战	前言	第1部分 基础知识	案例研究：eBay奇事	第1章 Cisco网络设计模型及其安全概述
1.1.3 双层模型	1.1.4 环形模型	1.1.5 网状和部分网状模型	1.1.6 网络安全区	1.1.2 星形模型
1.1.7 IDS传感器部署指南	1.2 Cisco层次化设计及网络安全	1.2.1 核心层	1.2.2 分发层	
1.2.3 访问层	1.3 小结	第2章 Cisco网络安全要素	2.1 公共的Cisco设备安全特征	2.2
Cisco防火墙	2.2.1 包过滤防火墙	2.2.2 状态包过滤防火墙	2.2.3 代理过滤	2.2
PIX防火墙故障转移	2.2.5 Cisco防火墙硬件类型	2.3 Cisco Secure IDS及攻击预防	2.3.1	
独立的硬件IDS传感器	2.3.2 模块化IDS传感器	2.3.3 Cisco IOS IDS软件	2.3.4 以Cisco	
PIX防火墙作为IDS传感器	2.3.5 Cisco Traffic Anomaly Detector XT 5600	2.3.6 Cisco Secure IDS		
管理控制台	2.4 Cisco VPN解决方案	2.4.1 IPsec	2.4.2 PPTP	2.5 Cisco AAA和相关
务	2.5.1 AAA方法概述	2.5.2 Cisco与AAA	2.6 Cisco互联网设计及安全要素的安全隐患	
2.7 小结	第3章 现实世界Cisco安全问题	3.1 为什么黑客想启用你的设备	攻击者获得什	
么	3.2 Cisco设备和网络：攻击者的观点	3.2.1 攻击网络协议	3.2.2 隐藏路由器和交换机	
上的踪迹和证据	3.3 Cisco网络设备安全审计与渗透测试基础	评估过程	3.4 小结	第2部
“获得控制权”：入侵设备	案例研究：一项NESSUS报告	第4章 概述并列举Cisco网络	4.1 联机	
搜索与Cisco google肉鸡	4.1.1 基本搜索	4.1.2 利用Google算子搜索	4.1.3 利用Google	
搜索Enable	4.1.4 对策：如何避免成为Cisco google肉鸡	4.2 路由列举	4.2.1 自治系统发	
发现和映射：BGPv4询问	4.2.2 Internet路由注册表、路由服务器和Looking Glasses查询	4.2.3		
将IP地址映射到自治系统	4.2.4 列举自治系统	4.2.5 寻找属于某个机构的自治系统		
4.2.6 AS路径列举，构建BGP树，寻找边界路由器	4.2.7 BGP列举对策	4.2.8 路由域编号		
发现与IGP的网络映射	4.2.9 映射RIP、IGRP和IRDP	4.2.10 列举OSPF	4.2.11 分	
析OSPF列举数据	4.2.12 IGP列举对策	4.3 小结	第5章 列举与Cisco设备指纹识别	5.1
探Cisco特有的协议	5.1.1 剖析CDP帧	5.1.2 应对基于CDP和其他Cisco专有协议的列举的措施	5.2 Cisco设备的主动式列举和指纹识别	
