



- 探讨所有安全工作者无可回避的话题
- 揭秘网络服务器群组如何被渗透入侵
- 基于原理与实例的全面渗透防御方案
- 视频CD全程再现数十种黑客攻击战法

网络渗透攻击与 安防修炼

一本内行人写给行内人的网络安全著作

最易被用来攻击的RFI漏洞

渗透网站数据库核心

肉鸡变跳板，端口转发

Cisco路由器攻击案例

无可检测的密码后门

SNMP威胁Windows网络安全

从Tomcat到3389肉鸡

内网中的DNS欺骗



肖 遥

飞思科技产品研发中心

编著

监制



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn



CD-ROM

光盘包含视频教程与案例源代码



- 1. 网络安全与信息安全
- 2. 网络安全与信息安全
- 3. 网络安全与信息安全
- 4. 网络安全与信息安全

网络安全与 安防维修

本书由人民邮电出版社出版

本书由人民邮电出版社出版





网络渗透攻击与 安防修炼

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

肖 遥

飞思科技产品研发中心

编著

监制



内容简介

这是一本关于网络渗透攻击与防范的书籍。全书共分为 9 章, 主要内容包括: 网络渗透攻击行为及分析、攻击者如何打开渗透突破口、渗透中的入侵与提权、远程控制入侵、大型网络环境的深入探测、渗透入侵中的社会工程学等。

本书与其他书籍不同的特色之处在于, 本书特别有针对性地以曾经热炒一时的“入侵腾讯事件”为例, 以再现“入侵腾讯事件”为流程, 对渗透入侵过程进行了深入的分析揭秘。书中全面系统地讲解了攻击者在渗透中可能采取的各种入侵手法, 并给出了高效的防范方案, 有助于网络安全维护人员掌握黑客的攻击行为, 更好地维护网络安全。

本书可作为专业的网络安全管理人员、网络安全技术研究者阅读, 在实际工作中具有极高的参考价值; 也可作为相关专业学生的学习资料和参考资料。光盘中提供攻防实战演练与视频讲解, 以及书中涉及的实例源代码。

未经许可, 不得以任何方式复制或抄袭本书的部分或全部内容。
版权所有, 侵权必究。

图书在版编目(CIP)数据

网络渗透攻击与安防修炼 / 肖遥编著. —北京: 电子工业出版社, 2009.4

(网络安全专家)

ISBN 978-7-121-08319-8

I. 网... II. 肖... III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字 (2009) 第 022293 号

责任编辑: 王树伟 李新承

印 刷: 北京东光印刷厂

装 订: 三河市皇庄路通装订厂

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编: 100036

开 本: 787×1092 1/16 印张: 41.5 字数: 1062.4 千字

印 次: 2009 年 4 月第 1 次印刷

印 数: 4 000 册 定价: 79.00 元 (含光盘 1 张)

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010) 88254888。

质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

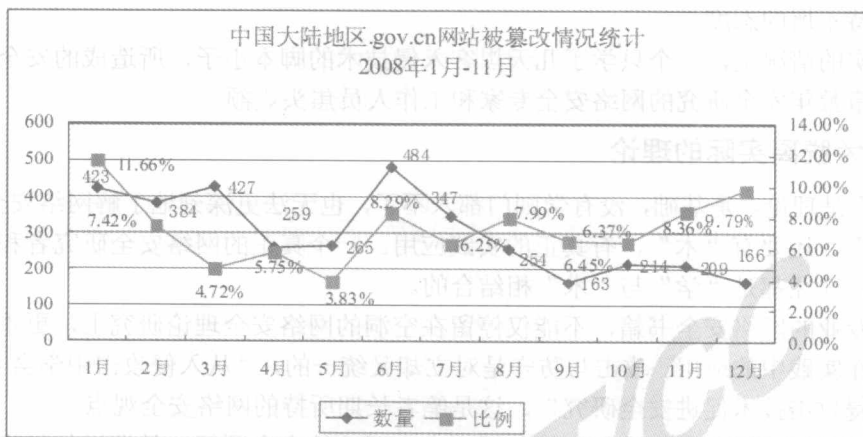
服务热线: (010) 88258888。

应广大读者朋友的要求,《网络渗透攻击与安防修炼》终于和广大读者见面了。这部网络安全专著分9章,随书附带教学视频。本书兼顾学习与参考两个目的,以广大网络管理员、安全工作者和高级网络用户为服务对象,也可供普通电脑用户了解和学习网络安全技术之用。

笔者不避寒暑,历时一载有余,三易其稿,反复修改、增删,其所追求的目标,可以概括为6个字:专业、深入、权威。

挑战与危机

近几年来,随着网络应用的飞速发展,各种网络攻击事件也层出不穷,对网络管理员和网络安全工作者提出了更高的要求。以“国家计算机网络应急技术处理协调中心(CNCERT)”于2008年底发布的网站攻击统计表为例,在2008年1月至12月,中国大陆地区.gov.cn网站被篡改数量各月累计达3595次,其中不重复的即有2891个。



