<<黑客大曝光>>

图书基本信息

书名：<<黑客大曝光>>

13位ISBN编号：9787121117503

10位ISBN编号：7121117509

出版时间：2010-10

出版时间：电子工业出版社

作者：(美)恩德勒，科利尔　著，李祥军，周智，魏冰　译

页数：451

前言

出于工作的需要，我经常需要和国内外的各安全厂商进行技术交流，在此过程中我发现，很多安全厂商在IT系统安全、IP网络系统安全，包括操作系统安全、数据库安全、网络设备安全等方面都有着深厚的技术积累，然而在通信网络安全方面，往往了解得较少。
许多安全厂家在进行通信网络或者通信业务系统的安全评估、安全加固等工作时，通常不会涉及到通信业务中的安全需求。
随着国内安全厂商的不断发展、国内安全从业人员的不断努力，在IT及IP网络系统安全方面，国内外的差距越来越小，然而在通信网络安全方面，国内外的差距还是很明显。
许多文献都提到，最早的黑客并不是在计算机领域产生的，如70年代美国的电话飞客（Phreaker），就通常被认为是黑客最早的雏形。
通过BlueBox向全世界打电话，是那个时代黑客最酷的行为。
直到今天，美国一直都有许多热衷于通信网络安全的研究人员，而在国内，却鲜有精于通信网络安全的专业人员。
VoIP技术已经广泛应用到当前的各种通信网络之中，VoIP技术的应用使得通信网络更加开放，但也同时面临着更大的风险，因此，通信网络安全解决方案将面临更大的挑战。
随着VoIP技术应用的进一步普及，很多研究机构都预测VoIP将会成为黑客的下一个乐园。
实际上，前几年，美国就曾经发生过利用VoIP网络漏洞窃取价值超过100万美元通话时长的案件，并且美国的几大著名运营商也都曾曝出存在VoIP计费方面的严重安全漏洞。
我曾经阅读过国内外的许多关于VoIP安全的文章和书籍，发现国内的相关文献更多是关注于理论层面，很少有真正讨论安全实战的文献，相比较而言，国外关于VoIP安全实战的书籍更多一些。
在安全领域，与那些随手可得的关于IT及IP网络系统安全的书籍和文献相比较，关于通信网络安全或者是说与VoIP安全相关的书籍实在是少得多。
本书的原版书在2007年刚出版后不久，我就有幸拜读，获益匪浅。
当时，我就认为本书的原版书是市面上介绍VoIP安全最好的书籍之一。
时至今日，虽然市面上又出现了大量关于VoIP安全的书籍，但我仍然认为本书是最好的VoIP安全书籍之一。
这几年中，我曾经向很多安全界的朋友、很多安全厂商推荐过这本书，为了让国内安全行业的从业人员能够更好地了解VoIP安全，我们特意翻译了此书，并将之献给安全界的朋友。
本书是一本绝佳的关于VoIP安全的入门级书籍，作者利用丰富的实例深入浅出地介绍了VoIP安全方面涵盖的关键内容。
仅从安全的角度来看，VoIP技术是一把双刃剑，应用得当，可以带来很多安全优势，应用不得当，就有可能带来安全灾难。
本书介绍的内容以及攻击场景都基于企业VoIP网络应用，而VoIP技术在运营商的通信网络应用中的安全性与可靠性方面，与企业应用相比，有着明显的区别：通信网络中的VoIP安全水平比企业网络VoIP应用的安全水平高出很多。
即便如此，本书也是一本上好的了解运营商通信网络安全的入门级书籍。
本书在介绍VoIP安全时，部分重点内容描述了SIP协议的主要安全问题，SIP协议是现在很多通信网络系统（如IMS、固网软交换等）或者即时通信系统（如MSN、飞信等）的基础协议，同时，SIP协议将越来越多地应用到更多系统之中。
因此，本书也有助于读者更好了解SIP协议安全以及许多相关系统的安全。

<<黑客大曝光>>

内容概要

冒用他人的电话号码打电话、窃听他人的通话内容、在他人通话时加入一些背景噪声、在他人通话时恶意强行挂断……所有这些都是很多“黑客”的梦想，然而，在以前的通信网络中，基于一些技术原因，这些都难以实现。
随着VoIP技术的应用和普及，黑客们终于等到了机会，在VoIP时代，特别是端到端的VoIP应用时代，在一些安全防护不严的网络中，黑客们的这些梦想就可以成真了。
本书立足于企业VoIP通信网络，以大量丰富的实例和各种VoIP攻击工具的应用为基础，详细描述了各种针对VoIP应用的攻击方式及解决对策，包括号码采集、呼叫模式跟踪与语音窃听、针对服务器和电话的DoS攻击、恶意语音的插入与混淆、垃圾语音电话、语音钓鱼，等等。
针对企业VoIP网络安全攻击与防护，本书绝对是一本安全管理员、安全研究人员等必读的实战型的教材。
同时，本书也是了解运营商通信网络（如IMS网络）及安全问题的不可多得的入门级教材。

