<<黑客大挑战>>

图书基本信息

书名：<<黑客大挑战>>

13位ISBN编号：9787302057338

10位ISBN编号：7302057338

出版时间：2002-10

出版时间：清华大学出版社

作者：Mike Schiffman

页数：347

字数：439

<<黑客大挑战>>

内容概要

全书分为两部分，第1部分包括20个挑战，其中囊括了安全领域中的重要专题，包括拒绝服务攻击、无线技术、Web攻击、恶意代码。
每个挑战包括一个详细的事件描述——入侵是如何检测到的、证据和可疑的线索（诸如日志文件和网络图等），以及要解决的一系列问题。
然后，在第2部分，将给出针对每个挑战的解决方案，从中你将看到专家级的事件分析、问题解答，以及预防和缓解措施。

本书适合于安全管理员和网络管理员，企业及组织的政策制定者也会从中受益。

作者简介

关于本书的主笔
Mike Schiffman，CISSP(认证信息系统安全专家),@stake公司安全架构的负责人，@stake是专业安全服务的主要提供商。
他已研究和开发了许多前沿技术，包括像firewalk和tracerx这样的工具，还有到处使用的低层的数据包整形函数库（packet shaping library），libnet。
他还在一些事业机构和政府部门做过报告，例如NSA（美国国家安全局）,CIA（美国中央情报局）,DOD（美国国防部）,AFWIC,SAIC和军情处。
Mike已在和上发表过多篇文章,参与过《黑客大曝光》一书的编写。

关于本书的技术评论者
Tom Lee (MCSE)是Foundstone公司的IT经理。
他的工作是保证Foundstone的系统正常运转和阻止入侵者的攻击。
Tom在系统和网络管理方面有数十年的工作经验，他维护过许多不同的系统的安全，从Novell网，Windows NT/2000到Solaris、Linux和BSD。
在加入Foundstone公司之前，Tom在加州大学担任IT主任。

关于本书的技术评论家
这是我的第一本书，特别献给两个人：第一个是我去世的父亲，是他当初点燃了我胸中对计算机浪漫主义的火焰；其次是我迷人的女友，Alisa Rachelle Albrecht。

书籍目录

，如果对新的风险没有认识，则是非常危险。
就像《Maggie的经历》中，通过寻呼系统通知管理员一些必要的警报和相关信息，本来是安全措施的一部分，但是就是这个措施带来了新的被监听的问题。
另外，在防火墙的前后都安装NIDS来进行安全评估非常有帮助。

行业：计算机工程
攻击难度：极高
预防难度：中等
缓解难度：中等
6 基因植入——　如果二楼防护严密，你可以选择从三楼过去。
而有价值的东西可能正好就在三楼。
数据库系统和应用系统常常是关键业务价值所在；而设计数据库、开发引用系统的人员的安全技能常常不足；这方面的专业安全人才和工具也不足；三楼的安全问题已经成为攻防双方共同关注的新大陆。

行业：基因研究
攻击难度：困难
预防难度：低
缓解难度：困难
7 悬案——我们已经多次感到无线网络的安全隐患。
嗅探和监听也是比较难于发现的攻击方法。
而脆弱的密码策略也为这种嗅探提供了很多的有用信息，特别是明文传输的密码。
在网络中多布置一些IDS，可能对我们提早发现可以情况提供帮助。

行业：软件工程
攻击难度：极难
预防难度：中等
缓解难度：中等
8 冰山一角——现在很多黑客攻击手法和后门都与病毒和蠕虫相结合，这样可以扩大攻击的影响范围和感染速度。
作为防护一方，就要尽力发挥防病毒软件在防入侵中的作用。
当然，不管怎么说，将一个没有足够防护的机器放在防火墙外面都是非常愚蠢的。

行业：金融服务
攻击难度：中等
预防难度：低
缓解难度：中等
9 不可靠的银行——作为一个网上银行的系统仅仅采用Windows操作系统作为业务平台是非常冒险的决策。
作为如此重要的系统要比较彻底地解决安全问题还是应当采用B1级（CC EAL4）以上的系统比较恰当。
即使采用C级的系统，也一定要配备IDS系统，而且应当结合采用基于网络和基于主机的IDS。