针对网站的攻击是明显的、易于统计的,但是针对网络进行的综合渗透攻击事件相对则要隐蔽得多,统计也不容易,因此也未能像其他网络攻击事件一样引起广泛重视。事实上,渗透攻击的发生率和危害性远远大于普通的网络攻击事件。许多网络被渗透入侵长期控制,造成大量机密信息泄露和巨额经济损失。

网络渗透攻击事件的发生极为普遍,众多的网络管理员和网络安全工作者却对网络安全环境所面临的严峻考验缺乏足够的认识,因而也未曾采取全面的防范补救措施应对各种攻击行为。

入侵腾讯事件,暴露“学”与“术”的误区

目前,市面上关于网络入侵与安全防护的书籍已经非常多了,其中不乏许多资深安全专家的精品之作。同时,有越来越多从事网络安全的管理人员和工作者,开始认识到所面临的网络安全危机,积极参加各种安全培训与认证考试。然而,许多安全书籍和各种认证培训,往往都走入了一个不易察觉的误区。

2006年轰动网络的“入侵腾讯事件”，很典型地暴露了这个误区的存在——一个年仅16岁的少年黑客，利用木马诱骗攻击入侵了著名公司腾讯的网络，控制了该公司80余台计算机的信息系统，获取了该公司的域密码及其他重要资料，进而取得多个系统数据库的超级用户权限。

作为一个国内知名的大型网络公司，其对网络安全必定极为重视。旗下众多网络安全专家及安全管理人员设置的严密安全防范措施，在一个年仅16岁的少年攻击者面前却形同虚设。不得不说，许多网络管理人员和安全工作者，对网络安全的理解与研究，往往侧重于脱离实际的理论，而对理论在现实工作中的应用则缺乏足够的认识。

目前，国内的网络安全界面临着一个非常尴尬的局面，本应该提供网络安全服务的研究组织与培训机构，却大多难以适应和满足实际工作的需求。长期以来，“学”与“术”两极分化，各执一端。

所谓“学”，是指学院式的各种网络安全理论研究，而“术”则是指实用性的技术、方法与手段。其中，“术”的最直接体现，就是各种黑客入侵攻击技术。在许多安全研究者和工作人员的眼中，往往厚“学”而薄“术”，甚至瞧不起“术”，对各种入侵行为和入侵技术持不屑的态度。

但现实的情况是，一个只学了几天黑客入侵技术的脚本小子，所造成的安全破坏，往往会让从事数年安全研究的网络安全专家和工作人员焦头烂额。

专业≠脱离实际的理论

“学”是理论，是基础，没有学则门都入不了，也无法更深刻地了解网络安全的本质；有了“学”，还要有“术”，有真正的实践应用。一个真正的网络安全研究者和合格的安全工作者，往往都是“学”与“术”相结合的。

一本专业的网络安全书籍，不能仅停留在空洞的网络安全理论研究上，更重要的是体现于理论在实践中的应用。攻击与防守是对立却又统一的，“从入侵攻击中学会安全防守，以黑客入侵攻击技术促进安全研究”，这是笔者长期所持的网络安全观点。

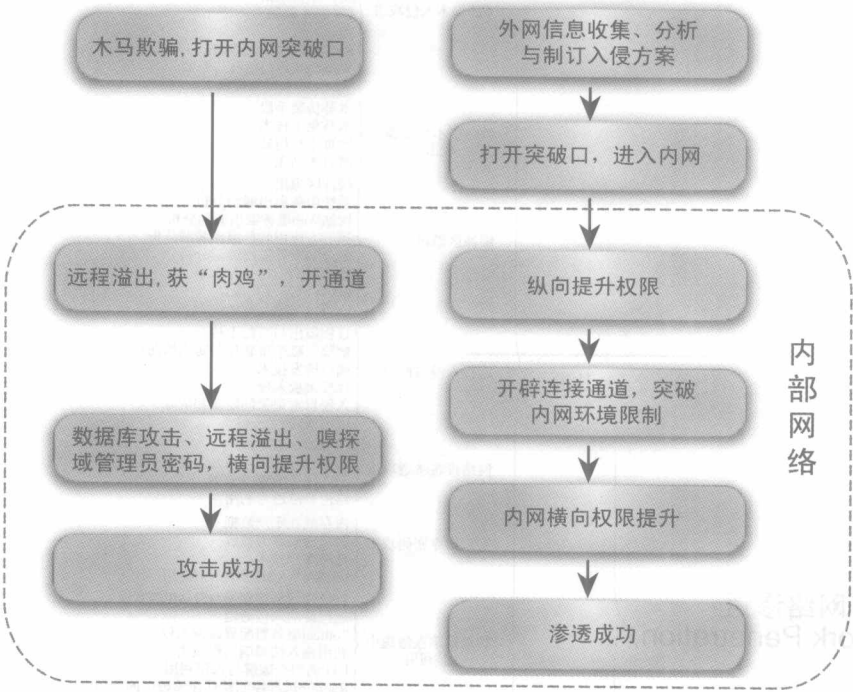
笔者从事网络安全工作多年，担任国内多家网站的安全顾问，长期进行网络渗透测试与网络风险评估。在实际的工作过程中，笔者深知国内网络环境存在着很多漏洞，也了解到部分网络安全从业人员因忽视对黑客入侵攻击事件的关注和研究，在技术上往往存在较大不足。

