郝永清［藏锋者］ 编著

网络安全攻防实用技术深度案例分析

黑客

FTP攻击剖析与实用防御技术精解

- 实用级暴力破解技术实战攻防
- FTP经典权限提升漏洞深度解析
- FTP协议缺陷下的嗅探攻防案例模拟
- 构建足够安全的IIS FTP Server

科学出版社
www.sciencep.com

网络安全攻防实用技术深度案例分析

黑客 FTP 攻击剖析与实用防御技术精解

郝永清 [藏锋者] 编著

科学出版社

北京

内 容 简 介

本书以网络应用中，普及率和使用率仅次于 Web 服务的 FTP 服务安全为核心题材（Web 安全技术请参考此系列书籍第一本《黑客 Web 脚本攻击与防御技术核心剖析》），通过案例剖析的方式，以由浅入深、浅显易懂的行文笔调，结合藏锋者网络安全网站（www.cangfengzhe.com）上的大众关注热点，详细阐述了三大主流 FTP 服务器的攻击案例与安全防护方案。

本书中，以 Windows 系统自带 FTP 系统服务、国内使用率超高的 Server-U FTP 服务器、国外最流行的 Gene6 FTP 服务器为蓝本，穿插地简单介绍了三大主流 FTP 服务器的搭建方式，进而分析其中存在的设置、配置缺陷，最后深入到服务本身缺陷与漏洞的攻击分析。以实际攻击案例和有很强针对性的防范技术并重的方式，辅以最后全功能的、安全度很高的 FTP 服务器搭建方法，力求清楚、实用地为读者阐述时下流行的黑客 FTP 攻击方法与防范方法。

本书适合以下人员阅读：对网络安全技术有兴趣并想从事相关行业的大学生；就读于网络信息安全相关专业的研究生；负责企业、公司网络信息安全的从业者；网络安全技术专业研究人员；所有对网络安全有兴趣的爱好者参考阅读。

图书在版编目（CIP）数据

黑客 FTP 攻击剖析与实用防御技术精解 / 郝永清编著. —北京：科学出版社，2010

（网络安全攻防实用技术深度案例分析）

ISBN 978-7-03-026018-5

Ⅰ.黑… Ⅱ.郝… 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 206783 号

责任编辑：田慎鹏 霍志国 / 责任校对：张小霞

责任印制：钱玉芬 / 封面设计：耕者设计工作室

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

骏走印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2010 年 1 月第 一 版 开本：787×1092 1/16

2010 年 1 月第一次印刷 印张：24 1/2

印数：1—4 000 字数：572 000

定价：49.80 元

（如有印装质量问题，我社负责调换）

作 者 简 介

郝永清 CISSP、CISP、MCSE 资深讲师，藏锋者网络安全网（www.cangfengzhe.com）核心成员之一，主要从事信息安全相关工作，负责深入分析用户安全需求；有近十年的授课经验，为 300 多家企业千余 IT 经理及 IT 技术人员做过安全培训；有丰富的项目经验，同时密切跟踪国内外的安全动态，对严重安全事件进行快速响应；对各种恶意软件进行分析，提供检测和解决方案，并完成产品的安全评估，如防火墙、入侵检测、漏洞扫描等；参与众多公司网络的渗透测试项目，并对病毒和木马有深入了解。

丛 书 序

攻防技术辩证一体

辩证地看，网络安全技术包含两个方面，正面是防御，反面是攻击，二者缺一不可：没有了攻击技术，防御技术无从谈起；没有了防御技术，攻击技术就成为摆设，没有丝毫存在的意义。

本系列书从始至终贯彻这一基本要点，和其他同类图书的最大区别就在于此：

我们虽然会详细模拟攻击者的攻击过程，但其目的是为了在防御的时候更加清楚地明白需要防御的“缺口”在什么地方。

我们也会详细讲解防御体系的搭建思路和过程，但是也会讨论突破这样的防御体系的新的攻击技术和思路，进而推出适当的防御技术。

更多的时候，本系列书籍的角度是在攻击者和防御者两者之间进行切换模拟——就好比现在工作在岗位上的网络安全技术工程师一样，经常都需要扮演攻击测试者和防护者的双重身份。

贯彻始终的“黑客”思维正面导向

有圈内人曾用“妖魔化”来形容今天的黑客，这很贴切但本质很荒谬、很无奈。

原本作为褒义的“黑客”一词，是指热心于计算机技术，水平高超的电脑专家。在负面新闻不明真相的炒作下，在无数恶意攻击事件的曝光之后，在利欲熏心者的盲目追崇中，“黑客”一词目前几乎已经完全沦为贬义的破坏者的代名词。