作者简介

作者：（美国）恩德勒（David Endler） （美国）科利尔（Mark Collier） 译者：李祥军 周智 魏冰

<<黑客大曝光>>

书籍目录

第1部分 收集情报 第1章 VoIP网络踩点 1.1 为什么要先踩点 1.2 VoIP踩点方法 1.2.1 确立攻击范围 1.3 小结 1.4 参考文献 第2章 VoIP网络扫描 第3章 VoIP网络枚举第2部分 VoIP网络攻击 第4章 VoIP网络设施的DoS攻击 第5章 VoIP网络侦听 第6章 VoIP干扰及篡改第3部分 针对VoIP特定平台的攻击 第7章 Cisco Unified CallManager 第8章 Avaya Communication Manager 第9章 Asterisk 第10章 新兴的软终端技术第4部分 VoIP会话和应用攻击 第11章 VoIP Fuzzing攻击 第12章 基于泛洪攻击的服务中断 第13章 信令和媒体信息操纵第5部分 社交攻击 第14章 SPIT（SPAM over Internet Telephony，垃圾网络电话） 第15章 语音钓鱼

章节摘录

插图：如图1.1中所示的许多VoIP应用攻击将在随后的章节中详细讲解和演示。
需要强调的一点是：图1-1中列举的一些其他攻击，如SQL注入、SYN泛洪攻击等，已经出现多年，几乎很难有新的变化。
这些正是那些如今困扰着绝大多数传统数据网络的攻击方式。
然而，在一些特殊情况下，这些攻击形式可能给VoIP网络带来更加严重的后果。
例如，针对企业的路由器的SYN：flood拒绝服务攻击仅仅意味着内部员工网页浏览速度会变慢，而针对VoIP网络或者VoIP设备的同样攻击则意味着语音通话将会变得莫名其妙，这是因为攻击带来的较大网络抖动，或者由于网络中的巨大延迟而导致根本无法进行语音呼叫。
很显然，对黑客而言，最有利的是在进行网络攻击之前获取尽可能多的VoIP系统支撑设施的信息。
攻陷企业VoIP系统的最便利之路或许并不是直接向VoIP应用发起攻击，而是VoIP系统的带有脆弱点的支撑系统，如路由器、Web Server等。
当语音信箱所运行的Linux系统依然还存在默认root口令时，黑客为什么还要不辞辛苦地暴力破解web界面的密码呢？
前期只是简单地收集一下VoIP部署中常见的方式以及其依赖的支撑系统，就能够大大节省黑客的时间以及避免繁琐的暴力破解行为。
因此，评估自有的暴露给外部的系统的安全性，首先就要发现那些可能的黑客所能了解到的关于自有系统的信息。

<<黑客大曝光>>

编辑推荐

《黑客大曝光：VoIP安全机密与解决方案》：经典安全图书，知名行业专家打造!通过从恶意入侵者的角度学习如何审视自己的网络和设备，可以避免削弱VOIP网络的攻击。
《黑客大曝光：VoIP安全机密与解决方案》逐步向你展示了在线的攻击者如何实施网络探测、如何获取接入、如何窃取数据并入侵脆弱的系统。
《黑客大曝光：VoIP安全机密与解决方案》包含了不同厂家的硬件设备与网络相关的安全问题，并给出了具体的对策、透彻的案例及使用的实现技术。
通过《黑客大曝光：VoIP安全机密与解决方案》，读者还可以了解如何防护最新的DoS攻击、中间人攻击、呼叫泛洪攻击、窃听、VoIP Fuzzing、信令与语音操控、垃圾语音电话．以及语音钓鱼等。
发现黑客如何踩点、扫描、枚举及窃听VoIP网络和硬件设备。
加固CiSCO、Avaya和Aste risk系统。
预防DNS投毒、DHCP耗尽、ARP表操控等攻击。
阻止号码采集、呼叫模式跟踪及语音窃听等攻击。
测量并维护VoIP网络服务质量和VoIP语音通话质量。
阻断那些中断SIP代理服务器与电话的DoS攻击和报文泛洪攻击。
对抗REGISTER劫持、INVITE泛洪攻击和BYE呼叫拆除攻击。
避免恶意语音的插入和混淆攻击。
了解何为垃圾语音电话及如何预防。
防御语音钓鱼和身份窃取欺诈。

版权说明