本书从实际应用出发，通过详细讲解攻击者习惯采用的各种渗透攻击手段与方法，揭露出网络中广泛存在，却总被忽视的安全漏洞，并结合笔者长期积累的安全防护经验，指出相应的防范要点。本书具备较强的专业性和针对性，在网络安全工作中极具参考意义和实用价值。

深入揭秘入侵事件真相

为了尽可能深入地讲解各种网络渗透攻击与测试方法，笔者特意对曾经热炒一时的“入侵腾讯事件”进行深入分析，以此类入侵流程贯穿全书，并针对攻击者每一步入侵提供各种衍生攻击手法与安全防范方案，从而使本书对网络安全工作具有极高的可借鉴性。

本书在编著过程中，力求做到原理清晰、透彻，内容全面、深入，并为本书制作了配套教学视频，整理出部分程序代码，以帮助读者真正深入地掌握渗透攻击及防范技术。



以“腾讯入侵事件”为主线展现渗透入侵攻击流程

权威、全面的知识体系

随着技术发展，网络安全越来越依赖于整体防护。与此同时，网络结构越来越复杂，攻击者入侵网络的手法也不再单一，逐步渗透的入侵攻击技术与行为已经成为主流。而常见的网络安全图书往往仅针对网络入侵中的某一部分或某几部分进行介绍，因此适用面比较窄，实用价值不高。

渗透入侵技术非常隐蔽，难以检测，一旦网络中存在某个缺口，就很有可能导致整个网络的全盘崩溃。同时，渗透攻击本身又是一种高级的入侵手法，在入侵的过程中涉及普通入侵技术、特殊攻击技术和社会工程学等，是从“技术”与“人”两个层面展开的攻击。全面了解攻击者的渗透入侵行为，是维护网络安全所必需的，因此一本权威的网络安全著作要对网络渗透攻击进行深入的分析，帮助网络安全工作者了解黑客渗透攻击行为，最终更好地维护网络安全。

本书对黑客攻击中所使用到的渗透入侵技术和手段进行了全面的分析、讲解，从渗透入侵的基础开始，逐步深入到渗透入侵的各种常见及高级手法，覆盖完整、系统而严谨的安全知识体系。

网络渗透 (Network Penetration)

技术

Web脚本入侵攻击

- SQL Injection
- 旁注攻击
- 数据库入侵
- 文件上传攻击
- Cookies 欺骗
- 跨站入侵
- RFI远程文件包含攻击
- Webshell 后门伪装与隐藏
- Webshell入侵与提权

特洛伊木马欺骗攻击

- 木马伪装手段
- 木马免杀技术
- 网页木马伪装
- 网页木马免杀

缓冲区溢出

- 缓冲区溢出
- 系统服务溢出漏洞分析
- 网站Web服务溢出漏洞分析
- 第三方应用软件溢出漏洞分析
- 安全类软件溢出漏洞分析
- 溢出漏洞的扫描与探测
- 0DAY漏洞及其搜寻
- Exploit编译

远程入侵与控制

- 远程溢出与后门上传
- 解除突破杀毒软件与防火墙防护
- 端口转发技术
- 代理跳板入侵
- 入侵日志记录的隐藏和清除
- 内网入侵

网络设备渗透攻击

- Cisco路由攻击
- 路由器登录密码的暴力破解
- 无线路由的WEP破解
- 路由器渗透与利用

账户口令密码攻击

- 内存截获账户数据
- 账户密码暴力破解
- 克隆账户技术
- IPCS与WMI在入侵中的利用

管理缺陷在渗透中的利用

- 软硬件网络管理平台SNMP的入侵
- 远程终端入侵通道
- Tomcat服务器配置漏洞入侵
- 利用输入法漏洞入侵攻击
- FTP弱口令破解与入侵利用
- Radmin远程控制软件在渗透中的利用

嗅探欺骗技术

- “广播型”网络环境下的嗅探攻击
- 交换机环境下的网络嗅探
- ARP欺骗
- DNS欺骗劫持

人

(社会工程学Social Engineering)

- 敏感信息收集与攻击
 - 利用搜索引擎收集敏感信息
 - 利用社会调查收集敏感信息
 - 根据网络钓鱼或其他欺骗手法收集敏感信息
- 钓鱼式攻击手法
 - 制作虚假邮件攻击
 - 特洛伊木马欺骗攻击
 - 制作虚假网站进行攻击
- 密码心理学攻击
 - 利用生日、电话号码、身份证等信息猜解密码
 - 利用亲友姓名及相关信息猜解密码
 - 系统默认密码和常用的弱口令密码

本书所涵盖的渗透入侵技术体系

一本著作的完成离不开许多人的默默支持与帮助，是众人心血和汗水的结晶。本书在编写过程中，得到了来自多方面的大力支持和不同方式的关心及帮助，借此机会对他们表示诚挚的感谢。本书最终能够出版面世，首先要感谢电子工业出版社易飞思公司的策划编辑张春雨，他的帮助和指导使我受益匪浅。安全中国、黑客基地、黑鹰安全网、华夏黑客同盟、黑客组织 H.S.T 中多位给予帮助的好友，在此也一并表示感谢。还要感谢我的妻子张黎女士，她对本书同样付出了大量的心血和时间。最后，还要特别感谢的是一直给予我人生指引和教导的李老师。