网络需要发展，技术需要进步。让这样歪曲的思维误导的长期后果，就是越来越多的人远离“黑客”，远离本来可能为网络发展、技术进步而提供非常大助力的群体，让原本正面积极的群体变得愈加孤僻，愈加“妖魔”，甚至沦陷。

所以，本系列书籍坚持正面积极的正确“黑客”思维导向，并将其贯彻始终，力争明晰恶意攻击者和善意黑客之间的区别，力争将攻击技术这把锋利的刀用在推动技术进步之上，力争让更多即将误入歧途的被误导者看到光明的希望！

专注于热点技术的追踪和普及

时代在变，技术也在变，技术热点的推陈出新本质就是技术进步的演变过程。

关注并专注于最新的攻防技术，并将这些新的、热的网络安全技术普及给大众，这就是本系列书籍的重要目标之一。

就当下的网络安全状况来看，针对 Web 服务的攻防、针对服务器的渗透攻防、针对个人计算机长期精准的控制和安全、针对网络协议缺陷的研究和修补等，都是攻击者、防御者们津津乐道的话题——自然也就是本系列书籍关注的话题。

需要提出注意的是，本系列书籍是动态的，是持续变化的，是跟随着热点变化而进步的，所以本系列书籍将长期、持续、及时地推出！

案例化和可操作性的实现尝试

就本质来说，计算机技术是一门动手能力比较强的学科。作为书籍来说，可操作性的优劣将决定此书的成败。

我们采用案例化的方式来进行技术讨论，针对网络安全技术的攻击和防御两方面，采用有针对性的、螺旋上升的“攻防”对立案例进行演示，力求让各技术体系毫发毕现的出现在读者面前——注意这不是空泛的理论交锋，这是可以做到“按图索骥”一步一步攻击和防御操作的详细记录！

最大化的提升书籍的易用性

任何事情的起步都是艰辛的，作为过来人的编者深刻明白迈出第一步的艰辛，所以，对于刚刚接触网络安全相关领域的新手，对于理解书中相关概念略显吃力的读者，我们尽量将一些关键的概念以“基本概念解释”的方式贯穿在文中，并在书末提供速查表。目的只是为了提高系列书籍的易读性，让读者更能贴切的理解各种案例和操作中的原理所在。

系列书籍中，类似于“基本概念解释”的还有适当位置的“技巧”、“提示”，以及序言之后的“本书使用方法”，还有文末的基本概念速查、书中所用演示平台和工具的汇总介绍等项。

希望读者能将这些小项目利用起来，让其为深刻理解书中技术而起到应有的辅助作用。

辅助在线技术交流平台

作为人力有限的编者来说，遗漏在所难免，所以为了更好地为读者服务，也为了除了书籍之外读者还有更方面的解惑、交流、讨论平台，系列书和藏锋者网络安全网（www.cangfengzhe.com）合作，由其提供在线技术交流平台，以便本系列书籍读者更快、更好、更方便地提升技术层次——当然，这个平台肯定是免费的。

部分资料来源于藏锋者

任何技术都存在表现形式上的共性，网络安全技术也不例外。正是因为存在这样的共性，在案例的选取上，本系列书籍使用了部分藏锋者网络上的相关资料。

这样做的原因一来是很多经典资料的确很能明白的说明问题，二来是因为很多典型技术的推出就是因为存在这样的典型案例，三则是出于对实用性的考虑——我们倡导的方式是读者在通读全书后，去藏锋者网站下载并搭建书中案例的相关环境，使用相关工具进行模拟攻击和模拟防护，以达到真正地将书中的技术纳为己有的目的。