行业：在线银行
攻击难度：中等
预防难度：低
缓解难度：困难

10 Jack和Jill——作为一个小型公司的网上业务系统，可能不值得花费大量的资源来做安全，但是用一些小型的、廉价的或者免费的个人安全产品还是可以考虑的。
或者干脆考虑托管给能够提供相应安全服务的IDC。

行业: 在线零售
攻击难度: 中等
预防难度: 低
缓解难度: 低
11 意外的观光客——
意外的观光客 又是“无线”给我们带来的麻烦。
看来我们将来真的要认真对待这个问题。

行业: 半导体制造商
攻击难度: 低
预防难度: 困难
缓解难度: 中等
12 边缘地带——口令是网络和系统安全中永恒的问题。
许多攻击和防护技术都是围绕口令的争夺展开的。
一次性口令机制是从体制上解决口令安全问题的非常好的办法。
同时基于主机的IDS可以帮助我们提早发现针对口令的强力破解攻击。

行业: 银行业和金融服务
攻击难度: 极难
预防难度: 中等
缓解难度: 低
13 玩忽职守——在网络中尽量采用交换机而不是基线器，可以减少网络被嗅探和监听的几率。
可以考虑将这条写到企业的安全策略中
行业: 卫生保健
攻击难度: 中等
预防难度: 低
缓解难度: 中等
14 收获的日子——黑客为什么老是纠缠用户账户和口令？
要解决这个问题，我们至少要做到每人一个账号（不要共享账号），口令中至少要有大小写的字母、数字和特殊字符。
另外一个重要的方法就是备份。
有了备份，真有意外发生时，可以减少很多的损失。

行业: 高校/社区大学网络
攻击难度: 中等
预防难度: 低
缓解难度: 中等
15 尖峰时刻——拒绝服务攻击（DoS）是永远无法彻底解决的攻击现象。
其根本原理就是使用一些貌似合法的访问，通过超强度、超范围、超常规等方式，使得网络和系统的资源耗尽或者崩溃。
比较好地解决DoS需要上下游的机构协调配合。

行业: 政府承包商

攻击难度: 低
预防难度: 困难
缓解难度: 困难
16 多级跳 ——频繁地采用跳板是攻击者最基本的隐藏自己的方法。
能够顺着跳板反向侦查几乎是不可能的，因为这些跳板可能涉及多个机构，甚至多个国家。
指望别人将系统保护好是不切实际的，我们只能保证自己的系统不被攻击，并且不被滥用来攻击别人。

行业: 市政工程
攻击难度: 低
预防难度: 低
缓解难度: 困难
17 贪婪 ——又是拒绝服务攻击……
行业: 网络工程/销售
攻击难度: 低
预防难度: 低
缓解难度: 低
18 利器——没有安全策略、安全组织使得这个企业的安全处于无序和无助的状态；没有紧急响应流程，使得事件的处理也比较凌乱。
这家公司如果不从整体安全管理上有所改进的话，将来还要出问题。

行业: 医疗诊断设备工程
攻击难度: 中等
预防难度: 低
缓解难度: 困难
19 拒绝作证 ——打最新的补丁、保护好日志、采用IDS……这些都是百试不爽的好方法。

行业: 大学
攻击难度: 极难
预防难度: 低
缓解难度: 中等
20 乡愁——如果确认一个机器已经被攻破，对其上的所有东西都不能被完全信任。
如果你没有分布式日志系统或者网络IDS系统的话，就只能寄希望于攻击者的“幼稚”，并从蛛丝马迹中查找线索了。

行业: 制药/网页托管
攻击难度: 中等
预防难度: 低
缓解难度: 低
第2部分 解决方案
1 来自法国的连接 安氏点评
2 内部攻击者 安氏点评
3 停车场 安氏点评
4 关键因素 安氏点评
5 Maggie的经历 安氏点评

版权说明