由于时间仓促，本书难免存在不足之处，真诚地希望专家、学者和读者朋友们批评指正。

肖 遥

光盘资源清单

本光盘内容主要分为视频和源代码两部分，视频位于“\Video”文件夹中，源代码位于“\Code”文件夹中。

一、视频部分

- \data\Video\第2章\利用 Domain 进行自动化旁注攻击

一个安全的网站是如何被其他网站“陷害”的？Domain 是一个自动化的旁注攻击工具。本视频教程演示了如何利用 Domain 对一个安全性很好且没有漏洞的网站进行入侵。由于攻击者可通过入侵其他网站，绕道攻击安全的网站，所以只要在同一虚拟主机上的其他网站存在漏洞，安全的网站实际上毫无安全性可言。

- \data\Video\第2章\PHP X-CODE BUG SCAN 自动挖掘文件包含脚本漏洞

RFI 文件包含漏洞的情况在 PHP 程序中广泛存在，如果难以置信，不妨试试用 PHP X-CODE BUG SCAN 这个小工具，扫描一下自认为很安全的脚本程序，结果将会让人大吃一惊！

- \data\Video\第2章\利用 Goo 小跑堂的一次 RFI 攻击

Google 其实很危险！Google 这个最常用的搜索引擎，在黑客手中也能变成安全攻击的武器。黑客编制出一个特殊的小工具，可以自动化采集 Google 的搜索结果，最终实现自动化批量检测入侵漏洞的目的。本视频教程演示了攻击者如何利用一个叫做 Goo 小跑堂的工具，进行针对 RFI 远程文件包含漏洞的自动化攻击。

- \data\Video\第2章\secdrv.sys 核心驱动溢出 Webshell 提权实例

在 Windows 系统中曾经存在一个 secdrv.sys 核心驱动溢出漏洞，这个漏洞通常用于本地权限提升攻击。看看攻击者是如何在入侵了某个网站后，利用此漏洞在 Webshell 中提升权限，实现远程提权，得以入侵并控制整个网站服务器。

- \data\Video\第2章\木马程序加特殊壳使国内所有杀毒软件免杀实例

再厉害的杀毒软件也有软肋，让病毒、木马免杀有时其实很简单。在本视频教程中，攻击者仅仅是利用了一个不常见的加壳软件，对病毒、木马程序进行加壳处理，就让杀毒软件无法识别了。

- \data\Video\第2章\IE7 0day 制作网页木马过程演示

IE7 0day 是 2008 年底在网上秘密发布的一个 IE 溢出漏洞。本视频重现了漏洞始发不久，攻击者利用网络资源制作生成 IE7 0day 漏洞攻击的网页木马的全过程。

- \data\Video\第3章\MS08-067 远程溢出漏洞攻击演示

MS08-067 远程溢出漏洞是 2008 年曝出的危害最严重的漏洞之一。远程溢出漏洞现在并不多见，看看 MS08-067 远程溢出漏洞攻击演示，了解一下攻击者是如何从远程无声无息地控制你的电脑！

- \data\Video\第4章\溢出后利用 TFTP 上传木马演示

在入侵远程溢出获得 CMD Shell 后，在本地搭建一个 TFTP 服务器，可以很容易地将木马控制程序上传到被溢出的远程主机上，继续渗透入侵。

- \data\Video\第4章\溢出后利用 VBE 脚本上传木马演示

对于安装了防火墙的主机，可能关闭了 FTP 和 TFTP 端口，不能直接从本机上传木马服务。不过只要主机在网络中，只要写入小小的一段 VBE 脚本，就可让主机自动通过 80 端口连接网页下载，运行木马程序，百分百突破远程主机上的防火墙。

- \data\Video\第4章\溢出后利用批处理上传木马演示

在溢出入侵后往往可以通过转换的方法，将 EXE 文件转换成 BAT 文件，无论远程主机多 BT，一样可以成功上传。

- \data\Video\第4章\AIO 渗透中的简单利用演示

AIO, 这个不到几十千字节的小小入侵工具, 竟然包含了数十种入侵工具的功能! 看看这个恐怖的小工具, 是如何被攻击者在渗透入侵过程中利用。

- \data\Video\第 4 章\灰鸽子木马配置与生成

灰鸽子是国内一款大名鼎鼎的远程控制木马, 虽然历经各大杀毒软件厂商的围剿, 但仍然死而不僵。看看灰鸽子木马是如何被制作出来的。

- \data\Video\第 4 章\灰鸽子木马远程控制肉鸡

数据信息泄露、摄像头被偷窥。木马的危害远不止于这些, 攻击者可以利用种植在你电脑中的木马, 无声无息地远程控制你的一举一动。

- \data\Video\第 5 章\利用 SNMP 入侵 Cisco 路由器

不会配置 Cisco 路由器, 算不上一个合格的网管。但是 Cisco 路由器的安全配置, 又有多少网管能真正做到呢? 看看攻击者如何利用 Cisco 路由器的 SNMP 服务, 远程入侵、控制路由器, 让路由器成为渗透的跳板。