纠错及感谢

编著过程仓促，难免有所遗漏或者错误，如有发现，欢迎读者使用上述的网络交流平台与编者联系，提前致谢。

在系列书籍编著过程中，得到很多藏锋者网络上的技术伙伴们的支持和帮助，在此一并表示感谢。

最重要的是，系列书籍的出版和推出，得到科学出版社的大力支持。特别是责任编辑田 sir，事前、事中、事后均提供了莫大的支持，鞠躬谢过。

郝永清

2009 年 9 月于北京

本书使用方法

请用虚拟机

对任何一个网络安全技术爱好者来说，虚拟机都是必须的，也是必要的。

如果读者对本书中所讲案例有兴趣，想亲手操作，以达到最佳的阅读和理解效果，请使用虚拟机在本地虚拟相关系统，并在虚拟机上使用相关工具进行攻击和防御测试。

使用虚拟机的最大目的在于保障读者自身的系统安全；

其次是为了杜绝不经意间由读者兴趣而引发的网络恶意攻击；

然后是为了让读者更深刻的理解不同身份的攻击者和防御者的操作平台、操作方法和操作目的；

最后是为了使读者养成网络安全技术的基本构建、调试习惯，为以后可能遇到的网络安全问题提供最基本的环境支持。

基本概念解释

文中适当位置将出现“基本概念解释”，一般情况下是对上文中和本书主题无关，但却因为案例需要而有所涉及的理论概念。

整个网络安全体系庞大到难以想象的地步，对于有一定经验的读者来说，将文中所述技术和其他相关概念联系在一起是很有裨益的，对技术层次的提升和某方面技术的全面透彻的理解尤为重要。

对于刚刚接触网络安全技术的读者来说，直接的案例风格的书籍虽然可以很方便地提高读者的操作兴趣，快速让读者获得某一领域的相关技术理解，但是这也未免太过于片面，太过于单调。所以，对于新手来说，“基本概念解释”将是一个比较有用的全面地理解网络安全体系的机会，有关联的相关概念更能让新手在脑中构建完整的网络安全体系图。

当然，如果是已经有深入研究的读者，阅读此书只是因为想了解其中最新的技术，那么就大可略过这些内容。

提示

书中适当位置将有“提示”出现，“提示”的作用是编者对特定环境和情况的

说明。

比如是为了演示这个案例而进行的非常规操作，在实际情况中不建议使用这样的操作。

简单来说，“提示”就是编者因为行文需要，为了避免误导读者而做的防护措施。

技巧

和“基本概念解释”、“提示”不同，需要特别指出的是，“技巧”一般是以攻击者的角度给出的说明，这些说明一般是针对特定环境的非常有效的攻击手法。

书中可能出现在为了全盘需要，模拟攻击者进行攻击的时候，没有使用最好的、最灵巧的、最直接的攻击方式，而是采用了和书中相关概念深度符合的基本手法进行攻击模拟，所以以“技巧”的方式补充说明。

案例相关工具和程序平台

网络安全技术很多时候在明白原理之后，不用自己编写相关工具，网络上已经有很多前人编写了适当的攻击和防御工具，所以“站在巨人的肩上”是最好的快速进步的法门。

书中的相关工具除了在对应的章节出现以外，还可在文末以统一的附件形式进行速查。

另外藏锋者网络也专门为本书提供了相关工具和程序平台的下载支持，读者可以浏览并下载。

编者建议读者在虚拟机中搭建这样的相关环境，然后同样是在虚拟机中使用相关工具进行攻击模拟和防御模拟。

在线交流

为了给各技术层次的读者提供及时在线的交流平台，本书和藏锋者合作提供了一个免费的在线交流平台。

读者可以通过登录藏锋者网站（www.cangfengzhe.com）进行技术交流。

编者邮件

由于编著过程比较仓促，难免会出错，欢迎发现错误的读者与编者联系：cangfengzhe@live.cn。

目　录

第1章　透析FTP与FTP攻击

章节内容提点与概述

本章主要内容：

- ■ FTP概念及作用
- ■ FTP传输方式
- ■ FTP工作原理
- ■ FTP的主动和被动模式
- ■ 常用FTP程序

本章典型案例：

- □ 用FTP传输文件的一般步骤
- □ 被动模式下的详细数据连接分析
- □ 主动模式下的详细数据连接分析
- □ 命令行下的FTP使用案例

本章核心概念：

● FTP是英文File Transfer Protocol的缩写，即文件传输协议。它用于Internet上文件的双向传输，用户可以通过FTP把个人计算机客户端与世界各地所有运行FTP协议的服务器相连，访问服务器上的大量程序和信息。

1.1 FTP 概念及作用

一般来说，使用互联网的首要目的就是实现信息共享，而文件传输则是信息共享非常重要的内容之一。

Internet 早期的时候，要实现传输文件并不是一件容易的事，因为 Internet 是一个非常复杂的计算机环境，这些计算机可能运行不同的操作系统，有运行 UNIX 的服务器，也有运行 DOS、Windows 的 PC 机和运行 Mac OS 的苹果机等，各种操作系统之间的文件交互需要建立一个统一的文件传输协议，这就是所谓的 FTP。基于不同的操作系统有不同的 FTP 应用程序，而所有这些应用程序都遵守同一种协议，这样用户就可以把自己的文件传送给别人，或者从其他的用户环境中获得文件。