5.1.3 Cisco设备的被动式列举和指纹识别	5.2.1 Cisco路由器的主动式列举和指纹识别	5.2.2 Catalyst交换机的主动式列举和指纹识别	5.2.3 其他Cisco设备的主动式列举和指纹识别	
5.2.1 Cisco路由器的主动式列举和指纹识别	5.2.2 Catalyst交换机的主动式列举和指纹识别	5.2.4 利用IOS 11.X内存泄露列举远程Cisco路由	5.2.5 隐藏机器避免被窥探：列举和指纹识别对策	
5.2.3 其他Cisco设备的主动式列举和指纹识别	5.2.4 利用IOS 11.X内存泄露列举远程Cisco路由	5.2.6 “开门，开门！”		
器	5.2.5 隐藏机器避免被窥探：列举和指纹识别对策	5.2.6 “开门，开门！”		
谁在那？	”针对Cisco机器的端口扫描、OS指纹识别及其检测	5.3 小结	第6章 从外部进入：易如反掌	
6.1 口令攻击	6.1.1 针对开放的Cisco Telnet服务器的大规模猜测/暴力破解攻击	6.1.2 针对		
其他开放的Cisco服务的口令猜测和暴力破解攻击	6.1.3 针对Cisco设备口令猜测攻击的对策			
6.2 SNMP团体猜测、漏洞利用和安全措施	6.2.1 Cisco SNMP基础	6.2.2 SNMP大规模扫		
描	6.2.3 SNMP暴力破解和字典攻击	6.2.4 SNMP浏览和Cisco设备重配置	6.2.5 命令行	
远程Cisco设备SNMP操作——IOS主机	6.2.6 命令行远程Cisco设备SNMP操作——CatOS交换机			
6.2.7 针对SNMP团体字典和暴力破解攻击的对策	6.3 利用TFTP服务器漏洞接管Cisco主机			
6.3.1 列举TFTP服务器	6.3.2 嗅探出Cisco配置文件	6.3.3 暴力破解TFTP服务器以获取配		
置	6.3.4 针对TFTP相关攻击的对策	6.4 Cisco设备Wardialing	6.4.1 Cisco路由	
器Wardialing 101：接口、配置和逆向Telnet	6.4.2 发现拨入的号码	6.4.3 侵入Cisco路由器或		
访问服务器	6.4.4 拨号式扫描的安全对策	6.5 小结	第7章 入侵Cisco设备：中间途径	
初识协议实现调查与滥用：Cisco SNMP攻击	7.1.1 SilverCreek	7.1.2 SimpleTester		
和SimpleSleuth	7.1.3 Oulu University PROTOS项目	7.1.4 从SNMP Fuzzing到DoS和Reflective		
DDoS	7.1.5 从SNMP压力测试到特殊的DoS	7.1.6 隐藏的威胁——未公开的SNMP团体和远		
程访问	7.1.7 只通过观察技巧进入	7.1.8 针对Cisco SNMP攻击的高级对策	7.1.9	
SNMPv3安全性的简要分析	7.2 初识数据输入验证攻击——Cisco HTTP漏洞利用	7.2.1 Cisco		
Web配置界面基础	7.2.2 Cisco IOS HTTP管理访问	7.2.3 IOS HTTP管理访问的对策		