- \data\Video\第 5 章\快速入侵 ADSL 宽带路由器

ADSL 宽带路由器的应用非常普遍, 不过能做到安全配置的用户却非常少。攻击者只需短短几分钟, 就可随意控制数十台 ADSL 宽带路由器。

- \data\Video\第 6 章\利用 LC5 破解管理员密码

LC5 是一个老牌的破解工具, 不会用这个工具就算不上是一个合格的安全技术工作者。本视频教程将揭示如何利用 LC5 破解 Windows 主机管理员的密码和账号。

- \data\Video\第 6 章\利用 CA 进行账号克隆

CA 是出现最早的一款账号克隆工具, 可以让你的系统中凭空多出拥有几个管理员权限的账号, 然而你却无法从系统中看出任何端倪。

- \data\Video\第 7 章\Snmputil 刺探系统信息

SNMP 服务在很多主机和网络设备上都是默认开启的, 它所带来的安全隐患是你无法想象的! 看看攻击者如何利用 SNMP 服务, 轻易获得目标主机的详细信息。

- \data\Video\第 7 章\弱口令入侵 Tomcat Web Application Manager

Tomcat 服务器常被用在 JSP 网站中, 而很多 Tomcat 服务器的弱口令漏洞也是比较常见的。攻击者利用弱口令漏洞, 很容易就可以上传一个 WAR 木马, 从而获得整个服务器的最高控制权限。

- \data\Video\第 7 章\ImeRdp 利用输入法漏洞远程入侵终端

Windows 系统重现输入法漏洞! 输入法漏洞的危害实在太大了, 如今 Windows 系统中的第三方输入法漏洞再次出现。攻击者只需要利用一个小工具, 就可以在远程终端登录窗口中调用第三方输入法, 让原本无法利用的第三方输入成为系统的后门, 随意进入远程主机。

- \data\Video\第 8 章\RawSniffer 嗅探器的使用

在渗透入侵过程中, 攻击者往往会利用一些嗅探工具设下陷阱, 截取内部网络的机密信息和数据。本视频教程将演示 RawSniffer 嗅探器在渗透入侵过程中的应用。

- \data\Video\第 8 章\hijack 在嗅探中的利用

hijack 是一个综合性的 ARP 欺骗工具, 嗅探是其必备的功能之一, 而且可在交换环境中使用。本视频教程将演示如何在交换网络中利用 hijack 进行嗅探入侵。

- \data\Video\第 8 章\hijack 进行 ARP 欺骗挂马攻击

hijack 最恐怖之处莫过于它的 ARP 欺骗挂马功能。启动这个功能, 整个局域网中的所有主机, 在访问任何网站时, 都会被网页木马攻击! 攻击者在渗透入侵中, 只需采用这种攻击方法, 就可间接地控制任何内网主机, 危害极其巨大。

二、代码部分

- \Code\第 3 章\Blackice ICQ iss_pam1.dll remote overflow exploit.C

ISS RealSecure/BlackICE 的协议分析模块 (Protocol Analysis Module, PAM) 用于通过解析网络协议来执行进一步地分析和攻击检测, 使用在当前所有 ISS 入侵检测产品中。ISS RealSecure/BlackICE PAM 监视 ICQ 服务器应答处理函数中存在缓冲区溢出问题, 远程攻击者可以利用这个漏洞进行远程缓冲区溢出攻击, 最终以 SYSTEM 进程权限在系统上执行任意指令。这个文件是基于 Blackice ICQ 的 iss_pam1.dll 模块溢出漏洞进行攻击的程序源代码。

- \Code\第 3 章\CCProxy 6.2 Telnet Proxy Ping 远程栈溢出 POC.txt

CCProxy 6.2 是最流行的国产代理服务软件, 主要用于局域网内共享宽带上网、ADSL 共享上网、专线代理共享、ISDN 代理共享、卫星代理共享、蓝牙代理共享和二级代理共享等代理上网。CCProxy 6.2 代理服务器在远程进行 Telnet 代理时, 执行 Ping 命令, 如果命令长度超过许可的值就会造成溢出。本文文件是用于 CCProxy 6.2 Telnet Proxy Ping 远程栈溢出攻击测试的源程序代码。