作为最典型的网络应用之一，FTP 拥有极为庞大的用户群体和使用范围。

它和 Web 服务的页面访问一样，同样可以做到网络中的数据传送和交互，这也是 FTP 被推出并且使用至今的基本目的。

同样，FTP 也可以让网络中的用户端和服务器端忽略彼此的操作系统版本等外部因素，使用不同的操作系统、不同的软件程序，达到同样的文件交互的目的。这点也是 FTP 被大量使用的一个重要原因。

第 1 章对 FTP 的相关定义、协议说明和其他基本概念进行了阐述，目的是为了在开展以案例的方式进行 FTP 攻防讲解之前，让基础的读者有一个清晰的概念理解。

本节将主要介绍 FTP 定义和作用，如果是比较熟悉 FTP 的读者，则可以直接跳过此章，进入后面的攻防案例章节。当然，如果系统、全面、深入地重温 FTP 协议、工作流程等基础理论，对深入了解攻防实现技术会很有帮助——特别是新手可以多阅读第 1 章。

1.1.1 什么是 FTP

简单地说，FTP 就是完成两台计算机之间的复制。

换一个比较通俗的说法可能更多读者会比较容易理解：从远程计算机上使用 FTP 复制文件至自己的计算机上，称之为“下载（download）”文件。若将文件从自己计算机中复制至远程计算机上，则称之为“上载（upload）”文件。

1.1.1.1 FTP 定义

FTP 是英文 File Transfer Protocol 的缩写，即文件传输协议。它用于 Internet

上文件的双向传输，用户可以通过 FTP 把个人计算机客户端与世界各地所有运行 FTP 协议的服务器相连，访问服务器上的大量程序和信息。

FTP 协议是 TCP/IP 协议中的一员，FTP 协议的任务就是将文件从一台计算机传送到另一台计算机，这个实现方式与这两台计算机所处的位置、连接方式，甚至是是否使用相同的操作系统均无关。也就是说，假设两台计算机通过 FTP 协议连接，并且都能访问互联网，那就可以用 FTP 命令来传输文件，虽然每种操作系统上使用的 FTP 程序有某些细微差别，但是协议的基本命令结构是相同的，效果也是相同的。

因为是大家熟知的且是标准的 TCP/IP 协议，一般情况下默认的 FTP 端口号是 21。

> **基本概念解释：**什么是 TCP/IP 协议？
>
> TCP/IP 是 Transmission Control Protocol/Internet Protocol 的缩写，中文译名为传输控制协议/网际协议，又叫网络通信协议，这个协议是 Internet 最基本的协议、Internet 国际互联网络的基础。TCP/IP 是供已连接因特网的计算机进行通信的通信协议，它定义了电子设备（如计算机）如何连入因特网，以及数据如何在它们之间传输的标准。

在日常的网络应用中，没有严格区分 FTP 和 FTP 协议的说法，默认情况下这两者拥有同样的定义。

1.1.1.2　FTP 的作用

就像 FTP 的定义“File Transfer Protocol（文件传输协议）”一样，FTP 的主要作用就是让用户连接上一个运行着 FTP 服务器程序的远程计算机，查看远程计算机有哪些文件，然后把用户需要的文件从远程计算机上复制到本地计算机（下载），或把本地计算机的文件送到远程计算机上去（上传）。

1.1.2　FTP 传输方式

作为一个网络协议，FTP 肯定存在网络的交互性，而数据传输也肯定是通过网络数据交互实现的，在深入了解 FTP 的其他特性之前，很多读者可能会问一个问题：为什么 FTP 可以不考虑操作系统的因素？它是如何实现在不同操作系统之间进行数据完整交互的？要解决这个问题，就需要对 FTP 的传输方式进行简单了解。

FTP 的传输有两种方式：ASCII 传输方式和二进制数据传输方式。

在不同的情况下，FTP 需要使用不同的传输方式进行数据提交和收发。如果数据的传输方式出现错误，那么很可能传送的文件将出现错误，导致无法使用或者数据错乱。

1.1.2.1 ASCII 传输方式

ASCII 传输方式是比较独特的，因为如果采用了这种方式，那被传送的文件实际上是经过改变的，也就是说服务器上的文件和用户端的文件可能存在不一样的情况。采用这样的方式进行传输的目的其实恰恰就是为了保证文件以正确的方式存在于正确的系统之中。