<<Cisco网络黑客大曝光>>

7.2.4 Cisco ATA-186 HTTP设备配置暴露	7.2.5 设备配置暴露的对策	7.2.6 VPN集中器HTTP设备信息泄露
7.3.1 Cisco IOS 2GB HTTP GET缓冲区溢出漏洞	7.3.2 HTTP GET缓冲区溢出漏洞的对策	7.4 Cisco Web服务安全性评估
7.4.1 SPIKE及其相关知识	7.4.2 Peach Fuzzer	7.4.3 Fuzzer工具的对策
7.5 小结	第8章 Cisco IOS漏洞利用：正确的方式	8.1 Cisco IOS架构基础
Cisco IOS内存剖析	8.2 漏洞利用入门：IOS TFTP缓冲区溢出	8.3 IOS逆向工程的诅咒与祝福
8.3.1 可以被逆向工程师（滥）用的IOS特征和命令	8.3.2 简约的逆向工程军火库	8.4 小结
9.1.1 第7类口令的破解	9.1.2 MD5口令哈希的破解	9.1.3 防止口令遭破解的措施
9.1.4 社交工程攻击	9.1.5 应对社交工程攻击的措施	9.2 本地设备访问
9.2.1 路由器口令的本地重置或恢复	9.2.2 交换机口令的本地重置或恢复	9.2.3 PIX防火墙口令的本地重置
9.2.4 本地Cisco VPN集中器口令的重置或恢复	9.2.5 防范本地Cisco设备访问的措施	9.3 小结
第10章 利用漏洞并保留访问权限	10.1 常见的攻击者对Cisco路由器、交换机和防火墙配置的更改	10.1.1 有人吗？
10.1.2 掩盖踪迹	10.1.3 四处查看	10.1.4 用被控IOS路由器隐藏踪迹
10.1.5 被控IOS路由器或PIX防火墙允许恶意网络流通过的网路流	10.1.6 用被控IOS路由器镜像、捕获或更改经过的网络流	10.1.7 从受控PIX防火墙进行嗅探
10.1.8 用Cisco Catalyst交换机进行网络嗅探	10.1.9 远程SPAN的使用（滥用）	10.1.10 CatOS的使能工程师模式
10.2 进一步利用IOS并保留设备访问权限	10.2.1 IOS的二进制补丁：谬误与现实	10.2.2 用TCL操控路由器
10.2.3 防范已攻入者的措施	10.3 小结	第11章 针对Cisco设备的拒绝服务攻击
11.1 DoS攻击的动机	11.2 DoS攻击的分类	11.2.1 消耗资源
11.2.2 破坏信息流	11.2.3 破坏工具	11.3 Cisco的DoS攻击评估工具
11.3.1 Cisco Global Exploiter	11.3.2 Cisco的TCP Test Tool	11.4 众所周知的Cisco DoS漏洞
11.4.1 针对Cisco设备的常见DoS攻击	11.4.2 ICMP远程DoS漏洞	11.4.3 应对ICMP远程DoS攻击的措施
11.4.4 格式错误的SNMP消息DoS漏洞	11.4.5 应对格式错误的SNMP消息DoS攻击的措施	11.4.6 专门针对Cisco路由器的DoS攻击举例
11.4.7 针对Cisco IOS的IKE数据包格式错误远程DoS攻击漏洞	11.4.8 Cisco IOS的IKE数据包格式错误远程DoS攻击的应对措施	11.4.9 Cisco 44020漏洞
11.4.10 Cisco 44020漏洞的应对措施	11.4.11 专门针对Catalyst交换机及其他Cisco网络设备的DoS攻击举例	11.4.12 Cisco Catalyst交换机内存泄漏DoS攻击漏洞
11.4.13 Cisco Catalyst交换机内存泄漏DoS攻击的应对措施	11.4.14 利用错误的TCP校验和破坏通过PIX防火墙的通信	11.4.15 Cisco宽带操作系统TCP/IP栈DoS攻击漏洞
11.4.16 Cisco宽带操作系统TCP/IP栈DoS攻击的应对措施	11.4.17 Cisco Aironet AP1x00的HTTP GET格式错误DoS攻击的应对措施	11.4.18 Cisco Aironet AP1x00的HTTP GET格式错误DoS攻击的应对措施
11.4.19 Cisco Catalyst交换机非标准TCP标志位远程DoS攻击漏洞	11.4.20 Cisco Catalyst交换机非标准TCP标志位远程DoS攻击的应对措施	11.5 利用Cisco设备实施DDoS攻击
11.5.1 用Cisco设备大规模地ping，使用SNMP协议	11.5.2 应对SNMP攻击的措施	11.5.3 用Cisco设备大规模地ping，使用Telnet MK I
11.5.4 Telnet MK I的应对措施	11.5.5 用Cisco设备大规模地ping，使用Telnet MK II	11.5.6 Telnet MK II的应对措施
11.5.7 用Cisco设备大规模地发送洪流，使用SNMP协议	11.5.8 应对SNMP攻击的措施	11.6 大规模的DDoS：小子们的报复
11.6.1 直接DDoS攻击	11.6.2 反射式DDoS攻击	11.6.3 ihateperl.pl
11.6.4 drdos	11.6.5 关于Cisco设备的防范各种DDoS攻击的措施	11.6.6 应对措施：用NBAR应对DDoS攻击和由蠕虫引起的网络洪流
11.6.7 约定访问速率（CAR）	11.7 小结	第3部分 Cisco网络系统中的协议攻击
案例研究：空中的OSPF梦魇	第12章 生成树、VLAN、EAP-LEAP和CDP	12.1 生成树协议攻击
12.1.1 插入恶意根网桥	12.1.2 在无需成为根的情况下修改流量路径	12.1.3 重算STP及数据嗅探
12.1.4 STP DoS攻击	12.1.5 Cisco特有的针对STP型攻击的防御措施	12.2 攻击VLAN
12.2.1 DTP滥用	12.2.2 802.1q攻击和ISL攻击	12.2.3 双重标记VLAN跳跃攻击
12.2.4 专用VLAN跳跃攻击	12.2.5 使单向攻击成为双向攻击	12.2.6 VTP攻击
12.2.7 VLAN查		