- \Code\第 3 章\CCproxy 6.5 Connect BufferOverflow POC.pl

利用 CCProxy 6.5 版本的 Connect 连接进行溢出攻击的 Code。

- \Code\第 3 章\CCproxy 6.61 HTTP CONNECT 栈溢出漏洞 POC.pl

利用 CCProxy 6.61 版本的 HTTP 代理功能, 在进行 Connect 连接时进行栈溢出攻击的 Code。

- \Code\第 3 章\CCproxy 6.61 HTTP CONNECT 请求栈溢出漏洞 POC.pl

另一个 CCProxy 6.61 HTTP CONNECT 溢出的 Code。

- \Code\第 3 章\CCProxy Log Remote Stack Overflow Exploit POC.c

CCProxy 日志远程溢出漏洞攻击源 Code。

- \Code\第 3 章\IIS 的 index server .ida 和 .idq ISAPI 扩展远程缓冲溢出漏洞测试代码.c

经典的 IIS 服务器 IDQ 和 IDA 远程溢出漏洞攻击代码。

- \Code\第 3 章\iMail v8.05 LDAP service remote sploit by kralor.c

一个普遍存在于各种邮件服务器上的 LDAP 远程溢出攻击代码示例。

- \Code\第 3 章\IPSwitch IMail LDAP Daemon Remote Buffer Overflow Exploit .c

- \Code\第 3 章\IpSwitch IMAIL Server IMAPD Remote r00t Exploit by kcope.c

- \Code\第 3 章\IpSwitch IMAIL Server IMAPD Remote r00t Exploit by kcope.pl

以上是 3 个邮件服务器的经典溢出攻击 Code。

- \Code\第 3 章\Microsoft IIS 5 SSL exploit 溢出漏洞测试代码.c

IIS 服务器的又一个 SSL 安全连接溢出漏洞攻击 Code。

- \Code\第 3 章\MS05029 溢出工具源代码.c

- \Code\第 3 章\Ms05039 正向溢出源代码.c

- \Code\第 3 章\Serv-U 5.2 Remote Denial of Service Exploit.c

- \Code\第 3 章\Serv-U FTPD 3.x 4.x MDTM Command remote overflow.c

- \Code\第 3 章\Symantec Multiple Firewall DNS Response Denial-of-Service.c

Symantec 防火墙曾经存在的一个 DNS 拒绝服务攻击 Code。

- \Code\第 3 章\THCISSLame 0.3 - IIS 5 SSL remote root exploit.c

- \Code\第 3 章\THCISSLame.c

- \Code\第 3 章\WebDAV 溢出程序代码.c

- \Code\第 3 章\webdav 溢出程序源代码.c

- \Code\第 3 章\Windows Lsasrv.dll RPC [ms04011] buffer overflow Remote Exploit.C

- \Code\第 7 章\3389.vbs

在命令行下开启 3389 终端的一段代码, 简洁而强大。

第 1 章	分析入侵腾讯事件，初识网络渗透	1
1.1	网络渗透概述	2
1.1.1	以“蚁穴”引发“堤崩”——渗透的特质	2
1.1.2	入侵腾讯——典型的网络渗透攻击事例	4
1.1.3	学习网络渗透的意义	6
1.2	“渗透测试”与攻击密不可分	7
1.2.1	渗透测试/攻击的分类	7
1.2.2	探穴、控制与渗透——渗透过程与攻击手段	9
1.2.3	从入侵腾讯事件，看渗透的几个步骤	12
第 2 章	Web 脚本与木马欺骗，打开渗透突破口	15
2.1	木马控制客服主机，打开安全防线缺口——入侵腾讯事件剖析之一	16
2.1.1	内网主机是如何被控制的	16
2.1.2	外紧内松的安全堡垒与内网渗透思想	16
2.2	SQL 打开最脆弱的渗透突破口	18
2.2.1	Web 脚本攻击更利于渗透入侵	18
2.2.2	“常青”的 SQL 注入攻击	19
2.2.3	PHPCMS 网站管理系统的 PHP 注入攻击实例	22
2.2.4	拐弯渗透网站的“旁注”	28
2.3	RFI 远程文件包含，渗透不留踪迹	31
2.3.1	最易利用攻击的 RFI 漏洞	32
2.3.2	挖掘网页程序的 RFI 漏洞	34
2.3.3	赤手空拳，远程包含入侵 PHPCMS 2007	35
2.3.4	小跑堂与清扫员，利用 Google 发起 RTF 攻击	37
2.4	渗透网站数据库核心	40
2.4.1	暴库的成因，不仅%5c	40
2.4.2	风讯暴库与挂马渗透	40
2.5	文件上传为渗透铺路	45
2.5.1	上传功能导致的漏洞	45
2.5.2	打破数据库备份禁制，风讯后台上传获取 Webshell	46
2.6	长期渗透留下 Webshell 后门	52
2.6.1	让 ASP 木马躲过杀毒软件查杀	52
2.6.2	暗藏 Webshell 后门	53
2.7	夺取绝对权力，为 Webshell 提权	56