比如，假定用户正在复制的文件包含简单的 ASCII 码文本，如果在远程机器上运行的不是 UNIX 系统，当文件传输时，FTP 通常会自动地调整文件的内容以便于把文件解释成目标计算机存储文本文件的格式，也就是说 FTP 在工作的时候，可能已经将文件改变了。

但是有可能出现其他情况：用户正在传输的文件包含的不是文本文件，它们可能是程序、数据库、字处理文件或者压缩文件（尽管字处理文件包含的大部分是文本，其中也包含指示页尺寸、字库等信息的非打印字符）。这就需要在复制任何非文本文件之前，用 FTP 的 Binary 命令告诉 FTP 需要采用逐字复制，不要对这些文件进行任何处理，不能改变。这也就是另一种传输方式：二进制传输。

> **提示**：有时候，从 FTP 服务器上下载文件，发现部分文件下载后大小有出入，这就是使用不同的传输方式造成的。

1.1.2.2 二进制传输方式（Binary）

在二进制传输中，FTP 会保存文件的位序，以便原始和复制的是逐位一一对应的，也就是强制保证文件的数据结构不做更改——即使目的计算机上包含位序列的文件也是没意义的。例如，Mac 苹果系统以二进制方式传送可执行文件到 Windows 系统，在对方系统上，此文件是不能执行的。

如果用户在 ASCII 方式下传输二进制文件，即使不需要也仍会进行转译。这会使传输稍微变慢，也会损坏数据，使文件变得不可用。如果用户知道这两台机器是同样的，则 FTP 的二进制传输方式对文本文件和数据文件都是有效的。

一般情况下，二进制传输方式用来传送可执行文件、压缩文件和图片文件。

1.1.2.3　ASCII 和二进制传输方式的区别

ASCII 传输方式和二进制（Binary）传输方式的区别是回车换行的处理。在二进制（Binary）传输方式下，FTP 不对数据进行任何处理；ASCII 传输方式则将回车换行转换为本机的回车字符。

> **提示**：UNIX 下的回车换行符是“\n”，Windows 下是“\r\n”，Mac 苹果下是“\r”。

ASCII 模式下会转换文件，不能说是不同系统对回车换行解释不同，而是不同的系统有不同的行结束符。UNIX 系统下行结束符是一个字节，即十六进制的 0A，而 Windows 系统是两个字节，即十六进制的 0D0A，所以当用户用 ASCII 方式从 UNIX 的 FTP Server 下载文件到 Windows 系统上时（不管是二进制还是文本文件），每检测到一个字节是 0A，就会自动插入一个 0D，所以如果用户的文件是二进制文件，如可执行文件、压缩包等，经过传输就不可用了。如果用户的文件就是 UNIX 下的文本文件，则用 ASCII 传输方式是正确的，要是误用了二进制（Binary）传输方式，则用户在 Windows 上看这个文件是没有换行的，里面是一个个的黑方块。如图 1.1 所示。

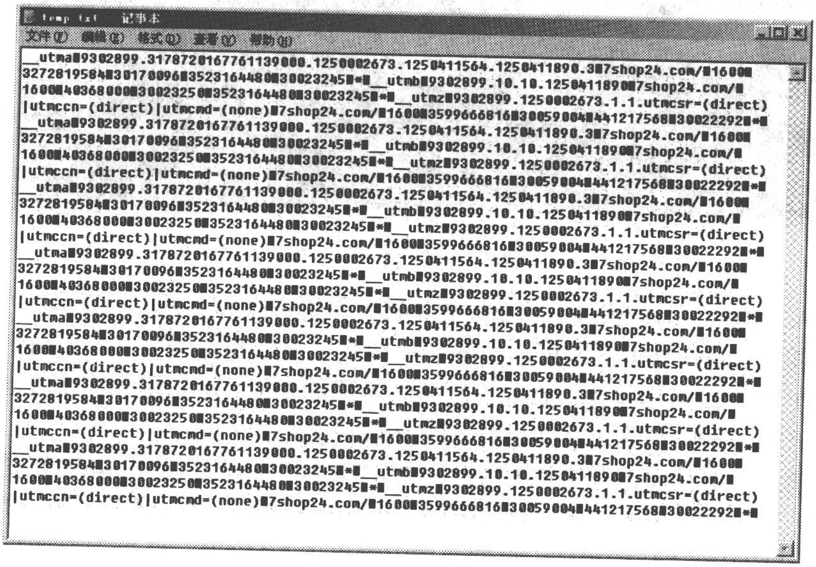

图 1.1