<<Cisco网络黑客大曝光>>

询协议 (VQP) 攻击	12.2.8 绕过VLAN分段的迂回方式	12.2.9 针对VLAN相关攻击的防御
措施	12.3 Cisco EAP-LEAP破解	12.3.1 EAP-LEAP基础
12.3.3 针对EAP-LEAP破解的防御措施	12.4 攻击CDP	12.4.1 CDP欺骗攻击
骗攻击的防御措施	12.5 小结	12.4.2 CDP欺骗
HSRP攻击的防范措施	第13章 HSRP、GRE、防火墙和VPN渗透	HSRP漏洞利用
GRE包注射	13.1 GRE漏洞利用	13.1.1 一种基于MTU的GRE攻击
13.2.2 攻击PIX MailGuard	13.1.3 GRE攻击防范措施	13.1.2 攻击PIX协议Fixup
Fixup防范措施	13.2 Cisco防火墙渗透	13.2.1 攻击PIX FTP Fixup
Cisco VPN攻击	13.2.3 PIX MailGuard防范措施	13.2.4 攻击PIX FTP Fixup
14.1 路由攻击简介	13.2.6 针对PIX防火墙的TCP重置攻击	13.2.5 PIX FTP
14.3.2 通过RIP插入恶意路由	13.3.1 IPsec相关攻击	13.3 攻击距离向量类路由协议
攻击的防御措施	14.2 设置流氓路由器	14.3.1 攻击RIP
措施	14.3 攻击距离向量类路由协议	14.3.2 通过RIP插入恶意路由
14.3.9 攻击EIGRP	14.3.4 RIP MD5哈希值破解攻击	14.3.3 RIP降级攻击
14.3.12 攻击已认证的EIGRP	14.3.5 针对RIP攻击的防御措施	14.3.4 RIP MD5哈希值破解攻击
14.4.1 通过OSPF插入恶意路由	14.3.6 攻击IGRP	14.3.5 针对RIP攻击的防御措施
解攻击	14.3.7 通过IGRP插入恶意路由	14.3.6 攻击IGRP
攻击的防御措施	14.3.8 应对IGRP攻击的防御措施	14.3.7 通过IGRP插入恶意路由
攻击场景	14.3.9 攻击EIGRP	14.3.8 应对IGRP攻击的防御措施
的破解	14.3.10 通过EIGRP插入恶意路由	14.3.9 攻击EIGRP
分 附录	14.3.12 攻击已认证的EIGRP	14.3.10 通过EIGRP插入恶意路由
Auto Secure配置范例	14.4.1 通过OSPF插入恶意路由	14.3.11 针对EIGRP网络的DoS攻击
	14.4.2 成为指定或备用指定OSPF路由器	14.4 攻击链路状态路由协议
	14.4.3 OSPF MD5哈希值破解攻击	14.4.1 通过OSPF插入恶意路由
	14.4.4 直接攻击OSPF路由器：OoopSPF攻击	14.4.2 成为指定或备用指定OSPF路由器
	14.4.5 针对OSPF的DoS攻击	14.4.3 OSPF MD5哈希值破解攻击
	14.4.6 针对OSPF攻击的防御措施	14.4.4 直接攻击OSPF路由器：OoopSPF攻击
	14.5 攻击BGPv4	14.4.5 针对OSPF的DoS攻击
	14.5.1 恶意BGP路由器重配置	14.4.6 针对OSPF攻击的防御措施
	14.5.2 恶意BGP路由器重配置的攻击场景	14.5 攻击BGPv4
	14.5.3 BGP路由器伪装攻击	14.5.1 恶意BGP路由器重配置
	14.5.4 针对BGP路由器的中间人攻击	14.5.2 恶意BGP路由器重配置的攻击场景
	14.5.5 BGP MD5认证的破解	14.5.3 BGP路由器伪装攻击
	14.5.6 针对BGP路由器的盲式DoS攻击	14.5.4 针对BGP路由器的中间人攻击
	14.5.7 如何防范对BGPv4的攻击	14.5.5 BGP MD5认证的破解
	14.6 小结	14.5.6 针对BGP路由器的盲式DoS攻击
	第4章	14.5.7 如何防范对BGPv4的攻击
	附录	14.6 小结
	案例研究：大规模战役	第4章
	附录A 网络设备安全测试模板	附录
	附录B 实验室路由器交互式Cisco	案例研究：大规模战役
	附录C 未公开的Cisco命令	附录A 网络设备安全测试模板

<<Cisco网络黑客大曝光>>

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OSI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 Design Professional）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802.15（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

<<Cisco网络黑客大曝光>>

, 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.shtml>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Cisco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14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 Controller Access 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1.1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 Router Resilience 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 Networking Services, 网络身

<<Cisco网络黑客大曝光>>

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 Protected Access,无线保护访问)业界认证需求的Cisco Aironet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802.11i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Cisco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

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>