2.7.1	Webshell, 权力不足	56
2.7.2	常见 Webshell 提权方法	57
2.7.3	杀毒软件为 Webshell 提权服务	59
2.7.4	本地溢出提权, Webshell 无限制	64
2.7.5	偏门木马, 提升权限	68
2.8	特洛伊, 内网渗透之计	73
2.8.1	客服被欺骗, 捆绑了灰鸽子的聊天记录查看器	73
2.8.2	免杀, 让灰鸽子横行	77
2.9	办公文档藏木马, 意想不到的渗透入侵	88
2.9.1	社会工程学与木马常见的欺骗手段	88
2.9.2	来自办公文档的安全威胁——Office 漏洞文档木马	93
2.10	利用网页木马, 从分站渗透到主站服务器	98
2.10.1	寻隙而入的网页木马	98
2.10.2	IE 7 的 0day 挂马程序, XML 做网马	99
2.10.3	百度搜霸与挂马漏洞	102
2.10.4	下载与视频, 网页木马泛滥	104
2.10.5	黑手利刃, 万能溢出所有目标	106
2.11	封锁关口, 追查入侵者	111
2.11.1	揪出隐藏的 ASP 木马后门	111
2.11.2	木马分析, 追踪入侵者	115
第 3 章	缓冲区溢出, 入侵与提权最常用手段	119
3.1	缓冲区溢出攻击	120
3.1.1	远程溢出, 获取第一台“肉鸡”——入侵腾讯事件剖析之二	120
3.1.2	内网中远程溢出极具威胁	120
3.1.3	dir 命令——身边的溢出实例	121
3.1.4	“数据长度”大于“缓冲区”——溢出的原理	123
3.1.5	深入缓冲区溢出攻击	123
3.2	安全第一守则——最小化服务模式	127
3.2.1	每次的漏洞都是一场灾难——RPC 服务远程溢出漏洞	127
3.2.2	RPC 带来的“冲击波”	128
3.2.3	Sasser 震荡波——RPC 服务漏洞又一波	132
3.2.4	疯狂的蠕虫病毒“VanBot”——MS07-029 Windows DNS RPC	137
	远程溢出漏洞	137
3.2.5	四年一遇, 扫荡波大发作——MS08-067 远程溢出漏洞大攻击	143
3.2.6	名称验证, 形同虚设——WINS 服务名称验证远程溢出	155
3.2.7	狙击波——“即插即用”服务等于“即攻即漏”	161
3.2.8	MSDTC 与 COM+ 服务联手“放水”	166

3.2.9	网络安全中的“最小化原则”	172
3.3	谨防网站服务器中的潜伏漏洞	173
3.3.1	多多并非益善，多余扩展引发溢出	173
3.3.2	打印扩展，多此一举	176
3.3.3	扩展变身网站杀手	177
3.3.4	安全协议不安全	180
3.4	第三方软件，安全防线上的蚁穴	183
3.4.1	代理之痛，不可信任的 HTTP CONNECT “请求”	183
3.4.2	邪恶的“伊妹儿”	192
3.4.3	FTP 服务器，泛滥了的权限	198
3.5	安全软件不安全，溢出漏洞依然在	203
3.5.1	SMB 协议边界检查不严——ISS RealSecure/BlackICE 防火墙 远程溢出	203
3.5.2	诺顿防火墙，一击即溃	205
3.5.3	Kerio 防火墙也不安全	208
3.5.4	VNC Owner 安全远控反被控	211
第 4 章	鸽子飞翔——溢出后开辟控制通道	217
4.1	不可缺少的控制通道——入侵腾讯事件剖析之三	218
4.2	渗透先遣，工具上传	218
4.2.1	反向 FTP，绕过禁制	218
4.2.2	穿越防火墙的 TFTP	222
4.2.3	一段 VBE 脚本代码	224
4.2.4	转换思路，网马上传	226
4.2.5	批处理解难题	228
4.2.6	WMI 为攻击者敞开大门	230
4.2.7	不被检测的 VBS 代码	231
4.3	清除障碍，打通渗透通道	233
4.3.1	掌控门牌口令	233
4.3.2	开启 3389 隧道	238
4.3.3	后门程序的上传与隐藏	239
4.3.4	端口转发渗透内网	241
4.3.5	清除入侵记录	242
4.4	暴力冲出杀毒软件与防火墙重围	243
4.4.1	终结杀毒软件与防火墙	243
4.4.2	在 IPSEC 上打开缺口	244
4.4.3	“安全中心”不安全	249
4.5	知己知彼，All In One	254

4.5.1	工具全在一起	254
4.5.2	攻击, 很邪恶	254
4.5.3	防守, 为我所用	260
4.5.4	AIO 命令详解表	263
4.6	鸽子飞翔, 穿越内网	266
4.6.1	生成灰鸽子木马	267
4.6.2	木马如何操作远程计算机文件	270
4.6.3	隐私外泄, 桌面与摄像头的监视控制	272
4.6.4	鼠标键盘不请自动——控制远程计算机鼠标键盘	273
4.6.5	系统全面失控——木马修改控制系统设置	274
第 5 章	打破隔离, 不同环境中的网络设备攻击	279
5.1	域中的嗅探——入侵腾讯事件剖析之四	280
5.1.1	主机身份角色与渗透方式的选择	280
5.1.2	网络分布与构成	280
5.2	网络分析与渗透方案的确定	286
5.2.1	命令行下的网络信息刺探	286
5.2.2	信息利用与手法制定	292
5.3	端口转发与代理, 内网潜入的基础	293
5.3.1	被误用的端口转发	293
5.3.2	“肉鸡”变跳板, Htran 端口转发	294
5.3.3	木马与终端, 助攻击者渗透内网	302
5.4	路由, 打开内网渗透的通道	308
5.4.1	路由器的安全隐患	308
5.4.2	Cisco 路由器攻击案例	311
5.4.3	路由器登录密码的暴力破解	319
5.4.4	无线路由的 WEP 破解	328
5.4.5	路由器渗透与利用	333
5.5	截断通道, 掐住内网入侵的命脉	341
5.5.1	限制代理上网, 阻止内网突破	341
5.5.2	路由安全配置手册	344
5.5.3	ADSL MODEM 的简单保护	349
5.5.4	无线路由安全设置	350
第 6 章	隐蔽通道中的密码权力争夺	355
6.1	管理员密码的失守——入侵腾讯事件剖析之五	356
6.2	被剥光的威胁——内存解密	356
6.2.1	针对 winlogon 的 pulist+Findpass 组合	356

6.2.2	LSASecretsView, 一秒解密 lsass 进程	358
6.3	暴力破解	362
6.3.1	Hash 与管理员密码	362
6.3.2	SAM 文件秘密不在	364
6.3.3	SYSKEY 双重加密, 亦难守密码	367
6.4	计算机通行证的争夺战	374
6.4.1	假借注册表攻击 SAM	374
6.4.2	手工克隆的无形账户	376
6.4.3	系统通行证伪造机	379
6.4.4	攻击者之矛为管理员之盾——揪出隐藏的克隆账户	383
6.5	无法检测的密码后门	386
6.5.1	无法检测与删除的后门	386
6.5.2	辅助工具为 3389 终端开门	388
6.6	隐藏账户开门, 渗透新隧道	391
6.6.1	突破被禁用的 IPC\$	392
6.6.2	一个 WMI 开启 3389 终端的脚本实例	393
6.6.3	WMI 远程攻击工具	398
第 7 章	秘密渗透, 横向提权的众多暗道	405
7.1	口令被窥, SQL 数据库失守——入侵腾讯事件剖析之六	406
7.2	防火墙上的缺口, SNMP 信息外泄	406
7.2.1	SNMP 安全机制很脆弱	406
7.2.2	SNMP 威胁 Windows 网络安全	409
7.2.3	绕过防火墙, 刺探系统信息	412
7.2.4	SNMP 图形浏览与暴力破解	418
7.2.5	加固 SNMP 服务, 防范信息泄露	421
7.3	攻击者偏爱的入侵通道——远程终端	429
7.3.1	远程终端, 为管理而生	429
7.3.2	为攻击所用——远程终端入侵的常见手法	431
7.3.3	溢出窗口下的终端开启	436
7.3.4	远程桌面入侵的一些秘密	441
7.3.5	暗藏后门的 Ghost 系统与终端危机	445
7.3.6	远程终端安全之道	452
7.4	从 Tomcat 到 3389 “肉鸡”	454
7.4.1	管理界面验证不严	455
7.4.2	Tomcat 主机暴露 8080 端口	456
7.4.3	关紧 Tomcat 管理之门——Tomcat Administration Web Application	462

826	网页配置	462
507	7.5 古老的输入法漏洞, 攻击者的新途径	463
507	7.5.1 新 Windows Vista 系统, 输入法漏洞	464
407	7.5.2 谁说输入法漏洞不能用	469
507	7.5.3 被扩大的输入法远程终端入侵	476
807	7.6 弱口令打开暗藏的入侵通道	479
507	7.6.1 虚设密码, 攻击者的方便之门	480
095	7.6.2 难以兼顾的 FTP 弱口令	483
072	7.6.3 Radmin 与 4899 “肉鸡”	489
	第 8 章 入侵不过是一场欺骗, 渗透入侵的高级手法	499
007	8.1 嗅探, 窃取域管理员密码——入侵腾讯事件剖析之七	500
185	8.1.1 网络中的窃听器——嗅探 (Sniff)	500
115	8.1.2 嗅探技术的分类与实施	501
507	8.2 “广播型”网络环境下的嗅探	503
607	8.2.1 经典嗅探攻击——Sniffer Protable	503
905	8.2.2 CommView Remote Agent 远程嗅探	505
306	8.2.3 命令行下的嗅探利器——RawSniffer	508
	8.2.4 隔墙有耳, 聊天信息的嗅探	512
707	8.3 “交换型”网络环境下的嗅探	515
004	8.3.1 ARP 欺骗, 迷惑交换机	515
004	8.3.2 “交换型”网络环境下的嗅探器 ARPSniffer	517
007	8.4 ARP 挂马攻击——嗅探欺骗的最恐怖方式	519
107	8.4.1 ARPSpoof 欺骗, 公司网页被黑挂马	519
507	8.4.2 内网中的 DNS 欺骗, 强大的欺骗工具 Cain	523
414	8.4.3 带 ARP 欺骗攻击的渗透利刃——hijack	527
134	8.5 ARP 防火墙, 拦截嗅探的黑手	531
904	8.5.1 金山 ARP 防火墙	532
107	8.5.2 360ARP 防火墙	533
107	8.5.3 彩影 ARP 防火墙	536
002	8.5.4 瑞星 ARP 防火墙	538
122	8.5.5 AntiARP-DNS 防火墙	539
314	8.5.6 ARP 卫士	541
104	8.6 挑战局域网安全极限, ARP 防火墙也无奈	543
124	8.6.1 无 ARP 欺骗的 Skiller	543
024	8.6.2 ARP 防火墙拦截不住的嗅探	545
081	8.6.3 无 ARP 欺骗与嗅探的分析	547
107	8.7 世界头号黑客的秘密武器——社工与渗透	549